

Marina Gavrilova et al. (Eds.)

LNCS 3984

Computational Science and Its Applications – ICCSA 2006

International Conference
Glasgow, UK, May 2006
Proceedings, Part V

5
Part V

 Springer

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Marina Gavrilova Osvaldo Gervasi
Vipin Kumar C.J. Kenneth Tan
David Taniar Antonio Laganà
Youngsong Mun Hyunseung Choo (Eds.)

Computational Science and Its Applications – ICCSA 2006

International Conference
Glasgow, UK, May 8-11, 2006
Proceedings, Part V

 Springer

Volume Editors

Marina Gavrilova
University of Calgary, Canada
E-mail: marina@cpsc.ucalgary.ca

Oswaldo Gervasi
University of Perugia, Italy
E-mail: ogervasi@computer.org

Vipin Kumar
University of Minnesota, Minneapolis, USA
E-mail: kumar@cs.umn.edu

C.J. Kenneth Tan
OptimaNumerics Ltd., Belfast, UK
E-mail: cjtan@optimanumerics.com

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

Antonio Laganà
University of Perugia, Italy
E-mail: lag@unipg.it

Youngsong Mun
SoongSil University, Seoul, Korea
E-mail: mun@computing.soongsil.ac.kr

Hyunseung Choo
Sungkyunkwan University, Suwon, Korea
E-mail: choo@ece.skku.ac.kr

Library of Congress Control Number: 2006925086

CR Subject Classification (1998): F, D, G, H, I, J, C.2-3

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

ISSN 0302-9743
ISBN-10 3-540-34079-3 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-34079-9 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11751649 06/3142 5 4 3 2 1 0

Preface

This five-volume set was compiled following the 2006 International Conference on Computational Science and its Applications, ICCSA 2006, held in Glasgow, UK, during May 8–11, 2006. It represents the outstanding collection of almost 664 refereed papers selected from over 2,450 submissions to ICCSA 2006.

Computational science has firmly established itself as a vital part of many scientific investigations, affecting researchers and practitioners in areas ranging from applications such as aerospace and automotive, to emerging technologies such as bioinformatics and nanotechnologies, to core disciplines such as mathematics, physics, and chemistry. Due to the sheer size of many challenges in computational science, the use of supercomputing, parallel processing, and sophisticated algorithms is inevitable and becomes a part of fundamental theoretical research as well as endeavors in emerging fields. Together, these far-reaching scientific areas contributed to shaping this conference in the realms of state-of-the-art computational science research and applications, encompassing the facilitating theoretical foundations and the innovative applications of such results in other areas.

The topics of the refereed papers span all the traditional as well as emerging computational science realms, and are structured according to the five major conference themes:

- Computational Methods, Algorithms and Applications
- High-Performance Technical Computing and Networks
- Advanced and Emerging Applications
- Geometric Modeling, Graphics and Visualization
- Information Systems and Information Technologies

Moreover, submissions from 31 workshops and technical sessions in areas such as information security, mobile communication, grid computing, modeling, optimization, computational geometry, virtual reality, symbolic computations, molecular structures, Web systems and intelligence, spatial analysis, bioinformatics and geocomputations, are included in this publication. The continuous support of computational science researchers has helped ICCSA to become a firmly established forum in the area of scientific computing.

We recognize the contribution of the International Steering Committee and sincerely thank the International Program Committee for their tremendous support in putting this conference together, the near 800 referees for their diligent work, and the IEE European Chapter for their generous assistance in hosting the event.

We also thank our sponsors for their continuous support without which this conference would not be possible.

Finally, we thank all authors for their submissions and all invited speakers and conference attendants for making the ICCSA Conference truly one of the premium events on the scientific community scene, facilitating exchange of ideas, fostering new collaborations, and shaping the future of computational science.

May 2006

Marina L. Gavrilova
Oswaldo Gervasi

on behalf of the co-editors
Vipin Kumar
Chih Jeng Kenneth Tan
David Taniar
Antonio Laganà
Youngsong Mun
Hyunseung Choo

Organization

ICCSA 2006 was organized by the Institute of Electrical Engineers (IEE)(UK), the University of Perugia (Italy), Calgary University (Canada) and Minnesota University (USA).

Conference Chairs

Vipin Kumar (University of Minnesota, Minneapolis, USA), Honorary Chair
Marina L. Gavrilova (University of Calgary, Calgary, Canada), Conference
Co-chair, Scientific
Osvaldo Gervasi (University of Perugia, Perugia, Italy), Conference Co-chair,
Program

Steering Committee

Vipin Kumar (University of Minnesota, USA)
Marina L. Gavrilova (University of Calgary, Canada)
Osvaldo Gervasi (University of Perugia, Perugia, Italy)
C. J. Kenneth Tan (OptimaNumerics, UK)
Alexander V. Bogdanov (Institute for High Performance Computing
and Data Bases, Russia)
Hyunseung Choo (Sungkyunkwan University, Korea)
Andres Iglesias (University of Cantabria, Spain)
Antonio Laganà (University of Perugia, Italy)
Heow-Pueh Lee (Institute of High Performance Computing, Singapore)
Youngsong Mun (Soongsil University, Korea)
David Taniar (Monash University, Australia)

Workshop Organizers

Applied Cryptography and Information Security (ACIS 2006)

Sherman S.M. Chow (New York University, USA)
Joseph K. Liu (University of Bristol, UK)
Patrick Tsang (Dartmouth College, USA)
Duncan S Wong (City University of Hong Kong, Hong Kong)

Approaches or Methods of Security Engineering (AMSE 2006)

Haeng Kon Kim (Catholic University of Daegu, Korea)
Tai-hoon Kim (Korea Information Security Agency, Korea)

Authentication, Authorization and Accounting (AAA 2006)
Haeng Kon Kim (Catholic University of Daegu, Korea)

Computational Geometry and Applications (CGA 2006)
Marina Gavrilova (University of Calgary, Calgary, Canada)

Data Storage Devices and Systems (DSDS 2006)
Yeonseung Ryu (Myongji University, Korea)
Junho Shim (Sookmyong Womens University, Korea)
Youjip Won (Hanyang University, Korea)
Yongik Eom (Seongkyunkwan University, Korea)

Embedded System for Ubiquitous Computing (ESUC 2006)
Tei-Wei Kuo (National Taiwan University, Taiwan)
Jiman Hong (Kwangwoon University, Korea)

4th Technical Session on Computer Graphics (TSCG 2006)
Andres Iglesias (University of Cantabria, Spain)
Deok-Soo Kim (Hanyang University, Korea)

GeoComputation (GC 2006)
Yong Xue (London Metropolitan University, UK)

Image Processing and Computer Vision (IPCV 2006)
Jiawan Zhang (Tianjin University, China)

**Intelligent Services and the Synchronization in Mobile
Multimedia Networks (ISS 2006)**
Dong Chun Lee (Howon University, Korea)
Kuinam J Kim (Kyonggi University, Korea)

**Integrated Analysis and Intelligent Design Technology
(IAIDT 2006)**
Jae-Woo Lee (Konkuk University, Korea)

Information Systems Information Technologies (ISIT 2006)
Youngsong Mun (Soongsil University, Korea)

Information Engineering and Applications in Ubiquitous Computing Environments (IEAUCE 2006)

Sangkyun Kim (Yonsei University, Korea)

Hong Joo Lee (Dankook University, Korea)

Internet Communications Security (WICS 2006)

Sierra-Camara José Maria (University Carlos III of Madrid, Spain)

Mobile Communications (MC 2006)

Hyunseung Choo (Sungkyunkwan University, Korea)

Modelling Complex Systems (MCS 2006)

John Burns (Dublin University, Ireland)

Ruili Wang (Massey University, New Zealand)

Modelling of Location Management in Mobile Information Systems (MLM 2006)

Dong Chun Lee (Howon University, Korea)

Numerical Integration and Applications (NIA 2006)

Elise de Doncker (Western Michigan University, USA)

Specific Aspects of Computational Physics and Wavelet Analysis for Modelling Suddenly-Emerging Phenomena in Nonlinear Physics, and Nonlinear Applied Mathematics (PULSES 2006)

Carlo Cattani (University of Salerno, Italy)

Cristian Toma (Titu Maiorescu University, Romania)

Structures and Molecular Processes (SMP 2006)

Antonio Laganà (University of Perugia, Perugia, Italy)

Optimization: Theories and Applications (OTA 2006)

Dong-Ho Lee (Hanyang University, Korea)

Deok-Soo Kim (Hanyang University, Korea)

Ertugrul Karsak (Galatasaray University, Turkey)

Parallel and Distributed Computing (PDC 2006)

Jiawan Zhang (Tianjin University, China)

Pattern Recognition and Ubiquitous Computing (PRUC 2006)

Jinok Kim (Daegu Haany University, Korea)

Security Issues on Grid/Distributed Computing Systems (SIGDCS 2006)

Tai-Hoon Kim (Korea Information Security Agency, Korea)

Technologies and Techniques for Distributed Data Mining (TTDDM 2006)

Mark Baker (Portsmouth University, UK)

Bob Nichol (Portsmouth University, UK)

Ubiquitous Web Systems and Intelligence (UWSI 2006)

David Taniar (Monash University, Australia)

Eric Pardede (La Trobe University, Australia)

Ubiquitous Application and Security Service (UASS 2006)

Yeong-Deok Kim (Woosong University, Korea)

Visual Computing and Multimedia (VCM 2006)

Abel J. P. Gomes (University Beira Interior, Portugal)

Virtual Reality in Scientific Applications and Learning (VRSAL 2006)

Oswaldo Gervasi (University of Perugia, Italy)

Antonio Riganelli (University of Perugia, Italy)

Web-Based Learning (WBL 2006)

Woochun Jun Seoul (National University of Education, Korea)

Program Committee

Jemal Abawajy (Deakin University, Australia)
Kenny Adamson (EZ-DSP, UK)
Srinivas Aluru (Iowa State University, USA)
Mir Atiqullah (Saint Louis University, USA)
Frank Baetke (Hewlett Packard, USA)
Mark Baker (Portsmouth University, UK)
Young-Cheol Bang (Korea Polytechnic University, Korea)
David Bell (Queen's University of Belfast, UK)
Stefania Bertazzon (University of Calgary, Canada)
Sergei Bessmamyatnikh (Duke University, USA)
J. A. Rod Blais (University of Calgary, Canada)
Alexander V. Bogdanov (Institute for High Performance Computing
and Data Bases, Russia)
Peter Brezany (University of Vienna, Austria)
Herve Bronnimann (Polytechnic University, NY, USA)
John Brooke (University of Manchester, UK)
Martin Buecker (Aachen University, Germany)
Rajkumar Buyya (University of Melbourne, Australia)
Jose Sierra-Camara (University Carlos III of Madrid, Spain)
Shyi-Ming Chen (National Taiwan University of Science and Technology,
Taiwan)
YoungSik Choi (University of Missouri, USA)
Hyunseung Choo (Sungkyunkwan University, Korea)
Bastien Chopard (University of Geneva, Switzerland)
Min Young Chung (Sungkyunkwan University, Korea)
Yiannis Cotronis (University of Athens, Greece)
Danny Crookes (Queen's University of Belfast, UK)
Jose C. Cunha (New University of Lisbon, Portugal)
Brian J. d'Auriol (University of Texas at El Paso, USA)
Alexander Degtyarev (Institute for High Performance Computing
and Data Bases, Russia)
Frederic Desprez (INRIA, France)
Tom Dhaene (University of Antwerp, Belgium)
Beniamino Di Martino (Second University of Naples, Italy)
Hassan Diab (American University of Beirut, Lebanon)
Ivan Dimov (Bulgarian Academy of Sciences, Bulgaria)
Iain Duff (Rutherford Appleton Laboratory, UK and CERFACS, France)
Thom Dunning (NCSA and University of Illinois, USA)
Fabrizio Gagliardi (Microsoft, USA)
Marina L. Gavrilova (University of Calgary, Canada)
Michael Gerndt (Technical University of Munich, Germany)
Osvaldo Gervasi (University of Perugia, Italy)
Bob Gingold (Australian National University, Australia)
James Glimm (SUNY Stony Brook, USA)

Christopher Gold (Hong Kong Polytechnic University, Hong Kong)
Yuriy Gorbachev (Institute of High Performance Computing
and Information Systems, Russia)
Andrzej Goscinski (Deakin University, Australia)
Jin Hai (Huazhong University of Science and Technology, China)
Ladislav Hluchy (Slovak Academy of Science, Slovakia)
Xiaohua Hu (Drexel University, USA)
Eui-Nam John Huh (Seoul Women's University, Korea)
Shen Hong (Japan Advanced Institute of Science and Technology, Japan)
Paul Hovland (Argonne National Laboratory, USA)
Andres Iglesias (University of Cantabria, Spain)
Peter K. Jimack (University of Leeds, UK)
In-Jae Jeong (Hanyang University, Korea)
Chris Johnson (University of Utah, USA)
Benjoe A. Juliano (California State University at Chico, USA)
Peter Kacsuk (MTA SZTAKI Research Institute, Hungary)
Kyung Wo Kang (KAIST, Korea)
Carl Kesselman (USC/ Information Sciences Institute, USA)
Daniel Kidger (Quadrics, UK)
Haeng Kon Kim (Catholic University of Daegu, Korea)
Jin Suk Kim (KAIST, Korea)
Tai-Hoon Kim (Korea Information Security Agency, Korea)
Yoonhee Kim (Syracuse University, USA)
Mike Kirby (University of Utah, USA)
Dieter Kranzmueller (Johannes Kepler University Linz, Austria)
Deok-Soo Kim (Hanyang University, Korea)
Vipin Kumar (University of Minnesota, USA)
Domenico Laforenza (Italian National Research Council, Italy)
Antonio Laganà (University of Perugia, Italy)
Joseph Landman (Scalable Informatics LLC, USA)
Francis Lau (The University of Hong Kong, Hong Kong)
Bong Hwan Lee (Texas A&M University, USA)
Dong Chun Lee (Howon University, Korea)
Dong-Ho Lee (Institute of High Performance Computing, Singapore)
Sang Yoon Lee (Georgia Institute of Technology, USA)
Tae-Jin Lee (Sungkyunkwan University, Korea)
Bogdan Lesyng (ICM Warszawa, Poland)
Zhongze Li (Chinese Academy of Sciences, China)
Laurence Liew (Scalable Systems Pte, Singapore)
David Lombard (Intel Corporation, USA)
Emilio Luque (University Autònoma of Barcelona, Spain)
Michael Mascagni (Florida State University, USA)
Graham Megson (University of Reading, UK)
John G. Michopoulos (US Naval Research Laboratory, USA)
Edward Moreno (Euripides Foundation of Marília, Brazil)

Youngsong Mun (Soongsil University, Korea)
 Jiri Nedoma (Academy of Sciences of the Czech Republic, Czech Republic)
 Genri Norman (Russian Academy of Sciences, Russia)
 Stephan Olariu (Old Dominion University, USA)
 Salvatore Orlando (University of Venice, Italy)
 Robert Panoff (Shodor Education Foundation, USA)
 Marcin Paprzycki (Oklahoma State University, USA)
 Gyung-Leen Park (University of Texas, USA)
 Ron Perrott (Queen's University of Belfast, UK)
 Dimitri Plemenos (University of Limoges, France)
 Richard Ramaroson (ONERA, France)
 Rosemary Renaut (Arizona State University, USA)
 René S. Renner (California State University at Chico, USA)
 Paul Roe (Queensland University of Technology, Australia)
 Alexey S. Rodionov (Russian Academy of Sciences, Russia)
 Heather J. Ruskin (Dublin City University, Ireland)
 Ole Saastad (Scali, Norway)
 Muhammad Sarfraz (King Fahd University of Petroleum and Minerals,
 Saudi Arabia)
 Edward Seidel (Louisiana State University, USA and Albert-Einstein-Institut,
 Potsdam, Germany)
 Jie Shen (University of Michigan, USA)
 Dale Shires (US Army Research Laboratory, USA)
 Vaclav Skala (University of West Bohemia, Czech Republic)
 Burton Smith (Cray, USA)
 Masha Sosonkina (Ames Laboratory, USA)
 Alexei Sourin (Nanyang Technological University, Singapore)
 Elena Stankova (Institute for High Performance Computing and Data Bases,
 Russia)
 Gunther Stuer (University of Antwerp, Belgium)
 Kokichi Sugihara (University of Tokyo, Japan)
 Boleslaw Szymanski (Rensselaer Polytechnic Institute, USA)
 Ryszard Tadeusiewicz (AGH University of Science and Technology, Poland)
 C.J. Kenneth Tan (OptimaNumerics, UK and Queen's University
 of Belfast, UK)
 David Taniar (Monash University, Australia)
 John Taylor (Streamline Computing, UK)
 Ruppa K. Thulasiram (University of Manitoba, Canada)
 Pavel Tvrdik (Czech Technical University, Czech Republic)
 Putchong Uthayopas (Kasetsart University, Thailand)
 Mario Valle (Swiss National Supercomputing Centre, Switzerland)
 Marco Vanneschi (University of Pisa, Italy)
 Piero Giorgio Verdini (University of Pisa and Istituto Nazionale di Fisica
 Nucleare, Italy)
 Jesus Vigo-Aguar (University of Salamanca, Spain)

Jens Volkert (University of Linz, Austria)
Koichi Wada (University of Tsukuba, Japan)
Stephen Wismath (University of Lethbridge, Canada)
Kevin Wadleigh (Hewlett Packard, USA)
Jerzy Wasniewski (Technical University of Denmark, Denmark)
Paul Watson (University of Newcastle Upon Tyne, UK)
Jan Weglarz (Poznan University of Technology, Poland)
Tim Wilkens (Advanced Micro Devices, USA)
Roman Wyrzykowski (Technical University of Czestochowa, Poland)
Jinchao Xu (Pennsylvania State University, USA)
Chee Yap (New York University, USA)
Osman Yasar (SUNY at Brockport, USA)
George Yee (National Research Council and Carleton University, Canada)
Yong Xue (Chinese Academy of Sciences, China)
Igor Zacharov (SGI Europe, Switzerland)
Xiaodong Zhang (College of William and Mary, USA)
Aledander Zhmakin (SoftImpact, Russia)
Krzysztof Zielinski (ICS UST / CYFRONET, Poland)
Albert Zomaya (University of Sydney, Australia)

Sponsoring Organizations

Institute of Electrical Engineers (IEE), UK
University of Perugia, Italy
University of Calgary, Canada
University of Minnesota, USA
Queen's University of Belfast, UK
The European Research Consortium for Informatics and Mathematics (ERCIM)
The 6th European Framework Project "Distributed European Infrastructure
for Supercomputing Applications" (DEISA)
OptimaNumerics, UK
INTEL
AMD

Table of Contents – Part V

Workshop on Parallel and Distributed Computing (PDC 2006)

Resource Demand Prediction-Based Grid Resource Transaction Network Model in Grid Computing Environment <i>In Kee Kim, Jong Sik Lee</i>	1
A CGM Algorithm Solving the Longest Increasing Subsequence Problem <i>David Semé</i>	10
Computer Assisted Source-Code Parallelisation <i>Peter J. Vidler, Michael J. Pont</i>	22
A Template Language for Agent Construction <i>Li Xiaohong, Feng Zhiyong, Li tie, Lv Li</i>	32
Efficient Parallel Processing for K -Nearest-Neighbor Search in Spatial Databases <i>Yunjun Gao, Ling Chen, Gencai Chen, Chun Chen</i>	39
An Adaptive Mobile System Using Mobile Grid Computing in Wireless Network <i>Jehwan Oh, Seunghwa Lee, Eunseok Lee</i>	49
Comparison of Allocation Algorithms for Mesh Structured Networks with Using Multistage Simulation <i>Leszek Koszalka, Dominik Lisowski, Iwona Pozniak-Koszalka</i>	58
The Election Problem in Asynchronous Distributed Systems with Bounded Faulty Processes <i>SeongHoon Park</i>	68
Improving the Genetic Algorithms Performance in Simple Assembly Line Balancing <i>Seren Özmehmet Tasan, Semra Tunali</i>	78
Reformulation and Solution Approaches for an Integrated Scheduling Model <i>Herbert Jodlbauer, Sonja Reitner, Andreas Weidenhiller</i>	88

Safety of a Client-Based Version Vector Consistency Protocol of Session Guarantees <i>Jerzy Brzeziński, Cezary Sobaniec, Dariusz Wawrzyniak</i>	98
A New I/O Architecture for Improving the Performance in Large Scale Clusters <i>L.M. Sánchez García, Florin D. Isaila, Félix García Carballeira, Jesús Carretero Pérez, Rolf Rabenseifner, Panagiotis Adamidis</i>	108
Performance Modeling of a Fully Adaptive and Fault-Tolerant Wormhole Switching Strategy in 2-D Mesh <i>Farshad Safaei, Mahmood Fathy, Ahmad Khonsari, Mohamed Ould-Khaoua</i>	118
Parallelization of Simulations for Various Magnetic System Models on Small-Sized Cluster Computers with MPI <i>Frank Schurz, Dietmar Fey, Dmitri Berkov</i>	129
A New Reflective and Reliable Context-Oriented Event Service Architecture for Pervasive Computing <i>Sung Keun Song, Hee Yong Youn, Ungmo Kim</i>	139
X-Torus: A Variation of Torus Topology with Lower Diameter and Larger Bisection Width <i>Huaxi Gu, Qiming Xie, Kun Wang, Jie Zhang, Yunsong Li</i>	149
Feedback Vertex Sets in Rotator Graphs <i>Chiun-Chieh Hsu, Hon-Ren Lin, Hsi-Cheng Chang, Kung-Kuei Lin</i>	158
Efficient Longest Common Subsequence Computation Using Bulk-Synchronous Parallelism <i>Peter Krusche, Alexander Tiskin</i>	165
Simulation of Internet Transport Protocols for High Bandwidth-Delay Networks <i>Junsoo Lee</i>	175
Performance Evaluation of Parallel Systems Employing Roll-Forward Checkpoint Schemes <i>Gyung-Leen Park, Hee Yong Youn, Junghoon Lee, Chul Soo Kim, Bongkyu Lee, Sang Joon Lee, Wang-Cheol Song, Yung-Cheol Byun</i>	185

A Purely Distributed Approach for Coupling Scientific and Engineering Applications <i>Vicente Berbegall, L.A. Drummond, Gumersindo Verdú, Vicente Vidal</i>	192
A Monitoring and Visualization Tool and Its Application for a Network Enabled Server Platform <i>Raphael Bolze, Eddy Caron, Frederic Desprez, Georg Hoesch, Cyril Pontvieux</i>	202
Parallel Hash Join Algorithms for Dynamic Load Balancing in a Shared Disks Cluster <i>Aekyung Moon, Haengrae Cho</i>	214
Workshop on Security Issues on Grid/Distributed Computing Systems (SIGDCS 2006)	
Towards Reliable and Trustworthy Cooperation in Grid: A Pre-evaluating Set Based Trust Model <i>Xiangli Qu, Jingwei Zhong, Xuejun Yang</i>	224
A Spreading MIMO-OFDM Transmission Scheme for Wireless Mobile Environment <i>Sang Soon Park, Tae Jin Hwang, Juphil Cho, Heung Ki Baik</i>	236
A Security Auditing Approach Based on Mobile Agent in Grid Environments <i>Zhenghong Xiao, Changqin Huang, Fuyin Xu</i>	243
XML-Signcryption Based LBS Security Protocol Acceleration Methods in Mobile Distributed Computing <i>Namje Park, Howon Kim, Kyoil Chung, Sungwon Sohn, Dongho Won</i>	251
Optimization of a Simulation for 300mm FAB Semiconductor Manufacturing <i>DongSik Park, Youngshin Han, Chilgee Lee</i>	260
Performance Analysis Using the Two Kinds of Receiving Gain of Smart Antenna in IS20001X System <i>Sungsoo Ahn, Minsoo Kim, Jungsuk Lee</i>	269
An Improved Popescu's Authenticated Key Agreement Protocol <i>Eun-Jun Yoon, Kee-Young Yoo</i>	276

SVM Based False Alarm Minimization Scheme on Intrusion Prevention System <i>Gil-Han Kim, Hyung-Woo Lee</i>	284
Lightweight Wireless Intrusion Detection Systems Against DDoS Attack <i>Hyung-Woo Lee</i>	294
One-Time Password Authentication Scheme Using Smart Cards Providing User Anonymity <i>Eun-Jun Yoon, Kee-Young Yoo</i>	303
Loss Reduction in Distribution Networks Using Cyclic Best First Search <i>Sang-Yule Choi, Myong-Chul Shin, Jae-Sang Cha</i>	312
Short-Term Power Demand Forecasting Using Information Technology Based Data Mining Method <i>Sang-Yule Choi</i>	322
A Design of the Flexible Mobile Agents Based on Web <i>Yun Ji Na, Il Seok Ko, Gun Heui Han</i>	331
A Sales Agent Using Case-Based Reasoning and Rule-Based Reasoning for E-Commerce System <i>Yun Ji Na, Il Seok Ko, Jong Min Kwak</i>	338
A New Ciphering Method Associated with Evolutionary Algorithm <i>Fouzia Omary, Abdelaziz Mouloudi, Abderrahim Tragha, Abdelghani Bellaachia</i>	346
Power Distribution Automation System Using Information Technology Based Web Active Database <i>Sang-Yule Choi</i>	355
Workshop on Image Processing and Computer Vision (IPCV 2006)	
Alternative Target Density Functions for Radar Imaging <i>Askin Demirkol</i>	365
A Novel Image Restoration Algorithm Based on High-Dimensional Space Geometry <i>Wenming Cao, Mei-fen Xie, Shoujue Wang</i>	375

A Fast Image Retrieval System Based on Color-Space and Color-Texture Features <i>Chuen-Hornq Lin, Kai-Hung Chen, Yung-Kuan Chan</i>	384
Generation of Dynamic Heart Model Based on 4D Echocardiographic Images <i>Michał Chlebiej, Paweł Mikołajczak, Krzysztof Nowiński, Piotr Ścisło, Piotr Bala</i>	394
Object-Based Image Retrieval Using Dominant Color Pairs Between Adjacent Regions <i>Ki Tae Park, Young Shik Moon</i>	404
Real-Time Vision Tracking Algorithm <i>Edgar R. Arce-Santana, Jose M. Luna-Rivera, Daniel U. Campos-Delgado, Ulises Pineda-Rico</i>	412
Efficient Method to Perform Isomorphism Testing of Labeled Graphs <i>Shu-Ming Hsieh, Chiun-Chieh Hsu, Li-Fu Hsu</i>	422
Camera Motion Parameter Estimation Technique Using 2D Homography and LM Method Based on Projective and Permutation Invariant Features <i>JeongHee Cha, GyeYoung Kim</i>	432
Automatic Generation Technique of Three-Dimensional Model Corresponding to Individual Vessels <i>Na-Young Lee, Gye-Young Kim, Hyung-Il Choi</i>	441
Modulating Energy Distribution of Reflected Light Based on Images <i>Zhanwei Li, Guolin Duan, Jizhou Sun, Lijuan Sun, Xinran Lv</i>	450
Workshop on Integrated Analysis and Intelligent Design Technology (IAIDT 2006)	
Aerodynamic Analysis on the Supersonic Separation of Air-Launching Rocker from the Mother Plane <i>Young Mu Ji, Young Shin Kim, Jae Woo Lee, Young Hwan Byun, Jun Sang Park</i>	457
Effect of Grid Resolution on the Statistics of Passive Scalar in an Injection-Driven Channel <i>Yang Na, Dongshin Shin, Seungbae Lee</i>	467

Test of Large Eddy Simulation in Complex Flow with High Schmidt Number <i>Yang Na, Seungmin Lee</i>	476
High-End Modeling and Simulation of Cookoff of HMX-Based Energetic Materials <i>Jack Jai-ick Yoh</i>	484
Multiojective Optimization Using Adjoint Gradient Enhanced Approximation Models for Genetic Algorithms <i>Sangho Kim, Hyoung-Seog Chung</i>	491
Development of Automated Generation Algorithm for Skipped Surface in Die Design <i>Sang-Jun Lee, Seung-Soo Lee, Jong-Hwa Kim, Yoon-Jung Kwon</i>	503
Development of Requirement Driven Design Concept Selection Process in Aerospace System <i>Hyeong-Uk Park, Mee-Young Park, Seung-Jin Lee, Jae-Woo Lee, Yung-Hwan Byun</i>	512
A TMO-Based Tele-operation Model: Supporting Real-Time Applications in Grid Environments <i>Chulgoon Kim, Karpjoo Jeong, Hanku Lee, MoonHae Kim, KumWon Cho, Segil Jeon, Jaehoon Ahn, Hyunho Ju</i>	522
Design Trade-Offs and Power Reduction Techniques for High Performance Circuits and System <i>Taikyeong T. Jeong, Anthony P. Ambler</i>	531
Cavitation Flow Analysis of Axisymmetric Bodies Moving in the Water <i>Changjin Lee, Doyoung Byun</i>	537
Workshop on Approaches or Methods of Security Engineering (AMSE 2006, Sess. B)	
Design and Implementation of Semantic Web Search System Using Ontology and Anchor Text <i>Nam-deok Cho, Eun-ser Lee</i>	546
Design Progress Management for Security Requirements in Ubiquitous Computing Using COQUALMO <i>Eun Ser Lee, Sang Ho Lee</i>	555

Web Document Classification Using Changing Training Data Set <i>Gilcheol Park, Seoksoo Kim</i>	565
Study on Contents Protection in M-Learning Environment <i>Jaekoo Song, Mingyun Kang, Seoksoo Kim</i>	575
Design of Security Session Reuse in Content-Based Load Distribution Server <i>Seoksoo Kim, Kunhee Han</i>	584
Design of POC System in Ubiquitous Environment <i>Seoksoo Kim, Gilcheol Park</i>	591
The Performance Evaluation of OFDM/HL-16QAM System for Optimizing Image Transmission Quality in Wireless Fading <i>Jae-min Kwak, Yang-sun Lee, Sung-eon Cho</i>	600
Reliable Evaluations of URL Normalization <i>Sung Jin Kim, Hyo Sook Jeong, Sang Ho Lee</i>	609
Enhanced Misuse Case Model: A Security Requirement Analysis and Specification Model <i>Sang-soo Choi, So-yeon Kim, Gang-soo Lee</i>	618
An Analysis of Policy Provisioning Complexity in Accordance with the Application Attributes of the Policy-Based Network <i>Hyung-Jin Lim, Moonseong Kim, Dong-Young Lee, Tai-Myoung Chung</i>	626
Privacy Preserving Unsupervised Clustering over Vertically Partitioned Data <i>D.K. Tasoulis, E.C. Laskari, G.C. Meletiou, M.N. Vrahatis</i>	635
Process Development Methodology for U-Integrated Management System <i>Seong-Man Choi, MalRey Lee, Cheol-Jung Yoo, Ok-Bae Chang</i>	644
A Study on Agent-Based Integrated Security Management System for Managing Heterogeneous Firewall Systems <i>Dong-Young Lee, Hyung-Jin Lim, Tai M. Chung</i>	655
Optimization of Fuzzy Rules: Integrated Approach for Classification Problems <i>Yunjeong Kang, Malrey Lee, Yongseok Lee, Thomas M. Gatton</i>	665

A Cooperation Model Using Reinforcement Learning for Multi-agent <i>Malrey Lee, Jaedeuk Lee, Hye-Jin Jeong, YoungSoon Lee, Seongman Choi, Thomas M. Gatton</i>	675
Development of Network Event Analysis Algorithm Applying Association Rule <i>Seakjae Han, Wooyoung Soh</i>	682
A New Secure Oblivious Transfer Protocol <i>Soon-gohn Kim, Heau-jo Kang</i>	690
Analysis of Security Session Reusing in Distribution Server System <i>Tai-hoon Kim, Seoksoo Kim, Hee-Un Park, Myoung-sub Kim</i>	700
Clustered OFDMA in the Multi-path Fading Channel <i>Kyujin Lee, Kyesan Lee</i>	708
Distribution Antenna Diversity System According to Adaptive Correlation Method for OFDM-DS/CDMA in a Frequency Selective Fading Channel <i>Kyesan Lee, Eunam Huh</i>	717
General Tracks	
MIDAS: Detection of Non-technical Losses in Electrical Consumption Using Neural Networks and Statistical Techniques <i>Íñigo Monedero, Félix Biscarri, Carlos León, Jesús Biscarri, Rocío Millán</i>	725
Hyperbolic Voronoi Diagram <i>Zahra Nilfroushan, Ali Mohades</i>	735
Effects of Confinement on Chemical Reaction Equilibrium in Nanoporous Materials <i>William R. Smith, Martin Lísal, John K. Brennan</i>	743
Multi-channel Estimation in Multiple Antenna MB-OFDM UWB System for Home Entertainment Network <i>Myung-Sun Baek, So-Young Yeo, Byung-Jun Jang, Young-Hwan You, Hyoung-Kyu Song</i>	752
Compiler-Optimized Kernels: An Efficient Alternative to Hand-Coded Inner Kernels <i>José R. Herrero, Juan J. Navarro</i>	762

Noise Subspace Fuzzy C-Means Clustering for Robust Speech Recognition <i>J.M. Górriz, J. Ramírez, J.C. Segura, C.G. Puntonet, J.J. González</i>	772
Using Box-Muller with Low Discrepancy Points <i>Tim Pillards, Ronald Cools</i>	780
A Fast Integration Method and Its Application in a Medical Physics Problem <i>Shujun Li, Elise de Doncker, Karlis Kaugars, Haisen S. Li</i>	789
Payment in a Kiosk Centric Model with Mobile and Low Computational Power Devices <i>Jesús Téllez Isaac, José Sierra Camara, Antonio Izquierdo Manzanares, Mildrey Carbonell Castro</i>	798
Survivable Mechanism for IEEE 802.11 WLAN Improvements <i>Flavio E. de Deus, Ricardo Staciarini Puttini, Luis Molinaro, Joseph Kabara, Luis Javier García Villalba</i>	808
Proposal of a System for Searching and Indexing Heterogeneous Vulnerabilities Databases <i>Robson de Oliveira, Fabio Buiati, Luis Javier García Villalba, Daniel Almendra, L. Pulcineli, Rafael de Sousa, Cláudia Jacy Barenco Abbas</i>	819
Performance Analysis of Dynamic Host Isolation System in Wireless Mobile Networks <i>Hyuncheol Kim, Seongjin Ahn, Junkyun Choi</i>	829
Meta-model Driven Collaborative Object Analysis Process for Production Planning and Scheduling Domain <i>Chang Ouk Kim, Jun-Geol Baek, Jin Jun</i>	839
Response Against Hacking and Malicious Code in P2P <i>Wongoo Lee, Sijung Kim, Bonghan Kim</i>	851
Two Efficient and Secure Authentication Schemes Using Smart Cards <i>Youngsook Lee, Junghyun Nam, Seungjoo Kim, Dongho Won</i>	858
Location-Aware Agent Using Data Mining for the Distributed Location-Based Services <i>Jaewan Lee, Romeo Mark A. Mateo, Bobby D. Gerardo, Sung-Hyun Go</i>	867

An Empirical Development Case of a Software-Intensive System Based on the Rational Unified Process <i>Kilsup Lee</i>	877
Color Preference and Personality Modeling Using Fuzzy Reasoning Rule <i>Am-Suk Oh, Tae-Jung Lho, Jang-Woo Kwon, Kwang-Baek Kim</i>	887
The Development of Reliability Verification Tool of RFID Tag for Effective Product Control Systems <i>Ki-Uk Kim, Hyun-Suk Hwang, Bong-Je Kim, Su-Hwan Jeong, Chang-Soo Kim</i>	895
Avoidance of State Explosion Using Dependency Analysis in Model Checking Control Flow Model <i>Sachoun Park, Gihwon Kwon</i>	905
Design and Implementation of Web Usage Mining System Using Page Scroll <i>IL Kim, Bong-Joon Choi, Kyoo-Seok Park</i>	912
A Security Architecture for Adapting Multiple Access Control Models to Operating Systems <i>Jung-Sun Kim, SeungYong Lee, Minsoo Kim, Jae-Hyun Seo, Bong-Nam Noh</i>	922
Rotor Design for the Performance Optimization of Canard Rotor/Wing Aircraft <i>Jae-Woo Lee, Kwon-Su Jeon, Min-Ji Kim, Yung-Hwan Byun, Chang J. Kim, Yung H. Yu</i>	932
Process Decomposition and Choreography for Distributed Scientific Workflow Enactment <i>Jae-Yoon Jung, Wookey Lee, Suk-Ho Kang</i>	942
Adaptive Multi-carrier Direct-Sequence CDMA System Using Fast-Frequency-Hopping <i>Kyesan Lee, Gigan Lee</i>	952
Object Modeling for Mapping XML Document Represented in XML-GDM to UML Class Diagram <i>Dae-Hyeon Park, Chun-Sik Yoo, Yong-Sung Kim, Soon-Ja Yeom</i>	958
A Two-Phase Local Server Security Model Based on XML Certificate <i>Yong-Hwa Kim, Jin-Sung Kim, Yong-Sung Kim, Jang-Sup Shim</i>	968

Integrated Object Modeling for Web-Based XML Application Documents <i>Chun-Sik Yoo, Jin-Sung Kim, Yong-Sung Kim, Jang-Sup Shim</i>	979
Model of Generating SMIL Document Using Temporal Scripts of Animation Component <i>Chun-Sik Yoo, He-Jue Eun, Yong-Sung Kim, Jang-Sup Shim</i>	990
Marginal Bone Destructions in Dental Radiography Using Multi-template Based on Internet Services <i>Yonghak Ahn, Oksam Chae</i>	1001
The Band Selection Algorithm in Supervised Classification Using Mixed-Pixels and Canonical Correlation Analysis <i>Hoon Chang, Hwan-Hee Yoo, Hong Sok Kim</i>	1010
Domain Analysis for Components Based Developments <i>Ha-Jin Hwang</i>	1018
Author Index	1029

Resource Demand Prediction-Based Grid Resource Transaction Network Model in Grid Computing Environment*

In Kee Kim and Jong Sik Lee

School of Computer Science and Information Engineering,
Inha University,
#253, Yonghyun-Dong, Nam-Ku,
Incheon 402-751, South Korea
md10002@naver.com,
jslee@inha.ac.kr

Abstract. This paper reviews existing grid resource transaction models in grid computing environment and proposes an efficient market mechanism-based grid resource transaction model. This model predicts a future grid resource demand of grid users and suggests a reasonable transaction price of each resource to customers and resource providers. The suggestion of transaction price infers the more transactions between customers and providers and reduces a response time after ordering resource. In order to improve accuracy of transaction price prediction, microeconomics-based statistics approach is applied to this grid resource transaction model. For performance evaluation, this paper measures resource demand response time, and number of transactions. This model works on the less 72.39% of response time and the more 162.56% of the number of transactions than those of single auction model and double auction model.

1 Introduction

There are tremendous demands on grid computing to solve computation-intensive problems. High-cost super computing and cluster computing were applied to solve these computation-intensive problems in the past. Now grid computing is taking over that role [1]. Grid computing integrates massive amount of geologically distributed resources to solve complicated computation-intensive problems like scientific problems of real world [2] and demand for grid computing is increasing as time goes on. Grid computing does not have resource limitation and is able to allocate and remove resources dynamically [3]. Therefore, transaction network model which can provide resource at reasonable transaction price when the grid user requests resources is essential in grid computing. Market and price decision mechanism of economics were applied to most of the transaction models. Market and Price decision mechanism is being used as a control tool to allocate grid computing resources [4].

In this paper, we propose Resource demand Prediction-based Grid Resource Transaction network (RPGRT) model. This model is improved from existing transaction

* This work is supported by INHA UNIVERSITY Research Grant.

network model. RPGRT model introduced prediction method for prediction user's demand for resources. It also adapted two methods for the transaction price decision. We have conducted two experiments to prove performance of RPGRT model. In first experiment, we decided the optimized ratio for two price decision models using empirical result. In second experiment, we measured reduction rate of response time and improvement rate of resource transaction by comparing RPGRT model with existing models.

2 Related Work

Resource management for using and dynamically allocating computer resource is very significant as demand of grid computing increases. Many models have been proposed to manage resources of grid computing. Buyya proposed distributed economic structure called GRid Architecture for Computational Economy (GRACE) [4] which allocates resources and controls supply and demand of ready-to-use resources. GRACE adapted market mechanism of economics and now applied in a resource management. Market mechanism can accurately describe resource allocation and removal of grid computing.

Tender/Contract-Net Model: Tender/contract-net model [4] is widely used models in distributed computing environment. This is modeled contract mechanism using economics fields for managing to service and product transaction. This model helps customer to find GSP prefer to execute jobs. When a customer propose price to grid resource broker, GSPs bid to grid resource broker. When grid resource broker finds suitable GSP, broker connects customer and GSP.

Single Auction Model: Single auction model [4] is widely used to real market such as e-commerce web sites. This model consists of three parts in grid computing environment. There are single grid resource owner, single auctioneer, and many customers. An auctioneer decides convincing rules of single auction. A grid resource owner provides grid resources and customers offer bid for grid resources. Customers increase bid price continuously. Consequently, the highest bidding price of customer wins single auction.

Double Auction Model: Double auction model is the most noticed model in recent days [5]. Unlike the standard single auction theory where trading mechanism is controlled by single seller, double auction model has both seller and buyer who bid mutually. Normally, bidding price starts at high price for a seller and low for buyer. Sellers and buyers have their own unique price elasticity [6]. As an auction progresses, a seller will bid by lowering price depends on seller's price elasticity and a buyer will bid by increasing price depends on buyer's price elasticity. When bidding price of a seller and buyer meet the market equilibrium [7], transaction will be made. Double auction model well represent the market transaction of the real world. Because of this, double auction model is well noticed and used in sophisticated economic model like trading agent. However, existing models like double auction model have two problems. In next section, we will address these two problems and propose RPGRT model to solve the problems.

3 Resource Demand Prediction-Based Grid Resource Transaction Network (RPGRT) Model

We reviewed existing grid resource transaction model based on GRACE in section 2. Out of those two problems we stated above the first problem is that they cannot dynamically adapt themselves to the rapid changes in grid resource demand. Because existing models are not able to predict the amount of resource that grid users demand. Another problem is not having standard transaction price. Because of this, it will take very long time and even worse no transaction may be made if resource provider and grid user wrongly set the bidding price. Double auction model also can be affected when initial bidding price is wrongly configured. It will increase response time and affects the number of transactions. We proposed RPGRT model to solve problems existing models have. We introduced mechanism that can predict grid resource demand of grid user in this RPGRT model. RPGRT model predicts and provides grid resource demand based on past and present data. Price is determined by provided resource from predicting and actual grid resource demand of grid user. Two different kinds of algorithm are applied in price decision due to the diversity of grid users. The goal of RPGRT model is to have more numbers of transactions by having faster response time compare to existing models.

To predict grid resource demand of grid user, we used to second-order exponential-smoothing prediction method [8] in RPGRT model. It is possible to reliably predict using data from the past and present by adapting this prediction mechanism. This prediction method is represented in (1) [8]. \hat{D} is estimated demand of grid user and D is real grid resource demand of grid user. d is current time and present T show the time elapse. α is smoothing constant and normally have value of $0 \leq \alpha \leq 1$. S_d is first-order exponential smoothing prediction model and $S_d(2)$ is double-smoothed statistic. And, they are expressed in (1).

$$\begin{aligned} \hat{D}(d+T) &= (2 + \frac{\alpha T}{1-\alpha})S_d - (1 + \frac{\alpha T}{1-\alpha})S_d(2) \\ S_d &= \alpha D(d) + (1-\alpha)S_{d-1}, S_d(2) = \alpha S_d + (1-\alpha)S_{d-1}(2) \end{aligned} \quad (1)$$

\hat{D} ; Estimated grid resource demand of grid user, D ; Grid resource demand of grid user d ; Current time, T ; Time elapse, α ; Smoothing constant, S_d ; First-order Exponential Smoothing Prediction model, $S_d(2)$; Double-smoothed statisti

In RPGRT model, grid user pays resource provider for the service and two algorithms for deciding price were applied. Two algorithms we used are the Cournot Model with Slight Variation (CMSV) [9], [10] and the Double Auction with Initial Price model (DAIP). In RPGRT model, grid users can choose from two price decision models depend on their own situation or purpose. These two methods are complementary to each other. Using the CMSV enables grid user to use resources quickly. However, the DAIP method may have slower response time, but it enables grid user to use resources at the price that are lower than the model originally proposed.

Cournot Model with Slight Variation (CMSV): Price decision making algorithm of the CMSV is showed in Fig.1. In order to adapt CMSV algorithm, the Trading Agent Competition (TAC)/Supply Chain Management (SCM) game [11] was referenced. This algorithm was also used in the jakaroo project [9] team of university of western sydney who participated in TAC/SCM game. *PredictionDemand* is quantity of grid user's grid resource demand that is measured using second-order exponential-smoothing method in RPGRT model, and *UserDemand* is actual quantity of grid user's grid resource demand. P_0 is pricing constant. It is theoretical price that occurs when market equilibrium occurs. When *PredictionDemand* are smaller than equal to *UserDemand*, transaction price of initial 80% of grid user becomes P_0 . And if *PredictionDemand* is bigger than *UserDemand* and smaller than $UserDemand + P_0/\gamma$, transaction price becomes $P_0 - \gamma \times (PredictionDemand - UserDemand)$. γ is depreciation coefficient and it is always larger than 0.

```

if ( PredictionDemand <= UserDemand ) Price = P0
else if( UserDemand < PredictionDemand && PredictionDemand <= UserDemand + P0/γ )
    Price = P0 - γ × (PredictionDemand - UserDemand)
else Price = 0

```

Fig. 1. Pricing algorithm of the CMSV

Double Auction with Initial Price (DAIP): Difference from existing double auction model is that initial price is acquired through the CMSV. Hence, grid users are able to decide the initial and the highest bidding cost based on the transaction price through the CMSV. The highest bidding price is configured to be less than or equal to the transaction price through the CMSV. Grid user starts bidding at initial bidding price and continues to bid by increasing its bidding price depends on its price elasticity. Initial bidding price of resource provider is set to be equal to the price from the CMSV. Then process continues to bid by lowering the price by the resource provider's price elasticity. Transaction occurs when the bid prices of grid user and resource provider meet the market equilibrium.

Fig.2-(a) shows the model layout that is constructed based on a price decision algorithm and demand predictability of grid resources we have described. RPGRT model is composed of *resource provider*, *broker* and *customer*. And these components have several sub-components.

Resource provider: It provides computing resources to the *customer*. It has sub-components of that are resource owner, resource manager, and resource provider coordinator. Resource owner is the actual resource owner. And resource owner provide resources to *customer*. Resource manager collects resources based on the predicted result from prediction component of *broker* and also manages them. Resource provider coordinator handles transactions through biddings and if there are shortage on resource, it request for additional resource from resource manager.

Broker: It predicts the grid resource demand of *customer* and decides the initial transaction price of resource. It also handles resource transactions between *customer* and *resource provider*. Sub-components are prediction component, pricing component and trading component. Prediction component predicts the grid resource demand

of *customer* using second-order exponential-smoothing prediction method and sends it to resource manager of *resource provider*. It also sends same information to pricing component and trading component. Pricing component determines the price based on the provided resources from *resource provider* using predict result of prediction component and actual requested grid resource demand of *customer*. The CMSV is used to determine price decision. Trading component handles actual resource transaction between *customer* and *resource provider*. It also manages bidding of *customer* and *resource provider*.

Customer: It receives each of grid user’s grid resource demand then request resource to *broker*. And, make transactions by bidding. It is composed of grid user and customer coordinator. Grid user is the group that request actual computing resource to perform. Customer coordinator request resource after receiving quantity of grid resource demand then decided whether to make a transaction or not in grid user’s perspective.

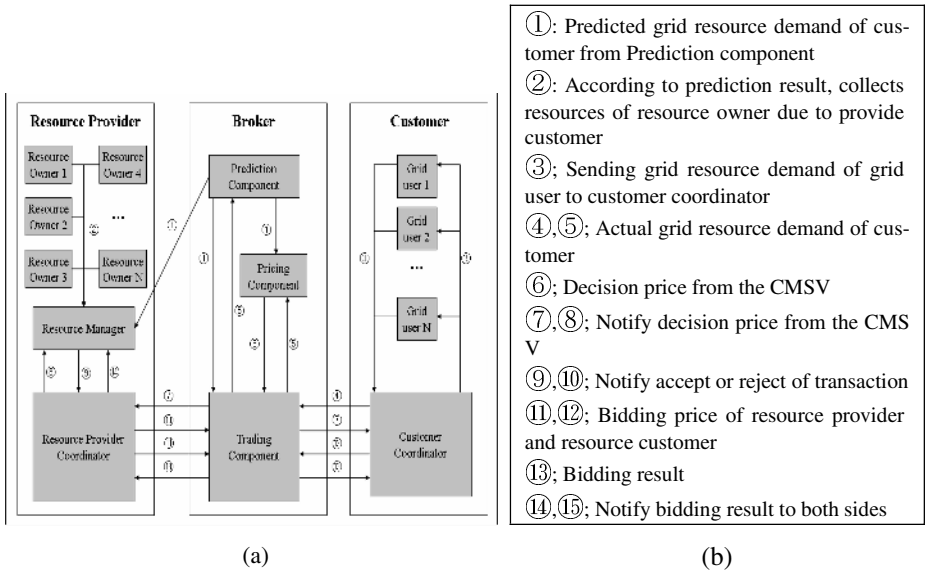


Fig. 2. (a) RPGRT model layout, (b) One cycle of data flow within RPGRT model

Fig.2-(b) shows the one cycle of data flow within the RPGRT model. The operating process of RPGRT model is mentioned as following. First, broker predicts grid resource demand of customer by using prediction component. With this predict, broker sends a request to resource manager of resource provider. Resource manager prepares exact quantity of predicted demand from resource owner. Customer transmits actual requested grid resource demand of grid user to the broker. Broker uses pricing component that uses CMSV to determine the initial transaction price. Grid users who want resource to be provided in rapid time will use this initial transaction price of CMSV. Then customer coordinator component of customer and resource provider component of resource provider attempt a bid by using DAIP method. When the transaction price is determined using this method, the transaction cost of remaining resource demand

will be determined using DAIP method. Shortage occurred from prediction error is provided through resource provider. After this procedure every transaction gets completed.

4 Analysis of Response Time

We analyzed the response time of RPGRT model and double auction model before the actual experiment. When we calculate the response time of double auction model, one bidding time of resource provider per each resource demand is TRP and total bidding time of resource provider per each resource demand is $\sum TRP$. Single bidding time of grid user is TGU and total bidding time of grid user is $\sum TGU$. Hence, if total resource demand of user is N , then response time for total resource demand of grid user in double auction model is $(N) \times (\sum TRP + \sum TGU)$. This equation can be expressed as shown in (2).

$$\begin{aligned} & \text{Total Response Time of Double Auction Model} \\ & = N \times 2 \times (\sum TBid) \quad (\because \sum TRP \approx \sum TGU) \end{aligned} \quad (2)$$

N ; total resource demand of grid user, $TBid$; one bidding time, $\sum TBid$; total bidding time per one resource demand resource provider or grid user, TRP ; one bidding time of resource provider, $\sum TRP$; total bidding time of resource provider of one resource demand, TGU ; one bidding time of grid user, $\sum TGU$; total bidding time of grid user of one resource demand

In RPGRT model, if the ratio of grid users who use CMSV for transaction is α ($0 \leq \alpha \leq 1$), then ratio of grid users who use DAIP becomes $1 - \alpha$. And total response time of RPGRT model is equivalent to (3). N is total resource demand of grid user, T_{cm} is transaction time using CMSV, $TBid$ is single bidding time and $\sum TBid$ is the total bidding time of either grid user or resource provider using DAIP. Therefore, total bidding time of both sides can be expressed as $2 \times (\sum TBid)$ using DAIP.

$$\begin{aligned} & \text{Total Response Time of Resource Demand Prediction-based Model} \\ & = \alpha \times T_{cm} + (1 - \alpha) \times N \times 2 \times (\sum TBid) \end{aligned} \quad (3)$$

N ; total resource demand of grid user, α ; ratio of grid users who uses CMSV ($0 \leq \alpha \leq 1$), $1 - \alpha$; ratio of grid users who uses DAIP, T_{cm} ; transaction time using CMSV, $TBid$; single bidding time, $\sum TBid$; total bidding time of grid user or resource provider

Order to predict the improvement of RPGRT model, we divided (3) by (2). It is $\{[\alpha \times T_{cm}] + \{(1 - \alpha) \times N \times 2 \times (\sum TBid)\}\} / \{N \times 2 \times (\sum TBid)\}$. And it can be expressed as $\{ \alpha \times T_{cm} / N \times 2 \times (\sum TBid) \} + \{ (1 - \alpha) \times N \times 2 \times (\sum TBid) / N \times 2 \times (\sum TBid) \}$. And we assume $\sum TBid$ of (2) and $\sum TBid$ of (3) are approximately identical. Since T_{cm} is a lot smaller than $N \times 2 \times (\sum TBid)$ and $0 \leq \alpha \leq 1$, so we assume that $\{ \alpha \times T_{cm} \} / \{ N \times 2 \times (\sum TBid) \}$ is also very small and is replaced with c_0 . Therefore when we divide (3) by (2), $(1 - \alpha) + c_0$ can be obtained. If we use (4) to get the reduction rate of response time, $100 \times (\alpha - c_0)$ can be obtained. Assuming $\alpha - c_0$ is

very close to α , since c_0 is very smaller than α , RPGRT model's reduction rate of response time is approximately $(100 \times \alpha)\%$ compared to double auction model. Therefore, if we set the usage ratio of CMSV and DAIP to 50:50, then we can obtain approximately 50% of reduction rate of response time and also if we set it to 80:20, then almost 80% of reduction rate of response time can be obtained.

$$\text{Reduction Rate of Response Time} = \left(1 - \frac{\text{Total Response Time of RPGRT Model}}{\text{Total Response Time of Existing Model}}\right) \times 100 (\%). \quad (4)$$

5 Experiments and Results

Through these experiments, we compared our proposed RPGRT model with existing double auction model and single auction model. We made RPGRT model, double auction model and single auction model based on DEVS formalism [12].

5.1 Measuring Optimized Ratio of CMSV and DAIP of RPGRT Model

RPGRT model uses two price decision methods. We conducted experiment to measure the optimized ratio of two price decision method. We set the ratio for CMSV and DAIP to 50:50, 60:40, 70:30, and 80:20. We excluded 90:10 ratios due to its impracticality. We generated average of 7500 grid user demands per day for 150 day for the experiment, then measure the average response time per grid resource demand to choose optimal usage ratio.

Table 1. Response time per each resource demand of grid user depend on CMSV and DAIP selection ratio

Ratio of CMSV and DAIP	50:50	60:40	70:30	80:20
Average Response Time per resource demand (time unit: hour)	26.08	10.45	4.97	2.26

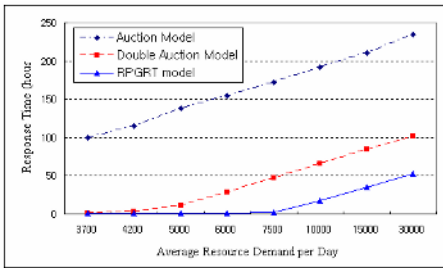
Table 1 shows the measurement of average response time per resource demand of grid user depend on CMSV and DAIP ratios when they were 50:50, 60:40, 70:30, and 80:20. Result shows that 80:20 ratios had most optimal response time which showed that RPGRT model is most optimal when CMSV and DAIP has the ratio of 80:20. In next experiment, we conducted experiment using CMSV and DAIP's ratio to 80:20.

5.2 Performance Evaluation

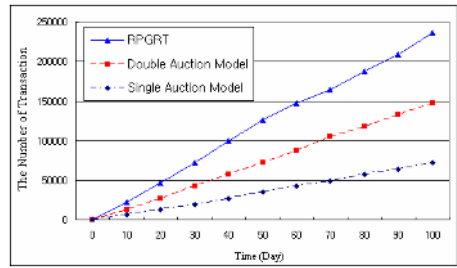
Response Time; We have generated resource demand of grid user for 100 days using Poisson distribution [8] to measure the response time of double auction, single auction, and RPGRT models. We conducted the experiment by increasing the number of demands from 3700 to 30000 each day. Response time for grid resource demand is the time that counts from the moment customer request resource to broker to the end of transaction. This response time includes time for adjusting grid resource demand

that customer requested, preparation time of resource provider, waiting time to receive bidding price and entire network transmission time.

The results from the experiment are shown in Fig. 3-(a). RPGRT model was more efficient response time if there were more number of customer grid resource demands per day. The reason is that RPGRT model prepares resource by predicting the grid resource demand of grid user, so that it needs smaller time to prepare. It also compares the actual grid resource demand with predicted grid resource demand then determines the price using the CMSV which enable grid user and resource provider to meet their price in short period of time. Even with bidding mechanism, it still has shorter response time than double auction and single auction model because the transaction progresses with price that is closed to initial price of real market world. As a result, reduction rate of response time for RPGRT model over double auction model was 71.39% and single auction model was 93.46%.



(a)



(b)

Fig. 3. Comparison RPGRT with Single Auction and Double Auction Model (a) Comparison of Response Time (b) Comparison of the Number of Transactions

The Number of Transactions: Comparing the number of transactions of RPGRT model, double auction model and single auction model was conducted by providing random grid resource demand of grid user for 100 days. Results are represented in Fig. 3-(b). RPGRT model had more efficient transaction rate than double auction and single auction model. Improvement rate of transactions in this experiment was 162.56% and 343.67% for RPGRT model compare to double auction and single auction model. As Fig. 3-(b) shows, difference in processing amount of RPGRT model, double auction model, and single auction model is increasing continuously. Resource demand prediction-based transaction network model and double auction model which started at same initial condition had 54953 transaction differences in 50 days and 89386 in 100 days. And, RPGRT model and single auction model which started at same initial condition had 91659 transaction differences in 50 days and 165575 in 100 days. Main reason for this result is that RPGRT model has shorter response time than double auction and single auction model and therefore it can process grid resource demand from customer faster. Hence, difference in processing resource continues to be increased as time goes on.

6 Conclusion

In this paper, we proposed Resource demand Prediction-based Grid Resource Transaction network (RPGRT) model to solve problems of existing models. The price of RPGRT model is determined by using the CMSV and the DAIP after comparing actual grid resource demand of grid user with provided predicted grid resource demand. We have conducted following experiments under same condition with single auction and double auction model to evaluate the performance of RPGRT model. We have conducted two experiments to prove performance of RPGRT model. In first experiment, we decided optimized ratio for CMSV and DAIP using empirical result. In second experiment, we measured reduction rate of response time of resource transaction and improvement rate of transactions by comparing RPGRT model with existing single auction and double auction model. The result from the first experiment, we decided optimized ratio of CMSV and DAIP which was 80:20. In second experiment, RPGRT model at least had 71.39% reduction rate of response time and 162.56% improvement rate of transactions.

References

1. Foster, I., Kesselman, C., Tuecke, S.: The Anatomy of the Grid: Enabling Scalable Virtual Organizations. *International Journal of High Performance Computing Application*, Vol.15, No.3 (2001) 200-222
2. Foster, I., Kesselman, C.: *The Grid. Blueprint for a new computing infrastructure*. Morgan Kaufmann, San Francisco (1999)
3. Berman, F., Fox, G., Hey, A.: *Grid Computing, Making the Global Infrastructure a Reality*. WILEY (2002)
4. Buyya, R.: *Grid Economy: A Market Paradigm for Distributed Resource Management and Scheduling for Service Oriented Grid Computing*. PhD Thesis, Monash University, Australia (2002)
5. Joita, L., Rana, O., Gray, W., Miles, J.: A Double Auction Economic Model. *Lecture Notes in Computer Science*, Vol. 3149. Springer-Verlag, Berlin Heidelberg New York (2004) 409–416
6. Chen, M., Yang, G., Liu, X.: *Gridmarket: A Practical, Efficient Market Balancing Resource for Grid and P2P Computing*. *Lecture Notes in Computer Science*, Vol. 3033. Springer-Verlag, Berlin Heidelberg New York (2004) 612–619
7. Lindsay, C.: *Applied Price Theory*. Dryden Press (1984)
8. McClave, J., Benson, P., Sincich, T.: *Statistics for Business and Economics*. 9th edn. Prentice Hall (2004)
9. Zhang, D., Zhao, K.: Economic model of TAC SCM game. in *Proceedings of 2004 IEEE/WIC/ACM International Conference on Intelligent Agent Technology(IAT2004)* (2004) 273-280
10. Besanko, D., Braeutigam, R.: *Microeconomics: An Integrated Approach*. WILEY (2001)
11. Sadeh, N., Arunachalam, R., Eriksson, J., Finne, N., Janson, S. : TAC-03: A supplychain trading competition. *AI Magazine*. *AI Magazine*, vol. 24, (2003)
12. Zeigler, B., Kim, T., Praehofer, H.: *Theory of Modeling and Simulation*. 2nd edn. Academic Press, New York (1998)

A CGM Algorithm Solving the Longest Increasing Subsequence Problem

David Semé

LaRIA: Laboratoire de Recherche en Informatique d'Amiens,
Université de Picardie Jules Verne,
CURI, 5 rue du Moulin Neuf, 80000 Amiens, France
seme@laria.u-picardie.fr

Abstract. In this paper, we consider parallel algorithm for the longest increasing subsequence problem. Although this problem is primitive combinatorial optimization problem, this is not known to be in the class NC or P -complete, that is, no NC algorithm have been proposed for this problem, and there is no proof which shows the problem is P -complete. We present a coarse grained parallel algorithm that solves the Longest Increasing Subsequence Problem shown as a basis for DNA comparison. It can be implemented in the CGM model with P processors in $O(N \log_2 \frac{N}{P})$ time and $O(P)$ communication steps for an input sequence of N integers. This algorithm is based on a new optimal and very simple sequential algorithm having a time complexity of $O(N \log_2 N)$.

Keywords: Parallel Algorithms, Coarse Grained Multicomputers, Longest Increasing Subsequence.

1 Introduction

In parallel computational theory, one of major goals is to find a parallel algorithm which runs as fast as possible. For example, many problems are known to have efficient parallel algorithms which run in $\Theta(1)$ or $\Theta(\log n)$ computational time, where n is the input size of problems. From the point of view of the complexity theory, the class NC is used to denote the measure. A problem is in the class NC if there exists a parallel algorithm which solves the problem in $O(T(n))$ time using $O(P(n))$ processors, where $T(n)$ and $P(n)$ are polylogarithmic and polynomial functions for n , respectively. Many problems in the class P , which is the class of problems solvable in polynomial time sequentially, are also in the class NC . On the other hand, a number of problems in the class P seem to have no parallel algorithm which runs in polylogarithmic time using polynomial number of processors. Such problems are called P -complete. A problem is P -complete if the problem is in the class P and we can reduce any problem in the class P to the problem using NC -reduction. It is believed that problems in the class NC admit parallelization readily, and conversely, P -complete problems are inherently sequential and difficult to parallelize.

In this paper, we consider parallel algorithm for the longest increasing subsequence problem. Although this problem is primitive combinatorial optimization

problem, this is not known to be in the class NC or P -complete, that is, no NC algorithm have been proposed for this problem, and there is no proof which shows the problem is P -complete.

The Longest Increasing Subsequence Problem (LIS for short) is a good illustration of dynamic programming and has interested many scientists [4], [10], [12], [21], [24], [25]. In July 1978, E.W. Dijkstra at Marktoberdorf's school, asked to his students to find the length of the longest increasing subsequence in a sequence of integers. Even though this problem seems relatively straightforward, few of them had been able to solve it. Today, this exercise remains a useful didactic example for topic of sequential programming methodology. In particular it shows how to strengthen an induction hypothesis in a very explicit way [18], [19], [23].

Finding the length is performed in time $O(N \log N)$ (where N is the length of the input sequence) sequentially [23]. On the other hand we are interested in actually finding the longest increasing upsequence. There are a lot of papers which deal with the longest increasing subsequence. Sequential algorithms [1],[2] show that we can solve the problem in $\Theta(n \log n)$ time sequentially in case that its input is a set of distinct integers. But these solutions are complex and the only known parallel algorithm that solves the problem in the CGM uses P processors with a $O(\frac{N^2}{P})$ time complexity and $O(P)$ communication steps [13].

In recent years several efforts have been made to define models of parallel computation that are more realistic than the classical PRAM models. In contrast to the PRAM, these new models are coarse grained, i.e. they assume that the number of processors P and the size of the input N of an algorithm are orders of magnitudes apart, $P \ll N$. By the precedent assumption these models map much better on existing architectures where in general the number of processors is at most some thousands and the size of the data that are to be handled goes into millions and billions.

This branch of research got its kick-off with Valiant [26] introducing the so-called Bulk Synchronous Parallel (BSP) machine, and was refined in different directions for example by Culler et al. [6], LogP, and Dehne et al. [8], CGM extensively studied in [3], [5], [7], [9], [11], [22], [14], [15], [16].

CGM seems to be the best suited for a design of algorithms that are not too dependent on an individual architecture. We summarize the assumptions of this model:

- all algorithms perform in so-called supersteps, that consist of one phase of interprocessor communication and one phase of local computation,
- all processors have the same size $M=O(\frac{N}{P})$ of memory ($M > P$),
- the communication network between the processors can be arbitrary.

The goal when designing an algorithm in this model is to keep the individual workload, time for communication and idle time of each processor within $\frac{T}{s(P)}$, where T is the runtime of the best sequential algorithm on the same data and $s(P)$, the speedup, is a function that should be as close to P as possible. To be able to do so, it is considered as a good idea the fact of keeping the number of supersteps of such an algorithm as low as possible, preferably $o(M)$.

As a legacy from the PRAM model it is usually assumed that the number of supersteps should be polylogarithmic in P , but there seems to be no real world rationale for that. In fact, algorithms that simply ensure a number of supersteps that are a function of P (and not of N) perform quite well in practice, see Goudreau et al. [17].

In this paper we present a CGM algorithm that solves the Longest Increasing Subsequence Problem using AVL trees as data structure. This algorithm is based on a new, optimal and very simple sequential algorithm having a time complexity of $O(N \log_2 N)$ and can be implemented in the CGM with P processors in $O(N \log_2 \frac{N}{P})$ time and $O(P)$ communication steps.

The paper is organized as follows. In section 2 we present the Longest Increasing Subsequence problem and some sequential algorithms. Section 3 presents the CGM solution of the LIS problem and the AVL tree data structure. Section 4 presents some experimental results and the conclusion ends the paper.

2 The Longest Increasing Subsequence Problem

2.1 Statement of the Problem

Definition 1. *Given a sequence A of N distinct integers, a subsequence of A is a sequence L which can be obtained from A in deleting zero or some integers (not necessarily consecutive).*

Definition 2. *A sequence is increasing if each integer of this sequence is larger than the previous integer. Given a sequence $A = \{x_1, x_2, \dots, x_N\}$ of N distinct integers, we define an increasing subsequence or upsequence of length l as a upsequence of $A : \{x_{i_1}, x_{i_2}, \dots, x_{i_l}\}$ with $\forall j, k : 1 \leq j < k \leq l \Rightarrow i_j < i_k$ and $x_{i_j} < x_{i_k}$.*

Definition 3. *A longest or maximal increasing subsequence is one of maximal length. Note that a maximal upsequence is not necessarily unique.*

2.2 Sequential Algorithm for the LIS Problem

Definition 4. *A decreasing subsequence of A is a subsequence of A where the numbers are nonincreasing from left to right.*

Definition 5. *A cover of A is a set of decreasing subsequences of A that contain all the numbers of A .*

Definition 6. *The size of the cover is the number of decreasing subsequences in it, and a smallest cover is a cover with minimum size among all covers.*

Lemma 1. *If I is an increasing subsequence of A with length equal to the size of a cover of A , call it C , then I is a longest increasing subsequence of A and C is a smallest cover of A .*

Proof. see [20].

□

We now summarize a sequential algorithm for the LIS due to [20], which is the basis of our CGM algorithm.

Let A be a set of N integers. We want to construct a decreasing cover of A . The idea is as follows: starting from the left of A , examine each successive number in A and place it at the end of the first (left-most) decreasing subsequence that it can extend. If there are no decreasing subsequences it can extend, then start a new decreasing subsequence to the right of all existing decreasing subsequences.

This algorithm produces a cover of A which is called the greedy cover in [20]. After the greedy cover is found, a LIS of A can be found easily as it is described in [20].

Sequential greedy cover algorithm 1

begin

0. Set i to be the number of subsequences in the greedy cover of A . Set I to the empty list; pick any number x the subsequence i and place it on the front of the list I .

1. While $i > 1$ do

begin

2. Scanning down from the top of the sequence $i - 1$, find the first number y that is smallest than x .

3. Set x to y and i to $i - 1$.

4. Place x on the front of the list I .

end

end.

At the end of the algorithm described in [20], I contains an LIS of A . The greedy cover of A is found in time $O(N^2)$ and the LIS found in time $O(N)$ given the greedy cover.

3 The CGM Solution for the LIS Problem

In this section we describe a CGM solution using the greedy cover approach described in section 2 as local computation phase. As we explained in this previous section, the greedy cover algorithm has a complexity of $O(N^2)$. Then the first CGM algorithm that solves the LIS problem using the greedy cover algorithm has a time complexity of $O(\frac{N^2}{P})$ and $O(P)$ communication rounds [13] with $O(P)$ processors. Experimental results of this solution showed that communication times represent less than 1% of total running times. So, we focus our attention on reducing the time of local computation phases. A good way for reducing the local computation complexity is the use of a better data structure.

3.1 Presentation of AVL Trees

Definition 7. *A binary tree is a tree with exactly two sub-trees for each node, called the left and right sub-trees.*

Definition 8. A **binary search tree** is a binary tree where, for each node m , the left sub-tree only has nodes with keys smaller than (according to some total order) the key of m , while the right sub-tree only has nodes with keys not smaller than the key of m .

Definition 9. The **height** of a tree is the number of nodes on its longest branch (a path from root to a leaf).

Definition 10. A **balanced tree** is a tree where every leaf is "not more than a certain distance" away from the root than any other leaf.

Definition 11. An **AVL tree** is a binary search tree where the sub-trees of every node differ in height by at most 1.

Remark 1. AVL trees are not perfectly balanced, but maintain $O(\log_2 N)$ search, insertion, and deletion times, when N is the number of nodes in the tree.

3.2 Description of the LIS Algorithm Using an AVL Tree

The greedy cover algorithm using an AVL tree (called sequential greedy cover algorithm 2) is based on the sequential greedy cover algorithm 1 described in section 2 and on the following insertion algorithm in an AVL tree.

AVL insertion algorithm

begin

0. After locating the insertion place (in respect of definition 8) and performing the insertion, there are three cases:

- 1.** The tree remains balanced: do nothing.
- 2.** A tree was left-heavy and became left-unbalanced: do a right rotation or a left-right rotation to balance the tree.
- 3.** A tree was right-heavy and became right-unbalanced: do a left rotation or a right-left rotation to balance the tree.

end.

Property 1. An insertion requires re-balancing but it does not modify the height of the tree and a rotation takes at most $O(\log_2 N)$ time.

Corollary 1. *Insertion requires at most two walks of the path from the root to the added node, hence indeed takes $O(\log_2 N)$ time.*

We describe here the sequential greedy cover algorithm 2 (as local computation phase) which combines the greedy cover approach and the insertion of an element in an AVL tree. Then, the algorithm constructs an AVL tree from the input sequence A by insertion of each element of A in the AVL tree. We consider that we can associate to each element of A an index, called *seq-index* which represents a decreasing sequence of the greedy cover. For example, an element A_i with an associated index equal to 3 signifies that the element A_i is in the 4th decreasing sequence of the greedy cover of A . Notice that the first decreasing sequence of

the greedy cover has the index 0. Moreover, we associate to each element A_i of the input sequence A another integer, called max_seq , representing the number of decreasing sequences of the greedy cover of A containing the elements of the left sub-tree of A_i . This variable max_seq is very important for the computation of the greedy cover. In fact, the insertion algorithm in an AVL tree is based on the definition 8 for locating the insertion place. Consider now an element A_i to be inserted and an element A_j of the AVL tree, if $A_i > A_j$ then A_i do not visit the left sub-tree of A_j and then has no information about it. This is not important for the insertion but very important for the computation of the greedy cover. As the elements in the sub-tree of A_j are smaller than A_j , these are also smaller than A_i and then A_i cannot be in a decreasing sequence containing these elements as defined in section 2 for the construction of the greedy cover. A_i should know the maximum number max_seq of decreasing sequences containing elements smaller than A_i in order to set up its own index of decreasing sequence seq_index . Then, the index seq_index associated to A_i should be communicated along the path from A_i to the root of the left sub-tree containing A_i in order to set up the variable max_seq if $seq_index > max_seq$.

Sequential greedy cover algorithm 2

begin

0. For each element A_i of the input sequence A .

begin

1. Perform the AVL insertion algorithm with an updating of the variable seq_index associated to the element to be inserted A_i in the localization phase such that seq_index is equal to the number of decreasing sequences containing elements smaller than A_i plus 1.

2. Propagate the index seq_index associated to A_i along the path from A_i to the root of the left sub-tree containing A_i in order to set up the variable max_seq if $seq_index > max_seq$.

end

end.

Property 2. The propagation of the value seq_index in a branch of the AVL tree takes at most $O(\log_2 N)$ time.

Corollary 2. *Sequential greedy cover algorithm 2 requires at most three walks (two for the insertion and one for the propagation of seq_index) of the path from the root to the added node, hence indeed takes $O(N \log_2 N)$ time.*

3.3 A Complete Example

Figure 1 shows a complete example with an input sequence $A = \{13, 12, 11, 10, 15, 1, 2, 14, 3, 4\}$. A node of the AVL tree is represented by the value of the element A_i of the input sequence A and contains a couple of value (max_seq, seq_index) . This example illustrates the evolution of the AVL tree containing the

elements of the input sequence A by insertion of each element of A . Rotations needed (for re-balance the AVL tree) are represented by the following notations: rd for a right rotation, rg for a left rotation, rdg for a right-left rotation and rgd for a left-right rotation. The root of the sub-tree which should be rotated is specified by an arrow.

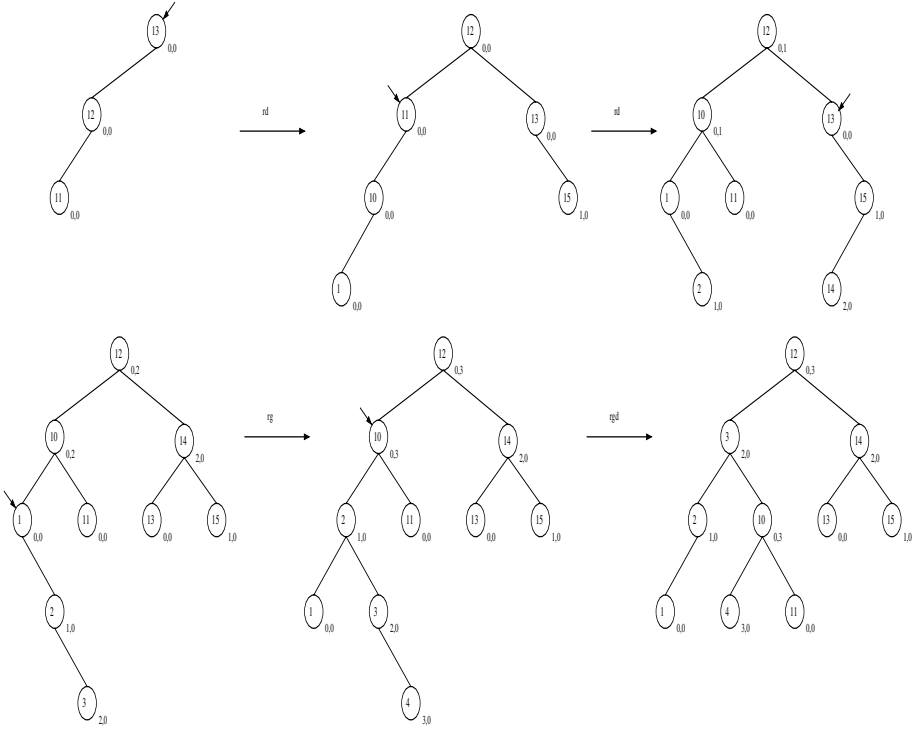


Fig. 1. A complete example for $A = \{13, 12, 11, 10, 15, 1, 2, 14, 3, 4\}$

3.4 Description of the CGM Algorithm

The CGM algorithm presented in this section uses the sequential greedy cover algorithm 2 as main local computation phase. Each processor num ($0 \leq num < P$) contains the num -th partition of $\frac{N}{P}$ elements of the input sequence A . Notice that an initialization phase is needed for all processors except for processor $num = 0$. This initialization phase on processor num consists of a set up of the variable seq_index associated to the element A_i to be inserted in the AVL tree taking into account the number of decreasing sequences containing elements smaller than A_i in the AVL tree received by processor num . This can be done in locating the place that A_i should take when we would like to insert it in the AVL tree received by processor num . This procedure is very closed to the insertion algorithm described before. The following CGM algorithm presents the program of each processor num and figure 2 shows communication rounds of this program.

CGM greedy cover algorithm

begin

1. If $num = 0$ then

begin

1.2. Perform the sequential greedy cover algorithm 2.

1.3. **Send**($num, AVL, ALL_SUCCESSORS$)

end

2. Else

begin

2.1. For ($num' = 0$ to num) do

begin

2.1.1. **Receive**(num', AVL')

2.1.2. Perform the initialization phase to set up from AVL' the value of seq_index associated to the element A_i .

end

2.2.. Perform the sequential greedy cover algorithm 2.

2.3. **Send**($num, AVL, ALL_SUCCESSORS$)

end

end.

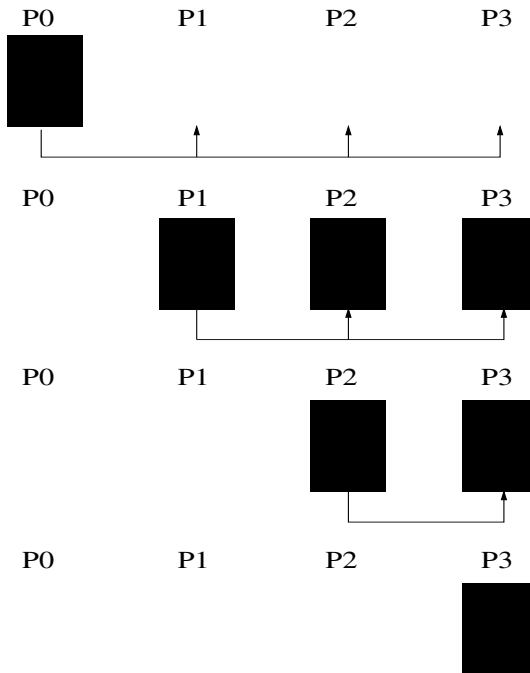


Fig. 2. Communication rounds for P=4

Remark 2. Note that our approach uses two functions called **Send** and **Receive** which are defined as:

- **Send** ($num, AVL, \mathbf{ALL_SUCCESSORS}$) where the values num and AVL are sent to all processors num' such that $num' > num$,
- **Receive** (num', AVL') where the values num' and AVL' are received from the processor num' .

Property 3. The initialization phase and the sequential greedy cover algorithm 2 take at most $O(\frac{N}{P} \log_2 \frac{N}{P})$ time each.

Corollary 3. *On the last processor, CGM greedy cover algorithm requires at most $P - 1$ initialization phases and performs sequential greedy cover algorithm 2 one time, hence indeed takes $O(N \log_2 \frac{N}{P})$ time and uses $O(P)$ communication rounds.*

4 Experimental Results

We have implemented the CGM greedy cover algorithm in C language using MPI communication library and tested them on a multiprocessor Celeron 466Mhz

Table 1. Total running times (in seconds)

N	P=2	P=4	P=8	P=16
4096	0.02	0.03	0.06	0.13
8192	0.06	0.06	0.08	0.17
16384	0.15	0.15	0.15	0.24
32768	0.37	0.38	0.35	0.35
65536	1.01	0.91	0.85	0.81
131072	2.51	2.35	1.97	1.87
262144	5.99	5.56	5.149	4.33
524288	28.06	12.86	12.08	11.12
1048576	59.43	30.51	28.30	25.33
2097152	115.93	75.27	64.86	58.85
4194304	347.52	174.72	150.52	135.15

Table 2. Total running times (in seconds)

N	P=2	P=4	P=8	P=16
4096	0.47	0.36	0.26	0.22
8192	1.87	1.41	0.83	0.58
16384	7.50	5.61	3.30	1.79
32768	32.19	22.42	13.11	7.06
65536	159.82	97.20	52.32	28.09
131072	650.94	480.69	225.16	112.12
262144	2618.04	1976.97	1104.40	488.97
524288	10527.97	7980.30	4593.70	2381.15
1048576	52321.23	32433.04	18533.05	9893.67

Table 3. Communication times (in seconds)

N	P=2	P=4	P=8	P=16
4096	0.0011	0.0026	0.0041	0.0079
8192	0.0029	0.0056	0.0083	0.0143
16384	0.0057	0.0113	0.0226	0.0452
32768	0.0122	0.0246	0.0519	0.1072
65536	0.0242	0.0480	0.1219	0.2756
131072	0.0474	0.0946	0.2261	0.4957
262144	0.0947	0.1883	0.3614	0.7060
524288	0.1899	0.3752	0.7324	1.4384
1048576	0.3795	0.7484	1.4663	2.8822

platform running LINUX. The communication between processors is performed through an Ethernet switch.

Table 1 presents total running times (in seconds) for each configuration of 2, 4, 8, and 16 processors respectively. We note that for small values of N (less than 65536) the best total running time is obtained for 2 processors. Communication rounds need more time (as shown in table 3) for 16 processors than for 2 processors. Moreover, the local computation time is as small as these communication times take the main part of the total running times. For $N \geq 65536$, the total running times become more interesting when we use 16 processors.

Table 2 presents total running times (in second) for each configuration of 2, 4, 8, and 16 processors respectively on the same platform using the CGM algorithm described in [13]. We note that the total running times presented in Table 1 are more interesting that these of Table 2. The average ratio between these total running times is about 197. This shows the efficiency of our CGM algorithm which is about 197 times (in mean) faster than this described in [13].

Table 3 presents communication times (in seconds) for each configuration of 2, 4, 8, and 16 processors respectively. These communication times correspond to a send of N integers by a processor to others (i.e. a broadcasting of N integers by a processor). Here, we have $N = 2^k$ and k is an integer such that $12 \leq k \leq 20$.

5 Concluding Remarks

This paper presents an coarse grained algorithm that solves the Longest Increasing Subsequence Problem shown as a basis for DNA comparison. It can be implemented in the CGM model with P processors in $O(N \log_2 \frac{N}{P})$ time and $O(P)$ communication steps for an input sequence of N integers. This algorithm is an improvement of the CGM algorithm proposed in [13] and is based on a new optimal and very simple sequential algorithm having a time complexity of $O(N \log_2 N)$.

In this paper we present a CGM algorithm using an interesting data structure called AVL tree. This data structure (named after their inventors G.M. Adel'son-Velskii and E.M. Landis) was the first dynamically balanced tree to be proposed in 1962 and mainly used since this date. The use of this data structure allowed a better local computation time complexity. In fact, the local computation time of one phase is optimal for that problem.

It will be interesting to reduce the number of communication steps: is there another approach yielding optimal communication rounds i.e. $\log P$? It seems to be a difficult problem since the LIS is based on a strong recursivity. Moreover, the complexity in time depends on the communication steps. As we have a work-efficient algorithm, reducing the communication steps yields the reduction of the complexity in time and then it will be necessary to have more processors in order to get work-efficiency.

The next step of this work consists of implementing our algorithm on many cluster of stations in order to study all its aspects.

References

1. A. Aldous and P. Diaconis. Longest Increasing Subsequences: From Patience Sorting to the Baik-Deift-Johansson Theorem. *BAMS: Bulletin of the American Mathematical Society*, 36:413–432, 1999.
2. S. Bespamyatnikh and M. Segal. Enumerating Longest Increasing Subsequences and Patience Sorting. *Information Processing Letters*, 71(1–2):7–11, 2000.
3. P. Bose, A. Chan, F. Dehne, and M. Latzel. Coarse grained parallel maximum matching in convex bipartite graph. *Proc. 13th International Parallel Processing Symposium (IPPS'99)*, pages 125–129, 1999.
4. C. Cérin, C. Dufourd, and J.F. Myoupo. An Efficient Parallel Solution for the Longest Increasing Subsequence Problem. In *Fifth International Conference on Computing and Information (ICCI'93) Sudbury, Ontario, IEEE Press*, pages 200–224, 1993.
5. A. Chan and F. Dehne. A note on coarse grained parallel integer sorting. *Parallel Processing Letters*, 9(4):533–538, 1999.
6. D. Culler, R. Karp, D. Patterson, A. Sahay, K. Schauser, E. Santos, R. Subramonian, and T. Von Eicken. Log^p: towards a realistic model of parallel computation. *4-th ACM SIGPLAN Symp. on Principles and Practices of Parallel Programming*, pages 1–12, 1996.
7. F. Dehne, X. Deng, P. Dymond, A. Fabri, and A. Khokhar. A randomized parallel 3d convex hull algorithm for coarse grained multicomputers. *Proc. 7th ACM Symp. on Parallel Algorithms and Architectures*, pages 27–33, 1995.
8. F. Dehne, A. Fabri, and A. Rau-Chaplin. Scalable parallel computational geometry for coarse grained multicomputers. *International Journal on Computational Geometry*, 6(3):379–400, 1996.
9. M. Diallo, A. Ferreira, A. Rau-Chaplin, and S. Ubeda. Scalable 2d convex hull and triangulation algorithms for coarse grained multicomputers. *Journal of Parallel and Distributed Computing*, 56(1):47–70, 1999.
10. P. Erdos and A. Szekers. A combinatorial problem in geometry. *Compositio Mathematica*, 2:463–470, 1935.
11. A. Ferreira and N. Schabanel. A randomized bsp/cgm algorithm for the maximal independent set problem. *Parallel Processing Letters*, 9(3):411–422, 1999.
12. M.L. Fredman. On Computing the Length of Longest Increasing Subsequences. *Discrete Mathematics*, pages 29–35, 1975.
13. T. Garcia, J.F. Myoupo, and D. Semé. A work-optimal cgm algorithm for the longest increasing subsequence problem. *International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA'01)*, 2001.
14. T. Garcia, J.F. Myoupo, and D. Semé. A coarse-grained multicomputer algorithm for the longest common subsequence problem. *11-th Euromicro Conference on Parallel Distributed and Network based Processing (PDP'03)*, 2003.
15. T. Garcia and D. Semé. A coarse-grained multicomputer algorithm for the longest repeated suffix ending at each point in a word. In *International Conference on Computational Science and its Applications (ICCSA'03)*, 2003.
16. T. Garcia and D. Semé. A load balancing technique for some coarse-grained multicomputer algorithms. In *21th International Conference on Computers and Their Applications (CATA-2006)*, 2006 (to appear).
17. M. Goudreau, S. Rao K. Lang, T. Suel, and T. Tsantilas. Towards efficiency and portability: Programming with the bsp model. *8th Annual ACM Symp. on Parallel Algorithms and Architectures (SPAA'96)*, pages 1–12, 1996.

18. A. Gram. *Raisonnement pour programmer*. Dunod, Paris, 1988.
19. D. Gries. *The Science of Programming*. Springer Verlag, 1981 (fifth printing 1989).
20. D. Gusfield. *Algorithms on Strings, Trees, and Sequences : Computer Science and Computational Biology*. Cambridge University Press, 1997.
21. G. Jacobson and K.P. Vo. Heaviest Increasing/Common Subsequence Problems. In *Proc. 3rd Annual Symp. CPM*, LNCS 644, pages 52–66, 1992.
22. S.R. Kim and K. Park. Fully scalable fault-tolerant simulations for bsp and cgm. *Journal of Parallel and Distributed Computing*, 60:1531–1560, 2000.
23. U. Manber. *Introduction to Algorithms, a creative approach*. Addison-Wesley, 1989.
24. J. Misra. A Technique of Algorithm Construction on Sequence. *IEEE Trans. Software Engineering*, SE-4(1):65–69, 1978.
25. T.G. Szymanski. A Special Case of the Max Common Subsequences Problem. Technical report, Dep. Elec. Eng. Princeton University, Princeton N.J. Tech. Rep., 1975.
26. L.G. Valiant. A bridging model for parallel computation. *Communications of the ACM*, 33(8):103–111, 1990.

Computer Assisted Source-Code Parallelisation

Peter J. Vidler and Michael J. Pont

Embedded Systems Laboratory, University of Leicester,
University Road, LEICESTER LE1 7RH, UK
{pjb3, mjp9}@le.ac.uk

Abstract. Many single-processor embedded systems are implemented using a time-triggered co-operative (TTC) scheduler. When considering possible alternatives to such a design, one option is a multi-CPU architecture, created using off-the-shelf processors or SoC techniques. In order to allow the rapid assessment of such design alternatives, we are exploring ways in which single-processor TTC code may be “automatically” converted to a multi-CPU equivalent. In this paper, we discuss the design of a prototype source code conversion tool. The input to this tool is the source code for the tasks of a single processor system using a TTC scheduler. The output from the tool (in the current version) is the equivalent multi-processor code based on either a “domino” scheduler or a shared-clock scheduler. In order to assess the effectiveness of the tool, we have used it in a non-trivial case study: the results from this study are presented in detail.

1 Introduction

Many resource-constrained embedded systems run without the use of an off-the-shelf “real-time operating system” and employ some form of simple (custom-built) scheduler instead. These schedulers can be “time-triggered” (which usually means that the tasks carried out by the system are started via a periodic timer) [1] or “event-triggered” (which usually means that tasks are started in response to specific – aperiodic – hardware interrupts) [2]. Time-triggered systems are widely recognised as providing benefits to both reliability and safety [3, 4, 5, 6] in some of the more safety-critical applications (such as those used in the automotive and aerospace industries).

Such schedulers can also be categorised as “co-operative” or “pre-emptive”. When compared to pre-emptive schedulers, co-operative schedulers have a number of desirable features, particularly for use in safety-related systems [3, 7, 4, 8]. For example, one of the simplest implementations of a co-operative scheduler is a cyclic executive [9, 10]: this is a fully co-operative design which has a “time triggered” [1] architecture. Provided that an appropriate implementation is used, time-triggered, co-operative (TTC) architectures are a good match for a wide range of applications. For example, previous studies have described in detail how such techniques can be used in data acquisition systems, washing-machine control and monitoring of liquid flow rates [11], in automotive applications [12], a wireless (ECG) monitoring system [13], and various control applications [14, 15].

Of course, a TTC solution is not always appropriate. As Allworth has noted: “[The] main drawback with this [co-operative] approach is that while the current process is running, the system is not responsive to changes in the environment. Therefore, system processes must be extremely brief if the real-time response [of the] system is not to be impaired.” [3]. We can express this concern slightly more formally by noting that if a system is being designed which must execute one or more tasks of (worst-case) execution time e and also respond within an interval t to external events then, in situations where $t < e$, a pure co-operative scheduler will not generally be suitable.

In such circumstances, it is tempting to opt immediately for a full pre-emptive design. Indeed, some studies seem to suggest that this is the only alternative [16, 10]. However, there are other design options available. For example, we have previously described ways in which support for a single, time-triggered, pre-emptive task can be added to a TTC architecture, to give what we have called a “time-triggered hybrid” (TTH) scheduler [17, 5]. A TTH solution can be effective and – with a time-triggered architecture and a limited degree of pre-emption – it can provide highly predictable behaviour. An alternative solution, which avoids even limited pre-emption, is to add one or more additional processor cores to the system, either in the form of “off the shelf” processors [5] or by assembling multiple “soft cores” on an FPGA [18, 19].

Both multi-processor and TTH designs allow the developer to schedule a frequent (typically short) task for periodic data acquisition, typically through an analogue-to-digital converter or similar device: such a requirement is common in, for example, a wide range of control systems [20]. If we are developing such a control system, we may wish to explore one or both of these design options. If so, then adapting a single-processor TTC design to create a TTH design is very straightforward [5]. However, converting a single-processor TTC design into a multi-processor equivalent is a rather more involved process, particularly if we wish to explore the use of different network architectures or to compare the use of off-the-shelf and system-on-chip solutions.

In order to reduce the effort required to explore multi-processor equivalents of single-processor TTC designs, this paper considers ways in which this conversion process can – at least in part – be automated.

The paper is organised as follows. The conversion process is covered in more detail in Section 3, while Section 2 discusses some of the previous work in this area. Section 4 gives the details of a case study used to test the automated part of the conversion process. Finally, in Section 5 we give some concluding remarks based on the results of this case study.

2 Previous Work

The automatic parallelisation of a system is a broad subject that has seen a great deal of previous work. Most of this work is in the area of Instruction Level Parallelism (ILP [21, 22, 23]), which is carried out at the compiler and hardware levels [24, 25, 26, 27], and is restricted by (amongst many other factors) data dependencies in the source code input. The approach taken in this paper is

rather different. We operate at the task level, splitting entire tasks off onto separate processors and generating the scheduler code required to communicate and synchronise between them.

A number of tools are available that perform automatic conversions at the source code level. Amongst these are EXPRESSION [28] and Giotto [29, 30]. When using these tools, the developer is required to supply additional information about the system, usually through an external file (written in a custom language) which specifies the communication and timing constraints between tasks. This is in contrast to our approach of directly splitting tasks off onto multiple processors, then allowing the developer to tune the task timing separately (by hand).

There are also many other tools that generate source code for embedded systems. The vast majority of these start from high-level system models, such as UML [31], but some use different representations (patterns, for example [32]). Such approaches differ from our own in that we convert directly between source code architectures, while they generally convert a high-level representation into source code.

3 Automatic Code Conversion

In this section we describe the method employed in this paper to partially automate the conversion process.

3.1 The Build Process

In connection with a pilot study [33] we discussed the implications involved in carrying out the parallelisation at various stages of the build process. Through a process of elimination we decided that the conversion should operate directly on the source code, receiving input from the preprocessor and passing its output directly to the compiler. This arrangement is shown in Fig. 1.

The main advantage of this arrangement is that we have access to all the system's tasks at the time of conversion. We can also make the tool relatively compiler (and platform) independent, provided that we use a source code parser capable of recognising the slight differences in syntax used by the different compilers that target embedded systems. Finally, it allows us the chance to use the standard interface between the preprocessor and the compiler – namely the “`#line`” compiler directive – to assist the compiler in providing its error messages in terms of the original input (as opposed to being in terms of the converted source code, which would not make sense to the user).

3.2 The Conversion Process

In effect, the conversion process consists of the generation of three layers of code, which are then combined into a new translation unit for each task (or at least, for each processor). The first layer is the code for each task, which is extracted by the tool from the single processor system provided by the user. This can be

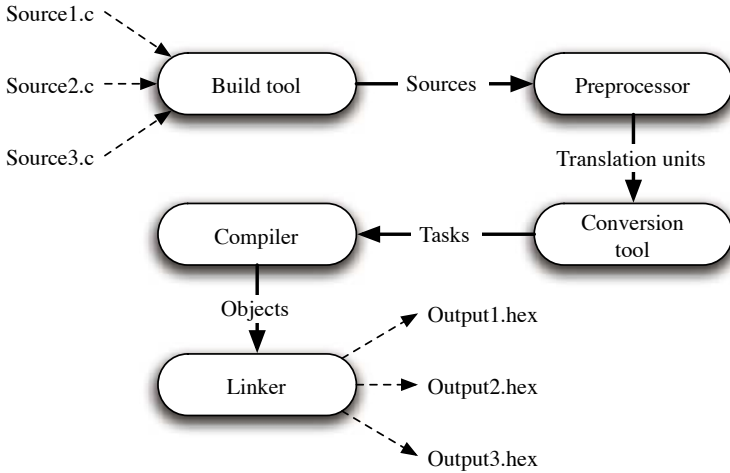


Fig. 1. Steps in the compilation process

considered the most robust, as it can usually be tested in isolation, preferably with a much simpler scheduler than the final system might employ.

The second layer of code required for the conversion process is the scheduler itself. This code must be applied separately to each new translation unit, and we can use one of several available versions in order to employ different scheduler types. This is “static” code in that it always remains the same, regardless of the input to the system. It works by using a specific set of variables for communication, without actually knowing the type of these variables. This lack of knowledge can make writing and testing such schedulers tricky, but in reality is no different from the use of generics in many modern programming languages (such as template functions in C++, where the function is written using the name of the template parameter, but usually without knowing its type).

The third (and final) layer of code required for the conversion process is the interface that sits between the other two layers. This interface provides the declaration of the scheduler’s set of variables, using the type that the tool extracts from the globals used by the tasks. It also provides functions to map these predefined variables onto the equivalent variables required by the task code provided by the user. This allows us to separate tasks onto different processors, without having to make any changes to the source code for the tasks themselves.

The interface layer must be generated separately for every task supplied by the user and may also be different for every scheduler architecture that can be employed. As such, it is difficult to fully test this piece of code in isolation, a fact that makes the generation of this layer a particular challenge – we wish to ensure that the generated code has predictable behaviour. We have therefore tried to ensure that this layer is as simple as possible. This allows us to more easily spot inconsistencies in the code, and reduces the impact of task changes on the system-supplied scheduler code.

Once the interface code has been generated for a task, it is combined with the static scheduler code and the code for the task itself. We then feed each resulting task unit into the compiler separately, producing one binary executable per task (as shown in Fig. 1).

4 Case Study

In order to evaluate the conversion process, we decided to use a simple case study. The study and its results are presented in this section.

4.1 Background

To fully test the correctness and flexibility of the conversion process, we employed a simple cruise control system [34, 12, 33] as the main case study for this paper. The system was chosen because it has been successfully implemented and tested using a single-processor co-operative architecture. This allows us to compare the results of various generated architectures to the original, in order to determine if the conversion process is working correctly.

The system consists of a car model and the Cruise Control System (CCS) itself. The CCS receives a single-wire input from the car model indicating the current speed (as a pulse rate modulated signal) and provides an eight bit output signifying the desired throttle setting. The single-processor system was implemented using three tasks. Figure 2 shows that the communication between these tasks was (deliberately) chosen to provide differing types and sizes of variables in the communication, in order to test the flexibility of the conversion tool.

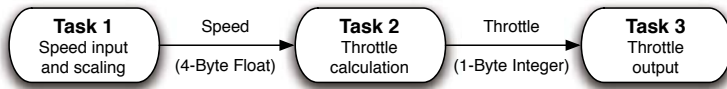


Fig. 2. The CCS tasks

These tasks make up the core of the system; they are used, unaltered, in all the architectures described in this paper.

4.2 Architectures

The single processor system executed the three tasks outlined in the previous section using a TTC scheduler [5, 34]. This system provided the benchmark performance figures against which the other designs were compared.

In addition, the conversion tool was used to create code for two more, multi-processor, architectures. Note that, in each case, the task timing in the converted code was left the same as the original.

Domino Architecture. In a previous pilot study, we described a very basic CCS implementation using a domino-scheduled architecture [33]. Such an

architecture takes advantage of the fact that communication in the CCS (as in many control systems) always flows in one direction; we used a pipeline approach to facilitate the use of multiple processors, controlled by a timer on the first processor and synchronised down the pipeline on each “tick”.

In the pilot study, the three processors were connected via a simple parallel port-to-port connection. Such an implementation provides a useful testbed but is not representative of the type of architecture that would be employed in a practical CCS implementation. In the present study, the three processors are connected using the Controller Area Network (CAN) protocol: a protocol that was originally intended for automotive designs [35].

Shared-Clock Architecture. The second test of the conversion tool involved a shared-clock architecture [5]: specifically, the design was based on the TTC-SC3 protocol [34]. In this system, all three processors communicate across a single CAN bus. The first node acts as the Master, responding to interrupts triggered by its internal timer. When the interrupt is raised, the Master sends a tick message to all Slaves (in this case, the other two processors in the system). On receipt of this, all Slaves are expected to send an acknowledgement within the same tick interval. This is illustrated in Fig. 3.

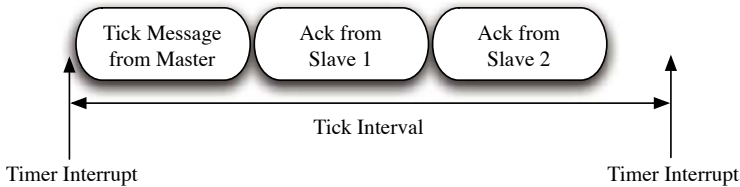


Fig. 3. TTC-SC3 message timing

Every message (regardless of whether it’s a tick or acknowledgement message) contains the latest output data from its associated task. Each task sends its acknowledgement (or tick for the Master) with a specific message identity, allowing easy differentiation between different task’s data. If a task requires input from a node other than the Master, we have to set up a second CAN receive buffer with the corresponding message identity filter. The conversion tool automates this process.

Architecture Comparison. For simplicity and to make it easier to compare the results, all three systems used the same timing for their tasks. Consequently, the only differences between the generated code and the original, single processor code were in the nature of the multi-processor designs. Each of the multi-processor designs was synchronised at the beginning of each tick interval, incurring a certain amount of overhead due to the communication involved. For architectures that employ CAN for their communication (including both multi-processor designs presented here) this delay will be variable, due to bit stuffing [36].

It is also possible (with most communication mechanisms) for the delay to be variable due to multiple messages (usually acknowledgements in our case) being transmitted at once, and the resulting arbitration that is required ???. Note that this is only a possibility for the shared-clock scheduler here, as the domino architecture uses separate buses between each processor and so will never suffer from simultaneous message transmission attempts.

These factors, combined with the fact that we are not altering the timing of the system, mean that we cannot expect the output of the multi-processor system to be identical to that of the single processor original. This is inevitable, since delays and timing variations are a factor in all distributed designs. It is not practical (in a general case) to adapt the code automatically (for example, by altering PID parameters) in order to deal with such timing changes. Instead, our system allows the developer the opportunity to tune the timing of the system after it has been generated.

4.3 Results

In order to test that each cruise controller architecture was working correctly, we set up a step increase in the desired speed from 30 mph to 60 mph after thirty seconds, followed by a step reduction in speed back to 40 mph after another

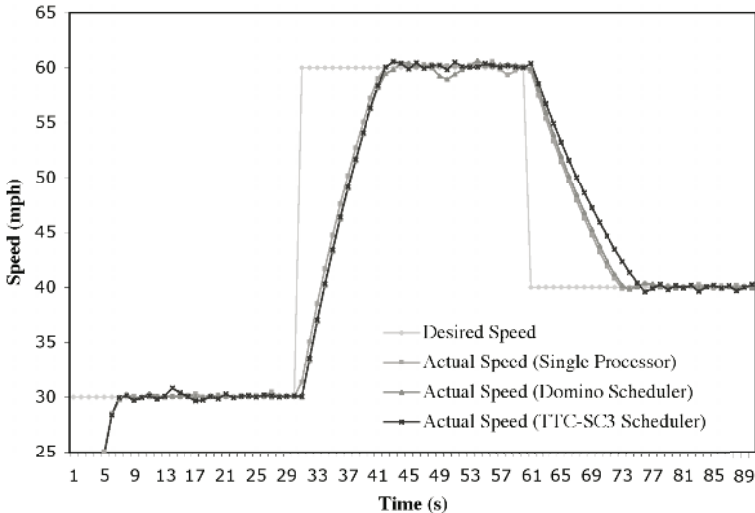


Fig. 4. Combined results for the three cruise controllers

Table 1. IAE results

Scheduler Type	IAE Results
Single Processor	267
Domino Scheduler	288
TTC-SC3 Scheduler	308

thirty seconds. In order to gain some idea of the relative performance of the three systems, we calculated the Integral of the Absolute Error values (IAE [37, 38]) across the range from 10 seconds to 80 seconds.

Figure 4 shows the desired speed values as well as the actual speed of the car model for all three systems. Although neither multi-processor scheduler perfectly matches the output of the original system, they are close enough to see that the source code conversion has been successful.

The IAE results (shown in Table 1) reflect the slight disparity between the performance of the single-processor system and that of the other two designs. However, the output from each of the generated systems is well within the tolerances of the model, despite the overhead of communication between the processors and other factors arising from the use of multi-processor schedulers.

5 Conclusion

In this paper, we have discussed the design of a prototype tool which is intended to assist in the migration between single- and multi-processor embedded systems. It was found that the performance of the designs created in this way was very similar to that of the original. This indicates that, in each case, the conversion process was completed successfully.

We mentioned earlier that the conversion tool did not in any way alter the timing of the tasks being carried out on each processor, meaning that we are not taking full advantage of the multi-processor nature of the resulting system. This was done because altering the timing of the tasks automatically would invalidate the assumptions on which several parts of the original task code were based.

Detecting a reliance on specific timing within an arbitrary section of input code would be impractical for the conversion tool [33]. A much easier (and potentially more reliable) solution is to view the conversion as being computer-assisted and requiring manual tuning, rather than a fully automatic process. This allows the tool to take much of the strain out of the conversion process, while the developer simply makes any necessary adjustments to the timing.

Of course, manual adjustments are not always required. Some systems must use a multi-processor architecture; not for the timing benefits, but because each task corresponds to a node that must be physically separated from the others. An example of this would be a intruder alarm system using separated sensor nodes in and around each room. The conversion tool presented here could then automate the required conversion process entirely, without any manual tuning required on the part of the developer.

References

1. Kopetz, H.: *Real-Time Systems: Design Principles for Distributed Embedded Applications*. Kluwer Academic (1997)
2. Siemers, C., Falsett, R., Seyer, R., Ecker, K.: Reliable event-triggered systems for mechatronic applications. *Journal of Systems and Software* **77** (2005) 17–26

3. Allworth, S.T.: *Introduction to Real-Time Software Design*. Macmillan (1981)
4. Nissanke, N.: *Realtime Systems*. Prentice-Hall (1997)
5. Pont, M.J.: *Patterns for Time-Triggered Embedded Systems*. Addison-Wesley (2001)
6. Storey, N.: *Safety-Critical Computer Systems*. Addison-Wesley (1996)
7. Bate, I.J.: Introduction to scheduling and timing analysis. In: *The Use of Ada in Real-Time Systems*, IEE Conference Publication 00/034 (2000)
8. Ward, N.J.: The static analysis of a safety-critical avionics control system. In: *Air Transport Safety: Proceedings of the Safety and Reliability Society Spring Conference*, SaRS, Ltd. (1991)
9. Baker, T.P., Shaw, A.: The cyclic executive model and ada. *Real-Time Systems* **1**(1) (1989) 7–25
10. Locke, C.D.: Software architecture for hard real-time applications: Cyclic executives vs. fixed priority executives. *Real-Time Systems* **4**(1) (1992) 37–53
11. Pont, M.J.: *Embedded C*. Addison-Wesley (2002)
12. Ayavoo, D., Pont, M.J., Parker, S.: Using simulation to support the design of distributed embedded control systems: A case study. In Koelmans, A., Bystrov, A., Pont, M., eds.: *Proceedings of the 1st UK Embedded Forum*, University of Newcastle upon Tyne (2004) 54–65
13. Phatrapornnant, T., Pont, M.J.: Reducing jitter in embedded systems employing a time-triggered software architecture and dynamic voltage scaling. *IEEE Transactions on Computers* **55**(2) (2006) 113–124
14. Edwards, T., Pont, M.J., Scotson, P., Crumpler, S.: A test-bed for evaluating and comparing designs for embedded control systems. In Koelmans, A., Bystrov, A., Pont, M., eds.: *Proceedings of the 1st UK Embedded Forum*, University of Newcastle upon Tyne (2004) 106–126
15. Key, S., Pont, M.J.: Implementing PID control systems using resource-limited embedded processors. In Koelmans, A., Bystrov, A., Pont, M., eds.: *Proceedings of the 1st UK Embedded Forum*, University of Newcastle upon Tyne (2004) 76–92
16. Bate, I.J.: *An Architecture for Distributed Real-Time Systems*. University of York, Department of Computer Science, University Technology Centre (UTC). (1997)
17. Maaita, A., Pont, M.J.: Using ‘planned pre-emption’ to reduce levels of task jitter in a time-triggered hybrid scheduler. In: *Proceedings of the 2nd UK Embedded Forum*. (2005)
18. Lysecky, R., Vahid, F.: A study of the speedups and competitiveness of FPGA soft processor cores using dynamic hardware/software partitioning. In: *Proceedings of the European Conference on Design, Automation and Test (DATE)*, Munich, Germany, IEEE Computer Society (2005) 18–23
19. Gray, J.: *Designing a Simple FPGA-Optimized RISC CPU and System-on-a-Chip*. Gray Research LLC, <http://www.fpgacpu.org>. (2000)
20. Buttazzo, G.C.: Rate monotonic vs. EDF: Judgement day. *Real-Time Systems* **29** (2005) 5–26
21. Rau, B.R., Fisher, J.A.: Instruction-level parallel processing: History, overview, and perspective. *The Journal of Supercomputing* **7**(1 - 2) (1993) 9–50
22. Johnson, M.: *Superscalar Microprocessor Design*. Prentice-Hall (1991)
23. Torng, H.C., Vassiliadis, S., eds.: *Instruction Level Parallel Processors*. IEEE Computer Society Press, Los Alamitos, CA (1995)
24. Aditya, S., Mahlke, S.A., Rau, B.R.: Code Size Minimization and Retargetable Assembly for Custom EPIC and VLIW Instruction Formats, HPL-2000-141. HP Laboratories, Palo Alto. (2000)

25. Aditya, S., Rau, B.R.: Automatic Architecture Synthesis and Compiler Retargeting for VLIW and EPIC Processors, HPL-1999-93. HP Laboratories, Palo Alto. (1999)
26. Pillai, S., Jacome, M.F.: Compiler-directed ILP extraction for clustered VLIW/EPIC machines: Predication, speculation and modulo scheduling. In: Proceedings of the European Conference on Design, Automation and Test (DATE), Munich, Germany, IEEE Computer Society (2003) 422–427
27. Rajagopalan, S., Rajan, S.P., Malik, S., Rigo, S., Araujo, G., Takayama, K.: A retargetable VLIW compiler framework for DSPs with instruction-level parallelism. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* **20** (2001) 1319
28. Halambi, A., Grun, P., Ganesh, V., Khare, A., Dutt, N., Nicolau, A.: EXPRESSION: A language for architecture exploration through compiler/simulator retargetability. In: Proceedings of the European Conference on Design, Automation and Test (DATE), Munich, Germany, IEEE Computer Society (1999) 485
29. Henzinger, T.A., Benjamin, H., Kirsch, C.M.: Embedded control systems development with giotto. *SIGPLAN Notices* **36** (2001) 64
30. Jie, L., Lee, E.A.: Timed multitasking for real-time embedded software. *IEEE Control Systems Magazine* **23** (2003) 65
31. Mellor, S.J.: Automatic code generation from UML models. C++ Report **11**(4) (1999) 28–33 automatic code generation;UML;high-level language compilers;notation;object-oriented systems;.
32. Mwelwa, C., Pont, M.J., Ward, D.: Code generation supported by a pattern-based design methodology. In Koelmans, A., Bystrov, A., Pont, M., eds.: Proceedings of the 1st UK Embedded Forum, University of Newcastle upon Tyne (2004) 36–55
33. Vidler, P.J., Pont, M.J.: Automatic conversion from ‘single processor’ to ‘multi-processor’ software architectures for embedded control systems. In Koelmans, A., Bystrov, A., Pont, M.J., Ong, R., Brown, A., eds.: Proceedings of the 2nd UK Embedded Forum. (2005)
34. Ayavoo, D., Pont, M.J., Parker, S.: A ‘hardware-in-the-loop’ testbed representing the operation of a cruise-control system in a passenger car. In: Proceedings of the 2nd UK Embedded Forum. (2005)
35. ISO/DIS 11898: Road Vehicles — Interchange of Digital Information — Controller Area Network (CAN) for High Speed Communication. (1992)
36. Nahas, M., Short, M.J., Pont, M.J.: The impact of bit stuffing on the real-time performance of a distributed control system. In: Proceedings of the 10th International CAN Conference, Rome (2005)
37. Marti, P., Fuertes, J.M., Fohler, G.: A control performance metric for real-time timing constraints. In: Proceedings of the 14th Euromicro International Conference on Real-Time Systems. (2002)
38. Dorf, R.C., Bishop, R.H.: Modern Control Systems. Seventh edn. Addison-Wesley (1995)

A Template Language for Agent Construction

Li Xiaohong, Feng Zhiyong, Li tie, and Lv Li

School of Computer Science and Technology,
Tianjin University,
300072, Tianjin, P.R. China
{xiaohongli, zhiyongfeng}@tju.edu.cn

Abstract. This paper proposes a XML based Agent template language (ATL) for Agent construction upon blackboard pattern. Agent analysis and design model can be mapped upon ATL under forward engineering, and ATL can be translated into a Java source code by given compiler ATLC, which can be operated by JDK again. Therefore, a bridge between Agent-oriented analysis and design Model and existing OO program environment is constructed to develop Agent system rapidly. The open source platform, IBM Eclipse, is used as the base to implement the ATL integrating environment.

1 Introduction

With the deepening of agent techniques research, agent-oriented analysis and design model, and the agent-oriented software engineering (AOSE) gradually become a research focus in recent years. Wooldridge, etc.[1] have proposed Gaia of agent-oriented model language, which is based on static structure, therefore it is difficult to describe the dynamic change of structure to express the complicated structure and control flow. Thomas Juan[2] put forward an open complicated system by extending the Gaia. Giovanni Caire, etc.[3] have proposed a method by improving and expanding UML to describe agent-oriented system. Li B, etc.[4] based on BDI model and situation calculus, provide an Agent architecture, in which some facilities for representing intelligent agent are provided, such as belief, goal, strategy and so on, reasoning about action and planning. Zhang Wei, etc.[5] base on π -calculus and the chemical abstract machine(CHAM), provide a formal semantics of process of agent organization structure, in which the components associated with the organization structure are taken as molecules of CHAM and use the executions of the CHAM to express procedures of Agent organization structure. Guo L, etc.[6] propose an agent-oriented programming language with intention driver based on opened situation calculus, which is called AOPLID. AOPLID is inconvenience of describing the agent's mental state, lack of communication. In this paper, we designed an agent template language(ALT), which aims at the field of integration of enterprise information system. Agent analysis and design model can be mapping on ATL by engineering, and ATL can be translated into Java source code through its compiler ATLC, Java source code compiled out like this passes compiling and becoming java code that can be operated by JDK again, namely agent program that

can be operated actually. Then, we erect a bridge among agent-oriented design and object-oriented programming. Finally, we regarded IBM Eclipse system as the platform and offered an integrated developing environment for ATL, offered GUI for design and interact, perfected text editor and integrated edit, compile, operation platform.

2 System Architecture

Fig.1 is a multi-agent platform, which includes agents, runtime platform (multi-agent operation platform) and a J2EE agent server. We code the agent program with ALT and compile to java. The operation of the agent needs the assistance of the platform (Runtime Platform) while operating. Agent server is built in J2EE server, can offer name service, Ontology service and search service base ability.

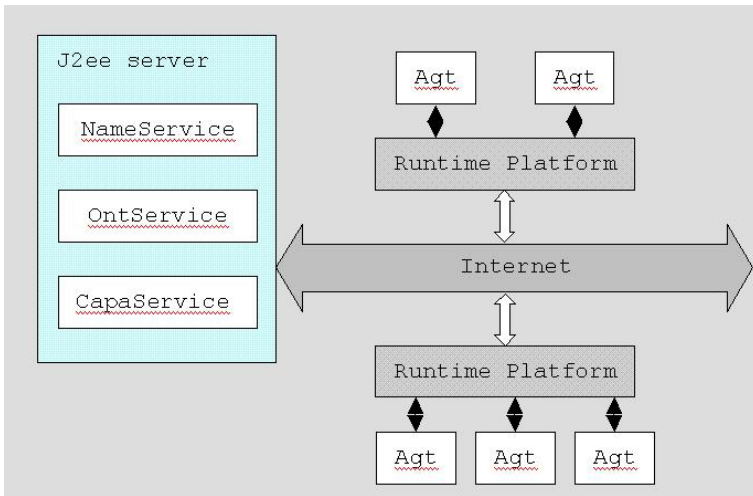


Fig. 1. Multi-agent Platform

An application protocol, ARCP, is defined for interact between agent and platform (the communication protocol among agent - operation platform). The protocol works by client/server, adopt Java's RMI to transfer and transmit mechanism as floor. The main function of ARCP includes connect, identity verify, name and ability register and message transmit, each function can be encapsulated and become a Java class. The advantage of RMI is that it can make agent and platform at the distributed computer.

The message transmitting between platform on JMS, a message middleware service provide by J2EE, offer a perfect solution for communication between the packages of application program. So the platform can be divided into two

layers: The upper, ARCP servers, implement the main function of ARCP, the lower, JMS customer, transmits the message between platform.

The agent services are constructed on J2EE server as EJB. Some agent services, such as name service, Ontology service and ability service, are showed in Fig 1. The name service is a catalogue service, JNDI can be used to register agent name, physics address and state information. Ontology service provide modeling and formalizing the enterprise resources, offer semantic support for agent communication. Ability service is used for finding and releasing/subscribing platform, it is responsible for registering ability key word and service that each agent can be offered to the external. Agent can inquire about ability of other agent and service information by platform.

3 Agent Structure and ATL Language

In paper[7], we have structure the agent by blackboard pattern. The blackboard is for common data exchanging, message parts and goal structure are designed as knowledge source, and Agenda based blackboard controller is in charge of agent action planning.

Definition 1: Agent is a six member group $\langle X, S, G, P, M, R \rangle$, where
 X is blackboard object aggregation:
 $X = \text{DataStructure, ClauseStructure, MessageStructure, ControlData}$
 S is scale of the blackboard object value
 G is goal structure set, goal structure is a mapping from goal expression to action plan, viz. $\text{IntentionExpression} \rightarrow \text{Plan}$
 P is action plan aggregation:
 $P = \langle \text{StateSet, TransactionSet, TransactionRule} \rangle$
 M is message action, $M : \text{Message} \rightarrow X$
 R is the relation between goal structure

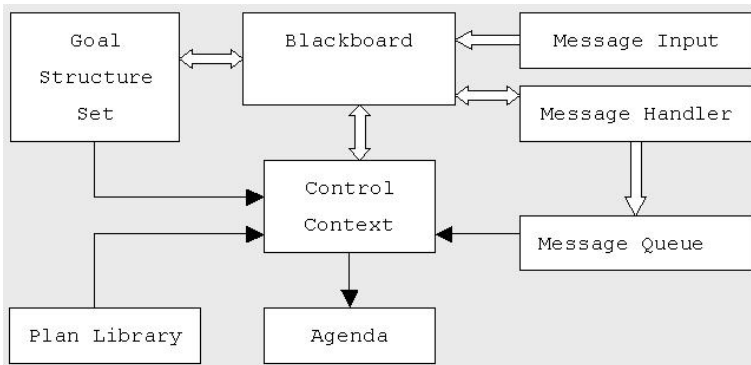


Fig. 2. Blackboard based Agent model

On the basis of Blackboard based Agent model, a rapid development tool, ATL(Agent Template Language), is developed, which is enterprise business process integrating and interaction oriented. The specification of ATL is described with EBNF as follow:

```

<AgentProgram> ::= AGENT_PROGRAM <AgentName>
                <DefOntology>
                <DefR_Fluents><DefF_Fluents><DefServices>
                <DefPlanTemplate>
                <Beliefs>
                <Goals>
<DefOntology> ::= DEF_ONTOLOGY
                [<DefFrameClass>;]*
                [<InsertOperation>;]*
<DefR_Fluents> ::= DEF_RELATIONAL_FLUENTS
                [<R_FluentName>[( <VarType>*)]];)*
<DefF_Fluents> ::= DEF_FUNCATIONAL_FLUENTS
                [<FunctionType><F_FluentName>[( <VarType>*)]];)*
<DefServices> ::= DEFINE_SERVICES
                [<DomainName>.<ServiceName>[( <VarType>*)]];)*
<DefPlanTemplate> ::= DEFINE_PLAN_TEMPLATE
                (PLAN_TEMPLATE <TemplateName>[( <VarType> <Variable>]*)
                :INIT_STATE <StateConst>
                :FINIAL_STATES <StateConst>*
                :RULE {( <StateConst,<ActionName>*)}* );
                {(ACTION <ActionName>
                :NEXT_STATE <StateConst>
                [:PRECONDITION <Sentence>]
                [:DO <send>|<recv>|<ServiceCall>]
                [:EFFECT <EffectFormula>]);)*
<Beliefs> ::= BELIEFS <Sentence>
<Goals> ::= {GOALS(<Intention>,<TemplateName>
                ( [<Variable>]* ),<Weight>);}*
<DefFrameClass> ::= (TYPE <ClassName>
                :SUPER_TYPE<ClassName>[,<ClassName>]*
                [:SLOT (<SlotName> <SlotType>
                [RESTRICTION <Value>]*
                [DEFAULT <Value>])]);)*
<SlotType> ::= <ClassName> | <PrimaryType>
<Value> ::= value of slot that fits the slot type.
<InsertOperation> ::= INSERT <InstanceName> INTO <ClassName>
                [WITH] [<AssertStatement>]* ;
<AssertStatement> ::= <SlotName>=<Value> | <SlotName> {<Value>}*}
<VarType> ::= <ClassName> | <PrimaryType>
<FunctionType> ::= <ClassName> | <PrimaryType>
<Sentence> ::= <Literal> [and <Literal>]*;

```



```

<Literal> ::= <Condition> | <R_FluentName>[( <term>*)] |
           not <Literal>
<Condition> ::= <term> <op> <term>
<term> ::= <F_FluentName>[( <term>*)] | <Variable> | <Value> |
           <InstanceName>[. <SlotName>]+
<op> ::= > | >= | < | <= | =
<send> ::= send(<receiver>, <performative>, <conversation>, <content>);
<recv> ::= recv(<sender>, <performative>, <conversation>,
               <contentPattern>);
<ServiceCall> ::= <Domain>.<ServiceName>(<term>)*;
<EffectFormula> ::= <wff>[and <wff>]*
<wff> ::= <Literal> | <Literal> [and <Literal>] -> <Literal>
           [and <Literal>]*
<OntFile> ::= String specifying the ontology definition file.
<ClassName> ::= String specifying the frame class.
<SlotName> ::= String specifying the slot.
<PrimaryType> ::= all primary types of Java Language.
<R_FluentName> ::= string specifying the relational fluent.
<Variable> ::= String specifying the variable.
<StateConst> ::= String specifying the state const.
<ActionName> ::= String specifying the action.

```

4 ATL Based Agent Implementation

ATL based Agent includes the following parts: external program or the software, resource assemble, control rule sets , action sets and interactive protocol sets. Therefore, agent has offered support components, as Fig.3. Agent model is relevant with program segments of ATL, rule controlling manager is in charge of management control rule, which is compiled into one java class. Interactive manager manages conversation adapter which forward conversation process. Action manager handle the action expression, in which an action queue is used to select the actions to execute in turn. At last, service request has been transmitted to service interface, and the services are activated dynamically and returned the results immediately.

Interactive protocol is corresponding to a finite state automatically, and ATL compiler compile it into a cooperation compose by Java class. In Fig. 3, agent component about interactive protocol is interaction manager and protocol adapter, the protocol adapter is responsible for communication rule management. The interaction manager maintains the message queue, and deliver it to message adapter. The protocol adapter manages communication rules, and match corresponding messages from the message queue to communication rules. In addition, the adapter maintains the present conversation state, and activate corresponding communication rules dynamically.

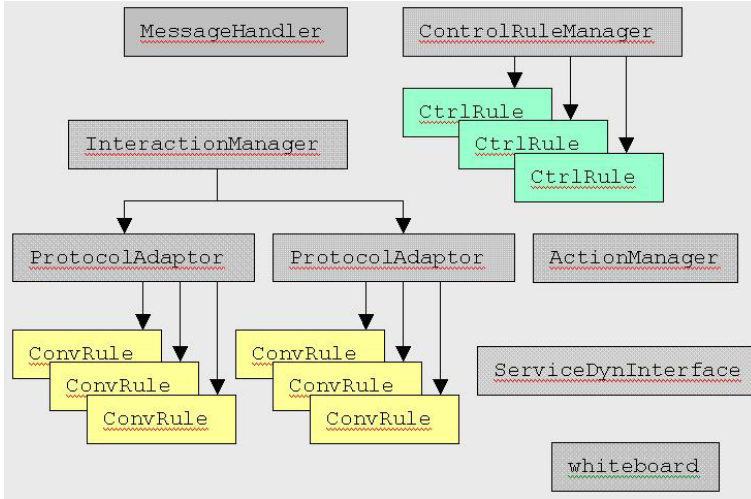


Fig. 3. Agent Implementing

5 ATL Integrating Development Environment Based on Eclipse

Eclipse, a general integrated development environment developed by IBM, is used to develop ATL IDE. Eclipse tool including: Regard ATL development environment as the core, offered an interactive protocol editor with GUI, an automatically editor tool base on guide and serve manage interface to configure platform. In implementation, A complete class library supporting those layers is being written. Object routing layer, implemented as some EJB components, serves as the runtime environment for our platform. Now we plan to develop an IDE for this platform. We need develop some new tools based on Eclipse runtime and JDT. The following is a brief summary of these tools.

ATL development environment. For ATL, we want to build a JDT-like tool, with the user interface in a UI plug-in and non-UI infrastructure in a separate core plug-in. UI plug-in uses the perspective-view-editor pattern environment, just like JDT. We define four views: task connector view, task object view, conversation pattern view and rule set view. Non-UI infrastructure consists of interpreter plug-ins, class library structure model, conversation pattern model, java compiler plug-in and its project nature.

User writes ATL codes in the editor. When finished, java code is generated by the interpreter and compiled into class files later. Finally, classes representing the real node agent are generated.

Conversation protocol editor. Conversation protocol editor is a new type of editor, which supplies user with graphic elements to depict a DFA (Determinate Finite Automata), and the logical relationship between the elements is interpreted into a XML file, which serves as the conversation pattern. User should append

other necessary information to that file to complete a conversation protocol, and register it to the conversation manager. This editor can serve as a tool plugging into ATL development environment.

Code generator tool. Code auto-generator is built on JDT and our finished class library. Wizard is provided to help user inputting necessary information, and skeleton code is generated according to the inputting information. User can extend these codes to form a complete program. Such tools should be useful for data provider, which wraps the database and serves as a database interface to upper layers. User input the data source information and table schemes using such wizard, and the entity bean skeleton code can be generated. Because code generation technique has been involved in the ATL development environment, the main idea of this tool is integrating code generation with wizard.

Service management tool. This tool connects the projects in workspace with EJB services that have been deployed to user's J2EE Application server. These EJB services form the Object Routing Layer, serving as the runtime kernel.

6 Conclusion

A new manage mode of smart supply chain, business process reengineering etc put forward the challenge to enterprise information system. In this paper, multi-agent architecture is tried to construct a dynamic, expandable and high flexible information system. In this way, a solution facing specific area is offered to customize information system fast and to realize the dynamic alliance of enterprise under the uncertain condition.

References

1. Michael Wooldridge, Nicholas R Jennings, David Kinny. The Gaia Methodology for Agent-Oriented Analysis and Design. *Autonomous Agents and Multi-Agent Systems*, 3 (2000): 285-312.
2. Thomas Juan, Adrian Pearce, and Leon Sterling. ROADMAP:Extending the Gaia Methodology for Complex Open Systems
3. Giovanni Caire, Francisco Leal, et al. Agent Oriented Analysis using MESSAGE/UML
4. Li B, L J, Zhu WJ. An Agent architecture based on situation calculus. *Journal of Software*, 2003,14(4): 733 742.
5. Zhang Wei, SHI Chun-yi, A Formal Semantics of Agent Organization Structure Design,, *journal of software* , 2002, 13(3): 447-452
6. Guo L, Ge YT, Chen SF, Zhang DM. An agent-oriented programming language with intention driver. *Journal of Software*, 2003,14(3):383 391.
7. Agent design and implementation base on Blackboard, technological report, Agent research group, Tianjin University, P R China.

Efficient Parallel Processing for K -Nearest-Neighbor Search in Spatial Databases

Yunjun Gao, Ling Chen, Gencai Chen, and Chun Chen

College of Computer Science, Zhejiang University,
Hangzhou, 310027, P.R. China
{gaoyj, lingchen, chengc, chenc}@cs.zju.edu.cn

Abstract. Even though the problem of k nearest neighbor (k NN) query is well-studied in serial environment, there is little prior work on parallel k NN search processing in parallel one. In this paper, we present the first Best-First based Parallel k NN (BFP k NN) query algorithm in a multi-disk setting, for efficient handling of k NN retrieval with arbitrary values of k by parallelization. The core of our method is to access more entries from multiple disks simultaneously and enable several effective pruning heuristics to discard non-qualifying entries. Extensive experiments with real and synthetic datasets confirm that BFP k NN significantly outperforms its competitors in both efficiency and scalability.

1 Introduction

Given a query point q and a dataset s , a k NN query retrieves the k closest objects in s whose distances (in this paper we use *Euclidean distance*) from q are not larger than that of the k -th furthest NN of q . Formally, k NN(q) = $\{p \in s \mid \text{dist}(p, q) \leq \text{dist}(p_k, q)\}$, where p_k is the k -th farthest NN of q and dist is a distance metric. For instance, “*find the k nearest hotels to the airport*”. In the last decade, the problem has already attracted considerable attention in the database community, since it is one of the most important operations in spatial databases, and its application domains mainly involve location based services, advanced traveler information systems, and so forth.

Surprisingly, in spite of the problem is well-studied in serial environment, there is little prior work on parallel processing for k NN search in parallel one (e.g., multi-disk setting etc.). Most of previous methods are based on either Depth-First (DF) algorithm [2, 3] or Best-First (BF) one [1, 4]. They can efficiently perform in the serial context that uses only a single disk. In particular, various algorithms relied on BF are the optimal ones in terms of query cost (including CPU time and I/O overhead) and the number of node accesses. Their efficiency, however, significantly degrades in parallel environment, because they do not exploit any kind of parallelism. Specifically, query cost is increasing, such that it can not satisfy user requirements. Also, I/O overhead is large, easily leading to the I/O bottleneck. Hence, it is evident that efficiently parallel processing techniques for k NN retrieval need to be developed.

Motivated by aforementioned problem, in this paper, we focus on multi-disk architecture (consisting of one processor with several disks attached to it), as this

architecture is simple and cheap, i.e., it requires only widely available off-the-shelf components, without multiple CPUs and specialized operating system. On the architecture, we develop the first Best-First based Parallel k NN (BFP k NN) query algorithm for efficient processing of k NN search with arbitrary values of k , using a parallel R-tree [9] (described in Section 2.1 of this paper). The key idea of our method is to access more entries from multiple disks in parallel, and enable some effective pruning heuristics to discard the non-qualifying entries that can not contribute to the final answer. Finally, extensive experiments with real and synthetic datasets verify that BFP k NN is efficient, and clearly outperforms by factors alternative approaches (containing FPSS and CRSS [5]) in both efficiency and scalability.

The rest of the paper is organized as follows. Section 2 surveys the previous work related to ours. Some definitions and problem characteristics are studied in Section 3. Section 4 presents BFP k NN algorithm. Extensive experimental evaluations are described in Section 5. Section 6 concludes the paper with directions for future work.

2 Related Work

2.1 R-Trees

Among various spatial indexing structures, R-tree [6] and its variants (e.g., R^+ -tree [7], R^* -tree [8], etc.) are the most widely accepted and used ones due to their popularity and efficiency in the literature. They can be thought of as extensions of B-trees (e.g., B^+ -tree) in multi-dimensional space. Figure 1a shows a set of points $\{a, b, \dots, l\}$ indexed by an R-tree (shown in Figure 1b), suppose that each node encloses at most three entries (i.e., the capacity of per node is three). In this example, according to the spatial proximity, 12 points are clustered into 4 leaf nodes $\{N_3, N_4, N_5, N_6\}$, which are then recursively grouped into nodes N_1, N_2 that become the entries of a single root node. Each node of the tree corresponds to one disk page. Intermediate nodes (e.g., N_3, N_4) contain entries of the form $(R, childptr)$, where R is the *Minimum Bounding Rectangle* (MBR) that covers all the MBRs of its descendants and $childptr$ is the pointer to the page in which the specific child node is stored. Leaf entries (e.g., a, b, c) store the coordinates of data points and (optionally) pointers to the corresponding records. Generally, k NN query algorithms on R-trees utilize three bounds to prune search space, i.e., (i) $mindist(q, R)$, (ii) $maxdist(q, R)$, and (iii) $minmaxdist(q, R)$, where q denotes a given query point. As an example, Figure 1a also illustrates these distance metrics.

In this paper, we base our work on the parallel R-tree of Kamel and Faloutsos [9], which distributes the nodes of a traditional R-tree with cross-disk pointers depended on a simple hardware architecture comprising of one processor with several disks attached to it. For example, one possible parallel R-tree corresponding to the R-tree of Figure 1b is shown in Figure 1c, where the root node (representing as thick line) is kept in main memory, whereas other nodes (e.g., N_3, N_4 , etc.) are assigned over disks 1 and 2. It operates exactly like a single-disk

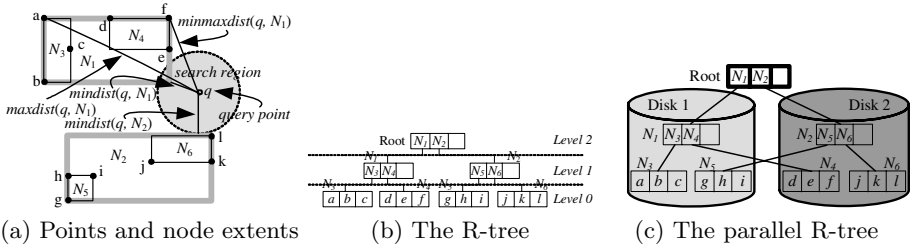


Fig. 1. Example of an R-tree, a parallel R-tree and three distance metrics in 2D space

R-tree. The only difference is that its nodes are carefully distributed over multiple disks. For the parallel R-tree, each pointer consists of a *diskid* (indicating the tag of one disk), in addition to the *pageid* (specifying the label of one page) of the traditional R-tree.

2.2 Existing Parallel kNN Search Algorithms

To our knowledge, the existing parallel algorithms for kNN queries are presented in [5, 11, 12, 14]. Specifically, Papadopoulos and Manolopoulos [5] present several parallel kNN search approaches using a parallel R-tree, which is distributed among the components of a disk array. But it provides no experimental results for large datasets (more than 10k bytes). In [11], a parallel method for NN search in high-dimensional data spaces is proposed. The solution concentrates on how to decluster data. [12] develops an efficient query processing strategy for parallel NN retrieval, based on multi-processor and multi-disk architecture, in which the processors communicate via a network and data objects are stored in a declustered R-tree (assuming an environment such as in [13]). However, it provides no experimental results for high-dimensional space (more than 2-dimensional space). Additionally, a parallel algorithm for solving the problem relied on the generalized Voronoi diagram construction is also presented in [14]. In this paper, the proposed algorithm is based on the multi-disk setting, which is similar to the environment in [5]. Thus, we experimentally evaluate our algorithm by comparing it against FPSS and CRSS presented in [5].

3 Definitions and Problem Characteristics

Even though three distance metrics (including *mindist*, *minmaxdist*, and *maxdist*) are defined in [2, 12], they can not directly be applied to the parallel environment. Thus, we need extend them and newly define a set of useful functions and distance metrics aiming at the multi-disk setting, in order to devise efficient parallel algorithms for kNN queries and derive several pruning heuristics for avoiding visiting the unnecessary entries. Let N_i be the i -th node's MBR of the parallel R-tree, and Q_i the i -th priority queue corresponding to the i -th disk. Then these functions and distance metrics are defined as follows.

Definition 1. Let p be a point in d -dimensional space (representing the NN of a given query point q) with coordinates $p = (p_1, p_2, \dots, p_d)$, and $D_{nn}(q, p)$ the distance between q and p . Then the $D_{nn}(q, p)$ can be defined as:

$$D_{nn}(q, p) = \sqrt{\sum_{i=1}^d (q_i - p_i)^2} \quad (1)$$

Definition 2. If a priority queue Q maintains k elements, $Firstmindist(Q)$ denotes the minimal mindist in Q . Then the $Firstmindist(Q)$ is defined as:

$$Firstmindist(Q) = \min_{1 \leq i \leq k} \{mindist(q, N_i)\} \quad (2)$$

Definition 3. If multi-disk setting has M disks, a priority queue Q is deployed for each disk. Let $min\text{-}mindist(Q_1, Q_2, \dots, Q_M)$ be the smallest mindist among all the non-empty priority queues Q_i ($1 \leq i \leq M$). Then it can be defined as:

$$min\text{-}mindist(Q_1, Q_2, \dots, Q_M) = \min_{1 \leq i \leq M} \{Firstmindist(Q_i)\} \quad (3)$$

Definition 4. If a priority queue Q stores k elements, $Firstminmaxdist(Q)$ represents the minimum minmaxdist in Q . Then the $Firstminmaxdist(Q)$ is defined as:

$$Firstminmaxdist(Q) = \min_{1 \leq i \leq k} \{minmaxdist(q, N_i)\} \quad (4)$$

Definition 5. If multi-disk architecture contains M disks, a priority queue Q is configured for each disk. Let $min\text{-}minmaxdist(Q_1, Q_2, \dots, Q_M)$ denote the minimal minmaxdist within all the non-empty priority queues Q_i ($1 \leq i \leq M$). Then it can be defined as:

$$min\text{-}minmaxdist(Q_1, Q_2, \dots, Q_M) = \min_{1 \leq i \leq M} \{Firstminmaxdist(Q_i)\} \quad (5)$$

Definition 6. If a priority queue Q encloses k elements, $Firstmaxdist(Q)$ specifies the smallest maxdist in Q . Then the $Firstmaxdist(Q)$ is defined as:

$$Firstmaxdist(Q) = \min_{1 \leq i \leq k} \{maxdist(q, N_i)\} \quad (6)$$

Definition 7. If multi-disk environment involves M disks, a priority queue Q is disposed for each disk. Let $min\text{-}maxdist(Q_1, Q_2, \dots, Q_M)$ indicate the minimum maxdist in all the non-empty priority queues Q_i ($1 \leq i \leq M$). Then it can be defined as:

$$min\text{-}maxdist(Q_1, Q_2, \dots, Q_M) = \min_{1 \leq i \leq M} \{Firstmaxdist(Q_i)\} \quad (7)$$

Lemma 1. Consider the definitions of $D_{nn}(q, p)$, $min\text{-}mindist$, $min\text{-}maxdist$, and $min\text{-}minmaxdist$, the inequalities involving $min\text{-}mindist \leq D_{nn}(q, p) \leq min\text{-}minmaxdist$ and $min\text{-}mindist \leq D_{nn}(q, p) < min\text{-}maxdist$ hold.

Proof. From the definitions of $D_{nn}(q, p)$, $min\text{-}mindist$, $min\text{-}minmaxdist$, and $min\text{-}maxdist$. \square

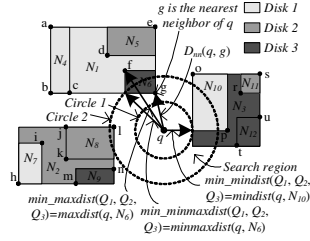


Fig. 2. Illustration of four distance metrics and search strategy in 2D space

Figure 2 illustrates the above distance metrics. Furthermore, following lemma can be also derived and proved according to these definitions. As demonstrated in Figure 2, where four distance metrics (indicated solid lines with arrows together) satisfy the Lemma 1. Also note that we follow a search strategy that finds k NNs of q from *circle 1* to *circle 2* (shown in Figure 2) in the proposed algorithm for processing kNN search.

4 Algorithm

4.1 Pruning Strategies

For effective processing of kNN retrieval, two parameters (containing *ResultQueue* and $kDist$) are introduced into BFP kNN . Specifically, *ResultQueue* maintains the current k most promising answers (which can be become the final NNs of q) sorted in descending order with respect to the *mindist* metric, such that the greatest *mindist* (representing *ResultQueue.MaxDist*) enclosed in it can be captured instantly. The $kDist$ specifies the current minimal *maxdist* ensuring that it contains at least k objects among all the *maxdist*(s) between q and entries retrieved so far. Associating with both arguments (i.e., *ResultQueue.MaxDist* and $kDist$), the following pruning heuristics can be developed in order to prune the search space and terminate the execution of the algorithm accordingly.

Heuristic 1: Let q be a given query point, and the entry E_{min} with the minimum distance to q among all the entries enclosed in priority queues. If the distance between E_{min} and q is greater than *ResultQueue.MaxDist*, then the remainder (including E_{min}) in all priority queues can be discarded and the algorithm can be also terminated accordingly, since their distances from q are all larger than that of the current k -th farthest NN in *ResultQueue* of q .

Heuristic 2: If a node entry E whose distance from a given query point q is larger than the current value of $kDist$, then the entry E can be safely pruned as it can not become one of the final k NNs of q .

Heuristic 3: If an actual distance from a given query point q is greater than the current value of $kDist$, then it can be safely discarded because it can not be enclosed in the final k NNs of q .

4.2 BFP k NN Algorithm

Toward BFP k NN algorithm, it implements an ordered best-first traversal. BFP k NN begins with the root node of parallel R-tree and proceeds down the tree. It consists of the following three different steps:

Step 1: Suppose that the number of disks is M , BFP k NN creates and initializes M priority queues (specifying Q_1, Q_2, \dots, Q_M) for M disks and *ResultQueue* used to keep the current k most promising answer.

Step 2: BFP k NN inserts all the entries enclosed in the root node of parallel R-tree into their corresponding priority queues (e.g., heaps), and records the current value of $kDist$ guaranteeing that it covers at least k objects.

```

BFPNN (QueryObject  $q$ , Parallel R-tree,  $M, k$ )
/* Temp_kDist maintains the temporal value of kDist; FindNextNode ( $Q_i$ ) finds the next non-data object
(i.e., intermediate node) in  $Q_i$ . */
1. Construct and initialize  $M$  priority queues (i.e.,  $Q_1, Q_2, \dots$ , and  $Q_M$ );
2. Construct and initialize ResultQueue; // initialize the ResultQueue infinity
3. For each entry  $E$  in the root node do
4.    $i = \text{FindDisk}(E)$ ; // find the tag of disk storing the entry  $E$ 
5.   EnQueue ( $Q_i, E, \text{Dist}(q, E)$ ); // insert the entry  $E$  into corresponding queue  $Q_i$ 
6. Record current  $kDist$  among all the entries in the root node;
7. While existing queue(s) is (are) not empty do
8.   Prune all unnecessary entries from each queue according to the heuristics 1, 2, and 3;
9.   Find the entry  $E_{min}$  with the minimum distance to  $q$  among all the entries enclosed in  $M$  queue(s);
10.  If  $\text{Dist}(q, E_{min}) \geq \text{ResultQueue.MaxDist}$  then
11.    Return ResultQueue;
12.  Else
13.    For  $i = 1$  to  $M$  parallel do
14.      If not IsEmpty ( $Q_i$ ) then
15.        If First ( $Q_i$ ) is not a data object then
16.           $N_i = \text{DeQueue}(Q_i)$ ;
17.        Else
18.           $E_i = \text{DeQueue}(Q_i)$ ;
19.          If  $\text{Dist}(q, E_i) < \text{ResultQueue.MaxDist}$  then
20.            Insert (ResultQueue,  $E_i, \text{Dist}(q, E_i)$ );
21.           $N_i = \text{FindNextNode}(Q_i)$ ; //  $N_i$  may be empty
22.          If not IsEmpty ( $N_i$ ) then
23.            For each entry  $E$  in  $N_i$  do
24.               $j = \text{FindDisk}(E)$ ;
25.              EnQueue ( $Q_j, E, \text{Dist}(q, E)$ );
26. Record current Temp_kDist among all the entries contained in all non-empty queue(s);
/* If current value of Temp_kDist is smaller than old value of
kDist, then algorithm has to update the value of kDist. */
27.  If Temp_kDist < kDist then
28.    kDist = Temp_kDist;
29. Enddo
End BFPNN

```

Fig. 3. Pseudo-codes of a BFP k NN algorithm

Step 3: BFP k NN iterates following operations until it finds the final k NNs of a given query point q . Algorithm discards all non-qualifying entries from each priority queue by the *heuristics* 1 to 3 firstly. Subsequently, the entry E_{min} with the minimal distance from q among all the entries contained in M priority queues is found. In practical implementation, the following two steps are exploited: (i) BFP k NN gets all entries $EH(s) = \{EH_1, EH_2, \dots, EH_M\}$ at the head of each priority queue firstly, assuming that all priority queues are sorted in ascending order with respect to the *mindist* metric. (ii) It discovers the entry E_{min} in $EH(s)$. Next, BFP k NN computes the distance from E_{min} to q , and judges whether $\text{Dist}(q, E_{min}) \geq \text{ResultQueue.MaxDist}$ holds or not. If the answer is true, BFP k NN returns *ResultQueue* (enclosing k NNs of q) and terminates the algorithm. In contrast, it fetches node entries or data points enclosed in all non-empty queues and enqueues them into corresponding priority queues in turn by parallelism. Here, we take two cases into account. The first one is

that if the heads of non-empty queues are not data objects (i.e., intermediate nodes), then $BFPkNN$ directly accesses these nodes and inserts all the entries within them in corresponding priority queue in parallel. Contrarily, the other case is that $BFPkNN$ computes the distances from q and compares them against $ResultQueue.MaxDist$. Without loss of generality, assume that $Dist(q, E_i) < ResultQueue.MaxDist$ holds, the entry E_i will be inserted into $ResultQueue$, since it may be enclosed in the final k NNs of q . Then, $BFPkNN$ finds the next non-data object N (notice that the N may be empty), and also enqueues its entries into corresponding priority queue by parallelism. To summarize the executive process of $BFPkNN$, Figure 3 shows the pseudo-code of a $BFPkNN$ algorithm.

5 Experimental Evaluation

This section evaluates the proposed algorithm using real and synthetic datasets. All algorithms (including $BFPkNN$, FPSS, and CRSS) were coded in C++. All experiments were performed on a Pentium IV 3.0 GHz PC with 2048 MB RAM.

5.1 Experimental Settings

We used two real datasets *Wave* that contains the 3-dimensional measurements of 60k wave directions at the National Buoy Center and *Color* comprising of the 4-dimensional color histograms of 65k images. Attribute values of both real datasets are normalized to the range $[0, 10000]$. We also created two synthetic datasets following the *Gaussian* and *Zipf* distributions, respectively. Specifically, the coordinates of each point in a *Gaussian* dataset are randomly distributed in $[5000, 250]$. For *Zipf* dataset, the coordinates follow a *Zipf* distribution with a skew coefficient 0.8. Every dataset is indexed by a parallel R-tree [9] distributed over multiple disks that are simulated on one 160 Giga disk (whose type is “*Maxtor 6Y160LO*”) using several labels of disks (specified *diskid*), and disk assignment straightforwardly follows the *Round-Robin* strategy. The node size of the parallel R-tree is fixed to 1024 bytes. The experiments examine the effect of following arguments: (i) k (representing the number of NNs), (ii) dimensionality, (iii) cardinality, and (iv) *disks* (denoting number of disks). Performance is measured by executing workloads, each consisting of 100 queries generated as follows: the query locations are uniformly distributed in the corresponding data space. For each experimental instance, the reported results represent the average cost per query for a workload with the same properties. Note that the query cost is calculated as the sum of the CPU cost and the I/O overhead computed by charging 10ms for each node access.

5.2 Experimental Results

The first set of experiments fixes *disks* to 5 (or 10), and measures the number of accessed nodes and the query cost of $BFPkNN$, FPSS, and CRSS as a function of k (varying from 1 to 800), using various real and synthetic datasets. Figures 4 and 5 demonstrate these experimental results. Clearly, the efficiency of $BFPkNN$

consistently outperforms that of its competitors for all cases. In particular, as illustrated in Figure 4, for excessively large k , these k accesses constitute a dominant factor in the overall overhead, which thus grows (almost) linearly with k . Specifically, with the growth of k , the number of accessed nodes of all algorithms ascends, as well as their performance difference enlarges gradually. The reason of these cases is that the algorithms need retrieve more node entries in order to prune the search space and find the best k NNs of a given query point q in the datasets, as k increases. Also, the query cost of BFP k NN is less than that of FPSS and CRSS (especially for FPSS), which is depicted in Figure 5.

Subsequently, we examined the impact of dimensionality. Toward this, we fix *disks* to 5 and k to 100 (which is the median value used in Figures 4-5) respectively, and compare the performance of three algorithms by varying dimensionality from 2D to 5D, using the *Gaussian* dataset with cardinality $N = 256k$. Figure 6 illustrates the number of accessed nodes and the query cost of all methods versus dimensionality for k NN search processing. As expected, the performance of all algorithms degrades because, in general, R-trees become less efficient as the dimensionality grows [10] (due to the larger overlap among the MBRs at the same level). However, the efficiency of BFP k NN is still evidently better than that of any other algorithm. Moreover, as dimensionality grows, the efficiency difference of three algorithms obviously increases between 3D and 5D, but similar performance is observed in 2D. Also notice note that the number of node accesses and the query cost grows (almost) exponentially with dimensionality, which is shown in the diagram.

To study the impact of dataset cardinality, we compared the performance of all algorithms under different cardinality varied from 32k to 2048k, fixing k to 100 and *disks* to 10, respectively. Figure 7 shows these experimental results on 3D (dimensionality = 3 is also the midvalue used in Figure 6) *Gaussian* dataset. As with the above experiments, BFP k NN is still significantly faster than FPSS and CRSS. In particular, note that the step-wise cost growth corresponds to an increase of the magnitude of cardinality from 32k to 2048k. In Figure 7, for instance, the growth obviously occurs at cardinality 256k with respect to 3D *Gaussian* dataset.

Finally, Figures 8 through 9 illustrate the number of node accesses and query cost as a function of *disks* (i.e., the number of disks), varying from 5 to 30. Similar to the phenomena of previous experiments, the efficiency of BFP k NN is more effective than that of FPSS and CRSS in all cases (over an order of magnitude). Also note that the query cost for each query workload clearly decreases as disks grows, which is due to the increase of parallelization.

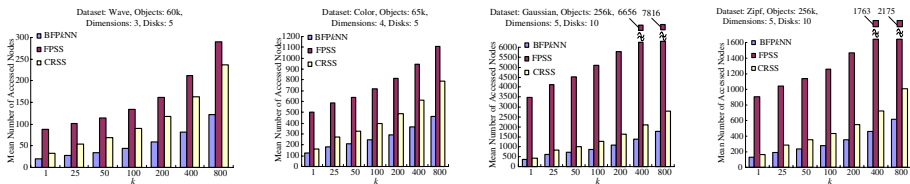


Fig. 4. Mean number of accessed nodes VS. k

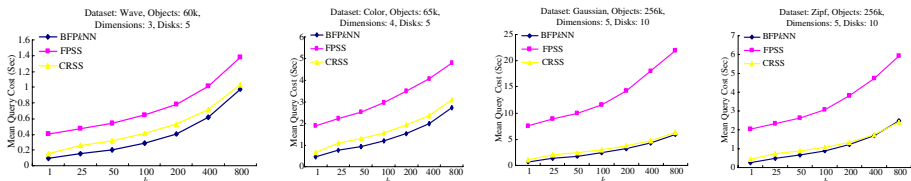


Fig. 5. Query cost (sec) VS. k

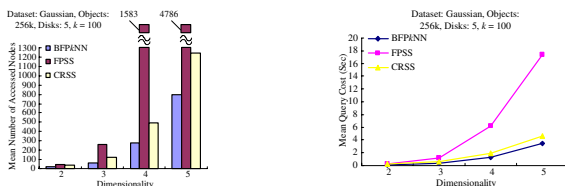


Fig. 6. Mean number of accessed nodes and query cost (sec) VS. Dimensionality

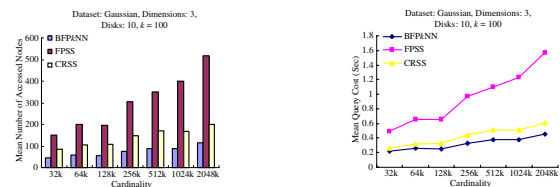


Fig. 7. Mean number of accessed nodes and query cost (sec) VS. Cardinality

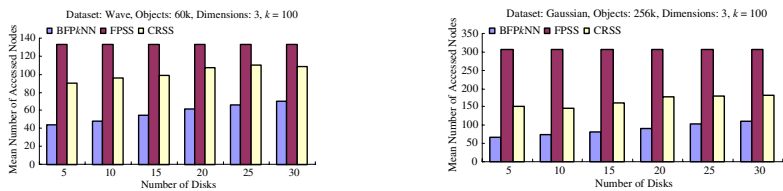


Fig. 8. Mean number of accessed nodes VS. Number of disks

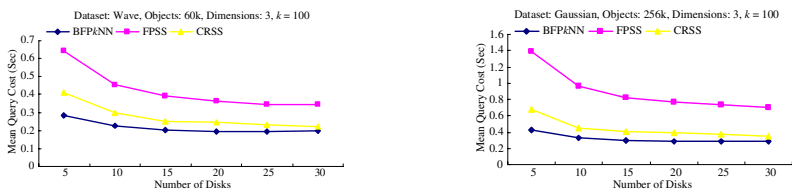


Fig. 9. Query cost (sec) VS. Number of disks

6 Conclusion

This paper investigates the problem of parallel processing for k NN queries over the multi-disk architecture. Our contribution is an efficient Best-First based Parallel k NN (BFP k NN) query algorithm for effective handling of k NN ($k \geq 1$) search by parallelism. Its core is to exploit parallelization to a sufficient degree through accessing more entries from multiple disks simultaneously, and enable several effective pruning heuristics to discard the non-qualifying entries. Furthermore, considerable experiments verify that BFP k NN significantly outperform its competitors in both efficiency and scalability, using real and synthetic datasets. In the future, some interesting directions for future work mainly concern the following issues: (i) study on various disk assignment approaches for enhancing parallelization, and (ii) derive analytical models for estimating the execution cost of parallel k NN search algorithm, so as to facilitate query optimization and reveal new problem characteristics that could lead to even faster algorithms.

Acknowledgement. This research was supported by the National High Technology Development 863 Program of China under Grant No. 2003AA4Z3010-03.

References

1. Henrich, A.: A distance-scan algorithm for spatial access structures. In: ACM GIS. (1994) 136–143
2. Roussopoulos, N., Kelley, S., Vincent, F.: Nearest neighbor queries. In: SIGMOD. (1995) 71–79
3. Cheung, K.L., Fu, A.W.-C.: Enhanced nearest neighbour search on the R-tree. ACM SIGMOD Record **27** (1998) 16–21
4. Hjaltason, G.R., Samet, H.: Distance browsing in spatial databases. ACM TODS **24** (1999) 265–318
5. Papadopoulos, A.N., Manolopoulos, Y.: Similarity query processing using disk arrays. In: SIGMOD. (1998) 225–236
6. Guttman, A.: R-trees: a dynamic index structure for spatial searching. In: SIGMOD. (1984) 47–57
7. Sellis, T., Roussopoulos, N., Faloutsos, C.: The R^+ -tree: a dynamic index for multi-dimensional Objects. In: VLDB. (1987) 507–518
8. Beckmann, N., Kriegel, H.-P., Schneider, R., Seeger, B.: The R^* -tree: an efficient and robust access method for points and rectangles. In: SIGMOD. (1990) 322–331
9. Kamel, I., Faloutsos, C.: Parallel R-trees. In: SIGMOD. (1992) 195–204
10. Theodoridis, Y., Sellis, T.K.: A model for the prediction of R-tree performance. In: PODS. (1996) 161–171
11. Berchtold, S., Böhm, C., Braunmüller, B., Keim, D.A., Kriegel, H.-P.: Fast parallel similarity search in multimedia databases. In: SIGMOD. (1997) 1–12
12. Papadopoulos, A., Manolopoulos, Y.: Parallel processing of nearest neighbor queries in declustered spatial data. In: ACM GIS. (1996) 35–43
13. Koudas, N., Faloutsos, C., Kamel, I.: Declustering spatial databases on a multi-computer architecture. In: EDBT. (1996) 592–614
14. Gavrilova, M.L.: On a nearest-neighbor problem under minkowski and power metrics for large data sets. J. of Supercomputing **22** (2002) 87–98

An Adaptive Mobile System Using Mobile Grid Computing in Wireless Network^{*}

Jehwan Oh, Seunghwa Lee, and Eunseok Lee^{**}

School of Information and Communication Engineering, Sungkyunkwan University,
300 Chunchun Jangahn Suwon, 440-746, Korea
{hide7674, jbmania, eslee}@selab.skku.ac.kr

Abstract. In order to overcome the constrained performance inherent in mobile devices, and to support services depending using wireless networks, an adaptive mobile system using mobile grid computing, is proposed. According to the mobile device environment, classes are composed of an application that executes on a specific mobile device, and allocated to surrounding devices containing idle resources. The effectiveness of this system is confirmed, by applying the system to an emergency environment, using mobile devices, which include a PDA and laptop.

1 Introduction

Using mobile devices to realize the full power of ubiquitous environments is becoming more widespread. Wireless Internet provides users with the ability to access information anywhere at anytime. This provision is continually developing in terms of technology and capability. However, mobile devices do not always satisfy user requests effectively, because they suffer from a small display, low speed CPU, and low capacity memory. In addition, because most existing content and services are optimized for desktop computing environments, the additional constraints of mobile devices in such environments are apparent. Mobile devices require adaptive services, to allow devices to recognize situations, analyze and adapt to data, and overcome the constrained performance of mobile devices. Ultimately reaching the goal of providing improved user satisfaction. There is the difficulty that when some devices solve adaptation services internally, intermediate systems, such as a proxy server are required, including middleware adaptation services. Most existing adaptive systems aim to solve the constraints of mobile devices through an intermediate medium (i.e. middleware, proxy server), however, middleware work load must assist in the satisfaction of mobile device users. For this reason, purchasing a more efficient computer or increasing the frequency of intermediate mediums may be costly, and only temporarily solves problems in the present situation. In order to effectively solve these issues, grid computing[1] is used. Grid computing uses the idle resources of many computers

^{*} This work was supported in parts by Ubiquitous Autonomic Computing and Network Project, 21th Century Frontier R&D Program and ITTA IT Research Center Program of Ministry of Information and Communication, Korea.

^{**} Corresponding author.

connected in a network, and therefore, appears similar to traditional wired networks. Grid computing enables the use of a connected, widely distributed set of traditional computing resources as an extremely efficient, large-scale, super-computing architecture, while operating in a cooperative environment.

Thus, in this paper, while considering technological and functional constraints of mobile devices, a method to process individual situations of each mobile device and problem(user's request) is proposed, efficiently solving issues, based on mobile grid computing, and extending traditional grid computing. Applications executed on the proposed system are implemented in object-oriented language. They divide requested tasks into object or component units, depending on their state of devices. Tasks are delivered to surrounding devices with idle resources. Finally, the result is received. These surrounding devices are not influenced by the total work required. Therefore, the problem of using the idle resources of devices connecting to the Access Point (AP) instead of an intermediate medium, is overcome. The various aspects of the proposed system expect to solve several constraints of wireless computing, offering a more efficient wireless computing environment.

The effectiveness of the proposed system is confirmed by applying the implemented prototype as a "Next Generation Healthcare Service", with mobile devices, including a PDA and laptop.

This study is composed of 5 sections. Related research is described in Section 2. The comprehensive structure and modules of the system are provided in Section 3. The evaluation of the system through implementation of a prototype is presented in Section 4. Conclusions are provided in Section 5.

2 Related Work

Using various methods, traditional research is progressing toward overcoming the limitations and computation-capacity of mobile devices in mobile environments [2,3,4,5,6,12].

Firstly, a method providing services to solve and manage required work using an intermediate medium, takes responsibility for a particular area. Representative research includes MobiPADS of Alvin T.S. Chan, et al.[2] and CARMEN of Paolo Bellavista, et al.[10] MobiPADS is designed to support context-aware processing by providing an execution platform enabling active service deployment and reconfiguration of service composition in response to varying context environments. The client(i.e. PDA, laptop) on MobiPADS determines adaptive services based on the current situation, the server on MobiPADS calculates a determined adaptation service and returns the result to the client. MobiPADS has the advantage of enabling adaptive service deployment and reconfiguration in response to varying context environments, but the server's workload increases since adaptive services for the client are executed on the server. CARMEN is capable of supporting the automatic reconfiguration of wireless Internet services in response to context changes without intervention of the service logic. CARMEN determines the context on the basis of declarative metadata, and provides adaptive services to the client in the proxy server accordingly. This system manages the client connecting to a proxy server using a mobile agent. This system also requires a server.

Secondly, the use of a specific intermediate medium(e.g. proxy server) that manages mobile devices is not required, however, a high performance computer is required. This computer exists independently and is used to solve the resource-constrained mobile device, according to the requirements. In the adaptive offloading system of Xiaohui Gu, et al.[9], the resource-constrained problem may be overcome by dynamically partitioning the application, and by offloading part of the application execution with data to a powerful nearby surrogate(i.e. a high performance computer). This system aims to solve resource-constraint issues, by employing a rich surrogate, however, but if it does not exist, it cannot execute.

Most related work solves the resource-constraint problem using an intermediate medium(e.g. proxy server, surrogate, middleware). However, this depends on the availability of the additional workload provided by the middle medium. The mobile device depends on an intermediate medium, to overcome the resource-constrained mobile device. Therefore, the intermediate medium can exist in any form.

3 Proposed System Architecture

3.1 Design Concepts

In this paper, the technological and functional constraints of mobile devices is considered, and a method is proposed for processing individual situations of each mobile device and problem (user's request), in order to be solved efficiently. The proposed system is based on mobile grid computing, which is an extension of traditional grid computing.

3.2 System Requirements

The following represent basic requirements for implementation of the proposed system.

- *System Profile*: The proposed system must recognize a change in resources, this is reflected in the proposed system. Information regarding resources may be divided into static resources and dynamic resources. Static resources represent information that does not change, such as CPU type, RAM size, storage size, and so on. Dynamic resources represent information that changes in response to varying environments, such as CPU load, free RAM, remaining battery, usable storage, and so on. The proposed system describes static and dynamic resource information using XML, and maintains a list of varying resources.
- *Application Profile*: The application is programmed in Java. Java is an object-oriented language, meaning that data is encapsulated and applications consist of a collection of objects. The application is designed so that distributed classes execute independently of each other. The *application profile* describes the required information for class execution.

3.3 System Architecture

The overall architecture of the proposed system is presented in Fig. 1, and is composed of two components: the Client Module, embedded in the client device, and the

Server Module, which operates on the server side. In addition, each module is composed of several components, as follows.

- *Resource Monitoring Module(RMM)*: The *Resource Monitoring Module* acts both as an aggregator of potential capacity, representing the characteristics of the devices used to create/manage the *System Profiles*, and as an inspector of the dynamically changing context information, i.e., CPU usage, network throughput, and so on, in order to perceive various environmental variations. This module determines the idle resources, and transmits AP(REMM) to the System Profile.

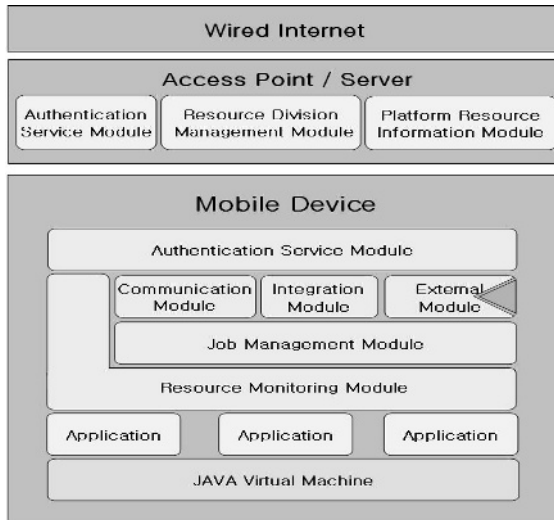


Fig. 1. Components of the Proposed System

- *Job Management Module(JMM)*: The *Job Management Module* divides required work based on the *System Profile* and *Application Profile*, collected by the *Resource Monitoring Module*.
- *Communication Module(CM)*: The *Communication Module* communicates with the AP and peer for interactions. It transmits surrounding objects to devices.
- *Integration Module(IM)*: The *Integration Module* integrates the results of the tasks that the surrounding devices execute.
- *External Module(EM)*: The *External Module* executes the object or component required by an external device.
- *Authentication Service Module(ASM)*: When a user connects to the AP for the first time, it identifies user information.
- *Platform Resource Information Module(PRIM)*: The *Platform Resource Information Module* stores the *System Profile* of devices that connect to the AP.
- *Resource Division Management Module(RDMM)*: The *Resource Division Management Module* represents mapping requested work and surrounding devices that have idle resources.

3.4 Proposed System Behavior

The overall flow of the proposed system is presented in Fig. 2.

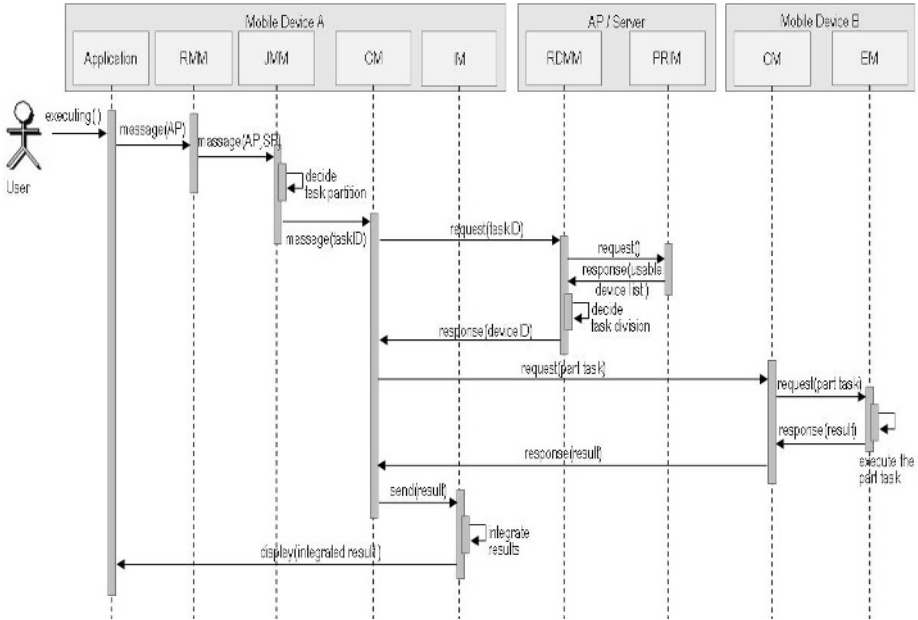


Fig. 2. Sequence Diagram of Overall System Behavior

The application transmits the AP to the RMM, when the user executes a specific application. The RMM maintains the *System Profile* describing the state of a device. The behavior algorithm of the RMM is presented in Fig. 3.

```

1 while(Resource Monitoring Module is on)
2 {
3     if(Current_resource > threshold)
4     {
5         if(monitored policy == true)
6             then after decision whether support the idle resource
7             and notify to sever
8         else
9             then notify the idle resource to Server
10    }
11    else
12        then notify server that it can't support the resource
13    if(require Application)
14    {
15        if(Application required_resource < Current_resource)
16            then execut all adaptation Service in internal
17        else
18            then send the System Profile to Job Management Module
19    }
20    if(Current_resource changes happen)
21        then send the System Profile to Job Management Module
22 }

```

Fig. 3. Pseudo Code of Resource Monitoring Algorithm

Line 5 shows that the RMM decides whether to offer idle resources based on monitoring policy. For example, even if a device contains sufficient idle resources, it cannot support idle resources if the battery level is insufficient. The JMM decisions enable work based on two profiles (*System Profile*, *Application Profile*) received by the RMM. The resource score of device can be expressed as RS . Using Formula (1), the RS of each object is obtained.

$$RS_A = \frac{\left(\frac{AE_{CPU}}{E_{CPU}} \cdot w\right) + \left(\frac{AE_{RAM}}{E_{RAM}} \cdot w\right) + \dots}{N_{resource}} \quad (1)$$

The element values of the profile are substituted to the required CPU of object A (AE_{CPU}) and current CPU (E_{CPU}). The RS_A expresses the relative value of object A, required for execution. The $N_{resource}$ is the frequency of resources. The RS_A of the object is added from a low value to S. The S means the sum of RS . When S is not over 1, add RS to S. When RS_A is added to S, and S is over 1, object A cannot execute on the specific device. A component consisting of objects that have a low RS are divided as a component unit.

```
while(S < 1) {
    S = S + RS_A
}
```

The RMM requests work from the RDMM by transmitting information through the CM. The RDMM requests the PRIM, which stores information of surrounding devices, in order to solve the required work. The RDMM maps requested work and surrounding devices possessing idle resources. The result of $\langle object\ name, device_address \rangle$ is transmitted to the device requesting work from the CM. The CM transmits the object(*object name*) to a specific device(*device address*). The IM integrates the result executed to the surrounding device. Finally, the IM transmits an integrated result to the application.

4 System Evaluation

The effectiveness of the proposed system is achieved by applying it to ‘Application for Emergency-situation’ with mobile devices. The Application for Emergency-situation has functions, such as identifying a patient’s identification, searching medical records and enabling video-conferencing, and so on. This application consists of objects that execute independently.

The capability and utility of the system have been validated using mobile devices developed for the Personal Java runtime environment on iPAQ Pocket PCs. Four PocketPCs were used in performance comparisons. PocketPC A was a iPAQ RZ1717,

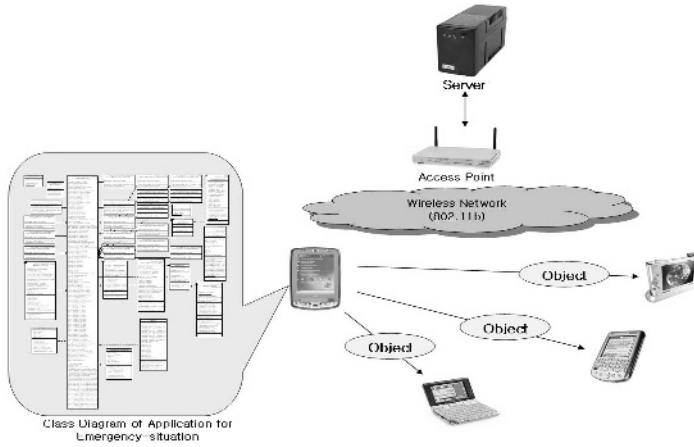


Fig. 4. The overall architecture of proposed system

equipped with a 200 MHz processor, 32 MB of RAM and a 11-Mbps IEEE 802.11b wireless card(representing insufficient resources), PocketPC B was iPAQ h5450, equipped with a 400 MHz processor, 64 MB of RAM and 11-Mbps IEEE 802.11b wireless card(representing sufficient resources). PocketPC C was the same as PocketPC A, and used only as a 733-Mhz desktop with 256 Mbytes of memory, classed as a surrounding device. PocketPC D was identical to PocketPC A, and used in the proposed system, illustrated in Fig. 4. It is assumed that the there are 10 devices identical to the Pocket PC A surrounding PocketPC D. For comparison, Each PocketPC executes an ‘Application of Emergency’ application, and is compared with each delay time. The Execution Delay Time(EDT) is the processing time from beginning an initial user task request, to executing the task. The experiment allows the evaluation of the EDT, and assumes different bandwidth values for communication.

The EDT of the device of C is given by:

$$EDT_{device C} = \alpha + \beta + \gamma + \delta \tag{2}$$

The EDT of the device of D is given by:

$$EDT_{device C} = s + \frac{\sum_{i=1}^k \alpha i + \sum_{i=1}^k \beta i + \sum_{i=1}^k \gamma i + \sum_{i=1}^k \delta i}{k} \tag{3}$$

s : transmission time of the list where the surrounding devices have idle resources

α : establishing the TCP socket between mobile devices

β : transmission time of the object

γ : transmission time of the result

δ : execution time of the object

k : the number of the surrounding device

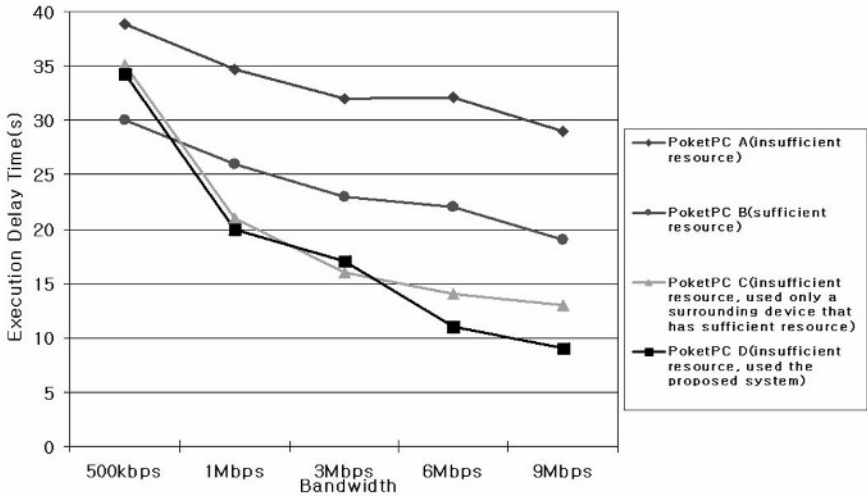


Fig. 5. Execution Delay Time, comparing the proposed system and the others

The Fig. 5 presents the results of the experiment. The analysis of Fig. 5 demonstrates the following:

- Lower than 500kbps of network bandwidth: PocketPC A, C and D represent the EDT over 30 ms. This is due to the fact that PocketPC A, B and D have insufficient resources and PocketPC C and D must transmit a required object to other devices.
- Between 1Mbps to 3Mbps of network bandwidth: Since the network speed is increased, the duration for object transmission of the PocketPC C and D is decreased accordingly. Therefore, PocketPC C and D decrease the EDT. However, PocketPC A and B do not significantly decrease the EDT.
- Between 6Mbps to 9Mbps of network bandwidth: All PocketPCs continuously decrease the EDT. However, the EDT of PocketPC D decreases by approximately 70% more than the EDT of PocketPC A, and decreases by approximately 50% more than the EDT of PocketPC B.

The result of the EDT of PocketPC C is similar to the result of the EDT of PocketPC D. PocketPC C requires additional expense, because a computer is required to solve the appropriate work.

The proposed system is shown to efficiently support a resource-constrained mobile device in a mobile environment.

5 Conclusion

This paper presents an adaptive mobile system, using mobile grid computing to overcome the constrained performance of mobile devices, and support suitable services, depending on the wireless network environment. Classes that compose an application that executes on a specific mobile device, are allocated to surrounding devices

possessing idle resources. The effectiveness of this system is confirmed by application to an emergency environment, using mobile devices that include a PDA and laptop. Various aspects of the proposed system are expected to solve the constraints discussed in wireless computing, offering a more convenient wireless computing environment.

References

1. Ian Foster, Carl Kesselman, Jeffrey M. Nick, Steven Tuecke, "The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration", OPEN Grid Service Grid Services Architecture for Distributed Systems Integration. Open Grid Service Infrastructure WG, Global Grid Forum, Jun 2002.
2. Alvin T.S. Chan, Siu-Nam Chuang, "MobiPADS: A Reflective Middleware for Context-Aware Mobile Computing", IEEE Transaction on Software Engineering. vol.29, no.12 pp.1072-1085, Dec.2003
3. A. Friday, N. Davies, G.S. Blair and K.W.J. Cheverst, "Developing Adaptive Applications: The MOST Experience", Journal of Integrated Computer-Aided Engineering, 6(2), pp.143-157, 1999.
4. Junseok Hwang, Praveen Aravamudham, "Middleware Service for P2P Computing in Wireless Grid Networks", IEEE Internet Computing vol. 8, no. 4, pp. 40-46, Jul/Aug 2004
5. Thomas Phan, Lloyd Huang, Chris Dulan, "Challenge: Integrating Mobile Wireless Devices into the Computational Grid", Proc. the 15th Annual ACM Symposium on Principles of Distributed Computing, ACM Press, MOBICOM'02, pp. 271-278, sep 2002.
6. Wai Yip Lum, Francis C. M. Lau, "User-Centric Content Negotiation for Effective Adaptation Service in Mobile Computing", IEEE Transaction on Software Engineering. Vol. 29, No.12 pp.1100-1111, Dec.2003
7. Vahe Poladian, João Pedro Sousa, David Garlan, Mary Shaw, "Dynamic Configuration of Resource-Aware Services", ICSE'04, pp.604-613, May 2004.
8. Richard S. Sutton, Andrew G. Barto, 'Reinforcement Learning: An Introduction (Adaptive Computation and Machine Learning)', The MIT Press, Mar 1998
9. Xiaohui Gu, Klara Nahrstedt, Alan Messer, Ira Greenberg, Dejan Milojicic, "Adaptive off-loading for pervasive computing", Pervasive Computing, IEEE Volume 3, Issue 3, pp.66-73, Jul-Sep. 2004
10. Paolo Bellavista, Antonio Corradi, Rebecca Montanari, Cesare Stefanelli, "Context-aware middleware for resource management in the wireless Internet", Software Engineering, IEEE Transactions on Vol. 29, Issue 12, pp. 1086-1099, Dec. 2003
11. <http://www.globus.org/>
12. Seunghwa Lee, Jehwan Oh and Eunseok Lee, "An Architecture for Multi-Agent based Self-Adaptive Systems in the Mobile Environment", LNCS 3578, pp.494-500, Jul.2005

Comparison of Allocation Algorithms for Mesh Structured Networks with Using Multistage Simulation

Leszek Koszalka, Dominik Lisowski, and Iwona Pozniak-Koszalka

Chair of Systems and Computer Networks, Faculty of Electronics,
Wrocław University of Technology, 50-370 Wrocław, Poland
leszek.koszalka@pwr.wroc.pl

Abstract. In multicomputers and computer networks a proper allocation of incoming jobs has a big impact on efficiency of parallel and distributed computing. In this paper, the mesh topology and processor allocation with using First Fit (FF) and Stack-Based (SBA) schemes, are considered. The algorithms proposed by authors SSBA (Stack-Based with Sorting) and BFSBA (Better Fit Stack-Based) are described and analyzed. Evaluation of algorithm's properties has been done with using the proposed experimentation system. This system consists of such modules like experiment design, visualization of allocation processes, presentation of results of series of experiments for the introduced measures of efficiency. The investigations, carried out in this system, show advantages of the proposed algorithms.

1 Introduction

Recently, multicomputers and computer networks with processors (nodes) connected through high-speed links have become common computing platform. The mesh topology (structure) of such a network has received increasing attention. The mesh has a simple and regular topology as a square or rectangle in (2D) two-dimensional space and a cube or rectangular parallelepiped in (3D) three-dimensional space (see Fig. 1). It becomes more and more popular for parallel and distributed computing systems due to its good scalability. This topology is utilized in large-scale computer systems for commercial and experimental application e.g. [1].

It is very important to find free resources for executing incoming jobs in a short time and with productive utilization of available supplies. A good job allocation algorithm should achieves these both objectives. In mesh-connected systems, the allocation algorithm is concerned with assigning the required number of executors to incoming jobs [2]. An incoming job specifies the size of the submesh it requires before joining the system queue [3]. An allocation algorithm is responsible for finding a free submesh. If such a submesh does not exist (there are no available processors in one coherent area), the job remains in the queue until an allocated job finishes its executions and releases a proper submesh (*dynamic case*) or, it is simply dropped (*static case*). In literature, there are presented many processor allocation algorithms for mesh-structured systems. They based on e.g. buddy strategy [4], frame sliding technique [5], quick allocation scheme [6]. In [6], the stack-based idea of allocation is presented, including the proof of recognition-completeness of SBA algorithm due to

its so-called rotating orientation mechanism. In this paper, it is assumed that: (i) jobs must be allocated in such a way that they do not overlap each other, (ii) once allocated jobs run until completion on the same assigned processors (no job migration), (iii) static case under consideration. Four allocation algorithms are evaluated, including FF-algorithm, SBA-algorithm in standard version [6], and two proposed algorithms: SSBA and BFSBA, being some modifications of SBA.

The kernel of the paper is the proposed experimentation system for evaluating properties of allocation algorithms. The system allows for observing relations between *inputs* like parameters of mesh-size (length, height, and depth), parameters of a set of jobs to be allocated (the total number of jobs, the range of sizes of jobs, features of probability density function e.g. mean and standard deviation), and first of all the allocation algorithm used and *outputs* which are the introduced measures to efficiency like the total completion time to allocation process, number of allocated jobs, number of holes, etc. The introduced *global measure* of efficiency being some composition of output values is regarded as the index of performance. This system gives opportunities for (i) designing experiment along with multistage approach [7], (ii) on-line observing the process of allocation, and (iii) presenting results of series of experiments on properly informative charts. On the basis of investigations made with using this system, the advantages of SSBA and BFSBA algorithms are pointed out.

The rest of the paper. is organized as follows: Section 2 contains the description of allocation algorithms. In Sections 3 and 4 the proposed experimentation system is shortly described. In Section 5 the analysis of results of series of experiments is presented. Finally, in Section 6 appear conclusions and perspectives.

2 Allocation Algorithms

Two-dimensional mesh $M(w_m, h_m)$ contains $w_m \times h_m$ nodes denoted as $N(x,y)$, where $0 \leq x < w_m$ and $0 \leq y < h_m$. In *three-dimensional mesh* $M(w_m, h_m, d_m)$, each node, $N(x,y,z)$, has additional third coordinate: z , where $0 \leq z < d_m$. Each node represents one executor e.g. a processor in multicomputers or a computer in a computer network.

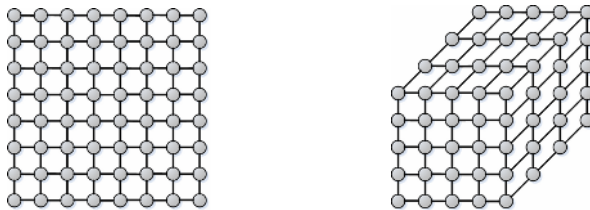


Fig. 1. Examples of 2D (*on the left*) and 3D (*on the right*) meshes

Two-dimensional submesh in mesh M is denoted as $S(\langle m1, n1 \rangle, \langle m2, n2 \rangle)$, where $0 \leq m1, m2 < w_m$ and $0 \leq n1, n2 < h_m$. Submesh S is a subgrid of M where m and n determine nodes that describe size and shape of the submesh. The pair $\langle m1, n1 \rangle$ describes the left-bottom corner and the pair $\langle m2, n2 \rangle$ describes the right-upper

corner of the submesh. *Three dimensional submesh* in mesh M is denoted as $S(\langle m1, n1, o1 \rangle, \langle m2, n2, o2 \rangle)$, where $0 \leq o1, o2 < d_m$. The triple $\langle m1, n1, o1 \rangle$ describes the front-left-bottom corner and the triple $\langle m2, n2, o2 \rangle$ describes the back-right-upper corner. It is said that a submesh is *free* when all of its nodes are available. If at least one of nodes is busy then the submesh is *busy* (BS). The *incoming job* is denoted as $J(w_i, h_j)$ and as $J(w_i, h_j, d_k)$ for 2D and 3D meshes, respectively. The 2D job is represented by $S(\langle m1, n1 \rangle, \langle m1+i, n1+j \rangle)$ and 3D job by $S(\langle m1, n1, o1 \rangle, \langle m1+i, n1+j, o1+k \rangle)$, respectively. That submesh contains a distinct node called the *Base Node* (BN). A *Base Block* (BB) is a submesh whose nodes can be used as the BN for a job. A *Candidate Block* (CB) is a free submesh during running of algorithm. It becomes a BB after the successful step of an algorithm. The *Coverage* C_j of a BS, related to a given job J , is a set of nodes such that the using any of them as BN for a given J will make this job be overlapped with BS. *Reject Area* R_j , with respect to a job J , includes nodes such that using any of them as BN will make this job cross the boundary of the mesh. The introduced notions are illustrated in Fig. 2, where $M(9,6)$ with just two allocated jobs (blackened area) is ready for $J(3,2)$.

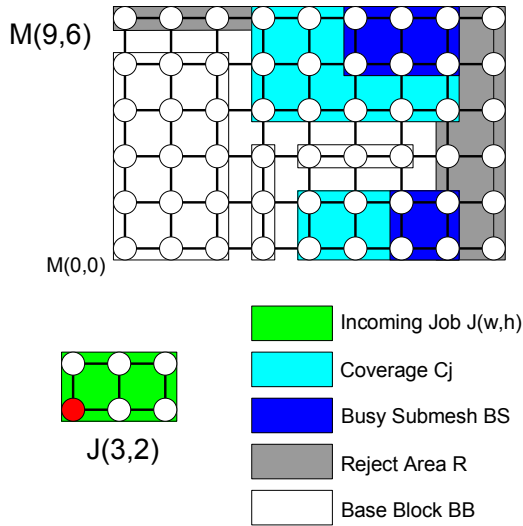


Fig. 2. Illustration of the introduced terms

The stack-based approach consists in finding BB for BN of an incoming J . To speed this process the search space is minimized by simple calculation and spatial subtraction (Fig. 3). The SBA maintains a queue of BSs and utilizes a stack to store CBs. During allocating a job $J(w,h)$ it firstly tries to allocate the job using the original orientation, then (if this allocation fails) the algorithm creates a new, symmetric request $J(h,w)$ by rotating the job's orientation and tries to allocate this new request.

SBA Algorithm. In this paper, the improved version of SBA [8] is considered. The improvement consists in no-rotating when sizes of the job J are all equal. At the

beginning the algorithm creates C_j for each item in a queue of BS-es. Next, it creates an initial CB by subtracting R_j from the entire M . Then, it puts this initial CB together with the first C_j from the queue onto the stack. From this step the algorithm works in a loop. At first, it checks whether the stack is not empty. If it is true, the algorithm checks from the top of the stack whether the position of C_j is null. If it isn't, SBA tests intersecting C_j and CB from the top of the stack.

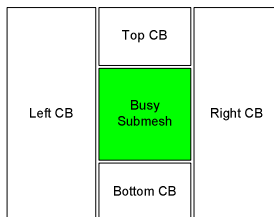


Fig. 3. Idea of 2D Spatial Subtraction

Now, two situations can be met: (i) if they have at least one shared node then the top of the stack is popped up from the stack, C_j is spatially subtracted from CB (Fig. 3) and newly created CBs are pushed up onto the stack with C_j for the next job from the queue, (ii) if they haven't got any shared node, SBA exchanges C_j with the next from the queue without any operation with the stack. When a CB with an empty Coverage position appears on the top of the stack, the desired BB is obtained. Each node from BB can be returned as the BN (the left-bottom corner is chosen). Finally, an incoming job can be accommodated and a new item can be added to the BSs.

SSBA Algorithm. In standard, classic version of SBA, a newly allocated submesh is added to the queue in the last place. When starting again, the whole list of BS-es has to be reviewed for intersecting items with the CB. The main idea of SSBA consists in reducing the number of tests for intersecting. It has been done by sorting the BS queue [9] through checking the coordinates of the recent CB and C_j , before doing test for intersecting. Checking begins with comparing horizontal coordinates of CB and C_j . Next, if the horizontal coordinates are equal, the vertical coordinates are to be compared, etc. If C_j has greater coordinates than CB then the remainder of items in the queue has greater coordinates, either. Thus, at that point a free submesh has been found. However, for ensuring good speed, two requirements should be satisfied: (i) choosing the correct sequence on the stack for a newly created CB - they have to be put onto the stack in the same order that the algorithm will test it later, (ii) choosing the correct CB node as the BN for a given job J – the implemented order is following (see Fig. 3): Right, Bottom, Top, Left, and the left-bottom corner of BB as a BN.

BFSBA Algorithm. The well-known Best Fit algorithm [5], [6] (based on frame sliding technique) tries to find the place for an incoming job in such a way that it will have a maximum number of busy neighbors. It is quite difficult to modify the SBA by utilizing this idea fully, because SBA algorithm is not able to recognize two (or more) Top (or Bottom) BBs, which are the closest neighbors and have the same height, as one. Trying to emulate the Best Fit it should be found all possible solutions and next, these solutions should be reviewed for all corresponded BBs [8]. Therefore, a

modification called the Better Fit has been applied. BFSBA chooses CB with the minimal height and with the minimal horizontal position. This operation is not extra time-consuming because it can be done during standard run of SBA scheme.

First Fit Algorithm. The well-known First Fit algorithm e.g. described in [6], is a simple algorithm but it can provide a relatively good performance. It is applicable to any mesh and can allocate submeshes of the requested sizes precisely. It maintains a busy array, which is a bitmap representing the allocation status of the mesh. In the first step, the FF algorithm tries to find the first available node by scanning all the entries in the busy array from left to right and then from top to bottom. When it finds one that does not belong to the C_j , in the second step it starts from this point and, in the same way, checks whether the job can be allocated with this founded BN. It checks the area such as job size. If there is at least one busy node FF returns to the first step.

3 Experimentation System

The process of allocation in mesh-structured system may be treated as an input-output system (Fig. 4). In this system a *controlled input* A is an allocation algorithm, and the *observed inputs* P are process parameters, i.e. mesh and incoming jobs parameters.

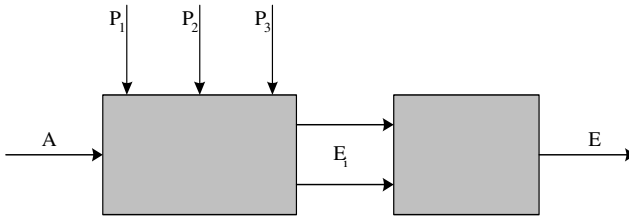


Fig. 4. Allocation process as input-output system

The *local outputs* E_i , $i=1,2,\dots$ are the considered indices of performance, including the completion time, the effectiveness, etc., and the *global output* E is the joint measure of efficiency regarded as the defined function f of the indices of performance

$$E = f(E_1, E_2, \dots) \quad \text{where} \quad E_i = R_i(A, P). \quad (1)$$

The function f in (1) depends on priorities taken by the user. Knowing the relationships R_i and the parameters P_1, P_2, P_3 , the user may choose A from the feasible set of algorithms (here the set contains four elements) such that to maximize E (*global case*) or extremize E_i (*local case*). The knowledge of R_i may be acquitted from experiments, thus, we designed and implemented an experimentation system allowing for computer simulations.

The following *input variables* (Fig. 4) can be fixed: A – allocation algorithm: FF or SSBA or SBA or BFSBA, P_1 – mesh-size (from the range $5 \leq w, h, d \leq 200$), P_2 - the

total number of requested jobs (denoted as NoR), P_3 - the parameters of probability distribution of sizes of incoming jobs (available: (i) normal distribution with *mean* from 1 to 50 and *standard deviation* being less than mean, (ii) uniform distribution within [1,50]. Remark: the random values of w and h and d are generated separately.

The following *output variables* are to be obtained: E_1 denoted as TAT – the total allocation time of the requested set of jobs, E_2 denoted as $NoBS$ – the number of allocated jobs (the number of BSs), E_3 denoted as $Used$ – the coefficient to describe the percentage of used nodes in relation to all nodes in a given mesh, expressed by (2),

$$Used = \frac{\sum_{i=1}^{NoBS} w_i \cdot h_i \cdot d_i}{w_m \cdot h_m \cdot d_m} \cdot 100 \cdot [\%], \tag{2}$$

E_4 denoted as $Weff$ – the effectiveness of allocation (3). It is defined as the percentage of used nodes in relation to the total number of nodes needed for the requested jobs,

$$Weff = \frac{\sum_{i=1}^{NoBS} w_i \cdot h_i \cdot d_i}{\sum_{j=1}^{NoR} w_j \cdot h_j \cdot d_j} \cdot 100 \cdot [\%], \tag{3}$$

E_5 denoted as NoH – the number of holes (separated free sub-meshes within the mesh) generated by A. Remark: An adaptation of (2) and (3) to 2D case required the substitution: $d_i = d_j = d_m = 1$.

The *global output* E denoted as Eff (4) is the proposed measure of the efficiency for the allocation algorithms with respect to the completion time and fragmentation.

$$Eff = \frac{Weff}{Weff + \beta * TAT + NoH} \cdot 100 [\%], \tag{4}$$

The standardization coefficient β in (4) can be chosen arbitrary or may be adjusted after preliminary analysis of results of experiments.

The proposed experimentation system is composed of the modules such that “Experiment Design” with opportunities for carrying out multistage experiments (see Section 4), “Allocation Process” with on-line visualization” (see an example in Section 4), and others. The structure of system is shown in Fig. 5.

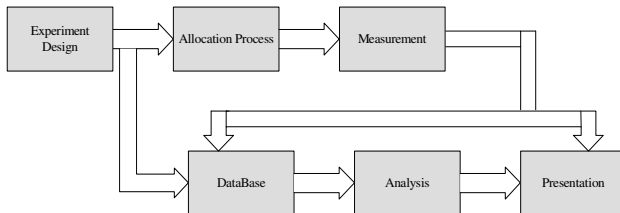


Fig. 5. The block-diagram of the experimentation system

4 Multistage Experiment

A *simple experiment* (simple simulation) means running the process of allocation once for the fixed values of inputs and observing the state of process and output values. An illustration of opportunities of Visualization Module is given in Fig. 6.

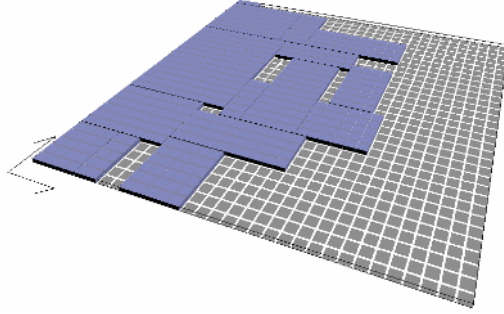


Fig. 6. Simple experiment - screenshot of the state of 2D allocation process (15th job is being allocated) for SBA, mesh of 32x32, NoR = 40, normal distribution with mean = 5, stdev = 3

A *series of experiment* (SoE) means repeating K-times the simple experiment for the same inputs. The random character of P_3 causes that output values may vary. Thus, as output values for series the average values over K-observed outputs are taken.

The *multistage experiment* consists in carrying out N-times SoE i.e. the total number of $(N \cdot K)$ simulations, where $N = N_1 \cdot N_2 \cdot \dots \cdot N_M$, and M is the number of distinct stages (here $M=4$). Each stage is corresponded to one of input variables. *At the first stage*, SoE are made for N_1 different P_3 (distinct levels of variable) while A, P_1 , P_2 are constant. *At the second stage*, variables A and P_1 are still constant, SoE are made $(N_1 \cdot N_2)$ -times for N_2 different P_2 but for each distinct level of P_2 the whole first stage experiment is carried out. Analogously, *at the third stage*, P_1 is changed on N_3 levels. For each distinct P_1 the variable A is constant (the same allocation algorithm) but the whole two-stage experiment is conducted. *At the fourth stage*, for each distinct A (here $N_4 = 4$) the whole three stage experiment is carried out.

5 Investigations

The complex, four-stage experiments have been made. Here, some results of two experiments focusing on the comparison between allocation algorithms are presented.

- *Experiment #1:* P_1 – 2D mesh of $w_m = h_m = 128$, P_2 – the total number NoR = 30 jobs, P_3 – the sizes of incoming jobs with *mean* = 20 and *stdev* = 10.
- *Experiment #2:* P_1 – 2D mesh of $w_m = h_m = 32$, P_2 – the total number NoR = 30 jobs, P_3 – the sizes of incoming jobs with *mean* = 20 and *stdev* = 10.

In both cases all SoE were carried out for all four allocation algorithms described in Section 3. The four considered features of algorithms were analysed and discussed.

Total Allocation Time. The total allocation time in terms of the number of the allocated jobs is shown in Fig. 7. We can see that the FF algorithm has allocated the total number of 30 jobs in a time seven times longer than SSBA did. SSBA is the fastest algorithm from the SBA-family, because its scheme reduces the search space significantly by using spatial subtraction and sorting the queue of BS-es. From the other side, BFSBA is the slowest from the SBA-family, because during a run it has to check all possible solutions. However, BFSBA is still faster than FF.

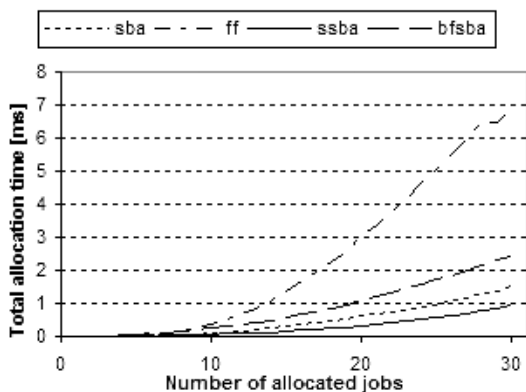


Fig. 7. Total Time of Allocation (*Experiment #1*)

Effectiveness of Allocation. The effectiveness (3) may be considered as one of the most important indices of performance because the main goal of multicomputers (computer networks) activity concern the completion of all incoming jobs. *Weff* may be interpreted as a measure of allocating incoming jobs ability. In Fig. 8 there are presented charts for all algorithms. It may be seen, that SBA-family algorithms retain *Weff* on a relatively high level longer than FF.

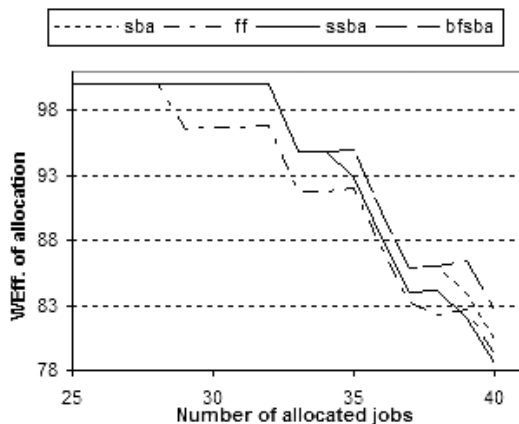


Fig. 8. The effectiveness (*Experiment #2*)

Fragmentation. Number of Holes (NoH) generated by each algorithm during the process of allocation is presented in Fig. 9. It may be observed, that BFSBA line is below the other lines. It means, that this algorithm fulfils the area of mesh in better, more efficient way than other algorithms.



Fig. 9. Number of Holes (*Experiment #2*)

The Global Efficiency. The standardization coefficient (4) was adjusted as equal to 5. In Fig. 10, the chart of E in relation to the number of allocated jobs is shown. It may be observed that for $NoBS > 10$ the algorithms from SBA-family perform better than the FF algorithm and for $NoBS = 40$ the difference is of 20 percent, approximately.



Fig. 10. Efficiency (*Experiment #2*)

6 Final Remarks

The evaluation of allocation algorithms in mesh-based systems is dependent on the considered index of performance. In the paper, there are distinct two scales: the *local*

case, where five proposed measures of quality may be considered and the *global case*, where the joint index of performance combining the total allocation time, the effectiveness (allocating ability), and the fragmentation has been introduced. *From the global point of view*, it may be concluded on the basis of simulation experiments that algorithms from SBA-family perform better than FF algorithm, and that there are no significant differences between SBA-family algorithms. *From the local point of view*, it is observed that SSBA is the fastest algorithm among all evaluated but BFSBA is the most effective i.e. it performs with the lowest fragmentation and the highest allocating ability. Moreover, SSBA and BFSBA do not strongly depend on mesh size.

The further research will be focused on considering the dynamic case of mesh-allocation problem and enlarging the set of algorithms A. In this field, two other algorithms, including well-known FS (a modification of FF) and the new algorithm WSBA (Window Stack Based) have been just implemented and preliminary tested. An example of research made with using the developed system is shown in Fig. 11.

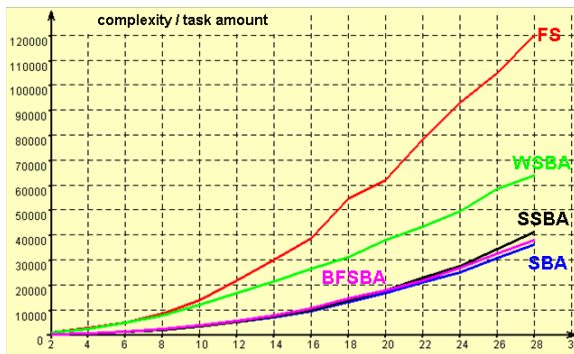


Fig. 11. Dependence of complexity on task (job) amount for mesh of $w_m = h_m = 30$

References

1. Kasprzak, A.: Topological Design of the Wide Area Networks. Wroclaw University of Technology Press, Wroclaw (2001)
2. Liu, T., Huang, W., Lombardi, F., Bhutan, L.N.: A Submesh Allocation Scheme for Mesh Connected Processor Systems. *Parallel Processing 11* (1995) 159-163
3. Yang, Y., Wang, J.: Pipelined all-to-all Broadcast in all-port Meshes. *IEEE Transactions on Computers 10* (2001) 1020-1031
4. Li, K., Cheng, K.H.: A two dimensional Buddy System for Dynamic Resource Allocation in Mesh Connected System. *Proc. of ACM Computer Science Conference 2* (1990) 22-28
5. Chuang, P.J., Tzeng, N.F.: An Efficient Submesh Allocation Strategy for Mesh Systems. *Proc. of Int. Conference on Distributed Computing 5* (1991) 256-263
6. Yoo, B.S., Das, C.R.: Fast and Efficient Processor Allocation Scheme for Mesh-Connected Multicomputers. *IEEE Transactions. on Computers 1* (2002) 46-59
7. Koszalka, L.: A Concept of Adaptive Control System for Experimentation and Controlling Described by Relation. *SAMS, 3* (1994) 219-235
8. Lisowski, D., Koszalka, L.: Processor Allocation Algorithms for Mesh Systems. *Proc. of Int. Conference on Systems Engineering, Vol. 2. Coventry, (2003) 410-416*

The Election Problem in Asynchronous Distributed Systems with Bounded Faulty Processes

SeongHoon Park

School of Electrical and Computer Engineering,
Chungbuk National Unvi., Cheongju,
ChungBuk 361-763, Korea
spark@chungbuk.ac.kr

Abstract. Determining the "weakest" failure detectors is a central topic in solving many agreement problems such as Consensus, Non-Blocking Atomic Commit and Election in asynchronous distributed systems. So far, this has been studied extensively for several of such fundamental problems. It is stated that Perfect Failure Detector P is the weakest failure detector to solve the Election problem with any number of faulty processes. In this paper, we introduce Modal failure detector M and show that to solve Election, M is the weakest failure detector to solve election when the number of faulty processes is less than $\lceil n/2 \rceil$. We also show that it is strictly weaker than P .

1 Introduction

Failure detectors are distributed *oracles* or a device that give hints about a set of processes that it suspects to have crashed. So far, "How to detect failures in asynchronous distributed systems?" has been a central research question to make asynchronous unreliable distributed systems fault-tolerant. The reason behind this widely studied research topic is that in an asynchronous system, the main difficulty in solving many agreement problems in the presence of process crashes lies in the detection of crashes. It was shown that many agreement problems such as Terminating Reliable Broadcast (TRB), Non-Blocking Atomic Commit (NBAC), Election and Consensus are unsolvable in asynchronous distributed systems if even a single crash failure can occur [1,3,4].

As a way of getting around the impossibility problem of Consensus, Chandra and Toug extended the asynchronous model of computation with unreliable *failure detectors* and showed in [8] that the FLP impossibility can be circumvented using some failure detectors.

The concept of (unreliable) failure detectors was introduced by Chandra and Toueg[6], and they characterized failure detectors by two properties: completeness and accuracy. Based on the properties, they defined several failure detector classes: perfect failure detectors P , weak failure detectors W , eventually weak failure detectors $\diamond W$ and so on. In [6] and [8] they studied what is the "weakest" failure detector to solve Consensus. They showed that the weakest failure detector to solve Consensus with any number of faulty processes is W and the one with faulty processes bounded by $\lceil n/2 \rceil$ (i.e., less than $\lceil n/2 \rceil$ faulty processes) is $\diamond W$.

After the work of [8], several studies followed. For example, the weakest failure detector for stable leader election is the perfect failure detector P [7], and the one for Terminating Reliable Broadcast is also P [6].

L. Sabel et. al., showed that the weakest failure detector to solve the stable leader election problems is P , a perfect failure detector, with any number of faulty processes. In this paper, we investigate the relationship between the necessary and sufficient capability of failure detectors for the stable leader election and the number f of faulty processes. We show that if f is only bounded by a value of less than $\lceil n/2 \rceil$, where n is the number of processes, the weakest failure detector to solve election is not P . We then propose a new failure detector class M that is necessary and sufficient to solve the stable leader election with less than $\lceil n/2 \rceil$ faulty processes, and show that M is strictly weaker than P . That is, there is a hardness gap to solve the stable leader election with respect to the number of faulty processes.

The rest of the paper is organized as follows. In Section 2 we describe our system model. In Section 3 we introduce the *Modal* Failure Detector M and show that to solve Election, M is necessary while P is not, whereas M is sufficient when a majority of the processes are correct. Finally, Section 4 summarizes the main contributions of this paper and discusses related and future work.

2 Model and Definitions

Our model of asynchronous computation with failure detection is the one described in [5]. In the following, we only discuss some informal definitions and results that are needed for this paper.

2.1 Processes

We consider a distributed system composed of a finite set of processes $\Omega = \{1, 2, \dots, n\}$ to be completely connected through a set of channels. Each process has a unique id and its priority is decided based on the id, i.e., a process with the lowest id has the highest priority. Communication is by *message passing*, *asynchronous* and *reliable*. Processes fail by crashing and the crashed process does not recover. Asynchrony means that there is no bound on communication delays or process relative speeds. A reliable channel ensures that a message, sent from process i to process j , is eventually received by j , if i and j are correct (i.e. do not crash). A failure detector is a distributed oracle which gives hints on failed processes. We consider algorithms that use failure detectors. An algorithm defines a set of runs, and a run of algorithm A using a failure detector D is a tuple $R = \langle F, H, I, S, T \rangle$: I is an initial configuration of A ; S is an infinite sequence of events of A (made of process histories); $T = t_0 \cdot t_1 \cdot t_2 \cdot \dots \cdot t_k$ is a list of increasing time values indicating when each event in S occurred where t_0 denotes a starting time; F is a failure pattern that denotes the set $F(t)$ of processes that have crashed through any time t . A *failure pattern* is a function F from T to 2^Ω . The set of correct processes in a failure pattern F is noted $correct(F)$ and the set of incorrect processes in a failure pattern F is noted $crashed(F)$; H is a failure detector history, which gives each process p and at any time t , a (possibly false) view $H(p, t)$ of the

failure pattern. $H(p,t)$ denotes a set of processes, and $q \in H(p,t)$ means that process p suspects process q at time t .

2.2 Failure Detector Classes

Failure detectors are abstractly characterized by *completeness* and *accuracy* properties [8]. Completeness characterizes the degree to which crashed processes are permanently suspected by correct processes. Accuracy restricts the false suspicions that a process can make.

Two completeness properties have been identified. *Strong Completeness*, i.e. there is a time after which every process that crashes is permanently suspected by every correct process, and *Weak Completeness*, i.e. there is a time after which every process that crashes is permanently suspected by some correct process. Four accuracy properties have been identified. *Strong Accuracy*, i.e. no process is never suspected before it crashes. *Weak Accuracy*, i.e. some correct process is never suspected. *Eventual Strong Accuracy* (\diamond Strong), i.e. there is a time after which correct processes are not suspected by any correct process; and *Eventual Weak Accuracy* (\diamond Weak), i.e. there is a time after which some correct process is never suspected by any correct process. A failure detector class is a set of failure detectors characterized by the same completeness and the same accuracy properties. (Fig. 1).

Completeness	Accuracy			
	Strong	Weak	\diamond Strong	\diamond Weak
Strong	P	S	$\diamond P$	$\diamond S$
Weak	Q	W	$\diamond Q$	$\diamond W$

Fig. 1. Failure detector classes

2.3 Reducibility and Transformation

The notation of *problem reduction* was first introduced in the problem complexity theory [10], and in the formal language theory [9]. It has been also used in the distributed computing [11,12]. We consider the following definition of problem reduction. An algorithm A solves a problem B if every run of A satisfies the specification of B . A problem B is said to be *solvable with* a class C if there is an algorithm which solves B using any failure detector of C . A problem B_1 is said to be reducible to a problem B_2 with class C , if any algorithm that solves B_2 with C can be transformed to solve B_1 with C . If B_1 is not reducible to B_2 , we say that B_1 is *harder than* B_2 .

2.4 The Stable Leader Election

The *stable leader election* problem is described as follows: at any time, at most one process considers itself the leader, and at any time, if there is no leader, a leader is eventually elected. Once a process is elected to be a leader, it can't be demoted before

crash. More formally, let $leader_i$ be a predicate that indicates that process i considers itself the leader. The *stable leader election* problem is specified by the following two properties:

- **Safety:** At any time, if a correct process has its *leader* set to true, then all other processes that had their *leader* set to true crashed.
- **Liveness:** At any time, there eventually exists a process that has its *leader* set to true.

The safety property ensures the stability of the leader, i.e., it ensures that the only reason to change the current leader is if it crashes. This property also precludes the possibility of two processes being the leader at the same time. The liveness property ensures the eventual presence of a leader. We simply call the stable leader election, *leader election* or *election*.

3 Failure Detector to Solve Election

As we pointed out in the introduction, Election can be solved with the *Perfect* failure detector P , which can be implemented in a synchronous system. One might naturally wonder whether P is indeed the weakest failure detector for Election among failure detectors that are implement-able only in a synchronous system. We show in the following that the answer is “no” and we derive an interesting observation on the practical solvability of Election. We define the *Modal* failure detector M , which is weaker than P . We show that, to solve Election: (1) M is necessary (for any environment), and (2) M is sufficient for any environment with a majority of correct processes. We then show that (3) P is strictly stronger than M for any environment where at least one processes can crash in a system of at least three processes.

3.1 Modal Failure Detector

Each module of failure detector M outputs a subset of the range 2^{Ω} . Initially, every process is suspected. However, if any process is once confirmed to be correct by any correct process, then the confirmed process id is removed from the failure detector list of M . If the confirmed process is suspected again, the suspected process id is inserted into the failure detector list of M . The most important property of M , denoted by *Modal Accuracy*, is that a process that was once confirmed to be correct is not suspected before crash. Let H_M be any history of such a failure detector M . Then $H_M(i, t)$ represents the set of processes that process i suspects at time t . For each failure pattern F , $M(F)$ is defined by the set of all failure detector histories H_M that satisfy the following properties:

- **Strong Completeness:** There is a time after which every process that crashes is permanently suspected by every correct process:

$$- \forall i, j \in \Omega, \forall i \in \text{correct}(F), \forall j \in F(t), \exists t' : \forall t' > t, j \in H(i, t').$$

- **Eventual Weak Accuracy:** There is a time after which some correct process is never suspected by any correct process. More precisely:

- $\forall i, j \in \Omega, \forall i \in \text{correct}(F), \exists j \in \text{correct}(F), \exists t: \forall t' > t, j \notin H(i, t')$.

- **Modal Accuracy:** Initially, every process is suspected. After that, any process that is once confirmed to be correct is not suspected before crash. More precisely:

- $\forall i, j \in \Omega: j \in H(i, t_0), t_0 < t < t', j \notin H(i, t) \wedge j \in \Omega \cdot F(t') \Rightarrow j \notin H(i, t')$

Note that *Modal Accuracy* does not require that failure detector M keeps the Strong Accuracy property over every process all the time t . However, it only requires that failure detector M never makes a mistake before crash about the process that was confirmed at least once to be correct.

If process M outputs some crashed processes, then M accurately knows that they have crashed, since they had already been confirmed to be correct before crash. However, concerning those processes that had never been confirmed, M does not necessarily know whether they crashed (or which processes crashed).

3.2 The Necessary Condition for Election

We show here that if failure detector D solves Election then D can be transformed into M . We give an algorithm in Fig. 2 that uses Election to emulate, within a distributed variable FL , the behavior of failure detector M . We assume the existence of a function *election* that satisfies the two properties defined in section 2.4. The election function returns a leader whenever it is called. That is, it returns the current leader if it doesn't crash, otherwise it elects a process with the lowest *id* as the new leader and returns it. Each process i has a local copy of FL , denoted by FL_i , which provides the information that should be given to the local failure detector module of M at process i . The basic idea of our algorithm is the following. Initially, the value of FL_i and CL_i is set to Ω and Φ respectively. That means that initially every process is

```

/* Algorithm executed by every process i */
1  $FL_i := \Omega;$ 
2  $CL_i := \Phi;$ 
3  $current\_leader := NULL;$ 
4 Periodically ( $\tau$ ) do
5   election();
6 Upon received (leader,  $j$ ) do
7   if ( $j \in FL_i \wedge j \notin CL_i$ ) then
8      $FL_i := FL_i - \{j\};$ 
9      $CL_i := CL_i \cup \{j\};$ 
10  end-if
11 if ( $current\_leader \neq j$ ) do
12    $FL_i := FL_i \cup \{current\_leader\};$ 
13    $current\_leader := j;$ 
14 end-if

```

Fig. 2. Emulating M using Election

suspected and none is confirmed. After that each process periodically invokes election and waits until the result of election is returned. If the received leader is in FL_i , then process i removes it from FL_i and puts it into CL_i . If it is not identical with the current leader then process i puts the id of the current leader into FL_i since the leader that was once confirmed to be correct has crashed.

Lemma 3.1. *The algorithm of Fig.2 uses Election to implement M .*

Proof. We show below that FL_i satisfies *Strong Completeness*, *Eventually Weak Accuracy* and *Modal Accuracy* properties of M .

- **Strong Completeness:** Once elected as a leader, the process can be demoted only if it crashes. Initially, every process is suspected by invoking $FL_i := \emptyset$ in line 2 of fig.2. Therefore, it satisfies strong completeness. After that the correct process i removes j from FL_i in line 8 of fig.2 only once at most and only if process i received j as a leader. Let assume that process j is elected as the leader and then crashes at time t , and let assume that process i is a correct process. Then by the *liveness* property of election, process i eventually receives the message $(leader, j)$. Assume by contradiction that strong completeness is violated. It implies that process i never puts j into FL_i even though it has crashed. This means that process i invokes election in line 5, but always receive j as a leader in line 6 of fig.2, even though it has crashed. However, because leader process j crashes at time t , there is a time t' so that for every $t'' > t'$, process i never receives process j as a leader by the *liveness* property of election: a contradiction. \square

- **Eventually Weak Accuracy:** By contradiction, assume that eventual weak accuracy is violated. It implies that with every correct process j , there is a correct process i that suspects it. Let process j be elected as a leader and it doesn't crash. That is to hold, there should be a correct process i that never stops suspecting j even though j is elected to be the leader in the algorithm of fig.2. However, by the *liveness* property of the election algorithm of fig. 2, once correct processes j is elected as a leader and doesn't crash, then every correct process eventually receives the message $(leader, j)$ and knows that j is a leader: contradiction. \square

- **Modal Accuracy:** By contradiction, assume that modal accuracy is violated. By algorithm fig. 2, the predicate $j \notin FL_i(t)$ implies that at time $t'' < t$, process j is elected and removed from FL_i . The predicate $j \in FL_i(t')$ implies that at time $t' > t$, process k ($k \neq j$) is elected as a leader when j is the current leader and j is inserted to FL_i . Given that a process was once elected as a leader in stable election, the process can be demoted only if it crashes. Thus, the new leader can be returned only if the current leader crashes. That implies $j \in F(t')$. So it is a contradiction. \square

The following theorem follows directly from Lemma 3.1.

Theorem 3.1. If any failure detector D solves election, then $M \preceq D$.

3.2 The Sufficient Condition for Election

The basic idea of our Election algorithm in Fig.3 is the following. When the *election* is invoked, the process waits for an output from M and decides the best candidate with a high priority that is not in the output of M by the *Next* function. Eventually a correct

process that is not suspected by every correct process is elected as a leader by the *consensus* protocol. If the elected process is itself, it sets its status to the leader by executing $leader_i = \text{true}$ as in Fig.3. Periodically processes wait for an output from M to ensure the leader's crash. If the process receives from M the information that the current leader has crashed and at the same time the status of current leader is not false, i.e., $(current_leader_i \neq \perp)$, the process invokes *consensus* with a new candidate for leader and decides the new leader returned by *consensus*. Otherwise the process decides the current leader. We assume that every process i , either crashes, or invokes *election* in Fig.3. The new leader candidate of participant i , denoted $new_candidate_i$, is decided by the *next* function. The current leader, denoted by $current_leader_i$, is decided by the *consensus* function. The status of participant i whether it is a leader or not is decided by the variable, $leader_i$. That is, if the variable $leader_i$ is set true, the process i considers itself a leader.

```

function election()
/* Algorithm executed by every process i */
1 leader_i := false;
2 current_leader_i :=  $\perp$ ;
3 new_candidate_i := Next(0);
4 current_leader_i := Consensus(new_candidate_i);
5 if (current_leader_i = i) then leader_i = true fi

6 Periodically ( $\tau$ ) inquiry  $M_i$ 

7 Upon received  $H_M(i)$  from  $M_i$  do
8 if ((current_leader_i  $\in H_M(i)$ )  $\wedge$  (current_leader_i  $\neq \perp$ )) then
9   new_candidate_i := Next(current_leader_i);
10  current_leader_i :=  $\perp$ ;
11  current_leader_i := Consensus(new_candidate_i);
12  if (current_leader_i = i) then leader_i := true fi
13 fi

```

Fig. 3. Transforming Consensus into Election with M

We define the *Next* function of process i in Fig.3 as follows.

$$Next(k) = \min \{ j \mid j \notin H(i, t) \wedge j \neq k \}.$$

Lemma 3.2. The algorithm of Fig.3 uses M to transform Consensus into Election.

Proof. We consider the properties of Election separately.

- **Safety:** A process that every correct process does not suspect is eventually elected as a leader by *Next* and *Consensus* functions. Let process i be the current leader elected at time t that is denoted by $current_leader(t) = i$, then clearly the process i is a correct process that the failure detector M of every correct process does not suspect at time t' , $t' < t$. By *Modal Accuracy* the new leader is elected only when the current leader i has crashed. \square

- **Liveness:** Consider leader i that is elected at time t in Fig.3. After that, if the leader process crashes at time t' , $t' > t$, then by Strong Completeness of M , there is a time after that some correct processes suspect the current leader. There is eventually some correct process which executes line 7-11 of fig. 3. They decide a prospective leader by using the Next function and transfer it as a parameter to Consensus function. With the Validity property of Consensus, a process decides its leader only if some process has invoked consensus. By the Termination property of Consensus, every correct process eventually decides a leader that ensures the Liveness property of Election. \square

We define here failure detector M . Each module of M outputs a subset of \mathcal{Q} . Failure detector M satisfies *Strong Completeness* and *Eventually Weak Accuracy*, together with *Modal Accuracy*. Since Consensus is solvable with *Strong Completeness* and *Eventually Weak Accuracy* for any environment with a majority of correct processes [8], then the following theorem follows from Lemma 3.2:

Theorem 3.2. M solves Election for any environment where a majority of processes are correct, $f < n/2$.

Finally, we can state the following theorem from Theorem 3.1 and Theorem 3.2.

Theorem 3.3. For any environment with $f < n/2$, M is the weakest failure detector to solve Election.

Proof: It is straightforward from Theorem 3.1 and Theorem 3.2.

3.3 Modal Failure Perfection Is Not Perfection

Obviously, failure detector P can be used to emulate M for any environment, i.e., $M \preceq P$. We state in the following that the converse is not true for any environment where at least one processes can crash in a system.

Theorem 3.4. $P \not\preceq M$ for any environment where at least one process can crash in a system.

Proof. (By contradiction). We assume that there is an algorithm $A_{M \rightarrow P}$ that transforms M into failure detector P . Then we show the fact that P , transformed by above the algorithm, satisfies *Strong Completeness*, but it does not satisfy *Strong Accuracy*: So it is a contradiction. We denote by $output(P)$ the variable used by $A_{M \rightarrow P}$ to emulate failure detector P , i.e., $output(P)_i$ denotes the value of that variable at a given process i . Let F_1 be the failure pattern where process I has initially crashed and no other process has crashed, i.e., $F_1(t_0) = \{ I \}$.

Let H_I be the failure detector history where all processes permanently output $\{ I \}$ at t' , $t' > t_0$; i.e., $\forall i \in \mathcal{Q}, \exists t' \in T, t' > t_0 : H_I(i, t') = \{ I \}$. Clearly, H belongs to $M(F_1)$. Since variable $output(P)$ satisfies *Strong Completeness* of P then there is a partial run of $A_{M \rightarrow P}$, $R_1 = \langle F_1, H_I, I, S_1, T \rangle$ such that $\exists j \in \mathcal{Q}, \exists t'' \in T, t'' \geq t' : \{ I \} \subset output(P)_j$. Consider failure pattern F_2 such that $correct(F_2) = \mathcal{Q}$ (F_2 is failure free) and define the failure detector history H_2 such that $\forall i \in \mathcal{Q}, \forall t \in T : H_2(i, t) = \{ I \}, t' \leq t \leq t''$ and $H_2(i, t) = \Phi, t > t''$.

Note that $H_2 \in M(F_2)$ and $t' \leq t \leq t''$, $\forall i \in \Omega - \{1\} : H_1(i, t) = H_2(i, t)$. Consider $R_2 = \langle F_2, H_2, I, S_2, T \rangle$ of $A_{M \rightarrow P}$ such that $S_1[k] = S_2[k]$, $\forall t \in T$, $t' \leq t \leq t''$. Let R_2 outputs a history $H_p \in P(F_2)$. Since partial runs of R_1 and R_2 for $t' \leq t \leq t''$ are identical, the resulting history H_p of process j is: $\forall t \in T$, $t' \leq t \leq t'' : \{1\} \subset \text{output}(P)_j$.

But in R_2 , at t , $t' \leq t \leq t'' : 1 \in \text{output}(P)_j$ and $1 \in \text{correct}(F_2)$, which means that P violates *Strong Accuracy*: a contradiction. \square

4 Concluding Remarks

The importance of this paper is in extending the applicability field of the results into the Election problem in asynchronous systems (with crash failures and reliable channels) augmented with unreliable failure detectors which Chandra and Toueg studied in regards to solving problems.

So far the applicability of these results to problems other than Consensus has been discussed in [6,13,14,15]. In [8], it is shown that Consensus is sometimes solvable where Election is not. In [7], it was shown that the weakest failure detector for Election is *Perfect* failure detector P , if we consider Election to be defined among every pair of processes. If we consider however Election to be defined among a set of at least three processes and at most one can crash, this paper shows that P is not necessary for Election. An interesting consequence of this result is that there exists a failure detector that is weaker than *Perfect* failure detector P to solve Election at the environment where a majority of processes are correct, $f < n/2$.

This paper introduces *Modal* failure detector M which is weaker than *Perfect* failure detector P , and shows that: (1) M is necessary to solve Election, (2) M is sufficient to solve Election, and (3) M is the weakest failure detector to solve Election when a majority of the processes are correct. A corollary of our results above is that we can construct a failure detector that is strictly weaker than P , and yet solves Election.

Is this only theoretically interesting? We believe not, as we will discuss below. Interestingly, failure detector M consists of $\diamond S + \text{Modal Accuracy}$ and it helps deconstruct Election: intuitively, $\diamond S$ conveys the pure agreement part of Election, whereas *Modal Accuracy* conveys the specific nature of detecting a leader crash. Besides better understanding the problem, this deconstruction provides some practical insights about how to adjust failure detector values in election protocols.

In terms of the practical distributed applications, we can induce some interesting results from the very structure of $\diamond S + \text{Modal Accuracy}$ on the solvability of Election. In real distributed systems, failure detectors are typically approximated using time-outs. To implement the *Modal Accuracy* property, one needs to choose a large time-out value in order to reduce false leader failure suspicions. However, to implement $\diamond S$, a time-out value that is not larger than the one for *Modal Accuracy* is needed. Therefore an election algorithm based on $\diamond S + \text{Modal Accuracy}$ might reduce possibility of violating the safety condition but speed up the consensus of electing a new leader in the case of a leader crash.

References

1. G. LeLann: Distributed Systems—towards a Formal Approach. Information Processing 77, B. Gilchrist, Ed. North-Holland, 1977.
2. H. Garcia-Molina: Elections in a Distributed Computing System. IEEE Transactions on Computers, C-31 (1982) 49-59
3. H. Abu-Amara and J. Lokre: Election in Asynchronous Complete Networks with Intermittent Link Failures. IEEE Transactions on Computers, 43 (1994) 778-788
4. G. Singh: Leader Election in the Presence of Link Failures. IEEE Transactions on Parallel and Distributed Systems, 7 (1996) 231-236
5. M. Fischer, N. Lynch, and M. Paterson: Impossibility of Distributed Consensus with One Faulty Process. Journal of ACM, (32) 1985 374-382
6. T. Chandra and S.Toueg: Unreliable Failure Detectors for Reliable Distributed Systems. Journal of ACM, 43 (1996) 225-267
7. L. Sabel and K. Marzullo. Election Vs. Consensus in Asynchronous Distributed Systems. In Technical Report Cornell Univ., Oct. 1995
8. T. Chandra, V. Hadzilacos and S. Toueg: The Weakest Failure Detector for Solving Consensus. Journal of ACM, 43 (1996) 685-722
9. J. E. Hopcroft and J. D. Ullman: Introduction to Automata Theory, Languages and Computation. Addison Wesley, Reading, Mass., 1979
10. Garey M.R. and Johnson D.S: Computers and Intractability: A Guide to the Theory of NP-Completeness. Freeman W.H & Co, New York, 1979
11. Eddy Fromentin, Michel RAY and Frederic TRONEL: On Classes of Problems in Asynchronous Distributed Systems. In Proceedings of Distributed Computing Conference. IEEE, June 1999
12. Hadzilacos V. and Toueg S: Reliable Broadcast and Related Problems. Distributed Systems (Second Edition), ACM Press, New York, pp.97-145, 1993
13. R. Guerraoui: Indulgent Algorithms. In: Proceedings of the ACM Symposium on Principles of Distributed Computing, New York: ACM Press 2000
14. Schiper and A. Sandoz: Primary Partition: Virtually-Synchronous Communication harder than Consensus. In Proceedings of the 8th Workshop on Distributed Algorithms, 1994
15. R. Guerraoui and A. Schiper: Transaction model vs. Virtual Synchrony model: bridging the gap. In: K. Birman, F. Mattern and A. Schiper (eds.): Distributed Systems: From Theory to Practice. Lecture Notes in Computer Science, Vol. 938. Springer- Verlag, Berlin Heidelberg New York (1995) 121-132.
16. Rachid. Guerraoui: On the hardness of failure-sensitive agreement problems. Information Processing Letter, 79(2):99-104, 2001.

Improving the Genetic Algorithms Performance in Simple Assembly Line Balancing

Seren Özmehmet Tasan and Semra Tunalı

Department of Industrial Engineering,
Dokuz Eylul University,
Bornova, 35100 Izmir, Turkey
{seren.ozmehmet, semra.tunali}@deu.edu.tr

Abstract. In this paper, a hybrid GA approach combining genetic algorithm (GA) and tabu search (TS) is proposed to solve simple assembly line balancing problem. As this problem is combinatorial and NP hard in nature, the optimum seeking methods are impractical. Therefore, we proposed a hybrid approach, which unites the advantages and mitigates the disadvantages of the two algorithms. To increase the performance of the hybrid GA, we also optimized the control parameters such as the population size, rate of crossover and mutation. Moreover, to gain more insight on the performance of hybrid GA, we implemented it to various benchmark problems and observed that the hybridization of GA with TS improves the solution performance of the balancing problem.

1 Introduction

Assembly lines are widely adopted in manufacturing plants. Most of the work related to the assembly lines concentrates on the assembly line balancing problem (ALBP). The ALBP deals with the allocation of the tasks among workstations so that the precedence relations are not violated and a given objective function is optimized. As ALBP falls into the NP hard class of combinatorial optimization problems, optimum seeking methods have proven to be of impractical use for large problems due to their computational inefficiency. Therefore, in recent years numerous research efforts have been directed towards the development of heuristics and meta heuristics, such as simulated annealing, tabu search and genetic algorithm to provide an alternative to traditional optimization techniques.

In this study, we particularly focused on balancing of single model assembly lines by using a hybridized approach, which unites two meta heuristics, i.e. genetic algorithm (GA) and tabu search (TS). It is well known that pure GAs can locate the promising regions for global optima in a search space, but in a large search space, they have difficulty in finding the exact minimum of these optima. Therefore, in this study, TS is used to overcome the local minima and hopefully to reach the global optimum by guiding the proposed GA to new areas. Furthermore, to improve the performance of the proposed hybrid GA approach, we also optimized the control parameters such as the size of the population,

the rate of mutation and crossover, the type of selection. Finally, computational experiments were conducted on various benchmark problems to investigate the performance of the proposed hybrid approach.

The rest of the paper is organized as follows. In section 2, the simple assembly line balancing is defined and an extensive literature review related to solving simple assembly line balancing using GAs is given. In section 3, the proposed approach is dis-cussed in detail. In section 4, the control parameters of GA are optimized in order to further improve the performance of the hybrid GA. In section 5, using the efficient control parameters, the proposed hybrid GA approach is implemented to various benchmark problems. Finally, concluding remarks and the future research directions are given in section 6.

2 Simple Assembly Line Balancing

Simple assembly line balancing problem (SALBP), which is the basic version of the single ALBP, deals with a production line capable of producing only one type of product. SALBP is characterized by paced line with fixed cycle time, deterministic processing times, no assignment restrictions, serial layout, one sided stations, equally equipped stations and fixed rate launching. Based on the objective functions used for performance evaluation, the SALBP can be classified into SALBP-F, SALBP-1, SALBP-2 and SALBP-E [1]. SALBP-F is a problem that aims to establish whether or not a feasible line balance exists for a given combination of number of workstations and cycle time. SALBP-1 and SALBP-2 have dual relationships, in the first one, the aim is to minimize the number of workstation for a given cycle time, while in the second one, the aim is to minimize the cycle time for a given number of workstations. SALBP-E is the most general version of the problem that aims to simultaneously minimize the cycle time and a number of workstations considering their interrelationship.

As assembly line balancing is a quite active research area, several GAs for solving SALBP have been published. Falkenauer and Delchambre [2] were the first to solve SALBP with GAs. They used the Grouping Genetic Algorithm (GGA) especially developed for solving grouping optimization problems, where the aim was to group members of a set into a small number of families in order to optimize objective function under given constraints. Other implementations of GGA for solving ALB problems can be found in Falkenauer [3], Rekiek et al. [4] and Brown and Sumichrast [5].

Following Falkenauer and Delchambre [2], SALB problem was studied by many researchers. Leu et al. [6] developed a GA to solve SALB Type-1 problems and used heuristic procedures to determine the initial population. They also proposed a number of techniques to deal with the feasibility problems during initialization of the population as well as after the reproduction phase. They also demonstrated the possibility of balancing assembly lines with multiple criteria and zoning constraints.

Kim et al. [7] developed a GA to solve multiple objective single model ALBP. They addressed several types of ALBP such as minimize number of workstations

(Type-1), minimize cycle time (Type-2), maximize workload smoothness (Type-3), maximize work relatedness (interrelated tasks are allotted to the same workstation as much as possible) (Type-4), and a multiple objective with Type-3 and Type-4 (Type-5). The authors placed the emphasis on seeking a set of diverse Pareto optimal solutions.

Rekiek et al. [4] proposed a GGA [2] based on Equal Piles approach for solving SALBP. They tried to assign tasks to fixed number workstations in such a way that the workload of each workstation is nearly equal by leveling on average the size of each workstation (minimizing the standard deviation of sizes). Therefore, the proposed method warranted to obtain the desired number of workstations and to equalize the workloads of workstations as possible.

Bautista et al. [8] considered the SALBP with incompatibilities between tasks, so that if two tasks are incompatible, they cannot be assigned to the same workstation. They developed a Greedy Randomized Adaptive Search Procedure (GRASP), also revised GRASP by using weights and called it Greedy Randomize Weighted Adaptive Search Procedure (GRWASP). Their comparative study showed that the proposed GA and GRWASP resulted in better performance than the greedy heuristics and GRASP.

Ponnambalam et al. [9] developed a multi objective GA for single model ALBP-1 to optimize several objectives simultaneously: the number of workstations, the line efficiency, and the smoothness index. They carried out various comparative studies and stated that GA performed better in all cases studied, however at the expense of a longer execution time.

Sabuncuoglu et al. [10] developed a new GA to solve the single model ALBP and also proposed a method called 'dynamic partitioning' that modifies chromosome structure of GAs to save CPU time. The method modifies the chromosome structure by allocating tasks to workstations (i.e. freezing certain tasks) that satisfy some criteria, and continues with the remaining unfrozen tasks. Furthermore, they constructed a new elitism structure adopted from the concept of simulated annealing. The results of extensive computational experiments indicated that the proposed GA approach outperforms the well-known heuristics in the literature.

Goncalves and De Almedia [11] presented a hybrid GA, which combines heuristic priority rules with GA to solve SALBP-1. Several problems from the literature have been used to demonstrate the effectiveness and robustness of the proposed hybrid GA. The result of the experiments showed that the proposed method performs remarkably well.

Stockton et al. [12, 13] investigated the use of GAs for solving various problems that arised when designing and planning manufacturing operations, i.e. assortment planning, aggregate planning, lot sizing within material requirement planning environments, line balancing and facilities layout. In Stockton et al. [12], the authors have examined the application of GA to the single model ALBP-1 and compared the performance of the GA with a traditional solution method, i.e. Ranked Positional Weight (RPW). In the other study [13], the authors

performed computational experiments in order to identify suitable genetic operators and parameter values.

Brown and Sumichrast [5] compared the performance of GGA against the performance of typical GA across a range of grouping problems, i.e. bin packing, machine part cell formation and SALBP-1. They applied the two techniques, i.e. standard GA and GGA, to a set of problems and compared the results with respect to solution quality and run time. They noted that both of the techniques managed to find the optimal solution for all test problems; however GGA found the optimal solution more quickly.

From this extensive literature survey, it can be clearly seen that there is a growing need for effective GAs, which obtain acceptable solutions in a short time. All of the studies surveyed here employed pure GAs to solve SALBP. It is known that Pure GAs [14] are able to locate the promising regions for global optima in a search space, but sometimes they have difficulty in finding the exact minimum of these optima. Especially, since the search space for the ALBP is very large, it is likely that the solutions found by pure GAs can still be improved. Hence, to improve the performance of GA further, in this study we hybridized GA with TS. Pure TS [15] uses basic, problem-specific operators to explore a search space and memory (which is called the tabu list) to keep track of parts already visited. By using TS to refine the solutions generated by GA, this hybrid approach can overcome the local minima, operate on a set of solutions at a time and finally reach the global optimum. In this extensive literature survey, we noted that little attention has been given to increasing solution performance by hybridization of meta heuristics, so to fill the gap in this area, a hybrid GA approach was proposed in this study. Considering the importance of solving large-scale real life assembly line balancing problems effectively, we hope that the proposed hybrid GA approach will be able to generate better solutions in a shorter time when compared with traditional approaches.

3 Hybrid GA for SALBP

This section discusses in detail how the two meta heuristics, GA and TS were combined to solve SALBP-1. The general structure of the proposed hybrid approach is given in Figure 1.

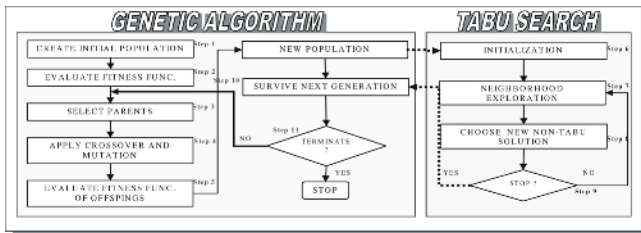


Fig. 1. General structure of the proposed approach to solve SALBP-1

The specifications of this hybrid approach such as chromosome representation, genetic operators, selection and survival schemes are explained throughout the following steps:

Step (1) Initialization of GA: To start the search process, GA is initialized with a randomly created population of individuals. The size of the population is defined by Ps. In the SALBP-1, we used a task based, natural encoding scheme to identify the feasible precedence sequences of tasks. Figure 2 represents the task based chromosome [6] whose length is defined by the number of tasks. Infeasible solutions, which violate the precedence constraints, are not allowed in the population. Once the chromosome is created, the workstation assignment process starts. The tasks of this chromosome are sequentially assigned to the workstations, as long as the predetermined cycle time is not exceeded. Once the cycle time is exceeded, a new workstation is opened for assignment, and the process is repeated.

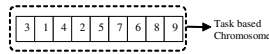


Fig. 2. Representation of chromosome

Step (2) Evaluation of Individuals: As mentioned earlier, the objective in solving SALBP-1 is to minimize the number of stations for a predetermined cycle time while satisfying the precedence constraints. However, it must be noted that this objective function only takes discrete values. When there are alternate optimal solutions having same objective value, this objective function does not give a strong distinction between the alternate solutions. To overcome this difficulty, in this study, instead we used the workload balance (Equation 1), as the fitness function. This fitness function aims at minimizing the workload balance, so the larger the fitness function, the more unfit the solution is.

$$f(s) = \frac{\sum_{k=1}^m \left(\sum_{j=1}^n (t_j * x_{jk}) / c \right)^2}{m} \quad (1)$$

where n is the number of tasks ($j=1,2,\dots,n$), m is the number of stations ($k=1,2,\dots,m$), c is the cycle time, t_j is the task process time of task j, and X_{jk} is 1 if task j is the assigned to station k or 0 otherwise.

Step (3) Selection of parents: We used the roulette wheel selection scheme, which scales the fitness values of the members within the population so that the sum of the rescaled fitness values equals to 1. To select a parent, first, a uniform random number within the interval (0, 1) is generated (wheel is spun), and then the member whose cumulative rescaled fitness value is greater than the generated number is selected as the parent.

Step (4) Crossover and Mutation: A typical GA uses two genetic operators, i.e. crossover and mutation, to direct the population towards convergence at the global optimum. Crossover operator allows solutions to exchange information in a way similar to that used by a natural organism undergoing sexual reproduction.

Mutation operator is used to randomly change the value of single genes within chromosomes. Mutation is typically applied very sparingly. We used modified two point crossover and scramble mutation [6], which both guarantee the feasibility of individuals by forcing.

The modified version of standard two point order crossover cuts each of the parent chromosomes into three parts. One of the offsprings keeps the first and the last part of the first parent. The middle part of the sequence is filled in by adding the missing tasks in the order in which they are contained in the second parent. The other offspring is built analogously based on the first and the last part of the second parent. Both of the resulting offsprings are feasible due to filling in the middle part in a precedence feasible order. The rate of crossover operation is defined by R_c . In the scramble mutation, first a point is selected randomly. Following, the head of the parent is placed in the new offspring and the tail of the new offspring is reconstructed using the procedure employed to generate the initial population to guarantee feasibility. The rate of mutation operation is defined by R_m .

Step (5) Evaluate the offsprings: The fitness of the newly formed offsprings is evaluated using the Equation 1.

Step (6) Initialization of TS: The best individual of the population from the GA is used as the starting solution s for TS.

Step (7) Neighborhood exploration of TS: All possible neighbors of the solution s are generated and evaluated. To refine the solutions, the sequence of tasks in a chromosome is kept originally as it resulted from the GA run. Only the workstation assignments are adjusted by using the assignment decision rules, i.e. the maximum task time and the maximum total number of follower task. So, during an iteration of TS, two neighbors that are generated through applying these assignment decision rules are evaluated to search for a solution.

Step (8) Choose a new nontabu design: A new design is chosen from the explored neighborhood. This design has the best fitness value among all neighbors and is not in the tabu list. The tabu list keeps track of previously explored designs and prohibits the TS from revisiting them again. Thus, if the best neighboring design is worse than the current design, the TS will go uphill. In this way, the local minima can be overcome. Instead of storing previously explored individuals, it is also possible to store each move (changes to previous individuals). Any reversal of these moves is then tabu, and they will remain so for a prespecified number of iterations.

Step (9) Stop for TS: If no more neighbors are present (all are tabu), or when after a predetermined number of iterations no improvements are found, the algorithm proceeds to step (10). Otherwise, the algorithm continues with step (7).

Step (10) Survive the individuals to next generation: Survival is an essential process in GAs that removes individuals with a low fitness and drives the population towards better solutions. After TS, a part of the existing population survives to next generation and forms new population in next generation. To ensure that best solution of previous generation is always present in a population, a modified

elitist strategy, which provides survival of best offspring to next generation, is used.

Step (11) Termination criteria for GA: The population convergence and the number of generations are defined as the termination criteria. The procedure stops when one of the following is achieved (i) the performance of the best solution does not improve more than 1% after a predetermined number of generations, i.e. $T_G = 50$, or (ii) the total number of generations exceeds a maximum number, i.e. $T_{max} = 200$.

4 Parameter Optimization

This section focuses on a critical dilemma faced in many GA applications; the selection of optimum GA parameters to ensure high performance. The genetic algorithm that is described in Section 3 can be defined by the control parameter set $\Pi = \{P_s, R_C, R_M\}$ where P_s is the size of the population, R_C is the crossover rate, and R_M is the mutation rate.

To optimize this parameter set, we employed statistical design of experiments (DOE) approach. As DOE approach allows us to also determine the contribution of each of the control parameters in the GA's convergence and any interactions of their effects, a simple assembly line balancing problem from Kilbridge and Wester's problem with medium complexity was chosen to identify the effects of different control parameters. Each control parameter was varied at three levels; for population size (P_s) 100 (small), 1000 (medium) and 5000 (large), for crossover rate (R_c) 0.50, 0.75 and 0.95, and for mutation rate (R_m) 0.002, 0.010 and 0.050. Further, in order to permit the detection of a possible interaction of factor effects, a 3^3 full factorial experimental layout was used to carry out the experiments.

In order to determine the variation in the results, we performed multiple runs, i.e. 5 runs, at each parameter setting for the problem. Therefore, a total of 135(27*5) runs was carried out. The scatter plot of workload balance for each 135 runs is graphically shown in Figure 3. Since one of the most obvious questions related to GA's performance is how it is influenced by population size, the experiments in the scatter plot was categorized according to the levels of population size, i.e. small, medium and large. It can be clearly seen from Figure 3 that the changes in the parameter settings have a profound impact on the best fitness value, i.e. workload balance. Particularly, it can be stated that medium and large sized problems gave better workload balance than the small sized population within 27 experiments. The experiments with the best workload balance are noted as $\Pi = \{100, 0.75, 0.01\}$ in 5th experiment for small sized populations, as $\Pi = \{1000, 0.95, 0.01\}$ in 17th experiment for medium sized populations and, as $\Pi = \{5000, 0.50, 0.05\}$ in 21st experiment for large sized populations.

In order to determine which control parameter effects are significant, a statistical analysis of variance (ANOVA) is conducted (Table 1). The results of ANOVA indicates that the effects of all parameters are each significant whereas in this particular problem instance, the interactions are not. As the interactions

between parameters do not exist, it will be easier for us to comment on the main effects. In summary, the results of ANOVA suggest that in order to increase the performance of GA in seeking the minimum fitness function, we may consider adjusting the control parameters of P_s , R_C , and R_M one factor at a time.

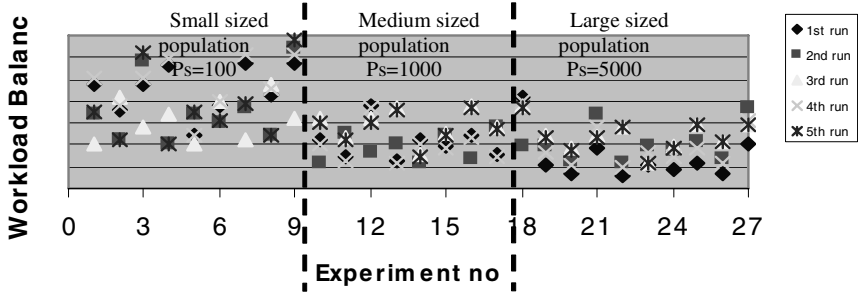


Fig. 3. The scatter plot of workload balance from 135 runs

Table 1. ANOVA results

Source of variation	SS	DF	MS	F_{calc}	Prob[F > F_{calc}]
Within+residual	5.01	108	0.05		
P_s	0.42	2	0.21	4.53	0.013
R_C	1.06	2	0.53	11.46	0.000
R_M	1.12	2	0.56	12.06	0.000
$P_s \times R_C$	0.08	4	0.02	0.43	0.787
$P_s \times R_M$	0.09	4	0.02	0.49	0.744
$R_C \times R_M$	0.20	4	0.05	1.08	0.369
$P_s \times R_C \times R_M$	0.21	8	0.03	0.56	0.805

Moreover, during the experiments the number of fitness evaluations needed to achieve an optimal workload balance was not noticeably reduced, when the population size was significantly increased from 1000 to 5000 and R_C and R_M are held at their optimal levels. In principle, it is clear that small populations run the risk of seriously undercovering the solution space, while large populations incur severe computational difficulties. Based on these results, it is possible to recommend the values of $\Pi = \{1000, 0.95, 0.010\}$ as efficient control parameters, which will require less computation time than $\Pi = \{5000, 0.50, 0.050\}$.

5 Experimental Results

To gain more insight on the performance of the proposed hybrid GA approach, we carried out various experimental studies using Talbot's and Hoffmann's benchmark problem sets [16]. Talbot's benchmark problem set includes 12 different

problems. Each problem is constructed by varying the cycle time to build a total of 64 instances. The number of tasks in these instances was varied from 8 to 111. Hoffmann's benchmark problem set includes 5 different problems with 50 instances and the number of tasks in these instances was varied from 30 to 111. In these two different problem sets, 13 of them resulted in the same instances. Hence, the comparative study involved only 101 of these instances.

The GA parameters used in the experiments are as follows, $P_S = 1000$, $R_C = 0.95$ and $R_M = 0.01$ (see section 4). All instances in the benchmarking problem sets are coded in Visual C++. Using the benchmark problem sets, the performance of pure GA and hybrid approach were compared with the optimal solutions reported in the literature.

To gain more insight on the performance of this hybrid approach, we summarized the experimental results. The summary statistics showed that the proposed hybrid GA approach outperformed pure GA with respect to all provided measures and all data sets. The hybrid GA approach found the optimal solution, i.e. minimum number of stations, in 70 instances out of 101 instances (optimally solved 69.3% of the instances). The pure GA found the optimal solutions only in 24 in-stances (optimally solved 23.8% of the instances). In comparison to the hybrid GA approach, the performance of the pure GA is rather poor. As a result, we could state that the hybridization of a GA with TS has potential to improve the performance of the pure GA.

6 Conclusion

In this study, we proposed a hybrid GA approach combining GA and TS to solve SALBP. ALBP is one of the most well-known optimization problems arising frequently in production management area. Due to the complexity of the problem, it is very hard to solve large scale real world ALBPs. In recent years, a growing number of researchers have employed GAs for solving ALBPs.

After an extensive survey of literature on GAs developed to solve assembly line balancing, we noted that there is a growing need for an effective hybrid GA approach, which can obtain acceptable solutions in a short time. Therefore, the proposed hybrid GA approach in this study aims at guiding the optimization to new areas and filling the research gaps in this area.

Furthermore, to improve the performance of the proposed hybrid GA approach, the control parameters such as population size, rate of crossover and rate of mutation were optimized using DOE. The results of the parameter optimization showed that the changes in the parameter settings had a profound impact on the problem solution. Additionally, to gain more insight on the performance of the proposed hybrid GA approach, we implemented the proposed hybrid GA approach to various benchmark problems given in literature. As a result of this comparative study, we could state that the performance of GA can improve noticeably by hybridizing it with TS. As a future work, we are particularly planning to adapt this hybrid approach for solving the complex mixed-model ALBP, involving stochastic task times and various assignment restrictions.

References

1. Scholl, A. (1999). *Balancing and Sequencing of Assembly Lines*. Heidelberg: Physica-Verlag.
2. Falkenauer E. and Delchambre A. (1992). A genetic algorithm for bin packing and line balancing. In the Proc of IEEE Int Conf on Robotics and Automation, 1189-1192.
3. Falkenauer E. (1997). A grouping genetic algorithm for line balancing with resource dependent task times. In the Proc of Int Conf on Neural Information Processing, 464-468.
4. Rekiek, B., de Lit, P., Pellichero, F., Falkenauer, E., Delchambre, A., (1999). Applying the equal piles problem to balance assembly lines, In the Proc of ISATP 1999, 399-404.
5. Brown E.C. and Sumichrast R. T. (2005). Evaluating performance advantages of grouping genetic algorithms. *Eng Appl of Artificial Intelligence*, 18, 1-12.
6. Leu, Y. Y., Matheson, L. A., and Rees, L. P. (1994). Assembly line balancing using genetic algorithms with heuristic generated initial populations and multiple criteria. *Decision Sciences*, 15, 581-606.
7. Kim Y. K., Kim Y. J. and Kim Y. H. (1996). Genetic algorithms for assembly line balancing with various objectives. *Computers and Industrial Engineering*, 30(3), 397-409.
8. Bautista, J., Suarez, R., Mateo, M., and Companys, R. (2000). Local search heuristics for the assembly line balancing problem with incompatibilities between tasks. In the Proc of IEEE Int Conf on Robotics and Automation, 2404-2409.
9. Ponnambalam S. G., Aravindan P., Naidu G., and Mogileeswar G. (2000). Multi-objective genetic algorithm for solving assembly line balancing problem. *Int Journal of Advanced Manufacturing Technology*, 16(5), 341-352.
10. Sabuncuoglu I., Erel E., and Tanyer M. (2000). Assembly line balancing using genetic algorithms. *Journal of Intelligent Manufacturing*, 11(3) 295-310.
11. Goncalves J. F. and De Almedia J. R. (2002). A hybrid genetic algorithm for assembly line balancing. *Journal of Heuristic*, 8, 629-642.
12. Stockton D. J., Quinn L. and Khalil R. A. (2004a). Use of genetic algorithms in operations management Part 1: applications. *Proc of Inst of Mech Eng-Part B: Journal of Engineering Manufacture*, 218(3), 315-327.
13. Stockton D. J., Quinn L. and Khalil R. A. (2004b). Use of genetic algorithms in operations management Part 2: results. *Proc of Inst of Mech Eng-Part B: Journal of Engineering Manufacture*, 218(3), 329-343.
14. Mitchell, M. (1996). *An Introduction to Genetic Algorithms*. Cambridge: MIT Press.
15. Glover, F., and Laguna, M. (1998). *Tabu Search*. Dordrecht: Kluwer Academic Publishers.
16. Scholl, A. (1993): Data of assembly line balancing problems. *Schriften zur Quantitativen Betriebswirtschaftslehre* 16/93, TU Darmstadt.

Reformulation and Solution Approaches for an Integrated Scheduling Model

Herbert Jodlbauer, Sonja Reitner, and Andreas Weidenhiller

FH-Steyr, Wehrgrabengasse 1-3,
A-4400 Steyr, Austria
herbert.jodlbauer@fh-steyr.at,
sonja.reitner@fh-steyr.at,
andreas.weidenhiller@fh-steyr.at
www.fh-steyr.at

Abstract. The time continuous integrated multi-item capacitated dynamic scheduling model with non-granular lot sizes and lot start times and dynamic demand functions as its key elements has recently been developed by Jodlbauer. Here we present a reformulation for improved ease of handling as well as several methods to obtain schedules close to the optimum.

1 Introduction

Since Harris' EOQ¹ model [3] and the EPL² formula developed by Taft [10], which were some of the first mathematical work on lot-sizing, many kinds of extension and improvement have been suggested, e.g. multi-product and multi-machine environments, capacity restrictions, and various approaches to consider setup activities. For details we recommend the work by Salomon [9].

Especially the earlier models can be grouped clearly into those using time-discrete approaches on a finite planning horizon and those considering cyclic schedules on an infinite continuous time scale; demand is modeled either as a constant function or as a set of due dates and quantities.

Optimal control theory also is a source of contributions to the field. The models developed by Holt et al. [4], Kimemia and Gershwin [7], and Kogan and Perkins [8] all to some degree take into account dynamic demand.

Almost any considered model results at least in a mixed-integer linear program; even moderately complex problems are already NP-hard. Consequently, we find solution approaches making use of heuristics such as genetic algorithms, Tabu Search and Simulated Annealing.

Based on ideas of both the discrete models and those from optimal control theory, Jodlbauer developed a new model in [5], describing a single-machine multi-product capacitated production system for a finite planning horizon. It considers setup times and costs and does not allow backlog. In [6], Jodlbauer presented a reformulation of his original model along with new concepts concerning the solution of the problem. These lines of thought are developed further in the present paper.

¹ Economic Order Quantity.

² Economic Production Lot.

2 Model

First, we give a short overview on the model developed in [5, 6], with several slight alterations to improve readability, handling, and/or performance. All symbols used are explained in Table 1.

Table 1. List of all parameters and variables used in the model

Parameters	
m	number of products
T	end of the planning horizon
c_i	capacity for production of product i
$d_i(t)$	demand of product i at time t
$y_{0,i}$	given initial inventory level
$y_{T,i}$	required inventory level at time T
$k_{I,i}$	unit holding cost
$k_{S,i}$	unit setup cost
$t_{S,i}$	necessary setup time for production of product i
$t_{R,i}$	necessary removal time after production of product i
E_i	set of Demand Entry Points
Variables	
n	total number of lots
a_k	time at which the production of lot k starts
b_k	time at which the production of lot k finishes
l_k	index of product produced in lot k

2.1 Basic Assumptions

In our one machine, m product environment we consider capacities, holding and setup costs as well as setup and removal times, which all may be different for each product i , but may not vary in time. At any time only one of the activities setup, production and removal may be scheduled for at most one product. Setup, production and removal must immediately succeed each other for every lot produced. Demand is described by some arbitrary integrable function $d_i(t) \geq 0$; backlog (or equivalently, negative inventory) is not allowed.

There are no upper bounds on the number of lots except those imposed by the planning horizon, i.e. $n \leq T / \min\{t_{S,i} + t_{R,i} : i = 1 \dots m\}$. Similarly, we assume that no positive lower or upper bounds on lot sizes exist.

To facilitate readability of the formulas, we define the inventory level function. Although not explicitly stated, this function is of course dependent on the model variables a_k , b_k , l_k and n .

$$y_i(t) = y_{0,i} + c_i \sum_{j=1}^n \left(\min\{b_j, t\} - \min\{a_j, t\} \right) - \int_0^t d_i(\tau) d\tau. \quad (1)$$

where $t_j = i$

The formulation with *minimum* operators ensures that only production before time t is taken into account.

Transferring the requirement that there must be no backlog into tractable constraints is non-trivial; to do so we need the concept of a *Demand Entry Point* as introduced in [5]. The definition has been changed here to incorporate the special case of demand functions comprised of due dates and quantities, which are basically sums of Dirac functions.

Definition 1. The time $\eta \in [0, T]$ is a Demand Entry Point for product i if:

$$\begin{aligned} \exists \varepsilon_0 > 0 : \forall \varepsilon \in]0, \varepsilon_0[: & \int_{\eta-\varepsilon}^{\eta} c_i - d_i(\tau) d\tau < 0 \\ & \wedge \int_{\eta}^{\eta+\varepsilon} c_i - d_i(\tau) d\tau \geq 0. \end{aligned} \quad (2)$$

In other words, within an arbitrarily small time interval ended by η , the inventory diminishes even if production is running, while this is not the case for small intervals immediately after the time η .

Instead of on a continuum, we want to check non-negativity of $y_i(t)$ at its local minima only. Now any time at which monotonicity of $y_i(t)$ changes from falling to rising has to be either a Demand Entry Point or a production start time; consequently, local minima can occur only there and of course at the interval borders. Since the values at the borders are *parameters* in our model, it is completely sufficient to check non-negativity of $y_i(t)$ at Demand Entry Points and production start times.

Remark 2. Demand entry points outside of production times for the considered product need not be checked, either; inventory can only increase during production.

2.2 Constraints

Before production of the first lot can start, the machine must be set up for the product; the lot must end *after* it started –

$$t_{S,i_1} \leq a_1 \leq b_1. \quad (3)$$

Between each lot and the next there must be time for removal and setup activity; at the end, again some time is required for removal:

$$\begin{aligned} \forall k = 2 \dots n : b_{k-1} + t_{R,t_{k-1}} + t_{S,t_k} & \leq a_k \leq b_k \\ b_n + t_{R,t_n} & \leq T. \end{aligned} \quad (4)$$

At the start time of each lot, we demand non-negative inventory ($y_i(a_k) \geq 0$) for the respective product:

$$\forall k = 1 \dots n : c_k \sum_{j=1}^{k-1} (b_j - a_j) + y_{0,k} - \int_0^{a_k} d_k(\tau) d\tau \geq 0. \quad (5)$$

where $t_j = t_k$

Furthermore, non-negative inventory ($y_i(\eta) \geq 0$) is required at all Demand Entry Points which coincide with production intervals of the considered product –

$$\forall i = 1 \dots m, \eta \in E_i \cap \bigcup_{j=1}^n [a_k, b_k]:$$

where $t_j = i$

$$c_i \sum_{j=1}^n \min\{b_j, \eta\} - \min\{a_j, \eta\} \geq -y_{0,i} + \int_0^{\eta} d_i(\tau) d\tau. \quad (6)$$

where $t_j = i$

Again, the formulation with *minimum* operators ensures that only production before time η is taken into account.

Finally, inventory at the end of the planning horizon has to be equal to a predefined level, $y_i(T) = y_{T,i}$; this implies that the overall amount of production for each product is a constant:

$$\forall i = 1 \dots m : c_i \sum_{j=1}^n b_j - a_j = y_{T,i} - y_{0,i} + \int_0^T d_i(\tau) d\tau. \quad (7)$$

where $t_j = i$

2.3 Objective

The objective function to be minimized takes into account setup and holding costs. Considering the latter, some further discussion is necessary. In [5] the holding costs are computed as follows:

$$\sum_{i=1}^m k_{I,i} \left(y_{0,i} T + \sum_{k=1}^n \left(c_i (b_k - a_k) \left(T - \frac{1}{2} (a_k + b_k) \right) \right) - \int_0^T d_i(\tau) d\tau \right). \quad (8)$$

where $t_k = i$

Contributions come from the initial inventory and from every lot produced in the schedule, while demand reduces inventory and thereby the holding costs.

Calculation of setup costs is difficult in the context of [5] – n is not considered a variable but an upper bound on the total number of lots. However, for an “unused” lot k the relation $a_k = b_k$ holds, and its setup and removal times are allowed to become zero. By this, calculation of the actual number of lots becomes possible. In the present paper, on the other hand, we consider n a variable; calculation of setup costs is thus much simpler.

The objective function can be simplified considerably if we omit all parts of the sum which are independent of the variables, such as the initial inventory, the total demand, and the overall amount of all goods produced.

The resulting objective consists of the setup costs and the amount of holding costs the current schedule saves in comparison to the hypothetical case where the total of all required products is already in stock at the time $t = 0$:

$$\sum_{k=1}^n k_{S,k} - k_{I,k} c_k \frac{b_k^2 - a_k^2}{2}. \quad (9)$$

3 Solution Approaches

In order to tackle the difficulties which a solver for this model can be expected to encounter, we are developing several approaches to the problem. Our main focus is on improving a given schedule using a heuristic which alternates between continuous and combinatorial methods.

We also created a solver which produces a schedule based on the multi-item EPL formula introduced by Hansmann in [2]. This solver is currently used mostly to generate a start solution to be improved by the aforementioned heuristic. The scope of this paper, however, will be limited to our main focus.

The improvement heuristic makes use of both combinatorial and continuous methods for improving a schedule. The process can be seen as consisting of an “outer” level of combinatorial operations such as exchange, creation and deletion of lots, thus producing changes in the production *sequence*. Each sequence is evaluated in respect to the minimum amount of setup and holding costs it generates. This evaluation is a matter for the “inner” level of continuous optimization, varying *lot sizes* and *lot start times* only. For this we also have developed specialized methods.

Remark 3. For the continuous part of the optimization, objective (9) can be simplified even further by omitting the setup costs – those can vary only because of some change of sequence.

3.1 Varying Lot Start Times and Lot Sizes

To establish what kinds of operations might be useful, we took a closer look at solutions of one machine, one product problems. The Wagner-Whitin property described in [11] – production of the next lot should start only when there is no stock left for this product – is obviously just as well suited for multi-dimensional problems. If at some time demand exceeds capacity, however, production might have to be started earlier than the Wagner-Whitin property suggests – here we again profit from the concept of Demand Entry Points.

First, we determine by what amount $\tilde{\delta}$ at most we can shift the currently considered lot k to the right (i.e. delay the start of production) in order to obtain zero inventory at the start time of the new lot $[\hat{a}_k, \hat{b}_k] = [a_k + \tilde{\delta}, b_k + \tilde{\delta}]$:

$$\tilde{\delta} = \sup \left\{ t \in [0, T - a_k - t_{R, i_k}] : \int_{a_k}^{a_k + t} d_{i_k}(\tau) d\tau \leq y_{i_k}(a_k) \right\}. \quad (10)$$

No values greater than that are possible. Since at the time $\hat{a}_k = a_k + \tilde{\delta}$ no inventory is left, further demand has to be satisfied by the current production. This however might be impossible if demand at some time exceeds the production capacity; in other words, in the vicinity of a Demand Entry Point η .

Delaying the lot start by δ reduces the inventory level at $\eta \in [a_k, b_k]$ by $c_{i_k} \delta$ and at $\eta > b_k$ by $\max\{0, \delta - (\eta - b_k)\} c_{i_k}$; consequently, the maximum right shift possible without getting negative inventory at η is $y_{i_k}(\eta) / c_{i_k} + \max\{0, \eta - b_k\}$.

A closer look at the inventory level function (1) reveals that the right shift which we are considering here has no influence on the shape of $y_{i_k}(t)$ for $t \geq \hat{b}_k = b_k + \tilde{\delta}$. Thus, only Demand Entry Points before this time need to be taken into account, as well as \hat{b}_k , because this is the right border of the considered interval. Since we assume that we are changing from a valid schedule, everything beyond \hat{b}_k is known to be feasible because unchanged.

The maximum right shift possible for lot k then is the smallest and therefore most restrictive of all these values:

$$\delta = \min \left(\left\{ \tilde{\delta} \right\} \cup \left\{ \frac{y_{i_k}(\eta)}{c_{i_k}} + \max\{0, \eta - b_k\} : \eta \in E_{i_k} \cap [\hat{a}_k, \hat{b}_k] \vee \eta = \hat{b}_k \right\} \right). \quad (11)$$

A second idea which proves very useful can be gleaned from the EPL-model introduced by Taft in [10]. For this model it can easily be shown that the lowest setup and holding costs are obtained by regular production of equal size lots. Thus it seems useful to introduce a method for the redistribution of the sizes of subsequent lots; e.g. in the case of a nearly constant demand rate, a redistribution towards lots of approximately equal size.

We introduce two new symbols:

- γ , the amount by which the first lot size is reduced (and the second lot size increased).
- δ , the amount by which the end time of the second lot is to be shifted to the right – this can be calculated using the method described above; δ is therefore dependent on γ .

Both parameters may assume negative values. We consider two subsequent lots $j < k$ of the same product; $k = \min\{\kappa > j : t_\kappa = t_j\}$.

Thus, a change with the parameters γ and δ would lead to the following new lot start and end times – the *hat* on a variable distinguishes the new values:

$$\hat{a}_j = a_j, \quad \hat{b}_j = b_j - \gamma, \quad \hat{a}_k = a_k - \gamma + \delta, \quad \hat{b}_k = b_k + \delta. \quad (12)$$

γ may assume values in the range

$$-(b_k - a_k) \leq \gamma \leq b_j - \max\left(\{a_j\} \cup \{t \in [a_j, b_j] : y_{l_j}(t) = 0\}\right). \quad (13)$$

The right-hand limit is due to the fact that any production prior to a time at which we have an inventory level of zero cannot be delayed further without incurring negative inventory levels.

The effects of different parameter values γ and δ can be compared by the difference in objective value from the hypothetical worst case, $\gamma = -(b_k - a_k)$.

The contribution of the lots j and k to the objective function is

$$-k_{l_j, c_j} \frac{b_j^2 - a_j^2 + b_k^2 - a_k^2}{2}. \quad (14)$$

From this, we obtain the difference in objective value between the new situation and the worst case (constant factors omitted):

$$\begin{aligned} & \frac{a_j^2 - (b_j + b_k - a_k)^2}{2} - \frac{\hat{a}_j^2 - \hat{b}_j^2 + \hat{a}_k^2 - \hat{b}_k^2}{2} = \\ & \dots = (a_k - b_j + \delta)(b_k - a_k + \gamma). \end{aligned} \quad (15)$$

The optimum lot size and position for the two considered lots in respect to each other can therefore be found by maximizing (15). Instead of now solving an entire optimization sub-problem, however, we make do with a rather rough approximation using Taylor series, which is sufficient for our purposes.

As will have been noted, the presented methods for the variation of lot sizes and lot start times do not consider their surroundings, i.e. any lots with which the modified lots might overlap after the operation. This is a deliberate sacrifice to improve speed and tractability, and is at least partially compensated for by the fact that we use the methods in question to create a search direction for a quasi-Newton method and apply a repair heuristic whenever overlap occurs.

3.2 Combinatorial Optimization and Potentials

Sequence evaluations are comparatively expensive, even though we are using specialized methods as described above. In order to reduce the amount of calculation necessary, we introduce the notion of a *Potential*, that is, an estimate for the cost reduction a certain combinatorial operation may allow for. These estimates can be calculated basically as shown in (15), additionally accounting for changes in setup costs.

An *exchange* of two adjacent lots k and $k+1$, $l_k \neq l_{k+1}$ can improve the objective if the additional holding costs caused by producing $k+1$ before k and therefore earlier are at least compensated for by the holding costs saved because k can be produced later. The right shift possible for lot k is computed using the Wagner-Whitin property as above.

A second, though much rarer, motivation for an exchange can occur if the lots k and $k+1$ have predecessors j_1 and j_2 respectively, i.e. $t_{j_1} = t_k \neq t_{k+1} = t_{j_2}$. Redistribution of the lot sizes as described in the previous section may then suggest a schedule where k and $k+1$ change places. This will not necessarily imply a positive potential for the first case described, so it needs to be considered separately.

If lot k is to be *removed* from the schedule, some other lot j of the same product has to be enlarged appropriately, always ensuring that this doesn't result in negative inventory levels. The main reason to remove a lot is that the reduction of setup costs at least compensates for the additional holding costs caused by producing the concerned amount as part of an earlier lot.

Conversely, *creating* a new lot j and simultaneously reducing the size of some other lot k of the same product may reduce the incurred holding costs by more than the setup costs for this new lot. The redistribution of the lot size between k and j is again calculated by the method described in the previous section.

Ideally, operations such as those just described should produce a new *feasible* schedule; to achieve this, the following requirements have to be met:

1. Inventory levels remain non-negative at all times; in consequence, the total amount of production time for each lot remains unchanged – cf. constraint (7).
2. No overlap occurs.

At present, we take care to fulfill the first condition but allow violation of the second, relying on our repair heuristic to ensure feasibility. By this, the correlation between potentials and actual change in the objective is somewhat lessened; however, in the context of separating the wheat from the chaff, which basically is the job of these potentials, they embody a very useful concept.

4 Results

Reitner and Weidenhiller are developing a C++ implementation of the concepts presented here; the results obtained with preliminary versions on problems of some diversity are already very encouraging.

For one product and constant demand our code found the analytical optimum as calculated by the EPL-Formula [10]; for two products the solution given by Hanssmann's multi-item EPL formula [2] (which guarantees only to find the optimum in the simplified common-cycle situation) is inferior to our code because we allow for non-uniformly sized lots and a different number of lots for each product.

Concerning demand modeled by sine-functions, which as an example of non-constant, dynamic demand exploits the true forte of the new model, we also obtained good results; benchmarking in this area is rather difficult, however, since to this date hardly any literature on the topic exists.

More details on these first tests are to be found in Jodlbauer [5, 6].

For further tests we benchmarked against a commercially available scheduling tool, the Advanced Planner and Optimizer (APO) from SAP³. To allow for a meaningful

³ SAP and SAP APO are trademarks or registered trademarks of SAP AG.

comparison, we had to extend our model; sequence-dependent setup costs and setup times are easily introduced, requiring only slight adaptations in (3), (4) and (9); the objective function used in APO, however, is a discrete linear underestimate of our quadratic objective and was therefore coded separately into the system. The behavior of our algorithm is influenced only slightly by this adaptation; namely, when several interim solutions are compared by objective value, a different candidate might be chosen depending on which objective is used.

For a first test run we prepared scenarios from 2 up to 10 products, with demand data comprised of due dates and order quantities. These tests are very encouraging; even though we had to adapt our model, putting our solver perhaps into a slight disadvantage, we consistently performed better than APO: We found the more efficient schedules in considerably less time; cf. Table 2 for an overview.

Remark 4. The regularity of the calculation times of APO as displayed in Table 2 is due to the fact that APO is controlled via time limits. With time limits lower than those displayed, APO mostly does not even produce *any* solution.

5 Conclusion

We recapitulated and slightly adapted the model developed in [5, 6], the generality of which poses some challenges for an efficient solution of the problem. Inspired by findings on simpler models and situations, we developed methods for suggesting promising changes which are used as search directions for a quasi-Newton optimization in the continuous part of the problem and as a way of identifying useful changes of sequence in the combinatorial part. The tests carried out confirm the usefulness of our approach for applications with continuous as well as discrete demand data and objective. Further developments will include a new approach for creating near-optimal schedules from scratch and eventually an extension of the model to incorporate layouts with several machines.

Table 2. Improvements our model achieved in comparison to APO – positive percentage values imply that our model is superior to APO

Number of products	Calculation time in seconds		Difference in calculation time	Difference in objective
	our model	APO		
2	0.02	240	~100%	0%
3	0.03	240	~100%	12%
4	2.34	480	~100%	11%
5	12.49	480	97%	14%
6	32.05	480	93%	17%
7	80.13	480	83%	11%
8	103.04	480	79%	2%
9	182.52	480	62%	8%
10	228.06	480	53%	10%

References

- [1] Bomberger E., 1966, A dynamic programming approach to a lot size scheduling problem, *Management Science* 12, 778-784
- [2] Hanssman F., 1962, *Operations Research in Production and Inventory Control*, New York, John Wiley
- [3] Harris F. W., 1913, How many parts to Make at once, *Factory: The Magazine of Management* 10(2), 135-136, Reprint, *Operations Research* 38 (6), 1990, 947-50
- [4] Holt C.C, Modigliani F., Muth J.F., Simon H.A., 1960, *Planning Production, Inventories and Workforce*, Prentice-Hall, Engewood Cliffs
- [5] Jodlbauer H., 2005, An Approach for Integrated Scheduling and Lot-Sizing, *European Journal of Operational Research*, In Press, Available online 21.12.2004
- [6] Jodlbauer H., An efficient algorithm for the integrated multi-item dynamic scheduling problem, submitted to the *European Journal of Operational Research*
- [7] Kimemia J.G., Gershwin S.B., 1983, An algorithm for the computer control of a flexible manufacturing system, *IIE Transaction* 15(4), 353-362
- [8] Kogan K., Perkins J.R., 2003, Infinite horizon production planning with periodic demand: solvable cases and a general numerical approach, *IIE Transaction* 35, 61-71
- [9] Salomon M., 1991, *Deterministic lot sizing models for Production Planning*, Springer-Verlag
- [10] Taft E. W., 1918, Formulas for Exact and Approximate Evaluation – Handling Cost of Jigs and Interest Charges of Product Manufactured Included. *The Iron Age* 1001, 1410-1412
- [11] Wagner, H.M, Whitin T.M., 1958, Dynamic Version of the Economic Lot Size Model. *Management Science* 5(1), 89-96

Safety of a Client-Based Version Vector Consistency Protocol of Session Guarantees*

Jerzy Brzeziński, Cezary Sobaniec, and Dariusz Wawrzyniak

Institute of Computing Science,
Poznań University of Technology, Poland

{Jerzy.Brzezinski, Cezary.Sobaniec, Dariusz.Wawrzyniak}@cs.put.poznan.pl

Abstract. Session guarantees are used to manage consistency of replicas in distributed systems with mobile clients. This paper presents and formally proves safety of a novel consistency protocol of session guarantees using client-based version vectors. Client-based version vectors represent sets of writes resulting from definitions of session guarantees more accurately, which results in a protocol performing better than the standard protocol using server-based version vectors.

1 Introduction

Replication is a key concept in providing high performance and availability of data and services in distributed systems. High availability directly results from redundancy; an unavailable server can be substituted by a correct one, or, from the client's perspective, the application may switch to another server. High performance is achieved through reduced latency due to access to a locally available replica, and distribution of workload on concurrently running servers. However, replication introduces the problem of data consistency that arises when replicas are modified. Required properties of a distributed system with respect to consistency depend, in general, on the application and are formally specified by *consistency models*. There are numerous consistency models developed for *Distributed Shared Memory* systems. These models, called *data-centric* consistency models, assume that servers replicating data are also accessing the data for processing purposes. However, in a mobile environment clients accessing the data are separated from servers; they can switch from one server to another. This switching adds a new dimension of complexity to the problem of consistency. *Session guarantees* [1], called also *client-centric* consistency models, have been proposed to define required properties of the system regarding consistency from the client's point of view. Intuitively: the client wants to continue processing after a switch to another server so that new operations will remain consistent with previously issued operations within a *session*.

Consistency protocols of session guarantees must efficiently represent sets of operations performed in the system. Version vectors based on vector clocks [2, 3]

* This work was supported in part by the State Committee for Scientific Research (KBN), Poland, under grant KBN 3 T11C 073 28.

may be used for this purpose. Bayou system [4] implementing session guarantees for the first time, and also other distributed systems, like LOCUS [5], Coda [6], or Ficus [7], use server-based version vectors, where every position of the version vector is assigned to a single server. Other approaches have been proposed in [8]. In this paper we prove safety of the VcSG consistency protocol of session guarantees, that uses client-based version vectors. Client-based version vectors, due to their structure represent sets of writes defined by session guarantees more accurately compared to server-based version vectors. The messages exchanged by the VcSG protocol in case of writes are also smaller than the appropriate messages of the VsSG protocol. Depending on the characteristics of a given application or system, the stability of structure of client-based version vectors may be comparable to server-based version vectors, or even higher. In a frequently changing environment some dynamic version vector maintenance mechanism can be used to alleviate the problem [9].

2 Session Guarantees

We consider a replicated distributed storage system. The system consists of a number of *servers* holding a full copy of a set of *shared objects*, and *clients* accessing the objects. Clients are separated from servers, i.e. a client application may run on a different computer than the server. A client may access a shared object after selecting a single server and sending a direct request to the server. Clients are mobile, so they can switch from one server to another during application execution. Session guarantees are expected to take care of data consistency observed by a migrating client.

The set of shared objects replicated by the servers does not imply any particular data model or organization. Operations performed on shared objects are divided into *reads* and *writes*. A read does not change states of shared objects, while a write does. A write may cause an update of an object, it may create a new object, or delete an existing one. A write may also atomically update states of several objects.

Operations on shared objects issued by a client C_i are ordered by a relation $\xrightarrow{C_i}$ called *client issue order*. A server S_j performs operations in an order represented by a relation $\xrightarrow{S_j}$. Writes and reads on objects will be denoted by w and r respectively, and operations for which the type is irrelevant will be denoted by o . An operation performed by a server S_j will be denoted by $o|_{S_j}$. The requests for operations are handled by clients synchronously, and operations are performed by servers sequentially.

Definitions of session guarantees depend on the definition of *relevant writes*:

Definition 1. *Relevant writes $RW(r)$ of a read operation r is a set of writes that have influenced the current state of objects observed by the read r .*

The exact meaning of relevant writes will strongly depend on the characteristics of a given system or application. For example, in case of simple isolated objects

(i.e. objects with methods that access only their internal fields), relevant writes of a read on object x may be represented by all previous writes on object x .

Session guarantees have been introduced in [1] in an informal and descriptive manner. The following formal definitions are based on those concepts (see also [10] for more detailed introduction). The definitions assume that operations are unique, i.e. they are labeled by some internal unique identifiers.

Definition 2. *Read Your Writes (RYW) session guarantee is a system property meaning that:*

$$\forall C_i \forall S_j \left[w \xrightarrow{C_i} r|_{S_j} \Rightarrow w \xrightarrow{S_j} r \right]$$

Definition 3. *Monotonic Writes (MW) session guarantee is a system property meaning that:*

$$\forall C_i \forall S_j \left[w_1 \xrightarrow{C_i} w_2|_{S_j} \Rightarrow w_1 \xrightarrow{S_j} w_2 \right]$$

Definition 4. *Monotonic Reads (MR) session guarantee is a system property meaning that:*

$$\forall C_i \forall S_j \left[r_1 \xrightarrow{C_i} r_2|_{S_j} \Rightarrow \forall w_k \in RW(r_1) : w_k \xrightarrow{S_j} r_2 \right]$$

Definition 5. *Writes Follow Reads (WFR) session guarantee is a system property meaning that:*

$$\forall C_i \forall S_j \left[r \xrightarrow{C_i} w|_{S_j} \Rightarrow \forall w_k \in RW(r) : w_k \xrightarrow{S_j} w \right]$$

To provide the above defined properties required by migrating clients, an appropriate mechanism, called a consistency protocol of session guarantees, must be implemented in the distributed system.

Clients express their requirements regarding consistency by assigning a set of session guarantees to their sessions. The set of session guarantees is then passed to the protocol along with every operation request.

3 The VcSG Protocol of Session Guarantees

The proposed VcSG protocol of session guarantees intercepts the communication between clients and servers: at the client side before sending a request, at the server side after receiving the request and before sending a reply, and at the client side after receiving the reply. These interceptions are used to exchange and maintain additional data structures necessary to preserve appropriate session guarantees. After receipt of a new request, a server checks whether its state is sufficiently up to date to satisfy client's requirements. If the server's state is outdated then the request is postponed and will be resumed after updating the server.

Servers periodically exchange information about writes performed in the past in order to synchronize the states of replicas. This synchronization procedure eventually causes total propagation of all writes directly submitted by clients. It does not influence safety of the VcSG protocol but rather its liveness, and therefore it will not be discussed in this paper (example procedure is presented in [4]). As opposed to [1] we do not assume total ordering of non-commutative writes; the problem of total ordering of non-commutative writes is in fact orthogonal to providing session guarantees.

Every server S_j records all writes performed locally as a sequence of writes called *history* of processing. The writes result from direct client requests, or are incorporated from other servers during synchronization procedure. The writes are performed sequentially, therefore the history is a totally ordered set denoted by $(\mathcal{O}_{S_j}, \xrightarrow{S_j})$.

Session guarantees define implicitly sets of writes that must be performed by a server before proceeding to the current operation. The sets of writes are monotonically increasing as the clients issue new operations. For this reason it is not realistic to exchange explicit sets of writes between clients and servers for the purpose of checking appropriate session guarantees. Therefore, for efficient representation of sets of writes, we propose version vectors of the form $[v_1 v_2 \dots v_{N_C}]$, where N_C is the total number of clients in the system, and a single position v_i denotes the number of writes requested by a client C_i and performed by the selected server. Every server S_j maintains its local version vector V_{S_j} , and updates appropriate positions upon every write. Every write in the VcSG protocol is labeled with a vector timestamp set to the current value of the version vector V_{S_j} of the server S_j performing the write for the first time.

Fig. 1(a) shows a time-space diagram of an example execution in a system using client-based version vectors. Client C_1 performs two writes: the first write $w(x)1$ at server S_1 , and then the second write $w(y)2$ at server S_2 ($w(x)1$ denotes a write of value 1 on object x). Let us assume that the initial values of server version vectors $V_{S_1} = V_{S_2} = [0\ 0]$ (there are two clients). After the first write, the server version vector V_{S_1} is incremented at the position representing client C_1 giving $V_{S_1} = [1\ 0]$. After the second write, server S_2 updates its local version vector to $V_{S_2} = [1\ 0]$, because it has not contacted server S_1 , and has not learned about the first write. Server version vectors V_{S_1} and V_{S_2} become equal, despite the fact that histories at the servers contain different write operations. As a result, the version vector representations of the sets of writes of server histories cannot reflect the differences. Therefore, the version vectors management must be enhanced, so that every write will be timestamped with a unique version vector. This can be achieved by global ordering of writes coming from respective clients. Fig. 1(b) shows an execution where writes of client C_1 are globally ordered. Before performing the second write at server S_2 , the server must perform all previous writes of the client. As a result, the server version vector is updated to $V_{S_2} = [1\ 0]$ before performing the second write, and the second write is timestamped with a unique version vector $[2\ 0]$ (information about the first write was transferred from server S_1 , which is denoted by a dashed line).

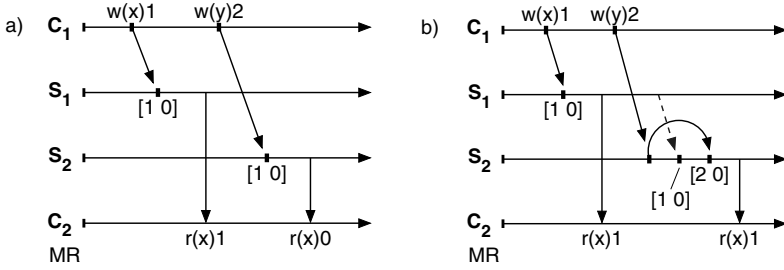


Fig. 1. Client-based version vectors and Monotonic Writes

Version vectors are used for representation of set of writes. The mapping between version vectors and sets of writes is represented by *write-sets*. The definition uses a function $T : \mathcal{O} \mapsto V$, returning the version vector of a given write w , stored in a history. A single i -th position of the version vector timestamp associated with the write will be denoted by $T(w)[i]$.

Definition 6. A *write-set* $WS(V)$ of a given version vector V is defined as

$$WS(V) = \bigcup_{j=1}^{N_S} \{w \in \mathcal{O}_{S_j} : T(w) \leq V\}$$

Let relation $V_1 \geq V_2$ on version vectors denote that version vector V_1 *dominates* a version vector V_2 , i.e. $\forall i : V_1[i] \geq V_2[i]$.

As it will be shown later, the sets of writes represented by client-based version vectors are supersets of the exact sets resulting from appropriate definitions of session guarantees. As a result, the protocol using such version vectors provides sufficient conditions for ensuring appropriate session guarantees, but not the necessary conditions. Depending on the characteristics of a given application or system, client-based version vectors may provide more accurate approximations of exact sets of writes than server-based version vectors proposed in [1].

The VcSG protocol (presented in Fig. 2) maintains some data structures at clients and servers for managing session guarantees. Every client C_i maintains two version vectors: W_{C_i} and R_{C_i} . W_{C_i} represents all writes issued by the client, while R_{C_i} represents all writes that have influenced the results of reads issued by the client. As it will be shown later, $WS(W_{C_i})$ and $WS(R_{C_i})$ are supersets of the exact sets of writes directly resulting from the appropriate session guarantees.

Every server S_j maintains a version vector V_{S_j} representing all writes performed by the server. The version vector is updated whenever a new write is requested by a client, or when a synchronization between servers is performed.

The VcSG protocol interacts with requests sent from clients to servers and with replies sent from servers to clients. A request message is a couple $\langle op, SG \rangle$, where op is an operation to be performed, and SG is a set of session guarantees required by a given client. A reply is a triple $\langle op, res, W \rangle$, where op is the operation just performed, res represents the results of the operation (delivered to

Upon sending a request $\langle op, SG \rangle$ to server S_j at client C_i

```

1:  $W \leftarrow \mathbf{0}$ 
2: if  $iswrite(op)$  or  $RYW \in SG$  then
3:    $W[i] \leftarrow W_{C_i}[i]$ 
4: end if
5: if ( $iswrite(op)$  and  $WFR \in SG$ ) or (not  $iswrite(op)$  and  $MR \in SG$ ) then
6:    $W \leftarrow \max(W, R_{C_i})$ 
7: end if
8: send  $\langle op, W \rangle$  to  $S_j$ 

```

Upon receiving a request $\langle op, W \rangle$ from client C_i at server S_j

```

9: while ( $V_{S_j} \not\geq W$ ) do
10:   wait
11: end while
12: perform  $op$  and store results in  $res$ 
13: if  $iswrite(op)$  then
14:    $V_{S_j}[i] \leftarrow V_{S_j}[i] + 1$ 
15:   timestamp  $op$  with  $V_{S_j}$ 
16:    $H_{S_j} \leftarrow H_{S_j} \cup \{op\}$ 
17:   send  $\langle op, res, \emptyset \rangle$  to  $C_i$ 
18: else
19:   send  $\langle op, res, V_{S_j} \rangle$  to  $C_i$ 
20: end if

```

Upon receiving a reply $\langle op, res, W \rangle$ from server S_j at client C_i

```

21: if  $iswrite(op)$  then
22:    $W_{C_i}[i] \leftarrow W_{C_i}[i] + 1$ 
23: else
24:    $R_{C_i} \leftarrow \max(R_{C_i}, W)$ 
25: end if

```

Server synchronization

Every Δt at server S_j

```

26: foreach  $S_k \neq S_j$  do
27:   send  $\langle S_j, H_{S_j} \rangle$  to  $S_k$ 
28: end for

```

Upon receiving an update $\langle S_k, H \rangle$ at server S_j

```

29: foreach  $w_i \in H$  do
30:   if  $V_{S_j} \not\geq T(w_i)$  then
31:     perform  $w_i$ 
32:      $V_{S_j} \leftarrow \max(V_{S_j}, T(w_i))$ 
33:      $H_{S_j} \leftarrow H_{S_j} \cup \{w_i\}$ 
34:   end if
35: end for
36: signal

```

Fig. 2. VcSG consistency protocol of session guarantees

the application), and W is a vector representing the state of the server just after having performed the operation.

Before sending to the server, the request $\langle op, SG \rangle$ is substituted by a message $\langle op, W \rangle$, where W is a version vector representing writes required by the client. The vector W is calculated based on the type of operation (checked by the `iswrite(op)` function), and the set SG of session guarantees required by the client. The vector W is set to either $\mathbf{0}$, or W_{C_i} , or R_{C_i} , or to the maximum of these two vector (lines 1, 3 and 6). The maximum of two vectors V_1 and V_2 is a vector $V = \max(V_1, V_2)$, such that $V[i] = \max(V_1[i], V_2[i])$. The vector W_{C_i} has a degenerated form in case of client-based version vectors comparing to server-based version vectors [11], because it uses only a single position $W_{C_i}[i]$ (lines 3 and 22).

Upon receiving a new request a server S_j checks whether its local version vector V_{S_j} dominates the vector W sent by the client (line 9), which is expected to be sufficient for providing appropriate session guarantees. If the state of the server is not sufficiently up to date, the request is postponed (line 10), and will be resumed after synchronization with another server (line 36). As a result of the write issued by a client C_i and performed by a server S_j , version vector of the server V_{S_j} is incremented at the i -th position (line 14), and a timestamped operation is recorded in history $(\mathcal{O}_{S_j}, \xrightarrow{S_j})$ (lines 15 and 16). For reads, the current value of the server version vector V_{S_j} is returned to the client (line 19) and it updates the client's vector R_{C_i} (line 24). For writes, the client increments its local write counter stored in vector W_{C_i} (line 22).

4 Safety of the VcSG Protocol

For the sake of the proof simplicity we define an additional notion: a supremum of a set of writes.

Definition 7. *A supremum of a set of writes \mathcal{O} , denoted by $\overline{V}(\mathcal{O})$, is a vector that is set to $\mathbf{0}$ for an empty set, and for nonempty sets its i -th position is defined as $\overline{V}(\mathcal{O})[i] = \max_{w \in \mathcal{O}} T(w)[i]$.*

An obvious consequence of the definition is that $\forall w \in \mathcal{O} : \overline{V}(\mathcal{O}) \geq T(w)$.

Lemma 1. *For every server S_j running the VcSG protocol after handling every client's request $\overline{V}(\mathcal{O}_{S_j}) = V_{S_j}$.*

Proof. By induction. (1) Basis. At the very beginning $V_{S_j} = \mathbf{0}$, and the set of writes $\mathcal{O}_{S_j} = \emptyset$, therefore $\overline{V}(\mathcal{O}_{S_j}) = \mathbf{0}$, and hence $\overline{V}(\mathcal{O}_{S_j}) = V_{S_j}$. (2) Induction step. Let us assume a state where condition $\overline{V}(\mathcal{O}_{S_j}) = V_{S_j}$ holds. The set \mathcal{O}_{S_j} and the version vector V_{S_j} can change only in the following two situations. (a) The server S_j accepts a new write requested from a client C_i . This causes the value of $V_{S_j}[i]$ to be incremented by 1, next the write is timestamped with the current value of vector V_{S_j} , and the write is added to \mathcal{O}_{S_j} (lines 14 and 16 of

the algorithm in Fig. 2). This causes $\overline{V}(\mathcal{O}_{S_j})$ to be also incremented at position i by 1. As a result, the condition $\overline{V}(\mathcal{O}_{S_j}) = V_{S_j}$ still holds. (b) The server S_j incorporates a write w received from another server. This causes the current value of V_{S_j} to be maximized with the vector $T(w)$ of the write being added (line 32). The new write is then added to \mathcal{O}_{S_j} (line 33). As a result, values of V_{S_j} and $\overline{V}(\mathcal{O}_{S_j})$ will be incremented at the same positions by the same values, therefore the condition $\overline{V}(\mathcal{O}_{S_j}) = V_{S_j}$ still holds. \square

Lemma 2. *For any two vectors V_1 and V_2 used by servers and clients of the VcSG protocol $V_1 \geq V_2 \Leftrightarrow WS(V_1) \supseteq WS(V_2)$.*

Proof. (1) Sufficient condition. By contradiction, let us assume that $V_1 \geq V_2 \wedge WS(V_1) \not\supseteq WS(V_2)$ which means that $\exists w \in \mathcal{O} [w \notin WS(V_1) \wedge w \in WS(V_2)]$ and, according to Definition 6:

$$\exists i (T(w)[i] > V_1[i] \wedge T(w)[i] \leq V_2[i]) \Rightarrow V_1[i] < V_2[i] \Rightarrow V_1 \not\geq V_2$$

— a contradiction. (2) Necessary condition. By contradiction, let us assume that $WS(V_1) \supseteq WS(V_2) \wedge V_1 \not\geq V_2$ which means that $\exists i : V_1[i] < V_2[i]$. Version vectors at position i are only incremented when a new write is requested by a client C_i (line 14). It means that $\exists w \in \mathcal{O}_{C_i} [w \in WS(V_2) \wedge w \notin WS(V_1)]$ and hence $WS(V_1) \not\supseteq WS(V_2)$ — a contradiction. \square

Lemma 3. *For every server S_j running the VcSG protocol after handling every client's request $\mathcal{O}_{S_j} = WS(V_{S_j})$.*

Proof. By contradiction: (1) Let us assume that $\exists w \in \mathcal{O}_{S_j} : w \notin WS(V_{S_j})$. According to Definition 6, a write w does not belong to $WS(V_{S_j})$ when $T(w) \not\leq V_{S_j}$. This implies that $\exists i : T(w)[i] > V_{S_j}[i]$, and, according to Lemma 1, $T(w)[i] > \overline{V}(\mathcal{O}_{S_j})[i]$, which implies $\overline{V}(\mathcal{O}_{S_j}) \not\leq T(w)$. Based on Definition 7, $w \notin \mathcal{O}_{S_j}$ — a contradiction. (2) Let us assume that $\exists w \in WS(V_{S_j}) : w \notin \mathcal{O}_{S_j}$. According to Definition 7, a write w does not belong to \mathcal{O}_{S_j} when $\overline{V}(\mathcal{O}_{S_j}) \not\leq T(w)$. This implies that $\exists i : T(w)[i] > \overline{V}(\mathcal{O}_{S_j})[i]$, and, according to Lemma 1, $T(w)[i] > V_{S_j}[i]$, which implies $T(w) \not\leq V_{S_j}$. Based on Definition 6, $w \notin WS(V_{S_j})$ — a contradiction. \square

Lemma 4. *For every client C_i running the VcSG protocol after handling every request, $WS(R_{C_i})$ contains all writes relevant to all reads issued by the client.*

Proof. A read issued by a client C_i and performed by a server S_j updates the client's vector R_{C_i} by calculating the maximum of its current value and value of the server version vector V_{S_j} (lines 19 and 24). Hence (according to Lemmata 2 and 3) $R_{C_i} \geq V_{S_j} \Rightarrow WS(R_{C_i}) \supseteq WS(V_{S_j}) = \mathcal{O}_{S_j}$. It means that the write-set $WS(R_{C_i})$ contains all writes performed at server S_j , therefore also all writes relevant to all reads requested by the client C_i at server S_j . The vector R_{C_i} monotonically increases, therefore no past write is lost in case of a migration to another server. \square

Theorem 1. *MW session guarantee is preserved by the VcSG protocol for all clients.*

Proof. Let us consider two writes w_1 and w_2 , issued by a client C_i requiring MW session guarantee. Let the second write follow the first write in the client's issue order, and let the second write be performed by a server S_j , i.e. $w_1 \xrightarrow{C_i} w_2|_{S_j}$. After performing w_1 , $WC_i[i]$ is incremented (line 22), and becomes the greatest value of all version vectors in the system at position i . If the next write is performed by the same server, MW session guarantee is fulfilled automatically. Other servers must fulfill $V_{S_j} \geq WC_i$ before performing w_2 (lines 3 and 9), and thus $V_{S_j}[i] \geq WC_i[i]$. The only way to increase $V_{S_j}[i]$ is to synchronize with another server that has performed other writes of the client C_i (line 32). Only after that synchronization write w_2 will be performed. Thus, we get $w_1 \xrightarrow{S_j} w_2$. This will happen for any client C_i and any server S_j , so $\forall C_i \forall S_j \left[w_1 \xrightarrow{C_i} w_2|_{S_j} \Rightarrow w_1 \xrightarrow{S_j} w_2 \right]$, which means that MW session guarantee is preserved. \square

Theorem 2. *RYW session guarantee is preserved by the VcSG protocol for clients requesting it.*

The proof is analogical to the proof of the previous theorem, and can be found in [10].

Theorem 3. *MR session guarantee is preserved by the VcSG protocol for clients requesting it.*

Proof. Let us consider two reads r_1 and r_2 , issued by a client C_i requiring MR session guarantee. Let the second read follow the first read in the client's issue order, and let the second read be performed by a server S_j , i.e. $r_1 \xrightarrow{C_i} r_2|_{S_j}$. After performing r_1 we have (according to Lemma 4) $\forall w_k \in RW(r_1) : w_k \in WS(R_{C_i})$. Because $V_{S_j} \geq R_{C_i}$ is fulfilled before performing r_2 (lines 6 and 9), we get (according to Lemma 2) $WS(V_{S_j}) \supseteq WS(R_{C_i}) \Rightarrow \forall w_k \in RW(r_1) : w_k \in WS(V_{S_j})$. Because local operations at servers are totally ordered, we get $\forall w_k \in RW(r_1) : w_k \xrightarrow{S_j} r_2$. This will happen for any client C_i and any server S_j , so $\forall C_i \forall S_j \left[r_1 \xrightarrow{C_i} r_2|_{S_j} \Rightarrow \forall w_k \in RW(r_1) : w_k \xrightarrow{S_j} r_2 \right]$, which means that MR session guarantee is preserved. \square

Theorem 4. *WFR session guarantee is preserved by the VcSG protocol for clients requesting it.*

The proof is analogical to the proof of the previous theorem, and can be found in [10].

5 Conclusions

This paper has presented the VcSG consistency protocol of session guarantees, and a correctness proof showing that the protocol is safe, i.e. appropriate guarantees are provided when required. It is worth mentioning, however, that though the client-based version vectors used in the VcSG protocol are sufficient for fulfilling session guarantees, they are not necessary. Thus, other approaches are also possible, and they have been discussed in [8]. The sets of writes represented by version vectors are supersets of the exact sets resulting from appropriate definitions. The accuracy of the write-set representation is therefore an important factor of a consistency protocol of session guarantees influencing its performance. This problem is currently being considered, and appropriate simulation experiments are being carried out.

References

1. Terry, D.B., Demers, A.J., Petersen, K., Spreitzer, M., Theimer, M., Welch, B.W.: Session guarantees for weakly consistent replicated data. In: Proc. of the Third Int. Conf. on Parallel and Distributed Information Systems (PDIS 94), Austin, USA, IEEE Computer Society (1994) 140–149
2. Mattern, F.: Virtual time and global states of distributed systems. In Cosnard, Quinton, Raynal, Robert, eds.: Proc. of the Int'l. Conf. on Parallel and Distributed Algorithms, Elsevier Science Publishers B. V. (1988) 215–226
3. Fidge, C.: Logical time in distributed computing systems. *Computer* **24** (1991) 28–33
4. Petersen, K., Spreitzer, M.J., Terry, D.B., Theimer, M.M., Demers, A.J.: Flexible update propagation for weakly consistent replication. In: Proc. of the 16th ACM Symp. on Operating Systems Principles (SOSP-16), Saint Malo, France (1997) 288–301
5. Parker, D.S., Popek, G., Rudisin, G., Stoughton, A., Walker, B., Walton, E., Chow, J., Edwards, D., Kiser, S., Kline, C.: Detection of mutual inconsistency in distributed systems. *IEEE Trans. on Software Engineering* **9** (1983) 240–247
6. Satyanarayanan, M., Kistler, J.J., Kumar, P., Okasaki, M.E., Siegel, E.H., Steere, D.C.: Coda: A highly available file system for a distributed workstation environment. *IEEE Transactions on Computers* **39** (1990) 447–459
7. Page, T.W., Guy, R.G., Heidemann, J.S., Ratner, D.H., Reiher, P.L., Goel, A., Kuenning, G.H., Popek, G.J.: Perspectives on optimistically replicated peer-to-peer filing. *Software Practice and Experience* **28** (1998) 155–180
8. Kobusińska, A., Libuda, M., Sobaniec, C., Wawrzyniak, D.: Version vector protocols implementing session guarantees. In: Proc. of Int. Symp. on Cluster Computing and the Grid (CCGrid 2005), Cardiff, UK (2005)
9. Ratner, D., Reiher, P., Popek, G.: Dynamic version vector maintenance. Technical Report CSD-970022, Univ. of California, Los Angeles (1997)
10. Sobaniec, C.: Consistency Protocols of Session Guarantees in Distributed Mobile Systems. PhD thesis, Poznań University of Technology, Poznań (2005)
11. Brzeziński, J., Sobaniec, C., Wawrzyniak, D.: Safety of a server-based version vector protocol implementing session guarantees. In: Proc. of Int. Conf. on Computational Science (ICCS2005), LNCS 3516, Atlanta, USA (2005) 423–430

A New I/O Architecture for Improving the Performance in Large Scale Clusters

L. M. Sánchez García¹, Florin D. Isaila¹, Félix García Carballeira¹, Jesús Carretero Pérez¹, Rolf Rabenseifner², and Panagiotis Adamidis²

¹ Computer Science Department,
Universidad Carlos III de Madrid,
Av. Universidad 30, 28911 Leganés, Madrid, Spain
{lmsan, florin, fgarcia, jcarrete}@arcos.inf.uc3m.es
<http://www.arcos.inf.uc3m.es>

² High Performance Computing Center Stuttgart (HLRS),
Universität Stuttgart,
Nobelstrasse 19, 70569 Stuttgart, Germany
{rabenseifner, adamidis}@hlrs.de
<http://www.hlrs.de>

Abstract. The technology advances made in supercomputers and high performance computing clusters over the past few years have been tremendous. Clusters are the most common solution for high performance computing at the present time. In this kind of systems, an important subject is the parallel I/O subsystem design. Parallel file systems (GPFS, PVFS, Lustre, etc) have been the solution used to obtain high performance I/O. Parallel file systems increase performance by distributing data file across several I/O nodes. However, cluster's size is increasing continuously, specially for compute nodes, becoming the I/O nodes in a possible bottleneck of the system.

In this paper, we propose a new architecture that solves the problem pointed out before: new hierarchical I/O architecture based on parallel I/O proxies. Those I/O proxies execute on the compute nodes offering an intermediate parallel file system between the applications and the storage system of the cluster. That architecture reduces the load on the I/O nodes increasing the global performance. This paper shows the design of the proposed solution and a preliminary evaluation, using a cluster located in the Stuttgart HLRS center.

keywords: Parallel File Systems, MPI-IO, High Performance Computing, Flash-IO, clusters.

1 Introduction

The technology advances made in supercomputers and high performance computing clusters over the past few years have been tremendous. Total performance of all systems on the Top500 has increased by a factor of 10 every four years [1]. The number of solutions based on clusters is growing, because they are relatively

inexpensive and can use commodity parts readily available from many suppliers. One of the most important design issues for clusters is I/O performance. There is an enormous interest on the development of high performance storage systems because the number of applications with high I/O requirements is increasing continuously.

A typical architecture for a high-performance computing cluster (HPCC) consists of compute nodes, network, and storage systems. The number of components is increasing continuously, and for large scale clusters there is a huge unbalance between the number of computing nodes and I/O nodes used by the storage system. For example, NEC Cacau cluster of HLRS center has 200 compute nodes and only 2 I/O nodes. Another example, MareNostrum of Barcelona Supercomputing Center has 2406 dual processors as compute nodes and only 20 I/O nodes. The IBM ASCI Purple has at least 1400 8-way processors as compute nodes and 128 I/O nodes. That can convert the I/O subsystem in a bottleneck, as shown in Figure 1. That Figure shows the performance (time in seconds) obtained testing Flash-IO benchmark [2] (described in the evaluation section), for different numbers of compute nodes and using the storage system of NEC Cacau cluster. As we can see, the I/O system does not scale with the number of compute nodes.

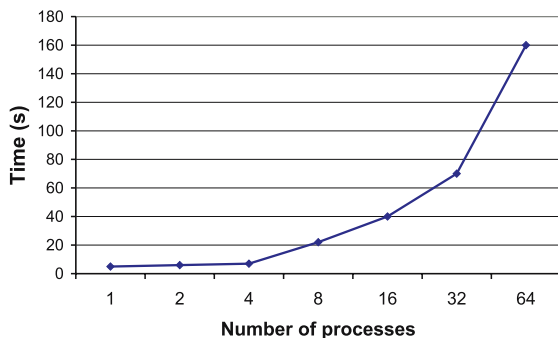


Fig. 1. Flash I/O results obtained with NEC cacau cluster using the cluster file system

This paper proposes a new I/O architecture for HPCC, based on hierarchical parallel I/O *proxies* that execute on computing nodes. Those parallel I/O proxies define an intermediate parallel file system between the applications and the storage system of the cluster. Our solution has two major goals: to increase data locality for applications, and reduce the number of I/O operations on the cluster storage system, in order to alleviate the possible bottleneck.

The paper is organized as follows: Section 2 describes the related work. Section 3 presents the new I/O architecture design. Section 4 describes the implementation of the system on NEC Cacau cluster. Performance evaluation is presented in Section 5. Finally, Section 6 presents our conclusions and future works.

2 Related Work

The use of parallelism in the file systems is based on the fact that a distributed and parallel system consists of several nodes with storage devices. The performance and bandwidth can be increased if data accesses are exploited in parallel [3]. Parallelism in file systems is obtained by using several independent server nodes supporting one or more secondary storage devices. Data are *striped* among those nodes and devices to allow parallel access to different files, and parallel access to the same file. Initially, this idea was proposed in [4] to increase the overall data throughput, striping data across several storage devices. This distribution technique is the basis for RAID systems [5].

Three different parallel I/O software architectures can be distinguished [6]: application libraries, parallel file systems, and intelligent I/O systems.

- *Application libraries* basically consist of a set of highly specialized I/O functions. Those functions provide a powerful development environment for experts with specific knowledge of the problem to model using this solution. Representative examples are MPI-IO [7], an I/O extension of the standardized message passing interface MPI.
- *Parallel file systems* operate independently from the applications, thus allowing more flexibility and generality. Examples of parallel file system are PVFS [8], Expand [9], GPFS [10].
- *An intelligent I/O system* hides the physical disk access to the application developer by providing a transparent logical I/O environment. The user describes what he wants and the system tries to optimize the I/O requests applying optimization techniques. This approach is used for example in Armada [11].

All these solutions are not enough for large scale clusters where the number of computing nodes is huge compared with the I/O nodes used by the storage system. For this kind of cluster, the current file systems for clusters can become the cluster I/O subsystem in a bottleneck.

There are other environments where the performance is improved with similar solutions as the one proposed here. *BAD-FS* [12] for GRID environment or *Scalable Lightweight Archival Storage Hierarchy (SLASH)* [13], and *High Performance Storage System (HPSS)* [14] for Mass Storage Systems propose the use of several disks as an intermediary cache system between the applications and the main storage systems. The main problem of those solutions is the difficulty to translate them to cluster environments.

3 Parallel I/O Proxies Architecture

Figure 2 shows the architecture of the proposed solution. The idea is to use the compute nodes for executing both applications and I/O proxies. An I/O proxy is a file server that executes on a compute node and uses the local disk for storage.

This solution is appropriated for clusters, because most clusters have compute nodes with several processors and local disks. We can define a virtual partition (VP) for each application by grouping several I/O proxies. As Figure 2 shows, a VP can be composed by nodes that could match or not the application ones, depending on the criteria used to form the VP.

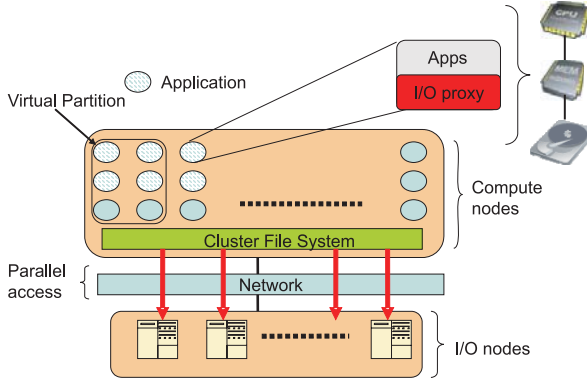


Fig. 2. Overview of the new proposed architecture

Let $C = \{c_1, c_2, \dots, c_n\}$ the set of compute nodes. Let $A = \{a_1, a_2, \dots, a_m\}$ the set of applications to run in C . Let $S = \{s_1, s_2, \dots, s_p\}$ the set of cluster storage I/O nodes. We define $P = \{p_1, p_2, \dots, p_q\}$ as the set of I/O proxies where p_i executes on c_i .

Formally, we define a virtual partition as a subset of proxy nodes, $VP \subseteq P$, strategically chosen to increase the data access parallelising degree for each application. The idea is to choose an optimal VP size, so that $\|S\| \ll \|VP\| \leq \|P\|$ and $\|S\| \ll \|VP\| \leq \|A\|$, in order to increase data locality for applications, and reduce the number of I/O operations on the cluster storage system.

When using the cluster file system, each file F of the application A is stored over S , and can be defined as $F = \{f_1, f_2, \dots, f_q\}$, where f_i is the subfile stored in s_i . A subfile is the subset of the file data store at a particular I/O node. The system defines a function $f : F \Rightarrow S$ to map data to storage nodes. Our solution creates a VP for A (let's say VP_n), and stores F in another file F' into VP_n , using a new function $g : F' \Rightarrow VP_n$, where $F' = \{f'_1, f'_2, \dots, f'_n\}$, and f'_j is the subfile stored at the p_j I/O proxy. As we have to store F in S , another function $h : VP_n \Rightarrow S$ is defined, so that $g \circ h : F \Rightarrow S$.

One important design aspect is to choose the VP size. Currently, we use an approach based on three parameters: the number of compute nodes (N) used by A , the size of each file F (F_s), and the size of local storage available (defined as $\frac{D}{k}$, where D the local disk size and k a constant defined by the system administrator or computed). The minimum number of I/O proxies used in VP would be $nio = \frac{F_s}{\frac{D}{k}} = \frac{(F_s * k)}{D}$. The maximum would be N . We are still working on strategies to maximize the performance of $g \circ h$.

We introduce a restriction for the assignment of files to VPs. Two virtual partitions can not store the same file. So, the files can not be duplicated in different virtual partitions, avoiding possible coherence problems. It could be formulated as $VP(f') \cap VP'(f') = \emptyset$.

The virtual partition contributes in providing file service to applications. Applications access the files using the virtual partition as intermediate storage, combining different local disk for storage.

For example, MareNostrum has 20 I/O nodes with 140 TB and 2400 compute nodes with 40 GB of local disk. If we use a $k = 4$ of local disk for each I/O proxy, we could build a virtual partition with 20 TB of total storage.

Our solution has the following major features: transparent use of the I/O proxies, unique image of a file across the system, persistent storage on I/O proxies, independence of cluster file system, and adaptive virtual partition to application level like stripe size, data allocation, number of I/O proxies, etc. Figure 3 shows a case where the stripe size in the virtual partition is independent of the block size of the Cluster File System (CFS). Furthermore, the number of I/O proxies is larger than the number of I/O nodes of the CFS.

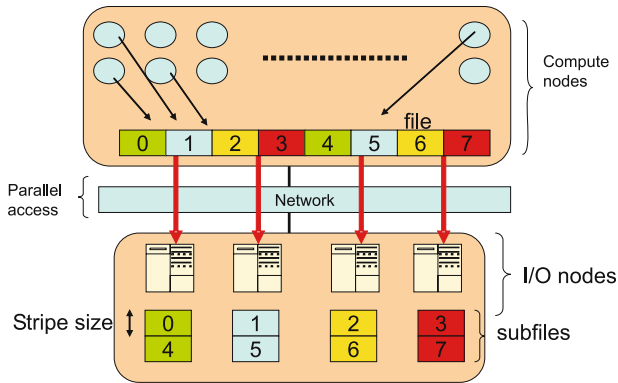


Fig. 3. Parallel files in I/O proxies are independent of the files stored in the CFS

3.1 I/O proxies

I/O proxies are responsible for managing and storing file data between the applications and the storage system of a cluster. We combine several I/O proxies for building a virtual partition where files are distributed. Main duties of an I/O proxy are: to serve data requests from compute nodes, to store data in their compute nodes until those data are stored in the CFS, and to provide to the compute nodes a fast access to the data.

I/O proxies use the local file system to store the data files, taking advantage of local cache, read ahead, and other optimizations of the local file system. That reduces the complexity of the I/O proxy and increases the performance. There are three major issues in I/O proxies: naming, metadata management, and I/O policies.

Our architecture assigns an internal id for the file F' , by composing F , and the local partition used to store data. F' metadata is included as a small header at the beginning of each subfile, to provide fault tolerance. Metadata include the following information: file id, *stripe size*, local partition, number of I/O proxies, id of I/O proxies, and *base node*. The base node identifies the I/O proxy where the first block of the file resides and the *file distribution pattern* used. At the moment, we only use files with cyclic layout. We also have a unique *master node*, that can be different from the base node, to be used as primary node for metadata. This approach is similar to the mechanism used in the Vesta Parallel File System [15] and Expand [9]. To simplify the allocation and naming process, and to reduce potential bottlenecks, a virtual partition does not use any metadata manager, as in PVFS [8].

To obtain the master node of a file, the file name is hashed into the number of node: $hash(namefile) \Rightarrow I/Oproxy_i$

The hash function used in the current prototype is:

$$\left(\sum_{i=1}^{i= strlen(namefile)} namefile[i] \right) \bmod numProxies$$

The use of this simple approach offers a good distribution of masters. Table 1 shows the distribution (standard deviation) of masters between several I/O nodes. This results have been obtained using a real file system with 145,300 files. The results shown in this table demonstrate that this simple scheme allows to distribute the master nodes and the blocks between all NFS servers, balancing the use of all NFS servers and, hence, the I/O load.

Table 1. Distribution (standard deviation) of masters in different distributed partitions

<i>Number of I/O nodes</i>	4	8	16	32	64	128
<i>Std. Dev.</i>	0.43	0.56	0.39	0.23	0.15	0.11

I/O proxies ensures that data of a file are stored eventually in S . However, there are several I/O policies that can be applied to transfer data from VP to S . The system must decide when data are transferred from the I/O proxies to the storage system in case of write operations (or vice versa in case of read operations. The behaviour of the I/O proxy is different depending on the requested operation:

- *Reading*: if the file is not stored in the virtual partition, the data is transferred from the storage system to the virtual partition using one of the next policies: on demand (taking the data by demand), on application start (all the data is transferred from the storage system to the virtual partition) or when the file is open.
- *Writing*: the write operations use the data stored in a virtual partition to write them to the storage system. Data are transferred to the storage system using one of the next policies: write on close, write through, delayed write or flush on demand.

The storage of the I/O proxies is limited. When space is required for storing new files in VP, we use a LRU replacement algorithm.

4 Implementation

This section gives an overview of the implementation of the I/O proxy components and their deployment using the Expand Parallel File System over NEC Cacau cluster. The new architecture is implemented as a user-level component in Expand software architecture [16]. Expand is transparently linked with the user application and provides parallel I/O. As shown in Figure 4, a new abstract device interface has been implemented below Expand to communicate with the I/O proxies using TCP/IP or another communication protocol when available.

Expand communicates with the I/O proxies by using the *g* mapping function defined before. I/O proxies are user level processes located on the compute nodes. They use local file system to store data on the local disk and cluster file system primitives to communicate with the CFS.

The configuration of a virtual partition is defined on the file configuration of Expand. In this file configuration declares the following parameters: the number of I/O proxies, the logical name of each I/O proxy, the stripe size, etc.

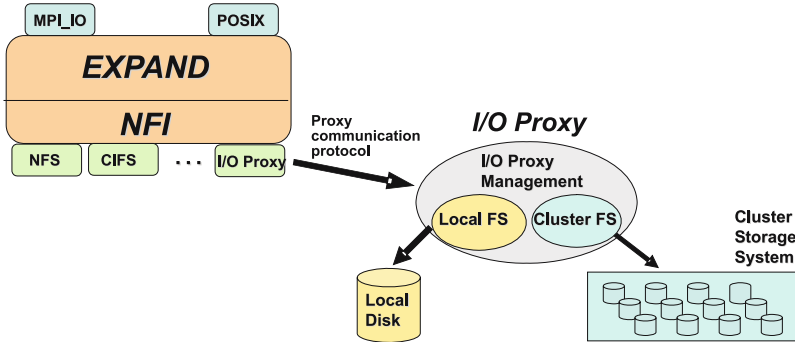


Fig. 4. Implementation of the I/O Proxy

In the current implementation, the transfer policies implemented are *delayed write* for write operations and *read at-begin* for read operations, without taking into account any hint of the I/O behaviour of the applications such as access pattern .

5 Evaluation

The existing prototype of this architecture was evaluated and compared with the I/O system of NEC Cacau cluster at the HLRS center by using FLASH-IO benchmark [2]. This cluster has the following characteristics: 400 Intel Xeon

EM64T CPU's, 160 nodes with 1 GigaByte of RAM memory and 40 nodes with 2 GigaByte of RAM memory, two frontend server to load balance, an Infiniband network interconnecting the compute nodes, a Gigabit Ethernet network for the communications between the compute nodes and the frontend server, and a Fiberchannel network to intercommunicate the frontend and the end-storage disks, NFS 2 protocol to access the disks of the end-storage and use a RAID 5 in the storage system.

FLASH-IO benchmark simulates I/O of FLASH Code. FLASH code is an adaptive mesh, parallel hydrodynamics code developed to simulate astrophysical thermonuclear flashes in two or three dimensioned space. FLASH-IO code produces a checkpoint file, a plotfile for centered data, and a plotfile for corner data. Those files are very different, because the first one is large and dense, as the last two ones are smaller and sparse.

The parameters used in the tests were the following: the number of I/O proxies is between 1 to 32 and the stripe size is between 1 KB to 2 MB.

Figure 5 shows time results for Flash-IO Benchmark using 32 processes. Each column shows the time spent to write the results of FLASH-IO to the CFS. The first column represents the time obtained using the CFS. The other columns represent the time obtained with our architecture and different configurations (tuning the different parameters of the Expand parallel file system cited in the before section, like I/O proxies (IOP), stripe size, etc). Time is obtained adding the time spent in the I/O proxies and the time consumed to flush data to CFS.

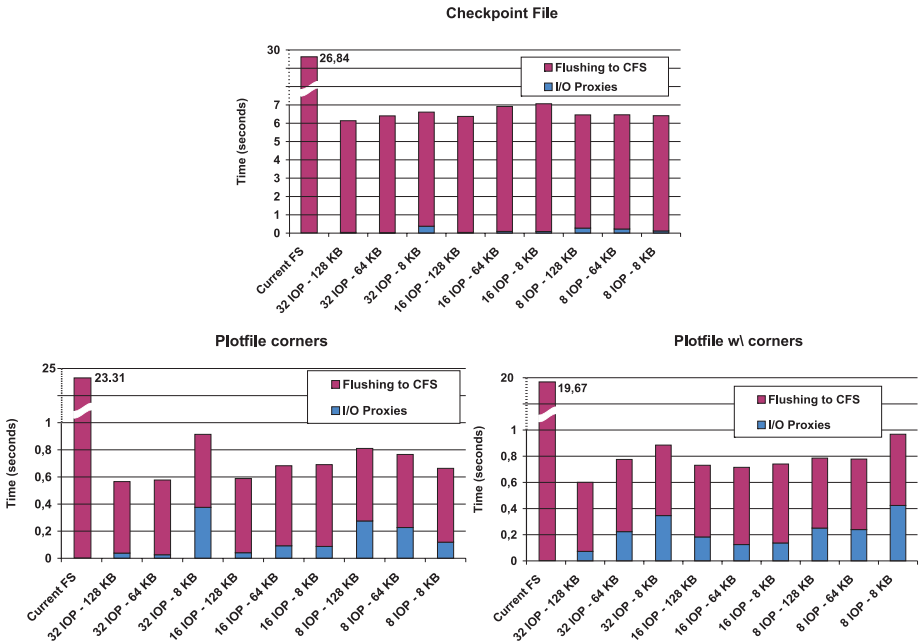


Fig. 5. Flash I/O Benchmark

The results show that this new architecture obtained better performance than the current I/O system of the cluster. Notice that, for check pointing we get a speedup of at least 6 for all the configurations. For both plotfiles, we increase the performance by a factor of 20.

6 Conclusions

In this paper we have argued that the design of I/O systems for HPCC may create a bottleneck, because the storage and the compute nodes are unbalanced. We have described a new I/O architecture that increases the performance of the storage system of a HPCC, without hardware and system modifications. Using I/O proxies as intermediary between the application and the storage system of a HPCC and an abstraction named virtual partition composed of several I/O proxies, most applications can obtain a better performance than if they use directly the storage system.

The evaluation performed in NEC Cacao cluster at the HLRS center, shows an important speedup (ranging 20 in some cases) for FLASH-IO benchmark. As this test is very demanding for I/O, we can expect even better results for more regular applications.

Some work is going on to test the system proposed in other HPCC and using more benchmarks. Moreover, we are working on virtual partition creation policies, I/O transfer policies, replacement policies, etc, to provide more flexibility and performance to the system.

Acknowledgements. We would like to thank all people of HLRS center for their support on this project. This work was carried out under the HPC-EUROPA project (RII3-CT-2003- 506079), with the support of the European Community - Research Infrastructure Action under the FP6 “Structuring the European Research Area” Programme). Also, this work has been supported by the Spanish Ministry of Education and Science under the TIN2004-02156 contract.

References

1. Vaughan-Nichols, S.J.: New trends revive supercomputing industry. **15**(2) (2004) 10–13
2. Fryxell, B., Olson, K., Ricker, P., Timmes, F.X., Zingale, M., Lamb, D.Q., MacNeice, P., Rosner, R., Truran, J.W., Tufo, H.: FLASH: An Adaptive Mesh Hydrodynamics Code for Modeling Astrophysical Thermonuclear Flashes. Volume 131. (2000) 273–334
3. del Rosario, J.M., Bordawekar, R., Choudhary, A.: Improved parallel i/o via a two-phase run-time access strategy. *SIGARCH Comput. Archit. News* **21**(5) (1993) 31–38
4. Salem, K., Garcia-Molina, H.: Disk striping. In: Proceedings of the Second International Conference on Data Engineering, February 5-7, 1986, Los Angeles, California, USA, IEEE Computer Society (1986) 336–342

5. Patterson, D.A., Gibson, G.A., Katz, R.H.: A case for redundant arrays of inexpensive disks (raid). In Boral, H., Larson, P.Å., eds.: Proceedings of the 1988 ACM SIGMOD International Conference on Management of Data, Chicago, Illinois, June 1-3, 1988, ACM Press (1988) 109–116
6. Schikuta, E., Wanek, H.: Parallel I/O. Volume 15. (2001) 162–168
7. MPI-Forum: Mpi-2: Extensions to the message-passing interface (1997)
8. Carns, P.H., Ligon III, W.B., Ross, R.B., Thakur, R.: PVFS: A parallel file system for linux clusters. In: Proceedings of the 4th Annual Linux Showcase and Conference, Atlanta, GA, USENIX Association (2000) 317–327
9. Garcia-Carballeira, F., Calderon, A., Carretero, J., Fernandez, J., Perez, J.M.: The design of the Expand parallel file system. The International Journal of High Performance Computing Applications **17**(1) (2003) 21–38
10. Schmuck, F., Haskin, R.: GPFS: A shared-disk file system for large computing clusters. In: Proc. of the First Conference on File and Storage Technologies (FAST). (2002) 231–244
11. Oldfield, R., Kotz, D.: Armada: A parallel file system for computational grids. In: CCGRID '01: Proceedings of the 1st International Symposium on Cluster Computing and the Grid, Washington, DC, USA, IEEE Computer Society (2001) 194
12. Bent, J., Thain, D., Arpaci-Dusseau, A., Arpaci-Dusseau, R.: Explicit control in a batch-aware distributed file system. (2004)
13. Nowoczynski, P., Stone, N., Sommerfield, J., Gill, B., Scott, J.R.: Slash - the scalable lightweight archival storage hierarchy. In: MSST. (2005) 245–252
14. Teaff, D., Watson, D., Coyne, B.: The architecture of the high performance storage system (hpss). In: Goddard Conference on Mass Storage and Technologies. (1995)
15. Corbett, P.F., Baylor, S.J., Feitelson, D.G.: Overview of the vesta parallel file system. SIGARCH Comput. Archit. News **21**(5) (1993) 7–14
16. Calderón, A., García, F., Carretero, J., Pérez, J.M., Fernández, J.: An implementation of mpi-io on expand: A parallel file system based on nfs servers. In: Proceedings of the 9th European PVM/MPI Users' Group Meeting on Recent Advances in Parallel Virtual Machine and Message Passing Interface, London, UK, Springer-Verlag (2002) 306–313

Performance Modeling of a Fully Adaptive and Fault-Tolerant Wormhole Switching Strategy in 2-D Mesh

Farshad Safaei^{1,2}, Mahmood Fathy², Ahmad Khonsari^{1,3},
and Mohamed Ould-Khaoua⁴

¹ IPM School of Computer Science, Tehran, Iran

{safaei, ak}@ipm.ir

² Dept. of Computer Eng., Iran Univ. of Science and Technology, Tehran, Iran

{f_safaei, mahfathy}@iust.ac.ir

³ Dept. of ECE, Univ. of Tehran, Tehran, Iran

⁴ Dept. of Computing Science, Univ. of Glasgow, UK

mohamed@dcs.gla.ac.uk

Abstract. In recent years, many researchers have devoted much efforts to construct high performance interconnect networks resilient to faults. Their studies motivated by the fact that a network can be a major performance bottleneck in parallel processors; such as multiprocessors system-on-chip (Mp-SoCs), multicomputers and cluster computers. This paper proposes a new analytical model to predict message latency in 2-dimensional wormhole-switched mesh with a routing scheme suggested by Linder and Harden [1], as an instance of a fault-tolerant routing widely used in literature to achieve high adaptivity. Furthermore, the validity of the proposed model is demonstrated by comparing analytical results to those conducted through simulation experiments of the actual system and show a good degree of accuracy with as many as 10% nodes faulty.

1 Introduction

The demand for increased performance in many compute-intensive applications is a persuasive justification for parallel processing. Parallel computer systems consisting of hundreds or thousands multiple processing units connected via some interconnection network that collectively may undergo high failure rates. The performance of such a given network greatly depends on its topology, switching method and routing scheme. Network topology defines the way nodes are interconnected. In a mesh-connected multicomputer, processors exchange data and coordinate their efforts by sending and receiving messages through the underlying network. The switching method determines the way messages visit intermediate routers. The *wormhole switching* [2] is a popular technique used to provide interprocessor communication for contemporary multiprocessor systems. In wormhole switching, a message is divided into *flow control digits* (or flits). The flits are routed through the network one after another in a pipeline fashion. A flit of the message is designated as the *header flit*, which leads the message through the network. When the header flit is blocked due to lack of output channels, all of the flits wait at their current nodes for available channels. Routing is the process of

transmitting data from one node to another node in a given system. Linder-Harden [1] as an instance of fully adaptive fault-tolerant routing algorithm has been widely reported in the literature. This paper proposes a novel analytical model to compute message latency for Linder-Harden fully adaptive and fault-tolerant routing scheme in 2-D mesh networks. The model achieves a good degree of accuracy which is evident by the results gathered from simulation experiments to validate the proposed model.

The paper is organized into 5 main sections. Section 2 describes some definitions and background that will be useful for the subsequent sections. Section 3 gives a detailed presentation of the analytical model while Section 4 illustrates the design validation, which was performed using simulations. Finally, Section 5 presents conclusions.

2 Preliminaries

This section briefly describes k -ary 2-mesh and with its node structure, and then explores the Linder-Harden's routing algorithm.

2.1 The Mesh and Its Node Structure

A 2-dimensional (2-D) $k \times k$ mesh with $N=k^2$ nodes has an interior node degree of 4 and a network diameter of $2(k-1)$. Each node u has an address (u_x, u_y) , where $u_x, u_y \in \{0, 1, 2, \dots, k-1\}$. Two nodes $u: (u_x, u_y)$ and $v: (v_x, v_y)$ are connected if their addresses differ in one and only one dimension. Each node consists of a Processing Element (PE) and a router. Messages generated by the PE are transferred to the router through the injection channel. Messages at the destination are transferred to the local PE through the ejection channel. Each physical channel is associated with some, say V , *virtual channels*. A virtual channel has its own flit queue, but shares the bandwidth of the physical channel with other virtual channels in a time-multiplexed fashion [3].

2.2 The Linder-Harden's Routing Algorithm

Linder and Harden [1] have proposed a fully adaptive and fault-tolerant routing algorithm for bidirectional k -ary n -cubes. The main idea behind the Linder-Harden approach is the partitioning of the bidirectional physical network into several *Virtual Networks*. Routing within each virtual network is fully adaptive (minimal). The Linder-Harden approach requires 2^{n-1} virtual networks where n is the dimension of the mesh, and therefore requires 2^{n-1} virtual channels per physical channel. The insight gained from Linder-Harden was that it was possible to convert algorithms with dead-lock into dead-lock free algorithms by partitioning the domain of the routing function, where each partition would use a different virtual network.

3 The Analytical Model

This section describes the assumptions and notations used in the derivation of the analytical model.

3.1 Assumptions

The model uses following assumptions that are widely used in the literature [3-9].

- I. Nodes generate traffic independently of each other, and which follows a Poisson process with a mean rate of λ messages per cycle. The arrival process at a given channel is approximated by an independent Poisson process. Therefore, the arrival rate at a channel can be calculated using formula borrowed from *Jackson's queuing networks* [10].
- II. Faults occurred statistically [2] and each node failed independently with probability θ . Moreover, Faults are uniformly distributed in the network and do not disconnect it [2].
- III. Nodes or processors are more complex than links and thus have higher failure rates [2]. So, we assume only node failures.
- IV. Message destinations are uniformly distributed across network nodes.
- V. Message length is fixed and equal to M flits. Each flit is transmitted in one cycle from one router to the next.
- VI. The local queue at the injection channel in the source node has infinite capacity. Moreover, messages are transferred to the local PE as soon as they arrive at their destinations through the ejection channel.
- VII. Four virtual channels are used per physical channel in dimension 0 and the number of virtual channels that used in dimension 1 is two virtual channels per physical.

3.2 Derivation of the Model

The mean message latency is composed of the mean network latency, \bar{S} , which is the time to cross the network, and then the mean waiting time, \bar{W}_s , seen by the message in the local queue before entering the network. However, to capture the effects of the virtual channels multiplexing, the mean message latency is scaled by a factor, \bar{V} , representing the average degree of virtual channels multiplexing, that takes place at a given physical channel. Therefore, we can write the mean message latency as [6]

$$\text{Mean message latency} = (\bar{S} + \bar{W}_s)\bar{V} \quad (1)$$

Let us first calculate the average message arrival rate on a given channel $\langle a, b \rangle$ where a and b are two adjacent nodes. Many distinct paths exist between every pair of nodes in a mesh network. By selectively dividing traffic over these paths, load can be balanced across the network channels. This path diversity also enables the network to be quickly reconfigured around fault channels, by routing traffic along alternative paths. In general, if there are n dimensions numbered 0 to $n-1$ and there are Δ_i hops from a to b in the i^{th} dimension, then the total number of minimal routes from a to b is given by

$$|R_{ab}| = \prod_{i=0}^{n-1} \binom{\sum_{j=0}^{n-1} \Delta_j}{\Delta_i} = \frac{\left(\sum_{i=0}^{n-1} \Delta_i\right)!}{\prod_{i=0}^{n-1} \Delta_i!} \quad (2)$$

Since a link survives if and only if both nodes at its ends survive, we have

$$\Pr[A \text{ link survives}] = (1-\theta)^2 \quad (3)$$

The expected number of surviving links crossing any dimension is given by

$$2k(k-1)(1-\theta)^2 \quad (4)$$

For every source-destination pair of surviving nodes, s and d , for which channel $\langle a, b \rangle$ may be used, the probability that channel $\langle a, b \rangle$ is traversed can be expressed as

$$P_{(s,d),\langle a,b \rangle} = \frac{|R_{sa}| \times |R_{db}|}{|R_{sd}|} \times (1-\theta)^2 \quad (5)$$

With uniform traffic pattern, messages generated at a node have an equal probability of being destined to any other surviving node. Hence, the rate of messages produced at a specific node and destined to another surviving node equals to the ratio of the message generation rate, λ , to the number of surviving nodes in the network except itself. Therefore, the rate of messages generated at a specific node, s , and destined to another surviving node, d , that traverse a surviving channel $\langle a, b \rangle$ on its path equals to

$$\lambda_{(s,d),\langle a,b \rangle} = \frac{\lambda}{N(1-\theta)-1} P_{(s,d),\langle a,b \rangle} \quad (6)$$

Where N equals to number of nodes in the network (i.e., $N=k^2$). The rate of messages traversing a specific channel can be calculated as the aggregate of Equation (6) over all source-destination pairs that have at least one path between each other that traverses surviving channel $\langle a, b \rangle$ which is given by

$$\lambda_{\langle a,b \rangle} = \sum_{(s,d) \in G_{\langle a,b \rangle}} \lambda_{(s,d),\langle a,b \rangle} = \frac{\lambda}{N(1-\theta)-1} \sum_{(s,d) \in G_{\langle a,b \rangle}} P_{(s,d),\langle a,b \rangle} \quad (7)$$

Where $G_{\langle a, b \rangle}$ is the set of all pairs of source and destination nodes that have at least one path between each other that traverses channel $\langle a, b \rangle$. Since the mesh topology is asymmetric, opposing to the case of symmetric networks (such as tori and hypercubes), the mean network latency seen by messages generated at a specific surviving source node, destined to other surviving nodes will not be equal to that of every other source node. Hence, the network latency, $S_{(s, d)}$, seen by a message crossing from s to d should be determined for each surviving source-destination pair. Let $S=(S_x, S_y)$ be the source node and $d=(d_x, d_y)$ denote a destination node. We define the set $H=\{h_x, h_y\}$, where h_x and h_y denote the number of hops that the message makes along X and Y dimension, respectively.

$$h_x = |s_x - d_x|, \quad h_y = |s_y - d_y| \quad (8)$$

Also, the number of total hops made by the message between source and destination node is given by

$$|H| = h_x + h_y \quad (9)$$

Let there are L different paths from s to d . Assume that the messages is using path j ($1 \leq j \leq L$). The network latency, $S_{(s, d), j}$ seen by the message crossing from source node s

to destination node d along path j , consists of two parts. One is the delay due to actual message transmission time, $|H|+M$, and another term is due to the message blocking in the network, $T_{blocking,(s,d),j}$. Hence, $S_{(s,d),j}$ can be expressed as

$$S_{(s,d)} = (|H| + M + T_{blocking(s,d),j}) \cdot V_{mean,(s,d),j} \tag{10}$$

Where $V_{mean,(s,d),j}$ is the average multiplexing degree of the virtual channels at different physical channels used along path j . By averaging over all L distinct paths, the average message latency for the message from s to d can be calculated as

$$\bar{S}_{(s,d)} = \frac{1}{\|G_{<a,b>}\|} \sum_{(s,d) \in G_{ca,bs}} S_{(s,d)} \tag{11}$$

A message is blocked at a given channel when all the virtual channels in both dimensions are busy. Each message can just cross over a virtual channel in each dimension, depends on the message is located in which virtual network and which level. The probability of blocking depends on the number of output channels, and thus on the virtual channels that a message can use at its next hop. When a message has not passed any dimensions entirely it can select each dimensions that has free virtual channel, but when a message has entirely crossed a dimension it should select just the reminder dimension to make its next hop. A message is blocked at its i^{th} hop, if all the virtual channels that can choose for its next hop, being busy. Let $Q_{H,i}$ be the set of possible ways that i hops can be distributed over two dimensions such that the number of hops made in dimension X and Y be at most h_x and h_y . $Q_{H,i}$ can be defined as

$$Q_{H,i} = \{(i_x, i_y) \mid i_x + i_y = i, 0 \leq i_x \leq h_x, 0 \leq i_y \leq h_y\} \tag{12}$$

The probability that a message has entirely crossed dimension X on its i^{th} hop is given by

$$P_{(s,d),i}^{passX} = \frac{\|Q_{H,i}\|_{i_x=h_x}}{\|Q_{H,i}\|} \cdot P_{mean,(s,d),i,4}^{passX} \tag{13}$$

Where $P_{mean,(s,d),i,4}^{passX}$ is the probability that all virtual channels may be used by a message over all the possible paths from s to d in dimension X being busy, this probability can therefore be written as

$$P_{mean,(s,d),i,4}^{passX} = \sum_{l=1}^4 \binom{4}{l-1} \cdot \frac{\sum_{j=1}^{\|Q_{H,i}\|_{i_x=h_x}} P_{(a_j,b_j),l}^X}{\|Q_{H,i}\|_{i_x=h_x}} \tag{14}$$

Similarly, the probability that a message has entirely crossed dimension Y on its i^{th} hop is determined by

$$P_{(s,d),i}^{passY} = \frac{\|Q_{H,i}\|_{i_y=h_y}}{\|Q_{H,i}\|} \cdot P_{mean,(s,d),i,2}^{passY} \tag{15}$$

$$P_{mean,(s,d),i,2}^{passY} = \sum_{l=1}^2 \binom{2}{l-1} \cdot \frac{\sum_{j=1}^{\|Q_{H,i}\|_{i_y=h_y}} P_{<a_j,b_j>,l}^Y}{\|Q_{H,i}\|_{i_y=h_y}} \tag{16}$$

Messages in the first dimension (i.e., X) can move in both direction but they can move just in one direction in the second dimension (i.e., Y) depends on the virtual network, so the number of virtual channel in the first dimension is two time greater than the number virtual channel in second dimension and the $P_{(s,d),i}^{passX}$ is differ from the $P_{(s,d),i}^{passY}$. On the other hand, the probability that a message has not entirely crossed dimension X on its i^{th} hop can be expressed as

$$P_{(s,d),i}^{\overline{passXY}} = \frac{\|Q_{H,i}\|_{i_x < h_x, i_y < h_y}}{\|Q_{H,i}\|} \cdot P_{mean,(s,d),i,4}^{\overline{passXY}} \quad (17)$$

$$P_{mean,(s,d),i,4}^{\overline{passXY}} = \frac{\sum_{j=1}^{|H|} \|Q_{H,i}\|_{i_x < h_x, i_y < h_y} P_{<a_j, b_j>,4}}{\|Q_{H,i}\|_{i_x < h_x, i_y < h_y}} \quad (18)$$

The blocking time, $T_{blocking,(s,d),j}$, is calculated as the aggregate of the product of the blocking probability at the hop i^{th} along path j , $P_{blocking,(s,d),i}$ and the mean waiting time to have at least one free channel among channels of dimensions still to be visited

$$W_{mean,(s,d),i}^{passX} = \frac{\sum_{j=1}^{|H|} \|Q_{H,i}\|_{i_x = h_x} W_{<a_j, b_j>}}{\|Q_{H,i}\|_{i_x = h_x}} \quad (19)$$

The $T_{blocking,(s,d)}$ can therefore be written as follows

$$T_{blocking,(s,d)} = \sum_{i=1}^{|H|} T_{blocking,(s,d),i} \quad (20)$$

$$T_{blocking,(s,d)} = \sum_{i=1}^{|H|} (P_{(s,d),i}^{passX} \cdot W_{mean,(s,d),i}^{passX} + P_{(s,d),i}^{passY} \cdot W_{mean,(s,d),i}^{passY} + P_{(s,d),i}^{\overline{passXY}} \cdot W_{mean,(s,d),i}^{\overline{passXY}}) \quad (21)$$

To determine the mean waiting time to acquire a virtual channel may be treated as an $M/G/1$ queue [10]. Since the minimum service time at a channel equals to the message length, M , following a suggestion proposed in [5], the variance of the service time distribution can be approximated by $(\bar{S}_{<a,b>} - M)^2$; where $\bar{S}_{<a,b>}$ is the average service time of channel $<a, b>$ and can be calculated as the mean of $S_{(s,d)}$ of all source and destination nodes that have at least one path between each other that traverse channel $<a, b>$. Hence, the mean waiting time becomes

$$w_{<a,b>} = \frac{\lambda_{<a,b>} \bar{S}_{<a,b>}^2 (1 + (\bar{S}_{<a,b>} - M)^2 / \bar{S}_{<a,b>}^2)}{2(1 - \lambda_{<a,b>} \bar{S}_{<a,b>})} \quad (22)$$

For a specific surviving node s in the network, the average latency seen by a message originated at that node to enter the network, \bar{S}_s , equals to the average of all $S_{(s,d)}$ resulting in

$$\bar{S}_s = \frac{1}{N(1-\theta) - 1} \sum_{d \in G - \{s\}} S_{(s,d)} \quad (23)$$

A message originating from a given source node, s , sees a network latency \bar{S}_s . Modeling the local queue in the source node an $M/G/1$ queue, with the average arrival

rate of $\lambda/4$ and service time \bar{S}_s with an approximated variance $(\bar{S}_s - M)$ yields the average waiting time seen by a message at the source node s as

$$\bar{W}_s = \frac{(\lambda/4)\bar{S}_s^2(1+(\bar{S}_s - M)^2/\bar{S}_s^2)}{2(1-(\lambda/V)\bar{S}_s)} \tag{24}$$

The average waiting time at the source node is given by

$$\bar{W} = \frac{1}{N(1-\theta)} \sum_{s \in G} \bar{W}_s \tag{25}$$

The probability $P_{\langle a,b \rangle, v}^X$ that v ($0 \leq v \leq 4$) virtual channels at a given physical channel $\langle a, b \rangle$ in dimension X are busy, can be respectively determined using a Markovian model (details of the model can be found in [3, 6]). In the steady state, the model yields the following probabilities [3].

$$P_{\langle a,b \rangle, v}^X = \begin{cases} Q_{\langle a,b \rangle, 0} = 1 \\ Q_{\langle a,b \rangle, v} = Q_{\langle a,b \rangle, v-1} \lambda_{\langle a,b \rangle} \bar{S} & (1 \leq v \leq 3) \\ Q_{\langle a,b \rangle, v} = \frac{Q_{\langle a,b \rangle, v-1} \lambda_{\langle a,b \rangle}}{1/\bar{S} - \lambda_{\langle a,b \rangle}} \\ P_{\langle a,b \rangle, 0} = (\sum_{l=0}^4 Q_{\langle a,b \rangle, l})^{-1} \\ P_{\langle a,b \rangle, v} = P_{\langle a,b \rangle, v-1} \lambda_{\langle a,b \rangle} \bar{S} & (1 \leq v \leq 3) \\ P_{\langle a,b \rangle, v} = \frac{P_{\langle a,b \rangle, v-1} \lambda_{\langle a,b \rangle}}{1/\bar{S} - \lambda_{\langle a,b \rangle}} \end{cases} \tag{26}$$

Similarly, the probability $P_{\langle a,b \rangle, v}^Y$ that v ($0 \leq v \leq 2$) virtual channels at a physical channel are busy in dimension Y can be achieved using Equation (26). When multiple virtual channels are used per physical channel in dimension X , they share the bandwidth in a time-multiplexed manner. The average degree of virtual channel multiplexing that takes place at a specific channel $\langle a, b \rangle$ in dimension X , can be estimated by

$$\bar{V}_{\langle a,b \rangle}^X = \frac{\sum_{v=1}^4 v^2 \cdot P_{\langle a,b \rangle, v}^X}{\sum_{v=1}^4 v \cdot P_{\langle a,b \rangle, v}^X} \tag{27}$$

Similarly, the average degree of multiplexing of virtual channels, that takes place at a specific physical channel in dimension Y , can be estimated by

$$\bar{V}_{\langle a,b \rangle}^Y = \frac{\sum_{v=1}^2 v^2 \cdot P_{\langle a,b \rangle, v}^Y}{\sum_{v=1}^2 v \cdot P_{\langle a,b \rangle, v}^Y} \tag{28}$$

The average virtual channel multiplexing degree can be then approximated by

$$\bar{V}_{\langle a,b \rangle} = \frac{1}{2} (\bar{V}_{\langle a,b \rangle}^X + \bar{V}_{\langle a,b \rangle}^Y) \tag{29}$$

$V_{mean, (s, d), j}$ is the maximum $\bar{V}_{\langle a,b \rangle}$ of channels traversed by the path enumerated j , between source s and destination d and can be calculated as

$$\bar{V}_{mean(s,d),j} = \frac{1}{|H|} \sum_{i=1}^{|H|} \bar{V}_{\langle a_i, b_i \rangle, j} \tag{30}$$

The average virtual channels multiplexing degree for the channels delivering a message from s to d is given by

$$\bar{V}_{(s,d)} = \frac{1}{L} \sum_{i=1}^L \bar{V}_{mean(s,d),i} \quad (31)$$

By averaging over all multiplexing degrees for all possible surviving source-destination pairs, results the overall virtual channels multiplexing degree

$$\bar{V}_s = \frac{1}{N(1-\theta) - 1} \sum_{d \in G - \{s\}} \bar{V}_{(s,d)} \quad (32)$$

$$\bar{V} = \frac{1}{N(1-\theta)} \sum_{s \in G} \bar{V}_s \quad (33)$$

As fully adaptive routing distributes traffic evenly among all channels, the average service time at each channel is the same regardless of its position, and equivalents to the average network latency (\bar{S}). Equation (10) gives the network latency seen by a message to cross from the source node s to the destination node d . Averaging over the $N(1-\theta)$ possible surviving nodes in the network, yields the mean network latency for a typical message as

$$\bar{S} = \frac{1}{N(1-\theta)} \sum_{s \in G} \bar{S}_s \quad (34)$$

The above equations reveal that there are several inter-dependencies between the different variables of the model. For instance, Equations (9) and (19) illustrate that $\bar{S}_{(s,d)}$ is a function of $w_{<a, b>}$ while Equation (20) shows that $w_{<a, b>}$ is a function of $\bar{S}_{(s,d)}$. Given that closed-form solutions to such inter-dependencies are very difficult to determine the different variables of the model are computed using iterative techniques for solving equations. A message originating from a given source node sees a network latency of \bar{S} (given by Equation (31)). Modeling the local queue in the source node as an $M/G/1$ queue, with the mean arrival rate λ/V (recalling that a message in the source node can enter the network through any of the V virtual channels) and service time $\bar{S}_{<a,b>}$ with an approximated variance $(\bar{S}_{<a,b>} - M)^2$ yields the mean waiting time seen by a message at source node as [5].

4 Experimental Results

In this section, we present simulation results for validation the analytical model of Linder-harden's routing algorithm.

4.1 Model Validation

Extensive simulation experiments are conducted to validate the analytical model. The simulator is a Visual C++ program that mimics the behavior of Linder-Harden fully adaptive and fault-tolerant routing at the flit level in a 2-D mesh. The simulator uses the same assumptions as the analysis, and some of these assumptions are detailed here with a view of making the network operation clearer. The network cycle time is

defined as the transmission time of a single flit from one router to the next. Processors at each node generate messages randomly with an exponential distribution of inter-arrival time. All of the buffers in the routing algorithm are assumed to be a single flit wide. We also assume that each node failed independently with probability θ and message lengths are fixed at M flits. The destination node of a k -hop message is determined using a uniform random number generator. The latency measure includes the network delay as well as the waiting delay at the source node. The mean message latency is defined as the mean amount of time from the generation of a message until the last data flit reaches the local PE at the destination node. The other measures include the mean network latency, the time taken to cross the network, and the mean queuing time at the source node, the time spent at the local queue before entering the first network channel. In each simulation experiment, a total number of 100,000 messages are delivered. Output data are not collected in the first 10,000 messages in order to allow the system to stabilize. The 95% confidence interval of the results is estimated to be within 1% of the mean. Numerous experiments are conducted for

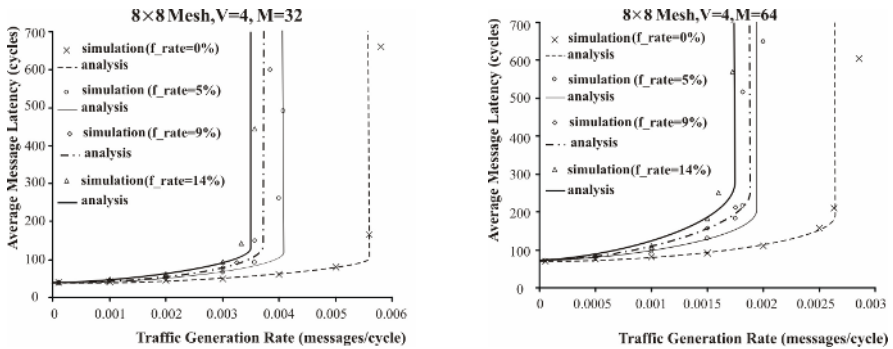


Fig. 1. Average message latency predicted by the model against simulation results in an 8×8 mesh with 0%, 5%, 9%, and 14% failure rates (f_rate)

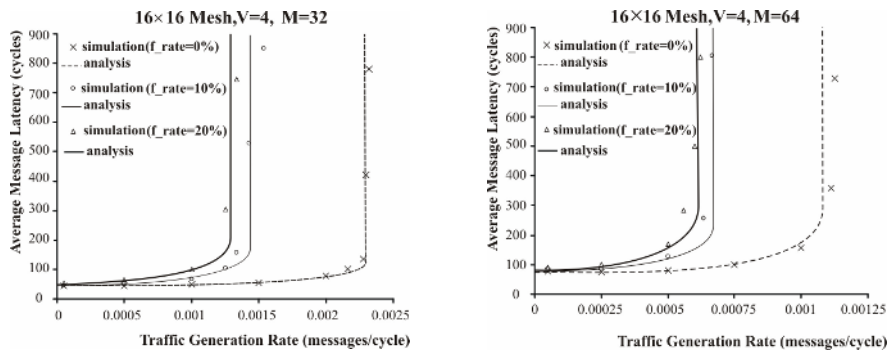


Fig. 2. Average message latency predicted by the model against simulation results in a 16×16 mesh with 0%, 10%, and 20% failure rates (f_rate)

different sizes of the network, failure rates, and message lengths to assess the accuracy of the analytical model.

Figs. 1 and 2 depict latency results predicted by the analytical model plotted against those provided by the simulator for 2-dimensional 8×8 and 16×16 mesh networks, respectively; with 0%, 5%, 9%, 10%, 14%, and 20% of the total network nodes faulty and different message lengths, $M=32, 64$ flits. In each case, we have randomly generated the required number of faulty nodes such that the remaining network is connected. The horizontal axis in the figures shows the traffic generation rate at each node (λ) while the vertical axis shows the mean message latency. The figures indicate that in all cases, the simulation measurements and the values predicted by the analytical model are in close agreement for various network operating environments. Moreover, the model predictions are still good even when the network operates in the heavy traffic region, and when it starts to approach the saturation region. However, some discrepancies around the saturation point are apparent. These can be accounted for by the approximation made to estimate the variance of the service time distribution at a channel. This approximation greatly simplifies the model as it allows us to avoid computing the exact distribution of the message service time at a given channel, and which is not a straightforward task due to the inter-dependencies between service times at successive channels as wormhole switching relies on a blocking mechanism for flow control. However, the main advantage of the proposed model is its simplicity which makes it a practical evaluation tool for assessing the performance behavior of a fully adaptive routing in 2-dimensional mesh.

5 Conclusions

As technology scales, efficiency and reliability of large-scale parallel computers becomes a significant concern in the performance of these systems. One of the key issues in the design of such systems is the development of an efficient communication network that provides high throughput and low latency under different working conditions and more importantly ability to survive beyond the failure of individual components (i.e., nodes or links). Fault-tolerant designs of these systems aim at providing continuous operations in the presence of faults by allowing the graceful degradation of system. A large number of fault-tolerant routing algorithms proposed in the literature for massively parallel systems, cluster-based systems, and multiprocessors system-on-chip (MP-SoCs). This paper proposes an analytical model to predict the mean message latency in wormhole-switched 2-dimensional mesh using the well-known Linder-Harden's routing algorithm. Simulation experiments have revealed that the message latency results predicted by the analytical model are in good agreement with those obtained through simulation under different working conditions. The novelty of the proposed analytic technique lies in its simplicity and accuracy. As future direction a number of interesting topics can be studied by tuning the model parameters in order to extend the proposed model to an n -dimensional mesh and consider the performance evaluation of the other well-known fault-tolerant routing algorithms.

References

1. Linder, D.H., Harden, J.C.: An adaptive and fault tolerant wormhole routing strategy for k-ary n-cubes, *IEEE TC*, 40 (1) (1991) 2-12.
2. Duato, J., Yalamanchili, S., Ni, L.M.: *Interconnection networks: An engineering approach*, Morgan Kaufmann Publishers, New York (2003).
3. Dally, W.J.: Virtual channel flow control, *IEEE TPDS*, 3 (2) (2002) 194–205.
4. Abraham, S., Padmanabhan, K.: Performance of the direct binary n-cube networks for multiprocessors, *IEEE TC*, 38 (7) (1989) 1000–1011.
5. Draper, J. T., Ghosh, J.: A comprehensive analytical model for wormhole routing in multicomputers systems, *JPDC*, 32 (1994) 202–214.
6. Ould-Khaoua, M.: A performance model of Duato's adaptive routing algorithm in k-ary n-cubes, *IEEE TC*, 44 (8) (1999) 1297–1304.
7. Duato, J.: On the design of deadlock-free adaptive routing algorithms for multicomputers: design methodologies, *PARLE'91, LNCS*, Vol. 505 (1991) 390–405.
8. Duato, J.: A new theory of deadlock-free adaptive routing in wormhole routing networks, *IEEE Transactions on Parallel and Distributed Systems*, 4 (12) (1993) 320-1331.
9. Lin, X., Mckinley, P.K., Lin, L.M.: The message flow model for routing in wormhole-routed networks, *Proceedings of the International Conference on Parallel Processing* (1993) 294–297.
10. Kleinrock, L.: *Queueing Systems*, Wiley, New York (1975).

Parallelization of Simulations for Various Magnetic System Models on Small-Sized Cluster Computers with MPI

Frank Schurz¹, Dietmar Fey¹, and Dmitri Berkov²

¹ Friedrich-Schiller-University Jena, Institute of Computer Science,
Ernst-Abbe-Platz 2, 07743 Jena, Germany

{Frank.Schurz, Dietmar.Fey}@inf.uni-jena.de

² INNOVENT Technologieentwicklung Jena, Prüssingstr. 27 B,
07745 Jena, Germany
db@innovent-jena.de

Abstract. The topic of parallelization of physical simulations has become an important part of scientific work today. However, except for the simple *Ising spin model*, simulations of various magnetic systems, e.g. the *Heisenberg model*, on small to moderate size cluster computers were not in strong focus within the field of Computational Physics. The work presented in this paper is a contribution to fill exactly this gap. The feasibility and the benefits of distributing such simulations among several processes are demonstrated by means of simulations of three physical models in this context: a 2-dimensional *Ising model*, the *Heisenberg model*, and a *magneto-dipolar glass model*. Herein we present these models and the applied parallelizational techniques. In the following, we show that with our parallelization scheme an almost ideal speed-up can be achieved on cluster computers by using *MPI*.

1 Introduction

Generally, physical simulations require a high computing effort. Consequently, the utilisation of parallel computing resources has become an inevitable part of Computational Physics [1], [2]. The attractiveness of cluster computers for simulation experiments grew due to their relatively low costs and convenient cost-performance ratio in the last decade. That is why they are now replacing the supercomputers or multiprocessor computers, which were once primarily used for that purpose, particularly in smaller research institutions.

A reasonable introduction in the field of magnetic models displays the *Ising model* [3]. It can be used to investigate the features of the thermodynamic equilibrium state in magnetic lattice systems with strong on-site anisotropy. In contrast to this, the *Heisenberg model* [4] and the model of the *magneto-dipolar glass* are also suitable for the investigation of the inherent dynamics of magnetic systems with the corresponding interatomic (interparticle) interaction. However, up to our knowledge no solutions have been published for simulations of the *Heisenberg model* and the model of the *magneto-dipolar glass* on cluster computers.

The simple *Ising model*, which was used for benchmark applications on cluster computers [5], has a so-called embarrassingly parallel solution, whereas the communication schemes of the *magneto-dipolar glass model* are much more complex. In this paper, we show that in spite of these higher communication efforts, even loosely-coupled cluster computers are an ideal parallel computing resource for efficiently carrying out compute-intensive magnetic simulation experiments for the *magneto-dipolar glass model*. On this ground, by means of measured speed-up values, we verify quantitatively the qualitative benefits of those models for the calculation on a cluster computer.

The *Metropolis algorithm* is commonly used for the simulation of the *Ising model*. The herein implemented parallel version is based on a so-called *checkerboard algorithm* [6]. For that model, solutions in *High Performance Fortran* were developed on fine-grained, closely-coupled shared memory parallel machines and MIMD parallel computers already twenty years ago, e.g. in [7]. Like the simple *Ising model*, the *Heisenberg model* is also used to describe ferromagnetic materials. Finally, the model of a *magneto-dipolar glass*, which consists of a disordered system of small magnetic particles, is investigated as well.

In the parallel solutions to all three models the effort for computation increases with $O(n^2)$ and the communication scales with $O(n)$, if n^2 is the number of considered magnetic moments. Hence, according to the *Amdahl effect* [8], [9] for a corresponding large n , the profit of the parallel computation should outperform the additional effort for communication, which is introduced due to the parallelization. By using experimental results, we show that the threshold for the break even is low. Furthermore, we found out that for a message-coupled system, like a cluster computer, the *Amdahl effect* is large enough to achieve very satisfying speed-up effects.

The programming language used for implementation was *FORTTRAN*. For the parallel programming environment, we selected the *de-facto* standard *MPI* [10]. The experimental results were measured on two Linux cluster computers.

The rest of this paper is organised as follows. First, we describe the models for the magnetic simulations in chapter 2. Chapter 3 focuses on our selected parallelization schemes. In chapter 4 we present and discuss the run time measurements achieved on our cluster computers – followed by a conclusion.

2 Models for Simulation of Magnetic Systems

2.1 The 2-Dimensional Ising Model

The *Ising model* is one of the standard models in statistical physics. It was originally invented to describe ferromagnetic phenomena. Though, it is appropriate for computer simulations of structured and unstructured complex systems in different disciplines. For example, in [11] the model is used to simulate the forming of opinions in a two-party-system. The 2-dimensional (2D) *Ising model* belongs to the simplest ones among those for magnetic systems with strong interaction. There are exact analytical solutions for it in 1D and 2D without an external field. However, the 3D model can only be solved by computer simulations.

The idea of the *Ising model* is based on the assumption that the magnetic moments of atoms can have only two opposite orientations which is justified for systems with a high on-site anisotropy. In this case the atomic spins are characterised entirely by two possible values: +1 or -1. The considered model describes a system of spins located on the sites of a square lattice. The number of spins within one row or column in the lattice is denoted as the lattice size N .

A fixed assignment of values to all spins is designated as configuration $\{s\}$. The energy of the whole system of a given configuration is determined by the interactions of the spins with their neighbours. We assume periodic boundary conditions (PBC) which are used to eliminate undesirable effects, arising from the system border. The *Hamilton function* of a given configuration $\{s\}$ is defined by $E\{s\} = -J \sum_{\langle i,j \rangle} S_i S_j$, in which S_i and S_j are spin projections, and J is the strength of interaction strength. For simplification we use a uniform interaction only between the nearest neighbours.

The usage of the *Hamilton function* for different configurations allows us to determine various characteristics concerning the whole system. If we denote the probability to find a certain configuration $\{s\}$ as $P\{s\}$, the mean energy can be calculated as $\langle E \rangle = \sum E\{s\}P\{s\}$. However, it is not possible to calculate all probabilities and to perform the summation over all possible configurations, because their number ($2^{N \cdot N}$) grows exponentially with the lattice size N .

An alternative possibility to determine the mean energy is the application of *Monte Carlo simulations* [12]. Instead of considering all configurations, only a sufficiently large sequence of configurations is selected. This sequence is generated in such a way that the frequency of occurrence $h\{s\}$ of a configuration $\{s\}$ converges to its probability $P\{s\}$ in the thermodynamic equilibrium. In this case, the calculation of the mean energy can be reduced to the arithmetic mean of the energies of all selected configurations. This can be achieved if the subsequent configuration is obtained from the previous one by flipping only one randomly determined spin. This new configuration is accepted with a certain probability depending on the energy difference between the new and the old configuration (*Metropolis algorithm* [13]).

2.2 The Heisenberg Model

The *Heisenberg model*, as well as the *Ising model*, is used to describe ferromagnetic effects. However, unlike the 1D and 2D variants of the *Ising model*, the *Heisenberg model* cannot be solved analytically, but only by means of computer simulations. In contrast to the *Ising model*, the spins in the *Heisenberg model* are described by vectors \mathbf{m} ($|\mathbf{m}| = 1$) with arbitrary orientation. Exactly this enables the study of system magnetization dynamics.

As in the simple *Ising model*, only an interaction between two neighbored spins is taken into account. Additionally, the influence of an external magnetic field \mathbf{H}_{ext} on the spins is included. In this case the *Hamilton function* is

$$E = J \sum_{\langle i,j \rangle} (\mathbf{m}_i \mathbf{m}_j) - \sum_i \mathbf{m}_i \mathbf{H}_{\text{ext}} \quad (1)$$

J describes again the exchange interaction strength. As in the *Ising model*, we also assume PBC. The total effective field acting on the magnetic moments contains contributions due to the exchange interaction and external field:

$$\mathbf{H}_i = J \sum_{\langle i,j \rangle} \mathbf{m}_j + \mathbf{H}_{\text{ext}} \quad (2)$$

The dynamics of magnetic moments is described by the equation of motion

$$\frac{d\mathbf{m}_i}{dt} = -\gamma[\mathbf{m}_i \times \mathbf{H}_i] \quad (3)$$

where γ denotes the so-called gyromagnetic ratio. For the integration of (3), we used the *Heun method* [14].

2.3 The Magneto-Dipolar Glass

In a *magneto-dipolar glass*, in contrast to the previous models, magnetic particles (represented as spheres) are randomly distributed in a 3-D space. At the beginning of the simulation we select the initial positions of the spheres in such a way that they do not overlap. This also holds true for spheres near the borders of the simulation cell because we again use PBC. The change of the magnetisation of a particle is described by the movement of a vector $\boldsymbol{\mu}$. The same equation of motion (3) can be used to model the spin dynamics.

The magneto-dipolar interaction between the particles in this model is a long-range one. Thus for a system with PBC we have in principle to sum over an infinite number of particles in order to compute the interaction field \mathbf{H}_{dip} on a given particle, which is obviously impossible. However, a fairly good approximation for the calculation of \mathbf{H}_{dip} is provided by the *Lorentz cavity method* (Fig. 1). In this method each particle is surrounded by a sphere with a fixed radius, called the cut-off radius R_c . Only the interactions with other particles within this sphere are taken into account exactly. The field from the rest of the system is computed within the approximation of a homogeneously magnetized medium which leads to an addition of a magnetization dependant constant. In [15], it has been shown that the double average distance $\langle \Delta r \rangle$ of the particles is sufficient for this critical radius.

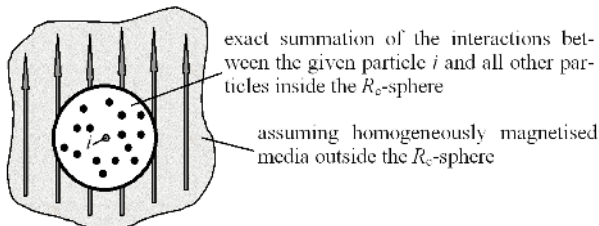


Fig. 1. Lorentz-cavity method

In addition, all particles possess a uniaxial magnetic anisotropy. A damping of the magnetic moment precession (rotation) is also taken into account, whose strength can be controlled by the factor λ . This leads to the equation of motion which is also solved numerically with the *Heun method*.

$$\frac{d\boldsymbol{\mu}_i}{dt} = \gamma[\boldsymbol{\mu}_i \times \mathbf{H}_i] - \underbrace{\gamma\lambda[\boldsymbol{\mu}_i \times [\boldsymbol{\mu}_i \times \mathbf{H}_i]]}_{\text{Damping}}. \quad (4)$$

3 Parallel Computing Schemes for the Models

3.1 Checkerboard Partitioning for the 2-D Ising Model

The selection of a uniform mapping of the lattice nodes onto the p parallel processes is appropriate for the parallel solution to the *Ising model*. Each process has its own local lattice with a local value for the energy. During the simulation, each process executes the *Metropolis algorithm* on its local lattice. Neighbourhood processes work on neighbored regions of the global lattice (Fig. 2). As a result of the PBC, this also holds true for the opposite outer edges of the lattice.

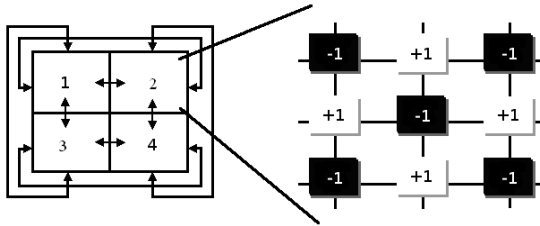


Fig. 2. Lattice partitioning with neighbour relations and checkerboard partitioning

Each process has to store information not only about its local part of the lattice, but also about its neighbored regions. Since in the above given model each partition has vertical and horizontal neighbour partitions, each change of the state of a spin, located at those edge sites, has to be performed in the neighbour process as well. This, however, requires a communication effort which is too high for the achievement of an effective parallelization. One possible solution to this problem is the partitioning of the lattice as a *checkerboard* in which each lattice node is assigned to be either black or white (Fig. 2). Due to the simple interaction, a spin placed on a white lattice site has only neighbours placed on black lattice sites and vice versa.

This partitioning scheme allows us to organise the program schedule in two parts. In the first part, the *Metropolis algorithm* is applied only to the white nodes. Afterwards the information located at the edges is exchanged between neighbored processes by means of *MPI* communication. Hence, all black nodes have the necessary information to update their states by applying the *Metropolis*

algorithm to all black nodes. The information at the edges is then again transmitted to the neighbour processes. At the end, the values for the energy of the local lattices are collected and added up to the value of the global system.

3.2 The Heisenberg Model

For the parallel realisation of the *Heisenberg model*, exactly as in the *Ising model*, the same uniform partitioning scheme can be used for the mapping of the lattice onto the parallel processes. With the *Ising model*, it is not possible to compute during the communication between the processes, because absolutely all transferred information is needed for the *Metropolis algorithm*. Contrary to this, the communication and the computation in the *Heisenberg model* can be carried out in parallel, as the differential equations are locally solved at each lattice site. Like in the *Ising model*, the lattice of every process possesses an outer edge which contains the magnetic moments of its neighbours (Fig. 3). The outer edge of the lattice is then followed by the inner one, consisting of the spins, which are transferred to the neighbours. The innermost part of the lattice is finally used for the local computation, because it does not play any role in the communication.

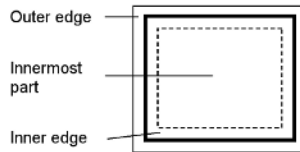


Fig. 3. Partition of the lattice of each process

First of all, each process sends the magnetic moments from the inner edge to its neighbours and receives magnetic moments from them, which are then stored on the outer edge. Since the algorithm uses only neighbored spins, the calculation in the innermost part runs parallel to the communication. This procedure cannot be used in the *Ising model* because the applied non-deterministic *Metropolis algorithm* needs the whole information for every calculation.

3.3 The Magneto-Dipolar Glass

In the parallelization the 3-dimensional space is divided into layers, so each process has only two direct neighbours. This enables the usage of a ring structure for the communication (Fig. 4). Each process P_i controls the information of the particles located in its own layer. This information goes through the ring in several phases. At the beginning the master process P_1 determines the particles' positions, dependent on input parameters, like e.g. the particle volume density, and distributes them evenly among the p processes. The exchange of information starts with the transmission of data by each process to its successor in the ring and correspondingly, with the receiving of data from its predecessor. At the same time, each process computes the interactions between its own particles.

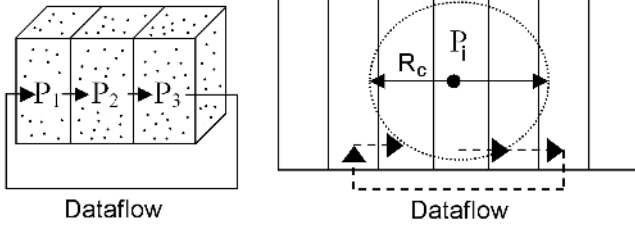


Fig. 4. Dataflow in entire ring and in reduced part of the ring

In the following phase, each process sends the data received in the previous phase to its successor and receives new ones from its predecessor. Meanwhile, the interactions between the particles, whose information has been received at last, and the particles of the process are computed. In this way, computation and communication can be executed simultaneously. The whole procedure takes place until each process has got all the required information. According to the results in [15], the communication process does not require $p - 1$ steps. The passing of the information is determined by the limitation of the interaction by the radius R_c . If the distance between each two particles of two different processes is greater than R_c , the communication between these processes can be omitted, as no interactions have to be computed. In this case, the information of each particle does not go through the entire ring, but only through that part of it which contains the processes using its information (Fig. 4). It can be shown that the number of neighbored processes p_{max} , which have to be passed, is given by

$$p_{max} = \lceil 2p / \sqrt[3]{n} \rceil. \quad (5)$$

4 Experimental Results

The simulations were carried out on two cluster computers. The first one consists of one master node (2.4 GHz P4/2 GB RAM) and eight worker nodes (2 GHz P4/512 MB RAM). In the second cluster computer we used eight nodes (3,06 GHz Dual Xeon/2 GB RAM). In both clusters the nodes are interconnected via Gigabit Ethernet. We achieved nearly the same speed-up values on both clusters. This confirms that our algorithmic design and our implementation is running stable on different environments. Owing to this, only the results on the second cluster computer are presented in the following. As MPI implementation we used LAM/MPI 7.1.1 [16]. For the measurements of the speed-up we selected problem sizes up to 5400 particles which are sufficient for dynamic simulations and which produced run times from 800 to 3000 seconds on a single node.

4.1 The 2-Dimensional Ising Model

As already mentioned, the computational costs increase by square with the lattice size ($k_1 \times N^2$), whereas the costs for communication increase linearly with $k_2 \times N$.

Furthermore, the constant factor k_2 is relatively low because we transmit only data of the type *integer*. Hence, we have already achieved very good speed-up values for comparatively small lattice sizes as displayed in Fig. 5.

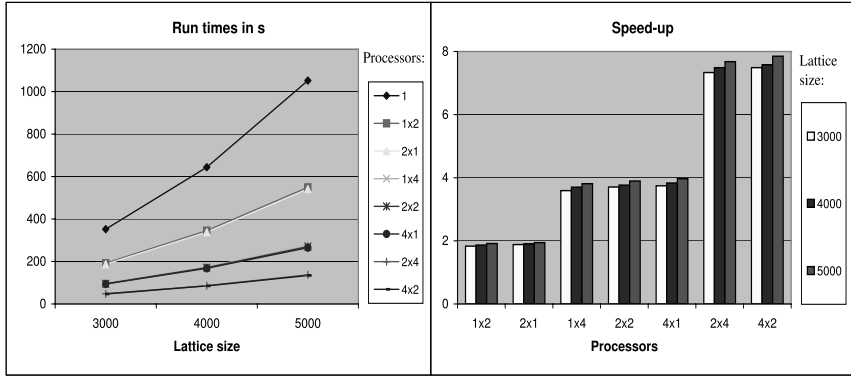


Fig. 5. Run times and speed-up values for the *Ising model* for different lattice sizes and various partitioning schemes

The measurement values also show that our developed algorithmic solution is independent from the exact partitioning scheme for a fixed number of processors. For example, we achieve almost the same values if the lattice is mapped onto a 1×4 , a 2×2 or a 4×1 processor array. This statement holds true for our simulation solution to the *Heisenberg model* as well.

4.2 The Heisenberg Model

Computation and communication costs have exactly the same relations to the lattice size as in the *Ising model*. However, because of the transmission of *vectors* of type *real* and not of *integers*, the effort to communicate is now higher. Additionally, the number of communicational steps is greater. Hence, the benefits of a parallelization affect only the higher lattice sizes as shown in Fig. 6.

4.3 The Model of the Magneto-Dipolar Glass

The computational costs increase as a square of the particle number. The speed-up values depend on the amount of reduction of the communication in the parallel simulation due to the limited radius of the used sphere in the *Lorentz cavity method* (see Fig. 4). For instance, by using 8 processors one saves 3 communicational steps, if less than 3600 particles are computed according to (5). However, the simulation of more particles can save even 5 communicational steps. It can be explained as follows: the higher the number of particles, the higher the particle concentration is, and the lower the critical radius R_c . Fig. 7 displays the run times and the speed-up values.

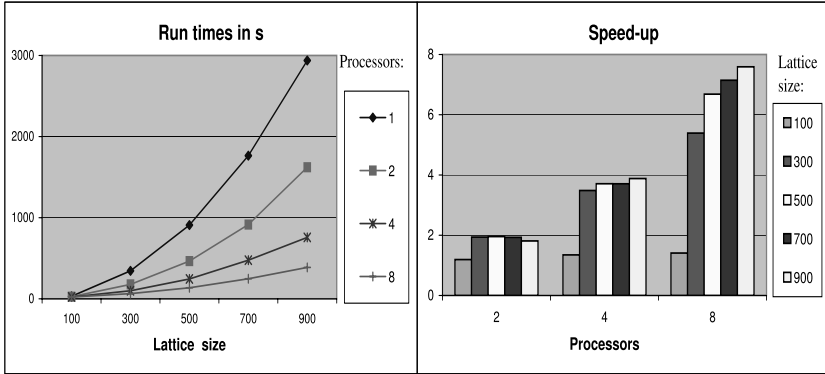


Fig. 6. Run times and speed-up values for the *Heisenberg model*

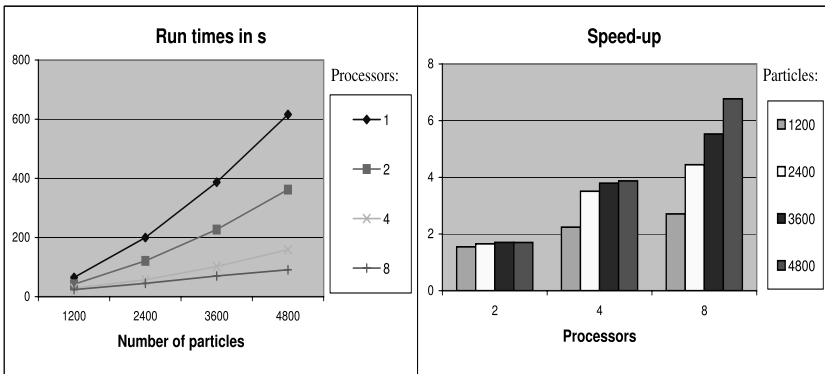


Fig. 7. Run times and speed-up values for *magneto-dipolar glass model*

We also calculated the *Karp-Flatt metric* [17], which expresses the experimentally determined serial fraction, for all three simulations. On condition that this value remains nearly constant for increasing numbers of used processors and particles, then, it means that the problem has been decomposed very well with respect to parallelization. We found out that this metric is decreasing with the number of processors. Hence, the influence of the serial fraction is reduced as the problem sizes increases, and we can achieve nearly ideal speed-up.

5 Conclusion

The herein presented work showed that an efficient parallelization of magnetic simulations, demanding intensive efforts for computation and communication, is possible even on small-sized cluster computers with a standard network like Gigabit Ethernet. This was demonstrated for three models. The well-known *Ising model* provides satisfying speed-up values at already small lattice sizes, and

this by means of the *checkerboard algorithm*. For the *Heisenberg model* and the *magneto-dipolar glass* we could achieve almost optimal speed-up values, which are dependent on the size of the system. Above all, this was made possible by the overlapping of communication and computation. In particular, for the *magneto-dipolar glass model*, which has the most challenging communication scheme, we achieved also good speed-up values. This was made possible by exploiting the fact that the information interchange can be limited to the critical distance length. Hence, it is to assume that for sufficiently large problem sizes these parallel simulations are also applicable for grid computing systems in which latency and bandwidth performance is much lower than in a cluster computer.

References

1. Hockney, R.W., Eastwood, J.W.: Computer simulation using particles. Institute of Physics Publishing, Bristol New York (1988).
2. Landau, R.H., Paez, M.J.: Computational physics - problem solving with computers. Wiley & Sons, New York (1997).
3. Ising, E.: Zeitschrift Fuer Physik 31. (1925) 253.
4. Anderson, P.W.: New approach to the theory of superexchange interactions. Phys. Rev. 115. (1959) 2-13.
5. Grove, D.A., et. al.: Cluster Computing with iMacs and Power Macintoshes. Proc. Parallel and Distributed Computing Systems (PDCS'99). Fort Lauderdale (1999).
6. Fox, G., et al.: Solving Problems on Concurrent Processors. Prentice Hall, Englewood Cliffs, NJ (1988).
7. <http://www.dhpc.adelaide.edu.au/workshops/CSSM/examples/ising/>
8. Amdahl, G.: Validity of the single processor approach to achieving large-scale computing capabilities. AFIPS Conference Proceedings (30). (1967) 483-485.
9. Quinn, M.J.: Chapter Performance Analysis in Parallel programming in C with MPI and OpenMP. McGraw-Hill, Boston, Mass. (2003).
10. <http://www.mpi-forum.org/>
11. Kohring, G.A.: J. Phys. I France 6. (1996) 301.
12. Landau, D.P., Binder, K.: A guide to Monte Carlo simulations in statistical physics. Cambridge University Press, Cambridge (2000).
13. Metropolis, N., et al.: J. Chem. Phys. 21. (1953) 1087.
14. Lambert, J.D.: Numerical methods for ordinary differential systems, the initial value problem. Wiley, Chichester (1991).
15. Berkov, D.V., Gorn, N.L.: Susceptibility of the disordered system of fine magnetic particles: Langevin-dynamics study. J. of Physics Condensed Matter. (2001) 13.
16. Burns, G., Daoud, R., Vaigl, J.: LAM: An open cluster environment for MPI. Proceedings of Supercomputing Symposium'94. Univ. of Toronto (1994) 379-386.
17. Karp, A.H., Flatt, H.P.: Measuring parallel processor performance. CM 33(5). (1990) 539-543.

A New Reflective and Reliable Context-Oriented Event Service Architecture for Pervasive Computing*

Sung Keun Song, Hee Yong Youn**, and Ungmo Kim

School of Information and Communication Engineering,
Sungkyunkwan University, 440-746, Suwon, Korea
kkskk103@skku.edu, youn@ece.skku.ac.kr,
umkim@yurim.skku.ac.kr

Abstract. Conventional middleware technologies lack the support for handling dynamic aspects of the new pervasive computing environment. Reflective middleware is a principal and efficient system which can deal with ubiquitous environment. It can reliably and quickly deliver important events and filter useless ones. In this paper we propose a new reflective and reliable context-oriented event service paradigm. The proposed event service supports reliable communication as well as reflective filtering through the adapters. It also supports reflective and dynamic context-oriented channel management for evenly distributing the load. An experimentation with six PCs reveals that the proposed scheme outperforms an existing popular commercial middleware in terms of event delivery speed. The improvement gets more significant as the size of event increases.

Keywords: Adapter, context-oriented channel, event service, middleware, reflective filtering.

1 Introduction

In the past many researchers have developed various middleware technologies to facilitate the development of the systems and applications in the distributed computing environments. Despite aiding the development of distributed applications, the conventional middleware technologies lack the support for handling the dynamic aspects of the new pervasive computing environment. In the pervasive computing environment the applications require a middleware that can be effectively adapted according to the changes in the environment. Such middleware is called adaptive and reflective middleware [1,2].

Adaptive middleware is a software system whose functional behavior can be modified to effectively react to the change in the environment or requirements [3,4]. Reflective middleware is the next logical step to take once an adaptive middleware is achieved. A reflective system is a one that can examine and reason about its capabilities and operating environment, allowing it to self-adapt at runtime. The re-

* This research was supported in part by the Ubiquitous Autonomic Computing and Network Project, 21st Century Frontier R&D Program in Korea and the Brain Korea 21 Project in 2005.

** Corresponding author.

flective middleware is a principal and efficient system for dealing with highly dynamic environments yet supporting the development of flexible and adaptive systems and applications [1,2,5].

In the pervasive computing environment the adaptive and reflective middleware needs to reliably and quickly deliver and receive the events, that is, the contexts on the environment, system, user, etc. to adapt itself at runtime. It also needs to be able to distinguish important events from useless ones frequently generated. The requirements have been tried to be satisfied by various middleware products that are characterized as the message oriented middleware, message queuing, or publish-subscribe model. The publish-subscribe model is a representative event transmission model widely used. The existing products based on the model are JMS (Java Message Service), CORBA event service [6], and TIBCO RV [7]. The event service provided by CORBA is intended to support decoupled, asynchronous communication among the objects. However, it is not reliable. Thereby, the event service of TAO [8] and Visibroker [9], the representative CORBA-based middleware, separately supports reliable communication. Most CORBA-based middleware including TAO and Visibroker also support filtering to process unwanted events, which is handled mainly by the event channels. In that case, the filtering causes an overhead at the event server in providing the event and notification service.

In this paper we propose a reflective context-oriented event service architecture extending the CORBA event service. The proposed event service supports reliable communication as well as reflective filtering in the adapters to reduce the overhead of filtering. It can be done by reflectively filtering the meaningless events out at the server, client, and channel, respectively. The proposed event service also supports reflective and dynamic context-oriented channel management for evenly distributing the loads. An experimentation with six PCs reveals that the proposed scheme outperforms the popular commercial event-based middleware, TIBCO RV, in terms of event delivery speed. The improvement gets more significant as the size of event increases.

The rest of the paper is organized as follows. Section 2 describes the publish-subscribe model. Section 3 presents the proposed reflective context-oriented event service for pervasive computing. Section 4 evaluates the performance of the proposed scheme, and Section 5 concludes the paper with some remarks.

2 The Publish-Subscribe Model

2.1 Event Service

In the publish-subscribe model the suppliers produce events while the consumers receive them from the event service server. Both the suppliers and consumers connect to one or more event channels. An event channel transfers events from the suppliers to the consumers without requesting the suppliers to have information on the consumers or vice versa. The event channel works as a central mediator in the event service server. It is responsible for supplier and consumer registration; clear, timely, and reliable event delivery to all the registered consumers; and controlling errors associated with unresponsive consumers. The event service server provides two models for event transfer - the push model and pull model. With the push model, the suppliers push events to the event channel through the proxyconsumer, and the proxysupplier of

the event channel pushes events to the consumers. Figure 1(a) shows the push type event delivery. Note that the arrow originated from the server points the client [6].

For the pull model, event transfer occurs in the opposite direction of the push model: the consumers pull events from the event channel mediator through the proxy-supplier, and the proxy-consumer of the event channel pulls events from the suppliers. The pull model is shown in Figure 1(b).

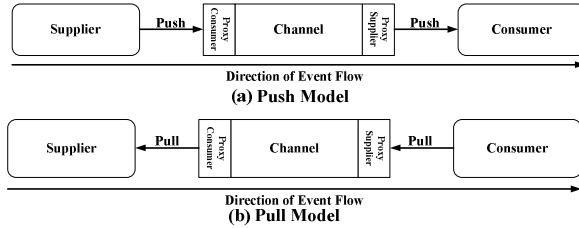


Fig. 1. The push and pull model

Event channels allow multiple suppliers and consumers to connect to them. Since the suppliers and consumers may want to use different models for event delivery, the event channel supports four different combinations of the push and pull model; push/push, push/pull, pull/push, and pull/pull model for supplier and consumer, respectively. These four models differ in the degree of activeness of the suppliers and consumers.

2.2 TIBCO

The standard components of TIBCO Rendezvous [7] include a TIBCO API library and a Rendezvous communications Daemon (RVD). Here each process links to a version of the Rendezvous API library. In most environments, one RVD process runs on a host computer. It has add-on components such as Router Daemon (RVRD) and transactional manager RVTX to enhance the capability. Figure 2 illustrates the structure of TIBCO Rendezvous, where Computer 1 runs Program A and a daemon process while Computer 2 runs two programs, B and C, which connect to the network through a single Rendezvous daemon process. All the three programs can communicate with one another through the daemons [7].

As seen in Figure 2, an RV, which connects to an RVD instance and a service port of a TIBCO Information Bus (TIB), is used for sending and/or receiving the

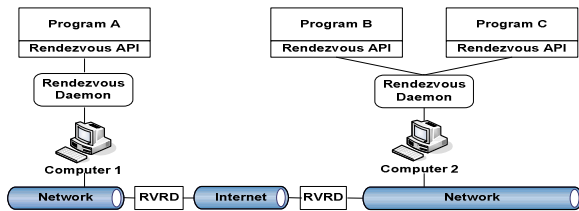


Fig. 2. The structure of TIBCO Rendezvous

messages. The TIB is a virtual channel in the TRDP/UDP/IP protocol. The TRDP (TIBCO Reliable Data Protocol) sits on top of the unreliable UDP to support reliable message delivery. To support WAN-wide communication, the TIBCO RV needs one RVRD on each subnetwork. It also needs one RVTX per network for transactional management. The TIBCO RV supports reliable, certified, and transactional messaging. For reliable messaging, the RVD manages message delivery and the RV infrastructure is used for sending or receiving the messages. In Certified Messaging (CM), for persistent and non-persistent messages, the RVD no longer concerns the reliability but used only as a message channeling media; the RV infrastructure contains additional services handling the CM. The RV peers can use either unicast, multicast, or broadcast to transmit the messages to the subject-based destination. The receiving peers need to subscribe to a subject to receive the relevant messages. In unicast mode, the sender uses the unique ID of the receiving peer represented by the subject to send the messages to the receiver (1-to-1). In multicast mode, the multicast IP addresses are used to specify a group of computers to which the messages need to be transmitted. In broadcast mode, the messages are transmitted to all the computers in the network, regardless of whether or not there exist active subscribing peers [7].

3 The Proposed Event Service

The proposed event service is a new reflective and reliable context-oriented event service embedded in the CALM (Component-based Autonomic Layered Middleware) research project [10,11].

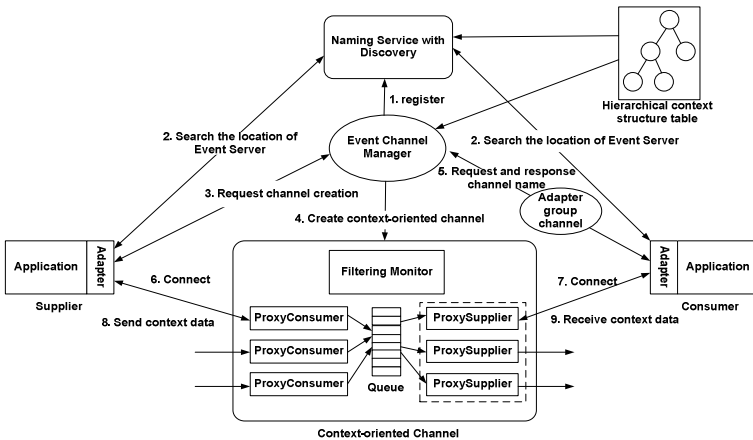


Fig. 3. The flow of context-oriented channel management using the adapters

3.1 Operational Mechanism

The proposed reflective and reliable context-oriented event service is an extension of CORBA-based omniEvent service [12]. It consists of adapters, event channel manager, and channels as shown in Figure 3. The operational mechanism of the proposed

event service is as follows. When operating as an event server, the event channel manager registers at the naming service (Act. 1). The supplier and the consumer search the location of the event server (Act. 2). When an adapter establishes a connection to a server, it uses a default channel to request a channel creation of certain properties, consisting of context and specific adapter information (Act. 3). The default channel is an adapter group channel, which is managed by the platform administrator residing in the discovery module. The event channel manager creates an event channel and assigns an appropriate name (Act. 4). Then the adapter is treated as a context supplier. The created event channel is monitored by the manager along with the context supplier for dynamic management. If other adapters request a specific context through the adapter group channel, the discovery agent provides the channel name matching to the context to let them connect to a context-oriented event channel (Act. 5). The context supplier transmits context information through the context-oriented event channel and then the adapter group receives them (Act. 6-9).

• Adapter

The adapter has various properties. First, it supports developers in the development of the systems and applications using the reflective context-oriented event service. The developers need not consider the details about channel creation, channel selection, etc. since the adapter automatically sends a request of a channel creation to the event channel manager and connects to the channel after it is created. Second, the adapter supports multithread and has one event queue per each supplier and consumer. The event queue is used to support reliable communication. Third, the adapter allows filtering. In case of the suppliers it filters out useless events the consumers do not want to receive according to the filtering criteria received from the filtering monitor of the channel it connects to.

• Event Channel Manager

The event channel manager is responsible for managing the context-oriented channels. When operating as an event server, it registers at the naming service. The supplier sends a request of a channel creation to the event channel manager using the registered information at the event server. The consumer inquires the event channel manager whether a relevant channel has been created or not.

• Context-Oriented Channel

The context-oriented channel decouples the communication between the suppliers and consumers for allowing asynchronous communication. It consists of a ConsumerAdmin object, a SupplierAdmin object, a filtering monitor, an event queue, and proxies. The ConsumerAdmin object is responsible for adding the consumers while the SupplierAdmin object is responsible for adding the suppliers. Whenever it adds a consumer, the ConsumerAdmin creates a proxysupplier. On the contrary, whenever a supplier is added, the SupplierAdmin creates a proxyconsumer. The event queue is a circular buffer. It stores the events received from the suppliers to support reliable communication. The size of the queue is determined according to the size of the system resource and context, and transmission frequency. The filtering monitor monitors and analyzes filtering criteria of the consumers through relevant proxysupplier, and informs the adapters of the suppliers on the outcomes.

3.2 Reflective Channel Management

Context-oriented channel creation and management of the proposed reflective and reliable context-oriented event service are dynamically performed according to the requested context by the agent via the discovery operation through the hierarchical context structure. The naming service with the discovery module and the context-oriented channel manager adopt a hierarchical context structure for reflection. Furthermore, the reflective context-oriented event service uses the COIDL (Context-oriented Interface Definition Language) to categorize the context into respective representative type, which is used in the hierarchical context structure. The COIDL defines and categorizes the contexts for specific intelligent agent service and groups the contexts into a hierarchical structure. The COIDL explicitly defines the role of the components by defining the prefix, middle, and suffix using the Hungarian Notation and CORBA IDL to efficiently manipulate the contexts. The context-oriented dynamic channel in the event service can assure rebinding of a protocol and optimized transmission according to the type of the transmitted event data. Here the client developers do not have to know the specific name of context channel or context structure. They only need to concern what kinds of context information will be used.

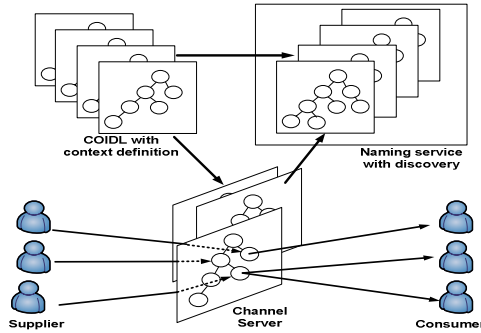


Fig. 4. The structure of context-oriented channel management

Each adapter has a default channel for the communication with other adapters. The transmitted event data correspond to specific context information of the agents. The reflective channel server employs a hierarchical context structure with the COIDL and the naming service as shown in Figure 4. The context information is used by the context-oriented channel which is managed by the event channel manager. The context-oriented channel is automatically created, named, and deleted with the channel message generated by the event channel manager. This mechanism lets the system administrator avoid unnecessary task and waste of the system memory due to unused channels.

3.3 Reliable Communication

The proposed event service uses event numbering and event queues to support reliable communication. The format of an event of the proposed event service is as follows;

```

struct EventHeader {
    bool                ACK;
    unsigned short     EventNumber;
    unsigned short     Size;
    any                EventData;
};
    
```

The event channel and adapter have an event queue, respectively. Reliable communication is provided as follows; the adapter of a supplier stores events at its own event queue before sending them to the event channel. Thereafter, it sends the events to the event channel. It waits for an acknowledgment from the event channel after sending the events. If the adapter receives an ACK from the event channel and the event queue is full, it overwrites the Acked events with new events until the events are Acked. In case that the adapter receives a retransmission request from the event channel, it resends the events stored in the event queue.

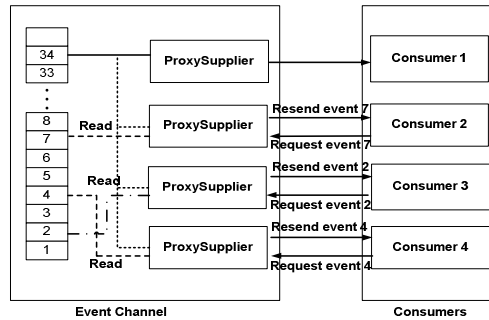


Fig. 5. The retransmission structure between the event channel and consumers

The event channel receives the events transmitted from the adapter of a supplier. It checks the number and size of the received event. In case that the number or size of the received event is invalid, the event channel requests the adapter of the supplier to resend the missing or invalid size event. Otherwise, the event channel stores the received event at its own event queue. The event channel receives an event as soon as it sends the events to the consumers. If the event channel receives retransmission requests from the consumers, it handles them separately. That is, each proxysupplier of the consumer requesting a retransmission resends the events stored in the event queue as shown in Figure 5.

The adapter of the consumer receives the events transmitted from the event channel. It checks the number and size of the received event. If they are invalid, it requests the event channel to resend the missing or invalid size event.

3.4 Reflective Filtering

The objective of the reflective filtering is to prevent waste of the event queue of the event channel due to useless events and reduce the network load. The process for reflective filtering is shown in Figure 6. The adapter of the consumer connects to an

event channel and sends its filtering criteria to the relevant proxsuppliers at the same time. The filtering monitor of the event channel monitors and analyzes the filtering criteria of the consumers and sends the result of analysis to the adapters of the suppliers. The filtering monitor is normally in sleeping mode but activates itself upon receiving a new filtering criterion from the consumers or an event channel of a new consumer connects to it. The adapter of the supplier receives the filtering criteria from the filtering monitor of the event channel. The adapter of the supplier filters out the events that the application has not indicated to receive from the event channel.

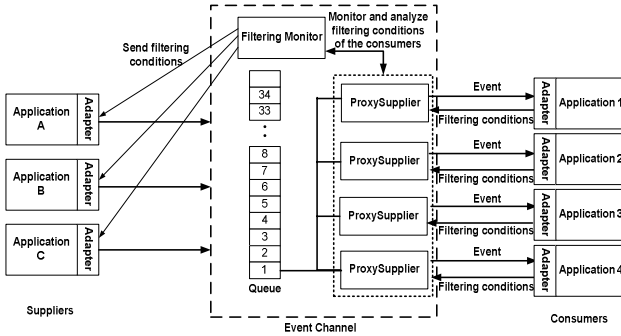


Fig. 6. The process for reflective filtering

An example of the reflective filtering process is shown in Figure 7. We assume that Consumer 1 wants only the contexts of Set AA, Consumer 2 wants only the contexts of Set BB, and Consumer 3 and Consumer 4 want only the contexts of Set CC and DD, respectively. We also assume that Consumer 1, 2, 4 connect to the event channel first. The filtering monitor of the event channel monitors and analyzes the filtering criteria of the consumers. It sleeps after sending the result of analysis, the filtering criteria of $(AA \cup BB \cup DD)$, to the adapters of the suppliers. The adapters of the suppliers filter out the events of $(\overline{AA \cup BB \cup DD})$ and send only the events of $(AA \cup BB \cup DD)$ to the event channel. When Consumer 3 connects to the event channel later, the filtering monitor wakes up and sends the filtering criteria of $(AA \cup BB \cup CC)$ to the adapters of the suppliers after analyzing the new filtering criteria. After this, it returns to sleep mode again.

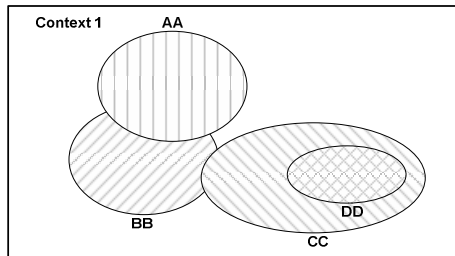


Fig. 7. An example of filtering process

4 Performance Evaluation

The performance evaluation has been carried out concerning message transmission efficiency and compares the proposed event service, omnient service, and TIBCO RV. The test platform includes six Windows XP-based PCs. These PCs are identical, each with one 2.1-Ghz CPU and 512-Mbyte RAM. In case of the proposed event service and omnient service two PCs host a supplier and a naming server, respectively and the remaining 4 PCs host the consumers. In case of the TIBCO RV one PC is a sender (supplier), which connects to its local RVD instance, and four PCs are subscribers (consumer), which are connected to their local RVD instances. Figure 8 and 9 show the average transmission time of 1000 test runs in case of one-to-one and one-to-many connection, respectively.

Figure 8 shows that the proposed event service is slightly slower than the omnient service since the omnient service does not support reliable communication. Figure 9 shows the performance of the proposed event service and TIBCO RV in case of one-to-one and one-to-four connection. Observe that the proposed event service always outperforms the TIBCO RV. Especially, the difference gets more significant as the event size increases for one-to-many connection. The elapse time of message transmission of the TIBCO RV exponentially increases while that of the proposed event service shows little increase. This reveals that the performance of the proposed event service is not so much influenced by the number of consumers, implying high scalability.

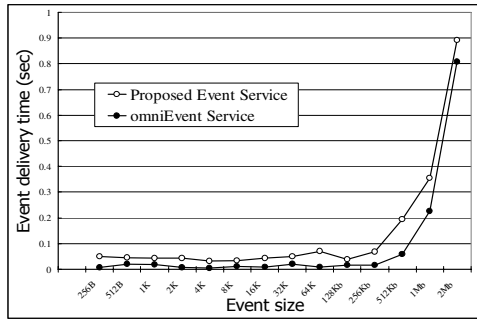


Fig. 8. The performance of the proposed event service and the omnient service

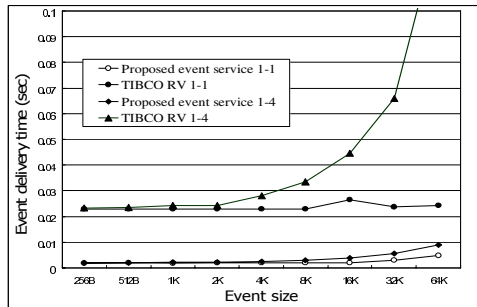


Fig. 9. The performance of the proposed event service and TIBCO

5 Conclusion

The importance of event service is very high in the pervasive computing environment. In this paper we have proposed a new reflective and reliable context-oriented event service supporting reliable communication, reflective channel management, and reflective filtering through the adapters. The proposed event service has been implemented in the CALM developed by the authors. It reduces the network load of CORBA-based event servers using reflective filtering and allows efficient and reliable event service using context-oriented channel management.

The future work is to implement additional functions of the reflective context-oriented event service; interoperability function supporting communication with heterogeneous platform such as DCOM, .NET, and EJB, dynamic protocol binding to adapt to diverse network environment, transaction service, etc. In the future more research will also be carried out to consider other middleware such as light weight CORBA and real-time CORBA.

References

1. Astley, M., Sturman, D., and Agha, G.: Customizable middleware for modular distributed software. *Commun. ACM* 44, 5 (2001) 99–107.
2. Coulson, G.: What is reflective middleware? *IEEE Distrib. Syst. Online* 2, 8 (2001); <http://computer.org/dsonline/middleware/RMarticle1.htm>.
3. Schantz, R.E., and Schmidt, D.C.: *Middleware for Distributed Systems - Evolving the Common Structure for Network-centric Application*, Encyclopedia of Software Engineering, New York, Wiley & Sons pp. 801-813.
4. Loyall, J.P., et al.: Comparing and Contrasting Adaptive Middleware Support in Wide-Area and Embedded Distributed Object Applications. *Proceedings of the 21st IEEE International Conference on Distributed Computing Systems (ICDCS-21)*, Phoenix (2001) 16-19.
5. Blair, G.S., et al.: The Design of a Resource-Aware Reflective Middleware Architecture, *Proceedings of the 2nd International Conference on Meta-Level Architectures and Reflection (Reflection'99)*, Springer-Verlag, Vol. 1616, Berlin Heidelberg France, (1999) pp.115-134
6. Object Management Group.: *Event Service Specification, Version 1.2*, October 2004. <http://www.omg.org/docs/formal/04-10-02.pdf>
7. TIBCO. : *TIBCO Rendezvous™ Concepts*, Software Release 7.1, October 2002. <http://www.tibco.com/>
8. <http://www.cs.wustl.edu/~schmidt/TAO.html>
9. <http://www.borland.se/visibroker/>
10. Han, S., Youn, H.Y.: A New Middleware Architecture for Community Computing with Intelligent Agents, *Ubiquitous Computing & Networking Systems 2005*
11. Han, S., Song, S.K., and Youn, H.Y.: CALM: An Intelligent Agent-based Middleware Architecture for Community Computing, *Software Technologies for Future Embedded & Ubiquitous Systems*, IEEE, 2006
12. <http://omniorb.sourceforge.net/>

X-Torus: A Variation of Torus Topology with Lower Diameter and Larger Bisection Width

Huaxi Gu¹, Qiming Xie¹, Kun Wang², Jie Zhang³, and Yunsong Li¹

¹ State key lab of ISN, Xidian University,
Xi'an, China 710071

² School of Computer Science, Xidian University,
Xi'an, China 710071

³ Dept. of Computing and Information Systems, Univ. of Luton,
UK, LU1 3JU

hxgu@xidian.edu.cn, kwang@mail.xidian.edu.cn,
Jie.Zhang@luton.ac.uk

Abstract. This paper introduces a new interconnection network called X-torus (cross-torus). An X-torus network is an enhancement of torus network by adding some crossing links. Hence, the distant nodes can be reached by using these links with fewer hops compared to the torus network. Comparisons with some popular networks such as 2D mesh, 2D torus and E-torus show that X-torus has shorter diameter, shorter average distance and larger bisection width. It also retains advantages such as symmetric structure, constant degree and scalability of the torus network. A simple distributed routing algorithm for X-torus network is also proposed, which identifies shortest path with only the address of the source and destination. In all, X-torus network is potentially an attractive interconnection network topology.

1 Introduction

The interconnection networks have been widely used in various areas, such as parallel multi-computer, multi-processor systems, networks of workstations and deep space communication. It can be represented as a graph, where a processor is represented as a node and the communication channel between each two nodes is represented as an edge. The interconnection networks are commonly evaluated by parameters such as diameter, average distance, bisection width and so on. The diameter and the average distance are commonly used to describe and compare the static network performance of the topology. The diameter of a network is the maximum distance between two nodes along a shortest path. The average distance is the mean distance between all distinct pairs of nodes in a network. An interconnection network with small diameter and average distance implies potentially small communication delay. Bisection width is defined as the minimum number of channels that must be removed to partition the network into two equal parts. It is a critical factor in determining the performance of a network because in most cases, the messages generated in one half of the network are needed by the other half. Large bisection width will remove the bottleneck of the bisection links.

Among the existing topologies, the family of torus is one of the most popular interconnection networks due to its desirable properties such as regular structure, ease of implementation and good scalability[1]. It has been used in many practical systems such as Cray T3D, Cray T3E [2], Fujitsu AP3000 [3], Ametak 2010 [4], Intel Touchstone [5] and so on. Recently, Avici Systems also uses torus as the switching fabrics of the terabit routers [6]. Nowadays, much of the community has moved on to lower-dimensional topologies such as 2D torus [7]. 2D torus can offer easy scalability compared with the high dimensional torus. But the diameter and the average distance of 2D torus are small. What’s more, the degree of 2D torus is only four, which cannot provide high path diversity. A variation of the 2D torus has been used in the MasPar MP-2 [8], called extended-torus (E-torus), which is an 8-degree network. E-torus can be viewed as a combination of two 2D torus topologies. It reduces the diameter at the cost of adding too many links. Hence, the cost is very high.

In this paper, we propose a new interconnection network called X-torus (cross-torus), which improves the performance of the torus topology. The suggested network has attractive properties such as smaller diameter, smaller average distance, larger bisection width and better scalability than the torus and its variation.

2 X-Torus Topology

2.1 Definition

As is shown in Fig. 1, X-torus network is a two-dimension topology. The topology can be placed in an X-Y frame and each node is labeled as (a,b). For notational simplicity, let $[s]_t = s \bmod t$ for all $s \in I$ and $t \in I^+$, where I is the set of integers and I^+ is the set of positive integers.

Definition 1. A $k_x \times k_y$ X-torus network is a graph $G_x = (N_x, C_x)$, defined as:

$$N_x = \{ (a,b) \mid 0 \leq a \leq k_x, 0 \leq b \leq k_y \}$$

$$C_x = \{ \langle (u_a, u_b), (v_a, v_b) \rangle \mid ((u_a = v_a \cap u_b = [v_b \pm 1]_{k_y}) \cup (u_a = [v_a + \lfloor k_x / 2 \rfloor]_{k_x} \cap u_b = [v_b + \lfloor k_y / 2 \rfloor]_{k_y}))$$

$$\cap ((u_a, u_b), (v_a, v_b) \in N_x) \}$$

where $k_x \geq 2, k_y \geq 2, (u_a, u_b)$ and (v_a, v_b) are the coordinates of the nodes \mathbf{u} and \mathbf{v} respectively.

We focus our attention on the case of $k_x = k_y = k$ in this paper. Results for the case of $k_x \neq k_y$ are omitted due to space limit and can be found in [9]. From Fig.1, we can see that X-torus use links to connect the node (a,b) and the node $([a + \lfloor k / 2 \rfloor]_k, [b + \lfloor k / 2 \rfloor]_k)$. This leads to better performance as will be seen in the next section. The degree of X-torus network is dependent on the parity of k. If k is even, the degree is 5 and if k is odd, the degree is 6. When k is even, the link that connects the node (a, b) and the node $([a + \lfloor k / 2 \rfloor]_k, [b + \lfloor k / 2 \rfloor]_k)$ is the same with the link that connects the node $([a + \lfloor k / 2 \rfloor]_k, [b + \lfloor k / 2 \rfloor]_k)$ and the node $([a + \lfloor k / 2 \rfloor]_k + \lfloor k / 2 \rfloor]_k, [b + \lfloor k / 2 \rfloor]_k + \lfloor k / 2 \rfloor]_k)$. Therefore, the degree for even k is smaller than that for odd k.

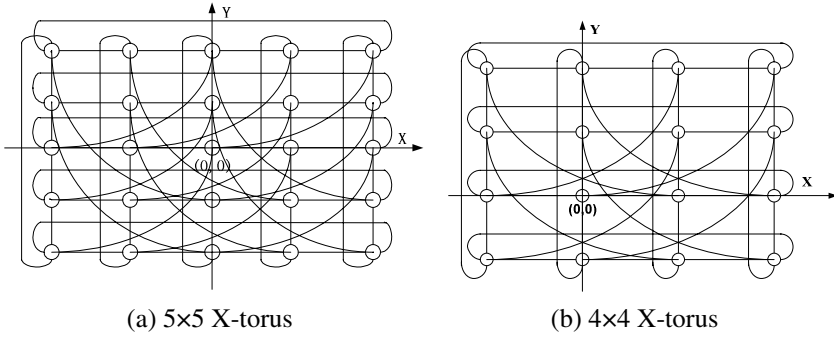


Fig. 1. Illustration of X-torus topology

2.2 Properties

A topology is evaluated in terms of a number of parameters. In this paper, we are interested in symmetry, diameter, degree, average distance, scalability and bisection width. Let D and d be the diameter and the average distance of a $k \times k$ X-torus respectively.

Theorem 1. The diameter of a $k \times k$ X-torus is $\lfloor k/2 \rfloor + 1$ if k is odd and $\lfloor k/2 \rfloor$ if k is even.

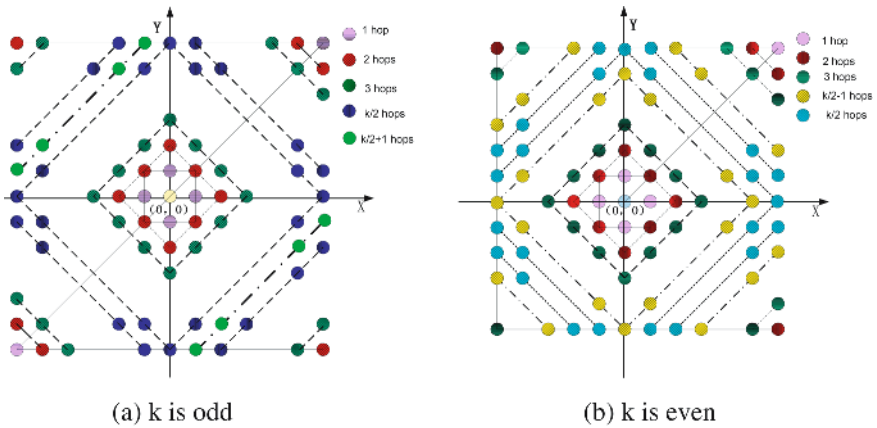


Fig. 2. Illustration of the distance of nodes from the source

Proof: Case 1: k is odd;

A $k \times k$ X-torus is shown in Fig. 2 with edges omitted for clarity. In the figure, the nodes use different labels to show their different distance from the source node $(0, 0)$. Nodes of the same distance from the source are connected with dashed lines and use the same labels. For example, nodes that are one hop away from the source node use purple color with horizontal lines inside. It is obvious that the grass-green nodes with

no lines inside are the furthest from the source. It takes $\lfloor k/2 \rfloor + 1$ hops to reach them. Hence, the diameter is $\lfloor k/2 \rfloor + 1$.

Case 2: k is even;

The diameter in this case can be derived in a similar way with that in Case 1. As is shown in Fig. 2 (b), it is obvious that the blue nodes with diagonal lines inside are the furthest from the source. It takes $\lfloor k/2 \rfloor$ hops to reach them. Hence, the diameter is $\lfloor k/2 \rfloor$. □

Before we present the average distance of X-torus, we introduce Lemma 1 below.

Lemma 1. For a $k \times k$ X-torus, let $s(i)$ be the number of the nodes that is i hops away from the source node $(0,0)$, it can be calculated by the following equations:

$$(a) \text{ when } k \text{ is odd } s(i) = \begin{cases} 8i - 2 & 1 \leq i < D \\ 2D - 2 & i = D \end{cases} \quad (1)$$

$$(b) \text{ when } k \text{ is even } s(i) = \begin{cases} 5 & i = 1 \\ 8i - 4 & 2 \leq i < D \\ 4k - 6 & i = D \end{cases} \quad (2)$$

Proof: Case 1: k is odd:

As is shown in Fig.2 (a), the node $(0, 0)$ has been chosen as the source. Other nodes use different labels to show their distance from the source. It is obvious that $s(1)=6$ because the source has six neighbors.

For $1 < i < D$, from the figure, we can see in Quadrant I there are $i+(i+1)=2i+1$ nodes that are i hops away from the source. Similarly, there are $(i-1)+(i+1)=2i$, $2i+1$ and $2i$ nodes in Quadrant II, III and IV respectively. Hence, the number of nodes that are i hops away from the source is the sum of these four parts minus 4 (because 4 nodes are calculated twice), i.e.

$$s(i) = 2i + 2i + (2i+1) + (2i+1) - 4 = 8i - 2$$

For $i=D$, it is obvious that $s(i) = 2 \lfloor k/2 \rfloor = 2D - 2$.

$$\text{Thus, } s(i) = \begin{cases} 8i - 2 & 1 \leq i < D \\ 2D - 2 & i = D \end{cases}$$

Case 2: k is even:

From Fig.2 (b), it can be easily seen that $s(1)=5$ because the source has five neighbors in this case.

For $1 < i < D$, in Quadrant I there are $i+(i+1)=2i+1$ nodes that are i hops away from the source. Similarly, there are $(i-1)+(i+1)=2i$, $(i-2)+(i+1)=2i-1$ and $2i$ nodes in Quadrant II, III and IV respectively. Hence, $s(i)$ is the sum of these four parts minus 4 (because 4 nodes are calculated twice), i.e.

$$s(i) = (2i+1) + 2i + (2i-1) + 2i - 4 = 8i - 4$$

For $i=D$, it is obvious that in Quadrant I, $s(i) = D + (D+1) = 2D + 1$. Similarly, there are $(D-1) + D = 2D - 1$, $(D-2) + (D-1) = 2D - 3$ and $2D - 1$ nodes in Quadrant II, III and IV

respectively. Hence, $s(i)$ is the sum of these four parts minus 2 (because 2 nodes are calculated twice), i.e.

$$s(i) = (2D+1) + (2D-1) + (2D-3) + (2D-1) - 2 = 8D - 6 = 4k - 6$$

$$\text{Thus, } s(i) = \begin{cases} 5 & i = 1 \\ 8i - 4 & 2 \leq i < D \\ 4k - 6 & i = D \end{cases} \quad \square$$

Theorem 2. The average distance of a $k \times k$ X-torus is $k/3 + 1/4$ when k is odd and $k/3 + 1/2(k^2 - 1) + 1/2 - 1/(k + 1)$.

Proof: Case1: k is odd;

From the definition of the average distance, we can obtain

$$d = \sum_{i=1}^D \frac{s(i) \times i}{N - 1} \tag{3}$$

Substituting equation (1) into equation (3) yields,

$$d = \sum_{i=1}^{D-1} \frac{(8i - 2) \times i}{N - 1} + \frac{D \times (2D - 2)}{N - 1} = \frac{1}{k^2 - 1} \sum_{i=1}^{\lfloor \frac{k}{2} \rfloor} (8i - 2) \times i + \frac{(\lfloor \frac{k}{2} \rfloor + 1) \times (2 \lfloor \frac{k}{2} \rfloor)}{k^2 - 1} = \frac{1}{3}k + \frac{1}{4}$$

Case 2: k is even;

$$d = \sum_{i=1}^D \frac{s(i) \times i}{N - 1} = \frac{1}{k^2 - 1} \sum_{i=2}^{\frac{k}{2}-1} (8i - 4) \times i + \frac{5}{k^2 - 1} + \frac{\frac{k}{2}(4k - 6)}{k^2 - 1} = \frac{1}{3}k + \frac{1}{2(k^2 - 1)} + \frac{1}{2} - \frac{1}{k + 1}$$

2.3 Routing Algorithm

Since X-torus topology is based on the torus topology, all the routing algorithms designed for torus topology can be used in X-torus. However, these algorithms cannot make use of the cross links. Hence, they are not the shortest path routing algorithms for X-torus. In this section, we propose a simple shortest path routing algorithm.

Definition 2. Z direction is defined as the rotation of X axis anticlockwise by 45° , as is shown in Fig. 3. The positive direction of Z (Z+) is defined as the direction from the node $(0, 0)$ to the node $(\lfloor k_x / 2 \rfloor, \lfloor k_y / 2 \rfloor)$. The negative direction of Z (Z-) is defined as from the node $(0, 0)$ to the node $(-\lfloor k_x / 2 \rfloor, -\lfloor k_y / 2 \rfloor)$.

Without loss of generality, we choose the node $(0, 0)$ as the source node and the node $(\Delta x, \Delta y)$ as the destination node. Fig. 3 plots a $k \times k$ X-torus for k is odd with edges omitted for clarity. From it, we can easily see that if the node $(\Delta x, \Delta y)$ is in the area A, the message can choose either X or Y direction. If the node $(\Delta x, \Delta y)$ is in the area B or D, the message can choose Z+ or Z- direction respectively. If the node $(\Delta x, \Delta y)$ is in the area C or E, the message can choose either Z+ or Z- direction

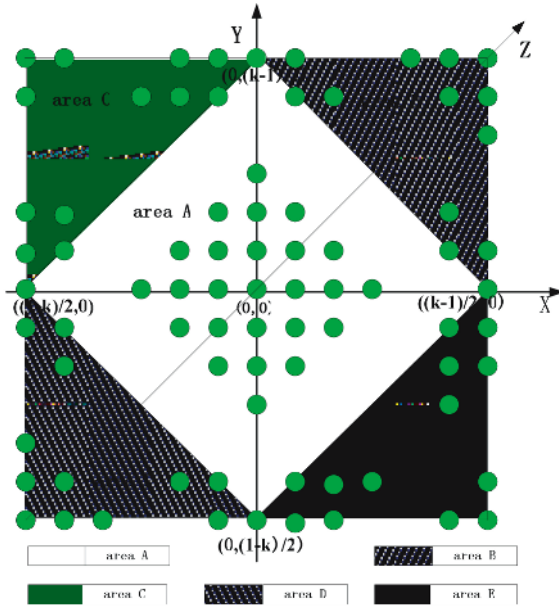


Fig. 3. Illustration of five parts divided by the routing algorithm

randomly. Similar results can be obtained when k is even. Since for each hop, the message is closer to the destination, the algorithm is optimal in terms of the length of a path. A formal shortest path routing algorithm is given as follows.

ShortestPathAlgorithm

// D_Forward: the direction to forward the current message;

Begin

switch (k)

case I: k is odd

{

if ($x = \Delta y = 0$)

send the message to the local node and EXIT;

if ($|\Delta x| + |\Delta y| \leq (k - 1) / 2$) // ($\Delta x, \Delta y$) is in the area A;

D_Forward=Select ($\Delta x, \Delta y$);

else if ($|\Delta x| > 0$ and $|\Delta y| > 0$) // ($\Delta x, \Delta y$) is in the area B;

D_Forward=Z+;

else if ($|\Delta x| < 0$ and $|\Delta y| < 0$) // ($\Delta x, \Delta y$) is in the area D;

D_Forward=Z-;

else // ($\Delta x, \Delta y$) is in the area C or E;

D_Forward=Z+ or Z-; //choose either Z+ or Z-;

}

```

case II: k is even
{
    if (x = Δy = 0)
        send the message to the local node and EXIT;
    if (|Δx| + |Δy| ≤ k / 2)
        D_Forward=Select (Δx, Δy);
    else
        D_Forward=Z+;
}
EXIT
Select(d1,d2)// choose one direction between d1 and d2;
{
    r=random(0,1); //choose 0 or 1 with equal probability for r;
    if (r=0)
        {
            if (d1>0) return X+;
            else return X-;
        }
    else
        {
            if d2>0 return Y+;
            else return Y-;
        }
}

```

3 Comparisons with Some Popular Topologies

In this section we compare X-torus with some popular topologies such as 2D mesh, 2D torus and E-torus. Table 1 summarizes the degree, diameter, average distance and bisection width of these topologies, each with $k \times k = N$ nodes. In the following, the topologies are compared in terms of symmetry, path diversity, scalability and so on.

Table 1. Comparisons of the popular topologies

Parameter Topology	Degree	Diameter	Average distance	Bisection width
2D Mesh	2 or 3 or 4	2k	k	k
2D Torus	4	k	k/2	2k
E-Torus	8	$\lfloor k/2 \rfloor$	$\approx k/3 + 1/2$	6k
X-Torus (k is odd)	6	$\lfloor k/2 \rfloor + 1$	$k/3 + 1/4$	$k^2 + k$
X-Torus (k is even)	5	$\lfloor k/2 \rfloor$	$\approx k/3 + 1/2$	$k^2/2 + 2k$

Symmetry

A graph is said to be regular if all the nodes in the graph have the same degree, and homogeneous if all the nodes in that graph are topologically identical [10]. Clearly homogeneity implies regularity but the reverse does not always hold. X-torus network is homogeneous and regular. Complete regularity of X-torus network can lead to a better performance.

Path Diversity

Interconnection networks should have path diversity to provide load balance and fault tolerance [11]. The degree of 2D mesh and 2D torus is less than that of the other two topologies, so the lower connectivity will naturally lower the degree of fault tolerance. X-torus network has a fixed degree, which is irrespective of the size.

Average Distance

As Table 1 shows, the average distance of X-torus is very small, because it makes use of the crossing links to reach the distant nodes with fewer hops. When compared with 2D torus, X-torus has half of the average distance. E-torus has a similar average distance with X-torus. But it is an 8-degree topology, which requires $4k^2$ links for a $k \times k$ network. However, $k \times k$ X-torus only requires $3k^2$ links and achieves similar average distance.

Scalability

Interconnection networks should scale economically and incrementally. Recently, much of the community has moved on to lower-dimensional topologies [7], which can offer better scalability than higher dimensional topologies. In an X-torus, the smallest extension unit is a row or a column, i.e. a one dimensional sub graph. In the high dimensional torus, for example, 3D torus, the smallest extension unit is a plane, i.e. a two dimensional sub graph. Therefore, the scaling complexity of X-torus is $O(n)$ compared to $O(n^2)$ which is higher. Hence, the X-torus network is superior to the high dimensional torus in aspect of scalability.

Bisection Width

Bisection width is defined as the minimum number of channels that must be removed to partition the network into two equal parts. For example, when a 4×4 2D torus expands to an 8×8 network, the bisection width doubles, but the messages that cross the bisection plane are increased by 4 times (because the number of nodes is increased by 4 times). Thus, the network performance will degrade after expansions. This problem doesn't exist in X-torus because it has $O(k^2)$ bisection width. The bisection links are no longer the bottleneck when the network scales.

Network Cost

The network cost is defined as $\text{degree} \times \text{diameter}$ [12,13,14]. From Table 1, the cost of X-torus is the smallest among the four topologies. The gap will become more apparent as the number of the nodes increases. Thus X-torus is superior to the other topologies with the same number of nodes in terms of the network cost.

In general, no single topology can provide every desired feature. Considering symmetry, path diversity, average distance, scalability and network cost, which are the basic requirements for the interconnection networks, X-torus network is an attractive candidate topology.

4 Conclusions and Future Work

In this paper, we proposed a new interconnection network, X-torus network. It has many advantages such as symmetry, easy scalability. The topological properties of the X-torus network indicate that it is a more cost-effective approach for interconnection networks, compared to the existing topologies. We also present a simple self-routing algorithm in X-torus network, which is optimal in terms of path length.

A lot of issues concerning X-torus network require further research. Some of them are: broadcasting, multicast routing and fault tolerant routing. Broadcasting and multicasting are fundamental collective communication operations. What's more, as the number of nodes in an X-torus network increases, the chance of failure also increases. Hence, it is essential to design a fault-tolerant algorithm that can route packets in the presence of faulty components.

Acknowledgment

This work was supported by the National Science Foundation of China under Grant No.60532060.

References

1. J. Duato, S. Yalamanchili and L. Ni., *Interconnection Networks, an Engineering Approach*, Morgan-Kaufmann Press, 2002
2. Ed Anderson, J. Brooks, C. Grassl and S. Scott., Performance of the Cray T3E multiprocessor, In *Supercomputing 97*, San Jose, California, pp 1-17, November 1997.
3. Fujitsu AP3000, white paper, On the Web at <http://jp.fujitsu.com/>, 2004
4. C. L. Seitz, The architecture and programming of the Ametek Series 2010 multicomputer, Proc. of the 3rd Conference on Hypercube Concurrent Computers and Applications, Vol. 1, Jan. 1988, 33-36.
5. L. Lillevik, The Touchstone 30 gigaflop DELTA prototype, Proc. of the 6th Distributed Memory Computing Conference, 1991, 671-677.
6. W. J. Dally, Scalable Switching Fabrics for Internet Routers, White paper, Avici Systems Inc. 2001
7. Y. Li, S. Peng, W. Chu, Efficient Communication in Metacube: A New Interconnection Network. *ISPAN 2002*: pp165-172
8. MasPar MP-2, On the Web at <http://www.top500.org>, 2004.
9. H.X. Gu and Q.M. Xie, Analysis of the X-torus Networks, BNRD at Telecommunication Engineering Department Technical Report, BNRD-04-068, Sep., 2004
10. M.-S. Chen, K. G. Shin, and D. D. Kandlur, Addressing, routing and broadcasting in hexagonal mesh multiprocessors, *IEEE Trans. on Computer*, vol. 39, no. 1, pp. 10-18, Jan 1990.
11. W. Dally and B. Towles, *Principles and Practices of Interconnection Networks*, Morgan-Kaufmann Press, 2004
12. H. Lee et al, Hyper-Star Graph: A New Interconnection Network Improving the Network Cost of the Hypercube, *EurAsia-ICT 2002*, LNCS 2510, pp. 858-865, 2002.
13. Efe, K., A Variation on the Hypercube with Lower Diameter. *IEEE Trans. Computer*, Vol. 40, No. 11, (1991) 1312-1316
14. Parhami, B., Kwai, D.-M., A Unified Formulation of Honeycomb and Diamond Networks. *IEEE Trans. Parallel and Distributed Systems*, Vol. 12, No. 1, Jan. (2001) 74-80

Feedback Vertex Sets in Rotator Graphs

Chiun-Chieh Hsu¹, Hon-Ren Lin², Hsi-Cheng Chang³, and Kung-Kuei Lin¹

¹ Department of Information Management,
National Taiwan University of Science and Technology,
Taipei, Taiwan, ROC

² Department of Information Management, National Taipei College of Business,
Taipei, Taiwan, ROC

³ Department of Information Management, Hwa-Shia Institute of Technology,
Taipei, Taiwan, ROC

Abstract. This paper provides an algorithm for finding feedback vertex set in rotator graphs. Feedback vertex set is a subset of a graph whose removal causes an acyclic graph and is developed in various topologies of interconnected networks. In 1992, Corbett pioneered rotator graphs, whose interesting topological structures attract many researchers to publish relative papers in recent years. In this paper, we first develops feedback vertex set algorithm for rotator graphs. Our algorithm utilizes the technique of dynamic programming and generates a feedback vertex set of size $n!/3$ for a rotator graph of scale n , which contains $n!$ nodes. The generated set size is proved to be minimum. Finding a minimum feedback vertex set is a NP-hard problem for general graphs. The time complexity of our algorithm, which finds a minimum feedback vertex set for a rotator graph of scale n , is proved to be $O(n^{n-3})$.

1 Introduction

Rotator graph, which is first proposed in 1992[1], is a family of Cayley graph and has rich topological properties, such as symmetric structure, recursive construction, low diameter, unique shortest path routing, and so on. A rotator graph of scale n , or denoted as an n -rotator, contains $n!$ nodes in which every node has a unique permutation of $123 \dots n$. The generation function g_i inserts first symbol of a permutation to the i th position, where $1 < i \leq n$. A 3-rotator is shown in Fig.1. The bold lines are bi-directional edges. A feedback vertex set, or called FVS, is a vertex subset of a graph whose deletion induces the remaining graph acyclic. The FVS are applied in many applications, such as mutual exclusion [2], data security[3], scheduling[4], optical networks[5][6], and so on. A minimum FVS, or denoted as MFVS, is a FVS that contains smallest number of vertices. Published papers[7][8] proved that finding MFVS is a NP-hard problem in general and bipartite graphs. In recent years, FVS algorithms are also developed in mesh and butterfly[9][10], hypercube[11], star graph[12], and shuffle-based interconnection networks[13]. We first proposed a FVS algorithm in rotator graphs in this paper. The dynamic programming techniques are applied in our algorithm. The main idea is that we utilize the FVS of a smaller scale graph to build that

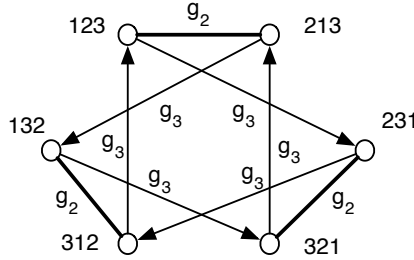


Fig. 1. A 3-rotator

of a larger one. The size of the feedback vertex set generated by our algorithm is proved to be minimum.

2 Definitions

Used lemmas and definitions are introduced in this section. A rotator graph of scale n is denoted as an n -rotator in which every node has a unique permutation of $123 \dots n$. The outgoing edges of one node can be represented as generation functions, g_2, g_3, \dots , and g_n . Function g_i inserts first symbol of a permutation to the i th position to form a resultant node. Terms of node, vertex, and permutation are interchangeable in this paper, so are edge and link.

Definition 2.1. Let u be a node in a rotator graph. Node u^*g_i denotes the resultant node of applying g_i to node u .

For example, $12345^*g_3=23145$.

Definition 2.2. Let $V_{i,j}$ of a rotator graph be the set of all permutations whose i th position is j .

For instance, $V_{2,1} = \{2134, 2143, 3124, 3142, 4123, 4132\}$ for a 4-rotator.

Definition 2.3. Let $FVS(n)$ denote a feedback vertex set of an n -rotator.

Although applying g_2 twice to one node makes a routing from itself to its neighbor and back, it does not be considered as a cycle in our discussion. As illustrated in Fig.2, a 3-rotator contains two node disjoint cycles, $123 \rightarrow 231 \rightarrow 312 \rightarrow 123$ and $213 \rightarrow 132 \rightarrow 321 \rightarrow 213$. If we remove node 123 and 132, the remaining graph will contain no cycle. Thus 123, 132 is a FVS of a 3-rotator. In addition, $g_3g_3g_3$ is the smallest cycle in a rotator graph and an n -rotator contains $n!/3$ disjoint cycles of length 3.

3 Algorithm

The FVS algorithm illustrated in this section applies the techniques of dynamic programming. That is, the FVS of an n -rotator, denoted as $FVS(n)$, is

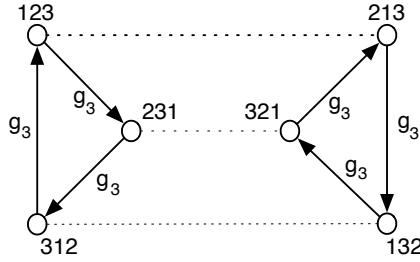


Fig. 2. Two node disjoint cycles in a 3-rotator

obtained by using that of a $(n-1)$ -rotator. $FVS(3)=\{123, 132\}$ is easily observed. The method of finding $FVS(4)$ is described below: Nodes in a 4-rotator can be categorized into $V_{1,1}$, $V_{2,1}$, $V_{3,1}$, and $V_{4,1}$ and each category consists of 6 nodes. $FVS(4)$ is initialized an empty set. We first add $V_{1,1}$ to $FVS(4)$. The remaining graph of removing $V_{1,1}$ from a 4-rotator is denoted as $G(4\text{-rotator} - V_{1,1})$. Indeed, $G(4\text{-rotator} - V_{1,1})$ does not contain any cycle that includes any node in $V_{2,1}$ or $V_{3,1}$. The reason is that any cycle contains at least one g_k , where $k \geq 3$, and the generation g_k will left shift symbol 1 of the permutations in $V_{2,1}$ or $V_{3,1}$. If cycle exists, symbol 1 must be shifted to the first position eventually and then rotated to a correct position. Because $V_{1,1}$ had already been removed, symbol 1 can not be left shifted to the first position. Thus the cycle does not exist. Therefore, $G(4\text{-rotator} - V_{1,1})$ does not include any cycle that contains node in $V_{2,1}$ or $V_{3,1}$. Hence, nodes in $V_{1,1}$ are the only candidates to add to $FVS(4)$. Nodes in $V_{1,1}$ are the form of $***1$, where $***$ represents any legal permutation. Hence, finding cycles in $G(4\text{-rotator} - V_{1,1})$ can be viewed as finding cycles in a sub 3-rotator of $V_{4,1}$. Because rotator graphs are node symmetric and the feedback vertex set of a 3-rotator, 123, 132, is already known, the FVS of the sub 3-rotator $V_{4,1}$ can be easily solved by a symbol transformation. For example, $FVS(3)=\{123, 132\}$ implies that 1234, 1324 is a FVS of $V_{4,1}$. By exchanging symbol 1 and 4, we obtain that 4231, 4321 is a FVS of $V_{4,1}$. Therefore, a FVS of a 4-rotator is the union of $V_{1,1}$ and $4231, 4321 = \{1234, 1243, 1324, 1342, 1423, 1432, 4231, 4321\}$.

Lemma 3-1. For an n -rotator, $G(n\text{-rotator} - V_{1,1})$ does not contain any cycle that includes any node in $V_{2,1}$ or $V_{3,1}$.

Proof. First, every node in a cycle has a predecessor and a successor node. Because $V_{1,1}$ has been removed, nodes in $V_{2,1}$ do not have any successor node. Thus $G(n\text{-rotator} - V_{1,1})$ contains no cycle that includes any node in $V_{2,1}$. Second, every cycle contains at least one g_3 function, which left shift symbol 1 of nodes in $V_{3,1}$ and connects to nodes in $V_{2,1}$. Because $V_{2,1}$ do not have any successor node in $G(n\text{-rotator} - V_{1,1})$, there is no cycle that includes any node in $V_{3,1}$. This lemma is verified. \square

Lemma 3-2. Let C be a cycle in $G(n\text{-rotator} - V_{1,1})$. Every node in C belongs to the same vertex set $V_{i,1}$, where $4 \leq i \leq n$.

Proof. Suppose cycle C contains nodes S_1 and S_2 , where $S_1 \in V_{i,1}$, $S_2 \in V_{j,1}$, and $j \neq i$. First consider the case that $i > j$. The path from S_2 to S_1 must pass at least one node $\in V_{1,1}$. Because $G(n\text{-rotator} - V_{1,1})$ does not contain any node $\in V_{1,1}$, the path from S_2 to S_1 does not exist. Second, if $i < j$, the path from S_1 to S_2 does not exist with the same reason. This lemma is proved. \square

By lemma 3-2, in the remaining graph of removing vertex set $V_{1,1}$ from a rotator graph, every node in a cycle belong to the same sub rotator graph $V_{i,1}$, where $i > 3$. That is, in $G(n\text{-rotator} - V_{1,1})$, nodes in a cycle have a property that symbol 1 in the same position. In order to indicate node properties, we divide a permutation into two parts, head sequence and tail sequence. Suppose that symbol 1 of permutation S is in the i th position. Head sequence of S is the first $i - 1$ symbols and tail is the i th to the last symbols. For example, for node 43125, head sequence is 43 and tail sequence is 125. In addition, we define length of head/tail sequence is the number of symbols in head/tail sequence. If symbol 1 is in the first position for a permutation, of course, this node has no head sequence. A property can be observed: An n -rotator contains one sub $(n - 1)$ -rotator graph in which every node has tail length is 1. In addition, n -rotator also contains $n - 1$ node-disjoint sub $(n - 2)$ -rotator in which every node has tail length 2. For example, in a 5-rotator graph there is one sub 4-rotator with tail length 1. Nodes in the sub 4-rotator are of the form ****1, where * represents any legal symbol. In addition, this 5-rotator also has four sub 3-rotator graphs with tail length 2. These four sub 3-rotator are ***12, ***13, ***14, and ***15. A general expression of the property is shown in lemma 3-3.

Lemma 3-3. An n -rotator contains P_{n-k-1}^{n-1} disjoint sub k -rotator graph in which every node has tail length $n - k$, where $k \geq 3$.

Proof. Every node in an n -rotator graph has permutation length n . Nodes in a sub k -rotator have the same tail sequence whose length is $n - k$. Because the first symbol of the tail sequence is 1, the number of distinct k -rotator is therefore $(n - 1)(n - 2) \dots (k + 1) = P_{n-k-1}^{n-1}$. In addition, because nodes in different sub rotator graphs have different tail sequences, these sub rotators are node disjoint. The lemma is verified. \square

The steps of finding a FVS in an n -rotator is described in the following: First, we add the set $V_{1,1}$ of an n -rotator to $FVS(n)$. Second, by lemma 3-3, the remaining graph can be divided into a number of isolated sub rotator graphs. The feedback vertex set of the whole graph can be obtained by joining the feedback vertex set of these distinct sub graphs. Since a rotator graph is node symmetric, the feedback vertex set of a rotator graph can be easily transferred to that of identical size of sub rotator graphs. For example, a feedback vertex set of a 3-rotator is 123, 132. Obviously, 1234, 1324 is the feedback vertex set of sub 3-rotator graph with the form ***4. The feedback vertex of sub rotator

graph $***1$, $***2$, and $***3$ is obtained by exchanging symbol $(1,4)$, $(2,4)$, and $(3,4)$ of node 1234 and 1324 , respectively. Thus the feedback vertex set of $***1$, $***2$, and $***3$ are 4231 , 4321 , 1432 , 1342 , and 1243 , 1423 , respectively.

We illustrate the steps of acquiring the feedback vertex set of a 5-rotator graph. In the beginning, $FVS(3)=\{123, 132\}$ and $FVS(4)=\{2134, 3124, 2143, 4132, 4132, 3142, 2341, 2431\}$ is already known. This assumption is reasonable because $FVS(4)$ is only a joint of 4 isolated sub 3-rotator graph and $FVS(3)$ is quite simple to be observed. We initialize $FVS(5) = V_{1,1} = \{12345, 12354, 12435, 12453, 12534, 12543, 13245, 13254, 13425, 13452, 13524, 13542, 14235, 14253, 14325, 14352, 14523, 14532, 15234, 15243, 15324, 15342, 15423, 15432\}$. By lemma 3-3, a 5-rotator contains one 4-rotator graph with tail length 1 and the sub 4-rotator is of the form $****1$. We use $FVS(4)$ to obtain the FVS of the sub 4-rotator $****1$. The FVS of the sub 4-rotator $\{25341, 35241, 25431, 45321, 45321, 35421, 23451, 24351\}$ is added to $FVS(5)$. In addition, a 5-rotator also contains four isolated sub 3-rotator graph with tail length 2, which are $***12$, $***13$, $***14$, and $***15$. Each of these 3-rotator contains a FVS of size 2. These FVS of these sub 3-rotator are easily obtains from $FVS(3)$, $\{123, 132\}$. The FVS of $***12$, $***13$, $***14$, and $***15$ are $\{34512, 35412\}$, $\{24513, 25413\}$, $\{23514, 25314\}$ and $\{23415, 24315\}$, respectively. These four sets are also add to $FVS(5)$. In summary, $FVS(5)$ contains $24+8+2*4=40$ elements.

The algorithm of finding feedback vertex set of a rotator graph is given below:

Algorithm 3-1. Feedback vertex set finding in rotator graphs.

Input: the scale of rotator graph, n .

Output: the feedback vertex set of an n -rotator, $FVS(n)$.

Steps:

1. Initialize $FVS(n) = V_{1,1}$.

2. for $k = 3$ to $n - 1$ do

Add FVS of P_{n-k-1}^{n-1} units of sub k -rotator graph to $FVS(n)$.

loop

Lemma 3-4. The output $FVS(n)$ of Algorithm 3-1 is correct.

Proof. The first step of Algorithm 3-1 adds $V_{1,1}$ to $FVS(n)$. By lemma 3-2, symbol 1 of every node in a cycle in $G(n\text{-rotator} - V_{1,1})$ must be in the same position. In other words, if symbol 1 is in the i th position, the generations in the cycle can only be g_2, g_3, \dots , and g_{i-1} . This cycle is therefore being limited in a sub $(i-1)$ -rotator. Our algorithm joins feedback vertex sets of these sub rotators to acquire the feedback vertex set of the whole graph. Step 2 adds all feedback vertex sets of sub graphs whose node has tail sequence length $n - 3, n - 4, \dots$, and 1 to the $FVS(n)$. All sub rotators are considered in our algorithm, the aggregation of the feedback vertex set is the feedback vertex set of the whole graph. □

Lemma 3-5. The size of $FVS(n)$ generated by Algorithm 3-1 is $n!/3$.

Proof. The number of nodes in $FVS(n)$ is denoted as $|FVS(n)|$. We prove this theorem by induction.

1. Because $FVS(3)=\{123, 132\}$, $|FVS(n)| =n!/3$ holds for $n = 3$.
2. We assume that $|FVS(n)|=n!/3$ is true when $n = k$.
3. When $n = k + 1$,

$$\begin{aligned}
 |FVS(n)| &= k! + P_0^k * |FVS(k)| + P_1^{k-1} * |FVS(k-1)| + \dots + P_{k-3}^k * |FVS(3)| \\
 &= k! + P_0^k * k!/3 + P_1^{k-1} * (k-1)!/3 + \dots + P_{k-3}^k * 3!/3 \\
 &= k! + k!/3 * (k-2) \\
 &= (k+1)*k!/3 \\
 &= (k+1)!/3 \\
 &= n!/3. \text{ This lemma is proved.} \quad \square
 \end{aligned}$$

Lemma 3-6. The size of $FVS(n)$ generated by Algorithm 3-1 is minimum.

Proof. An n -rotator contains $n!/3$ disjoint cycles of size 3 and these cycles are formed $g_3g_3g_3$. Therefore, to eliminate all possible cycles need to remove at least $n!/3$ nodes from an n -rotator. By Theorem 3-2, the size of $FVS(n)$ generated by Algorithm 3-1 is $n!/3$. Thus, it is minimum. \square

Lemma 3-7. The time complexity of Algorithm 3-1 is $O(n^{n-3})$, where n is the size of rotator graph.

Proof. Let $t(k)$ be the time complexity of finding $FVS(k)$ by using Algorithm 3-1. We assume $t(3) = 1$ because $FVS(3)$ can be easily observed. The time complexity $t(n)$ is expressed follows:

$$t(n) = P_0^{n-1} * t(n - 1) + P_1^{n-2} * t(n - 2) + \dots + P_{n-4}^{n-1} * t(3). \tag{1}$$

$$t(n + 1) = P_0^n * t(n) + P_1^{n-1} * t(n - 1) + \dots + P_{n-3}^n * t(3). \tag{2}$$

From (1) and (2):

$$\frac{t(n + 1)}{n} = \frac{t(n)}{n} + P_0^{n-1} * t(n - 1) + P_1^{n-2} * t(n - 2) + \dots + P_{n-4}^{n-1} * t(3). \tag{3}$$

From (2) and (3):

$$\frac{t(n + 1)}{n} = \frac{t(n)}{n} + t(n) \tag{4}$$

From (4): $t(n) = \prod_{k=4}^n = O(n^{n-3})$, $n \geq 3$. \square

4 Conclusions

This paper provides an algorithm for finding minimum feedback vertex sets for rotator graphs. Finding minimum Feedback vertex set is a NP-hard problem for general graph. For an n -rotator, our algorithm generates a feedback vertex set of size $n!/3$ in $O(n^{n-3})$. The size of the set is proved to be minimum.

Acknowledgement

This work was partially supported by the National Science Council of the Republic of China under Grant NSC94-2213-E-011-053.

References

1. Peter F. Corbett, Rotator Graphs: An Efficient Topology for Point-to-Point Multiprocessor Networks, IEEE Transactions on Parallel and Distributed System, Vol. 3, No. 5. (1995) 622–626
2. C. Chen, D.P. Agrawal and J.r. Burke, dBCube: A New Class of Hierarchical Multiprocessor Interconnection Networks with Area Efficient Layout, IEEE Trans. on Parallel and Distributed Systems, Vol. 4. (1993) 1332–1344
3. Caragiannis, C. Kaklamanis, P. Kanellopoulos: New Bounds on The Size of The Feedback Vertex Set on Meshes and Butterflies, Information Processing Letters, Vol. 83, No. 5. (2002) 275–280
4. M.M. Flood: Exact and Heuristic Algorithms for The Weighted Feedback Arc Set Problem: A special case of the skew-symmetric quadratic assignment problem, Networks, Vol. 20. (1990) 1–23
5. R. Floyd: Assigning Meaning to Programs, In Proceedings of Symposium on Applied Mathematics. (1967) 19–32
6. R. Focardi, F.L. Luccio, D. Peleg: Feedback Vertex Set in Hypercubes, Information Processing Letters, Vol. 76, No. 1-2. (2000) 1–5
7. M.R. Garey, D.S. Johnson: Computers and Intractability, Freeman, San Francisco, CA. (1979)
8. M. Yannakakis, Node-Deletion Problem on Bipartite Graphs, SIAM Journal on Computing, Vol. 10. (1981) 310–327
9. F.L. Luccio: Exact Minimum Feedback Vertex Set in Meshes and Butterflies, Information Processing Letters, Vol. 66, No. 2. (1998) 59–64
10. I. Caragiannis, C. Kaklamanis, P. Kanellopoulos: New Bounds on The Size of The Feedback Vertex Set on Meshes and Butterflies, Information Processing Letters, Vol. 83, No. 5. (2002) 275–280
11. R. Focardi, F.L. Luccio, D. Peleg: Feedback Vertex Set in Hypercubes, Information Processing Letters, Vol. 76, No. 1-2. (2000) 1–5
12. F.H. Wang, Y.L. Wang, J.M. Chang: Feedback Vertex Sets in Star Graphs, Information Processing Letters, Vol. 89, No. 4. (2004) 203–208
13. R. Kralovic, P. Ruzicka: Minimum Feedback Vertex Sets in Shuffle-based Interconnection Networks, Information Processing Letters, Vol. 86, No. 4. (2003) 191–196

Efficient Longest Common Subsequence Computation Using Bulk-Synchronous Parallelism

Peter Krusche and Alexander Tiskin

Department of Computer Science,
University of Warwick,
Coventry, CV47AL, United Kingdom
{peter, tiskin}@dcs.warwick.ac.uk

Abstract. This paper presents performance results for parallel algorithms that compute the longest common subsequence of two strings. This algorithm is a representative of a class of algorithms that compute string to string distances and has computational complexity $O(n^2)$. The parallel algorithm uses a variable grid size, runs in $O(p)$ supersteps (synchronization phases) and has linear communication costs. We study this algorithm in BSP context, give runtime estimations and compare the predictions to experimental values measured on three different parallel architectures, using different BSP programming libraries and an efficient implementation for sequential computation. We find that using the BSP model and the appropriate optimized BSP library improves the performance over plain MPI, and that scalability can be improved by using a tuned grid size parameter.

1 Introduction

In this paper, we discuss different performance results obtained for computing the length of the longest common subsequence (LLCS) of two strings, using the BSP model and optimized communication libraries. This is a standard problem for parallel dynamic programming. Hence, the results presented here can serve as a reference for the ability of different approaches to BSP programming to improve the performance on such problems (e.g. the edit distance problem and other types of string comparison).

Computing the LLCS sequentially is a well-studied problem. It can be solved using a simple dynamic programming algorithm [1], and parallelized on a BSP computer using a wavefront approach [2]. We extend this approach using the same method as in [3] to use a variable block size for parallel dynamic programming. This improves the performance, especially when the problem size is large. We study this BSP dynamic programming approach and give a performance model for predicting the running time. For sequential computation, both a linear space dynamic programming approach and a more efficient bit-parallel algorithm were implemented. A survey of bit-parallel algorithms for various kinds of string comparison can be found in [4].

In our experiments, we only compute the length of the LCS, which is a measure for the similarity of the input strings. The LCS itself can be obtained in a post-processing step. For a simple LLCS algorithm (without bit-parallelism), such a post-processing step is described in [5]. Extracting the actual longest common subsequence using bit-parallelism could be done in the same asymptotic time by saving the whole dynamic programming matrix and then running a second sweep of this matrix, using the method from [6]. A parallel (but non-BSP) LCS algorithm using bit-parallelism and a linear processor array is studied in [7]. Garcia et al. [5] propose a CGM algorithm for computing the LCS. Alves et al. [3, 8] describe CGM algorithms for computing the edit distance and string similarity, using different block grid sizes for dynamic programming. These results are similar to our experiments, and both CGM implementations achieve good speedup. However, none of the CGM algorithms used bit-parallel algorithms for sequential computation. Furthermore, none of these results were obtained using optimized BSP libraries like PUB [9] or the Oxford BSP Toolset [10] (Oxtool). Bit-parallel computation largely improves sequential computation performance and leads to lower communication costs, hence it is interesting to study under which circumstances speedup can still be obtained. Furthermore, we examine the running time predictability and show performance results for different parallel systems and libraries.

2 The BSP Model

The BSP model was introduced by Valiant in [11]. It describes a parallel computer with the tuple of parameters (p, f, g, l) . The performance of the individual processors in the parallel machine is characterized by the fixed time f needed to perform a primitive operation. The performance of the communication network is characterized by a linear approximation, using parameters g and l . The first parameter, g or *communication gap*, describes how fast data can be transmitted continuously by the network after the transfer has started. Its inverse $1/g$ is equivalent to the effective bandwidth. The *communication latency* l is the time overhead that is necessary for starting up communication. A BSP computation is divided into *supersteps*, each consisting of local computations and a communications phase. At the end of each superstep, the processes are synchronized using a barrier-style synchronization. Consider a computation consisting of S supersteps. For each specific superstep $1 \leq s \leq S$, let h_s^{in} be the maximum number of data units received and h_s^{out} the maximum number of data units sent by each processor in the communication phase. Further, let w_s be the maximum number of operations in the local computation phase. The whole computation has separate *computation cost* $W = \sum_{s=1}^S w_s$ and *communication cost*

$H = \sum_{s=1}^S h_s$ with $h_s = \max_p(h_s^{in} + h_s^{out})$. The total running time is given by

the sum $T = \sum_{s=1}^S T_s = f \cdot W + g \cdot H + l \cdot S$.

3 Problem Definition and Simple Algorithm

Let $X = x_1x_2 \dots x_m$ and $Y = y_1y_2 \dots y_n$ be two strings on an alphabet Σ of constant size σ . A *subsequence* U of a string is defined as any string which can be obtained by deleting zero or more elements from it, i.e. U is a subsequence of X when $U = x_{i_1}x_{i_2} \dots x_{i_k}$ and $i_q < i_{q+1}$ for all q with $1 \leq q < k$. Given two strings X and Y , a longest common subsequence (LCS) of both strings is defined as any string which is a subsequence of both X and Y and has maximum possible length. We consider the problem of finding the LCS length, which will be denoted as $LLCS(X, Y)$.

The basic dynamic programming algorithm for this problem defines the dynamic programming matrix $L_{0\dots m, 0\dots n}$ as follows (see e.g. [1]):

$$L_{i,j} = \begin{cases} 0 & \text{if } i = 0 \text{ or } j = 0, \\ L_{i-1,j-1} + 1 & \text{if } x_i = y_j, \\ \max(L_{i-1,j}, L_{i,j-1}) & \text{if } x_i \neq y_j. \end{cases} \tag{1}$$

The value $L_{i,j}$ is equal to $LLCS(x_1x_2 \dots x_i, y_1y_2 \dots y_j)$. Using dynamic programming [1], the values in this matrix can be computed in $O(mn)$ time and space.

The BSP version of the algorithm is based on a simple parallel algorithm for grid DAG computation. Matrix L is partitioned into a grid of rectangular blocks of size $(m/G) \times (n/G)$, where the parameter G specifies the grid size. A wavefront W_a consists of all blocks (b, c) for which $b + c - 1 = a$ (with $1 \leq a \leq 2G - 1$ and $1 \leq b, c \leq G$). The data in all blocks from wavefront W_a only depends on the data in the blocks of wavefront W_{a-1} . These blocks can be processed in parallel and we can compute matrix L in $2G - 1$ parallel stages, assuming $p = G$ processors are available. Our BSP algorithm requires $(2G - 1) \cdot G/p$ supersteps, assuming the ratio $\alpha = G/p$ to be an integer. After running the parallel algorithm, processor $G \bmod p$ holds the part of L which contains the LLCS. At the end of each superstep, we need to communicate the rightmost column and bottom row of the local part of L . When subproblem blocks are assigned to processors block-cyclically, the values in the bottom row and the corresponding part of string X can be kept locally and do not have to be transferred using the communication network, because one processor is always assigned blocks from the same column.

For simplicity, we assume that from now on the strings have equal length $n = m$ and that the input data distribution is block-cyclic with blocks of size $\lceil n/G \rceil$. In estimating the computation time, we need to consider that in general, there are less than G/p blocks in every wavefront. The number of blocks only equals G/p when the wavefront reaches the middle diagonal of the block grid. Input data and intermediate results have to be transferred for $G(G - 1)$ blocks (results have to be transferred for all blocks in the grid not located at the right border, and input data for the second string has to be fetched for all blocks not on the diagonal). Individual characters are stored in one byte, and 4-byte/32-bit integer values represent the dynamic programming matrix elements. Each

processor sends a column of matrix elements and receives a part of the second input string, which is distributed block-cyclically¹. Still assuming that $G = \alpha p$ with an integer α , we get

$$T(\alpha) = f \cdot (p\alpha(\alpha + 1) - \alpha) \cdot \left\lceil \frac{n}{\alpha p} \right\rceil^2 + g \cdot 5 \cdot \alpha(\alpha p - 1) \left\lceil \frac{n}{\alpha p} \right\rceil + l \cdot (2\alpha p - 1) \cdot \alpha . \tag{2}$$

The parameter α can be used to tune the performance of the algorithm. Knowing a minimum block size b for which the sequential algorithm achieves good performance (e.g. the processor’s cache size), the value of α can be pre-calculated before computation: $\alpha = \frac{5 \cdot n}{p \cdot b}$. This choice of α ensures that all the data necessary for computing one row of a dynamic programming matrix block can be stored in a memory block of size b . In the experiments, this method established good balance between having to minimize overhead from partitioning small problems into too many blocks, and achieving higher computation speed when the data for the local computations can be stored in the CPU cache.

4 Bit-Parallel Algorithm

Computing the LLCS using the standard dynamic programming approach is by far not the fastest method available. Let w be the bit-length of a machine word. Assuming that both integer and bitwise Boolean operations are available, the sequential computation time can be reduced by an approximate factor of $1/w$ using algorithms proposed by Crochemore et al. [12]. The basic idea of these algorithms is to work with the differences in the dynamic programming matrix $\Delta L_{i,j} = L_{i,j} - L_{i-1,j}$. These differences have either the values 0 or 1, and thus can be encoded as a bit string. The different bit-parallel algorithm variants have a general structure in common: they compute $\Delta L_{i,j}$ as a function of $\Delta L_{i-1,j}$ and a mapping $M(x)$, which maps a character x to a bit string of length n (i.e. the height of the dynamic programming table). Performance is gained because the values of $\Delta L_{i,j}$ can be computed using integer and bitwise Boolean operations, which work on w bits in parallel. In the following, we will use $\overline{\dots}$ to denote bitwise negation (one’s complement), $\dots \mid \dots$ to denote bitwise inclusive *or*, and $\dots \& \dots$ to denote bitwise *and* operations. Our implementation uses the algorithm from [12]. The other variants differ from this one in the number of operations used in the recurrence. However, all variants include integer operations that can create a carry which propagates downwards in the ΔL matrix. This keeps the data dependence pattern of the basic dynamic programming algorithm and makes the same wavefront approach necessary that was used in the previous section.

For implementing the mapping $M(x)$, we use the method of storing all the bit-vectors in an array of size $O(n \cdot \sigma)$, which is simple and fast, but also memory

¹ Another method would be to broadcast the second input string to all processors at the beginning. This is not done here to preserve memory-efficiency when working on long strings of equal length.

inefficient (see [13] for different methods). For computing parts of the dynamic programming matrix, the sequential algorithm gets the carry values and $\overline{\Delta L(m)}$ as input. For the left and top boundaries, the carry values can be initialized with zeroes, and $\overline{\Delta L_{0,\dots}}$ with ones respectively. The columns of $\overline{\Delta L}$ are computed as $\overline{\Delta L_{j,\dots}} = f(\overline{\Delta L_{j-1,\dots}}, M(x_j)) = Carry + \overline{\Delta L_{j-1,\dots}} + (\overline{\Delta L_{j-1,\dots}} \& M(x_k)) \mid (\overline{\Delta L_{j-1,\dots}} \& \overline{M(x_k)})$. The LLCS can be obtained by counting the number of zeros in $\overline{\Delta L(m, \dots)}$, as is proven in [12].

To obtain the LLCS in the parallel algorithm, the zero bits in all parts of $\overline{\Delta L_{m,\dots}}$ at the right side of the block grid are counted and summed up. This can be done in one additional superstep. We introduce a modified asymptotic computation speed f' , which will have a value of approximately $\frac{1}{w}f$ (see Table 1). The BSP running time for the parallel dynamic programming algorithm using bit-parallel computation is obtained similarly as described in the previous Section. We get:

$$T(\alpha) = f' \cdot (p\alpha(\alpha + 1) - \alpha) \cdot \left\lceil \frac{n}{\alpha p} \right\rceil^2 + g \cdot \frac{1}{2} \cdot \alpha(\alpha p - 1) \left\lceil \frac{n}{\alpha p} \right\rceil + l \cdot ((2\alpha p - 1) \cdot \alpha + 1) . \tag{3}$$

5 Experiments for the Simple Algorithm

All of the experiments were conducted on three different parallel machines at the Centre for Scientific Computing at the University of Warwick. The first one (**skua**) is an SGI Altix shared memory machine with 56 Itanium-2 1.6GHz nodes and a total of 112GB main memory. The second one (**argus**) is a Linux cluster with 31×2 -way SMP Pentium4 Xeon 2.6 GHz processors and 62 GB of memory (2 GB per 2-processor SMP node); it has good local computation performance but a slow communication network (100 Mbit Ethernet). The third system (**aracari**) is an IBM Myrinet cluster with 64×2 -way SMP Pentium3 1.4 GHz processors and 128 GB of memory (2 GB per 2-processor SMP node). It offers very good communication performance, but has slow individual processors. For the experiments, three different BSP programming frameworks were used: the Oxford BSP Toolset [10], PUB [9] and an MPI implementation that provides the same interface, based on MPI-1 (**aracari** and **argus**) or MPI-2 (**skua**).

Input strings were generated randomly and had equal length. The first set of experiments was run using string lengths between 8192 and 65536, and values of the grid size parameter α between 1 and 5, to study the predictability for small problem sizes. Table 1 shows the values of f used for prediction, which

Table 1. Experimental values of f and f'

Simple Algorithm (f)		Bit-Parallel Algorithm (f')	
skua	0.008 ns/op 130 M op/s	skua	0.00022 ns/op 4.5 G op/s
argus	0.016 ns/op 61 M op/s	argus	0.00034 ns/op 2.9 G op/s
aracari	0.012 ns/op 86 M op/s	aracari	0.00055 ns/op 1.8 G op/s

were obtained by measuring local computation times for one run. The values of l, g used to create the predictions were measured beforehand by timing random permutations using the `put` primitive, as this best matches the implementation’s communication pattern.

On the shared memory system (`skua`), the predictions for Oxtool and MPI matched the experimental results very well (see Table 3). The predicted running times were lower than the measurements using PUB, the same behavior was observed for the matrix multiplication algorithm. Good efficiency of up to 80% is achieved by Oxtool and MPI. PUB only achieves approximately 60% because its effective communication bandwidth is lower. On the distributed memory/Ethernet system (`argus`), best predictability is achieved by Oxtool. This is due to its low synchronization latency. The advantages of the optimized libraries for small messages can be seen particularly well on this system: the run time for the MPI version improves drastically when using smaller values of the grid size parameter α . When α is larger, the dynamic programming algorithm particularly benefits from the low synchronization latency of Oxtool. The implementation on top of MPI has very high latency, and thus produces long running times even for small problem sizes. Best efficiency and superlinear speedup on 4 processors is achieved by Oxtool and PUB with slight advantages for Oxtool. MPI cannot benefit from the lower computational costs for higher values of α , as these are compensated by higher synchronization costs. On the distributed memory/Myrinet system (`aracari`), best predictability is achieved by MPI and Oxtool, the mean relative prediction error is smaller than 5% for all numbers of processors. Best efficiency is achieved by PUB and Oxtool for similar reasons as on `argus`. PUB benefits from having a low synchronization latency, Oxtool has the better effective bandwidth. On average, both achieve similar performance. The performance for MPI drops when the number of processors is larger, as its synchronization latency becomes higher.

The performance of the algorithm was evaluated by running it on larger problems and using an optimized value of α . The speedup results are shown

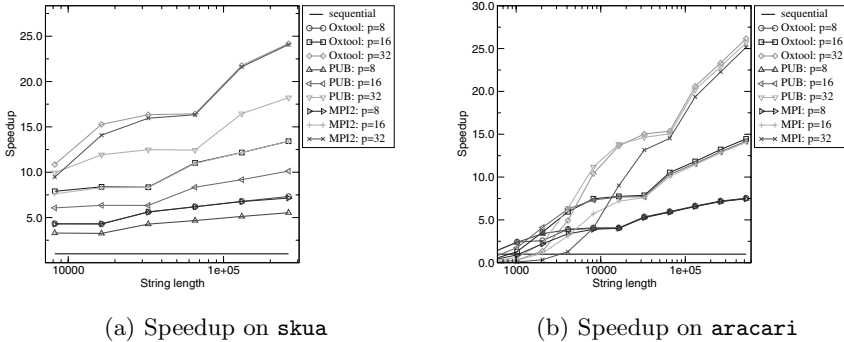


Fig. 1. LLCS computation — Speedup

in Figure 1. It can be seen that there are few differences between MPI, PUB and Oxtool for large problems. For short strings, Oxtool and PUB show advantages over MPI on the message passing systems (*aracari* and *argus*), particularly when the number of processors is large. On *skua*, PUB obviously has difficulties when the communication cost is too large, and achieves substantially lower speedup than MPI or Oxtool. The speedup graphs also demonstrate well that MPI only achieves comparable speedup to an optimized communication library if the problem size is large.

6 Experiments for the Bit-Parallel Algorithm

The bit-parallel algorithm shows much better local computation performance (see Table 1) on all systems and also has lower communication costs. However, the asymptotic computation speed on *skua* is only reached for very large problem sizes.

Supplying the sequential computation code in assembly instead of C++ is likely to improve performance and predictability for this algorithm on *skua*. However, we still used the C++ code to ensure portability. As the performance for the problem sizes that arise in our experiments is not constant using this code, running times on *skua* cannot be predicted accurately using a constant value of f . The predicted running times are smaller than the measured times, especially when the block size decreases if α is larger or more processors are used. On the other systems, the predictions were of similar quality as the ones made for the simple LLCS algorithm. On *aracari*, PUB shows a performance drop when the communication cost becomes larger than approximately 2048 bytes.

Table 3 shows the results for efficiency and prediction error. On all systems, the speedup (i.e. the efficiency multiplied with the number of processors) achieved when using the bit-parallel sequential algorithm is lower compared to the experiments using the standard algorithm (however, the running time using the bit-parallel algorithm is always lower than using the standard algorithm). On the shared memory machine, this is caused by a lower sequential computation speed for small subproblem sizes (as discussed above). An increased grid size leads to lower sequential computation performance, as this decreases the subproblem size. However, further increasing the problem size on the shared memory system presumably would yield better speedup.

On the distributed memory systems, the parallel speedup when using bit-parallel computation instead of the standard algorithm is also lower. Still, good speedup is obtained both on Myrinet (*aracari*) and Ethernet (*argus*). The best performance on *argus* is achieved by Oxtool, and the performance of PUB is

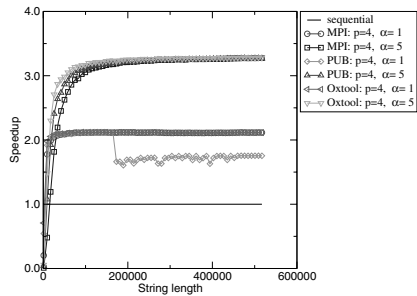


Fig. 2. Speedup on *aracari*, 4 processors

Table 2. Experimental result summary. The number of bullets specifies the performance that was achieved by each library, ranging from • (lowest performance compared to the other libraries) to ●●● (best performance).

Experiments	Oxtool	PUB	MPI
<i>Shared memory (skua)</i>			
LLCS (standard)	●●●	•	●●
LLCS (bit-parallel)	●●	●●●	•
<i>Distributed memory, Ethernet (argus)</i>			
LLCS (standard)	●●●	●●	•
LLCS (bit-parallel)	●●●	●●	•
<i>Distributed memory, Myrinet (aracari)</i>			
LLCS (standard)	●●●	●●	•
LLCS (bit-parallel)	●●	●●○ ^a	•

^a Best performance until drop at $h = 2048$ bytes.

only slightly worse. On 10 processors, the difference between plain MPI and the optimized libraries is most visible. When using higher values of α , PUB and Oxtool achieve better speedup, whereas MPI shows decreasing performance due to its high overhead for small communication costs. When using 4 processors on *aracari*, the performance drop of PUB, starting at a certain communication cost, is clearly visible (see Figure 2). When the number of processors and hence the block grid size increases, the communication cost becomes lower and PUB shows very good performance. When using a large grid size on *aracari*, PUB outperforms both MPI and Oxtool.

7 Conclusions

Experiments were conducted on three different parallel machines: a shared memory system and two PC clusters, one with an Ethernet, the other with a Myrinet interconnection network. We compared the performance of different communication libraries: PUB, the Oxford BSP Toolset, and a simple BSP library based on MPI. PUB and the Oxford BSP Toolset both implement optimizations to improve communication performance. Our benchmarking algorithm computes the length of the longest common subsequence of two strings. This algorithm has linear communication cost and quadratic computation cost. Performance predictability was very good. However, when using an efficient sequential implementation, good speedup could only be obtained for very large problem sizes. The PUB implementation of this algorithm showed very good performance when the communication cost is small. Table 2 shows a short summary of all results. In general, using an optimized communication library for bulk-synchronous parallel dynamic programming algorithms improves performance particularly when the problem size is small, or many processors are used. When using an efficient sequential implementation, it can be difficult to achieve good parallel speedup, as communication is a larger part of the overall running time then.

References

1. Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C.: Introduction to Algorithms. 2nd edn. MIT Press, Cambridge, MA (2001)
2. Gibbons, A., Rytter, W.: Efficient parallel algorithms. Cambridge University Press, New York, NY, USA (1988)
3. Alves, C.E.R., Cáceres, E.N., Dehne, F.: Parallel dynamic programming for solving the string editing problem on a CGM/BSP. In: Proc. of the 14th Annual ACM Symposium on Parallel Algorithms and Architectures (SPAA '02), New York, NY, USA, ACM Press (2002) 275—281
4. Navarro, G.: A guided tour to approximate string matching. ACM Computing Surveys **33**(1) (2001) 31—88
5. Garcia, T., Myoupo, J.F., Semé, D.: A coarse-grained multicomputer algorithm for the longest common subsequence problem. In: Euro PDP. (2003) 349—356
6. Crochemore, M., Iliopoulos, C.S., Pinzon, Y.J.: Recovering an LCS in $O(n^2/w)$ time and space. Colombian Journal of Computation **3**(1) (2002) 41—52
7. Michailidis, P.D., Margaritis, K.G.: New processor array architectures for the longest common subsequence problem. The Journal of Supercomputing **32**(1) (2005) 51—69
8. Alves, C., Cáceres, E., Dehne, F., Song, S.: A parallel wavefront algorithm for efficient biological sequence comparison. In: ICCSA. Volume 2668 of LNCS. (2003)
9. The PUB library: <http://www.uni-paderborn.de/~bsp/> (2005)
10. The Oxford BSP Toolset: <http://www.bsp-worldwide.org/implmnts/oxtool/> (1999)
11. Valiant, L.G.: A bridging model for parallel computation. Communications of the ACM **33**(8) (1990) 103—111
12. Crochemore, M., Iliopoulos, C.S., Pinzon, Y.J., Reid, J.F.: A fast and practical bit-vector algorithm for the longest common subsequence problem. Information Processing Letters **80**(6) (2001) 279—285
13. Hyvrö, H., Takaba, J., Shinohara, A., Takeda, M.: On bit-parallel processing of multi-byte text. In: Asia Information Retrieval Symposium, AIRS 2004, Beijing, China, Lecture Notes in Computer Science. Volume 3411. (2005) 289—300

Appendix: Tables

Table 3. Efficiency and mean relative prediction errors

	Oxtool		PUB		MPI	
α	Efficiency rel. error (in %)	Efficiency rel. error (in %)	Efficiency rel. error (in %)	Efficiency rel. error (in %)	Efficiency rel. error (in %)	Efficiency rel. error (in %)
LLCS Computation — Standard Algorithm						
... on skua						
16 processors						
1	52.15	1.9	39.65	23.4	56.29	4.0
3	76.76	4.1	66.49	18.9	75.94	5.7
5	83.03	5.4	63.37	16.5	80.91	9.2
32 processors						
1	51.07	4.8	37.03	27.0	50.81	3.8
3	71.29	9.5	51.93	22.4	67.16	9.2
5	68.17	15.2	52.64	19.6	57.34	16.4
... on argus						
4 processors						
1	80.41	1.7	80.54	2.2	79.96	3.3
3	110.35	3.7	109.15	11.0	-	-
5	117.90	5.1	115.41	17.7	108.83	1.4
10 processors						
1	70.59	8.1	71.22	6.7	67.39	7.3
3	96.80	12.0	96.44	20.0	-	-
5	96.79	13.4	94.14	30.0	43.31	1.4
... on aracari						
32 processors						
1	34.45	2.6	34.36	4.3	33.08	4.4
3	48.91	3.9	48.35	3.6	33.26	4.5
5	43.43	2.9	45.99	5.9	20.92	5.3
LLCS Computation — Bit-Parallel Algorithm						
... on skua						
16 processors						
1	42.48	53.8	44.71	51.1	42.39	53.7
3	30.38	77.4	30.50	76.1	30.23	77.2
5	21.78	84.4	22.23	82.8	21.43	83.7
32 processors						
1	27.33	71.0	27.95	70.3	27.11	70.8
3	16.30	84.9	16.80	84.1	16.07	82.8
5	11.41	86.5	11.68	85.4	11.16	82.8
... on argus						
4 processors						
1	56.09	2.0	56.34	3.4	56.11	2.9
3	79.27	3.9	79.35	10.4	77.53	1.0
5	86.33	8.5	86.44	17.1	81.93	2.8
10 processors						
1	47.93	8.9	48.17	8.8	46.95	7.4
3	71.25	1.7	70.33	20.0	-	-
5	74.26	2.5	71.25	30.4	42.90	1.9
... on aracari						
32 processors						
1	45.98	8.3	45.91	9.9	45.14	9.9
3	68.56	3.2	68.51	7.8	56.07	6.1
5	47.85	3.9	70.65	9.5	43.82	6.0

Simulation of Internet Transport Protocols for High Bandwidth-Delay Networks*

Junsoo Lee

Department of Computer Science,
Sookmyung Women's University,
Seoul, Korea 140-742

jslee@sm.ac.kr

<http://cs.sookmyung.ac.kr/~jslee>

Abstract. This paper addresses the simulation of communication networks with high bandwidth-delay products. We use hybrid models to overcome the computational/memory barriers that packet-level simulators encounter due to the large number of packets present in the network at every instant of time. We describe a set of software tools that constructs these hybrid models for general networks. The networks to be simulated and their parameters are specified in a *network description script language (NDSL)* and an *NDSL translator* automatically generates the corresponding a model in the hybrid systems specification language *modelica*. We also extend our previous hybrid modeling work to several variants of TCP that appeared recently to improve TCP's poor performance in high bandwidth-delay product networks. To demonstrate the usefulness of software tools developed and the new TCP hybrid models, we discuss simulation results from Internet-2 Abilene backbone.

1 Introduction

Packet-level models are the most widely used models to study communication networks because of their accuracy and simplicity. However, in tracking each individual packet as it travels across the network, they require significant processing and memory for large scale or high bandwidth-delay product networks.

Fluid models attempt to overcome these difficulties by tracking the average behavior of many flows [1, 2]. These models can be very efficient when the average rate of traffic does not change very frequently, at the expense of some loss in expressiveness: they do not capture the dynamics of individual flows neither the occurrence of discrete events such as drops and queues becoming full/empty.

A hybrid systems approach to modeling networks was proposed in [3]. It is based on the idea of reducing complexity by considering continuous approximations to variables like the queue and congestion window size (cwnd) of individual flows, and yet still modeling explicitly discrete events such as drops. It was shown

* This material is based upon work supported by the National Science Foundation under Grant No. ANI-0322476.

in [3] that UDP and TCP-Sack flows could be accurately simulated using hybrid models, with simulation times orders of magnitude smaller than `ns-2` [4].

This paper describes software tools to simulate computer networks on a significant larger scale than before. A *Network Description Scripting Language* (NDSL) was developed to specify communication networks, in terms of topology, link characteristics, traffic sources, queue parameters, etc. This scripting language is analogous to the `ns-2` [4] OTCL language component. An *NDSL Translator* was also developed to automatically transform NDSL scripts into the hybrid systems modeling language *modelica*, for which several simulation engines are available.

The only reliable transport protocol supported by the model in [3] is TCP-Sack. However, it has been well documented that TCP-Sack performs poorly in networks with high bandwidth-delay products. In this paper, we present hybrid models of several variants of TCP that were especially developed for these networks: FAST TCP [5], HighSpeed TCP(HSTCP) [6], and Scalable TCP(STCP) [7]. Because of complexity issues, the evaluation of these protocols has mostly been restricted to live networks, which limits the topologies and scenarios that can be tested. With the software tools developed we were able to carry out a simulation study on the effect of the Round-Trip Time(RTT) on the throughput of TCP flows and its variants over the Internet-2 backbone addition. This study is not exhaustive, but it clearly illustrates the use of the simulation tools developed and their potential impact.

The remainder of this paper is organized as follows. Section 2 presents hybrid systems models of transport protocols for high bandwidth-delay networks. Sections 3 and Section 4 describe the *Network Description Scripting* (NDSL) and the *NDSL Translator*. Section 5 presents a Abilene case study using TCP-Sack hybrid model and software tools discussed in Sections 3 and Section 4. Section 6 shows case studies of simulation using transport protocols for high bandwidth-delay networks. Finally, we present our concluding remarks in Section 7.

2 Hybrid Modeling Framework

Hybrid models in this paper are developed based on the hybrid modeling framework presented in [3]. In [3], hybrid models for Queues, TCP and UDP were introduced. By composing traffic sources and drop models, one can construct hybrid models for arbitrarily complex networks with end-to-end TCP and UDP connections. We introduce several new hybrid models of transport protocols for high bandwidth-delay product networks in this paper. These protocols have been recently introduced due to the high-speed networks commonly available today. Their motivation for developing new Internet transport protocols is that current TCP protocols do not perform well in high bandwidth-delay product networks. Thus, new protocols such as FAST TCP [5], HighSpeed TCP(HSTCP) [6], and Scalable TCP(STCP) [7] have been proposed. This section describes hybrid models of protocols for high bandwidth-delay networks.

2.1 FAST TCP

Recently, Low et al. proposed FAST TCP protocol [5] for high bandwidth-delay networks at speeds of upto 10 Gbps and 100 Gbps in the future. FAST TCP reacts to congestion by using queuing delay in addition to packet loss because in high bandwidth-delay product networks there is significant amount of time gap between drop events. For example, it may take over one hour to recover from a loss event in a TCP connection with 10 Gbps bottleneck and 180 ms RTT. Therefore, FAST TCP takes account queuing delay in addition to a packet loss to control size of congestion window (cwnd).

Hybrid model of FAST TCP is based on the algorithms in [5]. The congestion window control algorithm in this paper is based on the flow level algorithm and can be derived as follows.

From equation (6) in [5],

$$w_i(t+1) = \gamma \left(\frac{d_i w_i(t)}{d_i + q_i(t)} + \alpha_i(w_i(t), q_i(t)) \right) + (1 - \gamma)w_i(t)$$

by subtracting with $w_i(t)$ and dividing by RTT,

$$\dot{w} = \frac{\gamma}{RTT} \left(\left(\frac{baseRTT}{RTT} - 1 \right) * w + \alpha_i(w, q) \right)$$

where $\gamma \in (0,1]$, and $\alpha(w, q)$ is defined by

$$\alpha(w, q) = \begin{cases} a * w & \text{if } q_i = 0 \\ \alpha_i & \text{otherwise} \end{cases}$$

In this equation, when a bottleneck queue is empty the cwnd increases exponentially, but when queue starts to fill the cwnd increases by some parameter α . One of the important factors to decide performance of FAST TCP is how to decide α value.

Figure 1 shows simple hybrid model for FAST TCP which consists of congestion-avoidance, congestion-avoidance delay and loss-recovery state. Arrow represents transition between these states. Cwnd(w_f) and sending rate(r_f) in each state are defined by specific equation. FAST TCP starts with congestion avoidance state. If drop occurs, state changes to congestion-avoidance delay. The duration in the congestion-avoidance delay is a delay between drop and detection. After a RTT, state changes to loss-recovery and at this time the cwnd is divided by two. State changes back to congestion-avoidance after successful retransmission of lost packets.

2.2 HighSpeed TCP

HighSpeed TCP(HSTCP) [6] is a modification to current TCP's congestion control algorithm. While most algorithms of HSTCP are similar to those of TCP-Sack, HSTCP increases cwnd more aggressively and decreases more gently. To specify a faster response function, HSTCP maintains four parameters,

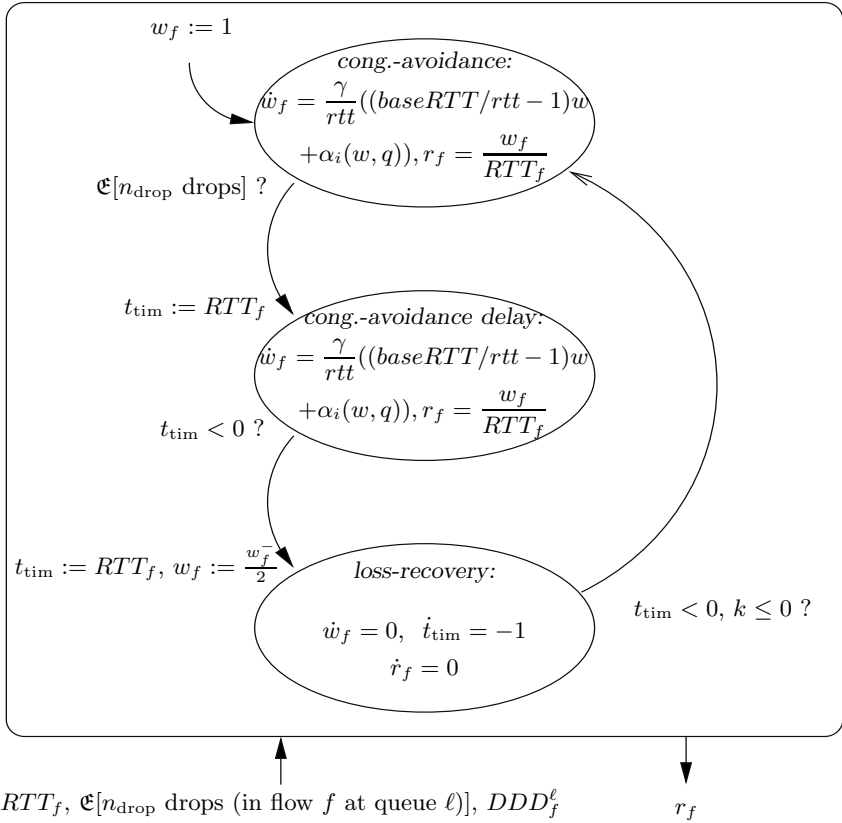


Fig. 1. Hybrid model for flow f under TCP-FAST

Low_{window} , $High_{window}$, $High_p$, and $High_{decrease}$. In addition, to ensure fairness, the HSTCP response function uses the same response function as standard TCP when the cwnd is below Low_{window} which is 38 packets. For a TCP connection in high bandwidth-delay networks where average cwnd is around 83,000 segments, $High_p$ is set to 10^{-7} . In other words, a packet drop rate of 10^{-7} allows the HighSpeed TCP connection to achieve an average cwnd of 83,000 segments.

The following equation specifies increase and decrease parameter $\alpha(w)$ and $\beta(w)$ respectively.

$$\alpha(w) := High_{window}^2 * High_p * 2 * \beta(w) / (2 - \beta(w))$$

Decrease parameter is computed as follows.

$$\beta(w) := (High_{decrease} - 0.5)(\log(w) - \log(W)) / (\log(W_h) - \log(W)) + 0.5$$

where $W = Low_{window}$ and $W_h = High_{window}$. The hybrid model of HighSpeed TCP uses the same parameter used as in the ns-2. We assume limited slow-start [8] is used to remove packet losses in the beginning of slow-start.

2.3 Scalable TCP

Scalable TCP (STCP) [7] is a sender side modification of the TCP congestion window update algorithm. The motivation behind Scalable TCP is also slow responsiveness of traditional TCP sender. To perform more aggressive increase of *cwnd*, STCP considers the use of the following increase and decrease parameters. For each acknowledgment received in a round trip time in which congestion have not been detected

$$cwnd := cwnd + \alpha, \alpha = 0.01$$

and on the detection of congestion

$$cwnd := cwnd * \beta, \beta = 0.875$$

Because *cwnd* increases by α for every received acknowledgment, *cwnd* size in the next round depends on the current size of *cwnd*. Increment of *cwnd* is proportional to the current *cwnd* and this is different from the algorithm of traditional TCP which increases *cwnd* linearly regardless of current size of *cwnd*.

3 Network Description Scripting Language (NDSL)

Hybrid models of protocols and queues can be simulated by a program written in hybrid systems modeling language such as *modelica* [9]. Because these languages are special-purpose languages designed to model physical systems, implementation becomes complex to computer scientist if large scale communication networks are simulated. Thus large scale communication networks have not been simulated with hybrid systems so far. However, Network Description Scripting Language (NDSL) enables us to simulate large and complex topology by providing simple user interface.

Developing the NDSL is inspired by **ns-2** packet-level simulator. User interface part of **ns-2** is written in Object Oriented TCL (OTCL) script language so that it can support convenient reconfiguration of topologies and traffic. The NDSL is analogous to the OTCL component of **ns-2** by specifying succinctly large, complex networks. Case studies using NDSL primitives are shown in Section 5 and Section 6.

4 NDSL Translator

The *NDSL translator* automatically translates NDSL specification into a hybrid model expressed in *modelica* [9] language. NDSL translator first parses the primitives and parameters. Then, it translates the NDSL primitives into the corresponding *modelica* objects. The program generated by NDSL translator can be fed directly into simulation engines.

The *Network library* is used when NDSL script is translated into *modelica* program. This library contains modules which correspond to the NDSL's basic

primitives. The *Network library* is updated when existing primitives are modified or a new one is added. The current version of the *network library* is divided into several packages, including *traffic source*, *traffic sink*, *node*, *link*, *connector*, *function*, etc.

The *traffic source* package contains *modelica* implementation of traffic sources such as variants of TCP or UDP. Because the traffic source typically requires a corresponding sink, the *traffic sink* package contains TCP sink models. Parameters associated with links are specified in the *link* package. These include bandwidth, propagation delay, and queuing policy. The *Connector* package consists of input and output “connectors” that are used to connect the basic components (e.g., sources, sinks, links). This is analogous to global variables shared by different functions in general-purpose programming languages. Finally, utility components are defined in the *function* and can be invoked by other models. An example of a utility component is a function computing the sum or minimum value out of an array.

5 Case Study 1: TCP Fairness on Abilene Backbone Network

The Abilene Network (shown in Figure 2) is an Internet-2 high-performance backbone network connecting research institutions to enable the development of advanced Internet applications and protocols. Recently, it has been upgraded to 10 Gbps using OC-192 circuits. In order to accurately simulate Abilene network, information related to the topology is required, and the measured propagation delays between router nodes are shown in Table 1.

In this experiment, we simulated three sets of ten TCP-Sack flows described in Table 2. Each flow starts randomly between 0 and 10 seconds in the beginning of simulation and terminates at 40,000 seconds.

This case study shows how hybrid model can be used to compare throughput of TCP-Sack in Abilene backbone as a function of queue size. To this effect, we varied throughput while changing the queue sizes from 25,000 to 150,000 packets in increments of 25,000. We ran 11 hours of simulation time. In high bandwidth-delay network simulation, one needs to simulate longer time than low or average



Fig. 2. Internet-2 Abilene Backbone Network

Table 1. Two-way propagation delay between nodes in the Abilene Backbone

source	destination	prop. delay
Seattle (STTL)	Denver (DNVR)	25.608ms
Sunnyvale (SNVA)	Denver (DNVR)	25.010ms
Denver (DNVR)	Kansas City (KSCY)	10.674ms
Kansas City (KSCY)	Indianapolis (IPLS)	9.340ms
Indianapolis (IPLS)	Chicago (CHIN)	3.990ms
Chicago (CHIN)	New York (NYCM)	20.464ms
Sunnyvale (SNVA)	Los Angeles (LOSA)	7.772ms
Los Angeles (LOSA)	Houston (HSTN)	31.624ms
Houston (HSTN)	Atlanta (ATLA)	19.756ms
Atlanta (ATLA)	Washington (WASH)	15.938ms
Washington (WASH)	New York (NYCM)	4.412ms
Sunnyvale (SNVA)	Seattle (STTL)	16.852ms
Houston (HSTN)	Kansas City (KSCY)	15.504ms
Atlanta (ATLA)	Indianapolis (IPLS)	10.950ms

Table 2. TCP flows simulated over Abilene Backbone

sets	number of flows	prop. delay	source/destination
set one	10	15 ms	ATLA to CHIN
set two	10	28.8 ms	HSTN to CHIN
set three	10	69.5 ms	SNVA to NYCM

bandwidth-delay network simulation. Note that for a 10 Gbps backbone with 70 ms RTT and 1000-byte packet size, the bandwidth-delay product is 87,500 packets. If the queue size is the same as the bandwidth-delay product, the maximum cwnd can be as large as 175,000 packets. If the sender detects a congestion loss at this time, the cwnd reduces from 175,000 to 87,500. Thus it takes 87,500 RTTs to reach queue full, which amounts to 1 hour and 42 minutes. Simulation of this type of high bandwidth-delay product network was not feasible in a packet level simulator such as ns-2. However, the hybrid systems simulation requires no more than 20 minutes of execution time. Although versions of TCP adapted to high-bandwidth networks reach steady-state much faster than TCP-Sack, packet level simulation is still very slow because of large number of packets in the simulator. This will be discussed in the next case study.

Figure 3 shows fairness ratio between flows in different sets (cf. Table 2). The *fairness ratio* $FR_{i,j}$ is defined as the ratio between the average throughput of flows in sets i divided by the average throughput of flows in j . When the queue size is 25,000, the average throughput of set one is 3.1 times bigger than the average throughput of set three but when the queue size increases to 150,000, the throughput ratio becomes only 1.5. This is consistent with the expectation that, when the queuing delay increases considerably, it will dominate the RTT ratio between the two flows sharing common bottleneck. However, in topologies

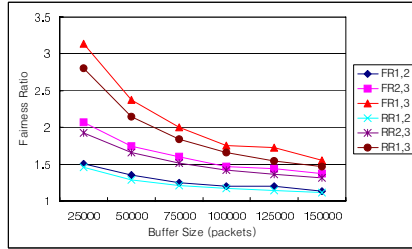


Fig. 3. Average throughput fairness between the three different TCP-Sack flow sets simulated on the Abilene Network

like this one, the precise dependence of the fairness ratio with the buffer size is difficult to predict without resorting to simulations.

Figure 3 also shows the ratio $RR_{i,j}$ between the average RTTs of the flows in sets i and j (in the reciprocal order). Since all the flows go through the same bottleneck (Chicago-Indianapolis), based on the TCP-friendly formula one could expect the fairness ratio to match the reciprocal of the RTT ratio. The simulations reveal that this generally underestimates the fairness ratio, especially when the ratio is far from one. This phenomenon has been confirmed by `ns-2` simulations in smaller networks and is further studied in [10].

6 Case Study 2: Simulation of High Speed Transport Protocols

In the second case study, Internet transport protocols for high speed networks are compared over Abilene backbone network. We simulated bulk data transfer using FTP from Los Angeles to New York City. According to Table 1, the propagation delay between these two cities is 71.7 ms. The Bandwidth-delay product is around 90,000 packets with 1000-byte packet size. Generally, the buffer size provided in low speed network simulation is as large as bandwidth-delay product to maximize the throughput. However, in a high-speed network the queue size often smaller than the bandwidth-delay product because queues require very high-speed memory [7].

We compared cwnd of four protocols as in the Figure 4 where buffer size is 5,000 packets in the hybrid system. Note that if the bandwidth is 10 Gbps and the round-trip time is 71.7 ms, the sender requires to send 90,000 packets per round-trip time to achieve 100% link utilization. However, TCP-Sack does not utilize full bandwidth most of the time as in the Figure 4. Cwnd of TCP-Sack goes up to 120,000 in the slow-start, then the sender detects a packet loss. The sender reduces cwnd to around half of 120,000, and starts to increase cwnd but only two thirds of the link bandwidth are utilized when cwnd is 60,000. Since the sender is in a congestion-avoidance mode, it increases cwnd by one for each round-trip time. Figure 4 illustrates this slow increase of TCP-Sack’s cwnd, and it takes 30,000 round-trip times (36 min) to fully utilize the total bandwidth.

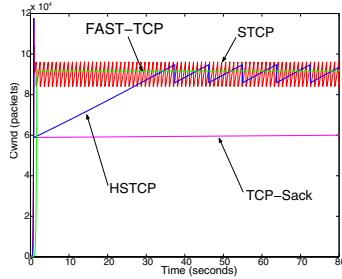


Fig. 4. Cwnd of Tcp-Sack, FAST TCP, HSTCP, STCP on the Abilene backbone network where buffer size is 5,000 packets

When cwnd reaches 95,000, another packet loss occurs, and it takes another 32,500 round-trip times to recover.

The cwnd evolution of HSTCP is the same as that of TCP-Sack until packet losses occur in the slow-start. However, increase rate of cwnd of HSTCP in congestion-avoidance is faster than that of TCP-Sack. Thus, HSTCP shows 100% utilization within 35 seconds. HSTCP's decrease parameter is around one fifth of TCP-Sack's in this example and this also enables HSTCP to recover faster than TCP-Sack from a loss event. HSTCP can recover from a loss event in 8 seconds.

STCP's cwnd is the same as TCP-Sack's while it is in slow-start but it does not reduce cwnd to half when a packet loss is detected. Rather, it reduces cwnd to 87.5% of previous cwnd. In the congestion-avoidance mode, STCP increases cwnd by 0.01 for every acknowledgment. In other words, increase parameter of STCP becomes larger than that of regular TCP when cwnd is over one hundred. STCP's recovery time is around one second in this example.

While previously discussed protocols experience a packet loss in the slow-start, FAST TCP does not experience a packet loss because its congestion control mechanism reacts to congestion by using queuing delay in addition to a packet loss. Cwnd of FAST TCP increases exponentially when there is no queuing delay in the beginning of simulation. However, if queuing delay is greater than zero, cwnd increases by a function of α value so that the source reduces the sending rate before the buffer becomes full. This type of simulation is not feasible in ns-2 due to large packet overhead. Therefore, this case study shows that hybrid system can be used to simulate variation of TCP protocols for high speed network with far less complexity.

7 Conclusion and Future Work

This paper proposes simulation of communication networks in high bandwidth-delay products. We use hybrid models to overcome the complexity of packet-level simulation. We describe a set of software tool that construct these hybrid models for general communication networks. We also extend our previous hybrid

modeling work to several variants of TCP that improve TCP's performance in high bandwidth-delay product networks. In order to demonstrate the developed software tools and extended hybrid model, we discuss two case studies on Abilene Internet-2 backbone network.

References

1. Yan, A., Gong, W.: Fluid simulation for high speed networks. *IEEE Trans. on Inform. Theory* (1999)
2. Kumaran, K., Mitra, D.: Performance and fluid simulations of a novel shared buffer management system. In: *Proc. of the IEEE INFOCOM*. (1998) 1449–1461
3. Bohacek, S., Hespanha, J.P., Lee, J., Obraczka, K.: A hybrid systems modeling framework for fast and accurate simulation of data communication networks. In: *ACM SIGMETRICS*. (2003)
4. The VINT Project, a collaboratoin between researchers at UC Berkeley, LBL, USC/ISI, and Xerox PARC: The ns Manual (formerly ns Notes and Documentation). (2000) Available at <http://www.isi.edu/nsnam/ns/ns-documentation.html>.
5. Jin, C., Wei, D.X., Low, S.H.: Fast tcp: motivation, architecture, algorithms, performance. In: *Proc. of the IEEE INFOCOM*. (2004)
6. Floyd, S., Ratnasamy, S., , Shenker, S.: Highspeed TCP for large congestion windows. RFC 3649 (2003)
7. Kelly, T.: Scalable TCP: improving performance in highspeed wide area networks. *SIGCOMM Comput. Commun. Rev.* **33** (2003) 83–91
8. Floyd, S.: Limited slow-start for TCP with large congestion windows. RFC 3742 (2004)
9. Tiller, M.M.: *Introduction to Physical Modeling with Modelica*. The Kluwer international series in engineering and computer science. Kluwer Academic Publishers, Boston (2001)
10. Bohacek, S., Hespanha, J.P., Lee, J., Obraczka, K.: Fairness of TCP/IP in high bandwidth-delay product networks. Technical report, USC, Los Angeles (2004)

Performance Evaluation of Parallel Systems Employing Roll-Forward Checkpoint Schemes*

Gyung-Leen Park¹, Hee Yong Youn^{2,**}, Junghoon Lee¹, Chul Soo Kim¹,
Bongkyu Lee¹, Sang Joon Lee³, Wang-Cheol Song³, and Yung-Cheol Byun³

¹ Dept. of Computer Science and Statistics,
Cheju National University, Cheju, Korea

{glpark, jhlee, chkim, bklee}@cheju.ac.kr

² School of Information and Communications Engineering,
Sungkyunkwan University, Suwon, Korea

youn@ece.skku.ac.kr

³ Faculty of Telecommunication and Computer Engineering,
Cheju National University, Cheju, Korea

{sjlee, philo, ycb}@cheju.ac.kr

Abstract. High performance and reliability are the main goals of parallel and distributed computing systems. To increase the performance and reliability of the systems, various checkpoint schemes have been proposed in the literature for decades. However, the lack of general analytical models has been an obstacle to compare the performance of systems employing different checkpoint schemes. This paper develops an analytical model to evaluate the relative response time of systems employing checkpoint schemes. The model has been applied to evaluate the relative response time of systems employing RFC (Roll-Forward Checkpoint), DMR-F (Double Modular Redundancy for Forward recovery), and DST (Duplex with Self-Test) schemes. The result shows the feasibility of the model developed in the paper.

1 Introduction

Due to the demand for high performance computing in numerous applications, parallel and distributed computation using multiple processors has become very important these days. In the parallel and distributed systems, one of the primary technical issues is failure handling. This is because the detrimental impact of any failure gets more significant as the system becomes more complicated. Therefore, the failure should be quickly identified and corrected to allow desired level of reliability, and this requirement is relatively more important to mission-critical applications.

Among software-oriented approaches for achieving this goal, Checkpoint and Rollback Recovery (CRR) scheme [1]-[4] has been recognized to be effective for

* This research was supported by the MIC, Korea, under the ITRC support program supervised by the IITA(IITA-2005-C1090-0502-0009).

** Corresponding author.

a large class of applications. In the CRR scheme the state of the system is periodically saved in a stable storage, which is called *checkpoint*. The checkpoint can be decided by a programmer or by a compiler[5]. Whenever a fault is detected, the system rolls back to the last checkpoint and retries the operation from that checkpoint. Compared to the error recovery from the very beginning, the task completion time is substantially smaller. The rollback recovery technique is important in designing reliable computer systems since the majority of failures in computer systems have been identified as transient or intermittent[6].

Roll-forward recovery approaches [7]-[10] have been proposed to further enhance the performance of a system with CRR scheme. The main idea of these schemes is to reduce the rollback probability by utilizing extra processors for identifying the faulty processor while the original process is continued. The roll-forward schemes can thus allow the error recovery without rollback for some cases of fault distribution, which results in a higher throughput. There exists a tradeoff between the performance and implementation overhead according to how the roll-forward approach is realized as shown later.

While numerous roll-forward checkpoint schemes have been proposed in the literature, the lack of a general model has been an obstacle to compare the performance of systems employing various checkpoint schemes. The paper develops general analytical models to evaluate the performance of various checkpoint schemes in terms of the relative response time. The models developed in the paper have been applied to the systems employing RFC (Roll-Forward Checkpoint), DMR-F (Double Modular Redundancy for Forward recovery), and DST (Duplex with Self-Test) schemes. The result shows the effectiveness of the models.

The rest of the paper is organized as follows. Section 2 briefly reviews roll-forward recovery schemes presented in the literature. Section 3 develops general analytical models to evaluate the relative response time of the system with roll-forward recovery schemes. Using the models, the performances of the schemes are also compared in the section. Finally, Section 4 concludes the paper.

2 Review of the Previous Schemes

In the CRR approach, a rollback recovery is required for every detected fault. In the roll-forward recovery approach, however, some rollbacks are avoided by identifying the fault-free processor. Earlier schemes differ from each other by the mechanism how this is done. They are briefly reviewed and compared in this section.

2.1 DMR-F Scheme

In this scheme[8], two processors, P_1 and P_2 , simultaneously execute the same task, and the checkpoints from the two processors are compared. If the checkpoints match, it is assumed that the system is fault-free and one of the identical checkpoints is saved in a stable storage. Such matching checkpoint is called *committed* checkpoint. If they mismatch, the system is assumed to be faulty and

another processor, P_3 is initiated to identify the fault-free one. In other words, P_3 executes the *validation task*.

In addition to P_3 for rollback validation, two processors are forked from each processor in the case of mismatch, P_{11} and P_{12} from P_1 , P_{21} and P_{22} from P_2 , to maintain the original duplex structure from each uncommitted checkpoint. The execution from each uncommitted checkpoint is called the *lookahead execution*. If any checkpoint from the two processors, P_1 and P_2 , agrees with that of P_3 after the rollback validation, the fault-free checkpoint is identified. The two lookahead tasks forked from the processor with the faulty checkpoint are abandoned thereafter, while those from the processor with the error-free checkpoint are continued for further execution. If there is no match out of the three checkpoints, the system needs to rollback to the last committed checkpoint. Therefore rollback can be avoided if two out of the three processors (P_1 , P_2 , and P_3) provide correct checkpoints. If not, the system needs to roll back two intervals. The rollback distance is two in this case.

2.2 RFC Scheme

It is similar to DMR-F, but uses only one additional processor when there is no match out of two checkpoints in the duplex system[9]. Between two processors P_a and P_b , suppose Processor P_b fails during Interval I_j . When there is no match between the checkpoint P_a and P_b because of the failure of P_b , the spare processor, P_s , is initiated to identify the fault-free processor. If P_s works correctly, the checkpoint of P_a and that of P_s will match after I_j . Since P_a is identified as the fault-free one, the checkpoint of P_a after Interval I_{j+1} is copied to P_b for further execution. Note that one more validation is needed in this scheme because the operation of P_a during Interval I_{j+1} has not yet been verified. P_s re-executes that operation while P_a and P_b continue the operation during Interval I_{j+2} . If the checkpoint of P_s after Interval I_{j+1} is identical to that of P_a , recovery is done without rollback. Otherwise, rollback recovery can not be avoided. Therefore, in RFC scheme, rollback can be avoided if at least two out of the three processors (P_a , P_b , and P_s) work correctly during Interval I_j and both of the two processors (P_a and P_s in this example) succeed for the operation during Interval I_{j+1} . In other words, RFC scheme can avoid the rollback when only a single processor fails within two consecutive intervals. Otherwise, the system rolls back two intervals.

2.3 DST Scheme

This scheme assumes the existence of a self-tester inside the processor since typical coarse grain processors contain built-in self-test facilities[10]. As other roll-forward schemes, the checkpoints of two processors, CP_A and CP_B , are periodically compared in the scheme. When the two checkpoints mismatch, the outcomes of the self-testers are compared. If the self-tester of a processor, for example Processor- A , identifies a fault, CP_B is copied to Processor- A assuming that CP_B is correct. Then the task caused the mismatch is executed again in both processors as a *background process* to verify the correctness of CP_B while

both processors continue the original computation (lookahead execution). If any background process produces the same CP_B , both processors continue the computation and thus a rollback can be avoided. If it does not, which means that Processor- B or the background process may not be good, a rollback is required to the last committed checkpoint prior to CP_B , since the correctness of CP_B can not be guaranteed. Also, if both self-testers do not identify any fault even though the two checkpoints mismatch, a rollback recovery can not be avoided. The rollback is also required if both of them identify the faults. The rollback distance, if required, is the response time of the background process plus one checkpoint interval.

3 Analytical Models

Many researchers have developed analytical models for evaluation of rollback recovery approach. In this section, we develop a general analytical model to evaluate the relative response time for roll-forward recovery approaches. The model is then applied to DMR-F, RFC, and DST scheme to show the feasibility. The variables which will be used for the modeling is introduced first.

3.1 Variables

- f : processor failure rate.
- ρ : utilization of a processor.
- P_{mf} : probability that a task migration occurs and the validation task fails.
- P_{ms} : probability that a task migration occurs and the validation task succeeds.
- P_m : probability that a task migration occurs. Then $P_m = P_{mf} + P_{ms}$.
- f_m : task migration overhead factor.
- c : error detection coverage of a self-tester.
- P_f : probability that a processor fails in one interval.
- T_I : relative expected execution time.
- P_r : rollback probability.
- P_{r1} : probability of an unit distance rollback in DST scheme.
- P_{r2} : probability of a multiple distance rollback in DST scheme.
- D : rollback distance.

3.2 Analytical Model

The relative response time, T_I , is the ratio of the expected execution time to the checkpoint interval, T . If it is close to one, the execution time will be close to the error-free execution time, demonstrating the effectiveness of forward recovery. Assume that each processor has a constant probability of failure, P_f . It is also assumed that a failure can occur during recovery, and the time to make and compare checkpoints and other overhead such as restart time are negligible. The following theorems develop the analytical models for obtaining T_I 's of various roll-forward recovery schemes.

Theorem 1: A general analytical model for T_I is

$$T_I = 1 + \frac{P_{ms}}{1 - P_r} f_m + \frac{P_r}{1 - P_r} (D + f_m)$$

Proof: The relative idle time due to a task migration is f_m , since T_I is defined as a ratio of the checkpoint interval. If no rollback occurs, $T_I=1$ if no task migration occurs, or $T_I = 1 + f_m$ if a task migration occurs and the validation succeeds. The conditional probability that the task migration occurs and the validation succeeds given that no rollback occurs is $\frac{P_{ms}}{1-P_r}$. Then $T_I = (1 - \frac{P_{ms}}{1-P_r})1 + \frac{P_{ms}}{1-P_r}(1 + T_{rm}) = 1 + \frac{P_{ms}}{1-P_r}T_{rm}$ for the case that no rollback occurs. If a rollback occurs once, the expected execution time is the execution time of D intervals which was lost, the idle time due to the task migration, and the time spent to recover the original failed task which might involve a task migration. Therefore, $T_I = D + f_m + 1 + \frac{P_{ms}}{1-P_r}f_m$ for the case. Since rollbacks can occur recursively during recovery, $T_I = 1 + \frac{P_{ms}}{1-P_r}f_m + \frac{P_r}{1-P_r}(D + f_m)$.

Theorem 2: For RFC scheme,

$$T_I = 1 + \frac{P_{ms}}{1 - P_r} f_m + \frac{P_r}{1 - P_r} (2 + f_m)$$

where $P_{ms} = 2P_f - 8P_f^2 + 12P_f^3 - 8P_f^4 + 2P_f^5$, $P_r = 7P_f^2 - 12P_f^3 + 8P_f^4 - 2P_f^5$.

Proof: The system employing the RFC scheme rolls back if any one of the following conditions is held; i) two processors fail, ii) one of the two processor fails and the spare processor fails and iii) one of the two processors fails and the spare processor succeeds but one or both of the fault-free and spare processors fail for the operations during the successive interval. Therefore $P_r = P_f^2 + 2P_f(1 - P_f)P_f + 2P_f(1 - P_f)(1 - P_f)(P_f^2 + 2P_f(1 - P_f)) = 7P_f^2 - 12P_f^3 + 8P_f^4 - 2P_f^5$. The task migration occurs and the validation succeeds when one of the two processors in the duplex system fails, the other one succeeds for two consecutive intervals, and that the validation task succeeds for two consecutive intervals. Thus, $P_{ms} = 2P_f(1 - P_f)^4 = 2P_f - 8P_f^2 + 12P_f^3 - 8P_f^4 + 2P_f^5$ while $D = 2$ since the rollback distance is two. Using Theorem 1, the equation is obtained.

Theorem 3: For DMR-F scheme, $P_{ms} = 2P_f - 4P_f^2 + 2P_f^3$, $P_r = 3P_f^2 - 2P_f^3$, and $D = 2$.

Proof: A task migration occurs and the validation succeeds if either one of the two processes in the original duplex system fails and the validation task on the spare processor succeeds. Thus, $P_{ms} = 2P_f(1 - P_f)^2 = 2P_f - 4P_f^2 + 2P_f^3$. The system rolls back if the validation task fails, or both of the two processes in the duplex system have already failed. $P_r = 2P_f(1 - P_f)P_f + P_f^2 = 3P_f^2 - 2P_f^3$ and $D = 2$ since the rollback distance is two.

Using Theorem 1 and 3, T_I for DMR-F scheme can be obtained.

Theorem 4: For DST scheme,

$$T_I = 1 + \frac{P_{r1}}{1 - P_{r1}} + \frac{P_{r2}}{1 - P_{r2}} \frac{1}{1 - \rho}$$

where $P_{r1} = 2P_f - 2cP_f - P_f^2 + 2c^2P_f^2$ and $P_{r2} = 2cP_f^2 - 2c^2P_f^2 + 2cP_f^3 - 2cP_f^4$.

Proof: The lost time for one unit distance rollback is one interval while that for one multiple distance rollback is $1 + \frac{\rho}{1-\rho} = \frac{1}{1-\rho}$. Thus, $T_I = 1 + \frac{P_{r1}}{1-P_{r1}} + \frac{P_{r2}}{1-P_{r2}} \frac{1}{1-\rho}$.

3.3 Case Study

Here we study an example to compare the relative response time of systems employing different checkpoint schemes using the analytical models developed in this section.

Example: Consider a system assuming exponential failure with the rate of $P_f = 10^{-3}$. The task migration overhead factor and error detection coverage are varied as parameters.

Using the analytical model developed in this section, we could evaluate the performance of systems employing various checkpoint schemes as shown in Table. 1. Table. 1 shows the relative response time of DMR-F, RFC, and DST scheme for various values of f_m and c when $P_f = 10^{-3}$ and $\rho = 75\%$.

Table 1. Comparison of roll-forward scheme in terms of T_I

f_m	RFC	DMR-F	c	DST
0.0	1.000014	1.000006	0.0	1.002003
0.1	1.000214	1.000206	0.1	1.001803
0.2	1.000414	1.000406	0.2	1.001603
0.3	1.000614	1.000606	0.3	1.001403
0.4	1.000814	1.000806	0.4	1.001203
0.5	1.001013	1.001005	0.5	1.001003
0.6	1.001213	1.001205	0.6	1.000802
0.7	1.001413	1.001405	0.7	1.000602
0.8	1.001613	1.001605	0.8	1.000402
0.9	1.001813	1.001805	0.9	1.000201
1.0	1.002013	1.002005	1.0	1.000001

4 Conclusion

While numerous checkpoint schemes have been proposed in the literature for decades, the lack of general analytical models has been an obstacle to compare the performance of systems employing different checkpoint schemes. The paper has developed a general model which can be applied to systems with various checkpoint schemes. After the development, the model is applied to evaluate the

relative response time of systems employing RFC, DMR-F, and DST schemes as a case study. The result shows that the model developed in the paper can be used effectively for the evaluation.

References

1. Park, G.-L., Youn, H. Y., Choo, H.-S.: Optimal Checkpoint Analysis Using Stochastic Petri Net. *IEEE Pacific Rim Int. Symp. Dependable Computing* (2001) 57-60
2. Baldoni, R., Helary, J. M., Raynal, M.: Rollback-dependency trackability: A Minimal Characterization and Its Protocol. *Inform. and Comput.* (2001)
3. Gao, G., Singhal, M.: Mutable Checkpoints: A New Checkpointing Approach for Mobile Computing Systems. *IEEE Trans. Parallel Dist. Syst.*, 12(2) (2001) 157-172
4. Rao, S., Alvisi, L., Vin, H. M.: The Cost of Recovery in Message logging Protocols. *IEEE Trans. Knowledge Data Eng.*, 12(2) (2000) 160-173
5. Long, J., Fuchs, W. K., Abraham, J. A.: Compiler-Assisted Static Checkpoint Insertion. *22nd Int. Symp. Fault-Tolerant Computing* (1992) 58-65
6. Gray, J.: Why do computers stop and what can be done about it. *5th Symp. Reliability in Dist. Software and Database Syst.* (1986) 3-12
7. Park, G.-L., Youn, H. Y.: A New Approach for High Performance Computing Systems with Various Checkpointing Schemes. *Journal of Supercomputing*, Vol. 33 (2005) 65-78
8. Long, J., Fuchs, W. K., Abraham, J. A.: Forward Recovery Using Checkpointing in Parallel Systems. *Proc. Int. Conf. Parallel Proc.* (1990) 272-275
9. Pradhan, D. K., Vaidya, N. H.: Roll-forward Checkpoint Scheme: Concurrent Retry with Nondedicated Spares. *Proc. of 1992 IEEE Workshop on Fault-Tolerant Parallel and Dist. Syst.* (1992) 166-174
10. Park, G.-L., Youn, H. Y., Shirazi, B.: Duplex with Self-Test: A Roll Forward Checkpoint Scheme for High Performance Computing. *High Performance Comp. Symp.* (1996) 314-319

A Purely Distributed Approach for Coupling Scientific and Engineering Applications

Vicente Berbegall¹, L.A. Drummond³, Gumersindo Verdu¹, and Vicente Vidal²

¹ Department of Chemical and Nuclear Engineering, Polytechnic University of Valencia
{vibergeri, gverdu}@iqn.upv.es

² Department of Computer Systems and Computation, Polytechnic University of Valencia
vvidal@dsic.upv.es
46022 Camino de Vera s/n, Valencia, Spain

³ Lawrence Berkeley National Laboratory, Computational Research Division,
94720 One Cyclotron Road, MS 50F 1650, Berkeley, CA
LADrummond@lbl.gov

Abstract. In recent years, developments in computational sciences have enabled scientists to create sophisticated software tools and techniques that have contributed to the development of high accuracy numerical models that are used to study physical phenomena. The next level of sophistication addresses the integration or coupling of one or more computational models to simulate a more complex physical system. These coupled systems, are generally multidisciplinary in nature and are now emerge in a broad spectrum of fields in science and engineering such are Earth Sciences, Fusion Energy, Structural Engineering and Astrophysics. This paper presents an introduction to the Distributed Coupling Toolkit (DCT). This library tool provides a user friendly and scalable approach to formulate model coupling in distributed computer environments.

1 Introduction

Many physical systems and phenomena in science and engineering are studied through a mathematical formulation that depicts the complex interactions between multiple physical components. For examples, climate models use formulations to characterize different cloud formations and atmospheric phenomena, as well as formulations to study interactions between the different layers in the atmosphere with the oceans at different spatial and time scales.

In the past two decades, the number of computational science fields that are paying attention to the coupling of numerical models has significantly increased. Originally, to couple two distinct, code-wise, models, a scientist will use data files to write out the output from one model that would be read as input conditions or parameters by a second model. With the emerging high-end computer technology, the data exchanges have been handled through software tools referred as couplers.

Nowadays, couplers ([1],[2] and [3]) use a form of message passing system to handle data exchanges between models, and in some cases the couplers have been designed and implemented to work in a specific scientific or engineering field. The Distributed Coupling Toolkit, DCT, is a coupler that provides a flexible and general-purpose approach to coupling numerical models. It minimizes the number of intrusive

lines from one model into the other and works in a purely distributed manner. Thus there is no need to centralize the exchange of data in a single processor but rather DCT parallelizes the data exchanges.

In this paper, we present basic design and functionality of DCT and highlight the advantages of enabling scientists and engineers to couple scientific applications in a distributed, scalable and flexible manner. We begin in Section 2 with a general definition of the coupling problem and issues of handling it centralized vs. distributed. In Section 3, we generally describe the DCT interface, and in Section 4, we model the performance of a centralized vs. a distributed coupling approach. Conclusions and future plans are presented in Section 5.

2 Design of a Distributed Coupling System

Without lost of generality, let us try to state a general basic formulation of the coupling problem, and we begin with a 2-model coupling formulation that can be generalized to any coupled multisystem involving more than two models. For the latter case we can construct a coupled system as a collection of one or more 2-model couplings between the independent models.

Let us take a *Model_A* and *Model_B*, such that each model has a set of input variables or fluxes and a set of output variables and fluxes. Back to the climate example, these variables and fluxes are data representations inside the numerical models of quantities like 3-dimensional velocities, energy and water fluxes, 2-dimensional sea surface temperature, etc. Henceforth, we will use the term variable to refer to either variables or fluxes and the DCT handling and implementation of each will become clearer in the next section. The set of input variables of *Model_A* are given by the set:

$$X = \{x_1, x_2, \dots, x_n\} \tag{1}$$

And output variables are given by the set:

$$Y = \{y_1, y_2, \dots, y_m\} \tag{2}$$

Considering that the computational model is at a given state t , in time, and each of the variables has been properly discretized and represented in the model's computational grid, we can rewrite the sets as

$$X(t) = \{x_1(t), x_2(t), \dots, x_n(t)\} \text{ and } Y(t) = \{y_1(t), y_2(t), \dots, y_m(t)\} \tag{3}$$

respectively, where every $x_i(t)$ and $y_i(t)$ represents the value of the variable at the model simulation time t .

Similarly, for *Model_B* there is a set of input variables $W(t) = \{w_1(t), w_2(t), \dots, w_r(t)\}$ and $Z(t) = \{z_1(t), z_2(t), \dots, z_s(t)\}$.

Coupling *Model_A* and *Model_B* can be understood as an insertion of one or more output variables from one model to the input set of the other one. Thus, we have

$$y_i(t) \Rightarrow w_j(t) \text{ and } z_k(t) \Rightarrow x_l(t) \tag{4}$$

For both equations on (4), the \Rightarrow denotes a data transformation from the domain of one model to the other one. Typically, these data transformations involve unit conversions, spatial domain interpolations or more generally adjustment of a data quantity represented in the grid of one model to the grid representation of the other model. Notice, in coupling *Model_A* and *Model_B*, there is only a subset of the output and input variables that are exchanged between the models, and there are many cases to consider for instance only *Model_A* insert data to *Model_B*, or vice versa, or a case where both models exchange data at different times and in both directions. In general, in DCT we refer to the model that sends the data as the **producer** and the receiver as the **consumer**.

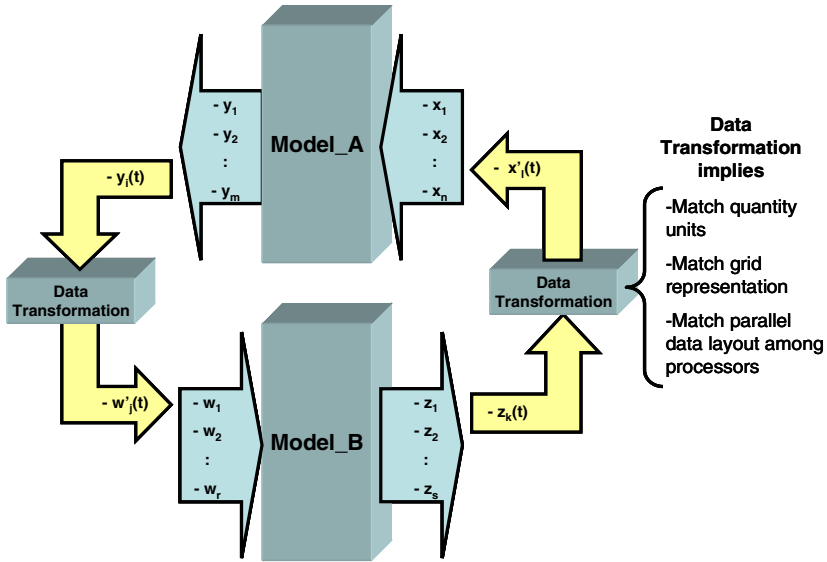


Fig. 1. Schema of coupling between *Model_A* and *Model_B*

A simple example is depicted in Figure 1, primed variables, w' and x' , represent the coupled variables after transformation. The source values for these variables are the variables y and z , respectively. Therefore, the data produced by one of the models is converted as input of the other model at every coupling time, and we have to first identify the matching domain or physical coupling interface area. This area is defined as the spatial domain covered by one model and the intersecting spatial domain covered by the other (see Figure 2). In the climate example, one could think of these as being a geographical region of intersecting domains between the models. In this case, the intersection of these geographical regions is determined by their longitude-latitude coordinates.

After determine the domain intersections, we have to adapt or transform the data output from one model to fit the other models demands. This step usually requires the insertion of intrusive code from one model into the other, because the modeler tries to convert the units and grid representations from one model to the input requirements of

the other model. This data transformation involves unit conversions (e.g., degrees centigrade to Kelvin, kilometers per hour to miles per hour, etc.) and interpolations or extrapolations (e.g. from simple linear interpolations to high-order interpolation schemes). DCT eliminates this by using a meta registration process and facilitating a library of subroutines to automatically carry a predefined set of unit conversions and data interpolation routines.

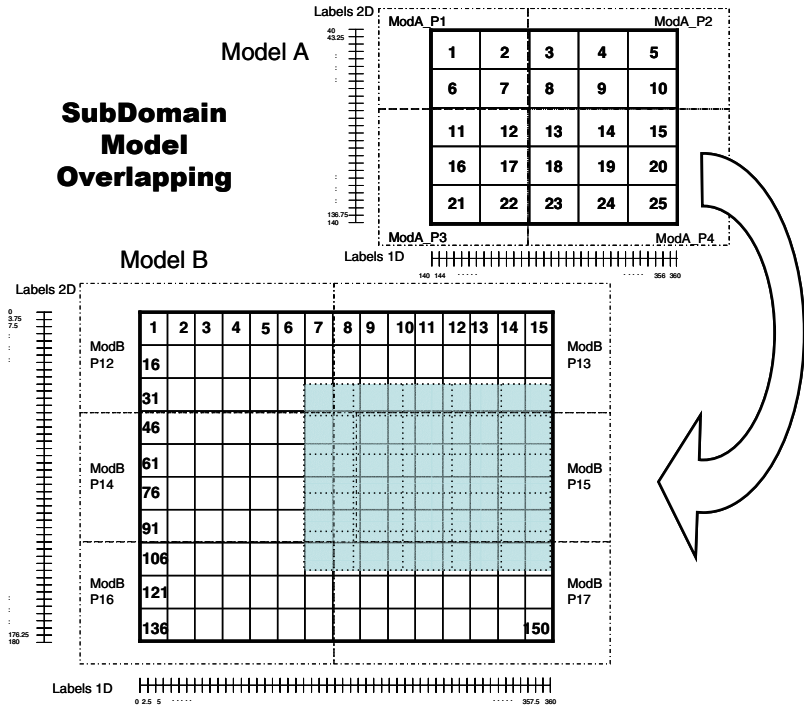


Fig. 2. Subdomain division and overlapping of Model_A and Model_B

Now, consider the case that Model_A and Model_B are to be executed in a distributed environment. Here, we assumed that the parallelization of each model is completely independent, this is, they run on a different number of processors and use different processor data layout strategies. Further, in this scenario we also consider the case that one or both of the models are sequential. DCT provides a registration interface in which users specified the parallel data layout of every model in the system, and it automatically devices a communication scheme that is used at every time coupling operation.

This is, at registration a user defines the variables to be exchanged, their units and domains of operation in a model, and at exchange time each processor has enough information to handle the data exchanges with its counterparts in the other models. This defines what is unique of the DCT coupler with respect to many other coupling tools available today.

Lastly, DCT does not provide a mechanism for managing the execution of neither processes nor defining parallel data layouts. Thus it avoids the existence of a centralized control implemented through a dedicated processor. DCT allows users to provide information about the parallel decomposition used when coding their models and after the registration it makes sure that every processor actively involved in the coupling has enough information to proceed without a central agent.

3 Distributed Coupling Toolkit for Multi-component Systems

At the core of the tasks of couple different models, we find the problem of managing the accurately and efficiently the data exchanges between the different computational models. These tasks require not only scientific understanding of the models being coupled and the algorithmic formulations of the coupling to be performed, but also the efficient and robust computer implementation of algorithms to carry out the data transportation and transformation between scientific codes.

Among the main coupling challenges addressed by DCT are management of different dimensionalities, time scales, resolutions, computational domains, and numerical formulations. And in summary, DCT provides functionality to handle:

(1) Coupling of numerical models that use different time and spatial domains, (2) Numerical models that were discretized using different techniques and grid representations, (3) Accuracy of data transformations are determined by the needs of the coupled system, (4) In a distributed environment, models have been parallelized independently using different data layout and distribution among a number of processors, (5) The number of processors assigned to one model is not fixed. Thus, a model can run with different data layout configurations depending on the number of processors assigned to it or perhaps the computational environment where it is being run.

If we take a look at the literature about coupling tools for multicomponent applications, we find numerous solutions and implementations to address these issues. There are a number of coupling tools [1], [2], and [3] for which the coupling formulation has been expressed through centralized computations, centralized data conversations/translations and main coupling control. However, this coupling formulation offers little flexibility, precludes dynamic coupling, and introduces computational bottlenecks at synchronization points and control. Moreover, changes to coupling formulations, coupled model components and parameters will result in major changes to the codes. In Figure 3 we can see two schemes of the communication between coupled models in a centralized manner.

Early work in distributed coupling [4] and [5], supported the coupling of an earth system model proved to effectively reduce the synchronization time and eliminated the need for reconstructing an entire computational domain from one model into the other. So, in this direction, we have decided to expand the distributed coupling to facilitate the coupling of many other scientific applications. DCT provides a bag of services to perform data translations, handle data representation and communication in an optimal and distributed manner.

The coupling formulation using the DCT requires mainly two steps; an initial registration step and consequent data exchange steps.

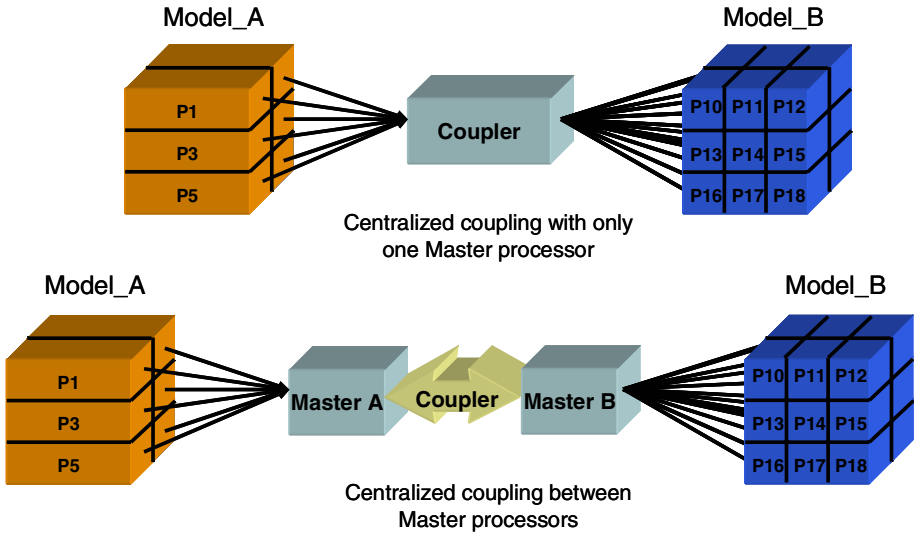


Fig. 3. Schemes of centralized coupling between two models

3.1 Registration

In the registration step, as its name indicates, the user provides DCT with all information related to coupling, definition of model variables to be exchanged, model spatial domains, model starting times, data exchange intervals, selection of data transformation routines to be used. Internally, DCT builds a metadata around the models, variables to be exchanged, and the coupling formulations. After the registration step, the metadata contain enough information to handle a purely distributed coupling, this is an M processor to N processor communication.

The first step of the coupling formulation is the registration, and this is handled through call DCT's interface to a collection of routines and structures that handle the model and variables information. The resulting metadata is embedded in several types and structures designed explicitly for the DCT and consist of many basic C Language structures.

In order to define the variables to be coupled, we count with `DCT_Field`, `DCT_3d_Var` and `DCT_4d_Var`. These DCT types wrap around the user data structures containing the actual model data. The users structures are basic language type structures (like real, complex, double, etc). Similarly, we provide the `DCT_Model` type to define the computational models or applications to be coupled. In this data type is possible to register the spatial domain, number of processors, description of the processor and data layout, initial model time, size of model's time step, list of variables to be consumed or produced, and other information for DCT internal handling.

Another DCT structure type is `DCT_Coupler`, which defines the coupling between two models. There can be more than one variable of this type, thus DCT can handle a more complex integration of one or more pairs of couplings. `DCT_Coupler` contains the frequencies in which the variables are to be exchanged. When a model's variable

is declared inside a DCT_Coupler structure, a match is made with another variable in the counterpart model. Therefore, an interpolation routine is assigned by default to handle the spatial data transformations. However, the user can change this behavior by specifying the transformation routine to use.

Only during the registration step, DCT uses a control process, which can be any of the processors taking part in the parallel-coupled model execution. The controller processor is refer here as the “Broker”. The Broker collects all the information being registered by all the other models. And uses this information to form sub-domain information that later allows the direct processor to processor data exchanges without a controller or master slave approach. Internally DCT uses a data type, DCT_Subdomain, which is formed of a small set of indices to the users data and is used for handling the parallel data exchanges. This data structure is for internal use by DCT routines only and it is transparent to the user. The subdomain concept is what allows DCT to exchange data in parallel and without the intervention of a centralized mechanism. Figure 4 presents an example.

The registration step begins with the identification of a process or a task as Broker with a call to the DCT_Register_Broker routine. There is only one Broker per coupled run and this task only exists during the registration step. So, it is important to emphasize a couple of points. First, the Broker coordinates the entire registration process,

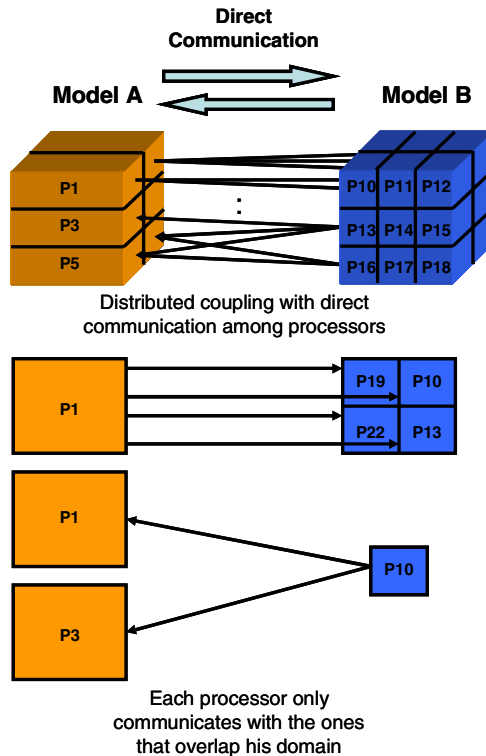


Fig. 4. Schemes of communication in distributed coupled system which consists of two models

and it receives information being registered by other models at this step. Second, after the registration step the process charged with the Broker role can work in other tasks inside one of the models being coupled, thus a process is never idle waiting for data transfer to handle as in other coupler toolkits.

In addition, each model must identify a Master processor at registration time. Each Master process is responsible for registering DCT metadata related to its own model. This information includes grid resolution, number of processes, data layout, and frequency of production or consumption, model's domain, etc. Generally, the Broker is the Master processor for one of the models. The Broker collects information at Registration time. Then, the Broker processes this information to match producers against consumers. Taking into account all the information provided by the DCT metadata (like different domains, grid resolution, number of processes, and frequencies of production and consumption), the Broker is able to resolve the relations among the different applications.

The registration step ends with a call to `DCT_Register_End`. All processes participating in the coupling have to call this routine as well as the corresponding `DCT_Register_Begin`. The Broker estimates the subdomains dependencies and returns to every process a list of subdomains and processes that it needs to exchange data with. As a result, every participating process in the coupling has enough information to send and receive data from its peers without the need of a centralized entity regulating the exchanges of information.

3.2 Communication

Mostly all the computational models have a time dependent integration loop, or time step. In which one simulates a step of the physical phenomena. That is, after an initialization step, that in the DCT context includes the register step, the models enter in a sort of iterative algorithm, in which the output variables are produced.

So, after the registration stage, the user is responsible to insert at strategic locations the calls to the communication routines, `DCT_Send_Data` and `DCT_Get_Data`. The position of these routines requires sound understanding of the application codes involved in the coupling.

Depending on configuration from the registration step, we will count with a frequency or coupling period that we can check with a simple "if" statement to execute a communication routine. The `DCT_Send_Data` operation will manage the transfer of data from a processing element to the buffer of the consumer processing element(s). This operation will transparently send data to one or more recipients or store data into a disk. Similarly, a `DCT_Get_Data` will retrieve data sent to a processing element and will transparently perform the necessary data transformations to serve the request of the processing element.

4 Performance Analysis: Centralized vs. Distributed Coupling

We now compare a model performance of the DCT vs. a general centralized approach. In the centralized approach we assume that every processor has to communicate to a master, recreate the full domain and then send it to its counter-part master

processor in the other model. At the other end, the received data needs to be transformed and redistributed to each individual process. In DCT, the registration process computes indexes to the data that are later distributed to all processes, along with information to automate the data exchanges between processes. Definitions:

v_1 = number of processes in model 1

v_2 = number of processes in model 2

τ_g = time spent gathering information from sub-domains to build a global domain

τ_s = time spent scattering information from global domain to sub-domains

τ_t = time spent translating the data from one model's global domain to the other model's domain

We now assume that:

- There is one sub-domain per computational process
- The communication bandwidth and latency are known

$$\tau_g = O_g + \sum_{i=1}^v C_i \text{ and } \tau_s = O_s + \sum_{i=1}^v C_i \quad (5)$$

Where, C_i denotes de communication between the control processor and the process- i . O_g and O_s refer to the overhead incurred while gathering or scattering, respectively, the data. These values are linear dependent of the number of processes in the system. Notice that in the distributed case, τ_g and τ_s are much smaller because there is only need to gather data from nearest neighbors. Likewise, τ_t is also smaller for the distributed case because there are fewer points to be translated. In addition, τ_t , in the centralized case, represents idle time for the remaining $v - 1$ nodes. The total expected time for the data distribution is:

$$\tau_{cent} = \tau_g + \tau_s + \tau_t \quad (6)$$

for the centralized data Brokerage and,

$$\tau_{dct} = \text{MAX} \left| \tau_{gi} + \tau_{si} + \tau_{ti} \right|_{i=1, \dots, v} \quad (7)$$

for the Distributed Coupled Toolkit

Thus, T_{cent} is always greater or equal T_{dct} .

5 Conclusions

We are currently working with an atmospheric code coupled to an oceanic code in order to check the operational performance of the group.

DCT provides a very flexible mechanism to formulate complex coupling scenarios. Among the advantages are performance scalability as well as problem scalability. Normally, in centralized coupling approaching the user is limited to the reproduction of a grid by the size of the memory available in one processor, namely the controller processor, thus making it difficult to scale the problem, for instance work with a finer spatial resolution of the model.

With today's emerging technology, it is vital to have independence between the model's data layout, the number of available processors to run a given coupled model, and the variables that are exchanged between the models. DCT provides a very flexible way to integrate all these variables parameters into the coupling paradigm without overwhelming the application scientist or engineer.

References

1. Larson, Jacob, Ong.: The Model Coupling Toolkit: A New Fortran90 Toolkit for Building Multiphysics Parallel Coupled Models. *I. J. High Perf. Comp. App.*, 19(3) (2005) 277-292
2. Chris Hill, Cecelia DeLuca, V. Balaji, Max Suarez, Arlindo da Silva, and the ESMF Joint Specification Team.: The Architecture of the Earth System Modeling Framework. *Computing in Science and Engineering*, Volume 6 Number 1 (2004)
3. Valcke S., E. Guilyardi, C. Larsson.: PRISM and ENES: A European approach to Earth system modelling. *Concurrency and Computation: Practice and Experience*, Volume 17 (2005) 1-16
4. L. A. Drummond, C. R. Mechoso, J. Demmel, K. Sklower, and H. Robinson.: Data Broker for Distributed Computing Environments. *Lecture Notes in Computer Sciences, LNCS2073* (2001) 31-40
5. L. A. Drummond, J. D. Farrara, C. R. Mechoso, J. A. Spahr, J. Demmel, K. Sklower, and H. Robinson.: An Earth System Model for MPP environments. Issues in coupling components with different complexities. In *Proceedings from High Performance Computing 1999, Grand Challenges in Computer Simulation* (1999) 123-127

A Monitoring and Visualization Tool and Its Application for a Network Enabled Server Platform*

Raphael Bolze¹, Eddy Caron¹, Frederic Desprez¹,
Georg Hoesch², and Cyril Pontvieux³

¹ LIP, ENS Lyon, F-69364 Lyon Cedex 07

Raphael.Bolze@ens-lyon.fr

² TU München, LRR, Boltzmannstr. 3, D-85748 Garching bei München

³ IUP informatique, UFR-ST, 16 route de Gray, F-25030 Besançon Cedex

Abstract. Monitoring grid platforms has recently gained a wide interest. This kind of platform highly distributed across different domains leads to several design and implementation problems. We have designed a new monitoring platform and visualization tool adapted for Network Enabled Server systems. This environment, highly tunable for different middleware platform has been successfully validated on the DIET platform. In this paper, we present its architecture and main features as well as details of the validation on the DIET environment and experimental results on a large scale grid platform.

1 Introduction

Understanding the behavior of distributed applications is indeed a difficult task. Grid computing adds another level of difficulty with heterogeneous sets of computers distributed over the network in different administrative domains. However, grid computing middleware developers face this problem daily to optimize the performance of their applications.

We have designed a complete monitoring system based on an hierarchical object-oriented approach. This model and its implementation are generic and have been validated it on our DIET environment. The first target environment to be monitored belongs to the Network Enabled Servers [9] class. These environments like NetSolve [2], Ninf [10], or DIET [4] are built upon sets of servers that solve computational requests on behalf of clients. These clients first send their requests to a agent (meta-scheduler) that has to find a server using performance metrics. Agents can be distributed to improve the scalability of the system. This kind of highly distributed platform needs a scalable and efficient monitoring software to understand its behavior.

A lot of work has been produced recently around grid platform monitoring [11] and a attempt of standardisation has started within the Global Grid Forum.

* This work was supported in part by the ACI GRID, the RNTL, and the GRID5000 projects of the french department of research.

Most of the existing platform are highly tuned for specific grid environments. Around monitoring of Network Enabled Server systems, few work has been produced. The closest environment is *visPerf* [6] developed around NetSolve at the University of Tennessee.

In the rest of the paper, we first introduce the overall architecture and concepts around our tool (Section 2). In the third section, we present an application to a Network Enabled Server system developed in our team called DIET (Section 3). And finally, before a conclusion and future work, we describe the cost model of our monitoring environment and some experimental results that show its small overhead.

2 Visualization of a Distributed Platform: VizTool

In this section, we discuss the basic functionality of a monitoring system. We first define the model provide for tools that needs to be monitored in distributed environments. Then we present the associate service that enable us to be aware of events that happened in a distributed environment.

2.1 Simple Model for a Distributed Environment: VizTool Model

To be general and to provide for developer the freedom of defining his/her own platform, the basic properties and methods needed to monitor a distributed environment are defined. The main goal of a monitoring tool is to gather all events happened in this environment. An event is the first atomic object. It characterizes a simple message sent by a component to notify an action or a modification. *LogEvent* is defined as this atomic event that happened in a distributed platform. This object has three main attributes: **componentName** gives the name of the component which is responsible of this event; **time** gives the time when this event happened, and **message** describes the event.

Then we define an object which represents a concatenation of two linked events in the platform. In distributed environments, an event is often followed by another event which is the response. In Network Enabled Server (NES) environments, these two linked events are called a *Request*: one event informs of the start of an action, and another event informs of its end. To be able to know if these two events are linked, we need to identify them by an unique number called the *request_id*. A *Request* has four main attributes: **request_id** identifies a request, **beginTime**, **endTime**, **status** gives the state of the *Request*. Four basic states have been defined: **CREATED** no information of begin or end time are available; **PROCESSING** the request has been created and the begin time is known; **DONE**: begin and end time of the request are known; **AMBIGUOUS**: the request has been created and only the end time is known. As components are distributed, there are some cases where a request has finished before being informed that it has began.

After modeling the activity of the platform, we need an object that manages all requests coming from different components of the platform: *ElementStats*. *ElementStats* stores all **DONE** requests in a vector. This class provides two basic functions. The **addRequest** method stores a requests in the vector if request has

DONE status else the request is stored in a buffer. The `findRequest` method finds a request with its `request_id`. This `ElementStats` object is a member of a more general object called `Element` which models a component of the distributed environment. The `Element` object can have several properties, but we do not define any other property to this object except his name. For example, an element can model a processor, but it can also model a server, or a cluster depends on the different levels of abstraction. This approach gives the developer the opportunity to model and monitor with the granularity needed. Finally the `vizTool` model of the distributed environment is very simple and consists of four main classes (Figure 1): **Element** with two basic attributes: `elStats` and `name`. **ElementStats** models the activities of an element. It contains methods to obtain statistical information based on a `requests` object. **Request** object takes into account events that happened to the element, `Requests` objects are stored in `elStats` objects. **LogEvent** is the basic event in the distributed platform. It represents all atomic messages sent by all components and two linked `LogEvent` defines `Request`.

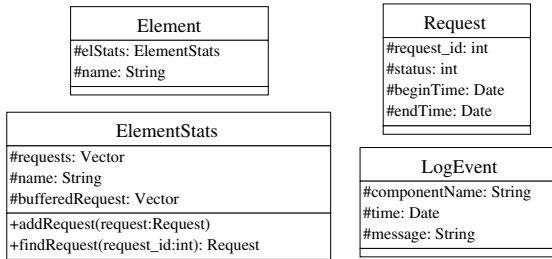


Fig. 1. Model of a monitoring tool

Indeed this model is very general, and it needs to be tuned to the specific environment we want to monitor. However it gives a framework and a common base to monitor the distributed environment. We will discuss in next section how to re-use and adapt the `vizTool` model for one specific distributed environment.

2.2 Event Monitoring: LogService

An event monitoring system called `LogService` [7] has been designed. This monitoring service offers the capability to be aware of information that need to be gathered from a distributed platform. The communication layer of `LogService` is based on Corba technology. `LogComponent` attaches to a component and relays information and messages to `logCentral`. `LogCentral` collects messages received from `LogComponents`, then it stores or sends these messages to `LogTools`. `LogTools` connect themselves to `logCentral` and wait for messages. The main interest in `LogService` is that information are collected by a central point `logCentral` that receives `logEvents` from `LogComponents` that are attached to the component that you want to monitor. The `logCentral` offers the possibility to re-send this

information to several tools (*LogTools*) which are responsible for analyzing these messages and offering a comprehensive information to the user.

LogService defines and implements several functionalities.

Filtering mechanisms are used to reduce the number of messages sent. In order to decide which messages are required by a tool. The tools have to declare their filter to the monitor (*logCentral*).

Event ordering is another important feature of a monitoring system. LogService handles this problem by the introduction of a global time line. When created, each message receives a time-stamp. The problem that can occur is that the system time can be different on each host. LogService measures this difference internally and corrects the time-stamps of incoming messages accordingly. The time difference is corrected using the time stamp of the last ping that *logCentral* sent to *LogComponent*. However, incoming messages are still unsorted. Thus, the messages are buffered for a short period of time in order to deliver a sorted stream of messages to the tools. Messages that arrive out of order within this time are sorted in the buffer and can be properly delivered. Although this induces a delivery-delay for messages, this mechanism guarantees the proper ordering of messages. As tools usually do not rely on true real-time delivery of messages this short delay is acceptable.

Dynamic system state: Components may connect and disconnect at runtime. A problem that arises in distributed environments is the state of the application. This state may for example contain information on connected servers, their relationships, the active tasks, and many other pieces of information that depend on the application. The system state can be constructed from all events that occurred in the application. Some tools rely on this state to work properly. The problem appears if those specific tools do not receive all messages. This might occur as tools can connect to the monitor after the application has been started. In fact, this is quite probable as the lifetime of the distributed application can be much longer than the lifetime of a tool. As a consequence, the system state must be maintained and stored. In order to maintain a system state in a general way, LogService does not store the system state itself, but all messages which are required to construct it. These messages are identified by their tag and stored in a special list. This list is forwarded to each tool connected. This process is transparent for the tool since it simply receives a number of messages that represent the state of the application. In order to further refine this concept, the list of important messages is also cleaned up by LogService. After a disconnection of a component the respective information is no longer relevant for the system state. Therefore, all messages sent by this component is removed from the list.

3 VizTool for DIET: VizDIET

3.1 DIET Architecture

DIET (Distributed Interactive Engineering Toolbox) [5, 4, 3] is a set of hierarchical components to design Network Enabled Server systems over the grid. These

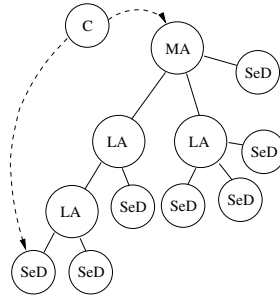


Fig. 2. DIET hierarchical organization

systems are built upon servers managed through distributed scheduling agents. Clients ask these scheduling components to find available servers (using some performance metrics and information about the location of data already on the network). The DIET architecture has been designed following a hierarchical approach. Thus it provides good scalability and can take into account physical network constraints. DIET is based on several components. First a **Client** is an application that uses DIET to solve problems in a RPC mode. The scheduler is scattered across a hierarchy of *Agents*. This hierarchy is made of one **Master Agent (MA)** and several **Local Agents (LA)**. Figure 2 shows a hierarchy built upon several DIET components. A **Master Agent** is the entry point of our environment and thus receives computation requests from clients attached to it. These requests refer to some DIET problems that can be solved by registered servers. A client can be connected to a MA by a specific name server or a web page which stores the various MA locations. The client asks the MA to find the most appropriate server to solve a specific request (**find step**). Then the MA collects computation abilities from the servers (by propagating the client request through its subtrees down to the servers) and chooses the best one according to some scheduling heuristics. A reference to the chosen server is sent back to the client. Computations (**solve steps**) are done by servers (both sequential and parallel) in front of which there are **Server Daemons (SeD)**. For instance, a SeD can be located on the entry point of a parallel supercomputer. The information stored on a SeD is a list of data available on its server, the list of problems that can be solved on it, and all information concerning its load (memory and/or number of resources available, ...).

3.2 VizDIET Model of DIET Components and Requests

DIET is a classic example of a distributed platform. There is a set of components which interact with each other. The goal for a monitoring tool for DIET is to know the state of the system, the activity of each component, and the status of user requests. We have integrated in all DIET components a *LogComponent* and they are able to relay information such as state and activity by using the LogService mechanism. The model used for vizDIET is based on the basic model of vizTool, but vizDIET's model has been specialized for DIET components. We

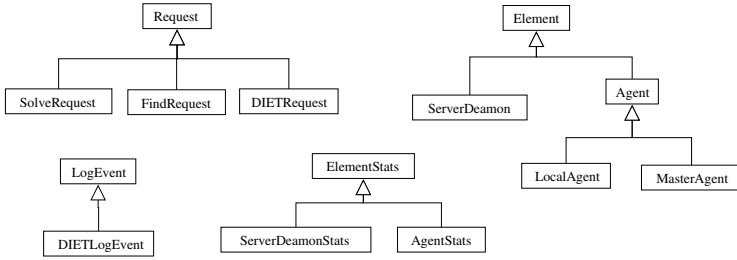


Fig. 3. DIET model of vizDIET

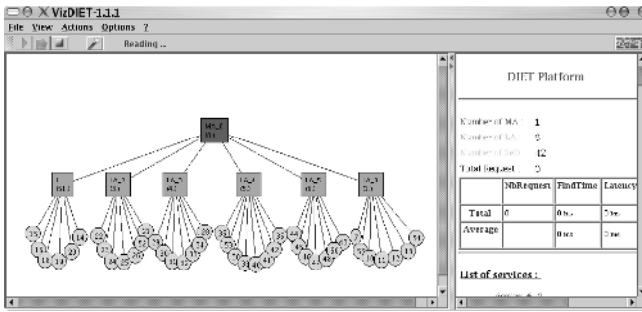


Fig. 4. vizDIET snapshot

consider each component of DIET (agents and server daemons) as an object which inherits from the element object. As there is a hierarchical architecture in DIET, the model will fit this property. Figure 3 shows the simplified UML schema of the model used to describe a DIET platform.

There are two main types of elements: *ServerDaemons* and *Agents* which inherit from *Elements*. *Agents* are then split into two classes: *MasterAgents* and *LocalAgents* which inherit from *Agents*. As described in the basic model each *Element* has a *ElementStats* object that stores and calculates information about the component that it monitors. MAs and LAs have nearly the same role in the DIET hierarchy, so their *ElementStats* share the same class: *AgentStats* which inherit for *ElementStats*. *ServerDaemons'* *ElementStats* is defined in its own specific object: *ServerDaemonStats* carries special methods and properties that differ from MAs or LAs.

As described in Section 3.1 there are two main steps; one step to find and schedule a service, and one step to solve this service. Two main activities are represented by: schedule and compute information. When an agent takes a scheduling decision for a task, it is useful to know how the agent made its decision. This information is represented by the *FindRequest* object. When a SeD is computing a job we need to be aware of its state and to know when the computation begins and ends. This information is represented by *SolveRequest* object. *FindRequest* are attached to agents and *SolveRequest* are attached to SeDs but they both inherit from *Request*. The vizDIET model includes one more type of request:

DIETRequest which is the aggregation of one *FindRequest* and one *SolveRequest*. *DIETRequest* object can be seen as a job execution in a DIET platform as seen by an end-user. This object carries one other information: **latency** which is the time between the end of a *FindRequest* and the start of a *SolveRequest* (see bottom right diagram in Figure 3).

Finally as proposed in the basic vizTool model, vizDIET uses a *DIETLogEvent* object inherited from *LogEvent* to define and characterize an atomic Event/Log message in the DIET environment. In *DIETLogEvent* there are two more properties: *logType* and *logCanal*. these two properties are used to separate log messages and manage priority of log (see bottom left diagram in Figure 3).

DIETLogEvent messages can be separated in two different types of messages: **state and configuration messages** (IN: a new element arrives in the platform, OUT: an element leaves the platform or fails, ADD_SERVICE: SeD declare a new service into platform) and **activity and informative messages** (ASK_FOR_SED: an agent looks for a SeD to execute a service, SED_CHOSEN: an agent has selected a list of SeD to execute a service, BEGIN_SOLVE: a SeD begins computation for a service request, END_SOLVE: a SeD has finished computation for a service request, DATA_STORED: a SeD has stored a dataset, DATA_RELEASED: a SeD has deleted a dataset, DATA_TRANSFER_BEGIN: a SeD begins to send data to another SeD, DATA_TRANSFER_END: a SeD ends data transfer). The first *DIETLogEvent* types define a DIET platform and indicate its state. Activity and informative messages are atomic events which are used to define objects such as *FindRequest* and *SolveRequest*. A pair of *DIETLogEvents* which are linked by the *request_id* define the corresponding type of request, for example one BEGIN_SOLVE and one END_SOLVE *DIETLogEvent* from the same SeD and with the same *request_id* define a *SolveRequest*.

3.3 Monitoring View of DIET with VizDIET

The first goal of *vizDIET* is to graphically represent the DIET hierarchy and to monitor its behavior. The *vizDIET* view is based on the basic view of Viz-Tool, giving the possibility to show a lot of information extracted from event information received from *logCentral* (see Figure 4).

All objects and information defined in Section 3.2 about the DIET components are used to compute some properties of the system.

Average: represent the mean of elapsed time for each request. So by considering each request we can calculate the average time for one type of request (i.e. findTime, SolveTime, and latency).

Max/min time: max/min time of all requests elapsed time.

Load: the number of requests computed at the same time. It is the number of requests that have a common intersection in the interval time represented by begin and end solve time.

Number of requests: this information is very useful. For example, one may be interested in the number of requests for a specific service on a specific SeD.

Latency: for each *DIETRequest* we can extract the latency between the end of a *FindRequest* and the beginning of a *SolveRequest*. This value represents the DIET's latency that includes the time to transmit data from client to server, network latency, and any other time introduced by scheduling policy (ex: request queueing ...).

Scheduling information: DIET's agent return the sorted list of SeD that can compute the service asked by the client. This list is returned in `SED_CHOSEN` logEvent with all values that help agent to make his scheduling decision.

data information: with the agregation of data information represented by logEvent such as `DATA_STORED` and `DATA_RELEASED`, we are able to know the amount of data presents in DIET, but also the time needed to transfert data and historic of transfert for this data (`DATA_TRANSFER_BEGIN`, `DATA_TRANSFER_END`).

Interaction with other systems: As LogService can relay whatever events, we can monitor the interactions of DIET components with JuxMem¹ [1] and know the amount of data read and write from JuxMem.

VizDIET can display a variety of information about the activity of a DIET platform. Figures 5 show some example of vizDIET statistic output. In the **Load graphic**, the load of Element is calculated as the number of requests executed on the element at the same time. This information is represented in a graphic (left of Figure 5) that draws the load of a SeD or the load of DIET platform. With this graphic one knows immediatly when requests are computed in parallel, and when there is overload or underload. In the **Taskflow graphic**, the flow of requests is vizualised. As requests are defined by a begin and end time, they can be represented in a taskflow chart to visualize scheduling information for each request. This view (middle of Figure 5) is very useful for observing the behavior of the scheduler and has been proven very useful for scheduler developers. Requests can be separated by using one color for requests executed on a SeD, or you can differentiate requests by using one color for each request involving a particular service. When requests are represented in a classic **Gantt chart**, the tasks repartition is known in the DIET platform, and also the number of tasks executed by a particular SeD. The Gantt chart (right of Figure 5 only uses the information of the *SolveRequest*.

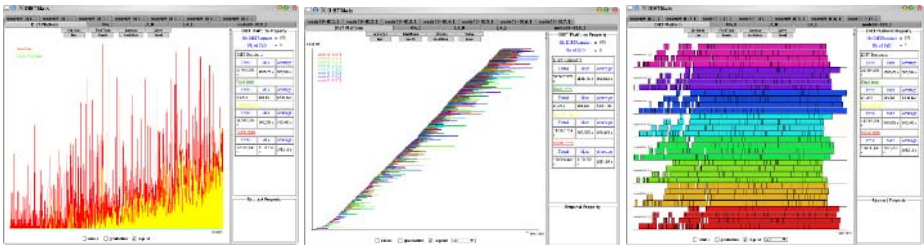


Fig. 5. Bar, taskflow, and Gantt graph in vizDIET stats

¹ JuxMem(Juxtaposed Memory) is a data sharing service for grid computing.

All of these methods can be applied to calculate values for one element such as a SeD, an Agent, or it can be applied to the entire DIET platform. It can also be applied to a specific set of requests restricted to one type of request.

4 Platform Model and Experimental Results

According to the activity description given in Section 3.1 in DIET and vizDIET model, we can easily write a formula that gives the number of logEvents (and so the amount of data) that are generated by LogService in DIET. Let $Nb_{log}(req_{serv})$ be the number of logs for one request of service $serv$. Nb_{act} is the number of logs corresponding to activity on platform. Nb_{desc} is the number of logs to describe the DIET platform. Nb_{agent} is the number of agents. Nb_{SeD} is the number of SeDs. $Nb_{SeD}(serv)$ is the number of SeDs that can compute service $serv$, $Nb_{act}(serv)$ is the number of activity logs for the service $serv$. $Nb_{agent}(serv)$ is the number of agents that have a SeD in their sub-tree that can compute service $serv$. req_{serv} is the number of requests for service $serv$.

$$\begin{aligned} Nb_{log}(req_{serv}) &= Nb_{desc} + req_{serv}.Nb_{act} \\ Nb_{desc} &= Nb_{Agent} + Nb_{SeD} + \sum_{serv} (Nb_{SeD}(serv)) \\ Nb_{act} &= \sum_{serv} (Nb_{act}(serv)) \\ Nb_{act}(serv) &= 2.(Nb_{agent}(serv) + 1) \end{aligned}$$

This formula can be simplified if we considerate a platform with only one service per SeD:

$$\begin{aligned} Nb_{log}(req) &= Nb_{desc} + req.Nb_{act} \\ Nb_{desc} &= Nb_{Agent} + 2.Nb_{SeD} \\ Nb_{act} &= 2.(Nb_{Agent} + 1) \end{aligned}$$

Now let's take care of the size of messages sent to logCentral in the case of one service per SeD. Let $S_{log}(req)$ be the size of logs depending of the number of requests. S_{desc} is the size of the message sent to logCentral to describe the platform (S_{desc}^{node} is the size of a message to describe one node). The message is the same for an agent, a SeD, and a service. S_{act} is the size of message that notify activity in the DIET platform: S_{ask} is the size of the message that notifies the event ASK_FOR_SED. S_f is a fixed size for the message SED_CHOSEN. S_{si} is the size of message containing schedule information of SeD. It is multiplied by $\sum_{agent} (Nb_{SeD}(agent))$ which represents the sum of SeDs that are under the sub-trees for each agent. And finally, S_{solve} is the size of message which notifies the SeD solves service.

$$\begin{aligned} S_{log}(req) &= S_{desc} + req.S_{act} \\ S_{desc} &= S_{desc}^{node} . (Nb_{Agent} + 2.Nb_{SeD}) \\ S_{act} &= Nb_{agent}.S_{ask} + Nb_{agent}.S_f + \sum_{agent} (Nb_{SeD}(agent).S_{si}) + S_{solve} \end{aligned}$$

Table 1. LogCentral behavior: 100 client requests with different numbers of DIET nodes

Nb of nodes	Nb_{act}	Min time/log	Mean time/log	Max time/log	Standard deviation
16	1800	3e-06 s	5.33e-06 s	1.8e-05 s	1.29e-06 s
32	3400	3e-06 s	6.60e-06 s	3.1e-05 s	2.30e-06 s
64	6600	3e-06 s	8.81e-06 s	1.94e-04 s	4.75e-06 s
128	13000	4e-06 s	1.53e-05 s	5.33e-04 s	1.42e-05 s

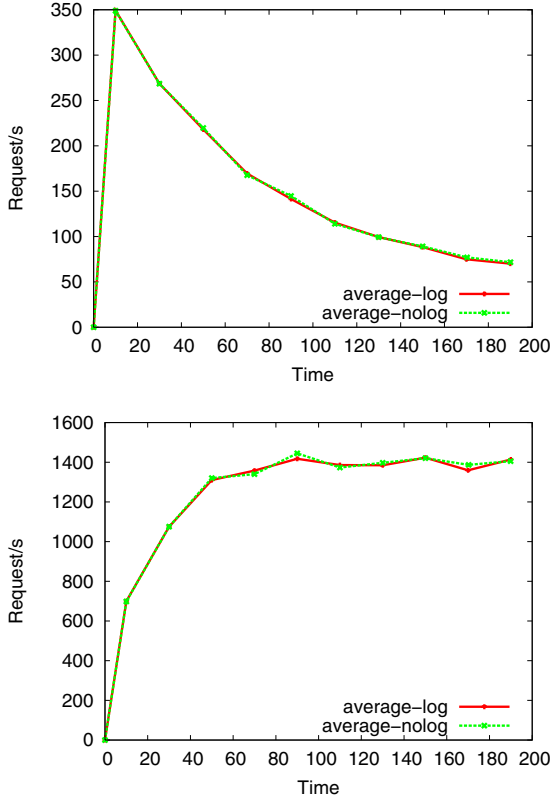


Fig. 6. Comparison of request processing rate with and without LogService

We made some experiments to evaluate the scalability of logCentral to manage a DIET platform. This experiments are made with the worst DIET platform topology (i.e.: that maximize the number and the size of messages that are sent to the logCentral). This topology is a rake tree² where there are the same number of SeDs and Agents³. There are 10 logTools connected to the *logCentral* to received messages, and for each experiment, there are 100 client’s requests on the DIET platform. The results of experiments are presented in Table 1.

² A rake tree is a chain where all leaves are attached on the last node.

³ This result has been proven, but this demonstration is not present in this paper.

These experiments show that logCentral is scalable. Even for a large platform, the maximum time to forward one log to 10 logTools is about 0.5 ms.

VizDIET and LogService are optional services that can be used with DIET. But as with any other [8] monitoring and information service for distributed systems, LogService introduces overheads with the transfer of data and information production. In this part we evaluate and quantify these overheads with a case study.

We choose a DIET hierarchy with 1 MA and 10 SeDs. Each SeD executes a DGEMM service. We study the performance of the DIET hierarchy in terms of number of requests per second the platform can compute. Each 20s there are two more clients that ask for the DGEMM service. All clients call DGEMM service on two small matrices (10x10), wait for the result, and then call the service again until the end of the experiment. Figure 6 shows the average on 4 experiments for the DIET platform with and without LogService.

The goal of the case study is not to know the DIET performance limits, but to compare the performance of DIET when LogService is turned on or off and also the behavior near the performance limits of the DIET platform. Figure 6 shows that the LogService does not significantly affect the overall performance of the platform, and the behavior of the platform is the same with or without LogService. The number of requests that was performed during the entire experiment is 256838 (mean on the 4 experiments).

Now thanks to formula given in Section 4. There were 21 informative logEvents and 1030804 activity logEvents. In total, the experience described above has generated 1030825 logEvents.

5 Conclusion and Future Work

VizTool is a basic framework that allows the specification of different models on distributed platforms. The VizTool model is very simple and generic to be used for various types of distributed environments. This model has been tested and validated in VizDIET for the monitoring of the DIET platform.

There are many others possibilities of improvement of VizDIET. More information can be added on the scheduling side (statistics, other measures like throughput, fairness, slowdown, . . .). The main improvement that remains to be done concerns the scalability of the visualization (which is a common issue for every large scale monitoring framework). Features like zooming on the architecture or more specifically for the DIET platform expand/un-expand a branch of the hierarchy will be developed.

References

1. G. Antoniu, L. Bougé, and M. Jan. Juxmem: An adaptive supportive platform for data sharing on the grid. *Scalable Computing: Practice and Experience*, 6(3):45–55, November 2005.
2. D. Arnold, S. Agrawal, S. Blackford, J. Dongarra, M. Miller, K. Sagi, Z. Shi, and S. Vadhiyar. Users' Guide to NetSolve V1.4. Computer Science Dept. Technical Report CS-01-467, University of Tennessee, Knoxville, TN, July 2001. <http://www.cs.utk.edu/netsolve/>.

3. E. Caron and F. Desprez. Diet: A scalable toolbox to build network enabled servers on the grid. Technical Report 2005-23, Laboratoire de l'Informatique du Parallélisme (LIP), June 2005. Also available as INRIA Research Report RR-5601.
4. E. Caron and F. Desprez. DIET: A Scalable Toolbox to Build Network Enabled Servers on the Grid. *International Journal of High Performance Computing Applications*, 2006. To appear.
5. DIET. <http://www.graal.ens-lyon.fr/DIET>.
6. D.W. Lee, J. Dongarra, and R.S. Ramakrishna. *visPerf*: Monitoring Tool for Grid Computing. In P.M.A. Sloot et al., editor, *ICCS'03*, volume 2659 of *Lecture Notes in Computer Science*, pages 233–243, 2003.
7. LogService. <http://graal.ens-lyon.fr/DIET/logservice.html>.
8. M.L. Massie, B.N. Chun, and D.E. Culler. The Ganglia Distributed Monitoring System: Design, Implementation, and Experience. *Parallel Computing*, 2003. (submitted).
9. S. Matsuoka and H. Casanova. Network-Enabled Server Systems and the Computational Grid. <http://www.eece.unm.edu/~dbader/grid/WhitePapers/GF4-WG3-NES-whitepaper-draft-000705.pdf>, July 2000. Grid Forum, Advanced Programming Models Working Group whitepaper (draft).
10. H. Nakada, M. Sato, and S. Sekiguchi. Design and Implementations of Ninf: towards a Global Computing Infrastructure. *Future Generation Computing Systems, Meta-computing Issue*, 15(5-6):649–658, 1999. <http://ninf.apgrid.org/papers/papers.shtml>.
11. S. Zanicolas and R. Sakellariou. A Taxonomy of Grid Monitoring Systems. *Future Generation Computer Systems*, 21:163–188, 2005.

Parallel Hash Join Algorithms for Dynamic Load Balancing in a Shared Disks Cluster

Aekyung Moon¹ and Haengrae Cho²

¹ Software Robot Research Team, ETRI,
Gajung-dong, Yusong-gu, Taejon 305-350, Republic of Korea
akmoon@etri.re.kr

² Department of Computer Engineering, Yeungnam University,
Gyungsan, Gyungbuk 712-749, Republic of Korea
hrcho@yu.ac.kr

Abstract. Most of previous parallel join algorithms assume a shared nothing (SN) cluster, where each database partition is owned by a single processing node. While SN cluster can interconnect a large number of nodes and support a geographically distributed environment, it may suffer from poor facility for load balancing and system availability compared to a shared disks sharing (SD) cluster. In this paper, we first propose a dynamic load balancing strategy by exploiting the characteristics of SD cluster. Then we parallelize conventional hash join algorithms using the dynamic load balancing strategy. We also explore the performance of parallel join algorithms using a simulation model of SD cluster. The experiment results show that the proposed parallel join algorithms can achieve higher potential for dynamic load balancing with the inherent flexibility of SD cluster.

Keywords: Cluster computing, shared disks, hash join, load balancing.

1 Introduction

There are two primary flavors of cluster architecture designs: *shared nothing* (SN) and *shared disks* (SD) [7, 8]. In SN cluster, each node has its own set of private disks and only the owner node can directly read and write its disks. On the other hand, the SD cluster allows each node to have direct access to all disks. The SD cluster offers a number of advantages compared to SN cluster, such as dynamic load balancing and seamless integration. Furthermore, the rapidly emerging technology of storage area networks (SAN) makes SD cluster the preferred choice for reasons of higher system availability and flexible data access. The recent parallel database systems using the SD cluster include IBM DB2 Parallel Edition [2] and Oracle Real Application Cluster [13].

In this paper, we propose parallel hash join algorithms in the SD cluster. The hash join is very efficient for large relations since it divides the joining relation into several buckets whose join key hash value is different so that the matching cost is substantially reduced [5, 12]. Moreover, the hash join provides natural opportunity for parallel processing because of generating disjoint buckets. With

regard to this viewpoint, there have been considerable research on the parallel hash join [1, 3, 4, 9, 10]. However, most of previous parallel hash join algorithms assume SN cluster, and the SD cluster has received very little attention with respect to parallel query processing. Fortunately, many of the techniques developed for parallel query processing in SN cluster can be utilized for SD cluster as well. However, the fact that each node can directly access all data gives SD cluster a higher flexibility, especially a higher potential for dynamic load balancing, for parallel query processing compared to SN cluster.

This paper is organized as follows: Sect. 2 presents the problems of previous algorithms and Sect. 3 proposes the parallel hash join algorithms in SD cluster. The simulation model is developed in Sect. 4, and Sect. 5 analyzes the performance of the proposed algorithms. Sect. 6 concludes this paper.

2 Problem Definition

The hash join algorithm comprises *partition phase* and *join phase* [12]. Suppose there are two joining relations R and S , where the join attributes are JA_R and JA_S , respectively. The partition phase is to partition R and S into n disjoint buckets, R_1, R_2, \dots, R_n and S_1, S_2, \dots, S_n . The join phase is to build hash tables for buckets from an inner relation, R , and probe the hash table using tuples of the corresponding buckets from an outer relation, S . Note that for any two tuples, r and s , where $r \in R_i$ and $s \in S_j$, if $i \neq j$ then $r.JA_R \neq s.JA_S$. In this way, R_i needs to be joined with S_i only. Thus,

$$R \bowtie S = \bigcup_{i=1}^{i=n} R_i \bowtie S_i \quad (1)$$

The effectiveness of parallel hash join algorithms depends upon the ability to equally divide the load among nodes. A factor which can impair the ability to parallelize join queries successfully is *the amount of data skew* present in the joining relations [1, 3]. Specifically, if some buckets are much larger due to data skew, the speed-up from parallel hash join algorithms may be severely limited because some nodes may be overloaded while others are underutilized.

To alleviate the data skew problem in SN cluster, the approach of data re-allocation or replication have been proposed [3]. However, both approaches may suffer from significant coordination and synchronization overhead. The idea of load balancing in SD cluster is to reduce the size of task allocation unit *smaller* than the bucket size. For example, Lu and Tan [6] proposed a task stealing approach, where an idle node can steal part of a bucket from an overloaded node that has not completed the join operation of a (big) bucket. To estimate the amount of bucket to be stolen, each node is assumed to share a global memory. Whenever a page is processed, the node updates the global memory - the number of pages of each bucket left and the number of pages of the result relation generated thus far. Note that this process should result in heavy message traffic if the global memory is not physically attached to each node, which is true in most commercial SD clusters [13].

3 Parallel Hash Join Algorithms

In this section, we first propose a task generation strategy for efficient dynamic load balancing. Then we propose three parallel hash join algorithms.

3.1 Task Generation Strategy

We assume a *task manager* that manages information for load balancing. The task manager is located in a specific node. Other nodes execute join operations and communicate to the task manager via message passing. We refer them as *join nodes*. The task manager has a task memory that stores the bucket information. The bucket information consists of five tuples: [bucket identifier (B_I), number of pages of a bucket (B_S), number of pages of a bucket to be processed at join phase (B_U), list of page identifiers of a bucket (P_B)].

The task manager determines the number of buckets at the partition phase. We try to set the bucket size nearly equal to the memory size to maximize parallelism with little overhead. When bucket overflow occurs due to data skew or limited memory size, the bucket is partitioned into several fragments. A *fragment* is a part of bucket that can be allocated entirely into memory. For each fragment, the task manager registers the following fragment information to the task memory: [fragment identifier (F_I), number of pages of a fragment (F_S), fragment allocation bit (F_A), list of page identifiers of a fragment (P_F)].

After the partition phase, the task manager generates the fragment information and allocates each fragment to a join node. The details are as follows:

1. A join node sends $[B_I, B_S, B_U, P_B]$ message for every bucket to the task manager after it finishes its partition phase. The task manager stores the bucket information into the task memory.
2. Then the task manager partitions each bucket into fragments. The number of fragments (N_F) is set to $\lceil B_U/|M| \rceil$, where $|M|$ is the number of pages that a join node can store in its memory. We assume that $|M|$ is equal for every join node. The size of each fragment ($F_S[i]$) is determined as follows:

$$F_S[i] = \begin{cases} \lceil B_U/N_F \rceil & i < N_F \\ B_U - \sum_{k=1}^{N_F-1} F_S[k] & i = N_F \end{cases} \quad (2)$$

For each fragment, the task manager registers $[F_I, F_S, F_A, P_F]$ into the task memory. At this time, F_A is set to '0' since the fragment is not allocated to any join node yet.

3. At the join phase, each join node requests next fragment to be joined. The task manager selects a fragment where $F_A=0$, and sends $[B_I, F_I, F_S, P_B, P_F]$ message to the join node. The bucket information of B_I and P_B corresponds to the outer relation (S) and the other fragment information corresponds to the inner relation (R). F_A of the fragment is set to '1'.
4. After receiving the message, the join node reads every page of P_F from disk and creates a hash table for the fragment of R . Then the join node reads each page of P_B of S and probes its hash table of R .

Note that a join node sends a request message to the task manager for each fragment. This is not true in [6], where the message passing is done for each page. Since a fragment includes large number of pages, the proposed strategy can reduce the message traffic significantly. The potential drawback of the proposed strategy is that it cannot provide “task stealing”. That means at the final stage of join phase some nodes would execute join operations for the last fragments while other nodes are idle. However, we believe that this kind of load imbalance is not critical since a fragment can be stored entirely into the memory of a join node. Join operations on the fragment should not take long time.

It is worthy to compare the proposed strategy with the task allocation strategy of Oracle Real Application Cluster (ORAC) [13]. ORAC divides an input relation into several partitions, each of which has the same number of pages. Specifically, the size of a partition is determined by dividing the number of nodes into the number of pages of input relation. Then ORAC assigns a partition to each node. As a result, every node can process the same number of pages. However, data skew could still happen and each node would not be under the same load. This is because the pages may have different numbers of tuples. Some of the pages could be completely empty [13]. The proposed strategy can alleviate this problem by allocating each fragment to the node with the on-demand approach. Dynamic load balancing can be achieved as a result.

3.2 Parallel Hash Join Algorithms

In this section, we propose three parallel hash join algorithms in SD cluster. The join phase of each algorithm is equal as described in Sect. 3.1. So we describe the partition phase of each algorithm in detail.

Parallel Grace Hash Join (PGHJ). A node partitions its part of the joining relation into buckets and writes them into disk. Then the join node sends $[B_I, B_S, B_U, P_B]$ message for every bucket to the task manager. B_U is equal to B_S since buckets are not joined at the partition phase.

The number of buckets ($|B|$) may have an impact on the performance of the PGHJ. If $|B|$ is too large, B_S may be much smaller than the memory size of a join node ($|M|$). This means that large number of small fragments are created at the join phase; hence, the join phase takes longer time. If $|B|$ is too small, B_S will increase. While the bucket of inner relation is partitioned into smaller fragments, the bucket of outer relation should be accessed entirely for each fragment. As a result, small $|B|$ may result in more disk I/Os. With regard to this viewpoint, we set $|B|$ as $\lceil |R|/|M| \rceil$, where $|R|$ is the size of joining relation.

Parallel Simple Hash Join (PSHJ). $|B|$ is set to the number of join nodes. As a result, there is an one-to-one relationship between a bucket and a join node. The join node executes join operations for the related bucket during the partition phase. Specifically, at the partition phase, each join node partitions the joining relation into buckets in parallel. When the size of a bucket exceeds a page, the bucket page is sent to its related join node. If the joining relation is

an inner relation, the receiving node inserts tuples of the page into a hash table. Otherwise, the node probes the hash table for each tuple of the page.

During the tuple insertions, a hash table overflow may occur. The overflow area is written to disk. After the partition phase, the join node sends $[B_I, B_S, B_U, P_B]$ message for its related bucket to the task manager. For inner relation, B_U is set to the number of overflow pages and P_B includes the identifiers of overflow pages. The bucket information of outer relation is equal to that of the PGHJ.

Parallel Hybrid Hash Join (PHHJ). The PHHJ combines the PGHJ and the PSHJ. $|B|$ is set to $\lceil |R|/|M| \rceil$, and some buckets are joined at the partition phase. Specifically, each join node creates $|B|$ buckets. Among them, $|N|$ buckets $(B_1, \dots, B_{|N|})$ are joined at the related join node, where $|N|$ is the number of join nodes. The remaining buckets $(B_{|N|+1}, \dots, B_{|B|})$ are written to disk. Overflow processing is still done as described in the PSHJ.

After the partition phase, each join node sends $[B_I, B_S, B_U, P_B]$ message for every bucket to the task manager. If a bucket belongs to the inner relation, B_U is set to either the number of overflow pages or B_S , depending on whether the bucket is joined at the partition phase $(B_1, \dots, B_{|N|})$ or not $(B_{|N|+1}, \dots, B_{|B|})$.

4 Experiment Model

We evaluate the performance of parallel hash join algorithms by simulation. Fig. 1 shows the experiment model of an SD cluster. The model was implemented using the CSIM discrete-event simulation package [11].

We model the SD cluster consisting of a single manager node plus a varying number of join nodes, all of which are connected via a local area network. Disks are shared by every node. The model of each join node consists of a *partition process*, which partitions the joining relation into a number of buckets, and a *join process*, which executes join operations on buckets or fragments. The details of both processes capture the semantics of given hash join algorithm. The *resource manager* models CPU activity and provides access to the disks and the network. The manager node consists of *task manager*, which manages bucket and fragment information, and *query manager*, which allocates part of joining relation to each join node for parallel partitioning.

Table 1 shows the simulation parameters. Many of the parameter values are adopted from [6, 7]. We perform the experiments by varying the number of join nodes and the memory size of each join node. The CPU speed of each join node is assumed to be equal. Disk access time is drawn from a uniform distribution between 10 milliseconds to 30 milliseconds. To increase I/O performance at the partition phase, tuples of each relation are distributed among the disks in a round-robin fashion. The *network manager* is implemented as a FIFO server with 100 Mbps bandwidth. The CPU cost to send or to receive a message via the network is modeled as a fixed per-message instruction count plus an additional per-page instruction increment. Note that the protocol processing (i.e., CPU overhead) dominates the on-the-wire time for message passing.

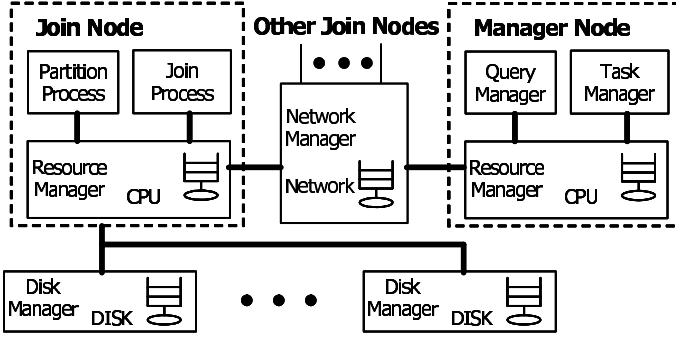


Fig. 1. Experiment model of an SD cluster

Table 1. Simulation parameters

System Configuration Parameters		
<i>CPU Speed</i>	Instruction rate of node CPU	1000 MIPS
<i>MemSize</i>	Per-node memory buffer size	40 Mbytes
<i>NetBandwidth</i>	Network bandwidth	100 Mbps
<i>NumNode</i>	Number of join nodes	4 ~ 40
<i>NumDisk</i>	Number of shared disks	16
<i>MinDiskTime</i>	Minimum disk access time	0.01 sec
<i>MaxDiskTime</i>	Maximum disk access time	0.03 sec
<i>RelSize</i>	Number of tuples per relation	10000 K
<i>DistinctTuples</i>	Number of distinct tuples	100 K
<i>PageSize</i>	Size of a page	8 Kbytes
<i>TuplesPerPage</i>	Number of tuples per page	50
System Overhead Parameters		
<i>FixedMsgInst</i>	Fixed number of instructions per message	20,000
<i>PerByteMsgInst</i>	Additional instructions per message byte	10,000 per page
<i>PerIOInst</i>	Number of instr. per a disk I/O	5000
<i>ReadTuple</i>	Number of instr. to read a tuple	500
<i>WriteTuple</i>	Number of instr. to write a tuple	500
<i>ProbeHashTbl</i>	Number of instr. to probe the hash table	200
<i>InsertHashTbl</i>	Number of instr. to insert a tuple to the hash table	100

For a relation R with a domain D distinct values ($DistinctTuples$), the i^{th} distinct join attribute value, for $1 \leq i \leq D$, has such number of tuples as given by the following Zipf-like distribution expression [6]:

$$\|D_i\| = \frac{\|R\|}{i^\theta \sum_{j=1}^D \frac{1}{j^\theta}} \quad (3)$$

where $\|R\|$ is the number of tuples of R and θ is the skew factor. When $\theta = 0$, the distribution becomes uniform. With $\theta = 1$, it corresponds to the highly skewed pure Zipf distribution.

The performance metric is *average response time* of join queries. The response time in second is measured as the difference when a join query is submitted and when every join result is returned. The time includes any time spent in the queue, disk I/O, and communication. A form of the batch mean method with 20 batches was used for the statistical analysis of simulation results.

5 Experiments and Results

This section explores the performance of parallel hash join algorithms using our simulation model of SD cluster. To evaluate the effect of task allocation unit, we implement two versions for each hash join algorithm: fragment allocation (PGHJ-F, PSHJ-F, PHHJ-F), and bucket allocation (PGHJ-B, PSHJ-B, PHHJ-B).

5.1 Experiment 1 – High Skew Workload

This workload models where the degree of data skew is high ($\theta = 1$ in Equation (3)). The number of join nodes is varied from 4 to 40. Fig. 2(a) shows the performance results of this workload.

For every algorithm, the fragment allocation strategy outperforms the bucket allocation strategy. This is because the bucket allocation strategy suffers from some big buckets when the degree of data skew is high. On the other hand, at fragment allocation strategy, a big bucket is partitioned into smaller fragments and each fragment can be joined at a number of join nodes in parallel. Due to its high potential of parallelism, the fragment allocation strategy performs better as the number of nodes increases. This property is well matched with the trend of ever-increasing scalability of parallel systems.

The PSHJ exhibits substantial performance improvements as the number of nodes increases. Note that at PSHJ the number of buckets is equal to the number of nodes. As the number of nodes increases, more buckets are created and thus the size of each bucket is reduced; hence, the amount of hash table overflow decreases. When there are small number of nodes, the PGHJ outperforms the PSHJ due to large bucket size of PSHJ. However, the PGHJ is outperformed by the PSHJ as the number of nodes increases, because at PSHJ a decreasing fraction of joining relation is written back to disk. Note that the amount of disk write at PGHJ is constant independent of the number of nodes. The PHHJ performs similar to the PGHJ at small number of nodes, while performs similar to the PSHJ at large number of nodes. Since the bucket size of PHHJ is determined according to the memory size like the PGHJ, the join execution time per bucket does not increase significantly at small number of nodes. Furthermore, at large number of nodes, the PHHJ can join most buckets without writing back to the disk like the PSHJ.

It is important to point out that the trends observed in Fig. 2(a) and its general shape are almost identical to the performance results in [12] for single node versions of the same algorithms and in [10] for SN clusters. It demonstrates that each of the algorithms parallelizes well in SD cluster. Furthermore, it serves

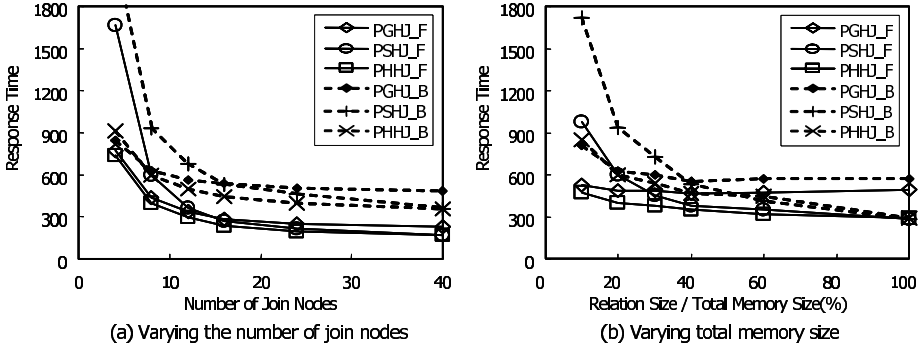


Fig. 2. Experiment results at high skew workload

to verify that our parallel implementation of each algorithm in SD cluster was done in a fair and consistent fashion.

We also explore the effect of memory size of each join node where the degree of data skew is high. The number of join nodes is set to 8, while the total memory size of all join nodes is varied from 10% of joining relation to 100%. Fig. 2(b) shows the experiment results. The performance of the bucket allocation strategy degrades rapidly as the size of memory decreases, especially when the percentage of total memory relative to the size of joining relations is small. This is because the bucket allocation strategy suffers from the frequent bucket overflows at the small memory size. On the other hand, in the fragment allocation strategy, the bucket overflow area is partitioned into smaller fragments and the join nodes can process the fragments in parallel.

When the joining relation fits entirely in memory (at 100%), both PHHJ and PSHJ perform in the same manner as expected. As the size of memory decreases, the PSHJ degrades rapidly because it repeatedly reads and writes the same data. The PGHJ is relatively insensitive to the memory size. This occurs because the PGHJ does not use the extra memory for join queries, and thus increasing memory simply reduces the number of buckets. However, at PHHJ, increasing memory from 50% to 100% allows the algorithm to stage every joining bucket into memory.

5.2 Experiment 2 – Uniform Workload

This workload models where values of join attributes are uniformly distributed, and thus data skew is not present ($\theta = 0$ in Equation (3)). Fig. 3 shows the performance results of this workload by varying the number of join nodes and by varying the total memory size.

Unlike the high skew workload, the task allocation strategy does not result in significant performance difference between join algorithms. This is because the size of buckets are almost equal to each other in the uniform workload. Hence, in the bucket allocation strategy, the load of each join node can be balanced similar to the fragment allocation strategy.

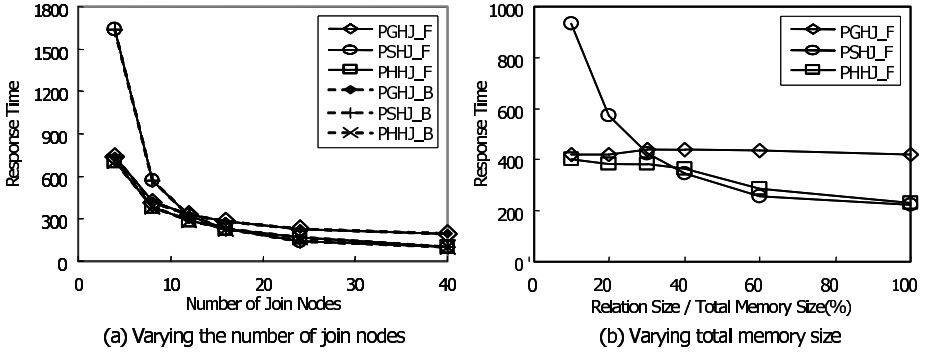


Fig. 3. Experiment results at uniform workload

Every hash join algorithm performs better compared to the high skew workload in Fig. 2. The reason also comes from the equal bucket sizes in the uniform workload. Note that there are some big buckets in the high skew workload. As we described in Sect. 5.1, join nodes that process the big buckets are overloaded and thus they delay the total response time. While the fragment allocation strategy may reduce the response time by partitioning the big buckets of inner relation into fragments, each fragment should be joined against the big bucket of outer relation. This means that the big buckets of outer relation may be accessed repeatedly for each fragment by the corresponding join node. As a result, the degree of performance improvement is limited somewhat.

The performance graphs exhibit similar pattern to that in the high skew workload. An interesting observation is that the PSHJ outperforms the PHHJ when the number of nodes is 16 and 24 in Fig. 3(a). This is due to the number of fragments. At PSHJ, fragments are created when a bucket overflow occurs and the size of buckets are nearly equal to each other in the uniform workload. This means that the number of fragments at PSHJ is always a multiple of the number of nodes in the uniform workload; hence, loads of join operations can be completely balanced. This feature may not hold on PHHJ since the number of buckets is determined with the memory size of join node.

6 Concluding Remarks

Most of previous parallel join algorithms assume SN cluster, and the SD cluster has received very little attention with respect to parallel query processing. However, the fact that each node can directly access all data gives SD cluster a higher flexibility, especially a higher potential for dynamic load balancing, for parallel query processing compared to SN cluster. With regard to this viewpoint, we first propose a fragment based task allocation strategy that can distribute load of join operations evenly into the participating join nodes. Then we parallelize the conventional hash join algorithms for SD cluster using the fragment based task allocation strategy.

We have explored the performance of parallel hash join algorithms under a wide variety of database workloads and system configurations using a simulation model of SD cluster. The considerable results obtained from the experiments can be summarized as follows. First, when the join attribute is skewed, the fragment based task allocation strategy exhibits substantial performance improvements, compared to the bucket based task allocation strategy. Next, as the number of nodes increases, the fragment based task allocation strategy performs better due to its higher potential of parallelism. This property is well matched with the trend of ever-increasing scalability of cluster systems. Finally, the PPHJ outperforms other hash join algorithms in most experiments.

Acknowledgements

The work of Prof. Cho was supported by the University ITRC Project.

References

1. Bamha, M., Exbrayat, M.: Pipelining a Skew-Insensitive Parallel Join Algorithm. *Parallel Processing Letters* 13(3) (2003) 317-328
2. DB2 Universal Database for z/OS Version 8 - Data Sharing: Planning and Administration. IBM SC18-7417-01 (2004)
3. Heal, A., Yuan, A., El-Rewni, H.: Dynamic Data Reallocation for Skew Management in Shared Nothing Parallel Databases. *Distributed and Parallel Databases* 5(3) (1997) 271-288
4. Imasaki, K., Nguyen, H., Dandamudi, S.: Performance Comparison of Pipelined Hash Joins on Workstation Clusters. *LNCS* 2552 (2002) 264-278
5. Lu, H., Ooi, B., Tan, K.: Query Processing in Parallel Relational Database Systems. IEEE Computer Society Press (1995)
6. Lu, H., Tan, K.: Dynamic and Load-Balanced Task Oriented Database Query Processing in Parallel Systems. *LNCS* 580 (1992) 357-372
7. Ohn, K., Cho, H.: Cache Conscious Dynamic Transaction Routing in a Shared Disks Cluster. *LNCS* 3045 (2004) 548-557
8. Ranade, D.: *Shared Data Clusters*. John Wiley, Inc. (2002)
9. Schikuta, E., Kirkovits, P.: Cluster Based Hybrid Hash Join: Analysis and Evaluation. In: *Proc. IEEE Conf. Cluster Computing* (2002) 461-466
10. Schneider, D., DeWitt, D.: A Performance Evaluation of Four Parallel Join Algorithms in a Shared-Nothing Multiprocessor Environment. In: *Proc. ACM SIGMOD Conf.* (1989) 110-121
11. Schwetman, H.: *CSIM18 Simulation Engine*. Mesquite Software, Inc. (1996)
12. Silberschatz, A., Korth, H.F., Sudarshan, S.: *Database System Concepts* (4th ed.). McGraw Hill (2002)
13. Vallath, M.: *Oracle Real Application Clusters*. Elsevier Digital Press (2004)

Towards Reliable and Trustworthy Cooperation in Grid: A Pre-evaluating Set Based Trust Model*

Xiangli Qu, Jingwei Zhong, and Xuejun Yang

School of Computer Science, National University of Defense Technology,
Changsha, China, 410073
cathysmile@eyou.com

Abstract. Without reliable trust relationship between cooperative parties, the paradigm of large scale resource sharing and cooperated problem-solving as envisioned by most will not come true in Grid. With wide application in Electronic Commerce and online communities, Reputation mechanism emerges as a promising solution for trust establishment in Grid, especially between unknown entities. With little consideration of Grid's distinct characteristics such as the sparseness of ratings and the strangeness of entities, most reputation evaluation methods currently available are not feasible to Grid. In this paper, we propose a pre-evaluating set based bias-tuned method for reputation evaluation in Grid. The introduction of the pre-evaluating set is to track an entity's rating criteria, overcome the sparseness and strangeness mentioned above. With this pre-evaluating set, we can reasonably filter out malicious ratings by examining inconsistency between ratings to this set and to real transactions, effectively tune a rater's bias to cater to the current evaluator's criteria by interpolation approach and scientifically weight a rater's rating in aggregation by the introduction of Criteria Coherent Degree.

1 Introduction

Grid computing has emerged as one of the key computing paradigms that enable the creation and management of Internet-based utility computing infrastructure for realization of e-Science and e-Business at the global level. Meanwhile, it shows from survey that, in Grid, collaborations often cross organizational lines, underscoring the significance of inter-organizational trust. The responses showed a high level of communication and collaboration with people from outside the respondent's department (90%), outside their company or organization (82%), and outside their country (69%) [1]. Therefore, in open Grid environment with large-scale resource sharing, it is frequent for unknown entities to collaborate with each other. To guarantee smooth and reliable ongoing of such cooperation, certain trust relationship must be established among cooperative parties. And with the wide spread and increasing adoption of Grid applications, we cannot escape from considering trust establishment in such scenarios. For completely unknown entities, traditional identity-based trust system obviously cannot work well because of its restricted scalability and flexibility. In such case, third

* This work is partially supported by the National 863 High Technology Plan of China under the grant No. 2002AA1Z201 and 2003AA115130.

parties' participation becomes a necessity for trust establishment; meanwhile, Grid's inherent sharing and cooperative characteristics provide an excellent support for this. Using shared information about past transactions, analyzing evidence of an entity's past behavior, evaluating its trustworthiness, based on which dynamically establishing corresponding trust relationship, this is the basic idea of reputation mechanism in Grid. In this environment, what reputation is to Grid is just what credit card is to human society and what brand is to a company.

The distinct feature of our trust model is the introduction of a pre-evaluating set, which aims at tackling the subjectivity and bias-proneness of reputation (Different people may have different rating criteria.) and some inherent characteristics of reputation mechanism in Grid, i.e. two entities usually have few entities cooperated in the same context in common, which is named the "prevalent strangeness" of Grid entities by us. Actually, this is a set consisting of many kinds of behaviors an entity might behave in transactions for all the entities to rate. With no specific benefits involved and other restrictions, it can be expected to truthfully reflect an entity's rating criteria. In 3 aspects, this set takes its effect: In filtering, it can help to filter out dishonest feedbacks by examining inconsistency between a rater's rating criteria and his actual ratings; In bias-tuning, it can help to estimate a certain relationship between some rater's rating criteria and the current evaluator's criteria; In aggregating, it can help to give reasonable weights to each rater's rating.

The rest of this paper is organized as follows: a brief introduction of current reputation evaluation method is outlined in section 2; our pre-evaluating set based trust model is detailed in section 3, including basic model, bias-tuning method for first-hand ratings and criteria coherent degree based aggregation method for tuned ratings etc.; specific tests and results are presented in section 4; and finally in section 5 the whole paper is concluded and our future work is briefed.

2 Related Work

The idea of reputation first appeared in Electronic Commerce, online communities [4], such as eBay, Amazon and so on, and currently is widely adopted in most popular ecommerce website. Recently, it is introduced to multi-agent systems, semantic web, P2P systems and Grid systems [7][8][9][11].

Generally speaking, most reputation evaluation methods currently available either do not take bias tuning into consideration or are not feasible to Grid environment: In [7], an EigenTrust mechanism is proposed. But, for the introduction of normalization process, much useful original information is lost. In [10] reputation evaluation is based on "Web of Trust". There are two interpretations: Path Algebra Interpretation and Probabilistic Interpretation. In [9], Dempster-Shafer theory is adopted as the underlying computing framework, and reputation is combined by means of orthogonal sum of mass function. For the above methods, evaluations are performed directly on the first-hand ratings, with no consideration of the obviously existing bias. In [3], "semantic distance" is used to describe the difference between a recommender's rating and the real outcome, according to which adjustment is made. In [11], the "personalized similarity" approach is proposed to evaluate an entity's credibility: first get the intersection of one's own rating set and the evaluatee's rating set, then compute the deviation of this set. The less the deviation, the more credible the entity is. The above

two methods are still not feasible in Grid, since any two Grid entities usually have few entities transacted with in common. And according to [12], not to say the Grid systems, even for the popular Internet web site epinions.com, this kind of sparseness is true.

As to dishonest feedback filtering: In [5], controlled anonymity is used to avoid unfairly low ratings and negative discrimination and cluster filtering techniques are used to reduce the effect of unfairly high ratings and positive discrimination. Such filtering method does not take an entity's rating habit into consideration and might filter out ratings from lenient raters. In [6], a statistical filtering technique is described for excluding unfair ratings. But it assumes the existence of cumulative rating vectors for each rater, which is infeasible in open Grid environment.

3 The Pre-evaluating Set Based Trust Model

The distinct feature of our trust model is the introduction of a pre-evaluating set, which is to track an entity's rating criteria, overcome the prevalent strangeness of most Grid entities and the sparseness of peers both has transacted with.

3.1 Basic Model

This model is built on top of SOA (Service Oriented Architecture) and is an improvement on the model proposed by us in [13], which has two fundamental components: Grid Reputation Service and Grid Contract Service. Grid Reputation Service is responsible for the acquisition, storing, dissemination, retrieving and aggregation of first-hand reputation ratings, while Grid Contract Service provides a supervising mechanism and help with the negotiation of service providers and consumers. Besides, we adopt the Service Negotiation and Acquisition Protocol (SNAP) proposed in [14], which gives 3 kinds of service level agreement: *RSLA* (Resource Service Level Agreement), *TSLA* (Task Service Level Agreement) and *BSLA* (Binding Service Level Agreement). The 3 agreements supplement each other, clarify an interaction's context, which are ideal container of first-hand reputation ratings. The main interactions among these components are as follows: before transaction service providers will publish their *RSLA* and service consumers will post their *TSLA*; by means of Grid Contract Service, *BSLA* will be formed between providers and consumers. After transaction, both participants will submit ratings of counterpart's behavior to Grid Reputation Service. Grid Reputation Service will insert this reputation information into *RSLA* and *TSLA*. After this modification, *RSLA*, *TSLA* and *BSLA* will be stored to reputation repository as first-hand reputation evidence (with *RSLA* and *TSLA* contain ratings and *BSLA* specifies context) for later retrieval. In this way, we can get related evidence for reputation evaluation as needed anytime and anywhere.

3.2 The Pre-evaluating Set Related

As a very important and characteristic component in our trust model, the pre-evaluating set is to track an entity's rating criteria. In fact, it consists of a set of scenarios describing an entity's behavior in a transaction, which includes three

subsets: trustworthy, untrustworthy and in-between subset. We have two considerations for this division: one is that people tend to have different criteria for trust and distrust behaviors; the other is to leverage the precision of the tuned result, which will be explained in section 3.5. There is a common pre-evaluating set in the whole Grid infrastructure, for example we can define it as: trustworthy subset={fulfill task ahead of time; correct and prompt results; contact immediately when the unexpected happens; no litter left when logout}; in-between subset={the task has completed but overtime; no illegal operation but mess up the system; result is given but not ideal; cooperation has completed but not smooth; there is suspected behaviors but with no concrete evidence}; and untrustworthy subset={leave Trojans; execute malicious code; modify files without permission; with litter left; use resources overtime; not fulfill task as required; delete important files; service QoS inconsistent with declaration}. Besides, each Grid VO can specify its own pre-evaluating set as a complement to the common set. In the following two scenarios, VOs will ask entities to submit ratings: when registering a Grid ID (in this paper, we assume that an entity is allowed to have only one Grid ID, so as to avoid the phenomenon of identity farm and liar farm.), the common pre-evaluating set will be asked to rate; joining in a VO: in this scenario, if this VO has its own pre-evaluating set, the entity will be asked to submit ratings for this set

In this way, any two Grid entities will at least have the common pre-evaluating set rated in common. Meanwhile, some specific requirements of VOs have been taken into account. Grid Reputation Service will store all the submitted ratings into distributed reputation repository. Once submitted, these ratings cannot be changed and can only be seen by those who have already rated the corresponding set. This is to prevent malicious entities from cheating.

3.3 Notations

In this paper, we define an entity e_i 's reputation R_i as an expectation of its future behavior based on other entities' observations or information about its past behavior, whose value is within the scope of $[0, 1]$. We also define that the value within the scope of $[0, 0.4]$ is an untrustworthy value, the value within the scope of $(0.4, 0.7)$ is an in-between value and the value within the scope of $[0.7, 1]$ is a trustworthy value. Since we only concern about evaluating an unknown entity's reputation where ratings from one's own direct experience are null, information for evaluation only consists of third parties' first-hand ratings for this unknown entity. Here, we denote the first-hand rating entity e_i given to e_j as $R_{\langle e_i, e_j \rangle}$. If there is more than one rating, we will use the method proposed in [15] to compute an aggregated value as a replacement. The three subsets of a pre-evaluating set: trustworthy subset, untrustworthy subset and in-between subset are denoted as $T_1 = \{t_1, t_2, \dots, t_1\}$, $U_m = \{u_1, u_2, \dots, u_m\}$ and $B_n = \{b_1, b_2, \dots, b_n\}$ respectively. An entity e_i 's ratings to these three subsets are denoted as $PR_{\langle T, i, i \rangle} = \{r_{\langle T, i, 1 \rangle}, r_{\langle T, i, 2 \rangle}, \dots, r_{\langle T, i, i \rangle}\}$, $PR_{\langle U, i, m \rangle} = \{r_{\langle U, i, 1 \rangle}, r_{\langle U, i, 2 \rangle}, \dots, r_{\langle U, i, m \rangle}\}$ and $PR_{\langle B, i, n \rangle} = \{r_{\langle B, i, 1 \rangle}, r_{\langle B, i, 2 \rangle}, \dots, r_{\langle B, i, n \rangle}\}$ respectively.

3.4 Filtering of First-Hand Ratings

The first step towards a scientific and reliable reputation evaluation method is to analyze the retrieved first-hand ratings and filter out those faked ones given by malicious raters. Here, by dishonest ratings we denote those ratings intentionally exaggerating or badmouthing the facts. But for those unintentionally introduced rating deviations such as ratings from lenient raters tend to be a bit higher while ratings from strict raters tend, we will not filter them out. In fact, no matter higher or lower, as long as ratings conform to their rater's rating habit, they will not be classified as dishonest. In this paper, we name this phenomenon by "false dishonesty". The basic idea for our filtering is trying to find inconsistency in a rater's ratings with his usual rating habit, which consists of two parts: "credibility filtering" and "on-spot filtering".

1. Credibility Filtering

This is to examine the trustworthiness of an entity's usual rating behavior. If a rater tends to lie often, no doubt we cannot trust his ratings. In this filtering, we examine ratings familiar to the current evaluator (i.e. the ratings given to entities that the current evaluator has transacted with, we name this the intersection set) and tries to find whether inconsistency exists. Deem that the entity whose ratings are under filtering is e_i . We perform "credibility filtering" in the following way: first get 4 rating sets: ratings given by e_i and the current evaluator to the common pre-evaluating set and the intersection set; then get 2 deviation sets D_{pre} and D_{trans} : D_{pre} is got by comparing e_i 's ratings to the pre-evaluating set with the current evaluator's corresponding ratings, and D_{trans} is got by comparing e_i 's ratings to the intersection set with the current evaluator's corresponding ratings; then compare the fluctuating feature of D_{trans} with D_{pre} , if they are approximately alike, we will not suspect the rater's credibility in this step. In "credibility filtering", we might meet 3 kinds of scenarios:

- 1). Elements in D_{trans} and D_{pre} most distribute in a small interval near 0, which means that e_i shares quite similar rating criteria with the current evaluator. This is the best scenario, and we can believe e_i 's ratings to a large extent with no tuning measures.
- 2). Elements in D_{trans} and D_{pre} most cluster in some same interval not near 0, which means that there is some unintentional deviation in this rater's ratings but can be corrected. This is just what we call "false dishonesty", which shall not be discarded.
- 3). Elements in D_{trans} distribute inconsistently with elements in D_{pre} , which means that e_i might not have a good credibility in rating and his rating shall be filtered out.

For the specific comparison of the distribution features of D_{trans} versus D_{pre} , currently we perform a kind of histogram analysis:

- 1) Divide the deviation space $[-1, 1]$ into n (n is an even natural number) intervals d_1, d_2, \dots, d_n and calculate the probability that elements in D_{trans} and D_{pre} falling into the above n intervals respectively, denoted by $p_{<i,trans>}$ and $p_{<i,pre>}$ ($i=1,2,\dots,n$);
- 2) Calculate the difference $\Delta p_i = |p_{<i,trans>} - p_{<i,pre>}|$ between $p_{<i,trans>}$ and $p_{<i,pre>}$;

- 3) With customized weights for the n intervals $w_1, w_2 \dots w_n$ ($w_1 = w_n > w_2 = w_{n-1} > \dots > w_{n/2} = w_{n/2+1}$ and $\sum_{i=1}^n w_i = 1$), calculate the final distribution deviation degree $DDD_{\langle trans, pre \rangle}$ between D_{trans} and D_{pre} , that is $DDD_{\langle trans, pre \rangle} = \sum_{i=1}^n w_i \times \Delta p_i$. The less the value of $DDD_{\langle trans, pre \rangle}$ is, the less suspicious this rater's credibility. Here, we use $1 - DDD_{\langle trans, pre \rangle}$ to measure a rater's credibility, which will be used in the next step of filtering: on-spot filtering. Given some threshold σ , ratings from this rater will be discarded as dishonest.

2. On-Spot Filtering

In a way, "credibility filtering" given above tends to be a kind of indirect filtering, which examines a rater's ratings familiar to the current evaluator and tries to find inconsistency. While, "on-spot filtering" given below can be seen as a kind of direct filtering, which will examine all the current ratings to the to-be-evaluated entity. This time, we will retrieve all the raters' ratings to the common pre-evaluating set and try to find if inconsistency exists when current rating added into the pre-evaluating set. For example, if an entity's ratings to the pre-evaluating set tend to be a bit higher than others, while his current rating is rather low among all the current ratings, it's probable his current rating is dishonest. Specifically speaking, we perform "on-spot filtering" in the following steps (Deem that the to-be-evaluated entity is e_p , we retrieve n raters $e_1, e_2 \dots e_n$'s rating to e_p : $R_{\langle e_1, e_p \rangle} R_{\langle e_2, e_p \rangle} \dots R_{\langle e_n, e_p \rangle}$):

- 1) Retrieve $e_1, e_2 \dots e_n$'s ratings to the common pre-evaluating set;
- 2) Calculate the average ratings given by the n raters to each item in the pre-evaluating set;
- 3) Calculate the difference ΔPR between each rater's ratings to the pre-evaluating set and the corresponding average ratings;
- 4) Divide the difference space of $[-1, 1]$ into the same n intervals as "credibility filtering" does for the deviation space, and calculate the probability that elements in each rater's difference set falling into the n intervals;
- 5) Modify ratings given by the n raters to e_p by multiply his first-hand rating by his credibility got in "credibility filtering";
- 6) Calculate the average rating of the n modified ratings;
- 7) Calculate the difference between each rater's modified rating to e_p and the average rating got in step 6;
- 8) Observe in which interval each rater's rating difference calculated in step 7 falling into, if elements in ΔPR seldom fall into this interval, then we can conclude that the corresponding current rating is dishonest and shall be filtered out.

3.5 Bias-Tuning of Filtered First-Hand Ratings

After filtering out the faked first-hand ratings, the next step is to remove each rater's bias from its first-hand rating. This is done in an evaluator-centered way, since any

evaluating result is to serve the specific current evaluator. As trust is context specific and the prevalent strangeness of Grid entities, any two entities will have quite few entities transacted with in common not to say in the same context. But with the introduction of the pre-evaluating set, any two Grid entities will at least have the common pre-evaluating set rated in common. In fact, this kind of pre-evaluating set can be seen as a test set while ratings from the current evaluator are the standard outcome and ratings from other entities are testing outcome. If we can find the relationship between an entity's ratings and the current evaluator's, then given any ratings this entity gave, we can estimate the ratings the current evaluator will give. By this means, we remove the other entity's bias and get a rating result conforming to the current evaluator's criteria. What's crucial here is the discovery of this relationship. Actually, this problem can be classified as such a problem: deem there is a function $f(x)$, we only know the function values at $n+1$ data points, that is $f_i=f(x_i), i=1,2,\dots,n+1$, y is another data point, then how to estimate the value of $f(y)$? Deem that an entity e_i wants to evaluate an unknown entity e_j 's reputation $R_{\langle e_i, e_j \rangle}$, which has got entity e_k 's first-hand rating $R_{\langle e_k, e_j \rangle}$ to e_j . Here, ratings of the pre-evaluating set from e_k act as x , while ratings from current evaluator act as $f(x)$; $R_{\langle e_k, e_j \rangle}$ acts as y , while $f(y)$ is the desired to-be worked out tuned result of $R_{\langle e_k, e_j \rangle}$. It is not difficult to find that interpolation is a good choice, for its simplicity and easy of implementation. We will solve this problem in the following three steps:

Step 1: e_i retrieves e_k 's rated pre-evaluating sets and the corresponding ratings from Grid Reputation Service. Since only those sets rated by both can be seen by e_i , the returned pre-evaluating set(s) contain(s) the maximum items rated by both.

Step 2: if the number of returned pre-evaluating set is more than one, perform union operation respectively on the three subsets of the returned pre-evaluating sets. Deem that after union, the three subsets are T_l , U_m and B_n , the ratings for them from e_k are $PR_{\langle T, k, l \rangle}$, $PR_{\langle U, k, m \rangle}$ and $PR_{\langle B, k, n \rangle}$, and the ratings for them from e_i are $PR_{\langle T, i, l \rangle}$, $PR_{\langle U, i, m \rangle}$ and $PR_{\langle B, i, n \rangle}$.

Step 3: according to which category (trustworthy, in-between or untrustworthy) the value of $R_{\langle e_k, e_j \rangle}$ falls into, perform interpolation on this category.

For the specific interpolation method, we can choose polynomial interpolation method such as Lagrange approach, Neville approach or Newton approach. As the Runge phenomenon tells us polynomial interpolation of high degree does not perform well, we will only use linear polynomial, quadratic polynomial and at most cubic polynomial for interpolation. And as is suggested that subsection interpolation can improve precision, we divide the whole pre-evaluating set into three subsets, based on which subsection interpolation is performed. If the number of items in a subset is very big, we can do subsection interpolation again in this subset. As interpolation can be easily implemented in Matlab, we will not elaborate on the specific methods of interpolation here. In Section 4, we will give experimental results.

3.6 Criteria Coherent Degree Based Aggregation of Bias-Tuned First-Hand Ratings

After tuning the bias of first-hand ratings, the next step is to aggregate them and give a final evaluation result. In this paper, we will use the method of weighted averaging where the choosing of a reasonable set of weights is very crucial. As can be seen from human society, if two persons tend to have similar opinion about a lot of affairs, for a specific affair it is probable that they will have similar opinion again. Inversely speaking, if we do not know one person's opinion about some affair, we can make an approximated prediction from the other person's opinion. In fact, this is a kind of incomplete induction. Inspired by this, it is reasonable to give high weights to entities that have similar rating criteria with the current evaluator's. Therefore, we introduce the notion of "Criteria Coherent Degree (*CCD*)" to describe this similarity. Once again, we use the pre-evaluating set as a test set. For the computation of *CCD*, we can adopt the method of approximation from Fuzzy Set such as Hamming approximation or Euclid approximation or Pearson correlation coefficient. With the *CCD* set in hand, we can normalize this set and get the desired weight set for aggregation.

4 Experimental Results

To validate the effectiveness of our method, we have performed a series of simulated experiments. The results show that our method is effective in filtering, tuning and aggregating. We will present results for this 3 aspects respectively in the following sections. The basic configuration of our simulation is: 128 entities; the common pre-evaluating set has 18 items: 7 trustworthy, 6 untrustworthy and 5 in-between; each entity has average 12 ratings for the other entities; 5 types of rating habits: stricter, strict, moderate, lenient and more lenient.

4.1 Results of Dishonest Feedback Filtering

In the experiments for filtering, the deviation space is divided into 8 intervals: $[-1, -0.4], (-0.4, -0.2], (-0.2, -0.07], (-0.07, 0], [0, 0.07], [0.07, 0.2], [0.2, 0.4], [0.4, 1]$ and $w_1 = w_8 = 1/5, w_2 = w_7 = 3/20, w_3 = w_6 = 1/10, w_4 = w_5 = 1/20$. Our simulation is carried out by varying the percentage of malicious entities and retrieving ratings to some randomly selected entity and performing filtering on these ratings. For different percentage of malicious entities from 5% to 75%, we perform 50 filterings each and get 2 average ratios: filtering successful ratio (the ratio of successfully filtered out dishonest feedbacks), and filtering mistaken ratio (the ratio that honest feedbacks being filtered out), as illustrated in Fig.1. As can be seen, our filtering method can effectively filter out dishonest feedback while maintaining the honest feedbacks to a large extent. Experimental results show that those escaped dishonest feedbacks are most exaggerated feedbacks from liars of lenient rating criteria or downplaying feedbacks from liars of strict rating criteria. For the former, since such exaggerated feedbacks will be multiplied by the rater's credibility for later use, its boosting effect will be largely reduced. For the latter, badmouthing a trustworthy entity will at most prevent cooperation with this entity, and there is no practical damage as compared to boosting

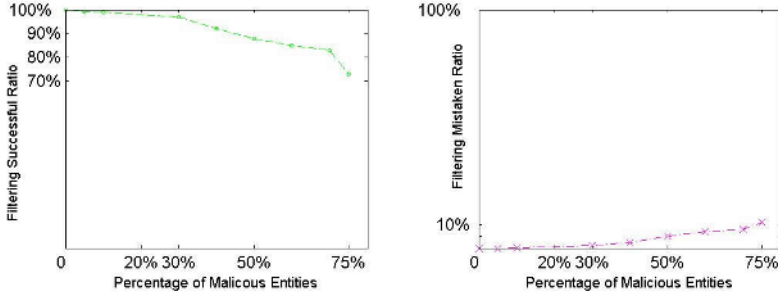


Fig. 1. Filtering successful ratio and filtering mistaken ratio

an untrustworthy entity that leads to cooperation. As a result, this kind of missed filtering will not bring too much harm.

4.2 Results of Bias-Tuning

In the experiment for bias-tuning, five types of entity's bias proneness are given as compared with the current evaluator's rating criteria: stricter, strict, similar, lenient and more lenient. Their ratings to some specific entity are: 0.72, 0.75, 0.83, 0.88 and 0.9. And these ratings have been filtered as honest ones. Ratings from them and the current evaluator to the common pre-evaluating set are listed in Table 2. Since these ratings are all within the trustworthy scope, in Table 1 we only list ratings in the trustworthy subset.

Table 1. Ratings to the trustworthy subset

Entity	Ratings for Trustworthy Subset						
	1	2	3	4	5	6	7
Current Evaluator	0.8	0.82	0.85	0.85	0.88	0.9	0.95
Stricter	0.7	0.73	0.78	0.76	0.8	0.82	0.86
Strict	0.74	0.76	0.8	0.78	0.82	0.84	0.88
Similar	0.81	0.82	0.84	0.86	0.87	0.91	0.95
lenient	0.84	0.87	0.9	0.91	0.93	0.96	0.98
More lenient	0.86	0.89	0.93	0.94	0.96	0.98	1

Table 2. Tuned ratings

Entity	First-hand Ratings	Tuned Ratings			Average Tuning Amount
		Linear Interpolation	Cubic Interpolation	Spline Interpolation	
Stricter	0.72	0.8133	0.8124	0.8041	0.0899
Strict	0.75	0.8100	0.8089	0.8075	0.0588
Similar	0.83	0.8350	0.8394	0.8403	0.0082
lenient	0.88	0.8300	0.8313	0.8341	-0.0482
More lenient	0.9	0.8275	0.8286	0.8310	-0.0710
Standard Deviation	0.0786	0.0109	0.0130	0.0165	

Using linear interpolation, cubic interpolation and spline interpolation in Matlab, we get the following tuned ratings, as shown in Table 2. From the listed average tuning amount, we can see that the more the bias, the more extent is tuned. And from the standard deviation given in the last row in Table 2, we can see that after tuning, deviation between entity's ratings is decreased by a large degree. Therefore, it can be concluded that our tuning method is effective and reasonable. Among the three kinds of interpolation method, the standard deviation of linear interpolation is the smallest.

4.3 Results of CCD-Based Aggregation

To compute *CCD*, we have to use ratings for the whole pre-evaluating set. In Table 1, we have only given ratings for the trustworthy subset. For the untrustworthy subset and in-between subset, ratings are given in Table 3. Using the methods of Hamming approximation, Euclid approximation and Pearson correlation coefficient, we get CCDs listed in Table 4. As can be seen from the last row of standard deviation, Euclid approximation makes a better distinction. Therefore, we choose to use the CCD results from this method. Using the tuned ratings from linear interpolation and normalized CCD results from Euclid approximation, the final result of reputation is: 0.8234.

Table 3. Ratings to the untrustworthy set and in-between set

Entity	Ratings for Untrustworthy Subset						Ratings for In-between Subset				
	1	2	3	4	5	6	1	2	3	4	5
Current Evaluator	0.15	0.20	0.24	0.30	0.32	0.33	0.50	0.52	0.60	0.64	0.66
Stricter	0.05	0.08	0.12	0.15	0.18	0.20	0.42	0.50	0.55	0.60	0.62
Strict	0.10	0.15	0.18	0.20	0.20	0.25	0.45	0.48	0.51	0.56	0.6
Similar	0.13	0.20	0.25	0.28	0.30	0.32	0.50	0.51	0.60	0.65	0.65
lenient	0.18	0.22	0.26	0.34	0.35	0.38	0.52	0.55	0.63	0.66	0.68
More lenient	0.22	0.28	0.31	0.35	0.37	0.40	0.53	0.57	0.65	0.66	0.69

Table 4. CCD results

Entity	CCD Results		
	Hamming	Euclid	Pearson
Stricter	0.9117	0.9050	0.9940
Strict	0.9328	0.9300	0.9974
Similar	0.9911	0.9889	0.9994
lenient	0.9639	0.9613	0.9991
More lenient	0.9400	0.9369	0.9974
Standard deviation	0.0305	0.0319	0.0021

5 Conclusions and Future Work

In this paper, we mainly focus on the problem of trust establishment between unknown entities in Grid, which frequently happens. We resort to reputation mechanism as a

solution, in which a scientific reputation evaluation method is crucial to the success of the whole mechanism. We propose a pre-evaluating set based trust model, which aims at tackling some particular obstacles for reputation evaluation in Grid such as the sparseness of ratings and the strangeness of entities, which is rarely considered in most evaluation methods currently available. Our distinct feature is the introduction of this pre-evaluating set, which provides context specific behaviors for entities to rate in common. As a common rated set with no specific benefits involved, ratings for this set can be expected to truthfully reflect an entity's rating criteria. These ratings have 3 fundamental usages in our trust model: 1) Dishonest feedbacks can be filtered out when inconsistency exists between these ratings and the actual ratings. With rating criteria in mind, our filtering method distinguishes well between real dishonesty and false dishonesty. 2) A certain relationship between rating flavors of some rater and the current evaluator can be estimated, with which we can effectively tune this rater's ratings to cater to the current evaluator's criteria. This is done by means of interpolation. 3) We can estimate how similar a certain rater's ratings will be to the current evaluator's. The more similar, the more his ratings should be considered. And we propose a notion of "Criteria Coherent Degree" to describe this similarity, which is used as weight for aggregation after normalization.

In this paper, we classify reputation values into three kinds: trustworthy, in-between and untrustworthy, and deem that first-hand ratings from all the raters will fall into the same category. Next, we will consider how if values are not classified and how if first-hand ratings fall into different categories.

References

1. Markus Lorch, Dennis Kafura: Grid Community Characteristics and their Relation to Grid Security. VT CS Technical Report, 2003. <http://zuni.cs.vt.edu/publications/draft-ggf-lorch-grid-security-version0.pdf>
2. Farag Azzedin and Muthucumar Maheswaran: Evolving and Managing Trust in Grid Computing Systems. Proceedings of the 2002 IEEE Canadian Conference on Electrical Computer Engineering
3. Alfarez Abdul-Rahman and Stephen Hailes: Supporting Trust in Virtual Communities. In proceedings of the 33rd Hawaii International Conference on System Sciences: volume 6, Jan, 2000
4. B. Yu and M.P. Singh. A Social Mechanism of Reputation Management in electronic Communities. In Cooperative Information Agents (2000) 154–165
5. Chrysanthos Dellarocas. Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior. In Proceedings of the 2nd ACM Conference on Electronic Commerce, Minneapolis, MN, October 17–20, 2000
6. A. Whitby, A. Josang and J. Indulska. Filtering out unfair ratings in bayesian reputation systems. In Proceedings of the Workshop on Trust in Agent Societies, at the 3rd International conference on Autonomous Agents & Multi Agent Systems, 2004
7. Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina: The EigenTrust Algorithm for Reputation Management in P2P Networks. In Twelfth International World Wide Web Conference, 2003, <http://www.stanford.edu/~sdkamvar/papers/eigentrust.pdf>

8. E. Damiani, D. C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante: Reputation-based Method for Choosing Reliable Resources in Peer-to-peer Networks. In Proc. of the 9th ACM Conference on Computer and Communications Security (2002)
9. B. Yu and M. P. Singh. An Evidential Model of Distributed Reputation Management. In Proceedings of the first international joint conference on Autonomous Agents and Multiagent Systems: Part 1 (2002) 294–301
10. M. Richardson, R. Agrawal, and P. Domingos. Trust management for the Semantic web. In Proceedings of the Second International Semantic Web Conference (2003) 351–368
11. Li Xiong and Lin Liu: PeerTrust: Supporting Reputation-Based Trust in Peer-to-Peer Communities. IEEE Transactions on Knowledge and Data Engineering (TKDE), Special Issue on Peer-to-Peer Based Data Management, 16(7), July, 2004
12. Paolo Massa and Bobby Bhattacharjee: Using Trust in Recommender Systems: an Experimental Analysis. *itrust 2004*. Lecture Notes in Computer Science, Vol. 2995. 221–235
13. Xiangli Qu, Nong Xiao, Guang Xiang, Xuejun Yang: Reputation-aware Contract-supervised Grid Computing. GCC Workshops 2004. LNCS, Vol. 3252. (2004) 44–51
14. K.Czajkowski, I.Foster, C.Kesselman: "SNAP:A Protocol for Negotiating Service Level Agreements and Coordinating Resource Management in Distributed Systems", LNCS, Vol. 2537. Springer-Verlag (2002) 153–183
15. Xiangli Qu, Xuejun Yang, Yuhua Tang and Haifang Zhou: A Behavior Characteristics-based Reputation Evaluation Method for Grid Entities. EGC 2005. Lecture Notes in Computer Science, Vol. 3470. Springer-Verlag Berlin Heidelberg (2005) 567–577

A Spreading MIMO-OFDM Transmission Scheme for Wireless Mobile Environment^{*}

Sang Soon Park¹, Tae Jin Hwang², Juphil Cho³, and Heung Ki Baik⁴

^{1,2} Department of Electronic Engineering,
Chonbuk National University,
Jeonju, Korea

spwman@chonbuk.ac.kr

³ School of Electronics and Information Engineering,
Kunsan National University, Kunsan, Korea

⁴ Division of Electronics and Information,
Chonbuk National University,
Jeonju, Korea

Abstract. In this paper, we propose a simple MIMO-OFDM with time and frequency domain spreading for mobile environment. The transmission scheme that we propose in this paper is a simple method with low complexity for improving the performance of conventional SFBC-OFDM. Using Hadamard transformation in time and frequency domain, we can obtain space, time and frequency diversity gain. Also we propose the spreading hybrid MIMO-OFDM system combined spreading SFBC-OFDM with SM scheme.

1 Introduction

The explosive growth of wireless communications is creating the demand for high speed, reliable, and spectrally-efficient communications over the mobile wireless medium. Space-time block coding (STBC) is a attractive technique as a simple transmit diversity scheme for providing highly spectrally efficient wireless communications[1]. The STBC was applied to the OFDM (Orthogonal Frequency Division Multiplexing) as an attractive solution for a high bit rate data transmission in a multi-path fading environment. This system was referred to as the space-time block coded OFDM (STBC-OFDM)[2]. And the space-frequency block coded OFDM (SFBC-OFDM) has been proposed where the block codes are formed over the space and frequency domain[3].

In this paper, we propose a simple MIMO-OFDM with time and frequency diversity gain. This transmission scheme is a simple method for improving a performance of conventional SFBC-OFDM[3] by means of Hadamard transformation in time and frequency domain. Also we propose the spreading hybrid MIMO-OFDM system combined spreading SFBC-OFDM with SM (spatial multiplexing) scheme[5][6].

^{*} This work was supported by Korea Research Foundation Grant (KRF-2003-041-D00394).

2 Spreading SFBC-OFDM Transmission Scheme

In this section, we will propose a simple SFBC-OFDM transmission scheme to achieve time diversity gain. We can achieve time diversity gain by means of Hadamard transformation in time and frequency domain. The encoding of our SFBC codes is carried out in two successive stages: Hadamard transformation in time domain and SF component coding as Fig. 1.

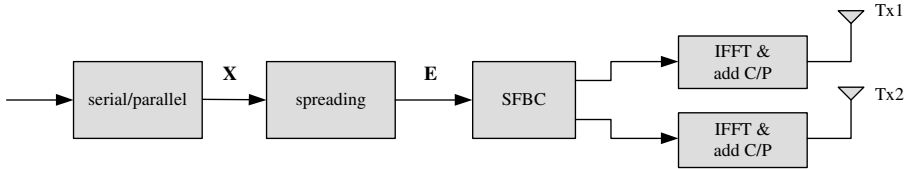


Fig. 1. Spreading SFBC-OFDM transmission scheme

2.1 Spreading in Time and Frequency Domain

At the transmitter, the input data bits are modulated to $x(m)$ where $x(m)$ denotes the input serial data symbols with symbol duration T_s . The modulated symbols are serial to parallel converted and the resulting data vector $\mathbf{x}(n)$ and data block \mathbf{X} are given by

$$\begin{aligned} \mathbf{x}(n) &= [x_0(n) \quad x_1(n) \quad \cdots \quad x_{N-1}(n)]^T \\ \mathbf{X} &= [\mathbf{x}(BK) \quad \mathbf{x}(BK + 1) \quad \cdots \quad \mathbf{x}(BK + K - 1)] \end{aligned} \tag{1}$$

Let \mathbf{E} be the Hadamard transform of \mathbf{X} in time and frequency domain, and we can express \mathbf{E} as follows.

$$\mathbf{E} = (\mathbf{W}_M \otimes \mathbf{I}_{N/M}) \mathbf{X} \mathbf{W}_K \tag{2}$$

where \mathbf{W}_M represents Hadamard transform matrix of order M

$$\mathbf{W}_2 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \mathbf{W}_{2^a} = \mathbf{W}_2 \otimes \mathbf{W}_{2^{a-1}} \tag{3}$$

where \otimes represents Kronecker product. Hadamard transform spreads each symbol to M subcarriers and K successive OFDM symbols. Therefore matrix \mathbf{E} is a symbol matrix spreaded in time domain.

2.2 Space-Frequency Component Coding

After spreading the data matrix in time domain, perform the SFBC. During the block instant n , the spreaded symbol vector $\mathbf{e}(n)$ can be expressed as follows.

$$\mathbf{e}(n) = [e_0(n) \quad e_1(n) \quad \cdots \quad e_{N-1}(n)]^T \tag{4}$$

The spread symbol vector $\mathbf{e}(n)$ is coded into two vectors $\mathbf{e}^{(1)}(n)$ and $\mathbf{e}^{(2)}(n)$ by the SFBC as follows.

$$\begin{aligned} \mathbf{e}^{(1)}(n) &= [e_0(n) \quad -e_1^*(n) \quad \cdots \quad e_{N-2}(n) \quad -e_{N-1}^*(n)]^T \\ \mathbf{e}^{(2)}(n) &= [e_1(n) \quad e_0^*(n) \quad \cdots \quad e_{N-1}(n) \quad e_{N-2}^*(n)]^T \end{aligned} \tag{5}$$

During the block instant n , $\mathbf{e}^{(1)}(n)$ is transmitted from the first transmit antenna Tx1 while $\mathbf{e}^{(2)}(n)$ is transmitted simultaneously from the second transmit antenna Tx2. Let $\mathbf{e}_e(n)$ and $\mathbf{e}_o(n)$ be two length $N/2$ vectors denoting the even and odd component of $\mathbf{e}(n)$.

$$\begin{aligned} \mathbf{e}_e(n) &= [e_0(n) \quad e_2(n) \quad \cdots \quad e_{N-2}(n)]^T \\ \mathbf{e}_o(n) &= [e_1(n) \quad e_3(n) \quad \cdots \quad e_{N-1}(n)]^T \end{aligned} \tag{6}$$

Table 1. shows the SF component coding for two-branch transmit diversity scheme [3]. The SF coded symbols are modulated by IFFT into SF-OFDM symbols. After adding the guard interval, the proposed SF-OFDM symbols are transmitted as Fig. 1.

Table 1. Space-Frequency component coding

Subcarrier index	Tx1	Tx2
Even	$\mathbf{e}_e(n)$	$\mathbf{e}_o(n)$
Odd	$-\mathbf{e}_o^*(n)$	\mathbf{e}_e^*

2.3 Decoding of Spreading SFBC-OFDM

Decoding processes are the reverse order of the encoding and carried out following two stages.

- First stage: perform the decoding with SF component decoding to obtain $\hat{\mathbf{E}}$, the estimation block of \mathbf{E}
- Second stage: perform the reverse of Hadamard transformation to obtain decision matrix $\hat{\mathbf{X}}$ from $\hat{\mathbf{E}}$. And \mathbf{X} is recovered by ML decision.

Let $\mathbf{y}(n)$ be a demodulated signal vector at the receiver and $\mathbf{y}_e(n)$, $\mathbf{y}_o(n)$ be two length $N/2$ vectors denoting the even and odd component of $\mathbf{y}(n)$. Let $\mathbf{\Lambda}(n)$ be a diagonal matrix whose diagonal elements are the DFT of the channel impulse response.

$$\mathbf{\Lambda}(n) = \text{diag}(\lambda_0(n) \quad \lambda_1(n) \quad \cdots \quad \lambda_{N-1}(n)) \tag{7}$$

Let $\mathbf{\Lambda}^{(1)}(n)$, $\mathbf{\Lambda}^{(2)}(n)$ be channel responses of transmit antenna1, 2, and $\mathbf{z}(n)$ be the channel noise. The demodulated signal vector at the receiver is given by

$$\begin{aligned}
 \mathbf{y}_e(n) &= \mathbf{\Lambda}_e^{(1)}(n)\mathbf{e}_e^{(1)}(n) + \mathbf{\Lambda}_e^{(2)}(n)\mathbf{e}_e^{(2)}(n) + \mathbf{z}_e(n) \\
 \mathbf{y}_o(n) &= \mathbf{\Lambda}_o^{(1)}(n)\mathbf{e}_o^{(1)}(n) + \mathbf{\Lambda}_o^{(2)}(n)\mathbf{e}_o^{(2)}(n) + \mathbf{z}_o(n)
 \end{aligned}
 \tag{8}$$

Assuming the complex channel gains between adjacent subcarriers are constant, i.e., $\mathbf{\Lambda}_e^\alpha(n) \approx \mathbf{\Lambda}_o^\alpha(n)$, and the estimate vectors $\hat{\mathbf{e}}(n)$ as follows.

$$\begin{aligned}
 \hat{\mathbf{e}}_e(n) &= \mathbf{\Gamma}^{-1}(\mathbf{\Lambda}_e^{(1)*}(n)\mathbf{y}_e(n) + \mathbf{\Lambda}_o^{(2)}(n)\mathbf{y}_o^*(n)) \\
 \hat{\mathbf{e}}_o(n) &= \mathbf{\Gamma}^{-1}(\mathbf{\Lambda}_e^{(2)*}(n)\mathbf{y}_e(n) - \mathbf{\Lambda}_o^{(1)}(n)\mathbf{y}_o^*(n))
 \end{aligned}
 \tag{9}$$

where $\mathbf{\Gamma} = |\mathbf{\Lambda}_e^{(1)}(n)|^2 + |\mathbf{\Lambda}_e^{(2)}(n)|^2 \approx |\mathbf{\Lambda}_o^{(1)}(n)|^2 + |\mathbf{\Lambda}_o^{(2)}(n)|^2$.

The estimate vector $\hat{\mathbf{e}}(n)$ is vectors to estimate the magnitude of $\mathbf{e}(n)$ as well as phase. Let estimate matrix $\hat{\mathbf{E}}$ be the matrix composed of K estimate vectors, and we can express $\hat{\mathbf{E}}$ as follows.

$$\hat{\mathbf{E}} = [\hat{\mathbf{e}}(0) \quad \hat{\mathbf{e}}(1) \quad \dots \quad \hat{\mathbf{e}}(K-1)]
 \tag{10}$$

Perform the reverse of Hadamard transformation to obtain decision block $\hat{\mathbf{X}}$ from $\hat{\mathbf{E}}$, and

$$\hat{\mathbf{X}} = (\mathbf{W}_M \otimes \mathbf{I}_{N/M})^{-1} \hat{\mathbf{E}} \mathbf{W}_K^{-1} = (\mathbf{W}_M \otimes \mathbf{I}_{N/M}) \hat{\mathbf{E}} \mathbf{W}_K
 \tag{11}$$

$\hat{\mathbf{X}}$ are vectors to estimate the magnitude of \mathbf{X} as well as phase. Therefore we can recover \mathbf{X} by means of equation (9) in paper [1], even if \mathbf{X} has the unequal energy constellations.

3 Spreading Hybrid MIMO-OFDM

In this chapter, we will consider the spreading hybrid MIMO-OFDM system. This system is hybrid system combined spreading SFBC-OFDM with SM(spatial multiplexing) scheme.

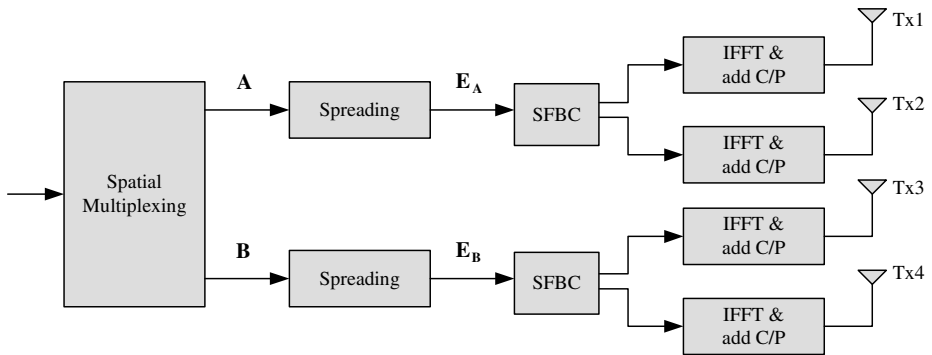


Fig. 2. Spreading Hybrid MIMO-OFDM transmission scheme

Fig. 2 shows the spreading hybrid MIMO-OFDM system for 4-transmit antennas. As Fig. 2, the individual data matrices A and B are coded by spreading SFBC-OFDM and transmitted through 4-transmit antennas.

4 Simulation Results

In this section, we present the results of computer simulation. Table 2 shows the simulation parameters.

Table 2. Simulation parameters for performance evaluation

Carrier frequency(f_c)	2 GHz
Channel Bandwidth	5 MHz
Mobility (Maximum Doppler Frequency: f_D)	120km/h (222Hz)
Sampling frequency(f_s)	5MHz
RMS delay spread(τ_{RMS})	1 μ s
Channel Model	COST-207 [TU]
Subcarrier spacing	19.531 kHz
FFT size(length: T_s)	512 (102.4 μ s)
CP size(length : T_G)	28(5.6 μ s)
OFDM symbol length(T_{sym})	108 μ s

Fig. 3 shows the simulation results of conventional SFBC-OFDM and the spreading SFBC-OFDM at the velocity =120 km/h. The COST207 six-ray typical urban (TU) channel power delay profile was used throughout the simulations [4]. The SFBC-OFDM systems employed 512 subcarriers with QPSK modulation. The SFBC-OFDM schemes using two transmit antennas and one receive antenna.

Fig. 4 show the simulation results of the hybrid MIMO-OFDM and the spreading hybrid MIMO-OFDM at the velocity =120 km/h with QPSK modulation. These systems use four transmit antennas and two receive antennas. Also we use the ZF(zero forcing) and MMSE(minimum mean square error) detection schemes in Fig. 4.

In Fig. 3 and Fig. 4, each channel is uncorrelated. And it was assumed that perfect channel estimation was available at the receiver.

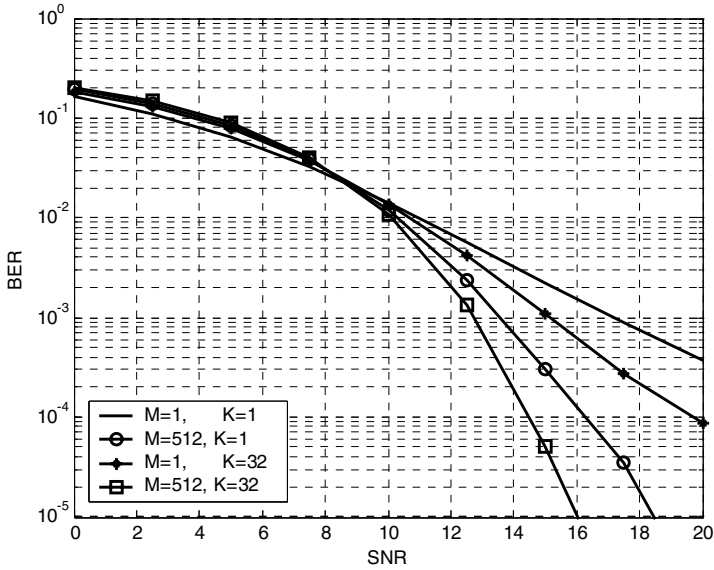


Fig. 3. Performance comparison of spreading SFBC-OFDM

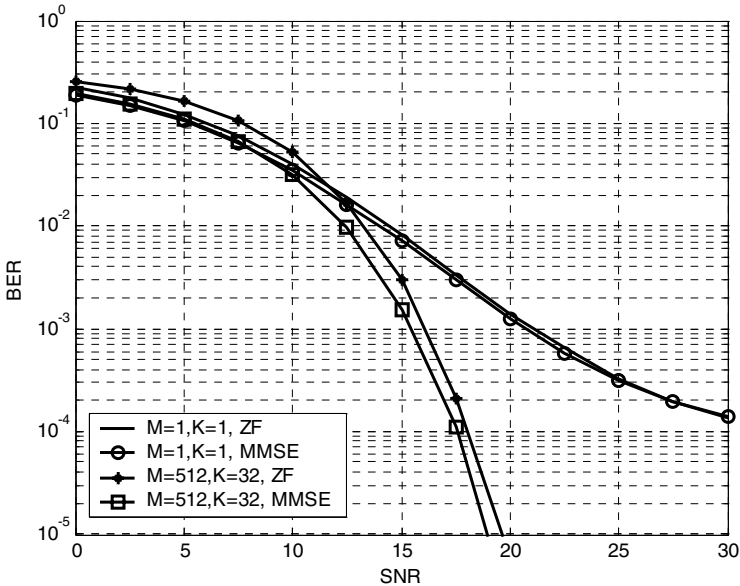


Fig. 4. Performance comparison of spreading hybrid MIMO-OFDM

5 Conclusions

We have proposed a spreading SFBC-OFDM transmission scheme that is a method for improving the performance of conventional SFBC-OFDM, by means of Hadamard

transform in time and frequency domain. And we compared the performance of spreading SFBC-OFDM transmission schemes with conventional SFBC-OFDM. In frequency selective channels, we can obtain frequency diversity gain. Also the Doppler spread is large, complex channel gains over K successive OFDM symbols vary rapidly. In this case, the spreading SFBC-OFDM can obtain time diversity gain and improve the BER performances. Also we have propose a spreading hybrid MIMO-OFDM and show the BER performances.

References

- [1] S. M. Alamouti, "A simple transmitter diversity scheme for wireless communications," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 1451-1458, Oct. 1998.
- [2] K. F. Lee and D. B. Williams, "A space-time coded transmitter diversity technique for frequency selective fading channels," *IEEE Sensor Array and Multichannel Signal Processing Workshop*, pp. 149-152, Cambridge, MA, Mar. 2000.
- [3] K. F. Lee and D. B. Williams, "A space-frequency transmitter diversity technique for OFDM system," *IEEE GLOBECOM 2000*, vol. 3, pp. 1473-1477, San Francisco, USA, Nov. 2000.
- [4] COST207 TD(86)51-REV 3 (WG1), "Proposal on channel transfer functions to be used in GSM tests late 1986," Sept. 1986.
- [5] A. J. Paulraj, D. A. Gore, R. U. Nabar, and H. Bolcskei, "An overview of MIMO communications – A key to gigabit wireless," *Proc. of IEEE*, vol. 92, no. 2, pp.198–218, Feb. 2004.
- [6] E. Telatar, "Capacity of multiple-antenna Gaussian channel," *AT&T Bell Labs Tech. Memo.*, June 1995.

A Security Auditing Approach Based on Mobile Agent in Grid Environments*

Zhenghong Xiao¹, Changqin Huang², and Fuyin Xu²

¹ Department of Computer Science and Technology,
Hunan University of Arts and Science, Changde, 415000, P.R. China
xiaozh@tsinghua.org.cn

² Department of Computer Sciences and Technology,
South China Normal University, Guangzhou, 510631, P.R. China
cqhuang@zju.edu.cn, xufy@scnu.edu.cn

Abstract. Due to the dynamic and multi-institutional nature, auditing is fundamental and difficult to solve in grid computing. In this paper, we identify security-auditing requirements, and propose a Cross-Domain Security Auditing (CDSA) architecture, in which mobile agent is applied to help gathering security information in the grid environment. Whilst a new authorization mechanism is presented to improve the performance by changing the traditional manner "route once, switch many" over the network into the "audit once, authorize many" in the Grid, and a multi-value trust relationship model is constructed in order to carry out the dynamic auditing. The system enforces these mechanisms to enable cross-domain security in the aid of special services based on Globus Toolkit version 3.0 and IBM Aglet.

1 Introduction

Security is one of the most challenging issues in grid computing. In recent years, grid security has been paid widespread attention as an important new branch in the field of Computing Grid, Data Grid, and Semantic Grid etc. The majority of existing researches on grid security have taken place in the field of naming and authentication, Secure Communication, Trust, Policy, and Authorization, Enforcement of Access Control [1]. As one of fundamental requirements, although some relevant discussion has occurred and/or is going on at GGF, auditing and accounting solutions are still in the early stages [2]. Significant challenges [1] remain for computing grid as cross-domain auditing, privacy management, denial of service, and integrated. In general, grid security and computer security will never be completely "solved", but undoubtedly our works will make the Grid infrastructure trustworthy.

In this paper, we focus on the design and deployment of cross-domain security auditing architecture based on mobile agent by Globus Toolkit 3.0 and IBM Aglet. The key of auditing in the Grid is how to get security information cross-virtual organization (VO) and how to process security information. The usual ways of getting packs from the network are not suitable for auditing in the Grid at all. By our method,

* The work is supported by the Scientific Research Fund of Hunan Provincial Education Department(Grant No. 04A037), and the Hunan Natural Science Fund (Grant No. 05JJ40098).

Surveillant Agent is used to gather security information of hosts, and Mobil agent is used to transfer cross-domain security information. To decrease impact on the grid performance, a new secure authorization mechanism is presented by changing the traditional manner "route once, switch many" over the network into the "audit once, authorize many" in the Grid. The dynamic auditing is carried out via dividing domain trust relationship into complete trust type, partial trust type, and least trust type.

This paper is organized as follows: Section 2 describes security-auditing requirements. In Section 3, the proposed cross-domain security auditing architecture and related work are described. Authorizing policy: "Audit once, authorize many" is presented in Section 4. By constructing a multi-value trust relationship model, the enforcement of dynamic auditing is introduced in Section 5. In section 6, based on Globus Toolkit version 3.0 and IBM Aglet, the implementation of CDSA is described. Finally, conclusions and future work are addressed in Section 7.

2 Security Auditing Requirements

Grid resource auditing is the more traditional manner of accounting for resources usage and billing. Grid Auditing is a focus of accounting as a security component and the need for a seamless relationship between accounting, the authentication and authorization components of Grid [2]. It is necessary for system administrator and grid administrator to audit Grid resource, this auditing information can be used as either billing, or security auditing, it is also be used to intrusion detect. The contents of auditing are various, and system administrator and Grid administrator determine the auditing granularity. Security auditing requirements comprise: (a) it must strictly make a record for grid user access to node resources, which includes the access time, grid user's IDs, job's IDs, results (success, failure). (b) Logging them based upon the specified policies, only authorized users can browse related records, unauthorized users' trace records should be registered. (c) Due to existing of lots of grid users, it is essential to adopt appropriate auditing policies to enhance auditing efficiency. (d) During monitoring the access to resources, we should identify abnormal behavior, such as intrusion. If necessary, corresponding measures are taken. (e) It is necessary to establish a new mechanism for creating security-auditing trails that can be used to validate if the authorization policy is enforced correctly on local resources.

3 The Cross-Domain Security Auditing Architecture

At present, there exist many trust researches for the grid. A CA-based trust model was drafted [3] and is being proposed to Global Grid Forum (GGF). The X.509 trust [4] is a centralized approach such that each participant has a certificate by a central CA. The SPKI trust model [5] offers more flexibility by supporting delegation certificates. The literature [6] proposes a two-level trust model, the upper level defines the trust relationships among virtual organizations in a distributed manner, and the lower level justifies the trust values within a grid domain. However, all trust model related only to an authorization mechanism, didn't related to auditing system.

In the paper, the Cross-Domain Security Auditing architecture is concerned with the gathering security information from different nodes, transferring security

information, authorizing management policy, and auditing policy based on trust relationship type. This architecture has some distinct features, such as flexibility, scalability, platform independence, and reliability. The CDSA applies two sets of software entities, called surveillant agents and mobile agents. Surveillant agents reside in each virtual organizations, and responsible for gathering security information of hosts. Mobile agents are software components that can migrate to all the virtual organizations in grid environments, and autonomously execute the tasks of transferring security information. The components of CDSA are identified as follows: Central Mobile Agent (CMA), Global Database (GD), Mobile Agent (MA), Surveillant Agent (SA), Local Database (LD), User Agent (UA), and Database Agent (DA). The overall architecture of the CDSA is shown in Fig.1.

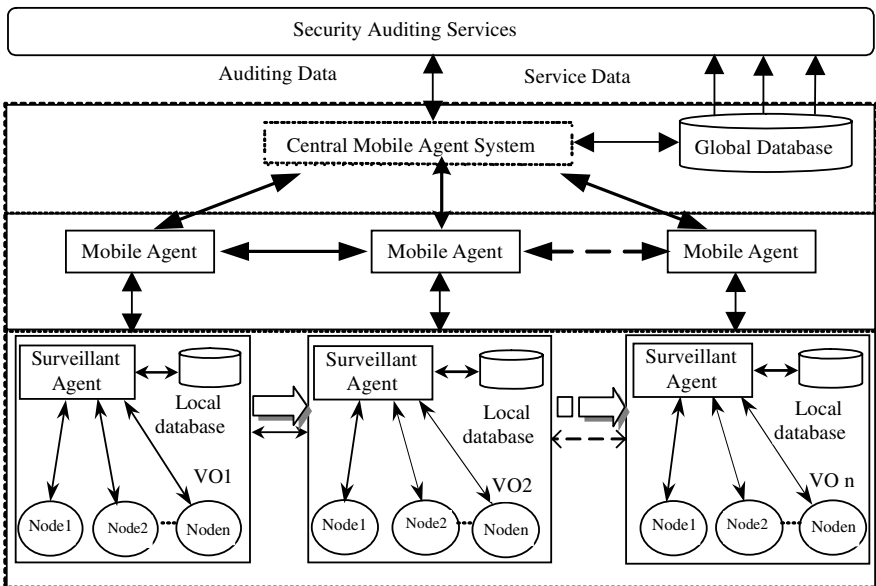


Fig. 1. The architecture for cross-domain security auditing

4 Authorization Policy: “Auditing Once, Authorize Many”

"Route once, switch many" means that when packets pass through routing switches, if an IP address of packets itself exists in the hardware route table; the packet is forwarded directly via switch hardwires. If an IP address of packets is not found in the route table, it needs to be routed. After it is processed by filter module, CPU writes the route entry into the route table after routing. In our security auditing system utilizes in the similar manner.

The important problem of security auditing is how to analyze and filter user access information with little interference of forwarding performance. The base architecture and user’s authorization request of cross-domain is analyzed by referring to Fig.2.

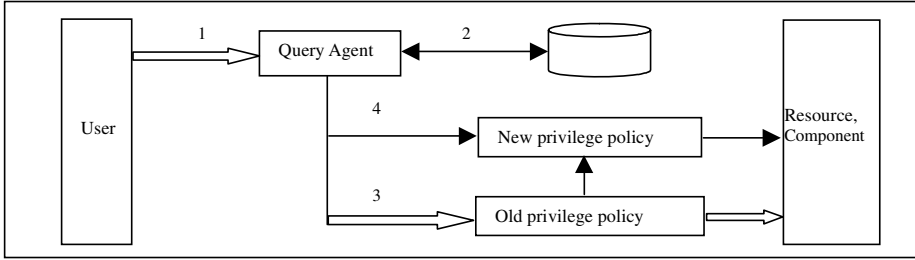


Fig. 2. Authorization policy: "Auditing once, authorize many"

1. A user’s request to Grid resources, after getting into currently domain by Migrate Agent, Query Agent searches security auditing records such as user’s ID, user’s authentication, task management privilege, etc, in local database.
2. If user’s ID is not founded, or there is not enough privilege to grid resource, user’s request needs to be audited, then users access grid resources according to a new privilege policy, which is formed by integrating feedbacks of authorization into local privilege policy of domain, finally, it updates the local database.
3. If user’s ID is found and there is enough privilege to grid resource, then users access the grid resource according to old privilege policy.

Because QA has little influence on forwarding performance, a new secure mechanism of authorization is given to modify the traditional manner "route once, switch many " over the network to the "audit once, authorize many" in the Grid.

5 Auditing Policy Based on Trust Relationship Type

This paper proposes trust relationship type for auditing policy, our approaches divide trust relationship among domains into three trust relationship type: complete trust type, partial trust type, least trust type. Complete trust type is most trust relationship among domains, when user from one domains request Grid resource of another, it is not necessary to audit and authorize. Partial trust type is medium trust relationship among domains, when Grid resource requested, there are a selection auditing or no auditing. Least trust type is least trust relationship among domains, when users request Grid resource, it is essential to authorize and audit. The strength of trust relationship among domains varies as shown Fig.3:

The reputation of an entity is an expectation of its behavior based on other entities’ observations or information about the entity’s past behavior within a specific context at a given time [7]. Trust relationship among domains varies according to x direct relationship with y as well as the reputation of y, the trust model should compute the eventual trust based on a combination of direct trust and reputation and should be able to weight the components differently, trust relationship exponent computation and trust relationship conversion are as follow:

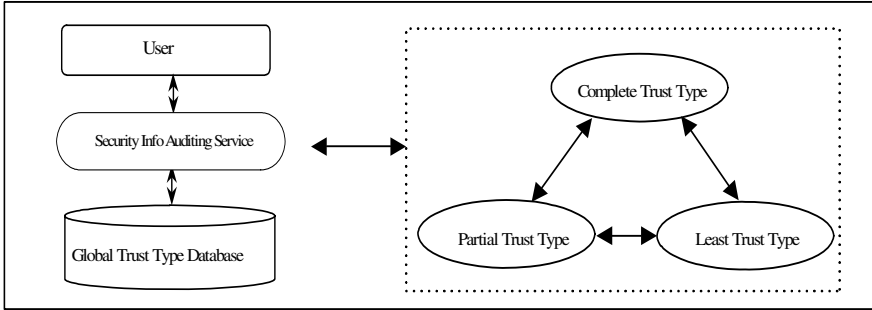


Fig. 3. Auditing mechanism based on trust relationship type

1. Let T_{α} denote trust relationship exponent among domains, T_{α} computation impose similar $\Gamma[11]$, Let M and N denote two domains, the direct relationship of M and N denotes $DR(M, N)$, the reputation of N denote $RR(N)$, the weights given to direct and reputation relationship are α and β , in the decay function $\gamma(t-t_{ij})$, t is the current time and t_{ij} is the time of the last update or the last transaction between M and N , the literature[11] introduced the recommend trust factor $R(M,N)$ to prevent cheating via collusions among a group of domains. In this paper, instead of mentioned above $R(M, N)$, feedback of auditing expressed R , R is a value between 0 and 1. we suppose that one domain borders K domains. Trust relationship exponent compute as follows:

$$T_{\alpha} = \alpha * DR(M, N) * \gamma(t - t_{ij}) + \beta * \sum_{k=1}^n RR(N) * R(M, N) * r(t - t_{ij}) / K \quad (1)$$

2. Let T_{η} denote the threshold of convert according to feedback of auditing, if partners of transaction are satisfied, the trust exponent of among domains increases, while $T_{\alpha} > T_{\eta}$, Least trust relationship convert into Partial Trust Type (PTT), or From PTT to Complete trust Type. If partners of transaction are not satisfied, the trust exponent of among domains decreases, while $T_{\alpha} < T_{\eta}$, Complete Trust Type converts into Partial Trust Type (PTT), or from PTT to Least trust Type.

6 Implementation of CDSA Based On GT3 Core and IBM Aglet

6.1 Agent Service Based On GT3 Core

In this paper, we define Surveillant Agent Service and Mobile Agent Services as user-defined services of grid nodes, which are built on the top of the GT3 core [8]. Mobile agents facilitate Gathering Security Auditing Information Service to implement its functions, and the mobile agent service is based on IBM Aglets by modifying core component. The architecture of agent service based on GT3 core is as shown in Fig.4.

Mobile Agent Service	
Surveillant Agent Service	
Base Services	
System-Level Services	
OGSI Reference Implementation	Security Infrastructure
Web Service Engine	
Globus GT3 Core Environment	

Fig. 4. Agent Service Based On GT3 Core

6.2 Building Mobile Agent Platform Based on IBM

Because these natures of grid applications (such as distribution) very closely resembles that of mobile agent applications, both applications are characterized by heterogeneity of participating nodes with varying trust relationship between constituent nodes, and each agent is autonomous, cooperative, coordinated, intelligent, rational and able to communicate with other agents. Our work applied mobile agent to resolve the problem of cross-domain security auditing in the Grid. The CDSA is a distributed mobile agent system based on user-defined services of Globus Toolkit Version 3.0 and IBM Aglet that comprised of six types of agent [9][10]: Central Mobile Agent (CMA), Mobile Agent (MA), Surveillant Agent (SA), User Agent (UA), Query Agent (QA), and Database Agent (DA). They coordinate and cooperate with each other to accomplish gathering security information of hosts, dumping into a local database, and transferring cross-domain security information.

1. UA provides services for user, and accepts security auditing request, and returns auditing results. In addition, user agent can translate request into commands that the agent can identify.
2. CMA is the key to implements of cross-domain security auditing architecture, it is responsible to collect and administrate all kinds security auditing information. At the same time, it acts as Certificate Authority center, and ensures security communication among agent's subsystem. Via DA, all security information of CMA for auditing is stored in a global database.
3. SA is distributed in every virtual organization; it gathers user name, password, user's ID, access time, user's authentication, digital certificate information, and task management privilege by user-defined Gathering Security Information Service of GT3 after completing authentication. This primitive information will be sent to DA or MA according to user's requests.
4. MA receives security auditing information from SA, or receives UA request commands, which can be transferred from one node to another node.

5. DA acts as an application server or database middleware, it is used to securely access data in local database in the Grid by using interface of Servlet, via DA, all security information of SA is stored in local database.
6. QA receives UA request, and queries security auditing information in global database according to user's request, if there is no record found, user's request information is dispatched to every sites by MA, then QA queries security auditing information in local database.

The system security is guaranteed by authenticating, authorizing, and Aglet's secure mechanism. When agents communicate in virtual organization, they share a key, Aglet's Workbench considers trust each other. When agents communicate in different virtual organization, it provides a secure interface by a proxy, Aglet connects remote Aglet, and the system generates a proxy in local context environment, which is similar to authorization management chain in the Grid.

All components of the CDSA are developed using JAVA platform; Aglet system can implement agent's security by using `com.ibm.aglets.security` packets, and can accomplish interoperability among agents by using `com.ibm.maf.mAFAgentSystem` packets. Whilst it can fulfill interaction with user by applying Servlet technology and accomplish communication among agents based on KQML semantic representation.

6.3 User Auditing Services

User auditing Services are constructed by utilizing the services defined at each lower layer. Auditing requirements processing utilizes Apache AXIS as their Web service engine, which executes in a J2EE/J2SE Web container. Such an application can directly access the auditing result, or can monitor the heterogeneous resource and the status of each node.

7 Conclusions and Future Work

In this paper, we identify security-auditing requirements in grid environments, and propose a Cross-Domain Security Auditing architecture based on Mobile Agent. The task of auditing in the Grid is how to get cross-domain user's security log and analyze it according to auditing rules. Our method applies surveillant agent to collect security information of hosts, and invoke Mobile Agent to deliver the security information in a manner of all to one. To reduce impact on the performance, a new secure mechanism is enforced by changing the traditional "route once, switch many" over the network into the "audit once, authorize many" in the Grid. To implement dynamic auditing policy, the trust relationship among domains is divided into three trust types. The system enforces these mechanisms to enable cross-domain security auditing in the aid of user-defined services of Globus Toolkit version 3.0 and IBM Aglet.

At present, the CDSA architecture is a prototype, and many issues need to be resolved. So we plan to improve the CDSA architecture in practice via the test of complex applications. Secondly, we will further study the auditing policy to bring the less impact on the performance in the Grid.

References

1. V. Welch, F. Siebenlist, I. Foster, et al.: Security for Grid Services. Proceedings of the 12th IEEE International Symposium on High Performance Distributed Computing (HPDC'03), pp.48-57, 2003.
2. GGF SAAAR RG: Grid Authentication Authorization and Accounting Requirements Draft 5. <https://forge.gridforum.org/projects/saaa-rg/document/draft-ggf-saaar-reqs-5.txt/en/1>. At current 2006.
3. M. Thompson, D. Olson, R. Cowles, et al.: CA-Based Trust Model for Grid Authentication and Identity Delegation, Proceedings of Grid Certificate Policy Working Group, 2002.
4. Mendes, and C. Huitema, A New Approach to The X.509 Framework: Allowing A Global Authentication Infrastructure Without A Global Trust Model, Proceedings of NDSS'95, pp.172-190, 1995.
5. Ellison, B. Frantz, B. Lampson, et al.: SPKI Certificate Theory, Internet Request for Comments: 2693, 1999.
6. T.Y. Li, H.F. Zhu, and K.Y. Lam: A Novel Two-Level Trust Model for Grid, Proceedings of ICICS 2003, LNCS 2836, pp. 214-225, 2003.
7. F. Azzedin, M. Maheswaran: Evolving and Managing Trust in Grid Computing Systems. Canadian Conference on Electrical and Computer Engineering, Proceedings of IEEE CCECE 2002, pp.1424-1429, 2002.
8. I. Foster, C.Kesslman, J. Nick, et al.: The Physiology of the Grid: An Open Grid Services Architecture for Distributed System Integration. http://www.nesc.ac.uk/talks/ggf5_hpdc11/physio_o_grid220702.pdf, Global Grid Forum, 2002.
9. S. Raghnnathan, A. Mikler, C. Cozzolino: Secure Agent Computation: X.509 Proxy Certificates in a Multi-lingual Agent Framework. The Journal of Systems and Software, 75(1-2), pp.125-137, 2005.
10. X.T. Gou, W.D. Jin, G.X. Zhang: Multi-agent Based Security Auditing System of Broadband MAN. Proceedings of the 2004 International Conference On Intelligent Mechatronics and Automation, pp.939-944, 2004.

XML-Signcryption Based LBS Security Protocol Acceleration Methods in Mobile Distributed Computing

Namje Park¹, Howon Kim¹, Kyoil Chung¹, Sungwon Sohn¹, and Dongho Won^{2,*}

¹ Information Security Research Division, ETRI,
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Korea
{namjepark, khw, kyoil, swshon}@etri.re.kr
² School of Information and Communication Engineering,
Sungkyunkwan University, 300 Chunchun-dong, Jangan-gu,
Suwon-si, Gyeonggi-do, 440-746, Korea
dhwon@security.re.kr

Abstract. This paper describes the open security architecture for LBS (Location-based Services) platform ensuring interoperability among the wireless networks and various location-based application services and the functional security requirements for the LBS platform. The goal of this paper is to investigate how well the most limited wireless devices can make use of LBS security services. In this paper, we suggest security acceleration methods for high speed open LBS using XML signcryption mechanism. And proposed secure LBS security protocols allows a client to offload mobile certificate handling to the server and to enable the central administration of privacy polices. The idea is to create a signcryption technique for software based XML signature acceleration.

1 Introduction

Given the recent advancement of mobile telecommunications technology and rapid diffusion of mobile devices, the importance of wired and wireless Internet services utilizing the past and present location information of users carrying mobile terminals with location tracking function is growing. LBS refer to value-added services that detect the location of the users using location detection technology and related applications. LBS is expected to play an essential role in creating value-added that utilizes wired and wireless Internet applications and location information, since these are very useful in various fields.

In view of the current controversy on the information-collecting practices of certain online sites concerning their members particularly with regard to the disclosure of personal information, it is only natural that there is heightened concern on the disclosure of personal information regarding the user's present location, given the unique characteristics of LBS. Easily disclosed information through certain online sites include member information, i.e., name, resident registration number, and address. Moreover, there is a growing concern that such personal information are leaked for

* Dongho Won is the corresponding author for this paper. The fifth author of the research was supported by the University IT Research Center Project funded by the Korean Ministry of Information and Communication.

purposes other than what has been originally intended. Such concern is even more serious since location information on customers and possibility of tracking their movements can constitute a direct encroachment of other people's privacy by themselves. Hence, there is a growing need to conduct research on LBS security both in Korea and abroad to prevent disclosure of personal information of individuals especially in the areas of authentication and security. Furthermore, an open LBS service infrastructure will extend the use of the LBS technology or services to business areas using web service technology. Therefore, differential resource access is a necessary operation for users to enable them to share their resources securely and willingly[10,11].

The goal of this paper is to investigate how well the most limited wireless devices can make use of lbs security services. This paper describes a novel security approach on high speed LBS services based on current mobile web services platform environment using XML signcryption mechanism.

2 Background

2.1 Security Problems of Open LBS

For the revitalization of LBS, their negative effect, i.e., ensuring user's privacy and securing authentication through prevention, is as important as their positive effect. One notable adverse effect of LBS is that the location of each user is exposed 24 hours a day in real time. Considering the present situation wherein the issue of network hacking has become a serious social problem, the fact that the location information of an individual is disseminated freely on the Internet is a serious encroachment of the user's privacy.

2.2 The Performance Problem

XML-based messaging is at the heart of the current lbs based on web services technology. XML's self-describing nature has significant advantages, but they come at the price of bandwidth and performance. XML-based messages are larger and require more processing than existing protocols such as RMI, RMI/IIOP or CORBA/IIOP: data is represented inefficiently, and binding requires more computation. For example, an RMI service can perform an order of magnitude faster than an equivalent web service-based lbs. Use of HTTP as the transport for web services messages is not a significant factor when compared to the binding of XML to programmatic objects.

Increased bandwidth usage affects both wired and wireless networks. Often the latter, e.g. mobile telephone networks, have bandwidth restrictions allotted for communication by a network device. In addition, larger messages increase the possibility of retransmission since the smaller the message, the less likely it will be corrupted when in the air.

Increased processing requirements affects network devices communicating using both types of networks (wired and wireless). A server may not be able to handle the throughput the 'network' demands of it. Mobile phone battery life may be reduced as a device uses more memory, performs more processing and spends more time transmitting information. As the scale of web services usage increases, these problems are likely to be exacerbated.

High-speed LBS security services attempts to solve these problems by defining binary-based messages that consume less bandwidth and are faster and require less memory to be processed. The price for this is loss of self-description. High-speed LBS security service is not an attempt to replace XML-based messaging. It is designed to be an alternative that can be used when performance is an issue.

3 Framework Model for Providing Secure Open LBS Services

Web services can be used to provide mobile security solutions by standardizing and integrating leading security solutions using XML messaging. XML messaging is considered the leading choice for a wireless communication protocol. In fact, there are security protocols for mobile applications that are based on XML messaging. Some of these include SAML (Security Assertion Markup Language), which is a protocol for transporting authentication and authorization information in an XML message. It can be used to provide single sign-on web services. On the other hand, XML signatures define how to sign part or all of an XML document digitally to guarantee data integrity. The public key distributed with XML signatures can be wrapped in XKMS (XML Key Management Specification) formats. In addition, XML encryption enables applications to encrypt part or all of an XML document using references to pre-agreed symmetric keys. Endorsed by IBM and Microsoft, WS-security is a complete solution to providing security to web services. It is based on XML signatures, XML encryption, and same authentication and authorization scheme as SAML[7,12,13].

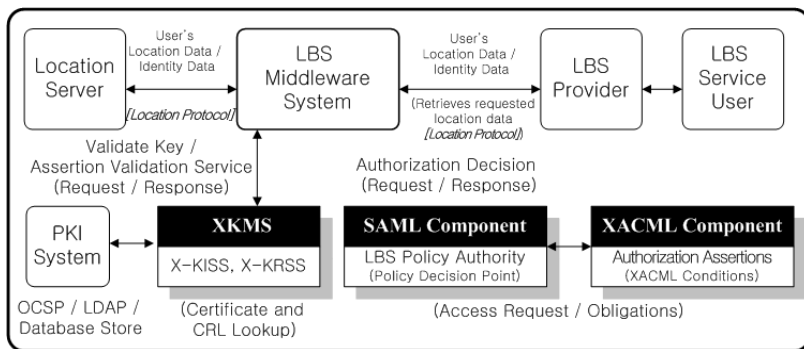


Fig. 1. Proposed Secure LBS Middleware Service Model

When a LBS mobile device client requests access to a back-end application, it sends authentication information to the issuing authority. Depending on the credentials presented by the LBS-mobile device client, the issuing authority can then send a positive or negative authentication assertion. While the user still has a session with the mobile applications, the issuing authority can use the earlier reference to send an authentication assertion stating that the user was in fact authenticated by a particular method at a specific time. As mentioned earlier, location-based authentication can be

done at regular time intervals. This means that the issuing authority gives location-based assertions periodically as long as the user credentials enable positive authentication.

Security technology for LBS is currently based on KLP (Korea Location Protocol). Communication between the LBS platform and Application Service Providers should be examined from the safety viewpoint vis-à-vis XML security technology. As shown in the security service model of the LBS platform in figure 1, the platform should have an internal interface module that carries out authentication and security functions to provide the LBS application service safely to the users[2].

4 Security Protocol for Secure Open LBS Middleware Services

Three types of principals are involved in the proposed protocol: LBS application (Server/Client), SAML processor, and XKMS server (including PKI). The proposed invocation process for the secure LBS security service consists of two parts: initialization protocol and invocation protocol.

The initialization protocol is a prerequisite for invoking LBS web services securely. Through the initialization protocol, all principals in the proposed protocol set the security environments for their web services (Fig. 2). The following is the flow of setting the security environments:

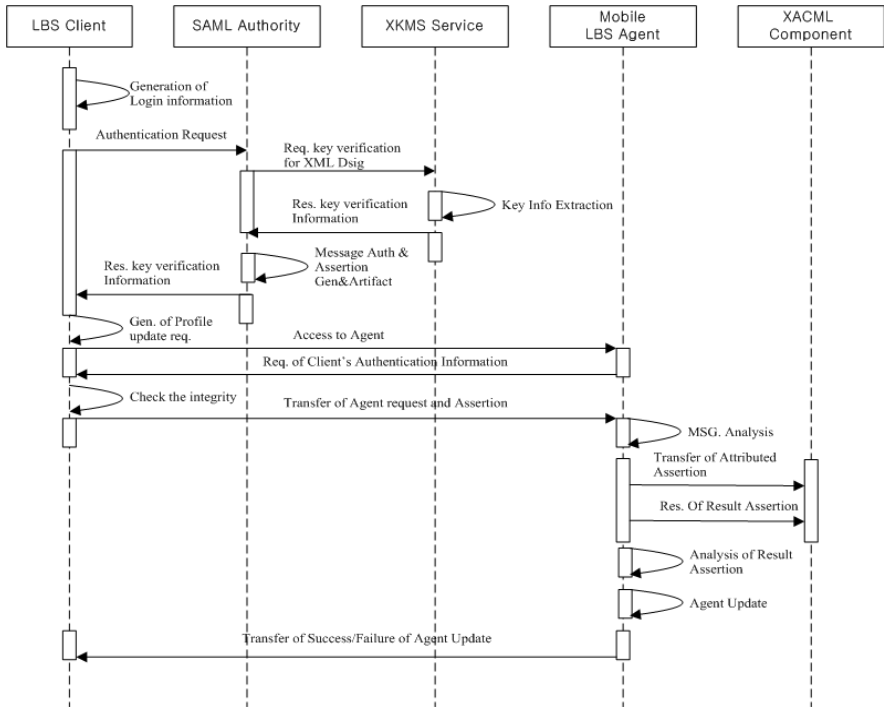


Fig. 2. Security protocol for secure open LBS services

LBS client performs an update for its own agent in the registry agent, where applying security modules to implement business processes satisfies security requirements. In this scenario, a business partner already been authenticated can do 1-to-N businesses (from one partner to multiple partners) as well as 1-to-1 business (from one partner to one partner), because he can search and access to various agents registered in the registry agent. To offer more flexible access to multiple business partners, distributed registries need to be integrated, but it causes the problems of user authentication and security vulnerability. By applying single sign-on scheme, we can simplify user authentication and overcome the problems.

The procedure for Scenario is presented in the form of a sequence diagram in figure 2, where each box in the diagram denotes a Web Service or an application program. Each step denoted by an arrow and number in the diagram is explained as follows:

- (1) Generation of login information: A Client logs into the local LBS intranet system through authentication using user-id and password. An SAML assertion request is generated from this authentication information.
- (2) Authentication request: Generated SAML assertion is transferred to the SAML Web Service to get an access to registry.
- (3) Request of key verification information for digital signature: The SAML Web Service requests the client's public key information to XKMS Web Service to verify the received message.
- (4) Extraction of key information: XKMS Web Service extracts public key information.
- (5) Response of key verification information: Extracted client's public key information is transferred to the SAML Web Service using response protocol.
- (6) Message authentication and generation of assertion and artifact: Authentication on the message is performed using the public key information, and then authentication assertion, attribute assertions, and artifact are generated.
- (7) Response of authentication assertion, attribute assertion and artifact: Generated assertions and artifact are transferred to the client using response protocol.
- (8) Generation of agent update requests: Received assertions and agents to be updated, and update requests are assembled in the message in the SOAP format.
- (9) Access to Registry A: An artifact generated by SAML Authority is transferred to Registry A.
- (10) Req. of LBS Client's authentication information: To request LBS Client's authentication information, Registry of agent sends the artifact, which is received from LBS Client, to LBS Client.
- (11) Check the integrity of returned artifact: LBS Client verifies the integrity of returned artifact from LBS Registry of agent.
- (12) Transfer of agent updated requests and assertions: A generated message is transferred to the registry agent.
- (13) Message analysis: The registry agent analyzes the received message and perceives the requests. The update of agent is possible when the user of the client has a role of "ContentOwner". To check the role, the positive response from the XACML Web Service is required.
- (14) Transfer of attribute assertion: Attribute assertion of the client is transferred to the XACML Web Service.

- (15) Response of result assertion: Authorization decision assertions are generated and transferred to the registry agent, if the attribute assertion meets the XACML policy for documents.
- (16) Analysis of result assertion: The registry analyzes the response from the XACML Web Service, and proceeds to the agent update in case it receives authorization decision assertion. Otherwise, it cannot update agent.
- (17) Agent update: Agent is updated following the updated request.
- (18) Transfer of success/failure of Agent update: Message on success/failure of Agent update is transferred to the client.

From (19) to (29) is the same to from (9) to (18).

5 XML Signcryption Method for High-Speed LBS Security

XML signcryption structure and schema has been proposed. Shown below is the XML signcryption XML document.

```

<?xml version="1.0" encoding="UTF-8" ?>
< XML_Signcryption >
  <SignedInfo>
    <CanonicalizationMethod Algorithm />
    <SignatureMethod Algorithm />
    <EncryptionMethod Algorithm />
    <Reference URI>
      <DigestMethod1 Algorithm />
      <DigestMethod2 Algorithm />
      <DigestValue />
    </Reference>
  </SignedInfo>
  <SigncryptionValue></SigncryptionValue>
  <Rvalue></Rvalue>
  <Svalue></Svalue>
</ XML_Signcryption>

```

Fig. 3. Proposed XML Signcryption Basic Structure

The root element XML signcryption is the fundamental element of the XML documents. Within the root element are contained various other elements such as signed info and the Signcryptionvalue, [R]value and [S]value[7,8,9].

The SignedInfo element contains the information about the Signcryption methodology used. It described about the implementation details about Signcryption. Within the signed info element there are other elements such as Canonicalization-Method Algorithm, SignatureMethod Algorithm, EncryptionMethod Algorithm and Reference URI. The CanonicalizationMethod indicates the method that is used for canonicalization. The canonical method allows the use of different characters in the XML document. For example, if there are white spaces in the XML document, these are removed because of the XML canonicalization method used.

The signatureMethod element indicates the signature element used in the signcryption process. EncryptionMethod is the encryption method that is used in the

signcryption process. In our example, the algorithm used is DES. The element Reference indicates the link of the file that is being signcrypted. It contains the path of the file that is being signcrypted. The reference URI also contains the different Hashing algorithms that are being used in the signcryption process. In our implementation, we are using MD5 and SHA1.

As indicated in sections above, the result of signcryption are three values, namely c, r and s. these three values are required by the system to create the plain text from these messages. When signcryption is performed on a data, the output is a signcryption value. Signcryption requires different digest functions. The description of the hash functions and also the different parameters required for encryption. The encryption method that is used for signcryption is also shown in the XML document. This information is also shown in the Canonicalization method is used to embed a document in another document. Using Xpath filtering, an appropriate file is opened so that the file is opened using the application specified.

Signcryption technique has two different variations. These variations are Shortened Digital Signature Standard 1 [7,8] and Shortened Digital Signature Standard 2 [7,8,9]. Using JCE based crypto library, signcryption will be programmed using verification to [7,8].

```
<element name="XML_Signcryption" type="SigncryptionType"/>
  <complexType name="SigncryptionType">
    <sequence>
      <element ref="SignedInfo"/>
      <element ref="SignatuereMethod"/>
      <element ref="EncriptionMethod" />
      <element ref="Reference" minOccurs="0"/>
    </sequence>
    <attribute name="Id" type="ID" use="optional"/>
    <attribute name="MimeType" type="MIME" use="optional"/>
    <attribute name="Mode" type="MODE" use="required"/>
    <attribute name="Type" type="TYPE" use="required"/>
    <attribute name="Encoding" type="CODING" use="optional"/>
  </complexType>
</element>
```

Fig. 4. Signcryption Schema

XML signcryption schema is shown above. The schema is required to validate the received XML message for its integrity. A part of the XML signcryption module is to create a technique where in badly formed XML documents need to be removed. Survey shows that a lot of attacks on XML servers are due to the fact that the XML documents created are not properly formed. The hardware-based solutions perform this additional task. The software-based module also needs to check the validity of the schema before the document is passed onto the next stages for verification.

The schema defines the various attributes and the elements that are required in a XML document. These attributes declare the feature of the XML document. The Id the element possesses and Multipurpose Internet Mail Extensions (MIME) so as to allow non-textual message to be passed can be incorporated into the XML document. The mode in which the signcryption has occurred, Type specifies a built-in data type.

The XML signcryption schema and is being used with Java Crypto Extensions and SAX parser to create a XML signcryption module. As the signcryption algorithm is faster compared to other signature algorithms, because of its reduced computation, the system is faster. This system introduces faster processing and also provides an additional feature of encryption along with the signature.

Hence, the XML signcryption not only performs the integrity of the XML document, but also performs the confidentiality of the system. This additional facility is provided to the system with faster execution time.

6 Simulation Result

We have modeled our architecture as a closed queuing system, and we analyzed of approximate Mean Value Analysis. LBS system has been implemented based on the design described in previous section. Components of the LBS Middleware are xml security library, service components API, application program. Although LBS middleware service component is intended to support xml applications, it can also be used in order environments where the same management and deployment benefits are achievable. LBS middleware has been implemented in java and it runs on JDK ver. 1.4 or more.

Fig. 5 shows the plotted information presented in the simulation. It can be seen that the time taken for verification of the signature takes a longer time than the generation of the signcryption value itself.

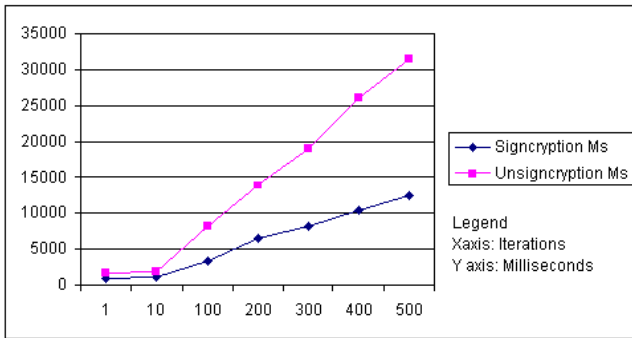


Fig. 5. Time taken plotted against number of iterations for Signcryption and Unsigncryption

7 Conclusion

This paper sought to present a location-based platform that can block information leak and provide safe LBS as well as to establish methods for authentication and security application between service systems for presentation. Toward this end, LBS security requirements were examined and analyzed. In particular, the trend of technology and standard was analyzed to provide safe LBS. To formulate an authentication method as well as a security technology application method for LBS on MLP (Mobile Location

Protocol), MLP security elements were identified based on LBS security requirements by defining the MLP security structure, which serves as the basis for KLP.

We propose a novel security approach on fast LBS security services based on current mobile web services platform environment using XML signcryption mechanism. Our approach will be a model for the future security system that offers security of open LBS security. The proposed approach is expected to be a model for the future security system that offers open LBS security.

Acknowledgement

The authors are deeply grateful to the anonymous reviewers for their valuable suggestions and comments on the first version of this paper.

References

1. M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, RFC 2560 (1999)
2. Namje Park, et. Al.: The Security Consideration and Guideline for Open LBS using XML Security Mechanism. ASTAP 04/FR08/EG.IS/06 (2004)
3. M. Naor and K. Nissim: Certificate Revocation and Certificate Update. IEEE Journal on Selected Areas in Communications. 18 (4) (2000)
4. Yuichi Nakamura, et. Al.: Toward the Integration of web services security on enterprise environments. IEEE SAINT '02. (2002)
5. Sungmin Lee et. Al.: TY*SecureWS: An integrated Web Service Security Solution based on java. LNCS 2738 (2003) 186-195
6. Minsoo Lee, et. Al.: A Secure Web Services for Location based Services in Wireless Networks. Networking2004 (2004)
7. Woo Yong Han, et. Al.: A Gateway and Framework for Telematics Systems Independent on Mobile Networks. ETRI Journal, Vol.27, NO.1 (2005) 106-109
8. Y. Zheng: Digital Signcryption or How to Achieve $\text{Cost}(\text{Signature} \ \& \ \text{Encryption}) \ll \text{Cost}(\text{Signature}) + \text{Cost}(\text{Encryption})$, Advances in Cryptology -- Crypto'97, Lecture Notes in Computer Science, Vol. 1294, Springer-Verlag, (1997) 165-179
9. F. Bao and H. Deng.: A Signcryption scheme with signature directly verifiable by public key. proceeding of public key cryptography(PKC'98), LNCS Vol. 1431 (1998) 55-59
10. Jang Hyun Baek, et. Al.: An Enhanced Location-Based Location Update Scheme in Mobile Cellular Networks. ETRI Journal, Vol.27, NO.4 (2005) 457-460
11. Seunghun Jin, et. Al.: Cluster-based Trust Evaluation Scheme in Ad Hoc Network. ETRI Journal, Vol.27, No.4 (2005) 465-468
12. Namje Park, et. Al.: XKMS-based Key Management for Open LBS in Web Services Environment. AWIC 2005. LNAI 3528, (2005) 367 - 373
13. Young-Guk Ha, et. Al.: Towards Ubiquitous Robotic Companion: Design and Implementation of Ubiquitous Robotic Service Framework. ETRI Journal, Vol.27, No.6 (2005) 666-676

Optimization of a Simulation for 300mm FAB Semiconductor Manufacturing

DongSik Park¹, Youngshin Han², and Chilgee Lee¹

¹ School of Information and Communication Engineering SungKyunKwan University 300, Chunchun-dong, jangan-gu, Suwon, Kyunggi-do 440-746, S. Korea

² Division of Multimedia Sungkyul University, Anyang 8 dong, Manan gu, Anyang-city, Gyeonggi-do, 430-742, S. Korea
yshan@sungkyul.edu

Abstract. Many processes are composed of Bays with equipments. Most 300mm wafer lines use AMHS (Automated Material Handling System) for inter-bay and intra-bay lot transportation. In particular, the inter-bay AMHS moves lots between stockers, whereas intra-bay AMHS moves lots between stockers and tools, or between tools within the same bay. Most companies are trying to reduce average cycle time to increase productivity and delivery time. In this paper, we proposed simulation process standardization method in 300mm FAB semiconductor manufacturing process to propose simulation model verification method. Also we tried to prove efficiency of adopting the simulation theory in real production line.

1 Introduction

Semiconductor industry is growing each year. And consequently, its production environment is shifting from 200mm wafer process to 300mm wafer process and to cluster type facilities. Therefore every year many existing FAB lines are changing and being reconstructed. So far, the growth of semiconductor industry was dependent on the technology developments in chip design, manufacturing facility design, chip size minimization. However, since the semiconductor manufacturing technologies are being widely spread and market competitions are being stiffened, cost-down techniques became basis of growth. In other words, in the new era of semiconductor industry, systematic management and control tactics can decide whether semiconductor industry can grow or not. FAB Line Automation is a key issue that semiconductor industry is facing in shifting from 200mm wafer fabrication to 300mm wafer fabrication. Semiconductor makers that conduct in-depth study and analysis on 300mm FAB are heading to adopt Line Automation[1, 2]. In doing so, there are difficult obstacles related with integration of automation components. There semiconductor companies realized necessity of cost-down on FAB operation and selected FAB automation as a cost-down implementation method. Poorly planned automation schema doesn't do any help in cost-down. As 300mm FAB is developed to lower manufacturing cost, 300 FAB Automation should be accessed in the same direction. One interesting thing in Cost-down Automation is that semiconductor

companies are heading for overall automation program for 300mm FAB. It is evidence proving those companies recognized that success in 300mm FAB is not dependent on each independent components but on overall system integration. Semiconductor manufacturing has many special situations such as, bifurcation and replacement characteristics. Therefore usage of mathematical model is very limited. So access through simulation after appropriate design process sounds reasonable. In this paper, we proposed simulation process standardization method in 300mm FAB semiconductor manufacturing process to propose simulation model verification method. Also we tried to prove efficiency of adopting the simulation theory in real production line[3].

2 Computer Modeling and Simulation

2.1 Benefits of Simulation

Generally, we gain some advantages through the simulation of FAB lines.

Using the simulation, the system can be investigated appropriately even though there are little changes which are not normally easy to see.

Specific benefits of FAB line simulation are listed below

- Can be used to system efficiency
- Gives the ability to determine if the system is working the way it should be
- Reduces the time of system construction
- Issues of important systems can be considered in an early stage
- Can result in cost reduction of the system construction.

2.2 Current Line Design’s Validity Verification

Current Line Design Validity Proving Methods are as following[4]

First: Step (From-To) Table analysis using Major Device’s RUN Sheet.

Second: Calculating automatic transport capacity based on monthly production quantity.

The calculation formula uses following calculation theme:

Table 1. Calculation formula

Storage estimation	Production per month x (1.25 ~ 1.3)
Transport capacity estimation	Production per month x (1.25 ~ 1.3)
In other words, apply marginal rate of 25% to 30% in calculation	

Finally, We can use Simulation Data from automatic transport logistics company to prove the validity of line design. Table 2 shows advantage and disadvantage of simulation.

Table 2. Analytic vs. Simulation

Item	Analytic	Simulation	Remark
Basis theory	Queuing, LP	Discrete/Continuous Static/Dynamic Deterministic/ <i>Stochastic</i>	
Level of realization	<i>Simple</i>	Complex	
Level of understanding	Hard	<i>Easy</i>	Animation
Speed	<i>Fast</i>	Slow	7Hr for 150Day
Output	Average	Average, Min/Max, <i>Trend</i>	
Flexibility	Medium	<i>High</i>	
Correctness	Medium	<i>High</i>	
Adopting Semiconductor	Production or Distribution	<i>Logistics Integration</i>	

2.3 Simulation Model

Our simulation models are implemented with discrete-event simulation. All the experiments are executed on a Pentium 4 personal computer with Microsoft Windows 2000. The modeling tool is a Automod 9.0 for 3-D simulation.

3 300mm Semiconductor Fabrication Line Simulation Sequence

In this paper, we propose 300mm semiconductor fabrication line simulation sequence as following:

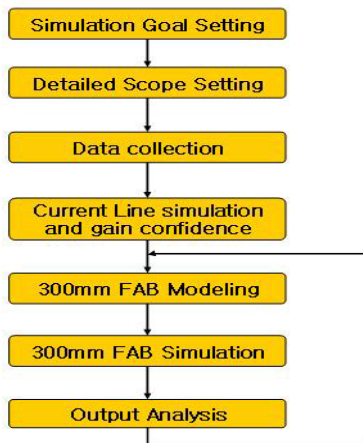


Fig. 1. Proposed Simulation Sequence

3.1 Simulation Goal Setting

Simulation goals should be established before starting simulation. Following table shows detailed goals in terms of two aspects: manufacturing aspect and logistics aspect.

Table 3. Simulation goals and Measure of performance

Items	Simulation Goals	Measure of Performance
Manufacturing aspect	<ul style="list-style-type: none"> - Reduce TAT - Reduce WIP - Achieve Throughput - Layout test - Prevention of Bottleneck - Target operation rate and ST calculation 	<ul style="list-style-type: none"> - TAT - WIP - Throughput - EQ Utilization rate - Real Operation rate - Run Down ratio
Logistics aspect	<ul style="list-style-type: none"> - Optima Investment for automated material handling - Number of OHS/OHT Vehicle - Storage capacity & logic 	<ul style="list-style-type: none"> - OHS/OHT Delivery time - Vehicle Utilization - Stocker Robot Utilization - Stocker Inventory

3.2 Detailed Scope Setting

We used existing 200mm Line as a simulation target line to obtain credibility, and then simulated 300mm Line based on the obtained credibility. In line modeling, first of all, we built an abstract model to check if the model is working properly, and then built a full version of computer model. Each model is divided into three levels in terms of detailed implementation elements.

Table 4. Level of Detail in Line modeling

Line	Model	Level	Note
Current 200mm Line	Abstract Computer	Level 1, 2	Function test using Prototype
New 300mm Line	Abstract Computer	Level 1, 2, 3	Function test using Prototype

Those levels are as following

Prototype : model for verifying simple functions

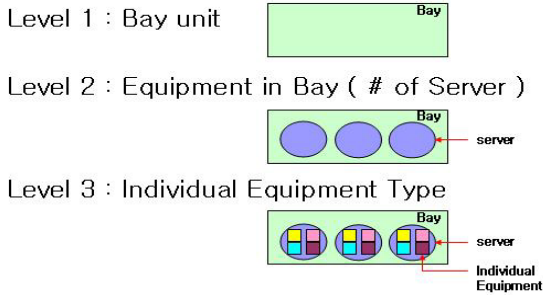


Fig. 2. Level of Detail in modeling

3.3 Data Collection

To construct a computer model of a system, it is necessary to understand the system properly, and the data for the objects and parameters that compose the computer model are also needed. All the data used in this paper was taken from a real FAB line that is currently running in a domestic facility. This real data was preprocessed prior to use for our purpose.

- Step Data
- Equipment Data
- Vehicle Data
- EOH Data(initially provided)
- Shift Data for New Lot Input

Following Output Data List should be analyzed once model is established.

Table 5. Output for analyze

Production	Distribution
- TAT - WIP - Throughput - UPEH per EQ - Real operation rate - Run Down ratio	- OHS/OHT Delivery time - Vehicle Utilization - Stocker Robot Utilization - Stocker Inventory

3.4 Current 200mm Line Simulation

By using existing 200mm simulation model, we could compare and verify simulation data with accumulated data from real FAB lines. Therefore we could get validity of the 300mm FAB simulation model[5].

- Used assumptions are as following

- a. Model's basic unit is Bay
- b. Basic unit (moving entity) of logistics: Lot
- c. 5 Major Device Types
- d. 1st floor: 10 vehicles per rail
3rd floor: 7 vehicles per rail
- e. Number of lifters: 3 each, Lifter Capacity: 2
(Note: dumb waiter(via S042B) capacity is regarded as equivalent as 12 lifters)
- f. Moving rate between Inner Rails and Outer Rails in each floor is 45:55.
- g. Rework , Skip step and CMP processes are not included.

Figure 3 and 4 shows individual model implementations

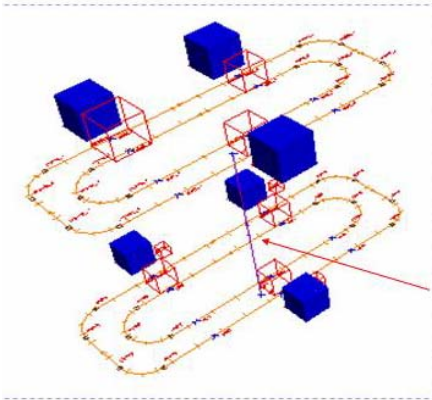


Fig. 3. Prototype Model Implementation

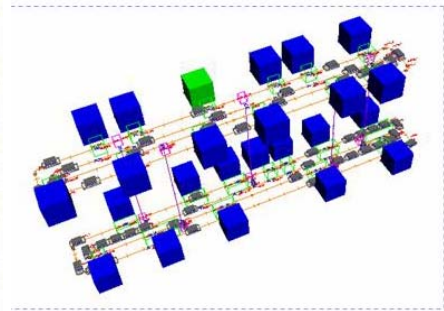


Fig. 4. Computer Model Implementation

3.5 300mm Line Simulation

Although we doesn't have any accumulated data, we established the validity of the simulation model based on obtained credibility obtained during 200mm line simulation. Although validity of simulation model is established, still there are many differences between 200mm line and 300mm line. In following table, some of these differences are listed.

- Assumption

- a. Basic unit of the model is equipment
- b. Basic unit of a moving entity is a lot
- c. 2 device types are used
- d. Capacity of a stocker is infinite
- e. Up/Down is applied to equipment.
- f. There are buffers in equipment
- g. Interval of entering lots is constant

Table 6. Difference 200mm Line and 300mm Line

200mm Line	300mm Line
8 inches wafer size	12 inches wafer size
1 kind of Vehicle (OHS)	2 kind of Vehicle (OHS, OHT)
Manual Handling (Operator)	Full automated system
Multiple layered structure	Single layer structure
5 Major Device	2 Major Device

- Rules

- a. Use OHT for transferring between bays within a cell
- b. Apply reservation rules to prevent deadlock in equipment ports
- c. If the in-port of equipment is full, the lot will wait in a stocker
- d. Equipment will be applied if there are the same types of equipments in the same bay
- e. Processes never stop while in service

- Scenario

We configured a verity of scenarios models to check output form various environments. We focused on following Scenarios.

- a. Implementing simulations under various Scenario to find optimum outputs in different situations
- b. Direct or Indirect transport
 - i) Direct : Equipment to Equipment
 - ii) Indirect : Equipment to Stocker, Stocker to Equipment
- c. Adjusting the number of Vehicles
 - i) Adjusting the number of OHS and OHT to find optimum results
- d. Batch processing
 - i) 1st plan : collecting Lots in Stocker
 - ii) 2nd plan : collecting Lots in Equipment
 - iii) Conclusion : the first plan was more effective

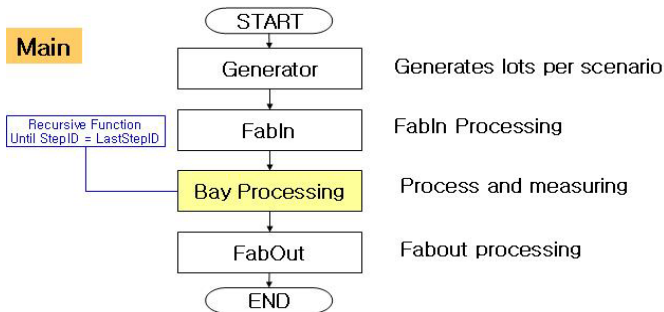


Fig. 5. Abstract Model

- Output Analysis

a. Comparison with existing methods

i) Results of mathematical model calculation

ii) Simulation results from automated logistics companies

iii) Manufacturer's opinion

b. Single lot result

c. Selecting the number of Stockers

d. Selecting the number of Vehicles

e. OHS transport time result

f. Selecting the number of OHT

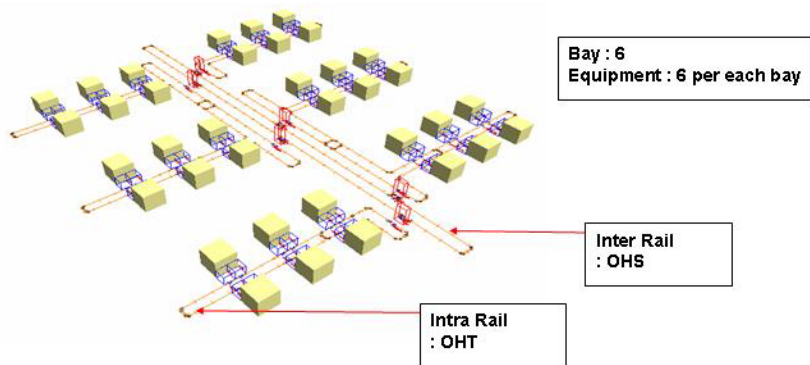


Fig. 6. Computer Model

4 Conclusion

The scope and cost of semiconductor fabrication line are incomparable with those of general manufacturing lines. Therefore problematic elements should be prevented, and expected problems in line fabrication should be monitored all the time. Since its scope and cost are so huge, those who are trying to build such lines must be prepared before they get into construction. We believe that scientific and objective simulations, rather than mathematical models or more traditional methods, are more effective methods while fulfilling enterprises' goals: profit.

In this paper, we proposed how to access on Simulation Modeling. There can be a lot of different methods in accessing Simulation Modeling. However we proposed Simulation Model Standardization method obtained from experiences in model adaptation in real industrial sites. We expect that if a project is conducted following simulation sequence proposed in this paper, one can fulfill industry's requirements and complete the project successfully.

References

- [1] B.K. CHOI and B.H. KIM, "MES (manufacturing execution system) architecture for FMS compatible to ERP(enterprise planning system)", INT. J. Computer Integrated Manufacturing, 2002, Vol. 15, NO. 3, 274-84.
- [2] SEMI E53-1296 Event Reporting , SEMI Standard 2000
- [3] Wein, L.M., "On the relationship Between Yield and Cycle time Semiconductor Wafer
- [4] Izak D., John W. F and Schruben, L. W., "Planning and Scheduling in Japanese Semiconductor Manufacturing, Journal of Manufacturing Systems", Vol.13, No.5, pp.323-332,1993
- [5] Y.S. HAN, D.S. Park, C.G. Lee, "Full Fabrication Simulation of 300mm Wafer Focused on AMHS (Automated Material Handling Systems)", LNCS/Springer-Verlag GmbH, Vol 3398, p514-p520, 2004.10.05.

Performance Analysis Using the Two Kinds of Receiving Gain of Smart Antenna in IS20001X System

Sungsoo Ahn¹, Minsoo Kim², and Jungsuk Lee³

¹ Dept. of Information Technology and Communication,
Myongji College, Korea
ssan64@empal.com

² Dept. of Information and Communication,
HanJung University, Korea
mskim1019@hanmir.com

³ Dept. of Mechatronics, Inha Technical College, Korea
ungboleee@inhatec.ac.kr

Abstract. In order to achieve the diversity gain with antenna arrays for moderate angle spread, we propose a beamforming algorithm that utilizes multiple eigenvectors, and apply this beamforming technique to IS2000 1X systems equipped with antenna arrays under a time-varying multipath fading channel environment. In the proposed beamforming method, the channel vector has been estimated using two basis vectors. Since the proposed beamforming algorithm utilizes two-dimensional signal subspace, it provides better performance than the conventional beamforming algorithm, which uses one beamforming signal space.

1 Introduction

Smart antenna system (SAS) can be used one of the methods to increase the capacity of wireless systems. It has been shown that the use of multiple antennas can improve the performance and capacity of wireless systems, because it weights and combines the signals to enhance desired signal reception and null interference. SAS also generates an antenna pattern that has a main beam in the direction of the desired signal and a null in the direction of interferes[1][2].

In order to achieve the maximum signal to noise ratio beamforming, covariance matrices of desired signals and interfering signals are required. After beamforming (spatial combining), the outputs of the beamformers are combined in the time domain. Depending on the angle spread of incoming signals, it has been shown that the total diversity order[3] varies from M to LM , where M and L stand for the numbers of multipaths and antenna elements, respectively. If the channel coefficients of each antenna perfectly correlated, the resulting diversity order becomes M . That is, only the path diversity is available. On the other hand, if the channel coefficients of each antenna are uncorrelated, the diversity order becomes LM due to the spatial diversity and path diversity. Generally, the spatial correlation between the channel coefficients of each antenna decreases with the angle. Therefore, we need to deal with the case of moderate angle spread in mobile communication systems.

2 System Modeling

Assuming a linear array consisting of L antenna elements, the received signal vector after the spreading procedure can be written as

$$\underline{y}[n] = \underline{h}[n]\underline{s}[n] + \underline{u}[n] \tag{1}$$

where $\underline{y}[n]$ denotes the n -th sample of the received data, $\underline{h}[n]$ is the channel vector representing the channel gain for the transmitted symbol $\underline{s}[n]$, and $\underline{u}[n]$ is the undesired term including the interfering and noise parts. In this paper, every parameter representing vector quantity is underlined. Since there exists the angular spread in actual communication paths, the channel vector should be written as

$$\underline{h}[n] = \frac{1}{\sqrt{Q}} \sum_{q=1}^Q \alpha_q[n] \underline{a}(\theta + \theta_q) \tag{2}$$

where Q is the number of scattered components associated at a given propagation path, and $\alpha_q[n]$ is the fading factor corresponding to the q -th component. where θ is the arrival angle of desired signal due to the mobility of the subscriber. $\underline{a}(\theta)$ is the steering vector treated as a constant for a symbol period whereas the fading factor $\alpha_q[n]$ as being a time-varying scalar changing at every symbol.

Most beamforming algorithms for CDMA systems have been developed for the case of small angular spread. Therefore, θ_q has been considered to be negligible. As the carrier frequency get higher, the path loss gets severer. Hence, for reliable communication quality, the radius of cells shall be shorter. Since the radius of the local scatters around the mobile station does not change, the angular spread can get larger in this case. So, we need to deal with the case of moderate angular spread in cellular systems, as the carrier frequency gets higher.

When the spreading gain of a given CDMA system is large enough, the weight vector that maximizes the SNR can be obtained from the eigenvector corresponding to the largest eigenvalue of the following eigen-equation[4]

$$\mathbf{R}_y \underline{w} = \lambda \underline{w} \tag{3}$$

where \mathbf{R}_y is the covariance matrix of the received signal \underline{y} obtained at the output of the despreader.

Fig. 1 illustrates the distribution of the eigenvalues of \mathbf{R}_y . As shown in the figure, the dominance of the primary eigenvalue decreases as the angle spread increases from 0° to 20° . It means that the optimal weight vector that maximizes the SNR cannot likely be obtained from the primary eigenvector only as the angle spread increases. In order to obtain a more appropriate weight vector in the signal environment of angle spread, the weight vector is to be found by a linear sum of the two primary eigenvectors.

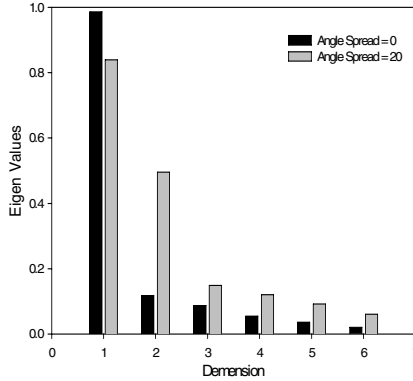


Fig. 1. Distribution of eigenvalues

Basically, the entire procedure consists of a repetition lagrange algorithm[4] to find weight vector. First, the primary eigenvector is computed using the lagrange algorithm and then the secondary eigenvector is obtained by invoking the deflation method [5].

3 Adaptive Beamforming

Here, we describe an adaptive beamforming procedure based on the eigenspace method. When the spreading gain of the IS2000 1X system is large enough, the weight vector maximizing the power of array output can be obtained from the eigenvector corresponding to the largest eigenvalue of the following eigen-equation [6].

$$\mathbf{R}_{yy}[k] \underline{w}[k] = \lambda \underline{w}[k] \tag{4}$$

Where $\mathbf{R}_{yy}[k]$ is the autocovariance matrix of the received signal vector $\underline{y}[k]$ at the k th snapshot of the despreader, $\underline{w}[k]$ is the weight vector and λ is the eigenvalue of eigen equation. If the channel vector is approximated with the first two terms of Taylor series as in (4), the autocovariance matrix of the channel vector can be approximated by a matrix of rank 2. Therefore, $\underline{h}[n]$ is in the subspace span $(\underline{e}_1, \underline{e}_2)$, and the channel vector in (4) can be rewritten as [7]

$$\underline{h}[k] \approx \alpha \underline{e}_1 + \beta \underline{e}_2 \tag{5}$$

where \underline{e}_1 and \underline{e}_2 are first and secondary eigen-vectors of the autocovariance matrix and α, β are the constants representing the channel coefficients $\bar{\alpha}, \bar{\beta}$. We note, therefore, that the channel vector is a linear sum of the two primary eigenvectors. We now propose a new estimation technique for the channel vector which utilizes two eigenvectors, the first eigenvector corresponding to the first largest eigenvalue and the secondary eigenvector corresponding to the second largest eigenvalue, of the autocovariance matrix of the received signal. In the proposed technique, we can be obtained the first weight vector by lagrange algorithm[8] after computing the lagrange multiplier γ using the autocovariance matrix following as equation (6).

$$\underline{w}_1 = (1 - \mu\gamma_1)\underline{w}_1 + \mu\mathbf{R}_y \underline{w}_1 \tag{6}$$

Where \underline{w}_1 is first weight vector which is almost same as \underline{e}_1 , μ is relative gain to find the weight vector, γ is lagrange multiplier.

The secondary weight vector \underline{w}_2 is determined from the new autocovariance matrix obtained by the deflation method. If any further eigenvectors are needed, the procedure can be repeated.

If the carrier frequency of the forward link is not far different from that of the reverse link, the weight vector obtained during the receiving mode can be used as the transmitting weight vector for the same subscriber to enhance the transmitting performance as well as the receiving performance.

The step in the proposed adaptive beamforming algorithm are: Step 1) Find the autocovariance matrix \mathbf{R}_y using the deflation method. Step 2) Calculate the first lagrange multiplier γ_1 . Step 3) Find the first weight vector using the lagrange algorithm. Step 4) Apply the lagrange algorithm to \mathbf{R}_y to find the secondary weight vector. Step 5) Calculate the first lagrange multiplier γ_2 . Step 6) Find the secondary weight vector.

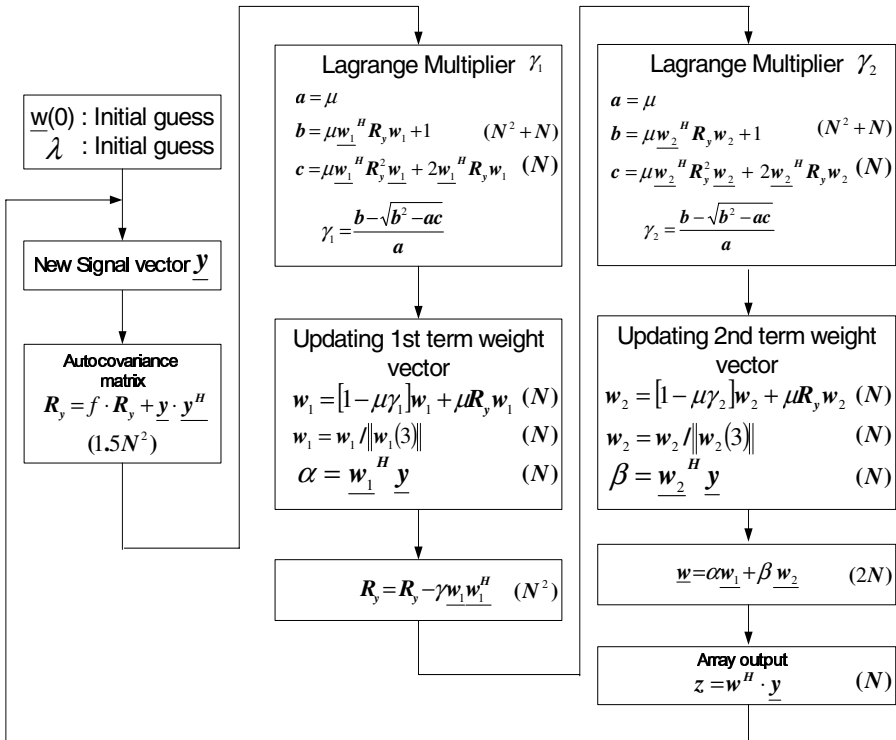


Fig. 2. Flow chart of the proposed method with computational load at each step

These steps are shown in figure 2. Since the procedure consists of applying the Lagrange algorithm twice, the entire procedure has computational complexity of $O(4.5N^2 + 13N)$ at each snapshot where $O(N)$ denotes the order of computational load required to compute a scalar product of two $N \times 1$ complex-valued vectors. Using a high speed DSP(Digital Signal Processor) such as TMS320C67X, the proposed technique can be implemented in real-time for most practical cases including IS2000 1X systems.

4 Simulation Results

The proposed technique has been applied to IS2000 1X uplink signal. In this section, we present the results of various computer simulations. We consider 3 channels, i.e., fundamental, supplemental 1, and supplemental 2, at each interfering user while the desired user transmits the signal through its fundamental channel. For this simulation, we consider signal environments encountering the following parameters. First, the integration period in the pilot channel[7], which determined the processing gain in computing the weight vector, has been set to 384-chip duration. Second, the angle spread is set to $\pm 10^\circ$ from the center DOA (Direction Of Arrival) for the desired signal. Third, the number of fingers for RAKE reception has been set to 2. Finally, the number of interferers is set to 20 and the target subscriber changes its DOA by $0.01^\circ/\text{snapshot}$ where the snapshot period is set to 1ms.

Figure 3,4,5 shows the uncoded Bit Error Rate(BER) performance of the proposed technique. As can be seen in Figure 3,4,5, the weight vector employing 2 basis far outperforms than that employing only one basis, the largest eigenvalue. The main reason for the improvement is that the first eigenvector alone cannot adequately represent the array response vector of the desired signal when the AOA of the desired signal is spread widely from the center AOA due to severe scattering. For

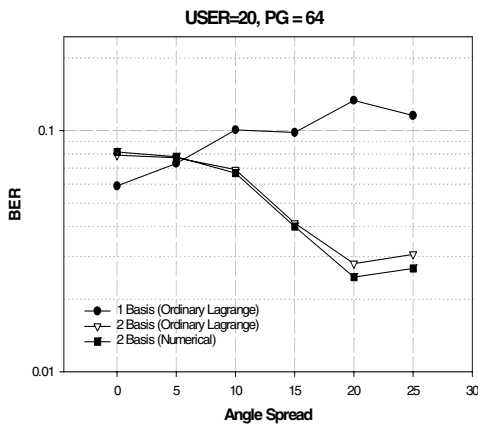


Fig. 3. Comparison of performance for the various value of angle spread (Number of user =20, Processing gain=64)

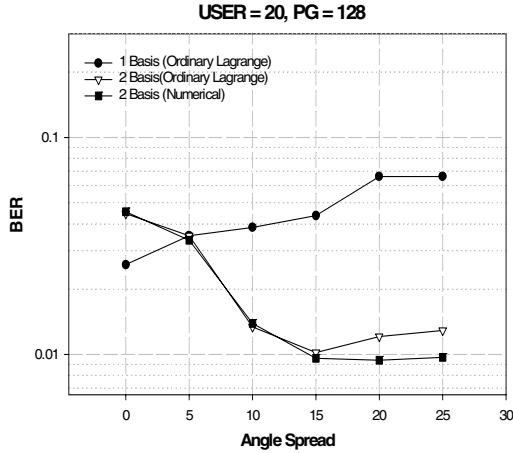


Fig. 4. Comparison of performance for the various value of angle spread (Number of user =20, Processing gain=128)

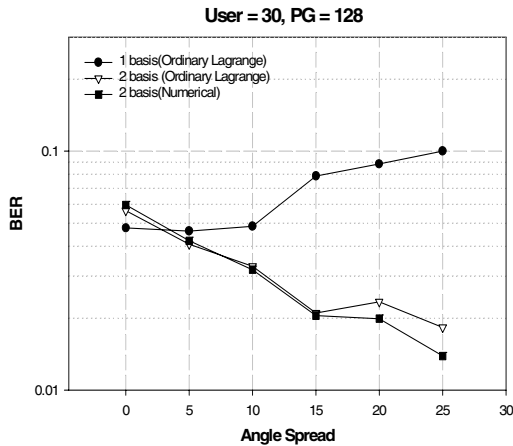


Fig. 5. Comparison of performance for the various value of angle spread (Number of user =30, Processing gain=128)

the case of no angle spread there is slight degradation in the performance of the proposed 2 basis system when compared to the conventional 1 basis system. But this rarely causes serious problem since, in most practical environments, especially in urban areas with densely populated tall buildings near the base station, the signal transmitted from each subscriber is inherently subject to the multipath effect and each propagation path must encounter many scattered components of the signal, resulting in a wide angle spread.

It is noteworthy that, while the BER performance using the single eigenvector becomes worse as the angle spread increases, the BER of the proposed technique is improved to the contrary. This characteristic is due to the diversity gain resulting from

the use of two basis in the weight vector. In fact, the diversity gain becomes effective as the angle spread of the desired signals increases, which in turn causes the received signal at each antenna element to fluctuate more independently, thus the signal received at each antenna element to be more independent of each other. In summary, the improvement of the receiving performance of the propose method can be attributed to the angle spread caused by the diversity gain which is exploited by the proposed technique.

5 Conclusions

We have presented a new adaptive beamforming technique based on the lagrange algorithm. The new technique is particularly useful for the cases of wide angle spread which is common in practical mobile communication. The proposed technique utilizes the first and second primary eigenvectors to form the weight vector. When the desired signal is scattered from the center arrival angle, which results in an angular spread in the desired signal, the proposed method shows a conspicuous superiority in its receiving performances. This can be explained by the fact that the new procedure exploits the diversity gain available due to the wide angle spread.

References

1. J. H. Winters, "Smart antennas for wireless systems", IEEE Person. Commun. Mag., pp.23-27, Feb., 1998.
2. F. Adachi, M. Sawahashi, and H. Suda, "Wideband DS-CDMA for next-generation mobile communications systems," IEEE Commun.Mag.,pp.56-59, Sept. 1998
3. J. Choi and S. Choi, "Diversity gain in antenna arrays and its use in CDMA systems equipped with antenna arrays", submitted to IEEE Tr. Veh. Tech.
4. T. K. Sarkar, S. Choi and M. S. Palma, " A Pragmatic Approach to Adaptive Antennas," IEEE Antenna and Propagations Magazine, Vol. 42, No. 2, April 1999.
5. Howard Anton, Elementary Linear Algebra, John Wiley & Sons, 1982
6. R. A. Monzingo and T.W. Miller, Introduction to Adaptive Arrays, John Wiley & Sons, 1980.
7. A. F. Naguib, Adaptive Antenna for CDMA Wireless Networks, Ph.D. Dissertation, Stanford Univ., 1996
8. S. Choi, D. Shim, "A Novel Adaptation Beamforming Algorithm for a Smart Antenna System in a CDMA Mobile Communication Environment", IEEE Transaction on Vehicular Technology, vol.49, no.5, pp.1795-1799, Sep., 2000

An Improved Popescu's Authenticated Key Agreement Protocol

Eun-Jun Yoon and Kee-Young Yoo*

Department of Computer Engineering, Kyungpook National University,
Daegu 702-701, South Korea
ejyoon@infosec.knu.ac.kr, yook@knu.ac.kr

Abstract. In 2004, Popescu proposed an efficient and secure key agreement protocol based on the Diffie-Hellman key agreement, which works in an elliptic curve group. The protocol, however, is still susceptible to a key-compromise impersonation attack, a reflection attack, and a replay attack. Accordingly, the current paper demonstrates the vulnerability of Popescu's protocol against such attacks and then an improved protocol is presented in order to resolve such problems.

Keywords: Cryptography, Security, Cryptanalysis, Key agreement, Elliptic curve cryptosystems.

1 Introduction

The elliptic curve cryptosystems [1][2], which are based on the elliptic curve discrete logarithm problem (ECDLP) over a finite field, have some advantages over other cryptosystems: The key size can be much smaller than those of the other cryptosystems since only exponential-time attacks have been known to occur so far, if the curve is carefully chosen [3], and that the elliptic curve discrete logarithms might still be intractable even if factoring and the multiplicative group discrete logarithm turn out to be tractable problems.

Recently, Popescu [4] proposed an efficient and secure key agreement protocol based on the Diffie-Hellman key agreement, which works in an elliptic curve group. Popescu showed that their protocol is more efficient than previously authenticated key agreement protocols with regard to computational costs, because it requires only one (1) integer multiplication per entity. Also, Popescu claimed that the protocol satisfies security attributes under the assumption that the elliptic curve discrete logarithm problem (ECDLP) is secure.

Unlike Popescu's claim, the protocol, however, is still susceptible to a key-compromise impersonation attack, a reflection attack, and a replay attack [5][6]. Accordingly, the current paper demonstrates the vulnerability of Popescu's protocol against such attacks and then an improved protocol is presented to resolve such problems. In contrast to Popescu's protocol, the proposed protocol is able to provide greater security.

* Corresponding author. Tel.: +82-53-950-5553; Fax: +82-53-957-4846.

The remainder of the paper is organized as follows: Section 2 briefly reviews Popescu's key agreement protocol, then Section 3 demonstrates its security weaknesses. Our proposed protocol is presented in Section 4, while Section 5 discusses the security of the proposed protocol. Conclusions are presented in Section 6.

2 Related Works

This section briefly reviews Popescu's key agreement protocol.

2.1 Notations

Some of the notations used in this paper are defined as follows:

- A, B : two communicating parties.
- ID_A, ID_B : the identity information of users A and B .
- C : an attacker.
- E : an elliptic curve over a finite field F_q of characteristic p .
- P : the generating element (point) $\in E(F_q)$ of order n .
- s_A, s_B : the long-term secret keys selected from the interval $[1, n-1]$ of A and B , respectively.
- Y_A, Y_B : the public keys of A and B , where $Y_A = -s_AP$ and $Y_B = -s_BP$, respectively.
- K_S : the long-term secret key shared by A and B , where $K_S = -s_A Y_B = -s_B Y_A = s_A s_B P$.
- $H(\cdot)$: a one-way hash function such as SHA-1.

2.2 Elliptic Curve Domain Parameters

The elliptic curve domain parameters [9][10] are defined as follows:

- A field size q , where q is a prime power (in practice, either $q = p$, an odd prime, or $q = 2^m$).
- Two field elements $a, b \in F_q$, which define the equation of the elliptic curve E over F_q (i.e., $y^2 = x^3 + ax + b$ in the case $p > 3$, where $4a^3 + 27b^2 \neq 0$).
- Two field elements x_p and y_p in F_q , which define a finite point $P = (x_p, y_p)$ of prime order in $E(F_q)$ ($P \neq O$, where O denotes the point at infinity).
- The order n of the point P .

2.3 Popescu's Key Agreement Protocol

Fig. 1 illustrates Popescu's key agreement protocol. The protocol is comprised of the following four Steps:

- Step 1. A generates a random integer k_A (ephemeral key) from the interval $[1, n-1]$, computes the point $V_A = -k_AP$ on E and $e_A = H(x_{V_A}, x_{K_S})$, where x_{V_A} is the x -coordinate of V_A and x_{K_S} is the x -coordinate of K_S . A sends V_A and e_A to B .

- Step 2. B generates a random integer k_B (ephemeral key) from the interval $[1, n - 1]$, computes the point $V_B = -k_B P$ on E and $e_B = H(x_{V_B}, x_{K_S})$, where x_{V_B} is the x -coordinate of V_B and x_{K_S} is the x -coordinate of K_S . B sends V_B and e_B to A .
- Step 3. A checks to see whether $e_B = H(x_{V_B}, x_{K_S})$ holds. If it does not hold, then A terminates the execution. Otherwise, A computes the point $K_A = -k_A V_B$.
- Step 4. B checks to see whether $e_A = H(x_{V_A}, x_{K_S})$ holds. If it does not hold, then B terminates the execution. Otherwise, B computes the point $K_B = -k_B V_A$.

After Step 4, A and B acquire the same shared secret session key $K = K_A = K_B = k_A k_B P$.

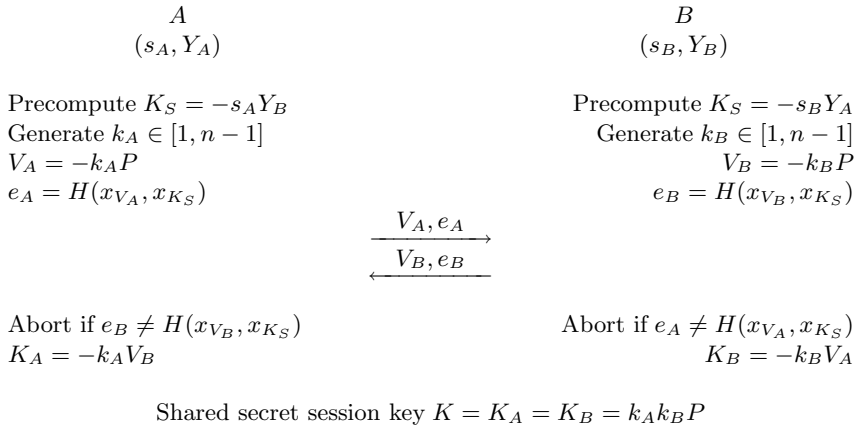


Fig. 1. Popescu’s key agreement protocol

3 Cryptanalysis of Popescu’s Key Agreement Protocol

This section shows that Popescu’s key agreement protocol is vulnerable to a key-compromise impersonation attack, a reflection attack, and a replay attack [5][6].

3.1 Key-Compromise Impersonation Attack

A key-compromise impersonation attack is as follows: First, assume that entities A and B are two principals. Then, suppose that A ’s long-term private key is disclosed. Obviously, an attacker who knows this long-term private key can impersonate A to other entities. It is desired, however, that this disclosure does not allow the attacker to impersonate other entities to A .

In Popescu’s key agreement protocol, suppose an attacker C obtains a long-term private key s_A (or s_B) from the compromised user A (or B), then C can

easily compute a long-term secret key K_S , which is shared by A and B , by computing $K_S = -s_A Y_B$ (or $K_S = -s_B Y_A$), where Y_A and Y_B are the public keys of A and B , respectively. As a result, C can freely impersonate user B (or A) to A (or B) by using K_S . Obviously, Popescu's protocol is vulnerable to a key-compromise impersonation attack.

3.2 Reflection Attack

A reflection attack is a potential way of attacking a challenge-response authentication system, which uses the same protocol in both directions. The attacker initiates two separate connection attempts to the same target, and sends back the challenges received on one connection as its responses on the second connection.

In Popescu's key agreement protocol, suppose that attacker C interposes the communication between A and B . Then, C can perform the reflection attack as follows:

- Step 1*. Upon intercepting the message (V_A, e_A) sent by A , C reflects it to A .
 Step 2*. Similarly, upon intercepting the message (V_B, e_B) sent by B , C reflects it to B .

After all, A and B will compute the wrong shared secret session key $K_A^* = k_A k_A P$ and $K_B^* = k_B k_B P$, respectively. A and B , however, cannot detect the generation of this wrong shared secret session key because the verification equations $e_A = H(x_{V_A}, x_{K_S})$ and $e_B = H(x_{V_B}, x_{K_S})$, which were performed by A and B in Step 3 and 4, always hold.

From this point, A and B will be using the wrong secret session key in encrypting/decrypting their messages during encrypted communication. Through this attack, an attacker C cannot obtain K_A^* or K_B^* , but it can make the two parties believe and use an unintended secret session key. Furthermore, since the elliptic curve Diffie-Hellman problem (ECDHP) based shared secret session key $K = K_A = K_B$ is invalid, it cannot guarantee the integrity of the session secret key. Obviously, Popescu's protocol is vulnerable to a reflection attack.

3.3 Replay Attack

A replay attack is similar to the above mentioned reflection attack. This is an offensive action whereby an attacker impersonates or deceives another legitimate participant through the reuse of information obtained in a protocol.

In order to do this, one should consider a simple replay attack in Popescu's key agreement protocol. After a protocol session for users A and B , an attacker C stores all the messages sent that were in the session. C tries to re-send the messages to B by impersonating as A . If C can trick B to finish its session by believing that it is talking to A , then the protocol is flawed and is discarded. Similarly, C can launch a simple replay attack on A as well. This attack can be launched because the users A and B do not check to see whether the random integers k_A and k_B are used in the correct way. Therefore, Popescu's protocol is vulnerable to a replay attack.

4 Proposed Key Agreement Protocol

This section proposes improvements to Popescu's key agreement protocol. Fig. 2 illustrates the proposed key agreement protocol. The protocol is comprised of the followings four Steps:

Step 1. A generates a random integer k_A (ephemeral key) from the interval $[1, n - 1]$, and computes the point $V_A = k_A P$ on E and $Q_A = k_A Y_A$. A sends V_A and Q_A to B .

Step 2. B generates a random integer k_B (ephemeral key) from the interval $[1, n - 1]$, and computes K_{BA} and K_{AB} as follows:

$$K_{BA} = k_B Q_A = k_A k_B s_A P \quad (1)$$

$$K_{AB} = k_B s_B V_A = k_A k_B s_B P \quad (2)$$

Then B computes the point V_B on E , Q_B , e_B and C_B as follows:

$$V_B = k_B P \quad (3)$$

$$Q_B = k_B Y_B \quad (4)$$

$$e_B = H(ID_A, ID_B, x_{V_B}, x_{K_{BA}}, x_{K_{AB}}) \quad (5)$$

$$C_B = e_B^{-1}(s_B - x_{V_B} k_B) \bmod q \quad (6)$$

where x_{V_B} is the x -coordinate of V_B , $x_{K_{BA}}$ is the x -coordinate of K_{BA} and $x_{K_{AB}}$ is the x -coordinate of K_{AB} . Finally, B sends V_B , Q_B and C_B to A .

Step 3. A computes K_{AB} and K_{BA} as follows:

$$K_{AB} = k_A s_A V_B = k_A k_B s_B P \quad (7)$$

$$K_{BA} = k_A Q_B = k_A k_B s_A P \quad (8)$$

Then A computes e_B as follows:

$$e_B = H(ID_A, ID_B, x_{V_B}, x_{K_{BA}}, x_{K_{AB}}) \quad (9)$$

and checks to see whether $V_B = x_{V_B}^{-1}(Y_B - e_B C_B P)$ holds. If it does not hold, then A terminates the execution. Otherwise, A can ensure that B is legal and it can compute e_A and C_A as follows:

$$e_A = H(ID_A, ID_B, x_{V_A}, x_{K_{AB}}, x_{K_{BA}}) \quad (10)$$

$$C_A = e_A^{-1}(s_A - x_{V_A} k_A) \bmod q \quad (11)$$

where x_{V_A} is the x -coordinate of V_A , $x_{K_{AB}}$ is the x -coordinate of K_{AB} and $x_{K_{BA}}$ is the x -coordinate of K_{BA} . Finally, A sends C_A to B .

Step 4. B computes e_A as follows:

$$e_A = H(ID_A, ID_B, x_{V_A}, x_{K_{AB}}, x_{K_{BA}}) \tag{12}$$

and checks to see whether $V_A = x_{V_A}^{-1}(Y_A - H(x_{V_A}, x_{K_{AB}}, x_{K_{BA}})C_{AP})$ holds. If it does not hold, then B terminates the execution. Otherwise, B can ensure that A is legal.

After Step 4, A and B acquire the same shared secret session key $K = H(ID_A, ID_B, x_{V_A}, x_{V_B}, x_{K_{AB}}, x_{K_{BA}})$.

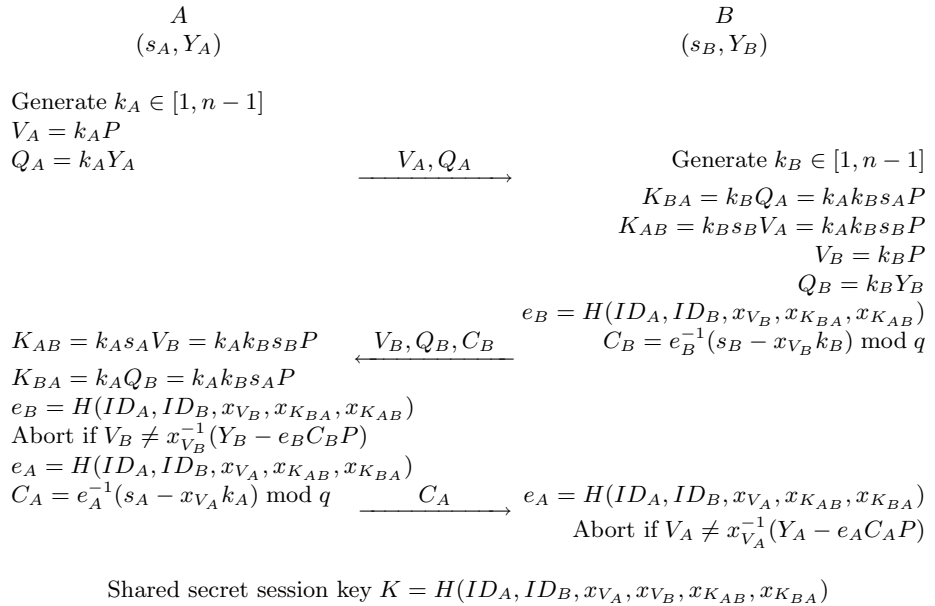


Fig. 2. The proposed key agreement protocol

5 Security Analysis

This section analyzes the security of the proposed key agreement protocol. First, we define the security terms [1][2][5][6][7][8] needed to conduct an analysis of the proposed protocol. They are as follows:

Definition 1. *The elliptic curve discrete logarithm problem (ECDLP) is as follows: given a public key point $V_i = k_i P$, it is hard to compute the secret key k_i .*

Definition 2. *The elliptic curve Diffie-Hellman problem (ECDHP) is as follows: given point elements aP and bP , it is hard to find abP .*

Definition 3. *A secure one-way hash function $y = H(x)$ is one where given x to compute y is easy and given y to compute x is hard.*

Here, the following six security properties [5][6][8] must be considered for the proposed protocol: a key-compromise impersonation attack, a reflection attack, a replay attack, a known-key security, a session key security, and perfect forward secrecy. Regarding the above mentioned definitions, the following theorems are used to analyze the six security properties of the proposed protocol.

Theorem 1. *The proposed protocol can resist a key-compromise impersonation attack.*

Proof. First, suppose an attacker C obtains the long-term private key s_A from the compromised user A . In order for the key-compromise impersonation attack to succeed, C must know A 's ephemeral keys k_A . In this case, C would also have to extract k_A from A 's ephemeral public value Q_A , so as to generate the same session key K with A . C , however, will face the ECDLP. Therefore, the proposed protocol is secure against a key-compromise impersonation attack.

Theorem 2. *The proposed protocol can resist a reflection attack.*

Proof. Due to the verification equation $V_B = x_{V_B}^{-1}(Y_B - e_B C_B P)$ and $V_A = x_{V_A}^{-1}(Y_A - e_A C_A P)$ performed by A and B in Steps 3 and 4, A and B can detect the generation of a wrong session secret key unlike Popescu's protocol. Therefore, the proposed protocol is secure to a reflection attack.

Theorem 3. *The proposed protocol can resist a replay attack.*

Proof. C can intercept V_A, Q_A, C_A (or V_B, Q_B, C_B) and can use them to impersonate A (or B) when sending the next key agreement message. For a random challenge, however, k_A and k_B , which are separately generated by A and B , are different every time. Since A and B always verify the integrity of the fresh session key K by checking C_A and C_B in Steps 3 and 4, the replayed messages can be detected by A and B , respectively.

Theorem 4. *The proposed protocol provides known-key security.*

Proof. Known-key security means that each run of a key agreement protocol between two entities A and B should produce unique secret keys; such keys are called session keys. Knowledge of a session key K and the random values k_A and k_B will not help in computing the other session keys $K' = H(x_{V'_A}, x_{V'_B}, x_{K'_{AB}}, x_{K'_{BA}})$. This is because without knowing k'_A and k'_B , it is impossible to compute the other session key K' .

Theorem 5. *The proposed protocol provides session key security.*

Proof. Session key security means that at the end of the key exchange, the session key is not known by anyone but A and B . This is because the random values k_A and k_B are protected by the ECDHP and the secure one-way hash function. Only A and B know about $K = H(x_{V_A}, x_{V_B}, x_{K_{AB}}, x_{K_{BA}})$ and this information is not revealed to anyone else.

Theorem 6. *The proposed protocol provides perfect forward secrecy.*

Proof. Perfect forward secrecy means that if the long-term private keys of one or more entities are compromised, the secrecy of previous session keys, which was established by honest entities, is not affected. If the user's password itself is compromised, an attacker will not be able to determine the session key K for the past sessions nor to decrypt them, since the attacker is still faced with the ECDHP. Therefore, the proposed protocol satisfies the properties of perfect forward secrecy.

6 Conclusion

The current paper demonstrated the vulnerability of Popescu's key agreement protocol with regard to a key-compromise impersonation attack, a reflection attack and a replay attack, and then an improved protocol was presented in order to resolve such problems. As a result, in contrast to Popescu's protocol, the proposed protocol is able to provide greater security.

Acknowledgements

This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

References

1. Miller, V.: Uses of Elliptic Curves in Cryptography. Proceedings of Crypto'85. Santa Barbara. USA. (1986) 417-426
2. Koblitz, N.: Elliptic Curve Cryptosystems. Mathematics of Computation. Vol. 48. (1987) 203-209
3. Koblitz, N. CM-Curves with Good Cryptographic Properties. Proceedings of Crypto'91. Santa Barbara. USA. (1992)
4. Popescu, C.: A Secure Authenticated Key Agreement Protocol. Proceedings of the 12th IEEE Mediterranean (MELECON 2004). Vol. 2. (2004) 783-786
5. Boyd, C., Mathuria, A.: Protocols for Authentication and Key Establishment. Springer-Verlag. (2003)
6. Menezes, A.J., Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptograph. CRC Press. New York. (1997)
7. Diffie, W., Hellman, M.: New Directions in Cryptography. IEEE Transaction on Information Theory. Vol. IT-22. No. 6. (1976) 644-654
8. Schneier, B.: Applied Cryptography-Protocols. Algorithms and Source Code in C. 2nd edi. John Wiley & Sons Inc. (1995)
9. Popescu, C.: An Identification Scheme based on the Elliptic Curve Discrete Logarithm Problem. Proceedings of The Fourth International Conference/Exhibition on High Performance Computing Asia-Pacific Region. Beijing. China. (2000) 624-625
10. Popescu, C.: A Secure Key Agreement Protocol Using Elliptic Curves. International Journal of Computers and Applications. Vol. 3. No. 202-1501 (May 2005)

SVM Based False Alarm Minimization Scheme on Intrusion Prevention System

Gil-Han Kim and Hyung-Woo Lee

Div. Computer Information of Software, Hanshin University,
411, Yangsan-dong, Osan, Gyunggi, 447-791, Korea
gillyty@hs.ac.kr, hwlee@hs.ac.kr

Abstract. The existing well-known network based intrusion detection / prevention techniques such as the misuse detection technique, etc., are widely used. However, because the misuse detection based intrusion prevention system is proportionally depending on the detection rules, it causes excessive large false alarm which is linked to wrong correspondence. This study suggests an intrusion prevention system which uses multi-class Support Vector Machines(SVM) as one of the rule based intrusion prevention system and anomaly detection system in order to solve these problems. When proposed scheme is compared with existing intrusion prevention system, it show enhanced performance result that improve about 20% and propose false positive minimize with effective detection on new variant attacks.

Keywords: False Alarm, Intrusion Detection/Prevention, Multi-class SVM, Network Security.¹

1 Introduction

The popularization of the Internet is also bringing forth the increase of actions damaging the integrity, confidentiality and availability of computer resources and destroying security policies. Thus, we need to design various intrusion detection/prevention systems to protect system resources and data on network from intrusions.

IPS is an in-line tool that can decide whether to pass a traffic or not based on the result of attack detection. Like IDS, IPS is divided into host-based IPS and network-based IPS according to data source[1]. In addition, according to detection model, it is divided into misuse detection IPS and anomaly IPS. Misuse detection IPS detects attacks using rules defined by experts. It is widely used because of the high detection rate but is vulnerable to variant attacks or those not captured by the rules. In addition, with the increase of rules, the rate of false detection (false positive) that detects a normal behavior as an attack also rises in geometrical progression.

¹ This work is supported by the University IT Research Center(IITRC) Project(IITA-2005-(C1090-0502-0020)).

In IPS that can make an active response, these problems may cause wrong responses to normal/attack packets, which in turn may disrupt the flow of normal services. Thus, the removal of false alarms (false positive, false negative) is an important issue in improving IPS performance [2]. On the other hand, anomaly IPS detects attacks by analyzing users' patterns and comparing them with input patterns using machine learning or data mining rather than depending on experts' knowledge. This method is flexible in attack detection but its detection rate is low [3]. Thus, the present study proposes a method of minimizing false alarms while maintaining the attack detection rate of misuse detection IPS by applying the mutually complementary features of misuse detection IPS with high attack detection rate and IPS based on learning using multi-class SVM with 'normal' modeling function.

Chapter 2 introduces previous researches to reduce false alarms, and Chapter 3 explains SVM used as a learning tool in this research. Chapter 4 describes the intrusion prevention technique using SVM to be proposed in this paper, and Chapter 5 explains experiment on the proposed model and its results. Lastly, Chapter 6 draws conclusions and discuss future researches.

2 Previous Researches for Minimizing False Alarms

In network security system, false alarm means false detection (false positive) that detects a normal behavior as an attack and miss detection (false negative) that judges an attack to be normal. False alarm causes the security system make a unnecessary response, spending resources and impairing the reliability of the security system. Thus, to reduce false alarms, researches have been made as follows.

2.1 False Alarm on Intrusion Detection

Normal packets are misunderstood as intrusion basically because intrusion patterns used in detection are wrong. Thus, to reduce false positive, signature should be precise. It is difficult to make false positive that detects intrusions precisely in every situation. Thus, when false positive occurs, it may be informed to developers so that they improve signature and reduce *false alarm* such as false positive[4].

False positive can be reduced not by developers but by system managers through tuning the system in accordance with system and network situation. If rules against intrusions are set by default, normal packets may be misunderstood as hacking. Thus, the system manager should change the signature in accordance with the network setting through trials and errors. In addition, false positive can be reduced by setting IPS environment fittingly to the protection policies of the corporation or organization and disabling signatures inconsistent with the protection policies.

2.2 Problems in Previous Researches

Previous researches to reduce false alarm (false positive) and miss detection (false negative), such as data mining[5,6] and correlation analysis technique[7,8], have

problems such as vulnerabilities inherent in system management and structure and lack of abilities to cope with new attacks.

Thus, the present study proposes as a behavior-based analysis method[9] using SVM an IPS model that minimizes false alarms and copes with new variant attacks effectively by analyzing and identifying false alarm patterns in four types of IPS detection results (true positive: identify attack as attack, false positive: identify normal as attack, true negative: identify normal as normal, false negative: identify attack as normal) in order to detect new attacks without the loss of train data.

- **Change of environment setting:** Difficult to manage when network environment changes frequently, and difficult to use when protecting individual systems with different degree of vulnerability
- **Data mining:** Cannot avoid information loss due to its structure, neglecting attacks that occur infrequently, so lack abilities to identify anomaly and cope with new patterns of attacks.
- **Correlation analysis:** Dependent on selected attributes, and not suitable for exhaustive exploration of causal relations among alarm data.
- **Behavior-based analysis:** lots of cost to calculate, dependent on data, cannot cope with new patterns of attacks.

3 Support Vector Machine (SVM)

Support vector machine (SVM) was a learning algorithm developed and proposed by Vapnik in 1995. While traditional learning algorithms are based on empirical risk minimization (ERM) to minimize empirical errors of the learning group, SVM is based on structural risk minimization to minimize the probability of wrong classification of data of fixed but unknown probability distribution [10].

3.1 Linear SVM – Separable Case

The purpose of SVM is to infer a function that distinguishes two classes with given train data. SVM learning is a process of finding the linear optimal separating hyperplane (OSH) under the constraint of maximizing the distance between the points of the two classes.

To make it possible to separate linearly the sets of learning vectors belonging to the two classes, the system should learn a training data set $\{x_i, d_i\}_{i=1}^N$ to have hyperplane $(\omega_0^T \cdot x) + b_0 = 0$ composed of weight vector ω and bias b . Here, x_i is an input pattern and d_i is a target value. Hyperplane $(\omega_0^T \cdot x) + b_0 = 0$ satisfies the condition of Equation (1).

$$\exists \omega, b \text{ s.t. } \begin{cases} \omega^T \cdot x_i + b > 0 & \text{for } d_i = +1 \\ \omega^T \cdot x_i + b < 0 & \text{for } d_i = -1 \end{cases} \quad (1)$$

In Equation (1), input patterns that satisfy the condition of the equal sign and are positioned closest to the decision surface are called support vectors. Conceptually, because these vectors are closest to the hyperplane, they are difficult to be

separated. Thus, learning for separation is to find the optimal hyperplane that satisfies the constraint of Equation (2). This is a problem of optimization with constraints. It is a quadratic problem to find the optimal values of parameter ω and b for the optimal hyperplane when training data set $\{x_i, d_i\}_{i=1}^N$ is given.

$$\exists \omega, b \text{ s.t. } \begin{cases} \min \Phi(\omega) = \frac{1}{2} \|\omega\|^2 \\ d_i((\omega^T \cdot x_i + b) \geq 1 \quad \text{for } i = 1 \dots N \end{cases} \quad (2)$$

Here, the values that have the maximum margin are the optimal values, and the maximum margin hyperplane can separate two classes optimally. Consequently, if the optimal separating hyperplane is expressed as $g(x) = \omega_0^T \cdot x + b_0$, the distance between a support vector and $g(x)$ is $\frac{1}{\|\omega\|}$, and the hyperplane that classifies input patterns optimally minimizes cost function $\Phi(\omega)$ as in Equation (3).

$$\Phi(\omega) = \frac{1}{2} \|\omega\|^2. \quad (3)$$

3.2 Nonlinear SVM

Most patterns are not linearly separable. Thus, to classify nonlinear patterns, we need to convert the input space of nonlinear patterns into a specific space of linear patterns.

$$\begin{aligned} \Theta(\alpha) &= \sum_{i=1}^N \alpha_i - \frac{1}{2} \sum_{i=1}^N \sum_{j=1}^N \alpha_i \alpha_j d_i d_j K(x_i, x_j) \\ \text{s.t. } \sum_{i=1}^N \alpha_i d_i &= 0, 0 \geq \alpha_i \geq C, \forall i. \end{aligned} \quad (4)$$

By obtaining Lagrange multiple i from the model above, we can get Equation (5) below, the most plane function in the specific space.

$$\begin{aligned} f(x) &= \sin(\langle \omega, \phi(x) \rangle + b) \\ &= \sin\left(\sum_{i=1}^N \alpha_i d_i K(x_i, x) + b\right) \end{aligned} \quad (5)$$

SVM provides kernels as in (Table 1) to support non-linear mapping functions.

Table 1. Types of kernel functions

Type of kernel	Kernel	Remarks
Dot Kernel	$x \cdot y$	Inner product of x and y
Polynomial kernel	$(x \cdot y + 1)^d$	$d=1,2,3, \dots$
RBF(Radial Basis Function) kernel	$\exp(-g\ x - y\ ^2)$	g is the parameter determining the share of kernels.
Perceptron kernel	$\tanh(ax \cdot y + b)$	a, b are constants satisfying Mercer's condition.

4 Intrusion Prevention System Using SVM

4.1 Structure of SVM-Based Intrusion Prevention System

In order to minimize false detection (false positive) and miss detection (false negative) in misuse detection IPS (Snort_inline), the intrusion prevention system to be proposed in this research is composed of multi-class SVM modules trained with the results of rule-based detection, which are classified into 4 classes (true positive: identify attack as attack, false positive: identify normal as attack, true negative: identify normal as normal, false negative: identify attack as normal).

In IPS, network packet collection is made at Snort_inline of promiscuous mode, and whether abnormal traffic or not is determined by rules in the detection engine. Because detected packets include false detection packets as well as miss detection packets, they are filtered through the SVM module for multi-class classification according to the 4 classes trained off-line, and only attack packets identified as true positive and false negative are handled by the action engine in a safe way.

4.2 Process Data Set

(1) Data Set of DARPA 1998. For developing and evaluating intrusion detection systems, DARPA data set provides Solaris-based BSM audit data and tcpdump data for the period from 1998 to 2000, around 7 weeks per year, and 5 days per week (Monday ~ Friday). Tcpdump data itself was made simply by storing packets passing through the network, so it is impossible to distinguish attacks from normal packets just with tcpdump data. Thus, a separate list file, which identifies attacks included in the tcpdump data, is provided together.

(2) Conversion of SVM Train Data Set. In order to apply the raw tcpdump data provided in DARPA 1998 as training and test data to a SVM learning algorithm and to draw precise classification results, it is most important to select the features of packets used as train data. In this research, to apply behavior models to each packet, we generated a train data per packet of tcpdump type (using -vv option), and a train data is composed of the set of features. A total of 26 features were extracted from packet headers.

4.3 SVM Learning Model

The SVM learning model for minimizing false detection and miss detection in misuse detection IPS is applied to SVM to classify four detection types defined by Snort_inline (TP, FP, TN, FN).

Basically, however, in order to apply SVM, which performs binary classification, to this study having 4 classes, strategies using binary classification combination should be presented. In this study, we designed and experimented two multi-class SVM models for minimizing false alarms that adopted one-against-all

[12] and one-against-one [13] methods composed of the combination of binary SVMs.

(1) Application of One-Against-All Method. One-Against-All(OAA) method uses k binary SVMs to classify k classes. Each SVM is trained with train data to identify a class. In our research problem that distinguishes TP, FP, TN and FN. The first SVM identifies FP.

In order to distinguish class FP from other classes TP, TN and FN, train data corresponding to FP have +1 and the others have -1. Then, for test data, each SVM is given the same input data, and the output values from the SVMs are compared, and the data is identified as the class of the SVM that produced the largest output value.

(2) Application of One-Against-One Method. Different from OAA, One-Against-One(OAO) method uses $\frac{k(k-1)}{2}$ binary SVM to identify k classes. Each train data is divided into two classes. The first SVM has train data composed of class FP and class TP, and it also classifies only class FP and class TP in test data. When classifying test data, all of the SVMs performs classification and test data is identified as the class with the largest number of votes.

5 Experiment and Result Analysis

5.1 Composition of Experiment Data

In order to evaluate and analyze the performance of the intrusion prevention system using SVM proposed in this study to minimize false alarms in existing intrusion prevention systems, first, we need to analyze the results of detection using an intrusion prevention system based on misuse detection (Snort_inline).

From tcpdump files and attack list files by day of each week in DARPA data set to be used as learning and test data, we extracted normal tcpdump data and anomaly tcpdump data by comparing attack time including duration, source IP address and destination IP address. The tcpdump data classified into normal and anomaly was used as input data to identify false alarm patterns and measure precision in Snort_inline, and 4 patterns (TP, FP, TN, FN) of data set are generated by comparing with Alert_list detected by the rules in the detection engine of Snort_inline

We obtained packets in the form of tcpdump divided into 4 classes from data for Friday of Week 2, Wednesday and Friday of Week 3, Tuesday and Wednesday of Week 4, Tuesday and Wednesday of Week 6 and Wednesday of Week 7 in DARPA 1998 data set, and took 1000 packets for each class so a total of 4000 packets as SVM train data. SVM_light [14] was used as a SVM experiment tool.

5.2 Experiment Results and Analysis

To evaluate the performance of multi-class SVM when the number of parameters in train data was 26, at which classification performance was highest in the prior

Table 2. Training and Test data Set for SVM

	TP data	FP data	TN data	FN data	Total
Training set	1000	1000	1000	1000	4000
Test set	300	300	300	300	1200

experiment, we calculated the classification rate of each model and the precision and recall rate of each class classified.

$$P_i = \frac{C_TP_i}{C_TP_i + C_FP_i}, \quad R_i = \frac{C_TP_i}{C_TP_i + C_FN_i} \tag{6}$$

(Table 3) shows the results of classification by each model, and Equation (6) expresses the precision and recall rate of $Class_i$ identified by multi-class SVM.

In the test environment, we used kernel functions dot and polynomial. We showed the results of applying integer 1 and 4 for the parameter degree(d) of the polynomial kernel and the results of applying real number 0.01, which showed the best results using empirical information through multiple experiments.

Table 3. Contingency table for $Class_i$

$Class_i$	Label Yes	Label No
Classifier Yes	C_TP	C_FP
Classifier No	C_FN	C_TN

(Table 4) and (Table 5) below are the results of experiment with multi-class SVM model based on OAA and OAO methods for the two kernel functions using train data composed of all of the 26 feature parameters.

According to the results, SVM using OAO method produced somewhat better results than that using OAA method and this is probably because, due to the characteristics of SVM intended for binary classification, classification patterns are calculated more precisely in data composed of classes in equal ratio.

In addition, when degree 4 was applied to the polynomial kernel, the classification rate for the 4 classes was highest (84.91%). In addition, precision and recall rate for each class were also as high as 90% on the average but classification was not clear between FN (false negative) and TN (true negative), namely, between attack packets that are not detected in Snort_inline and normal packets. This may be because, in preparing the test data of FN class, we included new attack data not included in the train data to evaluate the ability to detect variant attacks and new attacks.

(3) Performance Evaluation. In order to compare the performance of SVM-based IPS proposed in this study to minimize IPS false alarm, we applied the test data used in the multi-class SVM model to case-based training technique using k-NN algorithm. The comparative experiment used TiMBL (Tilburg Memory

Table 4. Result of testing OAA(one-against-all)

Kernel	Parameter	C	C_TP	C_FP	C_FN	C_TN	P(%)	R(%)	A(%)
Dot	-	FN	95	2	205	898	97.93	31.66	82.75
		FP	300	0	0	900	100	100	
		TN	298	204	2	696	59.36	99.33	
		TP	300	1	0	899	99.66	100	
Polynomial	d=1	FN	72	2	228	898	97.29	24	80.83
		FP	300	2	0	898	99.33	100	
		TN	298	226	2	674	56.87	99.33	
		TP	300	0	0	900	100	100	

C=class, P=precision, R=recall, A=classification rate

Table 5. Result of testing OAO(one-against-one)

Kernel	Parameter	C	C_TP	C_FP	C_FN	C_TN	P(%)	R(%)	A(%)
Dot	-	FN	96	6	204	894	94.11	32	82.50
		FP	300	2	0	898	99.33	100	
		TN	294	202	6	698	59.27	98	
		TP	300	0	0	900	100	100	
Polynomial	d=1	FN	96	6	204	894	94.11	32	82.50
		FP	300	2	0	898	99.33	100	
		TN	294	202	6	698	59.27	98	
		TP	300	0	0	900	100	100	

C=class, P=precision, R=recall, A=classification rate

Table 6. Result of classification

	Rate(%)	FP(%)	FN(%)	P(%)	R(%)	F(%)
Snort_inline	89	6.8	20.36	52.36	79.56	63.15
OAA	82.75	0.33	34	99.49	65.94	79.31
OAO	84.91	0.5	29.6	99.29	70.33	82.33
1-NN	79	0	42	100	58	73.41

Rate=(attack detection + Normal detection) / total test data

FP = false positive / normal, FN = false negative / attack

P=precision, R=recall, F=F-measure

Based Learner, version 5.1) [15], and the performance of Snort_inline, SVM and k-NN for the test data was expressed in harmonic mean (F-measure) combining precision and recall rate. F-measure is as Equation (7) below.

$$F = \frac{2}{\frac{1}{P} + \frac{1}{R}} \quad (7)$$

When comparing F-measure resulting from the experiment, false detection and miss detection rate decreased significantly in existing IPS as shown in (Table 6). Here, the detection rates for attacks and normal packets are not much meaningful because they did not consider false detection and miss detection.

The high detection rate of Snort_inline despite many false alarms may be because the number of packets used in the experiment was much larger than that in the comparative experiment. Thus, when the performance of each model was evaluated based on F-measure, the SVM-based IPS proposed in this research was found to have the highest performance.

6 Conclusions and Future Works

The present study proposed SVM-based IPS as a system combining misuse detection IPS applicable to wired/wireless network environment and learning-based anomaly detection IPS to minimize false detection and miss detection in misuse detection IPS and process only genuine alarms (true positive, false negative) in the action engine of IPS.

To apply SVM, which is intended for binary classification, to the classification of 4 detection patterns in misuse detection IPS, we designed and experimented two multi-class SVM models using one-against-all (OAA) and one-against-one (OAO) methods. According to the results of experiment, classification was more precise in multi-class SVM using OAO method than in that using OAA method.

It is expected to be applicable as a highly reliable intrusion prevention system through precise detection of and response to attacks. However, to apply the model to actual systems, we need to measure its performance quantitatively in real-time systems. In addition, a larger volume of train data is necessary to enhance the efficiency of anomaly detection.

References

1. Jo Hyeon-jeong, "Intrusion prevention system based on next-generation network security technology", Journal of Information Science Association, Volume 23, No. 1, p21-26, 2005.
2. C.Kruegel and T. Toth, "Using decision trees to improve signature-based detection", 6th Symposium on Recent Advances in Intrusion Detection(RAID), Lecture Notes in Computer Science, Springer Verlag, September, 2003.
3. Gary Golomb. IDS v. IPS Commentary, Linuxsecurity.com News, 6/16/2003, http://www.linuxsecurity.com/articles /forums_article- 7476.html
4. Internet Security System. "The Truth about False Positive", White Technical Report. 2001.
5. R. Lippman et als., "Evaluation intrusion detection system : The 1998 DARPA Off-line intrusion detection evaluation", Proc. Of DARPA Information Survivability Conference and Exposition, pp.12-26, 2000.
6. K. Julisch. "Mining alarm clusters to improve alarm handling efficiency", In 17th Annual Computer Security Application Conference(ACSAC), pp12-21, 2000.
7. Cuppens, F., Mieke, A. "Alert correlation in a cooperative intrusion detection framework", In Proceedings of the IEEE Symposium on Security and Privacy, 2002.
8. H. Debar, A.Wespi, "Aggregation and Correlation of intrusion-Detection Alert", In Recent Advances in intrusion Detection, No. 2212, Lecture Notes in Computer Science, Springer Verlag, p85-103, 2001.

9. S. Manganaris, M. Christensen, D. Zerkle and K. Hermiz, "A Data Mining Analysis of RTID Alarms", 2nd Work-shop on Recent Advances in Intrusion Detection(RAID99), 1999.
10. Campbell, C and Cristianini, N. "Simple Learning Algorithms for Training Support Vector Machines", Technical report, University of Bristol, 1998.
11. <http://snort-inline.sourceforge.net>
12. Hsu, C.W. and Lin, C.J. "A Comparison of Methods for Multi-class Support Vector Machines", IEEE Transaction on Neural Networks. Vol. 13. No.2. pp 415-425, 2002.
13. Knerr. S., Personnaz, L. and Dreyfus, G., "Single-layer Learning Revisited: A Step-wise Procedure for Building and Training a Neural Network", Neuro-computing: Algorithms. Architectures and Applications. J. Fogelman, Ed. Springer-Verlag, New York, 1990.
14. Christopher J.C. Burges, A Tutorial on Support Vector Machines for Pattern Recognition, 1998.
15. Daelemans, W., Zavrel, J. van der Sloot, K, and van denBosch, A., "TiMBL:Tilburg Memory Based Learner, version 5.1, Reference Guide", Technical Report 01-04, Induction of Linguistic Knowledge, Tilburg University, 2001.

Lightweight Wireless Intrusion Detection Systems Against DDoS Attack

Hyung-Woo Lee

Div. Computer Information of Software, Hanshin University,
411, Yangsan-dong, Osan, Gyunggi, 447-791, Korea
hwlee@hs.ac.kr

Abstract. Wireless intrusion detection systems are important to the security of wireless local area networks (WLANs). Wireless networks are not only susceptible to TCP/IP-based attacks native to wired networks, they are also subject to a wide array of 802.11-specific threats. To aid in the defense and detection of these potential threats, WLANs should employ a security solution that includes an intrusion detection system (IDS). Intrusion detection systems attempt to identify computer system and network intrusions and misuse by gathering and analyzing data. IDS has traditionally been developed to detect intrusions and misuse for wired systems and networks. In this paper, we suggest lightweight wireless IDS module on AP with network monitoring, analysis and filtering module against malicious DDoS attacks. Suggested system provides good performance on wireless LAN environments.¹

1 Introduction

With the increasing popularity of the wireless network, the security issue for mobile user could be even more serious than we expect. We need to search for new architecture and mechanisms to protect the wireless networks and mobile computing application against malicious attack[1].

The advent of WLANs, however, has opened organizations up to new IT security threats, and many traditional countermeasures are ineffective in dealing with them. Wireless access to networks, for example, cannot easily be monitored and controlled through perimeter defenses such as firewalls and proxy servers[2].

A wireless access point may open the internal, non-protected network up to unknown and non-trusted users who are simply within communication range. The nature of mobile computing environment makes it very vulnerable to an adversary's malicious attacks. First of all, the use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering. Unlike wired networks where an adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless network can come from all directions and target at any node[3].

¹ This work was supported by 2006 Hanshin University Research Grant.

Damages can include leaking secret information, message contamination, and node impersonation. All these mean that a wireless network will not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly.

Threats to wireless local area networks (WLANs) are numerous and potentially devastating. Security issues ranging from mis-configured wireless access points (WAPs) to session hijacking to Denial of Service (DoS) can plague a WLAN. Wireless networks are not only susceptible to TCP/IP-based attacks native to wired networks, they are also subject to a wide array of 802.11-specific threats[4]. To aid in the defense and detection of these potential threats, WLANs should employ a security solution that includes an intrusion detection system(IDS)[5].

This study will describe the need for wireless intrusion detection on AP(Access Point) based lightweight module, provide an detailed architecture of wireless intrusion detection system, and identify the benefits and drawbacks of a wireless intrusion detection solution.

Chapter 2 introduces and overviews on wireless LAN attack and threat previous, and Chapter 3 explains common IDS concept with existing wireless IDS system to lessen the malicious attack. And we additionally reviewed attack detection and policy enforcement mechanism. Chapter 4 describes the proposed wireless intrusion detection technique with lightweight form on AP, and Chapter 5 evaluate the performance of proposed system and its results. Lastly, Chapter 6 draws conclusions and discuss future researches.

2 Threats to Wireless LAN

2.1 Wireless LAN Attack

Wireless local area networks are subject to a variety of threats. The standard 802.11 encryption method, Wired Equivalent Privacy (WEP) is weak. So even if WEP encryption is utilized on a WLAN, an attacker can potentially intercept and decrypt sensitive data from wireless communications. Hackers can also attack a WLAN and gather sensitive data by introducing a rogue WAP into the WLAN coverage area[4].

By installing a WAP on an established LAN, a user can create a backdoor into the network, subverting all the hard-wired security solutions and leaving the network open to hackers. It is for this reason that even organizations without a WLAN implementation must strongly consider deploying a wireless IDS solution. It is very possible that users can and will install a rogue WAP, exposing even an exclusively hard-wired organization to the risks of WLANs.

2.2 DoS Attack on Wireless LAN

Networks using 802.11 are also subject to a number of denial of service (DoS) attacks that can render a WLAN inoperable. Wireless communications are inherently vulnerable to signal degradation when encountering physical objects[6].

Hackers can also cause malicious DoS attacks by flooding WAPs with association requests and forcing them to reboot. In addition, they can use the aforementioned rogue WAP to send repeated disassociate/deauthenticate requests to deny service to a wireless client. A variety of other WLAN threats exist and additional vulnerabilities are being identified at an ever-increasing pace[7].

Without some sort of detection mechanism, it can be difficult to identify the threats to a WLAN. A lack of threat awareness can lead to a network not adequately secured against the threats facing it. Only when the threats to the network are realized can the WLAN be properly equipped with the necessary security measures.

3 Overview on Wireless Intrusion Detection

3.1 Intrusion Detection Systems

Intrusion detection systems (IDSs) attempt to identify computer system and network intrusions and misuse by gathering and analyzing data. IDSs have traditionally been developed to detect intrusions and misuse for wired systems and networks. More recently, IDSs have been developed for use on wireless networks. These wireless IDSs can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations for WLANs.

Wireless IDSs gather all local wireless transmissions and generate alerts based either on predefined signatures or on anomalies in the traffic. A Wireless IDS is similar to a standard, wired IDS, but has additional deployment requirements as well as some unique features specific to WLAN intrusion and misuse detection[6].

3.2 Wireless Intrusion Detection Systems[2]

(1) Host-Based IDSs. There is a more powerful approach to secure WLANs intrusion detection (ID), which is the art of detecting inappropriate, incorrect, or anomalous activity. ID systems (IDSs) that operate on a host to detect malicious activity on that host are called host-based IDSs, and IDSs that operate on network data flows are called network-based IDSs.

(2) Functionality-Based Network IDSs. The most common approaches to ID are statistical anomaly detection and pattern-matching detection. As we know that applying functionality-based network IDS models also has limitations. Anomaly detection model is built on a long-term monitoring and classifying of what is a normal system behavior.

Wireless networks are very dynamic in structure, giving rise to apparently random communication patterns, thus making it challenging to build a reliable behavioral model.

3.3 Existing System and Architecture

(1) Existing Wireless IDS System. Popular wireless IDS solutions include Airdefense RogueWatch and Airdefense Guard[7][10], and Internet Security

Systems Realsure Server sensor and wireless scanner products[11]. A home-grown wireless IDS[5] can be developed with the use of the Linux operating system, for example, and some freely available software. Open source solutions include Snort-Wireless[12] and WIDZ[13], among others.

(2) Centralized or Distributed IDSs. A wireless IDS can be centralized or decentralized(distributed). A centralized wireless IDS is usually a combination of individual sensors which collect and forward all 802.11 data to a central management system, where the wireless IDS data is stored and processed[2].

Decentralized or distributed wireless intrusion detection usually includes one or more devices that perform both the data gathering and processing/reporting functions of the IDS. The decentralized method is best suited for smaller (1-2 WAP) WLANs due to cost and management issues. The cost of sensors with data processing capability can become prohibitive when many sensors are required. Also, management of multiple processing/reporting sensors can be more time intensive than in a centralized model.

3.4 Attack Detection with Policy Enforcement

(1) Physical Attack Detection. A wireless IDS can aid in detecting the attacker's location by providing at least a general estimate of their physical location. By correlating the captured 802.11 data with the sensor location as well as the location of the victim WAP, the physical location of the attacker can be more easily identified.

Once the physical location has been narrowed, a response team equipped with tools like Kismet[9] can scan the general area identified by the IDS to further narrow the search for the attackers. With this dual-pronged identification approach (using the IDS and scanning tools), the physical response team should be able to identify and intercept the attackers quickly and effectively.

(2) Policy Enforcement. A wireless IDS not only detects attackers, it can also help to enforce policy. WLANs have a number of security-related issues, but many of the security weaknesses are fixable.

Features such as rogue WAP detection, and policy enforcement in general, go a long way to increase the security of the WLAN. The additional assistance a wireless IDS provides with respect to policy enforcement can also maximize human resource allocation. This is because the IDS can automate some of the functions that humans would ordinarily be required to manually accomplish, such as monitoring for rogue WAPs.

4 Proposed Lightweight Wireless IDS

4.1 Proposed Architecture

Proposed wireless IDS does a network monitoring function on AP(Access Point) with lightweight module. Specially, it is aimed at both packet filtering and detection/prevention on wireless traffic. Therefore, proposed system is for the monitoring on wireless packet by the functionality of wireless security sensor.

(1) **Proposed Model of W-IDS.** We developed the module of attack packet detection efficiency and efficiency analysis gained through cooperative detection, assessment of the risk to the network and client from the attack. Although currently developed systems were operate on wired network, it did not detect malicious traffic on AP by embedded module. So, we designed and implemented lightweight IDS module on AP(specially Linksys WRT54GS) for packet filtering and monitoring functions as Fig. 1.

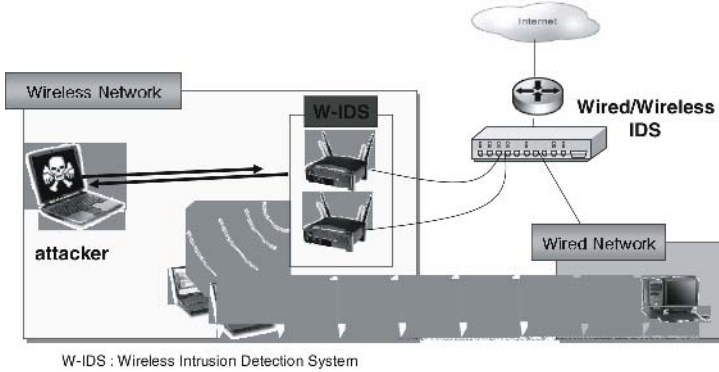


Fig. 1. System Model of AP based Wireless IDS

(2) **Proposed W-IDS Architecture on AP.** The proposed architecture is shown in Fig. 2. System consists of three sub modules : *Listener* for traffic monitoring, *Real Time analysis* for wireless attack detection, and *Alert Interface* for network log management.

Listener collects whole packet by 802.11 b/g channel hopping and monitors level 2 wireless traffic for sending log to integrated wired/wireless IDS system(such as ESM). Aggregated wireless packets sent to packet analysis module for analysis/classification of attack or normal traffic based on the intrusion signature. If alert is happen, it will be sent to the ESM server to block or drop packets.

The AP is consisted of two module, *Network Monitoring(MN)* module and *Analysis & Security(AnS)* module. On *MN* module, we can listen or capture the inbound wireless packet with parsing module after preprocessing the 802.11 frame. Preprocessed packet sent to *AnS* module for analyzing and filtering based on intrusion DB & Signature. *AnS* module determine attack packet from normal based on IDS engine.

- **Network Monitoring Module** passively sniffer 802.11 b/g frame for detecting attack by monitoring mode.
- **Rogue AP Detection Module** compare authenticated AP list and preregistered information for detecting legal or rogue AP.
- **Spoof, DoS & MITM Detection Module** trace sequence number for detecting MAC spoofing attack on DoS de-auth flooding traffic after checking the state of disassociate & deauthenticate frame packet.

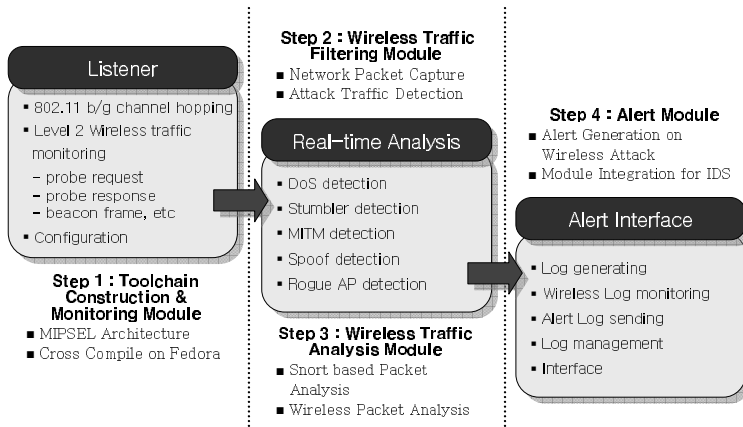


Fig. 2. W-IDS Module on AP

- **Alert Interface Module** send *micro-Perl* script to server for wireless network management, to which distributed AP sensors issue and send Alert Log script.

4.2 Interlocking with Intrusion Response System

Integrated Wired & Wireless Intrusion Response System (IRS) provide attack packet detection on wired & wireless traffic with *Firewall* module on 1st step, and misuse and anomaly detection with *IPS* module on 2nd step, which is done by inline mode. And on final 3rd step, *IRS* system shows us real-time log data through the integrated monitoring module.

4.3 Integrated W-IDS System

Fig. 3 shows the integrated W-IDS system proposed in this study. As shown it, the network manager can monitor whole wired & wireless network. Especially the distributed multiple APs send alert log to the *IRS*.

The *IRS* system consists of two main module, network and security module. *Network module* is divided into bridge and network monitoring modules. And *Security module* does firewall function in first, and then prevention module in next step.

5 Performance Evaluation

5.1 Threat Detection by W-IDS

A wireless IDS can also aid in the detection of a number of attacks. Not only can a wireless IDS detect rogue AP, identify non-encrypted 802.11 traffic, and help isolate an attacker's physical location, as mentioned earlier - a wireless IDS can

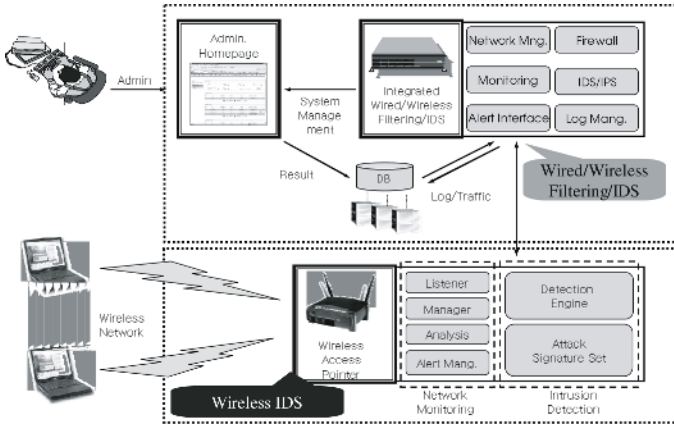


Fig. 3. Overall System Model for W-IDS

detect many of the standard (and not-so standard) wireless attacks and probes as well.

A wireless IDS can also detect some DoS attacks. DoS attacks are relatively common with wireless networks, as many DoSs occur from signal loss due to a frequency conflict or a building that just went up across the street. Sometimes though, as mentioned earlier, hackers can attack the WLAN with the intent of denying it service. A wireless IDS can detect many of the attacks used to DoS WLANs, such as flooding authentication requests or dissassociation/deauthentication frames.

Proposed wireless IDS can spot many of the other 802.11 threats as well. A wireless IDS can detect the presence of MAC address spoofing by sequence number analysis. In contrast, a wireless IDS can detect unique and non-standard threats through the utilization of user developed rules. This flexibility, common with standard IDSs, allows a wireless IDS to be scaleable and to address many distinctive detection requirements.

5.2 Efficiency Evaluation of W-IDS

The efficiency of the W-IDS is derived based on all possible attacks and *false alarms* raised during an observation period.

$$E_{WIDS} = Q \cdot H / (H + Q \cdot M) \tag{1}$$

where E_{WIDS} is the efficiency of the IDS, Q is the Alarm Confidence, H is the Average Detection Hit Rate, and M is the Average Detection Miss Rate. The alarm confidence, Q , is a quality indicator of the IDS system over the entire attack set defined as (2).

$$Q = x/G \tag{2}$$

where x is the summation of all detection hits based on an empirically generated alarm matrix and G is the alarm frequency defined as the summation of all raised

alarms in the monitoring period ($G = u + x + z$) denoted in the alarm matrix as false positives (u), hits (x) and confused alarms (z).

The average detection hit rate, H , is defined as: $H = x/F$ where F is defined as the attack frequency and is the summation of all real attacks within the monitoring period ($F = x + y + z$) including false negatives (y).

Finally, the average detection miss rate, M , is defined as $M = y/F$. The alarm frequency, G , is used to determine between two groupings of response strategies. The strategy selected within a group is chosen based on the maximum risk, R_{max} .

In order to determine the maximum risk, the average damage, D , must first be determined over all attack types. This can be expressed as an amount by estimating the monetary loss for each attack type if successful, then calculating the average over all attack types. The maximum risk multiplies the attack damage by the corresponding attack frequency and is defined as $R_{max} = D \cdot F$ [6]. We can simulate and evaluate the efficiency of IDS as follows Table 1.

Table 1. Evaluation of W-IDS

	Q(%)	H(%)	M(%)	E(%)	R(%)
Snort-Wireless	86.50	87.55	12.45	6.50	-
Proposed W-IDS	84.91	89.45	10.55	7.51	7.33

$E = (QH / (H + QM))$, Q=Alarm Confidence
H=Detection Hit Rate, M=Detection Miss Rate

The response strategy can be implemented in a response matrix, where m responses are mapped to n attacks. The same response may be effective against multiple attacks, and an attack may have more than one effective response. The IDS efficiency for each attack/response pair can then be measured and tabulated as the Hit efficiency and False/Miss efficiency based on learned behavior at the specific location, or previously tested results depending on the type of attack and response.

And overall traffic monitoring and summary on AP can evaluate the performance of developed system in Fig. 4. In addition, the false alarm measure on wireless traffic can estimate the functional efficiency of IDS system.

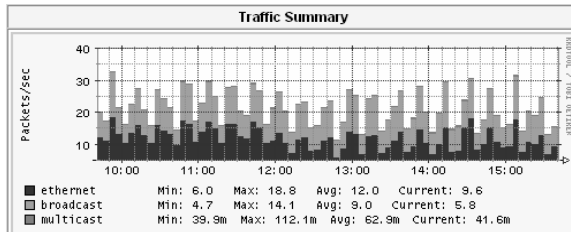


Fig. 4. Network Traffic with W-IDS

6 Conclusions

While there are drawbacks to implementing a wireless IDS, the benefits will most likely prove to outweigh the downsides. With the capability to detect probes, DoSs, and variety of 802.11 attacks, in addition to assistance with policy enforcement, the benefits of a wireless IDS can be substantial. Of course, just as with a wired network, an IDS is only one part of a greater security solution. WLANs require a number of other security measures to be employed before an adequate level of security can be reached, but the addition of a wireless IDS can greatly improve the security posture of the entire network. With the immense rate of wireless adoption, the ever-increasing number of threats to WLANs, and the growing complexity of attacks, a system to identify and report on threat information can greatly enhance the security of a wireless network.

Acknowledgement. This work was partially supported by the University IT Research Center(ITRC) Project(IITA-2005-(C1090-0502-0020)).

References

1. Hongyu Yang, Lixia Xie, Jizhou Sun, "Intrusion Detection Solution to WLANs," IEEE 6th CAS Symp. on Emerging Technologies: Mobile and Wireless Comm. pp.553-556, Shanghai, China, May 31-June 2, 2004.
2. Hongyu Yangla, Lixia Xie, Jizhou Sun, "Intrusion Detection for Wireless Local Area Network," CCECE 2004- CCGEI 2004, pp.1949-1952, May 2004.
3. Timothy R. Schmoyer, Yu Xi Lim and Henry L. Owen, "Wireless Intrusion Detection and Response, A case study using the classic man-in-the-middle attack," WCNC 2004, IEEE, pp. 883-888, 2004.
4. J. Bellado, 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions, Proceedings of the USENIX Security Symposium, August 2003, pp. 15-28.
5. Y. X. Lim, T. Schmoyer, J. Levine, H. Owen, Wireless intrusion detection and response, IEEE 4th Annual Information Assurance Workshop, West Point N.Y., pp. 68-75, June 2003.
6. Jamil Farshchi, "Wireless Intrusion Detection Systems," Security Focus, Article, 5th, Nov, 2003 (<http://www.securityfocus.com/infocus/1742>).
7. Airdefense Inc. "wireless LAN Security: Enterprise Rouge Detection?," 2002.
8. G. Helmer, J. Wong, V. Honavar, L. Miller, "Lightweight agents for intrusion detection," Technical Report, Dept. of Computer Science, Iowa State University, 2000.
9. Kismet 802.11 Wireless Sniffer, "<http://www.kismetwireless.net/>".
10. Accurate Wireless Intrusion Protection & Monitoring, "<http://www.airdefense.net/>," AirDefense, 2005.
11. RealSecure Server, "<http://www.iss.net/>," Internet Security System, 2005.
12. Snort Wireless, "<http://snort-wireless.org/>," Snort-Wireless, 2005.
13. WIDZ Wireless Intrusion Detection System, "http://www.loud-fat-bloke.co.uk/articles/widz_design.pdf".
14. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone (ed.), "Handbook of Applied Cryptography", CRC Press, (<http://www.cacr.math.uwaterloo.ca/hac/>), 1996.
15. B. Schneier, "Applied Cryptography", Second Edition, Wiley, 1996.

One-Time Password Authentication Scheme Using Smart Cards Providing User Anonymity

Eun-Jun Yoon and Kee-Young Yoo*

Department of Computer Engineering, Kyungpook National University,
Daegu 702-701, South Korea
ejyoon@infosec.knu.ac.kr, yook@knu.ac.kr

Abstract. In 2005, Lee and Chen proposed an improved one-time password authentication scheme that can prevent a stolen verifier attack and that is as efficient as the scheme of Yeh-Shen-Hwang. The current paper, however, demonstrates that Lee-Chen's scheme is still vulnerable to Denial-of-Service attacks and a simple solution is presented in order to isolate such a problem. Furthermore, we propose an efficiently optimized one-time password authentication scheme that can provide user anonymity. In addition the computational costs are lower than those of Lee-Chen's scheme.

Keywords: Cryptography, Security, One-time password, User authentication, Smart card, Denial-of-Service attacks.

1 Introduction

Internet applications and mobile techniques have been developed significantly in recent years. Since the Internet is an open network and users do not see each other, it is very important to authenticate the identity of the users. In order to identify the users, the password authentication scheme is the most common method. Many password authentication schemes [1][2][3] have been proposed for electronic commerce environments. The S/Key one-time password scheme is designed to detect replay attacks or eavesdropping attacks [2][3]. With this scheme, the user's secret pass-phrase does not need to cross the network at any time, such as during authentication or during pass-phrase changes. Moreover, no secret information needs be stored in any system, including the server being protected. Although the S/KEY scheme, thus protects against passive attacks based upon replaying captured reusable passwords, it is vulnerable to server spoofing attacks, preplay attacks and off-line dictionary attacks [1][4].

In 2002, Yeh-Shen-Hwang [4] proposed a secure one-time password authentication scheme using smart cards that can withstand many various attacks, such as replay attacks, server spoofing attacks, off-line dictionary attacks, and active attacks. Tsuji et al. [5] and Ku et al. [6], however, showed that Yeh-Shen-Hwang's scheme is still vulnerable to a stolen verifier attack [5][6]. In 2005, Lee-Chen [7] proposed an improved one-time password authentication scheme, which not

* Corresponding author. Tel.: +82-53-950-5553; Fax: +82-53-957-4846.

only keeps the security of the scheme of Yeh-Shen-Hwang [4], but it can withstand the stolen verifier attacks [5][6]. Lee-Chen's scheme, however, suffers from Denial-of-Service attacks, in which an attacker can easily make the server reject all subsequent login requests from any user. Accordingly, the current paper demonstrates that Lee-Chen's scheme is vulnerable to Denial-of-Service attacks [9] and a simple solution is presented to isolate such a problem. Furthermore, we propose an efficiently optimized one-time password authentication scheme that can provide user anonymity and the computational costs are less than that of Lee-Chen's scheme.

This paper is organized as follows: In Section 2, we briefly review Lee-Chen's one-time password authentication scheme and we will show the security flaws of the scheme. In Section 3, we present improvements on the scheme. In Section 4, we analyze the security of our proposed scheme. Finally, our conclusions are presented in Section 5.

2 Security Analysis of Lee-Chen's Scheme

This section briefly reviews Lee-Chen's one-time password authentication scheme and it will show the security flaws of the scheme. The abbreviations used in this paper are as follows:

- U, S, E : the user, the server, and the attacker, respectively
- ID : the identity of U
- x : the secret key of S
- $SEED$: a pre-shared secret of S and U
- D_i : a large random number generated by S
- K : a secret key/password of U
- $H(\cdot)$: a secure hash function
- T : a timestamp
- \oplus : bit-wise XOR operation
- \parallel : concatenation operation
- N : the number of logins
- C_i : the number of hash iterations, where $C_i = N - i$
- p_i : $p_i = H^{C_i}(K \oplus SEED)$. For example, $H^2(K \oplus SEED) = H(H(K \oplus SEED))$.

2.1 Review of Lee-Chen's Scheme

Lee-Chen's scheme is divided into three stages: the registration stage, the login stage, and the authentication stage. We describe the three stages of the scheme as follows:

Registration Stage. The registration stage of Lee-Chen's scheme is as follows:

1. $U \leftarrow S : SEED$

Initially, S computes $SEED = H(ID \oplus x)$, and issues a smart card containing $SEED$ to U .

2. $U \leftarrow S : N, H(SEED \oplus N) \oplus SK, H(SK)$
 S selects D and T , and computes $SK = D||T$. Then S decides N , and computes $H(SEED \oplus N) \oplus SK$. S sends $N, H(SEED \oplus N) \oplus SK$ and $H(SK)$ to U .
3. $U \rightarrow S : p_0 \oplus SK$
 U computes $SEED \oplus N$, and hashes it one time. U extracts SK by computing $(H(SEED \oplus N) \oplus SK) \oplus H(SEED \oplus N)$. Then, SK is hashed one time and compared with $H(SK)$. If it matches, the identity of S is authenticated. Then, U computes $p_0 \oplus SK$, where $p_0 = H^N(K \oplus SEED)$, and sends it to S .
4. S extracts p_0 by computing $(p_0 \oplus SK) \oplus SK$, and stores it as a verifier for authenticating U .

Login Stage. The login stage of the scheme is as follows:

1. $U \leftarrow S : C_i, H(SEED \oplus C_i) \oplus SK_i, H(SK_i) \oplus p_{i-1}$
 For the i th login, S computes $SEED = H(ID \oplus x)$, and generates D_i and T_i . S computes $SK_i = D_i||T_i$, and sends $C_i, H(SEED \oplus C_i) \oplus SK_i$ and $H(SK_i) \oplus p_{i-1}$ to U .
2. $U \rightarrow S : p_i \oplus SK_i$
 U extracts SK_i by computing $(H(SEED \oplus C_i) \oplus SK_i) \oplus H(SEED \oplus C_i)$, and checks T_i of SK_i . If T_i is valid, U computes p_{i-1} , and then uses it to extract $H(SK_i)$ from $H(SK_i) \oplus p_{i-1}$. Then, SK_i is hashed one time and compared with $H(SK_i)$. If it is equivalent, the identity of S is authenticated. Then, U computes $p_i = H^{C_i}(K \oplus SEED)$ and $p_i \oplus SK_i$, and sends $p_i \oplus SK_i$ to S .

Authentication Stage. Upon receiving $p_i \oplus SK_i$, S obtains p_i by computing $(p_i \oplus SK_i) \oplus SK_i$. Then, p_i is hashed one time and compared with p_{i-1} . If it is equivalent, the identity of U is authenticated. Finally, S replaces p_{i-1} and C_{i-1} with p_i and C_i in the database.

2.2 A Denial-of-Service Attack on Lee-Chen's Scheme

This subsection shows how the Denial-of-Service attack [9] can work on Lee-Chen's scheme. This attack prevents or inhibits the normal use or management of communications facilities. This attack may be directed to a specific user. For example, an attacker E may perform this attack to cause the server to reject the login of a specific user.

In Step 3 of the registration stage, E can simply replace $p_0 \oplus SK$ with the forged $p_0 \oplus SK \oplus X$, where X is a random number chosen by E . After receiving the replaced $p_0 \oplus SK \oplus X$, S will extract $p_0 \oplus X$ by computing $(p_0 \oplus SK \oplus X) \oplus SK$. Then, S will store $p_0 \oplus X$ as a verifier in order to authenticate U . Since $p_0 \oplus X$ is not equal to U 's p_0 , all subsequent login requests of U will be rejected until U has re-registered with S .

In another type of Denial-of-Service attack, in Step 3 of the registration stage, E can simply replace $p_0 \oplus SK$ with the forged X , where X is a random number chosen by E . After receiving the replaced X , S will extract $X \oplus SK$ by computing $X \oplus SK$. Then, S will store $X \oplus SK$ as a verifier for authenticating U . Since

$X \oplus SK$ is not equal to U 's p_0 , all subsequent login requests of U will be rejected until U has re-registered with S . Obviously, Lee-Chen's scheme is vulnerable to against Denial-of-Service attacks.

3 Proposed Solutions

This section proposes two solutions (a simple solution and an efficiently optimized one-time password authentication scheme providing user anonymity) in order to overcome the above mentioned problems inherent in Lee-Chen's scheme.

3.1 Countermeasures

This subsection proposes a simple solution to overcome the above mentioned problem inherent in Lee-Chen's scheme. Only the registration stage is modified. That is, in Step 3 of the registration stage, U sends the verification value $H(p_0)$ with $p_0 \oplus SK$. The proposed registration stage is as follows:

1. $U \leftarrow S : SEED$
2. $U \leftarrow S : N, H(SEED \oplus N) \oplus SK, H(SK)$
3. $U \rightarrow S : p_0 \oplus SK, H(p_0)$
 U computes $SEED \oplus N$, and hashes it one time. U extracts SK by computing $(H(SEED \oplus N) \oplus SK) \oplus H(SEED \oplus N)$. Then, SK is hashed one time and compared with $H(SK)$. If it matches, the identity of S is authenticated. Then, U computes $p_0 \oplus SK$, and sends it with $H(p_0)$ to S .
4. Upon receipt $p_0 \oplus SK$ and $H(p_0)$, S extracts p_0 by computing $(p_0 \oplus SK) \oplus SK$. Then, p_0 is hashed one time and compared with $H(p_0)$. If it is equivalent, the identity of U is authenticated. Finally, S stores p_0 as a verifier for authenticating U .

Theorem 1. *The proposed simple solution can resist Denial-of-Service attacks.*

Proof. In Step 3 of the proposed registration stage, E can replace $p_0 \oplus SK$ with the forged $p_0 \oplus SK \oplus X$, in which X is a random number chosen by E . After receiving the replaced $p_0 \oplus SK \oplus X$, S will extract $p_0 \oplus X$ by computing $(p_0 \oplus SK \oplus X) \oplus SK$. Then, $p_0 \oplus X$ is hashed one time and compared with $H(p_0)$. Since $p_0 \oplus X$ is not equal to $H(p_0)$ and E cannot compute $H(p_0)$ without knowing K and $SEED$, E cannot succeed in overcoming the Denial-of-Service attacks. Also, E can replace $p_0 \oplus SK$ with the forged X , in which X is a random number chosen by E . After receiving the replaced X , S will extract $X \oplus SK$ by computing $X \oplus SK$. Then, $X \oplus SK$ is hashed one time and compared with $H(p_0)$. Since $X \oplus SK$ is not equal to $H(p_0)$ and also E cannot compute $H(p_0)$ without knowing K and $SEED$, E cannot succeed in overcoming Denial-of-Service attacks.

3.2 Efficiently Optimized Authentication Scheme

This subsection proposes an efficiently optimized one-time password authentication scheme using smart cards by providing user anonymity. There are three phases in the proposed scheme including a registration stage, a login stage and an authentication stage. Fig. 1 illustrates the proposed one-time password authentication scheme.

Shared Information: Secure hash function $H(\cdot)$
 Information held by U : Identity ID , Secret key/password K , Smart card
 Information held by S : Secret key x , U 's account database($ID, H(ID||SEED), N, p_0$)

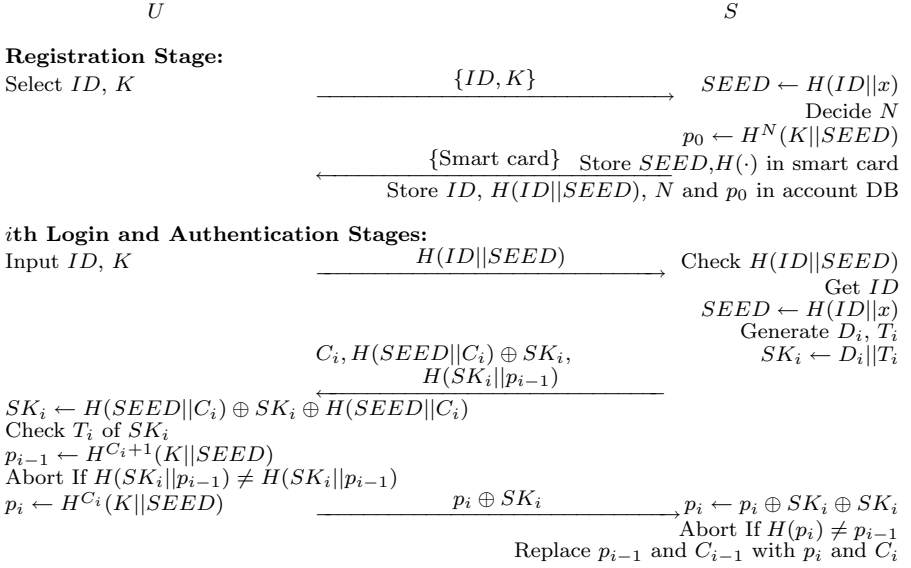


Fig. 1. Proposed One-time Password Authentication Scheme Providing User Anonymity

Registration Stage. The registration stage of proposed scheme is as follows:

1. $U \rightarrow S : ID, K$
 U selects his identity ID and secret key/password K freely. Then, U sends the ID and K to S through a secure channel.
2. $U \leftarrow S : \text{Smart card}$
 Initially, S creates an entry for U in the account database, and computes $SEED = H(ID||x)$. Then, S decides N , and computes the initial one-time password $p_0 = H^N(K||SEED)$. Finally, S stores the $ID, H(ID||SEED), N$ and p_0 in U 's account database as a verifier for authenticating U , and a smart card is issued containing $SEED$ and $H(\cdot)$ to U through a secure channel.

Login Stage. The login stage of proposed scheme is as follows:

1. $U \rightarrow S : H(ID||SEED)$
 U inserts his smart card into the card reader, keys in the ID and K . U 's smart card computes $H(ID||SEED)$ by using the stored $SEED$, and then sends it as a login request message to S .
2. $U \leftarrow S : C_i, H(SEED||C_i) \oplus SK_i, H(SK_i||p_{i-1})$
 For the i th login, S checks the validity of $H(ID||SEED)$ by using the account database. If $H(ID||SEED)$ is not a valid identity, S rejects U 's login request.

Otherwise, S gets the ID from U 's account field, and computes $SEED = H(ID||x)$ and $H(ID||SEED)$. Then, S generates D_i and T_i , and computes $SK_i = D_i||T_i$. Finally, S sends C_i , $H(SEED||C_i) \oplus SK_i$ and $H(SK_i||p_{i-1})$ to U .

3. $U \rightarrow S : p_i \oplus SK_i$

U extracts SK_i by computing $(H(SEED||C_i) \oplus SK_i) \oplus H(SEED||C_i)$, and checks T_i of SK_i . If T_i is valid, U computes p_{i-1} and $H(SK_i||p_{i-1})$, and then compares whether $H(SK_i||p_{i-1})$ is equal to the received $H(SK_i||p_{i-1})$. If it is equal, the identity of S is authenticated. Then, U computes $p_i = H^{C_i}(K||SEED)$ and $p_i \oplus SK_i$, and sends $p_i \oplus SK_i$ to S .

Authentication Stage. Upon receiving $p_i \oplus SK_i$, S obtains p_i by computing $(p_i \oplus SK_i) \oplus SK_i$. Then, p_i is hashed one time and compared with p_{i-1} . If they are equivalent, the identity of U is authenticated. Finally, S replaces p_{i-1} and C_{i-1} with p_i and C_i in the database.

4 Security Analysis

This section analyzes the security of the proposed scheme. First, we define the security terms [8] that are needed for the analysis.

Definition 1. A weak secret key (password K) is a value of low entropy $W(k)$, which can be guessed in polynomial time.

Definition 2. A strong secret key (x) is a value of high entropy $H(k)$, which cannot be guessed in polynomial time.

Definition 3. A secure one-way hash function $y = H(x)$ is one in which, given x , it is easy to compute y and in which, given y , it is hard to compute x .

Here, the security properties [8][9][10][11] must be considered in the proposed scheme: a guessing attack, replay attack, impersonation attack, stolen-verifier attack, Denial-of-Service attack, mutual authentication, and user anonymity. Under the above definitions, the following theorems are used to analyze the security properties in the proposed scheme.

Theorem 2. The proposed scheme can resist guessing attacks.

Proof. Suppose any attacker E captures all communication messages from the public channel in the login and authentication stages. Due to the fact that a secure one-way hash function is computationally difficult to invert, it is extremely hard for E to derive the secret value $SEED$ from $H(ID||SEED)$ and $H(SEED||C_i) \oplus SK_i$. It is also extremely hard for E to derive the U 's one-time password p_i (or p_{i-1}) from $H(SK_i||p_{i-1})$. Without knowing the randomness SK_i , E cannot derive p_i from $p_i \oplus SK_i$. Even if U 's smart card is picked up by E , it is still difficult for the attacker to derive x from $SEED$. Therefore, the proposed scheme can resist guessing attacks.

Theorem 3. *The proposed scheme can resist replay attacks.*

Proof. In order to protect from replay attacks, E can intercept $H(ID||SEED)$ which is sent by U in Step 1 and can use it to impersonate U when sending the next login message. For a random challenge, however, SK_i , which is separately generated by S , is different every time. As a result, the replay of U 's old login message in Step 3 is detected by S because E has no p_i to compute a correct $p_i \oplus SK_i$. Also, E may try to modify the random number D_i and the time stamp T_i in order to achieve the replay attack. It, however, does not work unless $p_i \oplus SK_i$ is modified to a correct value. It is also difficult to modify $p_i \oplus SK_i$ correctly without knowing p_i . Furthermore, neither the replay of U 's old login messages nor the replay of S 's response message in the login stage will fail in Step 3 due to the time interval check. Therefore, the proposed scheme can resist replay attacks.

Theorem 4. *The proposed scheme can resist impersonation attacks.*

Proof. E can attempt to modify a message $p_i \oplus SK_i$ into $p_i^* \oplus SK_i^*$ and send it to S , where p_i^* and SK_i^* are a random nonce selected by E . Without knowing the K and $SEED$, however, such a modification will fail in authentication stage, because E has no way of obtaining p_i and SK_i to compute the valid $p_i \oplus SK_i$. If a masqueraded S tries to cheat the requesting U , it has to prepare a valid message C_i , $H(SEED||C_i) \oplus SK_i$ and $H(SK_i||p_{i-1})$. If E can obtain $SEED$, then he/she can impersonate S to cheat U . However, this is not feasible, as there is no way to derive the $SEED$ in order to compute $H(SEED||C_i)$, due to the one-way property of a secure one-way hash function. Therefore, E has no chance to login by launching an impersonation attack.

Theorem 5. *The proposed scheme can resist stolen-verifier attacks.*

Proof. Servers are always the target of attacks. E may try to steal or modify the account database stored in S . If the account database is stolen by E , E may masquerade as a legitimate U . If the account database is modified, a legitimate U cannot successfully login to S . This results in a Denial-of-Service attack. Considering the stolen-verifier attacks, E may steal the verifier p_{i-1} from S after the $(i-1)$ th login and intercept the communication between U and S . It is very difficult to derive the $SEED$ by p_{i-1} in the login stage, unless E can reverse the one-way hash function. Therefore, E cannot forge a valid login request message in the i th login. Furthermore, if S provides the login services for m users, S must store the m preshared value $SEED$ in his/her database. The probability that the $SEED$ is stolen is relatively high. The proposed scheme computes $SEED_t$ by $SEED_t = H(ID_t||x)$, where $1 \leq t \leq m$. S only needs to keep x in secret. Thus, the proposed scheme can withstand stolen-verifier attacks.

Theorem 6. *The proposed scheme can resist a Denial-of-Service attack.*

Proof. Unlike Lee-Chen's scheme, the proposed registration stage performs via a secure channel. Therefore, it can simply prevent Denial-of-Service attacks on the registration stage. In Step 3 of the proposed login stage, E can replace $p_i \oplus SK_i$ with forged $p_i \oplus SK_i \oplus X$ (or X), in which X is a random number chosen by

E. After receiving the replaced $p_i \oplus SK_i \oplus X$ (or X), *S* will extract $p_i \oplus X$ (or $X \oplus SK_i$) by computing $(p_i \oplus SK_i \oplus X_i) \oplus SK_i$ (or $X \oplus SK_i$). Then, $p_i \oplus X$ (or $X \oplus SK_i$) is hashed one time and is compared with $H(p_i)$. Since $p_i \oplus X$ (or $X \oplus SK_i$) is not equal to $H(p_i)$ and *E* cannot compute $H(p_i)$ without knowing *K* and the *SEED*, *E* cannot succeed in the Denial-of-Service attacks. Thus, the proposed scheme can withstand Denial-of-Service attacks.

Theorem 7. *The proposed scheme provides mutual authentication.*

Proof. The proposed scheme uses the random value D_i and T_i to provide mutual authentication. Then, the $SK_i = D_i || T_i$ is explicitly authenticated by mutual confirmation values $H(SK_i || p_{i-1})$ and $p_i \oplus SK_i$, respectively. Therefore, the proposed scheme provides mutual authentication.

Theorem 8. *The proposed scheme provides user anonymity.*

Proof. To ensure personal communication privacy, it is necessary to protect a *U*'s identity from passive attacks such as eavesdropping. Also, identity protection is particularly useful for the *U* to whom a dynamic IP address is allocated by the DHCP. In Step 1 of the proposed scheme, upon receiving an *ID* request from *S*, the *U* sends $H(ID || SEED)$ instead of its real identity *ID* to prevent passive attackers, such as eavesdroppers, from knowing *U*'s identity. By using *U*'s account database, however, *S* needs to be able to match the pseudonym of the *U* to its real identity *ID*. Therefore, the proposed scheme provides user anonymity.

5 Conclusion

The current paper demonstrated that Lee-Chen's scheme is still vulnerable to Denial-of-Service attacks and it also presented a simple solution to isolate such problems. Furthermore, we proposed an efficiently optimized one-time password authentication scheme that can provide user anonymity and the computational costs are less. In contrast with Lee-Chen's scheme, the proposed scheme is more secure but equally as efficient.

Acknowledgements

This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment).

References

1. Mitchell, C.J., Chen, L.: Comments on the S/KEY User Authentication Scheme. ACM Operating Systems Review. Vol. 30. No. 4. (1996) 12-16
2. Haller, N.M.: The S/KEY One-time Password System. RFC 1760. (Feb. 1995)

3. Haller, N.M.: A One-time Password System. RFC 1938. (May 1996)
4. Yeh, T.C., Shen, H.Y., Hwang, J.J.: A Secure One-time Password Authentication Scheme Using Smart Cards. IEICE Trans. Commun. Vol. E85-B. No. 11. (Nov. 2002) 2515-2518
5. Tsuji, T., Shimizu, A.: Cryptanalysis on One-time Password Authentication Schemes Using Counter Value. IEICE Trans. Commun. Vol. E87-B. No. 6. (June 2004) 2756-2759
6. Ku, W.C., Tsai, H.C., Tsauro, M.J.: Stolen-verifier Attack on An Efficient Smartcard-based One-time Password Authentication Scheme. IEICE Trans. Commun. Vol. E87-B. No. 8. (Aug. 2004) 2374-2376
7. Lee, N.Y., Chen, J.C.: Improvement of One-time Password Authentication Scheme Using Smart Cards. IEICE Trans. Commun. Vol. E88-B. No. 9. (Sep. 2005) 3765-3767
8. Menezes, A.J., Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptograph. CRC Press. New York. (1997)
9. Lin, C.L., Hwang, T.: A Password Authentication Scheme with Secure Password Updating. Computers & Security. Vol. 22. No.1. (Jan. 2003) 68-72
10. Yoon, E.J., Kim, W.H., Yoo, K.Y.: Robust and Simple Authentication Protocol for Secure Communication on the Web. LNCS. ICWE 2005. Vol. 3579. (2005) 352-362
11. Ku, W.C., Chen, S.M.: Weaknesses and Improvements of an Efficient Password based Remote User Authentication Scheme Using Smart Cards. IEEE Trans. on Consumer Electronics. Vol. 50. No. 1. (2004) 204-207

Loss Reduction in Distribution Networks Using Cyclic Best First Search

Sang-Yule Choi¹, Myong-Chul Shin², and Jae-Sang Cha³

¹ Dept. of Electronic Engineering, Induk Institute of Technology,
San 76 Wolgye-dong, Seoul, South Korea

² School of Electrical and Computer Engineering,
Sungkyunkwan University,
Suwon 440-746, South Korea

³ Dept. of Media Technology,
Seoul National University of Technology,
Seoul, South Korea
cha.js@snut.ac.kr

Abstract. Network reconfiguration in distribution systems is realized by changing the status of sectionalizing switches, and is usually done for loss reduction or load balancing in the system. This paper presents an effective heuristic based switching scheme to solve the distribution feeder loss reduction problem. The proposed algorithm consists of two parts. One is to set up a decision tree to represent the various switching operations available. Another is to apply a proposed technique called cyclic best first search. The proposed algorithm identifies the most effective the set of switch status configuration of distribution system for loss reduction. To demonstrate the validity of the proposed algorithm, numerical calculations are carried out the 32 bus system models

1 Introduction

Electric distribution networks maintain radial structure with normally closed sectionalizing switches along a feeder and normally open interfeeder tie switches for proper protection coordination. For every tie switch closed, another sectionalizing switch is opened. Under normal operating conditions, distribution feeders may be frequently reconfigured by changing the open/close state of each switch in order to reduce line losses or to avoid overloaded network branches. The resulting feeders must remain radial, without any violations of branches loading and voltage limits. Because of these requirements, the problem of finding network reconfiguration with minimum losses is a very complicated mixed-integer, non-linear optimization problem. Since there are a numerous number of switches in a practical distribution networks, a combinatorial analysis of switch options(2^m) could require prohibitively long computation time. Therefore, the problem appears to be best solved by heuristic search methods. Cinvalar et al[1] proposed heuristics and computationally effective formulas for the loss change due to a switch exchange operation. Single loop optimization algorithm for determining the minimum loss configuration was presented [2]. Baran et al[3]

developed approximate power flow method for loss reduction and load balancing based upon considering branch exchange type switch operations. And Heuristic based switching indices were designed by [4], where it utilizes fuzzy notations for the loss reduction of distribution systems. Taylor et al [5] proposed a switch exchange type heuristic method to determine the network configuration for overloads, voltage problem, and for load balancing simultaneously. Its solution scheme sets up a decision tree which represents the various switching operations available, and a best first tree searching and heuristic rules are used to find feasible switching operations. Wu et al[6] extended the method Taylor et al[5] by developing explicit exhaustive method that solves the problem of overloads, phase current unbalance, service-restoration, and maintenance. This method taken is to set up a feasible switching options tree which represents possible switching options under constraint of radial structure. Evaluation functions and heuristic rules are used to find feasible switching options.

In this paper, the authors present a heuristic feeder reconfiguration algorithm based on an effective exhaustive search method. Its main steps have been implemented in two stages. First stage is to set up a sub-tree that was presented by Wu et al[6] Second stage is to find feasible switching operations with a proposed new search technique called cyclic best-first search. This procedure favors solutions with a fewer number of switching operations where the switching sequences may be acceptable to the operators. Numerical calculations are carried out to show the effectiveness of the proposed algorithm.

2 Solution Algorithm

A feasible switching options tree was suggested in [6] in order to decrease searching space, and is called sub-tree in this paper. To find reasonable switching options effectively, the authors developed a cyclic best-first tree searching strategy. The whole solution procedure as follows.

2.1 Constructing the Sub-tree

Sub-tree is a decision tree to represent the various switching options available under constraint of radial structure. Constructing the sub-tree methodology is the same that in the paper by Wu et al [6] in that a tree is adopted in order to decrease searching space. Under the constraint of the radial structure in the load transfer process, closing a normally open tie switch should follow the opening of a complementary normally closed sectionalizing switch. Therefore, If n tie switches are closed, then n sectionalizing switches has to be opened.

Fig. 1 shows a sample distribution network[3] consisting of three feeders with three normally opened tie switches and thirteen normally closed sectionalizing switches.

If feeder 2 experiencing an overload, then the amount of overload on feeder 2 must be transferred to feeder 1 and/or 3 without creating an overload on either of these feeders. To transfer load at node 11 from feeder 2 to feeder 1, the notation (T_1, S_4) is used to denote the operation of closing switch T_1 and opening switch S_4 , henceforth.

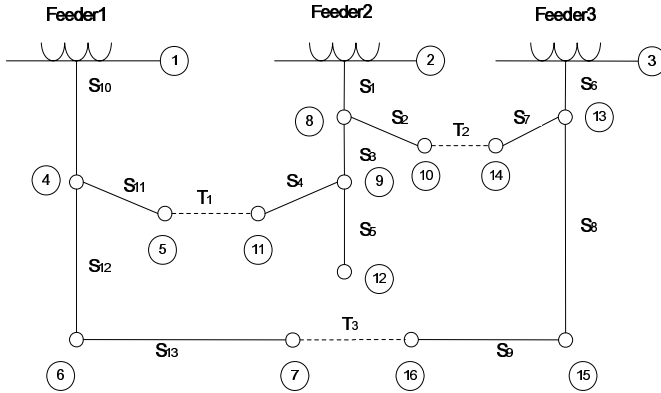


Fig. 1. Three-feeder example system

Feasible (close,open) switching options can be found by searching sectionalizing switches through the overloaded feeder.: When each tie switch of the overloaded feeder is closed, a complementary sectionalizing switch to be opened is found by searching from the tie switch, and moving upstream along the overloaded feeder to its source, the circuit breaker of the overloaded feeder.

Fig. 2 shows a searching path for finding feasible switching options when feeder 2 is overloaded.

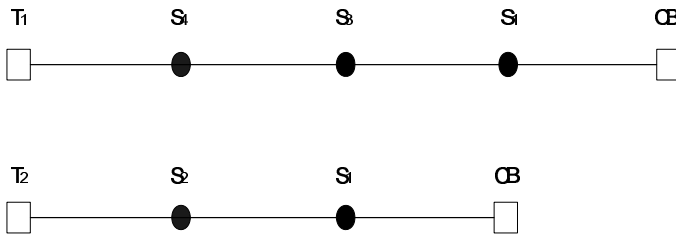


Fig. 2. Main search paths for example system

If the amount of overload on feeder 2 be transferred to only feeder 1, then T₁ and either S₄, S₃ or S₁ constitute a switching pair. So feasible switching options are expressed as {(T₁,S₄), (T₁,S₃), (T₁,S₁)}. And one of switching options would be a solution for relieving the overload.

Similarly, the amount of overload on feeder 2 may be transferred to feeder 1 and 3 simultaneously by choosing one of following feasible switching options {(T₁,S₄), (T₂,S₂)}, {(T₁,S₄), (T₂,S₁)}, {(T₁,S₃), (T₂,S₂)}, {(T₁,S₃), (T₂,S₁)}, {(T₁,S₃), (T₂,S₂)}. But when T₁ and T₂ are used simultaneously, the switching option {(T₁,S₁), (T₂,S₁)} is not a feasible one. Because it violates radial structure constraint.

If the results of these feasible options are examined, then the corresponding sub-tree of fig. 3 is obtained.

In fig.3, both T_1 and T_2 are tie switches of the overload feeder 2 and dotted line represents switching option.pairs.

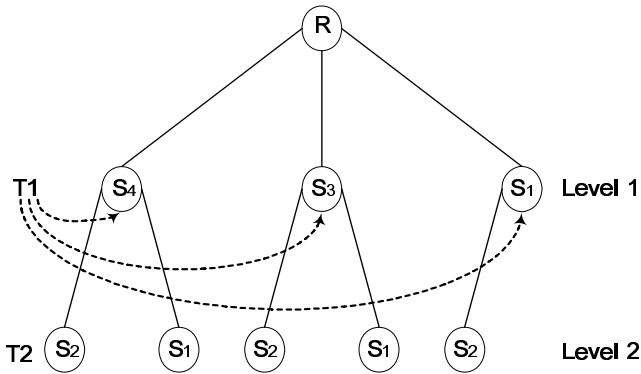


Fig. 3. Sub tree with two backup feeders

2.2 Cyclic Best-First Search

The advantage of the best-first search usually, but not always, yields solution faster than any other heuristic search. But the problem is that it does not always give the optimal solution: unexplored path would have given an optimal solution. In this paper, the new methodology (so called cyclic best-first search) is presented. This methodology is based on best-first search. But, by using cyclic methodology, it can usually find more accurate solution than best-first search technique. In best-first search, node at each level in the above sub-tree is chosen for switching option with the most potential to lead to a loss minimization. Then that node is expended into its children nodes. Similarly, one of its children nodes is chosen for switching option with minimum loss. This procedure is continued until it finds a goal node.

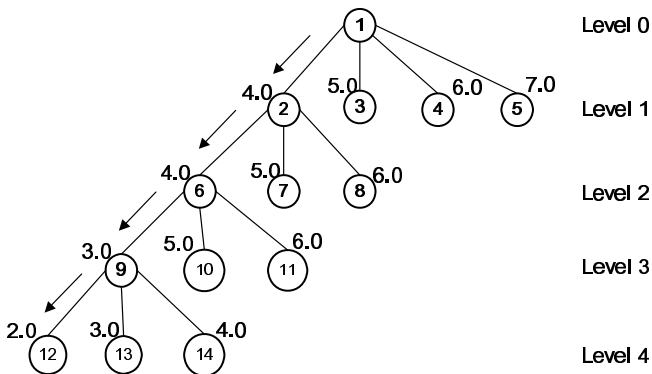


Fig. 4. First Step of best-first search

In the end, nodes {①,②,⑥,⑨,⑫} are found by best-first search. And these nodes may be a solution switching pair set to minimize line losses. By always expanding the most likely node, it is possible to get to a goal node or a solution quickly. But this procedure achieves the trade-off between optimality and computational speed. In cyclic best-first search, it gives circulatory function for best-first search to find more proper switching pair set in the sub-tree. With circulatory reevaluating the unexplored nodes and path, an effective solution with minimum switching operations would be found. Although the search space of cyclic best-first search is slightly larger than that of best-first search, the computation difference is negligible. The cyclic best-first search process is as follows:

First step) A path from a start node to a goal node is selected by using best-first search.

In fig 4, a selected path is ①→②→⑥→⑨→⑫, a start node is ① and a goal node is ⑫. However, this path is usually (not always) not an optimal solution: Selected node ⑥ seems to be an optimal switching pair in level-2 on condition that nodes in lower level are not selected. But it is hard to say that node ⑥ is a optimal switching pair if nodes in lower level are selected by expansion Therefore, different(or more accurate) path and nodes may be found under different lower level conditions.

Second step) Constructing the reversed sub-tree. And a new path is selected by using best-first search.

Reversed sub-tree can be constructed by reversing the level of sub-tree that was used in first step: The level-4 of the sub-tree in first step becomes the level-0 of the reversed sub-tree, and the level-3 of the sub-tree in first step becomes the level-1 of the reversed sub-tree. Similarly, the levels of sub-tree in first step can define the rest levels of the reversed sub-tree. Therefore, a goal node in first step becomes the start node of the reversed sub-tree in second step. Fig. 5 shows second step of best-first search to find near-optimal path in a reversed sub-tree.

In second step of best-first search, when nodes in each level are evaluated, it is assumed that nodes in the other lower levels are already chosen by first step of best-first search. therefore, node ⑨ is chosen assuming that nodes ⑥,②,① are already

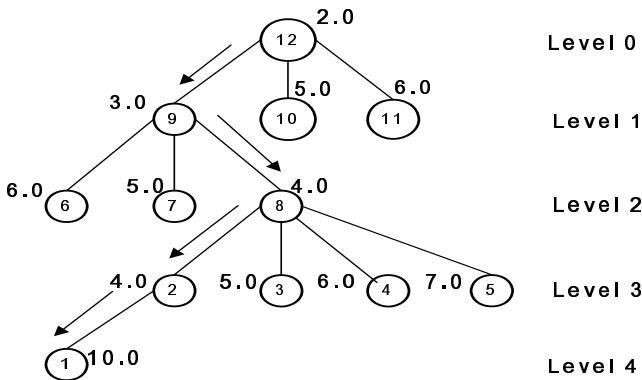


Fig. 5. Second step of best-first search

determined from first step. Similarly, Node ⑧ in level-2 is selected assuming that nodes ② ① are already determined from first step. This gradient measurement can determine nodes that appear to be closest to an optimal solution. Due to using near-optimal path from first step, new path from second step is more near-optimal solution than that from first step. After second step of best first search, a new path ⑫→⑨→⑧→②→① is selected. Comparing a new selected path with a previously selected path , a selected node ⑥ is changed into a node ⑧ from second step because of the other levels condition : In first step, the node ⑥ in level-2 is selected on condition that node ⑨ in level-3 and node ⑫ in level-4 are not selected by expansion. In second step, node ⑧ is choosing instead of node ⑥ on condition that node ⑫ in level-0 and node ⑨ in level-1 are already selected by expansion before evaluating nodes in level-2, and it is assumed that nodes ②,① are already determined from first step. Because two paths are different, more improved solution may be found if the way of second step is repeated to the next step.

Third step) Repeat the way of second step, until a newly selected path and a previously selected path are compared as the same. In third step, reversed sub-tree can be constructed by reversing the level of sub-tree that was used in second step. And the third step of best-first search is shown in fig.6.

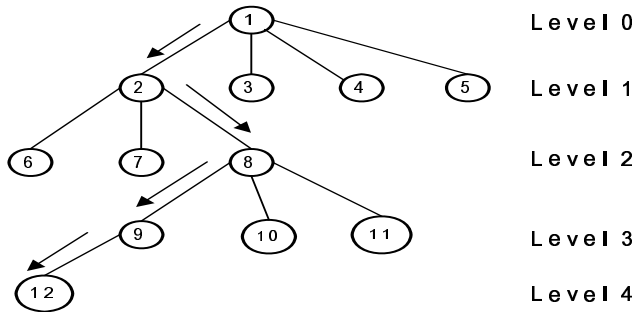


Fig. 6. Third step of best-first search

New path is ①→②→⑧→⑨→⑫. This path and the path chosen in second step are compared as the same. Therefore this path is appears to be a proper solution.

Fourth step) Terminate the iterative procedure, and nodes of newly selected path are converted to the complete switching pairs.

3 Result

The distribution network for reconfiguration presented in M.E Baran, 1898 is used to demonstrate the validity and effectiveness of the proposed algorithm. The network consisting of two feeders with 32 busbars and 5 tie switches {T₃₃, T₃₄,T₃₅, T₃₆, T₃₇}, as shown in Fig.7. The total load are 5084.26[kw], 2457.32[kvar], and initial losses

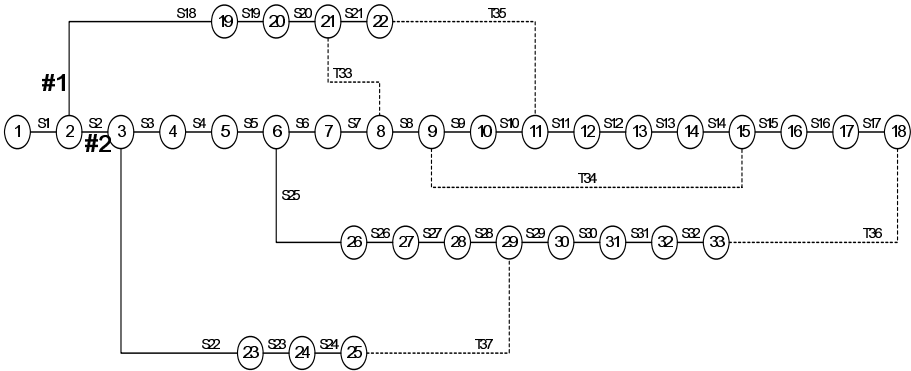


Fig. 7. Sample of distribution system with 32 bus

is 0.0203 p.u Table 1 shows initial feeder loadings and voltage difference across normally closed tie switches.

First step of best-first search for initial sub-tree is shown in fig.8. Initial sub-tree level is defined by T35, T37, T33, T34, T36 sequentially due to the different voltage across.

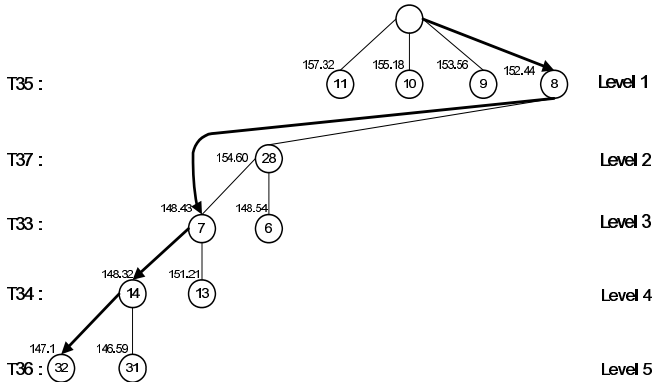


Fig. 8. First step of best-first search for 32 bus loss minimization

In Fig. 8, an selected (close,open)switching pair for level 1 is (T35,S8) and system losses are 152.44[kw] for the switching operation.

After first step of best-first search, selected (close, open) switching operations are (T35,8), (T33,7), (T34,14),(T36,32). This solution seems feasible but it is only locally optimal, because the first step of best-first search dose not examines all the possible nodes. It is possible that unexplored path would have presented more feasible solution. Thus, to find more feasible solution, reversed sub-tree is constructed by reversing the level of sub-tree that was used in first step and second step of best-first search is executed in fig. 9.

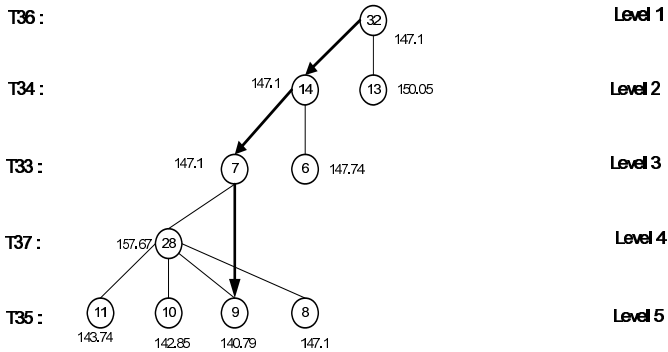


Fig. 9. Second step of best-first search for 32 bus loss minimization

In fig. 9, first checked node (T37, 28) in level 4 would increase system losses, therefore the rest of unchecked nodes in level 4 are ignored and searching is proceeded to level 5. After second step of best first search, switch pairs (T35,9), (T33,7), (T34,14), (T36,32) are selected to minimize system losses. Comparing new switch pairs with those of first step of best-first search, switch pair (T35,8) is changed into (T35,9). The reason why newly selected switch pairs are different from those of previously selected is that selected switch pair (T35,8) is operated before evaluating switching pairs of lower levels in first step of best-first search. Third step of best-first search is proceeded in order to find more improved solution in fig 10.

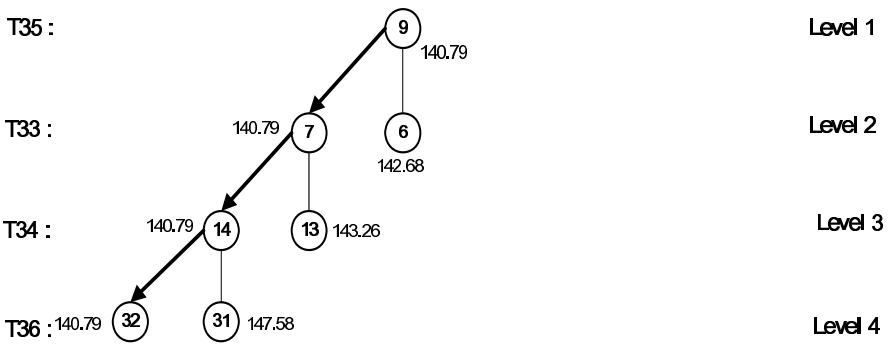


Fig. 10. Third step of best-first search for 32 bus loss minimization

As seen above fig. [8, 9], close/open switch options using T37 are always increase system losses. At third step of best-first search, tie switch T37 is excluded from reversed sub tree to avoid unnecessary search. Selected switch pairs (T36,32), (T34,14), (T33,7), (T35,9) are the same that those of second step. It is indicate that the solution obtained from third step would be the complete solution in the sense that the further search would be the same After selected switching operations, the percentage of total loss reduction is 31[%].

4 Effectiveness Comparison

The three methods proposed by Goswami[7], the three methods proposed by Baran[3] and the method by W-M.Lin[9] had used the same test system as shown in figure 7. Therefore, The effectiveness of proposed method was compared with these methods in table 1.

Table 1. Summary of test results

Methods	Switching times	Initial open switches	Last Open Switches	Total loss reductions [%]
Goswami [7]	M1	7	7, 9, 14, 32, 37	31.148
	M2	7		31.148
	M3	4		31.148
Baran Et al [3]	M1	5	11, 28, 31 ,33, 34	27.830
	M2	3	6, 11, 31 ,34, 37	23.826
	M3	3	33, 34, 35, 36,	23.826
W-M Lin Et al[9]	5	37	7, 9, 14, 32, 37	31.148
Proposed method	5		7, 9, 14, 32, 37	31.148

Proposed method needs fewer switching times than Gowami[7][M1,M2] and it is more effective than Baran[3] for loss reduction . Goswami[7] [M1]and W-M Lin[9] methods need more complicate numerical computation than proposed method.

5 Conclusion

A new heuristic algorithm has been presented in this paper for loss minimization of distribution networks. The proposed algorithm adopts the concept of sub-tree proposed by J.S Wu, 1991 and utilizes cyclic best-first search method developed by the authors. Cyclic best-first search is derived from best-first search, which gets a solution much faster even if it lies deep down in the tree. And it compensates best-first search for not obtaining the best solution every time by using reverred sub tree. For a feeder reconfiguration algorithm, it is sufficient to know the relative change in the line loss due to close/open switching operations. And absolute accuracy is not essential. Therefore, proposed algorithm is suitable for such applications even though it may not guarantees the optimal solution.

Acknowledgment

The research was supported by the Driving Force Project for the Next Generation of Gyeonggi Provincial Government in Republic of Korea.

References

1. S. Cinavanlar, J. J. Grainger, H. Yin, S. S. H. Lee : Distribution feeder reconfiguration for losses reduction. IEEE Trans. on Power Delivery, Vol. PWRD-3 (1988) 1217-1223
2. J-Y, Fan, L. Zhang, J.D. McDonald : Distribution Network Reconfiguration Single Loop Optimization. IEEE Trans, Power Systems, Vol. 10, No. 3, August (1996) 1643-1647
3. M. E. Baran, F. F. Wu : Network reconfiguration in distribution systems for loss reduction and load balancing. IEEE Trans. on Power Delivery, Vol. PWRD-4, 1989, April (1989) 1401-1407
4. W. M. Lin et al : An effective algorithm for distribution feeder loss reduction by switching operations. IEEE Trans on Power Delivery (1999) 597 - 602
5. T. Taylor, D. Lubkeman : Implementation of heuristic search strategies for distribution feeder reconfiguration. IEEE Trans. on Power Delivery, Vol. 5, No. 1 (1990) 239 - 246
6. J. S. Wu. K. L. Tomsovic, C. S. Chen : A heuristic search approach to feeder switching operations for overload, fault, unbalanced flow and maintenance. IEEE Trans. on Power Delivery, Vol. 6, No. 4, October (1991) 1579 - 1585
7. S. K. Goswami, S. K. Basu : A new algorithm for the reconfiguration of distribution feeders for loss minimization. IEEE Trans. on Power Delivery, Vol. 7, No. 3, July (1992) 1484-1491
8. D. Shirmohammandi, H.W. Hong : Reconfiguration of electrical distribution networks for resistive line losses reduction. IEEE Trans. On Power Delivery, 1989, Vol. 4, NO.2 (1989)
9. W-M.Lin : Distribution feeder reconfiguration with refined genetic lgorithm. IEE Proc-Gener. Transm.Distrib, Vol. 147, No.6, November (2000)

Short-Term Power Demand Forecasting Using Information Technology Based Data Mining Method

Sang-Yule Choi

Dept.of Electronic Engineering , Induk Institute of Technology,
San 76 Wolgye-dong, Seoul, South Korea
ppk99@induk.ac.kr

Abstract. This paper proposes information technology based data mining to forecast short term power demand. A time-series analyses have been applied to power demand forecasting, but this method needs not only heavy computational calculation but also large amount of coefficient data. Therefore, it is hard to analyze data in fast way. To overcome time consuming process, the author take advantage of universally easily available information technology based data-mining technique to analyze patterns of days and special days(holidays, etc.). This technique consists of two steps, one is constructing decision tree, the other is estimating and forecasting power flow using decision tree analysis. To validate the efficiency, the author compares the estimated demand with real demand from the Korea Power Exchange.

1 Introduction

Normally main method used in the field of power demand forecasting is time-series analyses.

Time-series analyses can cover very complicated process but it is difficult for crew to use even if he has been working many years.

Under deregulation of power system, five GENCO (Generation corporation) has been detached from Korean Electric Power Corporation and small scale co-generation corporation has been founded. All detached company and small co-generation company need power demand forecasting estimation. But few GENCO has power demand forecasting estimation because price of power demand forecasting estimator is high and hard to handle for small company.

The small companies usually depend on Korea Power Exchange to forecast the power demand. But, under deregulation, it is necessary for all GENCO to forecast power demand themselves and bid power according to power demand which is estimated by company itself.

The existing power demand forecasting method needs huge amount of database and uses time consuming time-series analyses, that makes small generation company hard to have that kind of software. Especially, under deregulation, price based power are needed to bid power demand, which makes small company more difficult to forecast the power demand. To overcome time consuming process, the author take advantage of universally easily available information technology based data-mining technique to analyze patterns of days and special days(holidays, etc.). This technique consists of

two steps, one is constructing decision tree, the other is estimating and forecasting power flow using decision tree analysis. To validate the efficiency, the author compares the estimated demand with real demand from the Korea Power Exchange.

2 Power Load Forecasting Techniques

You are strongly encouraged to use LaTeX2e for the preparation of your camera-ready manuscript together with the corresponding Springer class file lncs.cls; see Sect. 3. Only if you use LaTeX2e can hyperlinks be generated in the online version of your manuscript.

If you are unable to use LaTeX, you may use MS Word together with the template sv-lncs.dot (see Sect. 4) or any other text processing system. In the latter case, please follow these instructions closely in order to make the volume look as uniform as possible.

We would like to stress that the class/style files and the template should not be manipulated and that the guidelines regarding font sizes and format should be adhered to. This is to ensure that the end product is as homogeneous as possible.

2.1 ARIMA (Autoregressive Integrated Moving Average) Model

An ARIMA(Autoregressive Moving Average) is the model which time series analysis is differentiated.

That is, if time series analysis follows ARMA model as in Equation (1), it can be considered to be derived from ARIMA model [1].

$$W_t = \delta + \phi_1 W_{t-1} + \dots + \phi_p W_{t-p} + \theta_1 e_{t-1} + \dots + \theta_q e_{t-q} + e_t \quad (1)$$

The method uses statistics program SAS or ETS and has a complicated process including analysis of white noise, so it is hard for non-experts to use.

2.2 Exponential Smoothing

This method is most widely used at electric power companies. It provides stable results in weekday short-term forecasting without a special or irregularly changing variable like temperature.

A forecasted power demand F at t o'clock on day d can be expressed as Equation (2) using time series X of the past records [3].

$$F_{(dt+1)} = aX_{(d,t)} + (1+a)F_{(d,t)} \quad (2)$$

Although this method is stable in short-term forecasting and hard for non-experts, it has a large error range when there is a special and irregularly changing variable like temperature.

2.3 Neural Network

This method creates learning patterns using the maximum demand and weather data by local situation, and learns using back propagation (BP).

2.4 Knowledge Based

This model can be utilized in forecasting demand on special days. It analyzes the characteristics of demand on special days in the past, derives if-then rules from the characteristics, and uses Then Obj operator [3].

2.5 KULF(KPX-SNU Load Forecaster)

This is a demand forecasting method used in KPX. It is focused on the seasonality of time series and forecasts by analyzing the pattern of each season

The seasonality of power time series is caused by air-conditioning load and heating load, so it is basically determined by temperature

Thus, it estimates temperature distribution function at time point t by introducing the concept of temperature reaction function, and obtains temperature effect at time point t by integrating the temperature distribution function with the temperature reaction function (Equation 3).

$$\int g(s)f(s)ds \quad (3)$$

Here, temperature reaction function measures the change of electric power demand in portion to temperature, namely, the sensitivity of electric power demand concerning to temperature and reduces the error range [2].

This method has a narrow error range, but it has an extremely complicated process, so it is hard for non-experts.

3 The Method of Data Mining

A data mining is a technique which searches data among huge database and acquires necessary information through search algorithm.

The most commonly used method is KDD(Knowledge Discovery in database).

3.1 Procedure of Knowledge Discovery in Data-Mining

The procedure of Knowledge Discovery in data-mining is that the following processes are repeated until acquiring expecting knowledge.

- ① Data Cleaning : Cleaning of unnecessary or disagreement data
- ② Data Integration : Integration of much data source
- ③ Data Selection : Searching necessary data from database
- ④ Data Transformation : Using data to find suitable formation for mining by performing operation such as a summary and a total
- ⑤ Data Mining : Essential process which intelligent processes are applied to put outdata pattern
- ⑦ Data Evaluation : Evaluating pattern which knowledge shows based on several interesting standard
- ⑧ Data Presentation : Using visualization and a knowledge which express method to show fined knowledge for the user.

3.2 Association Rules

An association-rules mining is to find out necessary data among far-reaching data and common characteristics or connected relation which the data has, that is, the Association-Rules mining is presented to intersection in set. The process which finds out association-rules in a large scale database is presented to a process of following two steps.

- ① Every frequent Item set search : Every Item set according to definition generates frequently over a smallest popularity determined in advance
- ② Strong Association-Rule in frequent item set : these regulations is defined to satisfy a smallest popularity and a smallest reliability.

3.3 Decision Tree

The decision tree is a tree structure which similar to flow chart, In this tree, marks represent characteristics in intermediate node, and a branch shows results of the test. Also, leaf node presents class or distribution of class.

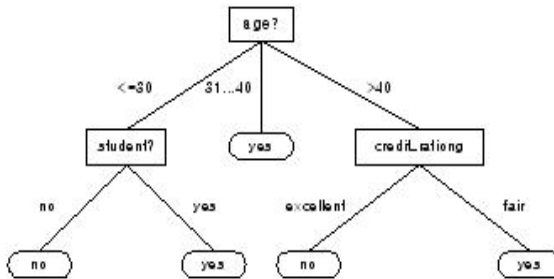


Fig. 1. Decision tree example

Fig. 1 shows predictive decision-making tree whether a customer purchases a computer or not, and intermediate node and leaf node is expressed as a square and an ellipsoid, respectively

4 Association-Rules Application of Data Mining

4.1 Comparison of Daily Load Pattern

If Korea's demand pattern is divided, it can be classified weekday, Saturday, holiday and special day.

At first, data is classified according to comparison between Power demand patterns for one week.

Load demand for one week on January in 2001, is presented as fig.2.

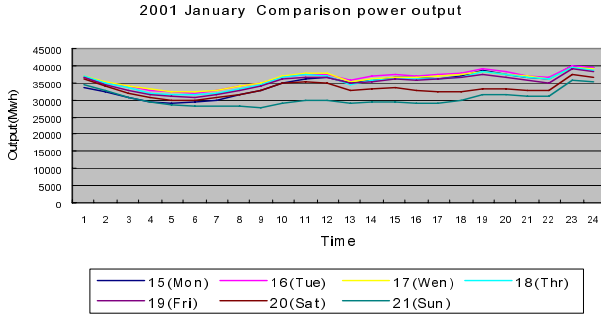


Fig. 2. 2001 January Comparison power output

Fig. 2 shows weekday’s load demand pattern is almost similar, but Saturday and Sunday’s demand pattern is different.

Therefore, in case of refining, unifying, or selecting data for load demand forecasting, it is necessary to classify weekday, Saturday and Sunday differently.

4.2 Demand Pattern Comparison by a Season

Load pattern is different every season because Korea has four seasons in a year.

Thus, the standard which classifies four seasons is normally divided as follows

- March ~ May : spring,
- June ~ August : summer,
- September ~ November : fall,
- December ~ Next year’s February : winter.

2001 Comparison power output by season

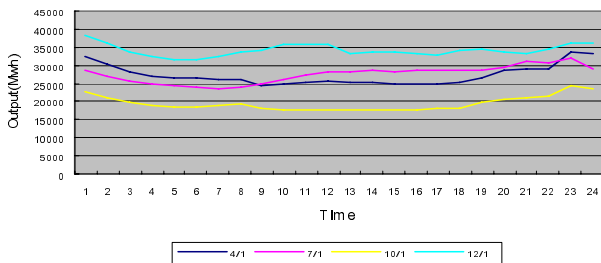


Fig. 3. Comparison between power outputs by season

Fig. 3 shows four season’s power outputs. This figure shows that the pattern from 00:00 to 08:00 is similar, but the demand pattern after 08:00 and from 23:00 to 00:00 is different by each season. It also shows that the demand pattern of April(spring) and October(summer) is similar. Therefore, it is considered that spring and fall is almost one pattern.

4.3 Comparison of Weekends and Special Days

The pattern of special days like Saturday and Sunday is different as shown fig. 2. In this paper, it will be omitted comparison between the demand pattern of Saturday and Sunday and compare the demand pattern of Sunday and special days like New Years Day, Thanks giving day consecutive holidays.

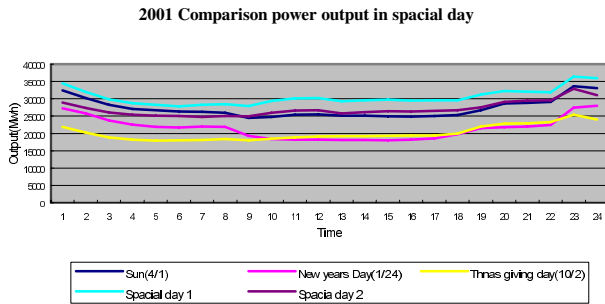


Fig. 4. Comparison power output in special day

Fig. 4 it shows Sunday's demand pattern is similar to usual holiday's and the pattern of New Years Day is similar to Thanks giving day. Therefore, the holiday's pattern is classified as Sunday, holiday and New Years Day, Thanks giving day's.

4.4 Comparison Between Pattern of Changes in Demand Owing to Temperature

The one of influencing factors in demand forecasting is weather. In particular, load is very fluctuant by the change of temperature. Although load demand is affected by cloudy, rainy or clean, In this paper, it is assumed that the weather is fine. Because temperature is considered to be a more important factor than weather condition.

4.5 Relationship Between Price and Load Demand

Korea is currently under deregulation. Thus, the relationship between price and demand for power is become important. However, the price of electricity is not dependant on the principle of market economy but dependant on KPX system marginal price per hour.

In power transaction, electric power companies will generate more power if the system marginal price is high. The optimal price will be set by demand and supply. Thus, price will be recognized as an important factor in estimating the load.

4.6 Application Decision Tree of Data-Mining

A decision tree is for making decisions, but In this paper it is not used not for making decisions but for data collection and operational relations.

Decision trees in data mining is as in Fig 5.

Fig 5 is expressed as follows

- ① Now Season: Divide into three parts - spring/autumn, summer and winter. Using correlation analysis to select the corresponding results
- ② Now Day: Divide into four parts - weekdays, Saturday, holidays and special days and select the corresponding results
- ③ Date: In case of weekdays, select the corresponding day among 1~30 (31)
- ④ Now Hour: Select the current hour
- ⑤ Data collection: Collect data such as power consumption, temperature and system marginal price
- ⑥ Calculation of forecasted values: calculate collection data using the time-series smooth method and forecasting factors
- ⑦ Forecasting factor: Apply the increase/decrease rate of the average power consumption for the latest three years
- ⑧ Forecasted: Calculate the forecasted value of short-term demand for electricity.

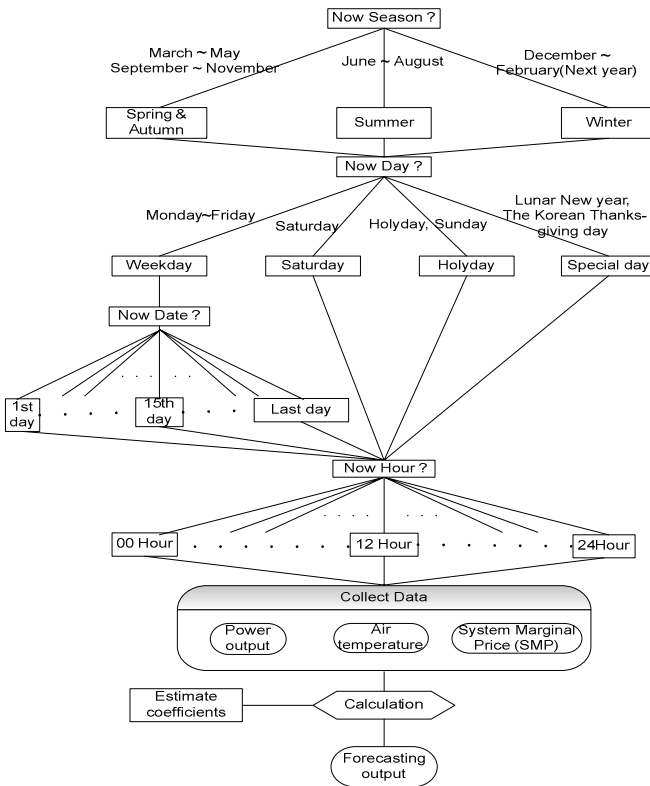


Fig. 5. Forecasted demands using the smoothing method in operational relations

4.7 Test Results

To validate proposed method, 2004 years real data is used. And Test result is compared with KPX load demand.

Table1. Comparison 2004-1.14 (Normal day) Demand forecasting.

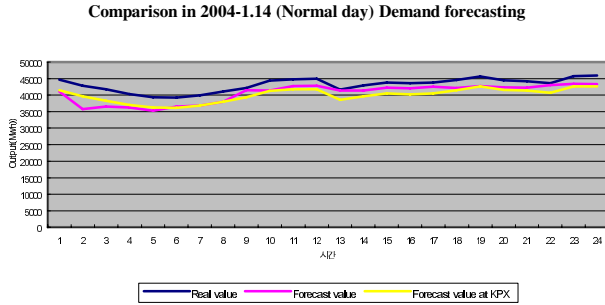


Fig. 6. Comparison between normal days demand forecasting

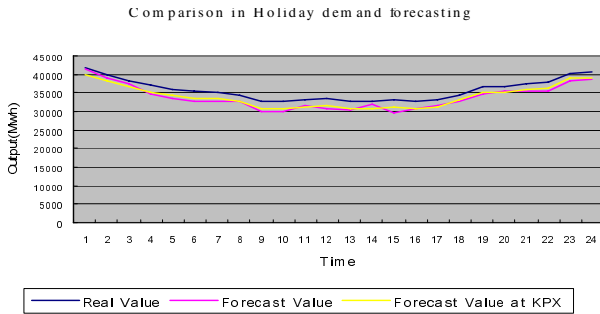


Fig. 7. Comparison between holidays demand forecasting

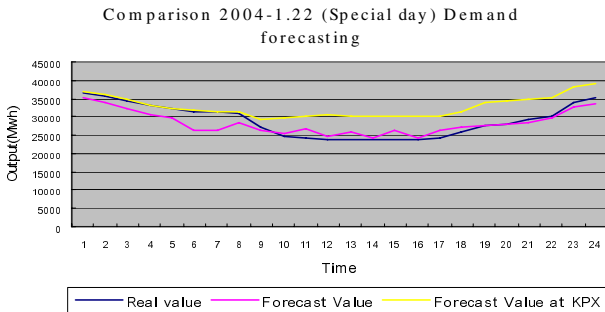


Fig. 8. Comparison between special days demand forecasting

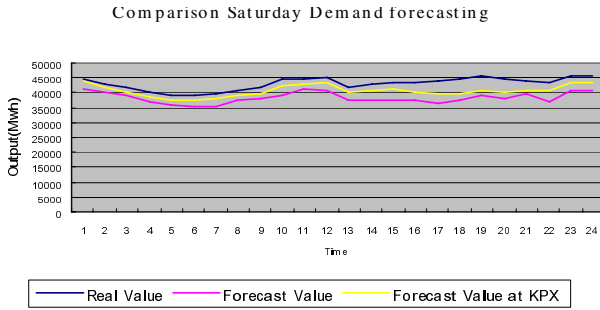


Fig. 9. Comparison between saturday demand forecasting

5 Conclusion

In this paper, the author take advantage of universally easily available information technology based data-mining technique to analyze patterns of days and special days(holidays etc.) and conclusion can be expressed as follows

- Forecasting for weekdays and the weekend were similar to those of KPX but large errors were observed in estimation for early morning. In case of special days, the results were superior to those of KPX but large error range was shown in estimation for Saturday.
- The average daily error was satisfactory but if is reserved by hour, it appeared difficult to forecast loads for early morning during significantly changing variables.
- The variation of errors shows that the reliability of data and forecasting factors are quite important.
- By using data mining, it is easy to obtain and define data to information through huge database.

Acknowledgment

The research was supported by the Driving Force Project for the Next Generation of Gyeonggi Provincial Government in Republic of Korea.

References

1. Shin-seop Cho, Sun-young Hwang, Geng-hee Lee: Time series analysis. Korea National Open University press (2001)
2. KPX-SNU Load Forecaster: Korea power exchanger(KPX). Seoul National University. December. (2002)
3. Kab-Ju Hwang, Kwang-Ho Kim, Sung-Hak Kim : Development of a Weekly Load Forecasting Expert System. KIEE press. vol.48A no 4. April(1999) 365~370
4. Jiawei Han: Data Mining : Concepts and Techniques. Elsevier(Singapore) Pte. Ltd(2000)

A Design of the Flexible Mobile Agents Based on Web

Yun Ji Na¹, Il Seok Ko², and Gun Heui Han³

¹ Department of Internet Software,
Honam University 59-1, Seobong-Dong,
Gwangsan-Gu, Gwangju 506-741, South Korea
yjna@honam.ac.kr

² Department of E-Commerce,
Chungbuk Provincial University of Science & Technology,
40 Gungu-ri, Okchon-gun, Chungbuk 373-807, South Korea
isko@ctech.ac.kr

³ School of Information Communication,
Cheonan University, 115 Anseo-dong,
Cheonan, 330-704, S. Korea
hankh@cheonan.ac.kr

Abstract. The key features of mobile agent systems are mobility, autonomy, and intelligence. On integrity protection within mobile agent technology, mobile agent integrity should be protected against attacks from malicious hosts and other agents. In this paper, we design flexible Mobile Agents (FMA). The traditional mobile agents consist of fixed code parts. But FMA consist of flexibly upgradeable agent code part for that new agent code modules can be added and redundant code modules can be deleted on the executing requirement. FMA prove to be more flexible in agent-based web systems compared to the traditional static-type mobile agent.

Keywords: Mobile Agent, Intelligent Agent, Security, Flexibility.

1 Introduction

An agent is a computer program can assist users' conduct by performing intelligent tasks [8, 13, 15]. Mobile agents have been proposed in many agent-based web systems and architectures such as information gathering, comparison-shopping [4,5], and agent-based payment systems [6], etc. From the agent user's perspective, mobile agents serve as personal software assistants. And intelligent agent is software that achieve various works that user must achieve directly instead of. Work that user wants needs complex process sometimes or process one task simply. Therefore, intelligent agent needs plan function to understand work that user requires and achieve this effectively and structure that a several agent solves problem by cooperation is required to achieve complicated work efficiently. Intelligent agent can establish and realize planning that can satisfy user's requirements effectively by cooperating multiplex agent each other. It can be embodied by method that agent in electronic commerce system is various according to each function special quality, In implementation, openness and mutual operation, and proper correspondence about

change must be considered. Intelligent agent does information gathering, data processing, knowledge abstraction, decision-making, decision-making achievement and reasoning, for state grasping of relevant condition and is divided to watching, learning, shopping, information abstraction agent according to the function that perform. Many researchers also have developed an electronic commerce framework using multi-agent technologies [7, 8, 9]. BargainFinder and Kasbah are examples for these electronic commerce systems. BargainFinder provides valuable information for the buyers through price comparison in online store. Kasbah is the marketplace architecture for buying and selling goods [9]. And the mobility, autonomy, and intelligence of mobile agents will bring in the flexible and smart e-commerce field. In agent-mediated web systems, security is the one of the important issue.

In this paper, we design Flexible Mobile Agents (FMA). The traditional mobile agents consist of fixed code parts. But FMA consist of flexibly upgradeable agent code part for that new agent code modules can be added and redundant code modules can be deleted on the executing requirement. FMA prove to be more flexible in web-based systems compared to the traditional static type.

A FMA is an agent whose code can be flexibly revised (addition and deletion). FMA agent function modules can be dynamically upgraded adding the new code to the existing agent code form the agent body. Each function module should include the function code and also the proper digital certificate regarding from which this code is fabricated, namely, the source agent factory as a proof of its validity. Addition of any particular code modules should get authorization from the proper parties. And FMA agent function modules can be dynamically upgraded deleting particular code to the existing agent code from the agent body. Deletion of function modules should also get authorization from the proper parties. The proposed method will reduce the size of agents and offer flexibility of mobile agents, enhance security of agent code.

2 Related Works

Because code parts are verified using the traditional cryptographic methods, code integrity is treated in a simple way. For the flexibly changeable data part, various approaches have been developed such as Multiple Hops (MH) [11]. Mobile agents use detection and prevention technique in order to protection of attacks from malicious hosts and agents [10].

- Detection: The goal of detection is detecting any malicious attack. This can be helpful to remedial procedures after attacks have been identified. Most detection schemes focus on dynamically changeable agent data or state.

- Prevention: The goal of prevention is preventing the compromise of mobile agents in a specific way. Prevention schemes focus on make impossible any modification to the code part.

Basically, code cannot be prevented from modification since it is executing on an external computing environment. There are two approaches to prevent code modification: hardware-based approaches and software-based approaches.

- Hardware-based approaches: We can prevent code modification employing tamper-resistant hardware to execute agents in a physically sealed environment. But these devices are relatively expensive.

- Software-based approaches: A black box security mechanism [12] proposes to create a black box out of an original agent. A black box is an agent that performs the same work as the original agent, yet with a different structure. Function hiding [13] is a software protection scheme applied to protecting mobile agents against malicious hosts. This approach hides important functions to hosts and makes real functions in the original code illegible. However, this has only been applied to specific cases for rational and polynomial functions.

SAFER (Secure Agent Fabrication, Evolution and Roaming) [14, 15, 16] provides an infrastructure for intelligent agent-mediated electronic commerce. The goal of SAFER is to construct a secure, standard, and evolutionary agent system for electronic commerce based applications and transactions. Figure 1 shows SAFER mobile agent community.

Each SAFER community is composed of various components and entities, such as the agent butler, clearing house, bank, agent factory, community administration center, agent Charger. The agent butler represented the agent owner for operating various mobile agents. The agent factory is responsible for fabricating mobile agents and other related code modules. Codes provided by the agent factory should bear the original signature of the factory to provide a means to verify the authenticity of the agent code.

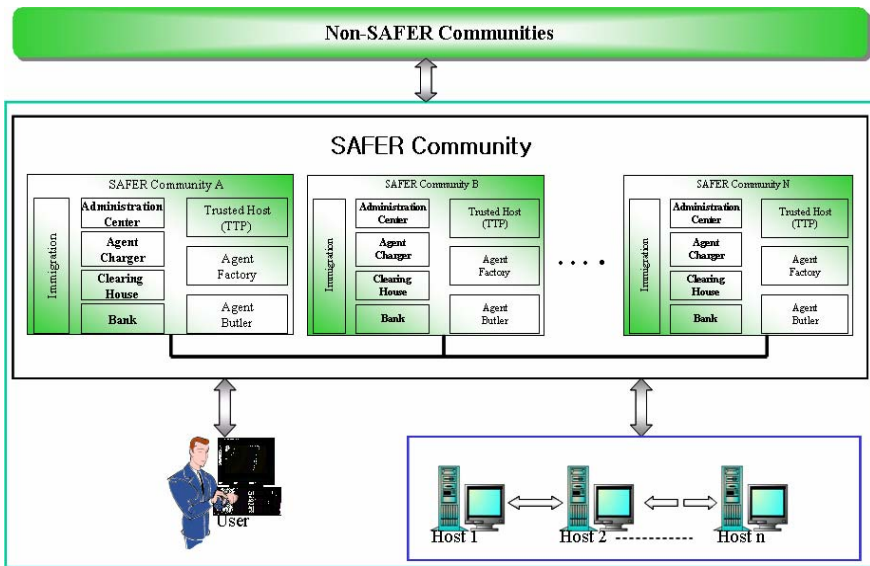


Fig. 1. Structure of SAFER Mobile Agent Community

3 FMA

A FMA (Flexible Mobile Agent) is flexibly revised (addition and deletion) as below.

- Addition: Agent function modules can be dynamically upgraded adding the new code to the existing agent code form the agent body. Each function module should include the function code and also the proper digital certificate regarding from which this code is fabricated, namely, the source agent factory as a proof of its validity.
- Deletion: Agent function modules can be dynamically upgraded deleting particular code to the existing agent code from the agent body.

In cases of addition and deletion on any particular code form function modules should get authorization from the proper parties

3.1 Structure of FMA

Figure 2 shows the structure of FMA. FMA consist of components of the agent factory, agent butler because FMA based on the SAFER. TTP and a few network hosts the agent is to visit. A user may download the agent program from the factory and dispatch it to remote hosts as figure 2.

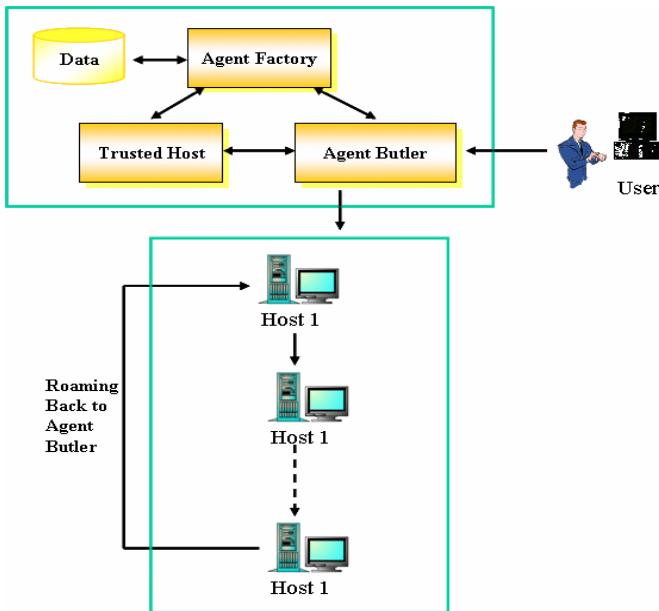


Fig. 2. Structure of FMA

After the original agent provided by the factory is sent out by the user, it travels to a series of hosts to complete the tasks. When it finds out it needs some additional modules, it will seek downloading these modules from the code provider on Agent Factory.

In figure 2, agent structure is as bellows.

Host 1: MA_i <and> DM₁

Host 2: MA_i <and> DM₁ + DM₂ <and> AFM₁

Host 3: MA_i <and> DM₁ + DM₂ <and> AFM₁ + AFM₂

.....

Host n: MA_i <and> DM₁ + ... + DM_j <and> AFM_k + ... + AFM_l

MA_i : Mobile Agent i

AFM_i : Agent Function Module

DM_i : Data Module i

Integrity protection has two purposes on the agent code part as bellows.

- Agent’s view: The verification of integrity protection will detect whether or not the agent code has been modified.
- Host’s view: The verification of integrity protection will offer the proper mechanism to verify the validity of an incoming agent to the host.

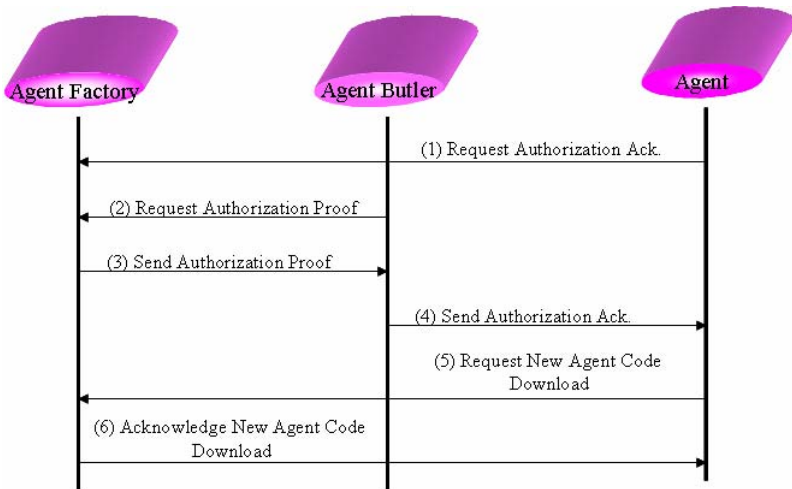


Fig. 3. Authorization Protocol for Agent Code Addition

Request include change type (addition or deletion), ID of mobile agent, ID of host, version of agent function module, ID of agent function module, download type etc..

For the code addition, the mobile agent will send a code addition request to the agent butler.

Request: Agent → Agent Butler(for addition):

Acknowledge Request (to permit): {Addition, Agent_Butler_ID, Mobile_Agent_ID, Agent_Function_Module_ID, Agent_Function_Module_Version, Host_ID, Download_Type}

If the request comes from a valid agent, the agent butler will verify the request and he sent out the change type. If request is a addition, the agent butler will forward the addition request to the agent factory as follows.

Request: Agent Butler \rightarrow Agent Factory(for addition):

Acknowledge Request (to proof): {Addition, Agent_Butler_ID, Mobile_Agent_ID, Agent_Function_Module_ID, Agent_Function_Module_Version, Download_Type}

For the code deletion, the mobile agent will send a code deletion request to the agent butler as code addition.

Request: Agent \rightarrow Agent Butler(for deletion):

Acknowledge Request (to permit): {Deletion, Mobile_Agent_ID, Host_ID, Agent_Function_Module_ID, Agent_Function_Module_Version, Download_Type}

The agent butler will verify if the request comes from a valid agent he sent out and identify the change type. If request is a deletion, the agent butler send the authorization permit if it is approved.

3.2 Comparison FMA with Fixed-Code Mobile Agent

FMA have merits compared with fixed-code mobile agent technology as below.

- Reducing cost: FMA can reduce the cost because FMA need not carry unnecessary agent code modules.
- Improvement of agent module security: Since agent code module will be added when needed irrelevant hosts will be less likely to spy on the important algorithms. And since agent code module will be removed when they become useless irrelevant hosts will be less likely to spy on the important algorithms like agent code addition. In these cases, the threat from malicious attack to mobile agent code should be reduced.

And when a malicious attack to mobile agent code has been detected, the proposed method will be helpful to recover an agent being examined and replaced of the bad mobile agent code module.

- Improvement the flexibility of code function module of mobile agent: Flexible mobile agent code will enable a mobile agent to create new code. And it will enable a mobile agent to process information that it originally cannot. And it can change a code function module of mobile agent when it needed.

4 Conclusion

In this paper, we design Flexible Mobile Agents (FMA). FMA is mobile agents whose code is revisable at execution time. FMA consist of flexibly upgradeable agent code part for that new agent code modules can be added and redundant code modules can be deleted on the executing requirement. FMA prove to be more flexible in agent-based web systems compared to the traditional static type. And the features improve the flexibility of mobile agents and may have much potential usage in the rapidly developing agent-mediated web system.

References

- [1] STONE P., and VELOSO M., "Multi-agent Systems: A Survey from a Machine Learning Perspective," IEEE-TKDE, Vol. 1, No. 1, pp.3-23, 1996.
- [2] BRADSHAW, J. M., Software Agents, AAAI Press/ The MIT Press, 1997.
- [3] Jiawei Han and Michaeline Kamber, Data Mining: Concepts and Techniques, Academic Press, 2000.
- [4] Greenberg, M.S., Byington, L.C., and Harper D.G., 1998. Mobile Agents and Security, IEEE Communications Magazine 36 (7), pp.76-85
- [5] Wang, T.H., Guan, S.U., and Ong S.H., 2000. An Agent Based Auction Service for Electronic Commerce. Proc. of International ICSC Congress on Intelligent Systems & Applications, **CD#1524-045**
- [6] Hua F., and Guan, S.U., 2000. An Agent-based Electronic Payment Scheme for E-commerce. In Rahman, S.M. and Bignall, R.J. (Eds.), Internet Commerce and Software Agents: Cases, Technologies and Opportunities, IDEA Group Publishing, pp. 317-330
- [7] SCHANK R., Dynamic Memory: A Theory of Learning in Computers and People. Cambridge University Press, NY, 1982.
- [8] LEEM J. S., "A study on Business Process Modeling based on Agents," Seoul National University, 1999.
- [9] JENNINGS N.R. AND WOOLDRIDGE M., "Applying Agent Technology, Applied Artificial Intelligence," An International Journal Taylor & Francis London, Vol. 9, No. 4, 1995.
- [10] Vigna, G., 1998. Cryptographic Traces for Mobile Agents, In Vigna G. (Ed.), Mobile Agents and Security, Spinger-Verlag, pp.137-153
- [11] Corradi, A., Montanari, R., and Stefanelli, C., 1999. Mobile Agents Integrity in E-commerce Applications. Proc. of the 19th IEEE International Conference on Distributed Computing Systems Workshops on Electronic Commerce and Web-based Applications/Middleware, pp.59-64
- [12] Hohl, F., 1998. Time Limited Blackbox Security: Protecting Mobile Agents from Malicious Hosts. In Giovanni Vigna (Ed.): Mobile Agents and Security. Springer-Verlag, pp.92-113
- [13] Sander, T. and Tschudin, C. F., 1998. Protecting Mobile Agents Against Malicious Hosts. In Giovanni Vigna (Ed.): Mobile Agents and Security. Springer-Verlag, pp. 44-60
- [14] Zhu, F.M., Guan, S.U., and Yang, Y., 2000. SAFER E-Commerce: Secure Agent Fabrication, Evolution & Roaming for E-Commerce. In Rahman, S.M. and Bignall, R.J. (Eds.), Internet Commerce and Software Agents: Cases, Technologies and Opportunities, IDEA Group Publishing, pp. 190-206
- [15] Guan, S.U. and Yang Y., 1999. SAFE: Secure-Roaming Agent For E-Commerce. Proc. of the 26th International Conference on Computers & Industrial Engineering, pp. 33-37
- [16] Yang, Y. and Guan, S.U., 2000. Intelligent Mobile Agents for E-Commerce: Security Issues and Agent Transport. In Rahman, S.M. and Raisinighani, M. (Eds.), Electronic Commerce: Opportunities and Challenges, IDEA Group Publishing, pp.321-336

A Sales Agent Using Case-Based Reasoning and Rule-Based Reasoning for E-Commerce System

Yun Ji Na¹, Il Seok Ko², and Jong Min Kwak³

¹ Department of Internet Software, Honam University,
59-1 Seobong-Dong, Gwangsan-gu, Gwangju 506-741, South Korea
yjna@honam.ac.kr

² Dept. of E-Commerce,
Chungbuk Provincial University of Science & Technology,
40 Gungu-ri, Okchon-gun, Chungbuk 373-807, South Korea
isko@ctech.ac.kr

³ ChungCheong dot Com, 40-10 Bokdae-Dong,
Heungdok-gu, Chongju, South Korea
webmaster@ccilbo.com

Abstract. Because of development of information technology and acceleration of enterprise e-business, the importance of electronic commerce system has been growing rapidly. Electronic commerce system must provide convenient interface, easy and fast searching function, and product information satisfied customer's requirement. For that many studies about the electronic commerce system that used a reasoning technique and an agent technology conducted largely. In this paper, we design a sales agent with hybrid reasoning method which is composed of case-based reasoning and rule-based reasoning for high customer satisfaction. Also, we were shown on an appropriateness of a proposal system by an experiment.

Keywords: Hybrid Reasoning, Intelligent Agent, Case base reasoning, Rule base reasoning.

1 Introduction

Electronic commerce has been growing rapidly due to the development of the internet and information technology such as high speed telecommunication network and visual reality technology [1, 2]. But many kinds of electronic commerce system don't satisfy customer's requirements or needs because the system doesn't give customer's suitable product-related information. To solve these problems, many researchers have studied reasoning techniques and agent-related electronic commerce systems [4, 5, 6].

An agent is a computer program can assist users' conduct by performing intelligent tasks [7, 8, 9]. And intelligent agent is software that achieve various works that user must achieve directly instead of. Work that user wants needs complex process sometimes or process one task simply. Therefore, intelligent agent needs plan function to understand work that user requires and achieve this effectively and structure that a several agent solves problem by cooperation is required to achieve complicated work efficiently. Intelligent agent can establish and realize planning that

can satisfy user's requirements effectively by cooperating multiplex agent each other. It can be embodied by method that agent in electronic commerce system is various according to each function special quality, In implementation, openness and mutual operation, and proper correspondence about change must be considered. Intelligent agent does information gathering, data processing, knowledge abstraction, decision-making, decision-making achievement and reasoning, for state grasping of relevant condition and is divided to watching, learning, shopping, information abstraction agent according to the function that perform. Many researchers also have developed an electronic commerce framework using multi-agent technologies.

In this paper, we suggest a sales agent using hybrid reasoning engines and customers' preference. This paper aims to develop an electronic commerce system with a sales agent using hybrid reasoning engine that reflects customer preference for high customer satisfaction as well as customer's or user's feedback. The presented system can find suitable product information according to customer's age, occupation, attainment in scholarship, sex, interest field, and customer preference according to price, sales quantity and production year. Also, we were shown on an appropriateness of a proposal system by an experiment.

2 Design of System

2.1 Sales Agent System

The structure of electronic commerce agent for sales is illustrated in Figure 1. It supplies together information that is learned through case-based reasoning and information that is based on rule-based reasoning.

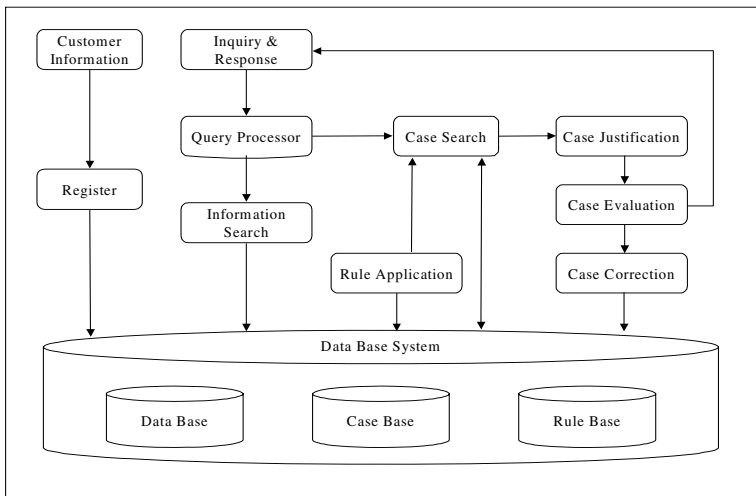


Fig. 1. Sales Agent System Structure

- Registering: In case of new customer, it adds customer's body information to customer information database.
- Customer query process: It discriminates customer and analyzes customer's query and draw keyword from inquiry.
- Case search: The system searches related case from case base by using customer's information and keyword. If customer's information and information that is abstracted from questions agree case in the searched cases, it chooses the case in case base. And it chooses the most appropriate case by calculation similarity degree if there is no relevant case and information that agree.
- Product Search: In case similarity degree of searched case is so low, at search step that search correct information suitable for customer's requirement, offer correct goods to customer through search engine. If case that similarity degree is high or similarity degree is same does not happen, supply the most appropriate information for the goods by searching goods information that corresponds to keyword that draw from customer's requirements in data base system.
- Case Evaluation: At the case evaluation step, in case searched case is impertinent case of customer's inclination, because customer inputs factors such as price, sales quantity, production year directly, the system supplies information for suitable goods for customer's needs.
- Case Correction: In equal case that bought recommended goods is in case base, increase case and add case in case base if case is new case. That is, in case customer did not buy goods, contents of case base are no change and in case customer bought product, correct information of case base. If there is no case in case base, rule base or customer preference input makes new case by selecting product information.

2.2 Similarity Degree

To evaluate whether searched case fits in customer's inclination or not must calculate similarity degree by searching the best suitable case according to customer's requirements. The calculation method of similarity degree is the following.

$$R_i = CUS_i(Customer_Special_Quality) + SEL_i(Case_Choice) \tag{1}$$

$CUS_i(Customer_Special_Quality)$: Similarity Degree of Customer Special Quality

$SEL_i(Case_Choice)$: Similarity Degree of Case Selection (Choice), $i = 1, 2, \dots, n$

$$CUS_i(Customer_Special_Quality) = CUS_i(Age) + CUS_i(Sex) + CUS_i(Sex)_i + CUS_i(Scholarship) + CUS_i(Occupation) + CUS_i(Interest_Field) \tag{2}$$

$$SEL_i(Case_Choice) = \left[\frac{SUC_i(Num_of_Success)}{Maximum_Num_of_Success} \right] \times C \tag{3}$$

Customer's special quality is various kinds condition, and can be applied differently according to goods. In this paper abstracted information in question is limited to contents of distinction of age, sex, attainments in scholarship (scholarship), occupation, interest field.

■ Similarity Degree of Age

$$CUS_i(Age) = W_{Age} - \frac{|Customer's_Age - CB_i(Age)|}{C_{Age}} \quad (4)$$

$CB_i(Age)$: Age in case base

W_{Age} : Weight about age of main target customer of product

C_{Age} : Constant for age.

■ Similarity Degree of Attainments in Scholarship

Attainments in scholarship is divided by graduate school 1, college or university 2, high school 3, middle school 4, and 2 in case do not know.

$$CUS_i(Scholarship) = W_{Scholarship} \times \left[1 - \frac{|Customer's_Scholarship - CB_i(Scholarship)|}{C_{Scholarship}} \right] \quad (5)$$

$CB_i(scholarship)$: Scholarship of case base

$W_{Scholarship}$: Weight about in scholarship

$C_{Scholarship}$: Constant for in scholarship

■ Similarity Degree of Sex

Customer's distinction of sex by goods does by man 1, woman 2, unknown 3.

$$CUS_i(Sex) = W_{Sex} \times \left[1 - \frac{|Customer's_Sex - CB_i(Sex)|}{C_{Sex}} \right] \quad (6)$$

$CB_i(Sex)$: Sex of case base

W_{Sex} : Weight for sex

C_{Sex} : Constant for sex

■ Similarity Degree of Occupation. According to Connection Degree About Goods and Profession, Give Weight

$$CUS_i(Occupation) = W_{Occupation} \quad (7)$$

$W_{Occupation}$: Weight for occupation

■ Similarity Degree of Interest Field. Give Weight If Goods and Interest Field Agree, and If Not, Can Apply Weight According to Relating Degree Differently

$$CUS_i(Interest_Field) = W_{Interest_Field} \quad (8)$$

$W_{Interest_Field}$: Weight for interest field

■ Similarity Degree of Case Selection (Choice). Case Choice Appears by Ratio of Success Number

$$SEL_i(Case_Choice) = \left[\frac{SUC_i(Nmber_of_Success)}{Maximum_Nmber_of_Success} \right] \times C \tag{9}$$

$SUC_i(Nmber_of_Success)$: Total numbers which customer bought goods

C : Basic constant by product.

3 Experiment and Results

3.1 Data Structure and Variables

To make prototype of system, we used Windows 2000 Server environment, IIS5.0 as web server, ASP3 and SQL2000 as DBMS. We designed prototype system for books sale. Data structure is followings.

- Product Information

Books Code	Title	Writer	Publishing Company	Price	Publication year	Sales Quantity
------------	-------	--------	--------------------	-------	------------------	----------------

- Customer Information

Customer Code	Name	Address	Telephone Number	Birthday
Scholarship	Age	Occupation	Interest Field	Secret Number

- Sale Information

Books Code	Customer Code	Sale Date	Payment Method	Sale Number
------------	---------------	-----------	----------------	-------------

- Index Information

Keyword	Books Code
---------	------------

Values given for calculation of Similarity Degree for conveniences is followings.

Maximum number of Success = 1000, $C = 10$,

$W_{Age} = C_{Age} = 5,10$,

$W_{Scholarship} = C_{Scholarship} = 3,10$,

$W_{Sex} = C_{Sex} = 3,10$,

$W_{Occupation} = 5$,

$W_{Interest_Field} = 5$.

3.2 Results

Tables 1 shows example of composed index. And Table 2 shows calculated similarity degree.

Table 1. Table of Index

Age	Scholarship	Sex	Occupation	Interest Field
30	Graduate School	Man	Student	IT

Table 2. Calculated Similarity Degree

Books Code	Field	Age	Scholar-ship	Sex	Occupation	Case Selection	Success Number
IT123	5.00	9.00	3.33	10.00	5.00	4.00	36.33
IT560	5.00	9.00	6.67	6.67	5.00	3.00	35.33
IT230	5.00	9.20	10.10	10.00	5.00	2.00	41.20
IT002	5.00	9.60	10.10	6.67	5.00	3.80	40.07
IB123	5.00	10.00	10.10	10.00	5.00	6.00	46.00

■ *Case Evaluation.* Product information for the highest similarity degree among case-base is presented. In case customer does not satisfy about product that is presented, case for index is not in case, or similarity degree is so low. It shows search result that is consider user's requirements and fit most on customer need by making customer input benevolent persons' reflection ratio such as price, sales quantity, production year differently.

Table 3. Example of Case Selection

IT	e-Business	30	Graduate School	Man	Student	IB123	600
----	------------	----	-----------------	-----	---------	-------	-----

■ *Customer Preference Input.* Customer can select product by preference input. Table 4 and Table 5 shows the result of product information in case customer input own preference when he or she didn't satisfy to given product information.

Table 4. Product information list in case of price is 100%, Sales Quantity is 0%, Publication year is 0%

Preference Condition	Books Code	Title	Writer	Publishing Company	Price [Won]	Publication Year	Sales Quantity
PRICE 100% SALES QUANTITY 0% PUBLICATION YEAR 0%	IT123	eBiz World	AAB	Press One	8000	200010	5800
	IT560	Web Information	SCS	Case World	8500	199905	5200
	IT230	IT World	DDF	SamBook	8800	200103	4700
	IT002	IT Architecture	DFG	Basic Books	9000	200101	7700
	IB123	Information Management	SFS	Tritent	11000	199612	6400

Table 5. Product information list in case price is 0%, Sales Quantity is 100%, Publication year is 0%

Preference Condition	Books Code	Title	Writer	Publishing Company	Price [Won]	Publication Year	Sales Quantity
PRICE 100% SALES QUANTITY 0% PUBLICATION YEAR 0%	IB123	IT Architecture	DFG	Basic Books	9000	200101	7700
	IT002	Information Management	SFS	Tritent	11000	199612	6400
	IT123	eBiz World	AAB	Press One	8000	200010	5800
	IT230	Web Information	SCS	Case World	8500	199905	5200
	IT560	IT World	DDF	SamBook	8800	200103	4700

■ *Case Correction.* It shows goods information about selected case in case base to customer. In case of customer bought goods or took answer of affirmative that information for goods were profitable, increase success number in case base. In case of did not use case, It can register as new case about selected product and make success number 1.

4 Conclusion

In this paper, we proposed electronic commerce system for sales that can enhance corporation's profit in electronic commerce that is accelerated along with development of internet, that can heighten customer's satisfaction accommodating complicated customer requirements and that can use various kind of information about customer in corporation dimension.

We reflected enough customers' requirements through customer preference input in case of product that is not reasoned in case base and used recommended product information to new case. The system could search more intelligent information by

doing so. Therefore we can know that the system can offer much more customer satisfaction to customer by giving customer more efficient information. This research needs to make corporation use data actually by applying web application in real enterprise. Corporation or enterprise can supply more information to customer thereby and corporation can accomplish marketing or better administration result by using various kind of information that get from customer.

References

- [1] Il Seok Ko, Choon Seong Leem, "An Improvement of response speed for electronic commerce system," *Information System Frontiers* 6:4, pp.313-323, 2004. 12.
- [2] FELLEINSTEIN, C. AND WOOD R., *Exploring E-commerce, Global E-business and E-Societies*. Prentice Hall, N.J., USA, 2000.
- [3] MOLLA A., "E-commerce systems success: an attempt to extend and respecify the delone and maclean model of IS success," *Journal of Electronic Commerce Research*, Vol. 2, No. 4, pp.1-11, 2001.
- [4] RIGGINS R. J. and RHEE H. S. "Toward a unified view of electronic commerce," *Communication of the ACM*, Vol. 41, No. 10, pp.88-95, 1998.
- [5] ROLF T., WIGNAD AND BENJAMIN. I. R., "Electronic Commerce: Effects on Electronic Markets," *JCMC*, Vol. 1. 1999.
- [6] LEE J. K., "A Comparison Shopping Architecture over Multiple Malls: the Meta-Malls Architecture," *ICEC'98*, pp.149-154, 1998.
- [7] STONE P., and VELOSO M., "Multi-agent Systems: A Survey from a Machine Learning Perspective," *IEEE-TKDE*, Vol. 1, No. 1, pp.3-23, 1996.
- [8] JENNINGS N.R. AND WOOLDRIDGE M., "Applying Agent Technology, Applied Artificial Intelligence," *An International Journal Taylor & Francis London*, Vol. 9, No. 4, 1995.
- [9] Jiawei Han and Michaeline Kamber, *Data Mining: Concepts and Techniques*, Academic Press, 2000.

A New Ciphering Method Associated with Evolutionary Algorithm

Fouzia Omary¹, Abdelaaziz Mouloudi², Abderrahim Tragha³,
and Abdelghani Bellaachia⁴

¹ Department of mathematics and computer sciences,
The science faculty –Rabat,
University of MohammedV-Morocco
omaryfouzia@yahoo.fr

² Department of mathematics and computer sciences,
The science faculty –Kenitra,
University of Ibnou Toufail-Morocco
Mouloudi_aziz@hotmail.com

³ Department of mathematics and computer sciences,
The science faculty Ben M'Sik Casablanca,
University of Hassan II-Mohammedia-Morocco
a.tragha@univh2m.ac.ma

⁴ Department of mathematics and computer sciences,
The Georges Washington University, USA
bell@gwu.edu

Abstract. In this article, we present a new cryptographic system which is a combination of our ciphering evolutionary algorithm and a new ciphering method called “fusion”. This latter allows the alteration of the appearance frequencies of characters from a given text, and can be used as a preparatory stage for our evolutionary algorithm. So, it constitutes the first part of the system cryptographic. Our system has at its disposed two keys, the first one is generated during “fusion” part and the second one is generated by the evolutionary algorithm. Both of them are symmetric, session keys and strengthening the security of our system. To underline this system, we performed applications on different texts and through a good debate, we illustrate its quality in comparison with others.

1 Introduction

Nowadays, cryptography is not reserved only to diplomatic and military aspects like in the past; every citizen has the right to make available his data only to his recipient. Besides its antiquity and necessity, cryptography is only in its early stages, and ciphering algorithms are minority.

The PGP (1992) [10], is an hybrid system; it is currently, the dominant crypto-system. RSA (1970) [1], is asymmetric and based on the modular arithmetic to define its public and private key. This algorithm always resists to the cryptanalysis. IDEA (1991) [1], symmetrical, a quite recent algorithm, with a key of 128 bits. AES (1997) replaced the DES, is symmetrical and capable to support keys of length equal to 256 bits. DES (1973) [5], symmetrical algorithm whose secret key is of length 64 bits.

Since, evolutionary algorithms (EA) achieved a great success in the resolution of optimisation problem and our ciphering problem is a combinatorial optimisation problem then solving this latter with EA was our contribution at ICCMSE 2005 [6].

Setting out our objective in to altering to the maximum, the appearance frequencies of the characters from a grew text in clear T, in order to make difficult the statistic cryptanalysis, we conceived a new method of ciphering called “fusion”. This latter constitutes also a preparatory stage towards the application of our EA and allow to start with an interesting initial population.

The paper is organized as follows. The next section describes the first part of our cryptographic system: “fusion”, the second part: evolutionary algorithm and illustrates the deciphering process via the keys generated at the two parts. Experimental results and evaluative discussion are given respectively in sections 3, 4.

2 Description of Our System

2.1 Formalisation of the Problem

Let T be a continuation of k characters and t_1, t_2, \dots, t_n its different characters. Denote by L_i ($1 \leq i \leq n$) the list of the different positions of t_i in T before the ciphering. L_1, L_2, \dots, L_n is a partition of the set $\{1, 2, \dots, n\}$. T can be represented by vector:

(t_1, L_1)	(t_2, L_2)	\dots	(t_n, L_n)
--------------	--------------	---------	--------------

The goal of our works is to alter to the maximum the frequencies of apparition of the characters in the text T and to establish more mess in their positions.

2.2 Our Ciphering System

This system is composed of two principal parts: the fusion and the application of evolutionary algorithm as descript in figure 1.

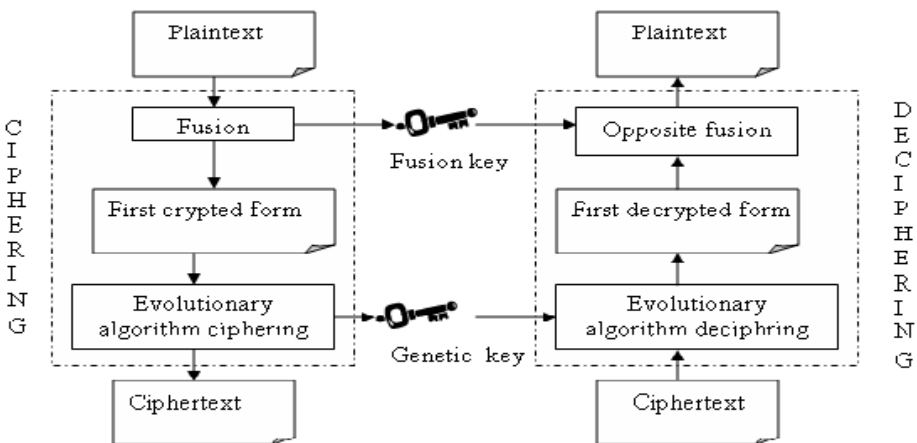


Fig. 1. Schema of our system

2.2.1 First Part: The Fusion

We sort the set of the lists L_1, L_2, \dots, L_n according to their sizes in the decreasing order then we divide it in three subsets of sizes near to $\lfloor n/3 \rfloor$ (floor of $n/3$), named respectively: E_L, E_M, E_P . Let us indicate respectively by N_L, N_M and N_P the cardinals of E_L, E_M and E_P . The process fusion is recursive. It is described below.

Let us indicate by L_m and L_p the smallest lists of E_M, E_P respectively and by S_k the desirable key size

- If the merge of these two lists brings to a key of undesirable size then fusion is applied only in E_P as follows:
 - o Let us take randomly a number of lists $L_{p_1}, L_{p_2}, \dots, L_{p_f}$ in E_P .
 - o Applying fusion to these lists means:
 - Replace the characters $t_{p_1}, t_{p_2}, \dots, t_{p_f}$ corresponding to these lists by one character c_f chosen randomly and not representing any other list.
 - Add the triplet: $([t_{p_1}, t_{p_2}, \dots, t_{p_f}]; [L_{p_1}, L_{p_2}, \dots, L_{p_f}]; c_f)$ to the fusion key.
 - $E_p \leftarrow E_p - \{L_{p_1}, L_{p_2}, \dots, L_{p_f}\}$.
 - o Repeat the application of fusion on E_P until reaching the size of the desired key.
- Else the fusion will be applied to $E_M \cup E_P$ as follows:
 - o Let us indicate initially the lists which we indeed to merge. These lists are composed of $L_{p_1}, L_{m_1}, \dots, L_{p_f}, L_{m_f}$ such as f is taken randomly in $\{1, 2, \dots, (\min(N_M, N_P))\}$, $L_{p_1}, L_{p_2}, \dots, L_{p_f}$ are selected in E_P in increasing order of their size, in alternation with $L_{m_1}, L_{m_2}, \dots, L_{m_f}$ which are taken in E_M in the same order, while taking account of the following iterative processing :
 - $r \leftarrow 1; E \leftarrow \emptyset$
 - repeat
 - $E \leftarrow E \cup L_{p_r} \cup L_{m_r}$
 - If size of E is smaller than S_k then $r \leftarrow r+1$
 - Until $r=f$ or size of E is bigger than S_k
 - $f \leftarrow r$
 - o Applying fusion to the lists above means:
 - Replace the characters $t_{p_1}, t_{m_1}, t_{p_2}, t_{m_2}, \dots, t_{p_f}, t_{m_f}$ corresponding to these lists by only one character c_f chosen randomly and not representing any list.
 - Add the triplet:
 - $([t_{p_1}, t_{m_1}, t_{p_2}, t_{m_2}, \dots, t_{p_f}, t_{m_f}]; [L_{p_1}, L_{m_1}, \dots, L_{p_f}, L_{m_f}]; c_f)$
 to the fusion key.
 - o Repeat the process of fusion on:
 - $E_M \leftarrow E_M - \{L_{m_1}, \dots, L_{m_f}\}$ and $E_p \leftarrow E_p - \{L_{p_1}, \dots, L_{p_f}\}$
 Until reaching the size of the desired key S_k .

- If we indicate by FO the number of fusions applied then the generated key representative of these operations is a set of FO triplets of the form:

$$([\ t^i_1, t^i_2 \dots t^i_{p_i}], [L^i_1, L^i_2 \dots L^i_{p_i}], c_i)$$

where c_i is the substitute of the characters $t^i_1, t^i_2, \dots, t^i_{p_i}$ whose lists of respective positions in the plaintext are: $L^i_1, L^i_2, \dots, L^i_{p_i}$.

Thus, after fusion, the number of characters (thus also of lists) is reduced to m ($m < n$). And the new ciphered text, T_f , will be denoted by the following:

(c_{f_1}, L_{f_1})	(c_{f_2}, L_{f_2})	...	(c_{f_m}, L_{f_m})
----------------------	----------------------	-----	----------------------

2.2.2 Second Part: Application of Our Evolutionary Algorithm

The body of our algorithm is the same as general evolutionary algorithm [2], [3].

- Step 0: coding

An individual (or chromosome) is a vector of size m . The genes are the L_{p_i} lists ($1 \leq i \leq m$). The i^{th} gene L_{p_i} contains new positions that the character c_i will take.

- Step 1: Creation of the initial population P_0 made of q individuals: X_1, X_2, \dots, X_q .

We designate by the Original-Ch the chromosome whose genes are L_1, L_2, \dots, L_m lists that represent the message before the application of the algorithm.

We apply q permutations on Original-Ch in order to get an initial population formed by q potential solutions of the problem.

$i:=0$;

- Step 2: Fitness function

Let X_j be an individual of P_i whose genes are : $L_{j_1}, L_{j_2} \dots L_{j_m}$.

We define the fitness function on the set of the individuals X_j by:

$$F(X_j) = \sum_{i=1}^m | \text{card} (L_{j_i}) - \text{card} (L_i) | \tag{1}$$

- Step 3: Selection of the best individuals

We use the classical method of the roulette [7], permitting to keep the strongest individuals.

- Step 4: Applications of the genetic operators

We apply the genetic operators adapted to this hand of problem, such as:

MPX Crossover: This operator has been proposed by Mühlenbein [9] for the traveller salesman problem. The operator’s idea is to insert a part of parent’s chromosome in the chromosome of the other parent so that the resulting crossover is the nearest possible to his parents. The two sons are obtained in a symmetrical manner. It is a two point crossover. This operator is applied to the selected individuals with a very precise rate. According to [8], the order of the best rate is between 60% and 100%.

Mutation of transposition [9]: We choose the mutation that consists in permuting randomly two genes of a chromosome. This operator is applied to the individuals derived from crossover with an adapted rate preferably from 0.1% to 5% [8].

Place the new offspring in a new population P_{i+1} .

- Repeat the steps 2,3 and 4 until a stop criteria.

Define the stop criteria :

The function F is bounded because $0 \leq F(X) \leq 2 * k$ for each individual X. In fact:

$$\sum_{i=1}^m |card(L_{k_i}) - card(L_i)| \leq \sum_{i=1}^m (card(L_{k_i}) + card(L_i)) \leq 2 * k \quad (2)$$

According to some results [9], the convergence of fitness function is guaranteed towards a value close to max, determined experimentally.

- Final step of our algorithm:

Let's Final-Ch the final solution given by our evolutionary algorithm. It contains the lists of characters positions in the encrypted text. The permutation allowing to obtain Final-Ch From Original-Ch, is a secret key, called the genetic key .

2.3 Deciphering

We start by deciphering the second part of the system. We represent the encoded text T' by a vector of lists. Let's designate by c_1', \dots, c_m' the different characters of T' and by L_1', L_2', \dots, L_m' their respective lists of positions. Thanks to the genetic key, the characters are going to recover their lists of corresponding positions in the text T_f obtained after the first part of ciphering.

Indeed, the key can be represent by a vector, that we denote Key, of size m such that:

Key(1)=p₁, Key(2)=p₂, ...Key(i)=1, ... Key(m)=p_m, where :

the character c_{p1}' is going to be associated to the list L₁'

the character c_{p2}' is going to be associated to the list L₂'

.....

the character c_{pm}' is going to be associated to the list L_m'.

Thus we get the text T_f.

Then, thanks to the fusion key which is clear and direct (see Sect. 2.2.1), we can immediately re-alter the merged lists L_{f_i} into sub-lists of origin and assign to each of these latter its corresponding character. Thus we obtain the initial text T.

3 Experimentation

We apply our algorithm on texts of different sizes, and for each of them, we make the application for different sizes of population. Then we record the important results to be known, value of the convergence of the fitness function and number of the generations reached at the time of this convergence. These results are mentioned in Table 1.

After application of the algorithm we obtained the genetic key, fusion key and the encoded form (see Fig. 3).

The fusion key is:

([ē, ś, Ĩ] ; [4 111 230 327 358 382 429 433 501 969,10 70 97 325 364 581 967, 29 141 152 187 865] ; ž)

([L, Ć, ☒] ; [24 57 128 201 208 276 341 402 641 802 852 904 914 945, 31, 42] ; Ć)

([I, †] ; [92 263 344 418 527 609 687 717 797 806 , 190 692 715 992 1017] ; é)

([Ī, D, Ê, ö, ç, Å] ; [33 144 165 191 , 44 189 632 693 697 701 705 709 713 883, 61 175 217 301 400 532 1007 , 89 452, 118,140, 168 518] ; »)

The genetic key is :

22 23 24 25 26 27 28 29 30 31 32 20 33 34 35 36 37 0 1 2 3 4 5 6 7 8 17 18 19 9 21 10 11 12
13 14 15 16

Table 1. Summary Statement of results

Size of population		16	20	24	30	32
Message1 1026 char.	Number of generations	35	33	57	44	58
	Value of convergence	1340	1378	1328	1710	1720
Message2 684 char.	Number of generations	35	46	163	72	62
	Value of convergence	762	822	912	914	912
Message3 1149 char.	Number of generations	31	26	30	47	42
	Value of convergence	1288	1850	1396	1876	1818
Message4 805 char.	Number of generations	35	80	172	54	54
	Value of convergence	950	1022	1024	1138	988

We note that the best values are reached for a population of size 30 and often after 50 generations. In some cases, a population of size 20 gives good results.

4 Discussion

4.1 Theoretical Comparison

We compare our ciphering system to IDEA which is used by the PGP. Its key length is 128 bits. Our system possesses two keys. The fusion key, witch size may be controlled by the system; then we can assign to it a value unbreakable nowadays. The genetic key size is at least 240 bits, a more important size since it resists much better to cryptanalysis via exhaustive search. These keys are session keys and randomly generated by our system, while the one of IDEA is not.

IDEA ciphers by blocs, this is an asset for the differential cryptanalysis[5]. Ours doesn't, therefore it's on one hand immune from such cryptanalysis, and on the other

Table 2. Comparison to IDEA and RSA

	IDEA	RSA	Without fusion	With fusion
Ciphering time	30 ms	330 ms	200 ms	225 ms
Deciphering time	40 ms	390 ms	20 ms	27 ms

hand inexpensive. However, the only formidable cryptanalysis in our case is the one based on the study of apparition frequencies of the letters in a text. Now, on one hand, thanks to the fusion the true frequencies of the characters are not recognized any more, therefore the cryptanalysis cannot rely on wrong statistic.

4.2 Practical Comparison

We compare the execution time in one hand of our ciphering system without fusion, and in the other hand with fusion, to the execution time of IDEA and RSA, on some messages. The table below gives an example of this comparison.

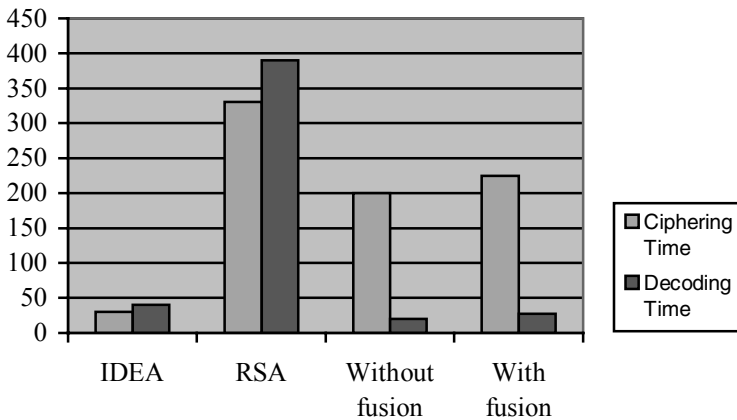


Fig. 4. Graphical representation of execution time

5 Conclusion

Through this work, we reached two objectives. The first one is the introduction of new method of ciphering “fusion” whose major advantage is strengthening the system against the most formidable attacks, as for the other advantages, they are mentioned above in the discussion.

The second objective is to exploit the EA in order to conceive and realize a ciphering that benefits from all its qualities (simplicity of genetic operations, performance...). We have assessed this work through comparison with other systems of the same nature.

In spite of the qualities mentioned above, we cannot confirm that our system is long time reliable, like the best actual cryptosystems, except the one-time-pad, according to Shanon [4]. Therefore, a long way remains to cover by cryptographers.

References

1. Menzes, A. J., Paul, C., Dorschot, V. , Vanstone, S. A. : Handbook of Applied Cryptography CRC Press fifth Printing (2001)
2. Catherine KhamPhang. BOUNSAYTHIP "Algorithmes heuristiques et évolutionnistes" Thèse de doctorat université de Lille. Octobre 1988.

3. Caux, C., Pierreval, H., Portmann M.C. : Les algorithmes génétiques et leur application aux problèmes d'ordonnancement. APII. Volume 29-N° 4-5 (1995) 409-443.
4. Claude Shannon : Communication Theory of Secrecy Systems. Bell Systems Technical Journal (1949).
5. Douglas, R. Stinson : Cryptography – Theory and Practice. CRC Press (1995)
6. Omary, F., Tragha, A., Bellachia, A., Lbekkouri ,A., Mouloudi A.: An Evolutionary Algorithm to Cryptography. Advances in Computational Methods in Sciences and Engineering, Vol. 4 (2005) 1749-1752
7. Goldberg, D.E.: Genetic algorithms in search optimisation & Machine Learning. Addison-Wesley. Publishing Company, Inc (1989).
8. Grenfenslette, J.J. : optimisation of control parameters for genetic algorithms. IEEE translation on systems Man, and cybernetics, Vol 16 N°1 (1986) 122-128..
9. Muhlenbein H.: Evolutionary Algorithms: Theory and applications. Wiley (1993).
10. Zimmermann, P. : Guide de l'utilisateur de PGP. Network-Associates, Inc. USA,(1994)

Power Distribution Automation System Using Information Technology Based Web Active Database

Sang-Yule Choi

School of Electrical and Computer Engineering,
Sungkyunkwan University,
Suwon 440-746, South Korea
ppk99@induk.ac.kr

Abstract. The electric utility has the responsibility to provide a good quality of electricity to their customers. Therefore, they have introduced DAS (Distribution Automation System) to automate the power distribution networks. DAS engineers need a set of state-of-the-art applications, eg. managing distribution system in active manner and gaining economic benefits from a flexible DAS architectural design. The existing DAS functionally could not handle these needs. It has to be managed by operators whenever feeder overloadings are detected. Therefore, it may be possible for propagating the feeder overloading area, if operator makes a mistake. And it utilizes closed architecture, therefore it is hard to meet the system migration and future enhancement requirements. This paper represents web based, platform-independent, flexible DAS architectural design and active database application. The recently advanced internet technologies are fully utilized in the new DAS architecture. Therefore, it can meet the system migration and future enhancement requirements. And, by using active database, DAS can minimize feeder overloadings area in distribution system without intervening of operator, therefore, minimizing feeder overloadings area can be free from the mistake of operator.

1 Introduction

The electrical utility has the responsibility to provide a good quality of electricity to their customers. Therefore, the DAS (Distribution Automation System) is introduced to control and operate complex power distribution system in an economical and reliable fashion. It includes important functions such as feeder automation, load control and telemetering. In Korea, the electrical utility company is now facing deregulation and privatization. Several privatized distribution companies will be appear in few years. And they will require new way of thinking and new solutions for open-access competitive electricity market. But the existing DAS could not meet these new requirements, because it has to be managed by passive manner and it utilizes closed system architecture.

In closed system architecture, DAS has utilized proprietary software which is tightly coupled to a particular operating environment. Therefore, system integration and data migration in a heterogeneous environment give pressures to DAS developers

and operators. And, due to the passive DAS management, DAS is always exposed to unintentional mistake from operators. Therefore, whenever feeder overloadings are detected, inexperienced operator may get worse feeder overloadings situation.

Despite of the above defects, a closed architecture and a passive management have been successfully applied to DAS until the present time. However, under open-access competitive market environment, data migration in a heterogeneous environment and reliable system management by active manor become critical issues to distribution utility companies. This environment gives DAS engineers require a set of state-of-the-art applications, eg using internet application for convenient data exchange and system openness and adopting active database application for reliable system management by active manor. Based on these requirements, the authors present new DAS architecture based on open system and an active rule application. An open DAS system architecture utilizes recently matured internet technology and relational active database.

2 An Active Database for DAS

An active database system is the result of combination of active techniques and DBMS, Production rules in active database system allow specification of data manipulation operations that are executed automatically whenever certain events occur or conditions are satisfied. Active database rules provide a general and powerful mechanism for maintaining many database features, including integrity constraint, data consistency, and so on, in addition, active database system provide a convenient platform for large and efficient knowledge bases and expert system [1].

2.1 Data Requirements for DAS Database

Data requirements for DAS database are substation, transformer, feeder, feeder section, switch, and information. And attributes of these requirements have to be easily applied to feeder reconfiguration program.

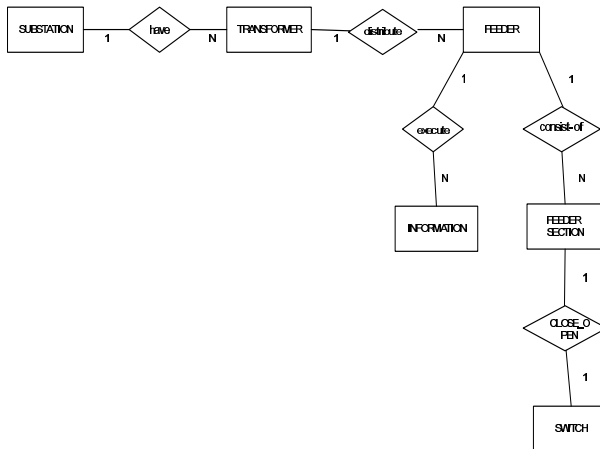


Fig. 1. ERD of feeder automation database

The entity-relationship is displayed by means of the graphical notation known as ER diagram in fig.1.

2.2 Rules Definition for DAS Database

Data acquisition system which is located in distribution networks detects currents, section loadings, voltage and the status of close/open in real time, and the present attribute values of switch is updated by detected ones. DAS active database monitors the present state of distribution networks by using updated values: If updated values trigger some events and condition are true, then they imply that distribution networks is in overloaded state. Therefore action for feeder reconfiguration is executed to relieve feeder overloadings and minimize line losses. Switches to be open(or closed) are selected after feeder reconfiguration is executed.

Feeder reconfiguration can fire other rules which update attribute close/open status value of selected switches and send close/open signal to appropriate intelligent switches installed in distribution networks.

Due to maintaining radial distribution networks structure, updated value of switch can trigger other rules that update close/open status value of another switch(not a selected one from feeder reconfiguration). And updated attribute value of switch can trigger rules which updates the close/open status value of appropriate feeder section that is connected to updated switch, because close/open status of feeder section is dependent on attribute values of appropriate switch object. Distribution networks can be operated with minimum losses, and radial structure can be maintained without intervening of operator with the definition of active rules which have update propagation characteristics.

The definition of active rules for DAS are as follows:

Rule 1) If initially attribute close/open status value of switch is changed from open to close then attribute close/open status value of appropriate feeder section which is connected to the switch is changed from open to close

Rule R1 for switch

Event : update to st

Condition : updated(switch(S)), NEW S.st=close

Action: update feeder section.st=close where feeder section.ssn = switch.ssn

Rule 2) If initially attribute close/open status value of switch object is changed from close to open then close/open status value of appropriate feeder section object, which is connected to the switch is changed from close to open.

Rule R2 for switch

Event : update to st

Condition : updated(switch(S)), NEW S.st=open

Action: update feeder section.st=open where feeder section.ssn = switch.ssn

Rule 3) If attribute loadings value of switch object is updated then section loadings value of feeder section is updated by the same value of loadings of switch.

Rule R3 for switch

Event : update to ssnmva

Condition : True

Action : update feeder section.ssnmva = switch. ssnmva where feeder section.ssn = switch.ssn

Rule 4) If updated section loadings value of feeder section is exceeded by 80[%] of feeder capacity then feeder reconfiguration program is executed to minimize line losses and relive overloadings.

Rule R4 for feeder section

Event : update to ssnmva

Condition : updated(feeder section(FD)),

NEW FD.ssnmva > FD.fnc

Action : reconfiguration()

Rule 5) If reconfiguration() is executed and switch to be closed(or opened) is selected, then attribute close/open status of selected switch is updated by close(or open).

Rule R5 for reconfiguration()

Event : reconfiguration()

Conditon : TRUE

Action : (update switch.st=open where switch.ssn

= result of open reconfiguration())

&&(update switch.st=close where switch.ssn=

result of close reconfiguration())

where, result of open reconfiguration() : a selected switch to be opened resulting from feeder reconfiguration.

result of close reconfiguration() : a selected switch to be closed resulting from feeder reconfiguration.

Rule 6) If attribute voltage value of switch is updated then the attribute voltage value of appropriate feeder section is updated

Rule R6 for switch

Event : update vv

Condition : updated(switch(S)), TRUE

Action : update feeder section.vv =

switch.vv— V_{drop}

where, feeder section.ssn = switch.ssn

Where, V_{drop} : Voltage drop of feeder section

Rule 7) If updated voltage value of feeder section is lower than minimum voltage value of feeder section then feeder reconfiguration program is executed to minimize line losses and relive overloadings.

Rule R7 for feeder section

Event : update to vv

Condition : updated(feeder section(FD)),

NEW FD.vv > FD.min_vv

Action : reconfiguration()

Rule 8) If initially attribute close/open status value of switch is changed from open to close then Active database sends signal to intelligent switch to be closed

Rule R8 for switch

Event : update to st

Condition : updated(switch(S)), NEW S.st=close

Action: signal to intelligent switch to be closed

Rule 9) If initially attribute close/open status value of switch is changed from close to open then active database sends signal to appropriate intelligent switch to be opened

Rule R9 for switch

Event : update to st

Condition : updated(switch(S)), NEW S.st=open

Action: signal to intelligent switch to be opened

Rule 10) If feeder reconfiguration executed then information is updated by the resulted data form feeder reconfiguration.

Rule R10 for reconfiguration

Event : reconfiguration()

Condition : TRUE

Action : (update information.rsn = history) &&

(update information.ploss= result loss of reconfiguraion())&&(update informa- tion.dploss = result of change_of_loss of reconfiguration())

Where, history = reconfiguration times

result loss of reconfiguraion(): total loss after feeder reconfiguration

result of change_of_loss of reconfiguration() : the amount of loss change resulting from feeder reconfiguration;

2.3 Active Rule Manager for DAS Active Database

The execution of a rule's action may trigger another rule, whose action may trigger other rule's event. Active rule manager coordinates active rule interaction and the execution of active rules during transaction execution by interfacing constraint manager. In this paper, rule interaction is represented by means of Triggering Graph[2].

Definition. Let R be an arbitrary active rule set. The triggering Graph is a directed graph $\{V,E\}$, where each node $v_i \in V$ corresponds to a rule $r_i \in R$. A directed arc $\langle r_j, r_k \rangle \in E$ means that the action of rule r_j generates events which trigger rule r_k . Fig 3 represents rule interaction using Triggering Graph

In fig.2, when intelligent switch loadings of distribution networks is changed because of the increasing of customer's consuming, data acquisition system detects the amount of loadings change and sends updating signals switches of DAS database. Due to the updating signals, rule R3 is triggered to update section loadings of appropriate feeder section that is connected to the switch. If this updated value exceeds 80[%] of feeder capacity then R4 is triggered to minimize line losses and to relive feeder overloadings by using feeder reconfiguration program. R4's action trigger R5 and R10 simultaneously. Due to R10's action, data resulted from feeder reconfiguration program is stored in information object. R5's action updates attribute close/open status value of switch

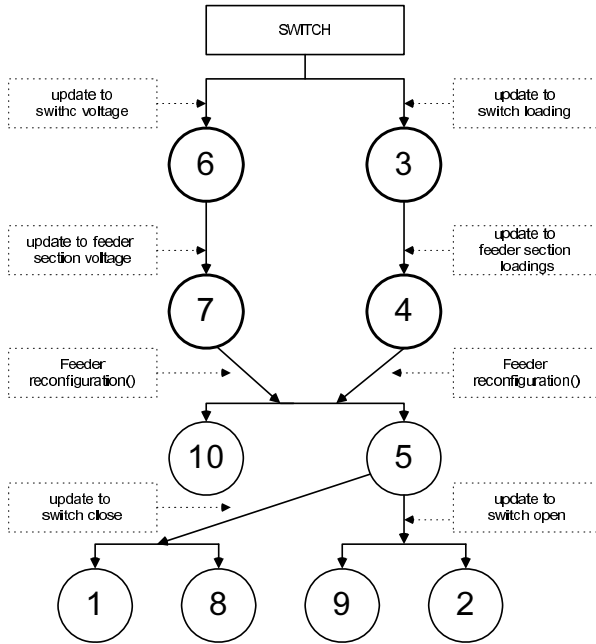


Fig. 2. Triggering graph for Feeder automation

selected from feeder reconfiguration program and triggers R1, R2, R8 and R9 simultaneously. Because of R1, R2, R8 and R9, close/open status of feeder section is updated by the same status of appropriate switch and close/open status of Intelligent switch located in distribution networks is changed by the same status of appropriate switch.

3 Web Based DAS Active Database System Architecture

A flexible open DAS system architecture has to satisfy the two-fold requirements[3] It is built to vendor neutral standards (easy in the use of software package).

It will provide the ability to enhance an existing DAS without relaying one vendor(easy in the continuing development and maintenance of the software package).

These requirements can be met by using the internet as the operating environment.

Using internet technology for DAS architecture will gain following benefits.

First, it support cross-platform architecture: In a standardized internet browser environment with HTML and TCP/IP protocols, users will continue using the platforms with which they are most familiar without conscious of different hardware platform.

Second, it follows open system standard: By following Structured Query Language(SQL), HTML, HTTP, FTP, TCP/IP, and PPP, data exchange and system expansion are easily done with minimum efforts[4]. The proposed new web based DAS architecture make uses of the Java 2 Enterprise Edition architecture which is a Web-based multitier architecture, as presented in fig. 3.

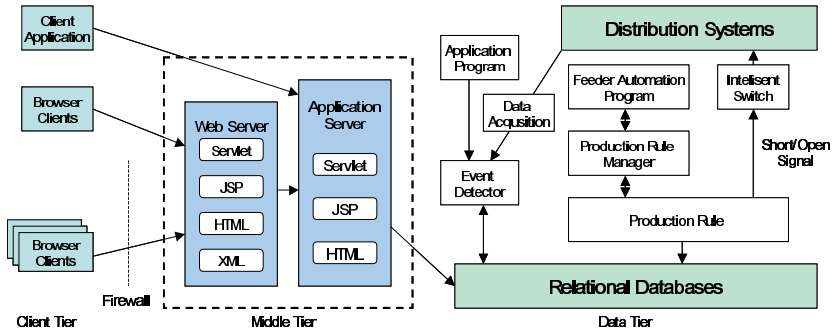


Fig. 3. Web based DAS active database system architecture

The architecture can be expressed by subdividing two parts in fig.3.

The one is web based architecture which support open system and the other is active database architecture which support DAS feeder automation.

For web based architecture, Its structure can be divided into three tiers[3].

Client tier: It provides user interface

Middle tier: It is subdivided into the Web server and the application server.

Data tier: It handles the information storage

In the middle tier, application server is transferring request from the web into appropriate functions in the system and also provide for interfacing different kinds of database. Web server acts as the gateway for Web-based clients to access the database.

Power distribution engineers and operators sent HTTP requests to Web server through the industrial standard web browser. If requested web page containing database SQL command, the database interprets SQL commands and returns matched data in the database back to Web server. Matched data is formulated as a web page and displayed web page in the client window[4].

For active database architecture shown in the right-side of fig.3.

Its structure can be expressed specifically by dividing into three parts

- Event detector :

It checks telemetered data and sends signal to production rule manager if integrity constraints are violated.

- Production rule manager

It accept signal from event detector and determines which rules to be fired.

- Production rule

It allows specification of data manipulation operations that are executed automatically whenever certain events occur or conditions are satisfied.

Data acquisition system located in distribution network detects switch's close/open status, current, voltage and loadings, and it sends a detected data to central DAS database system.

In DAS database system, event detector accepts detected data sending from data acquisition system and sends data modification operation to database. If integrity constraints is violated because of data modification then event detector send signal to

production rule manager. By using production rule manger, production rules are fired and resulted data is updated in database. After updating values in database, event detector checks if updating values satisfies integrity constraints or not. If integrity constraints are violated then event detector sends signals to production rule manager. And, when Rule R10 and Rule R5 are triggered, close/open signals are send to appropriate intelligent switch located in distribution networks.

4 Development of Web Based Power Distribution System

4.1 Initial Man-Machine Interface

In this paper, web based power distribution system is implemented using JAVA, Html, Oracle DBMS.

Target Distribution system is KPECO's Seoul K section 180 distribution network and Initial Man-Machine Interface is as follows in Fig 4.

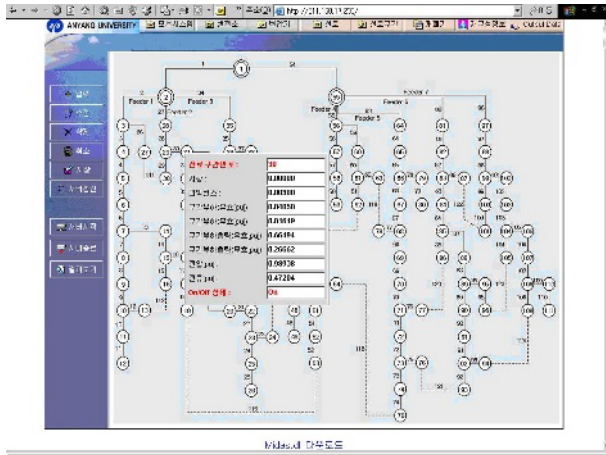


Fig. 4. Example of initial windows application program

4.2 Power Distribution Automation Using Web Based Active Database

If feeder 1 is overloaded to 17[MVA}, Intelligent switch equipped in feeder 1 detect the overloading and send the data to central database. which updates the attribute load of feeder 1. if the overloading exceeds 80% of overload limit then Rule 15 is triggered to activate program Cyclic_Reconfiguration()

After Cyclic_Reconfiguration() is activated, initial on switches { 16, 36, 42, 49, 67, 100} are turned off and Initial off switches { 113, 114, 115, 116, 119, 122} are turned on. Switch status changing triggers Rule 9, Rule 10, Rule 19, Rule 20.

After Switches are activated, feeder reconfiguration are as follows in fig 5.

ID	NAME	TYPE	STATUS
10001	10001	10001	10001
10002	10002	10002	10002

Fig. 5. Reconfiguration information table

5 Conclusion

This paper presents a new Web-based active database architectural design to the distribution automatic system applications. This architecture includes web-based architecture and active database parts. For web based parts, the authors utilize the Java 2 Enterprise Edition architecture for open system, which will easy in the continuing development and maintenance of the software package. Therefore, it is easy to meet open-access competitive market environment. For active database architecture, the author design production rule and production rule manager for DAS feeder automation by utilizing proposed rules, distribution network can be operated reliably with minimum operators intervening

Acknowledgment

The research was supported by the Driving Force Project for the Next Generation of Gyeonggi Provincial Government in Republic of Korea.

References

1. J. Widom, S.Ceri : Active Database Systems : Triggers and rules for Advanced Database Processing. MORGAN KAUFMANN PUBLISHERS
2. E. Baralis, S. Ceri and S.Paraboshi : Compile-Time and Runtime Analysis of Active Behavior. IEEE Trans, On Knowledge and Data Engineering, Vol. 10, No.3, (1998) 353 – 370
3. S.Chen, F.Y. LU : Web-Based Simulations of Power Systems. IEEE Computer Application in Power, January (2002) 35-40

4. J.T. Ma, T. Liu, L.F. Wu : New Energy Management System Architectural Design and Intranet/Internet Applications to Power Systems Conference Proc. Power industry computer application conference. (1995) 207- 212
5. E.Baralis, A.Bianco : Performance Evaluation of Rule Execution Semantics in Active Database. Tech. Rep. DAI.EB. 96.1, Aug. (1996)
6. IEEE Task Force on Power System Control Center Database : Critical Issues Affecting Power System Control Center Database. IEEE Trans. On Power System, vol, 11, no.2 , May (1996)
7. G.S. Martire, D.J.H. Nuttall : Open Systems and Database. IEEE Trans, On Power System, Vol. 8, NO. 2, May. (1993)

Alternative Target Density Functions for Radar Imaging

Askin Demirkol

University of Missouri-Rolla,
Department of Electrical and Computer Engineering,
Rolla MO 65409-0040 USA
demirkol@umr.edu

Abstract. In this paper, three alternative Target Density Functions (TDF) are proposed to image the radar targets. While the target density functions are developed by new techniques, they are obtained by considering a novel range and scanning angle plane different from the conventional methods. Although the imaging techniques are obtained via the linear phased array radars, the problem associated with beam-forming is bypassed in these algorithms.

Keywords: active sensor imaging, SAR-ISAR, phased array radar, target density function, direction density function.

1 Introduction

Target density function(TDF) is the reflectivity of spatially and continuously distributed targets and it is an important characteristic of radar imaging. TDF is known by different names such as ambiguity function, density function, object(target), object reflectivity function, doubly-spread reflectivity function, and reflection coefficient [1, 2, 3, 4, 5, 6].

There are two well known approaches on TDF. First one considers point scatterers reflected off the target scatterer centers. Integration of all point scatterers is able to obtain the whole object. This radar imaging technique is based on inverse Fourier transform(IFT) and used mostly in inverse synthetic aperture radar(SAR) studies [7, 8, 9, 10, 11, 12].

Second method on TDF is a dense target environment approach credited to Fowle and Naparst considering the ambiguity functions with two variables as range and velocity [13, 14]. As an advanced way, Naparst technique measures the the closeness of the targets to each other in a dense target environment rather than typical radar imaging.

In this paper, the radar imaging is studied by three alternative target density functions. In addition to Naparst-Fowle and SAR-ISAR techniques, these functions are inspired by the range-based target density functions [15]. The target density functions are theoretically developed by new approaches on a range-scanning angle plane different from the early approaches. While first technique estimates an alternative target density function, the second technique is developed by a direction density function by considering the targets at a fixed range.

The third one is produced by taking consideration into a new waveform, differently from the others. All of the techniques are developed considering the phase linear array radar system. However, the problem associating with the beamforming is bypassed.

2 Phased Array Radar

Phased array radar system is an advanced radar system, which includes the sensor elements in the system located in an equal distance to each other. All phased arrays operate on the same basic principle of addition in one direction and cancellation in other directions [16, 17, 18].

A general view of a phased array radar system is given in Figure 1. Each sensor element in the array system is equally distanced to each other.

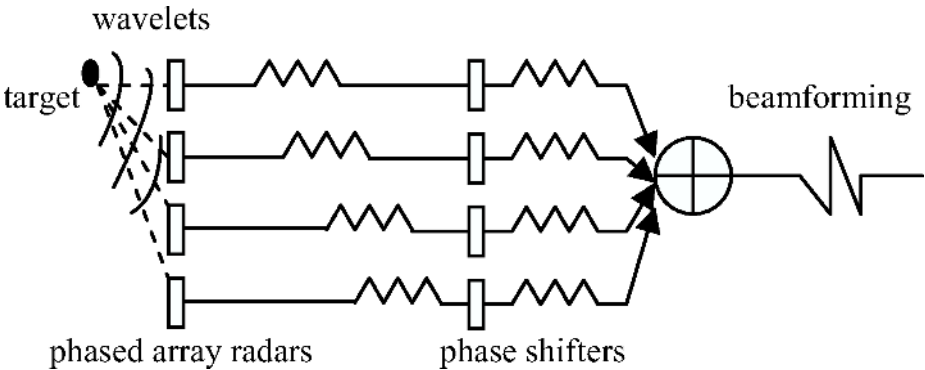


Fig. 1. General view of a phased array radar system

As it can be seen, the waves reflected off the targets are received by the radar system by phase differences. The differences are matched using a phase shifter, then the process is finalized by the beamforming.

If each one of total N element in array is located in equal distance d , each element in the array receive the propagated signal by the phase difference

$$\psi_n = \frac{2\pi}{\lambda} nd \sin\theta, 0 \leq n \leq N \tag{1}$$

As for the beamforming process [16, 17, 18], the radiation pattern with isotropic radiators, as the array factor, $E_a(\theta)$ forms the beam by;

$$\begin{aligned} E_a(\theta) &= [e^{-j(2\pi/\lambda)[(N-1)/2]d \sin\theta}] \frac{1}{N} \sum_{n=0}^{N-1} e^{j(2\pi/\lambda)nd \sin\theta} \\ &= \frac{\sin[N\pi(d/\lambda)\sin\theta]}{N \sin[\pi(d/\lambda)\sin\theta]} \end{aligned} \tag{2}$$

In case of non-isotropic radiation, the radiating element have a radiation pattern $E_e(\theta)$, as a element factor, the complete radiation pattern $E(\theta)$ is the product of the array factor and the element factor:

$$E(\theta) = E_e(\theta)E_a(\theta). \tag{3}$$

3 Preliminaries of Density Functions

In this section, the background of the target density functions consists of the following techniques;

- SAR-ISAR reflectivity functions
- Naparst’s target density functions.

3.1 SAR – ISAR Reflectivity Functions

Synthetic aperture radar(SAR) and inverse synthetic aperture radar (ISAR) are well known radar imaging techniques used for earth surface imaging[19, 20]. However, they have different configuration. In SAR imaging, the radar is flying in space and the object is stationary, while in ISAR imaging, the object is moving and the radar is stationary [7, 9, 10, 21].

ISAR is considered as an inverse Fourier transform(IFT) of a 3-D object on a 2-D [7, 9, 10, 22, 23]. If the target is composed of continuum point targets(scatterers), after demodulation and some pre-filtering processes, by the superposition principle, the echo(reflected signal) $x(t)$, from such a target at x, y points is:

$$x(t) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \rho(x, y)e^{-j2\pi f_0 \frac{2R_p(t)}{c}} dx dy \tag{4}$$

for $2R_p(t)/c \leq t \leq T_{PRI} + 2R_p(t)/c$. Here, $\rho(x, y)$ is the target reflectivity function, T_{PRI} is pulse interval repetition, c is the speed of light, f_0 is carrier frequency, and $R_p(t)$ is the range from the radar to the point-scatterer.

If Inverse Fourier Transform is applied to Equation (4), the image $\rho(x, y)$ is obtained as a 2-D form of 3-D object[7, 9, 10].

$$\rho(x, y) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} X(f_x, f_y)e^{j2\pi(xf_x - yf_y) \frac{2R_p(t)}{c}} df_x df_y \tag{5}$$

where

$$f_x = \frac{2f_0}{c} \cos\theta(t), \quad f_y = \frac{2f_0}{c} \sin\theta(t).$$

3.2 Target Density Functions

First *Density* term related to the target density function is called by Fowle et al [13]. Fowle is focused on the problem of the detection and resolution in two dimensions of a large number of targets in a fixed part of the target space and, he is inspired of ambiguity functions. Then, *Dense target environment* term is used

by Naparst’s paper [14] by taking advantage of Fowle work. His new approach is based on ambiguity and cross-ambiguity functions. In this work, the dense-target environment is defined the closeness of a lot of targets at a distance, which their velocities are so close to each other.

Definition by Naparst, density of targets at distance x and velocity y is $D(x, y)$. In this case, the echo or the reflected signal from targets is

$$e(t) = \int_0^\infty \int_{-\infty}^\infty D(x, y)\sqrt{y}s(y(t - x))dxdy \tag{6}$$

In this approach, it is assumed that all targets are illuminated equally. As stated, the target density function is a function of the range and velocity variables similar to the ambiguity functions.

Reconstruction of the target density function in Naparst algorithm is finalized as fallows(see Ref [14] for the details);

$$D(x, y) = \sum_{n,m=0}^\infty \langle e_n, s_m \rangle A_{nm}(x, y) \tag{7}$$

where s_m are signals sent out and e_n are their echoes. The cross-ambiguity function of the signals sent out (s_1, s_2, \dots) is

$$A_{nm}(x, y) = \int_{-\infty}^\infty s_n(y(t - x))\bar{s}_m(t)dt. \tag{8}$$

4 Active Sensor Imaging by Alternative Target Density Functions

In this paper, three alternative target density functions(TDF) are studied for active sensor imaging, which is based on a linear phased array radar system and the range-scanning angle. New target density function, $g(R, \beta)$ is composed of two variables as the range R , and the scanning angle β . It is considered as below.

Definition 1. Target Density Function is the limit of the ratio of the amplitude of the signal reflected from an infinitesimally neighborhood about the point (R, β) to the amplitude of the incoming signal.

By this definition, the new target density function $g(R, \beta)$ is;

$$g(R, \beta) = \lim_{d(\Omega) \rightarrow 0} \frac{A_r}{A_t} \tag{9}$$

where $d(\Omega)$ is the diameter of the disc about the point $(R, \beta) \in \Omega$, A_r and A_t are the amplitudes of the reflected and the transmitted signals, respectively. In this definition, the target density function(TDF) is relevant to the the reflectivity of spatially, continuously distributed targets.

As target plane, the following Figure 2, is considered for both methods. Where β is $\cos\theta$ and R is the range from the target to the radar.

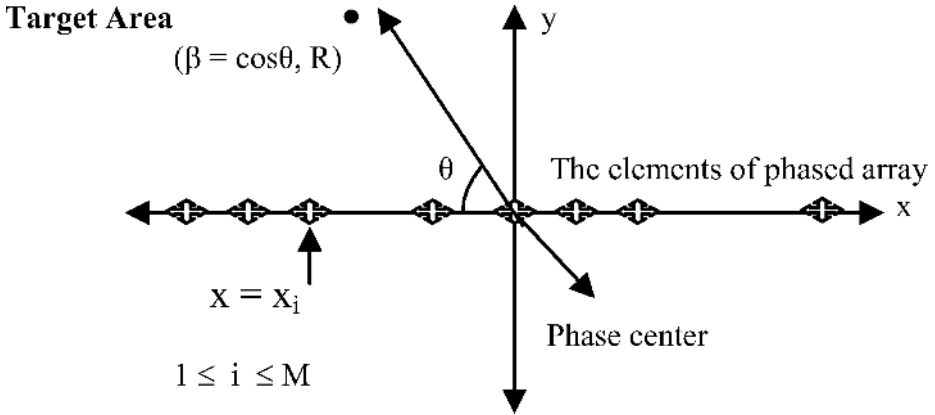


Fig. 2. Phased array imaging

As can be seen in Figure 2, the target density function is a function of the spatial coordinates (R, β) in the upper semi-plane.

Considering the pre-information above, the alternative target density functions are developed in sections 4.1, 4.2 and 4.3 respectively.

4.1 Radar Imaging by Range-Direction Target Density Function

In this section, first target density function called range-direction density function is estimated by a novel method below.

Let $P(t)$ be any periodic function of time, such as a train of pulses, where

$$p(t) = \sum_{k=-\infty}^{\infty} \alpha_k e^{jk\omega_0 t} \tag{10}$$

$$\omega_0 = 2\pi \times \text{PRF}, \tag{11}$$

where PRF is the pulse repetition frequency.

$$s_c(t) = e^{j\omega_c t} \tag{12}$$

Where $s_c(t)$ is the carrier signal.

$$s_m(t) = p(t)s_c(t) \tag{13}$$

Where $s_m(t)$ is the modulated signal.

The reflectivity of one point at $g(R, \beta)$

$$y(x, t) = s_m(t - 2R/c - \beta x/c)g(R, \beta) \tag{14}$$

Let generalize (14) to the whole radar-target semi upper plane by superposition principle;

If $g(R, \beta)$ is the reflectivity of the point (R, β) , and R_1 is the maximum range of interest target area; then

$$\begin{aligned}
 y(x, t) &= \int_{-1}^1 \int_0^{R_1} s_m(t - 2R/c - \beta x/c) g(R, \beta) dR d\beta \\
 &= \int_{-1}^1 \int_0^{R_1} p(t - 2R/c - \beta x/c) e^{-j\omega_c(2R/c - \beta x/c)} e^{j\omega_c t} g(R, \beta) dR d\beta \tag{15}
 \end{aligned}$$

where $y(x, t)$ is the output of the sensor located at center (the feature space), and c is the speed of light.

The algorithm is as follows,

$$y(x, t) = \sum_{k=-\infty}^{\infty} \alpha_k e^{j(\omega_c + k\omega_0)t} \int_{-1}^1 \int_0^{R_1} e^{-j(\omega_c + k\omega_0)2R/c} e^{-j(\omega_c + k\omega_0)\beta x/c} g(R, \beta) dR d\beta \tag{16}$$

Then, demodulation of the equation (16) via

$$s_d(t) = e^{-j(\omega_c + k\omega_0)t} \tag{17}$$

yields

$$Y(k, x) = \int_{-1}^1 \int_0^{R_1} e^{-j(\omega_c + k\omega_0)2R/c} e^{-j(\omega_c + k\omega_0)\beta x/c} g(R, \beta) dR d\beta \tag{18}$$

for each k and β , let be $G(k, \beta)$

$$G(k, \beta) = \int_0^{R_1} g(R, \beta) e^{-j(\omega_c + k\omega_0)2R/c} dR \tag{19}$$

Hence for each fixed k and β we obtain

$$Y(k, x) = \int_{-1}^1 G(k, \beta) e^{-j(\omega_c + k\omega_0)\beta x/c} d\beta \tag{20}$$

If this equation is considered as the following,

$$Y_k(x) = \int_{-1}^1 G_k(\beta) e^{-j(\omega_c + k\omega_0)\beta x/c} d\beta \tag{21}$$

If there are N sensors, each located at $x = x_i$, this gives us the inner product of $G_k(\beta)$ with

$$a_i(\beta) = e^{-j(\omega_c + k\omega_0)\frac{x_i}{c}\beta} \tag{22}$$

This enables us estimate $G_k(\beta)$ as

$$G_k(\beta) \cong \sum_{k=-\infty}^M b_i a_i(\beta) \tag{23}$$

for some constants b_i .

Then, if let the equation (19), consider as a

$$G_k(\beta) = G(k, \beta) = \int_0^{R_1} g(R, \beta) e^{-j(\omega_c+k\omega_0)2R/c} dR \tag{24}$$

Let consider it as a Fourier series as the following.

$$g(R, \beta) = \sum_{k=-\infty}^{\infty} G_k(\beta) e^{j(\omega_c+k\omega_0)2R/c} \tag{25}$$

If we change k , $-N \ll k \ll N$, (N and ω_c are chosen such that $\omega_c \cong N\omega_0$), for each fixed β we obtain the trigonometric Fourier series of $g(R, \beta)$ with respect to the variable R . Hence we estimate $g(R, \beta)$ (we obtain $2N + 1$ terms) as,

$$g(R, \beta) \cong \sum_{k=-N}^N G_k(\beta) e^{j(\omega_c+k\omega_0)2R/c} \tag{26}$$

Thus, by using a novel target density function $g(R, \beta)$, the desired radar targets can be imaged.

As realized that although a phased array radar system is used during the estimation of TDF, the problem associated with beamforming is bypassed.

4.2 Radar Imaging by Direction Density Function

Here, a different case of the first method is proposed with the same background. Second target density function called *direction density function* is derived from the range-direction density function in the section 4.1. It is calculated in the following steps.

Let us consider the same steps up to Equation 16 in section 4.1;

$$y(x, t) = \sum_{k=-\infty}^{\infty} \alpha_k e^{j(\omega_c+k\omega_0)t} \int_{-1}^1 \int_0^R e^{-j(\omega_c+k\omega_0)2R/c} e^{-j(\omega_c+k\omega_0)\beta x/c} g(R, \beta) dR d\beta \tag{27}$$

Then, demodulation of the equation 27 via $\frac{1}{\alpha} e^{-j(\omega_c+k\omega_0)t}$ yields

$$y_k(x) = \int_{-1}^1 \int_0^R e^{-j\omega_c \frac{2R+\beta x}{c}} e^{-jk\omega_0 \frac{2R+\beta x}{c}} g(R, \beta) dR d\beta \tag{28}$$

Now, the second target density function called *direction density function (DDF)* is taken as below by considering Definition 1 and Figure 2.

Definition 2. In a linear phased array of point sensor system, if β is the direction cosine of the line joining the point and the phase center, the direction density function (DDF) $g(\beta)$, is the reflectivity of the point at a fixed range, R , from the phase center of a linear array in the direction.

By this definition, $g(\beta)$ represents the values of the reflectivity as a function of the direction at the fixed range, R . Hence it represents the image.

Let us formulate this definition. The direction density function $g(R, \beta)$ at a fix range $R = R_0$,

$$g(R, \beta)_{R=R_0} = g(\beta) = g_R(\beta) \tag{29}$$

Thus, Equation 28 continues as follows

$$y_k(x) = \int_{-1}^1 e^{-j\omega_c \frac{\beta x}{c}} e^{-jk\omega_0 \frac{\beta x}{c}} g(\beta) d\beta \tag{30}$$

The additional delay term of $2R/c$ due to the round trip is omitted simplicity. Then,

$$y_k(x) = \int_{-1}^1 e^{-j(k\omega_0 + \omega_c) \frac{\beta x}{c}} g(\beta) d\beta \tag{31}$$

This final equation is a slightly modified form of Fourier transform. If inverse Fourier transform is applied in a similar way, the desired target density function

$$g(\beta) = \int_{-\infty}^{\infty} y_k(x) e^{j(k\omega_0 + \omega_c) \frac{\beta x}{c}} dx \tag{32}$$

which is desired function which is capable of imaging the objects.

4.3 Alternative Range-Direction Target Density Function

In this section, the third target density function is proposed by a new approach compared to the first and second ones. This target density function is generated by a new waveform considering the basic principles in the first technique.

Let consider Figure 2 with linear phased array radar system and let $W(t)e^{j\omega_c t}$ be the modulated signal transmitted in the β direction for a range R . The total reflected incoming signal to the phase center will be

$$y(x, t) = \int_{-1}^1 \int_0^{R_1} e^{j\omega_c(t-2R/c-\beta x/c)} W(t-2R/c-\beta x/c) g(R, \beta) dR d\beta \tag{33}$$

Then,

$$y(x, t) = \int_{-1}^1 \int_0^{R_1} e^{j\omega_c t} e^{-j\omega_c(2R/c+\beta x/c)} W(t-2R/c-\beta x/c) g(R, \beta) dR d\beta \tag{34}$$

If Equation 34 is demodulated by $e^{-j\omega_c t}$

$$y(x, t) = \int_{-1}^1 \int_0^{R_1} e^{-j\omega_c(2R/c+\beta x/c)} W(t-2R/c-\beta x/c) g(R, \beta) dR d\beta \tag{35}$$

Equation 35 is a slightly modified form of Fourier transform. Thus, the target density function $g(R, \beta)$ can be obtained similar to the inverse Fourier transform as

$$g(R, \beta) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} y(x, t) e^{j\omega_c(2R/c+\beta x/c)} W^*(t-2R/c-\beta x/c) dx dt \tag{36}$$

which is desired result. As notified, the problem associated with beamforming is bypassed during in the developing of the third density function as well.

5 Summary and Conclusion

In this paper, three alternative target density functions (TDF) were obtained by new algorithm and techniques differently from the conventional approaches. Main contributions of this study ;

- *First target density function algorithm:* An alternative target density function (TDF) was estimated considering a novel range and scanning angle plane.
- *Second target density function algorithm:* A new target density function called the direction density function was proposed by considering the range-direction density function.
- *Third target density function algorithm:* An alternative target density function is proposed by choosing an alternative waveform.
- *Bypassing the beam-forming problem:* While all techniques were generated via by the phased array radar, the problem associated with beamforming is bypassed.

The present TDF is generated partly by analogy to Fowle-Naparst and SAR-ISAR approaches.

- *Comparing to Fowle-Naparst:* As an advanced work of Fowle, Naparst target density function is developed for a high dense target environment with multiple targets, whose velocities are close to each other. This TDF acts like a separator rather than an imaging function for the targets at the distance with a given velocity.
- *Comparing to ISAR:* While ISAR imaging based on multi-aperture principle [24] and the integration of the point scatterers on the target, the proposed target density functions were produced by the integration of scanning angles and ranges.

Acknowledgement. I would like to thank Dr.Erol Emre of Sakarya University for helpful discussions.

References

1. Wald, L.: “Some terms of reference in data fusion,” IEEE Transactions on geoscience and remote sensing, v.37, no.3 May (1999) 1190–1193
2. Sarma, V.V.S., Raju, S.: “Multi-sensor data fusion and decision support for airborne target identification,” IEEE Transactions on systems, man, and cybernetics, v.21 no.5 (1991)
3. Zhou, Y.T.: “Multi-sensor image fusion,” Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference, v.1 13-16 November (1994) 193–197
4. Durrant-Whyte, H.F.: “elements of sensor fusion,” Intelligent Control, IEE Colloquium on, 19 Febuary (1991) 5/1–5/2
5. Varshney, P.K.: “multi-sensor data fusion,”electronics and communication engineering journal, December (1997)

6. Hall, D.L., Llinas, J.: "An Introduction to multi-sensor data fusion," Proceedings of the IEEE, vol.85 Issue.1 January (1997) 6–23
7. Chen, V.C., Ling, H.: Time-Frequency transforms for radar imaging and signal analysis,(2002)
8. Odendaal, J.W.: "2-D Radar Imaging," Communications and Signal Processing, 1994. COMSIG-94., Proceedings of the 1994 IEEE South African Symposium on, 4 October (1994) 146–151
9. Prickett, M.J.: "Principles of inverse synthetic aperture radar(ISAR) imaging," IEEE EASCON, (1980) 340–344
10. Ausherman, D.A., Kozma, A., Walker, J., Jones, H.M., Poggio, E.C.: "Developments in radar imaging," IEEE Transactions on Aerospace and Electronic Systems, v.20, no.4 (1984) 363–400
11. Woodward, P.M.: Probability and information theory with applications to radar,(1957)
12. Siebert, W.McC.: "A radar detection philosophy," IEEE Transactions on Information Theory v.2 Issue.3 September (1956) 204–221
13. Fowle, E.N., Kelly, E.J., Sheehan, J.A.: "Radar system performance in a dense-target environment," IRE Int.Convention record no.4 (1961) 136–145
14. Naparst, H.: "Dense target signal processing," IEEE Transactions on information theory v.37 no.2 March (1991) 317–327
15. Demirkol, A., Demir, Z., Emre, E.: "Estimation of target density function by a new algorithm", Second international image analysis and recognition conference September (2005), Toronto, Canada
16. Skolnik, M.I.: Introduction to radar systems, 1980.
17. Pell, P.: "Phased array radars," IEE Review, v.34 Issue.9 6 October (1988) 363–367
18. Van Veen, B.D., Buckley, K.M.: "Beamforming: A versatile approach to spatial filtering," ASSP Magazine, IEEE(also IEEE Signal Processing Magazine) vol.5 Issue.2 April (1988) 4–24
19. Hovanessian, S.A.: Introduction to synthetic array and imaging radars, Artech House, (c1980)
20. Birk, R., Camus, W., Valenti, E.: "Synthetic aperture radar imaging systems," Aerospace and Electronic Systems Magazine, IEEE v.10 Issue.11 November (1995) 15–23
21. Watts, S.: "Synthetic aperture techniques," Digital Signal Processing for Radar and Sonar Applications, Tutorial Meeting on, September 12 (1990) 7/1–7/22
22. Chen, V.C. Qian, S.: "Time frequency transform vs. fourier transform for radar imaging," Time-Frequency and Time-Scale Analysis, 1996., Proceedings of the IEEE-SP International Symposium on, 18-21 June (1996) 389–392
23. Krone, A.W., Munson, D.C.: "A Fourier model of ISAR imaging of approaching targets", Acoustics, Speech, and Signal Processing, 1992. ICASSP-92., 1992 IEEE International Conference on, v.3, 23-26 March (1992) 13–16
24. Chen, V.C., Lipps, R., Bottons, M.: "Radar imaging of ground moving targets", Radar Conference, 2001. Proceedings of the 2001 IEEE , 1-3 May (2001)-(2002) 426–431

A Novel Image Restoration Algorithm Based on High-Dimensional Space Geometry

Wenming Cao^{1,2}, Mei-fen Xie¹, and Shoujue Wang²

¹ Institution of Intelligent Information system, College of Information of Engineering, Zhejiang University of Technology, Hangzhou 310014, China

² Institute of semiconductors of Chinese Academy of Science, Beijing 100083, China
csann@zjut.edu.cn

Abstract. A novel image restoration approach based on high-dimensional space geometry is proposed, which is quite different from the existing traditional image restoration techniques. It is based on the homeomorphisms and “Principle of Homology Continuity” (PHC), an image is mapped to a point in high-dimensional space. Begin with the original blurred image, we get two further blurred images, then the restored image can be obtained through the regressive curve derived from the three points which are mapped from the images. Experiments have proved the availability of this “blurred-blurred-restored” algorithm, and the comparison with the classical Wiener Filter approach is presented in final.

1 Introduction

An image may be degraded by various factors in the process of acquisition, transmission, storage and processing. The task of image restoration is to remove these degradations to enhance the quality of the image for further use in domain applications such as image analysis, recognition and comprehension. Image restoration attempts to reconstruct or recover a degraded image by using a priori knowledge of the degradation phenomenon. Considerable studies have been carried out in the past years, proposing various techniques based on space domain and frequency domain [1][2][3]. Most traditional image restoration approaches restore images by deconvolution, however, if there exist “ill-problems” in the process of deconvolution, such as singular problem or multiple solutions, those existing classical approaches couldn’t solve problems perfectly. Especially in most conditions, the degradation modal is unknown or imprecise estimated, thus blocks the restoration for lacking of priori knowledge [1][2][3]. The great development of neural network theories in recent years, has provided a new approach to the image restoration [4][5], and such as image restoration using a modified Hopfield network has gained good effect [5], but its disadvantage of time and space complexity as well as time-consuming in the network learning and training is also a limitation.

Since form Academician Wang Shoujue presented high-dimensional space geometry method [6][7][8][9][10], and widely applied it to pattern recognition,

such as multi-camera human-face personal identification [7], omnidirectional oriented rigid objects recognition [7], continuous speech research [8] and so forth, have all gained better effects than the existing traditional methods. This paper proposed a novel image restoration approach based on point location in high-dimensional space geometry. It is quite different from the existing traditional image restoration techniques. An image is mapped to a point in high-dimensional space. Begin with the original blurred image, we get two further blurred images, then the restored image can be obtained through the regressive curve derived from the three points which is mapped from the images. Experiments have proved the availability of this “blurred-blurred-restored” algorithm in final.

2 Model of the Image Degradation

In digital image processing, discrete model for a linear degradation caused by blurring and additive noise can be given by the following equation:

$$g(x, y) = f(x, y) * h(x, y) + n(x, y) \quad (1)$$

Where $f(x, y)$ represents an original image, and $h(x, y)$ is the point spread function (SPF), $n(x, y)$ represents an additive noise introduced by the system, $g(x, y)$ represents the degraded image which is acquired by the imaging system. The degradation process is showed in Fig. 1,

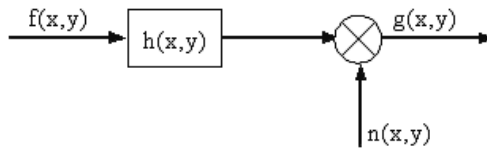


Fig. 1. Scheme of the degradation modal

In our experiments, for simplicity, the additive noise effect is not considered temporarily, then Equation(1) can be rewritten as follow:

$$g(x, y) = f(x, y) * h(x, y) \quad (2)$$

Photographic defocusing is a problem in many different imaging situations. This type of blurring is primarily due to effects at the camera aperture that result in the spreading of a point of incoming light across a circle of confusion. The following equations have been used as approximations of this kind of PSF [1].

- Uniform Out-of-Focus Blur: It models the simple defocusing found in a variety of imaging systems as a uniform intensity distribution within a circular disk,

$$h(x, y) = \begin{cases} \frac{1}{\pi r_0^2} & \sqrt{x^2 + y^2} \leq r_0 \\ 0 & \text{otherwise} \end{cases} \quad (3)$$



Fig. 2. (a) Original “lenna” (155×166); (b) Degraded by a 5×5 Uniform 2-D Blur

• Uniform 2-D Blur: A more severe form of degradation that approximates an out-of-focus blur, and is used in many research simulations. This is the model for the blur used in the examples throughout this article,

$$h(x, y) = \begin{cases} \frac{1}{(L)^2} & \text{if } -\frac{L}{2} \leq x, y \leq \frac{L}{2} \\ 0 & \text{otherwise} \end{cases}. \quad (4)$$

3 Image Quality

In applications of image restoration, image quality usually refers to the image’s fidelity to its original. There exist two kinds of criterions of image quality: Difference Measure and Correlation Measure.

In our experiments, we consider the ISNR (signal-to-noise -ratio) which is a kind of Correlation Measure as the criterion to evaluate restoration performance:

$$M = 10 \log \frac{\sum \sum [g(i, j) - f(i, j)]^2}{\sum \sum [\hat{f}(i, j) - f(i, j)]^2} \quad (5)$$

Where $f(i, j)$, $g(i, j)$, $\hat{f}(i, j)$, are the original image, the degraded image and the restored image, respectively.

4 Image Restoration Approach Based on High-Dimensional Space Geometry

4.1 Principle of the Algorithm

Definition 1. If X and Y are topological spaces, a Homeomorphism from X to Y is defined to be continuous bijective map $f : X \rightarrow Y$ with continuous inverse. If there exists a homeomorphism between X and Y , we say that X and Y are homeomorphic or topologically equivalent. It can be abbreviated $X \approx Y$ [11].

Lemma 1. Suppose set $A = \{[a(x)_{i,j}]_{M \times N} | 1 \leq x \leq n\}$, where $[a(x)_{i,j}]_{M \times N}$ is a $M \times N$ gray scale matrix, and $a(x)_{i,j} \in [1, 255]$, $a(x)_{i,j} \in \mathbb{Z}$, set $B = \{b(y) | 1 \leq y \leq n\}$ where $b(y)$ is an array with dimension of $M \times N$, and $b(y)_k = a(x)_{i,j}$, then $A \approx B$.

Proof: define $f : A \rightarrow B$ as: for arbitrary $[a(x)_{i,j}]_{M \times N} \in A$, there always exists $f([a(x)_{i,j}]_{M \times N}) = \{b(y)_k | b(y)_k = a(x)_{i,j}, k = (j - 1) \times M + 1, 1 \leq i \leq M, 1 \leq j \leq N, x = y\}$. Then f is homeomorphism, $A \approx B$.

Definition 2. If we degrade image A by convoluting a PSF, and get image B . Then we say image B is the blurred image of image A , written: $B \xleftarrow{\text{blur}} A$, and image A is the deblurred image of image B , written: $B \xrightarrow{\text{clear}} A$

Definition 3. If $C \xleftarrow{\text{blur}} B \xleftarrow{\text{blur}} A$, then write the blurred direction as \overline{ABC} , oppositely, deblurred direction written as \overline{CBA} , as showed in Fig. 3.

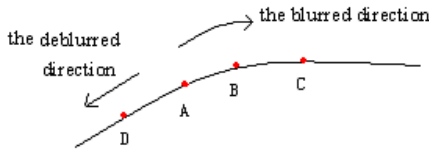


Fig. 3. Map of the directions

Definition 4. Suppose $C \xleftarrow{\text{blur}} B \xleftarrow{\text{blur}} A$, we call C, B are homologous.

The Principle of Homology Continuity (PHC) of homologous samples can be mathematically described as follow:

In the feature space R^n , suppose that set A be a point set including all samples in class A . For if $x, y \in A$ and $\varepsilon > 0$ are given, there must be set F

$$F = \{x_1, x_2, \dots, x_n | x_1 = x, x_n = y, n \subset N, \rho(x_m, x_{m+1}) < \varepsilon, \varepsilon > 0, n - 1 \geq m \geq 1, m \subset N\}, F \subset S$$

Easy to see that several homologous images distribute sequentially and gradually in high-dimensional space

4.2 Distribution of Points in High-Dimension Space

Suppose $X_1(x_1, x_2 \dots x_k), Y_1(y_1, y_2 \dots y_k)$ are two points of high-dimensional space, then the line which is fixed by the two points can be written as follow equation:

$$Y = Y_1 + \lambda(Y_1 - X_1) \text{ where } \lambda = \frac{\|Y Y_1\|}{\|Y_1 X_1\|} \tag{6}$$

Suppose $A(x_1, x_2 \dots x_k), B(y_1, y_2 \dots y_k), C(z_1, z_2 \dots z_k)$ are points of high-dimensional space, then the curve which is fixed by these points can be written approximately as follow equation:

$$D = \alpha A + \beta B + \gamma C \tag{7}$$

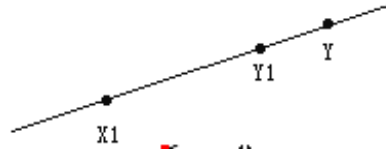


Fig. 4. Line in high-dimensional space

Where α, β, γ are constant coefficients, take $\alpha > 0, \beta < 0, \gamma > 0$ in our experiment, and these three coefficients must satisfy $\alpha + \beta + \gamma = 1$ to keep the gray scale of image invariable.

Equation (7) also can be written as:

$$D = A + k_1(B - A) + k_2(C - A) \tag{8}$$

Where $k_1 < 0, k_2 > 0$. Compare Equation (7) with Equation (8), we can easily find following relationship between them: $\alpha = (1 - k_1 - k_2), \beta = k_1, \gamma = k_2$

Note that the point D deduce from Equation (7) or (8) is guaranteed to be in the plane which is determined by point A and point B. And the solution is unique determined.

Suppose $k_1 = -0.8, k_2 = 0.3$, as showed in Fig. 5. We can adjust the value of k_1, k_2 to find a satisfied point D.

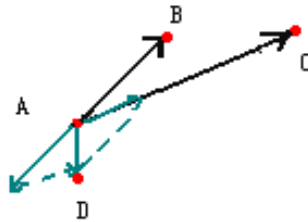


Fig. 5. Distribution of points in high-dimensional space

4.3 Algorithm

The “blurred-blurred-restored” algorithm process is described as following steps:

- Step 1.** Get the original blurred image A, then map A to F1, where $A \approx F1$.
- Step 2.** Get a further blurred image B1, where $B1 \xleftarrow{\text{blur}} A$, then map B1 to F2, where $B1 \approx F2$.
- Step 3.** Get a further blurred image C1, where $C1 \xleftarrow{\text{blur}} B1$, then map C1 to F3, where $C1 \approx F3$.
- Step 4.** Chose proper coefficients k_1, k_2 , obtain the first restored image D1, $A \xrightarrow{\text{clear}} D1$

Step 5. Replace A with D1, return to Step 2

Step 6. Stop the iteration until observe the satisfy image. Fig. 6 is the scheme of algorithm process.

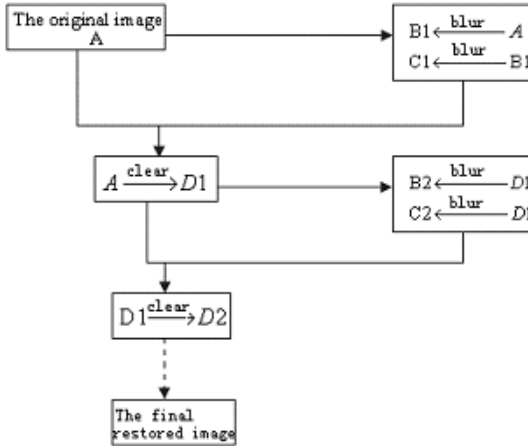


Fig. 6. Scheme of algorithm process

As the iteration goes on, restored image will be clearer than the last restored image, and the value of ISNR M will reduce each time, $M_1 > M_2 > \dots > M_k$, thus we can achieve the most clear image at last.

5 Experimental Results and Analysis

Experiments have been carried out to test the performance of the proposed algorithm. One of the experiment results is showed in Fig. 7.

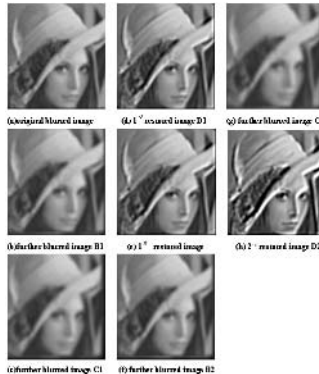


Fig. 7. Partial of the restore process with precise PSF

In Fig. 7,(a)-(b)-(c)-(d) denotes the first iterative restoration. (a) is the original blurred image “lenna” of size 155×166 , (b) is the degraded image of (a) with 5×5 Uniform 2-D Blur, (c) is a further blurred image of (b) with the same PSF, as showed in Fig. 7, we can see the first iterative restored image (d) is much clear than (a), and the second iterative restored image (h) also is clear than (d).

Fig. 8 showed us a restoration with an imprecise PSF. That is to say we use a PSF in restoration that is different from the PSF in the degradation. (a) is the original blurred image “lenna” of size 155×166 , which is blurred by 5×5 Uniform 2-D Blur, while (b) is a further blurred image of image(a) with 5×5 Uniform Out-of-Focus Blur. We can see the effect of second iterative restored image (h) in Fig. 8.



Fig. 8. Restoring with imprecise PSF

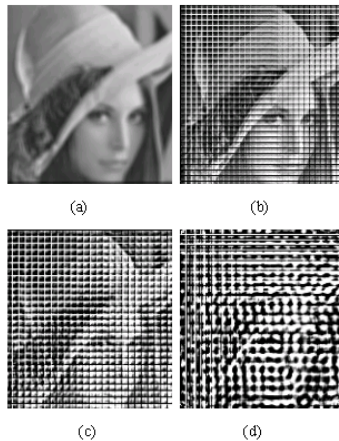


Fig. 9. Restoration of Classical Wiener Filter: ((a) is the original blurred image by a 5×5 Uniform 2-D Blur PSF; (b) is the restored image of (a) through a 5×5 Uniform 2-D Blur PSF; (c) is the restored image of (a) through 6×6 Uniform 2-D Blur PSF; (d) is the restored image of (a) through 5×5 Uniform Out-of-Focus Blur PSF)

The comparison between Fig. 8 and Fig. 9 demonstrate that if imprecise PSF is used in restoration, the proposed algorithm still can perform well, and its restored image is still satisfying. While the Classical Wiener Filter is not the case. The restoration result is satisfying when the estimated PSF is matched to the PSF of degradation, but a bit small variance in the estimated PSF will cause great vision effect, as showed in Fig. 9. We can see the approach presented in this paper is especially suite the situation when PSF in degradation is unable or hard to imprecise estimated.

6 Conclusion

This paper proposed a novel image restoration approach base on high-dimensional space geometry which is quite different from the existing traditional methods. It not only avoids complex mathematical operation such as deconvolution, but also avoids “ill-problems”, especially adapts to the case of PSF in degradation is unable or hard to imprecise estimated. Experiments have proved the availability of this “blurred-blurred-restored” algorithm, and the comparison with classical Wiener Filter also shows its superiority. In addition, this approach is also worth of further research in colour image restoration or blind image restoration. This high-dimensional space geometry method presented by Academician Wang Shoujue, provide another different way to solve problems in digital image processing , and it is expected for more people’s dedicating.

References

1. Banham,M., Katsaggelos,A.: Digital image restoration. IEEE Signal Processing Magazine. **24241** (1997) 24–38
2. Rafael, C.Gonzalez, Richard, E.Woods: Digital Image ProcessingSecond Edition. BeijingPublishing House of Electronics. **7** (2002) 175–216
3. Sun Jixiang: Image Processingin Chinese. Beijing: Publishing House of Science. **9** (2004) 201–250
4. Y.-T.Zhou, R.Chellappa, A.Vaid, and B.K.Jenkins: Image restoration using a neural network. IEEE Trans. Acoust. Speech. Signal Processing. **36** (1998) 1141–1151
5. J. K. Paik and A. K. Katsaggelos: Image restoration using a modified Hopfield network. IEEE Trans. Image Processing. **1** (1992) 49–63
6. WANG Shou-jue: Biomimetic(Topological) Pattern RecognitionDDA New Model of Pattern Recognition Theory and Its applicationsin Chinese. Chinese Journal of Electronics. **30** (2002) 1417–1420
7. WANG Shou-jue, XU Jian, WANG Xian-Bao, QIN Hong: Multi-Camera Human-Face Personal Identification System based on the BIOMIETIC PATTERN TRCOGNITIONin Chinese. Chinese Journal of Electronics. **31**(2003) 1–4
8. Wenming Cao, Xiaoxia Pan, Shujue Wang: Continuous Speech Research Based on Two-Weight Neural Network. Advances in Neural Networks-ISNN 2005:Second International Symposium on Neural Networks. Lecture Notes on Computer Science. **3497** (2005) 345–350

9. Shoujue Wang: Computational Information Geometry and its Applications. Keynote Speech for the second International Conference on Neural Networks and Brain. Proceedings of 2005 internal conference on neural networks and brains. Beijing . China. **1**(2005) 63–69
10. WANG Shoujue, CAOYu, HUANG Yi: A Novel Image Restoration Approach Based on Point Location in High-dimensional Space Geometry. Proceedings of 2005 internal conference on neural networks and brains,Beijing ,China. **3** (2005) 301–305
11. Liu Zhengshuai, Huang Ying ,Ren Zhenzhong: Analysissitus Fundamention (in Chinese). KaiFeng:Publishing House of HeNan University. (1992) 47–51

A Fast Image Retrieval System Based on Color-Space and Color-Texture Features

Chuen-Horng Lin¹, Kai-Hung Chen¹, and Yung-Kuan Chan²

¹ Department of Information Science, National Taichung Institute of Technology,
No. 129, Sec. 3, Sanmin Rd., Taichung, Taiwan, R.O.C.

linch@ntit.edu.tw {C. H. Lin}

fzworld@gmail.com {C. K. Chen}

² Department of Management Information Systems,
National Chung Hsing University,

No. 250, Kuokuang Rd., Taichung, Taiwan, R.O.C.

ykchan@nchu.edu.tw {Y. K. Chan}

Abstract. This paper presents two image features, multi-orientation color complexity (MOCC) and color-space relation (CSR). MOCC refers to the color complexity. CSR concerns the spatial relations of similar color pixels in an image. By combining both features, an image retrieval system was developed. The experimental results revealed that such a system can perform expressively at accurate recognition rate. To further speed up this system, a clustering based filer was applied to quickly sieve out the most unqualified database images.

1 Introduction

The color and texture attributes have been very successfully used in retrieving images with similar feature distributions. However, since these attributes do not describe the spatial distributions of pixel colors in an image, the retrieved results do not often make a lot of sense. For example, above features cannot describe the spatial distributions of the pixel colors in a landscape image with blue sky on the top and green countryside at the bottom. Spatial layout is about the absolute or relative position of color, texture, or shape information. Therefore, the attribute of the spatial relations among objects or pixels is also an important component for image content description and image access. To get the retrieval more accurate, this paper proposes a color-space and color-texture based image retrieval system (CSCT system).

Color histogram [7] is one of the most commonly used color features in color-based image retrieval systems. The advantages of color histogram include simple procedures and quick calculations. In addition, color histogram can resist noise and rotation variations of an image. However, it can state merely the principal colors rather than the texture of the image. Instead, multi-orientation color complexity (MOCC) was presented in depicting the relationship between pixel colors and textures of the image. The spatial distribution of the pixel colors in an image generally contains more meaningful information. To indicate the spatial

distribution of the pixel colors, an image feature color-spatial relation (CSR) is presented.

As a scanned query image Q into the system, this system compares the feature values of the query image with those of the pre-feature-extracted images in database. The database images that are the closest to Q are delivered to the user. The MOCC and CSR can characterize different properties of an image. To increase the performance of an image retrieval system, both features were integrated to develop CSCT system. The image properties as color, texture, and space relations are integrated into this image retrieval system. Besides, a clustering based filter using the CSR feature is proposed to accelerate execution of this system.

2 Multi-orientation Color Complexity

Two image features are studied in this paper: MOCC and CSR. MOCC describes the relationship between pixel colors and textures of an image while the CSR represents the spatial distributions of similar pixel colors in an image. Both features have their own distinguishable characteristics. MOCC is introduced in this section. CSR is detailed in the next section.

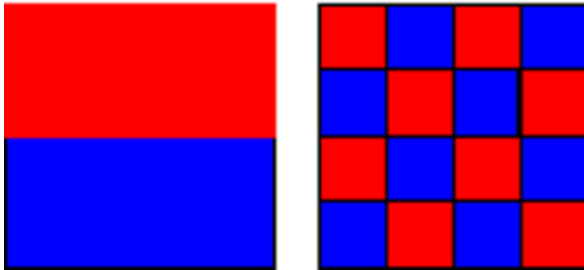


Fig. 1. Two images with the same color histogram but different

Let $G(x, y) : N_x \times N_y \rightarrow Z$ be the gray levels of an $N_x \times N_y$ image I , and $Z = \{0, 1, \dots, 255\}$. The $G(x, y)$ of each pixel $P(x, y)$ in I corresponds to a grey level difference $\nabla G(x, y)$ related to $(\delta x, \delta y)$, where $P(x, y)$ is located at the coordinates (x, y) . $(\delta x, \delta y)$ is the displacement vector specifying the relative position of the pixels $P(x, y)$ and $P(x + \delta x, y + \delta y)$. $\nabla G(x, y)$ is defined as:

$$\nabla G(x, y) = |G(x + \delta x, y + \delta y) - G(x, y)|.$$

$NP(\delta x, \delta y, g, \nabla)$ is a function the number of pixels $P(x, y)$'s in I , where $g = G(x, y)$ and $\nabla = \nabla G(x, y)$. $GD_{\delta x, \delta y}$ is a 256×256 matrix. Cell $GD_{\delta x, \delta y}[i, j] = NP(\delta x, \delta y, i, j)$ gives the number of pixels for $i = G(x, y)$ and $j = |\nabla G(x, y)|$. $GD_{\delta x, \delta y}[i, j]$ and $NP(\delta x, \delta y, g, \nabla)$ hence counts the pixel number of those $P(x, y)$ with gray-level g and ∇ (the grey level difference between $P(x, y)$ and $P(x + \delta x, y + \delta y)$). Let $MOCC_{\delta x, \delta y}$ be the $1 \times K_1$ matrix which is the MOCC of I on $(\delta x, \delta y)$. $MOCC_{\delta x, \delta y}$ splits $NP_{\delta x, \delta y}$ into K_1 groups. The element $MOCC_{\delta x, \delta y}[k]$

describes the mean, standard deviation, and skewness of the k -th group of $NP_{\delta_x\delta_y}$, notated by $MOCC_{\delta_x\delta_y}^\mu[k]$, $MOCC_{\delta_x\delta_y}^\sigma[k]$, and $MOCC_{\delta_x\delta_y}^S[k]$. For $k = 0, 1, \dots, K_1 - 1$,

$$MOCC_{\delta_x\delta_y}^\mu[k] = \frac{1}{\frac{256}{K_1} \times 256} \sum_{i=0}^{\frac{256}{K_1}-1} \sum_{j=0}^{255} GD_{\delta_x\delta_y}[k \times \frac{256}{K_1} + i, j],$$

$$MOCC_{\delta_x\delta_y}^\sigma[k] = \sqrt{\frac{1}{\frac{256}{K_1} \times 256} \sum_{i=0}^{\frac{256}{K_1}-1} \sum_{j=0}^{255} \{GD_{\delta_x\delta_y}[\frac{256k}{K_1} + i, j] - MOCC_{\delta_x\delta_y}^\mu[k]\}^2},$$

$$MOCC_{\delta_x\delta_y}^S[k] = \frac{1}{\frac{256}{K_1} \times 256} \sum_{i=0}^{\frac{256}{K_1}-1} \sum_{j=0}^{255} \left\{ \frac{GD_{\delta_x\delta_y}[k \times \frac{256}{K_1} + i, j] - MOCC_{\delta_x\delta_y}^\mu[k]}{MOCC_{\delta_x\delta_y}^\sigma[k]} \right\}^3.$$

The mean $MOCC_{\delta_x\delta_y}^\mu[k]$ is the average number of pixels at each gray-level in the interval between $\frac{256k}{K_1}$ and $\frac{256(k+1)}{K_1-1}$. The standard deviation $MOCC_{\delta_x\delta_y}^\sigma[k]$ describes the variation of the gray-level differences of those pixels with color intensities are within the interval of $\frac{256k}{K_1}$ and $\frac{256(k+1)}{K_1-1}$. The skewness $MOCC_{\delta_x\delta_y}^S[k]$ indicates the direction and shifting degree of $MOCC_{\delta_x\delta_y}^\mu[k]$.

The MOOC at specified different pairs (δ_x, δ_y) can describe various textures at different resolutions and in different directions. As $\delta_y=0$, δ_x increases with the lower resolution in 0° direction. At $\delta_x=0$, δ_y raises with the bigger



(a) Some query images



(b) The database images corresponding to the images in Figure 2(a)

Fig. 2. Some of testing images

resolution in 90° direction. Based on different pairs $(\delta x, \delta y)$, one can integrate the different MOCC of an image to more precisely describe the image. Let $MOCC_{\delta_{x1}\delta_{y1}+\delta_{x2}\delta_{y2}+\dots+\delta_{xn}\delta_{yn}}$ be the $1 \times K_1$ matrix which combines $MOCC_{\delta_{x1}\delta_{y1}}$, $MOCC_{\delta_{x2}\delta_{y2}}$, \dots , and $MOCC_{\delta_{xn}\delta_{yn}}$, where

$$MOCC_{\delta_{x1}\delta_{y1}+\delta_{x2}\delta_{y2}+\dots+\delta_{xn}\delta_{yn}}^{\mu}[k] = \frac{MOCC_{\delta_{x1}\delta_{y1}}^{\mu}[k]+MOCC_{\delta_{x2}\delta_{y2}}^{\mu}[k]+\dots+MOCC_{\delta_{xn}\delta_{yn}}^{\mu}[k]}{n},$$

$$MOCC_{\delta_{x1}\delta_{y1}+\delta_{x2}\delta_{y2}+\dots+\delta_{xn}\delta_{yn}}^{\sigma}[k] = \frac{MOCC_{\delta_{x1}\delta_{y1}}^{\sigma}[k]+MOCC_{\delta_{x2}\delta_{y2}}^{\sigma}[k]+\dots+MOCC_{\delta_{xn}\delta_{yn}}^{\sigma}[k]}{n},$$

$$MOCC_{\delta_{x1}\delta_{y1}+\delta_{x2}\delta_{y2}+\dots+\delta_{xn}\delta_{yn}}^S[k] = \frac{MOCC_{\delta_{x1}\delta_{y1}}^S[k]+MOCC_{\delta_{x2}\delta_{y2}}^S[k]+\dots+MOCC_{\delta_{xn}\delta_{yn}}^S[k]}{n}.$$

The performance of these MOCCs will be tested with experiments in this paper.

Table 1. ACC variation with L and different combinations of $(\delta x, \delta y)$ for $K_1 = 16$ and $r_1 = 2$

ACC(%) (δ_x, δ_y) 's \	L	1	2	3	4	5	10	20	30	40
$(1,0)$		65.96	73.05	76.45	79.93	80.90	83.16	87.95	90.06	90.98
$(0,1)$		67.43	75.34	77.28	79.39	80.13	84.18	87.67	89.51	90.62
$(1,1)$		64.95	72.86	76.92	79.02	79.50	83.07	86.20	89.05	90.52
$(1,-1)$		65.05	73.33	76.63	80.40	81.40	83.62	87.03	88.78	90.43
$(1,0)+(0,1)$		67.34	75.44	78.38	79.94	81.69	85.65	88.68	89.88	90.80
$(1,0)+(0,1)+(1,1)$		66.80	73.50	77.60	78.38	80.24	83.64	87.65	89.20	90.80
$(1,0)+(0,1)+(1,-1)$		67.25	74.89	78.01	80.50	81.23	84.36	87.86	89.70	90.98
$(1,0)+(0,1)+(1,1)+(1,-1)$		67.07	74.70	77.92	79.30	80.68	84.36	88.41	89.51	90.89

For a full color image, each pixel consists of color components R, G, and B. During MOCC extraction, the three color components are considered to be independent to each other. Color components R, G and B of each full color image can be converted into three gray-level images, respectively. The MOCC of three-gray-level images are then converted into the MOCC of the color image. Each cell of MOCC contains three values: mean, standard deviation, and skewness. Hence, there are $3 \times 3 \times K_1$ values in MOCC of a color image.

3 Color-Space Relationship

The color and texture attributes had been very successful in retrieving images with similar feature distributions [2, 3, 4, 5]. However, since these attributes do not describe the local properties of an image, the retrieved results often came out nonsense. In this section, as an image feature, the color-space relation (CSR) between the pixel colors and their spatial distributions is discussed. The CSR describes the spatial distribution of similar pixel colors in a color image.

In a full color image, a pixel color is generally described using a 24-bit memory space. There are a total of 2^{24} different possible pixel colors. Before computing

CSR of an image, the pixels of whole the database images are categorized into K_2 clusters using K-means algorithm [6] according to their colors. The mean of all the pixel colors in each cluster is considered to be one color value in a color palette. With K_2 different colors, this color palette is used as the common color palette (CCP) for all images (including all database images and query images).

Table 2. ACC for $K_1 = 16$, $r_1 = 2$, and different combinations of $(\delta x, \delta y)$

$ACC(\%)$ (δ_x, δ_y) 's	L		1	2	3	4	5	10	20	30	40
$(1,0)+(0,1)$	67.34	75.44	78.38	79.94	81.69	85.65	88.68	89.88	90.80		
$(2,0)+(0,2)$	64.95	73.05	77.92	79.39	83.35	87.35	87.67	89.60	90.62		
$(4,0)+(0,4)$	65.96	73.05	75.25	77.00	77.74	81.60	85.74	87.67	89.14		
$(8,0)+(0,8)$	64.58	73.78	76.63	77.83	78.75	82.06	86.11	87.76	89.14		
$(1,0)+(2,0)+(0,1)+(0,2)$	67.99	75.25	78.01	79.21	80.96	84.27	87.76	89.33	90.80		
$(1,0)+(2,0)+(4,0)+$ $(0,1)+(0,2)+(0,4)$	66.15	73.78	76.82	78.29	80.13	84.27	87.03	88.50	89.14		
$(1,0)+(2,0)+(8,0)+$ $(0,1)+(0,2)+(0,8)$	66.42	74.43	78.01	79.12	80.22	82.56	86.38	88.22	89.88		
$(1,0)+(2,0)+(4,0)+(8,0)+$ $(0,1)+(0,2)+(0,4)+(0,8)$	66.40	73.97	76.45	78.66	79.85	82.34	85.92	88.32	89.60		

To extract the CSR of an image I , each pixel color C in I is replaced by the color in CCP that is most similar to C . Every pixel in I was classified into K_2 clusters. Each K_2 cluster consists of similar color pixels. Let (x_i^k, y_i^k) be the coordinates of pixel i in cluster k , and n^k be the number of the pixels in the k th cluster. The CSR of an image I is a K_2 -dimension array with k th element $CSR[k]$ defined as the following:

$$CSR[k] = \frac{\sum_{i=1}^{n^k-1} \sum_{j=i+1}^{n^k} \sqrt{(x_i^k - x_j^k)^2 + (y_i^k - y_j^k)^2}}{n^k}$$

CSR can be used to characterize the spatial distribution of similar color pixels in an image. With similar color histograms, one image has most of pixels with homologous colors scattered over the whole image, while other image has most of pixels of the analogous colors gathering in some small regions. Figure 1 shows such two images of similar pixel color histograms but different spatial distributions. Undistinguishable with color histogram method, these two images can be discerned by their CSR.

4 Image Retrieval System

Regardless the shift variation influence of objects [1], MOCC is useful to describe the relationship between the color and texture of an image. However, it is sensitive to the noise variation [1] in images. Given the spatial information of an image, CSR is highly tolerant to the noise variants, but is also easily affected by shift variation of objects. Due to significantly complementary, these two features are integrated to establish a color-space and color-texture based image retrieval system (CSCT system).

Table 3. ACC variation with L and r_2 for $K_1=16$, $(\delta x, \delta y)'s=(1, 0)/(2, 0)/(0, 1)/(0, 2)$ and various r_1

ACC(%) r_2 \ L	1	2	3	4	5	10	20	30	40
0.5	70.01	77.92	80.13	81.87	83.07	86.11	88.78	90.62	91.63
0.6	70.19	77.83	80.13	81.51	83.07	86.02	88.96	90.71	91.81
0.7	70.10	78.20	80.40	81.60	83.35	86.11	89.24	90.71	91.81
0.8	72.01	78.31	80.50	82.06	85.53	89.24	90.80	92.27	92.64
0.9	69.64	77.92	80.40	81.78	82.98	85.74	89.33	90.80	91.63
1	69.37	77.64	80.50	81.69	82.89	85.37	88.87	90.89	91.72
2	67.99	75.25	78.01	79.21	80.96	84.27	87.76	89.33	90.80

MOCC of the query image Q and one database image D as $(\mu_1^{qR}, \sigma_1^{qR}, S_1^{qR}, \mu_2^{qR}, \sigma_2^{qR}, S_2^{qR}, \dots, \mu_K^{qR}, \sigma_K^{qR}, S_K^{qR}, \mu_1^{qG}, \sigma_1^{qG}, S_1^{qG}, \mu_2^{qG}, \sigma_2^{qG}, S_2^{qG}, \dots, \mu_K^{qG}, \sigma_K^{qG}, S_K^{qG}, \mu_1^{qB}, \sigma_1^{qB}, S_1^{qB}, \mu_2^{qB}, \sigma_2^{qB}, S_2^{qB}, \dots, \mu_K^{qB}, \sigma_K^{qB}, S_K^{qB})$ and $(\mu_1^{dR}, \sigma_1^{dR}, S_1^{dR}, \mu_2^{dR}, \sigma_2^{dR}, S_2^{dR}, \dots, \mu_K^{dR}, \sigma_K^{dR}, S_K^{dR}, \mu_1^{dG}, \sigma_1^{dG}, S_1^{dG}, \mu_2^{dG}, \sigma_2^{dG}, S_2^{dG}, \dots, \mu_K^{dG}, \sigma_K^{dG}, S_K^{dG}, \mu_1^{dB}, \sigma_1^{dB}, S_1^{dB}, \mu_2^{dB}, \sigma_2^{dB}, S_2^{dB}, \dots, \mu_K^{dB}, \sigma_K^{dB}, S_K^{dB})$. Here the superscripts q and d stand for the query and database images; $R, G,$ and B indicate that this feature value is extracted from the image merely with $R, G,$ or B color components of Q or D . The subscript i is related to the feature value computed from cluster i . The definition of the image matching distance ∇^{MOCC} between Q and D based on the MOCC is shown as the following equation:

$$\nabla^{MOCC} = r_1 \sqrt{\nabla_R^{MOCC} + \nabla_G^{MOCC} + \nabla_B^{MOCC}},$$

where $\nabla_C^{MOCC} = \sum_{k=1}^K [\mu^{Ck} + \sigma^{Ck} + S^{Ck}]$, for $C = R, G,$ or B , and

$$\begin{aligned} \mu^{Ck} &= \left(\frac{\mu_C^{qk} - \mu_C^{dk}}{\max(\mu_C^{dk}) - \min(\mu_C^{qk})} \right) r_1, \\ \sigma^{Ck} &= \left(\frac{\sigma_C^{qk} - \sigma_C^{dk}}{\max(\sigma_C^{dk}) - \min(\sigma_C^{qk})} \right) r_1, \\ S^{Ck} &= \left(\frac{S_C^{qk} - S_C^{dk}}{\max(S_C^{dk}) - \min(S_C^{qk})} \right) r_1, \text{ and} \end{aligned}$$

r_1 is a constant. $\mu_C^{qk}, \sigma_C^{qk}, S_C^{qk}$ and $\mu_C^{dk}, \sigma_C^{dk}, S_C^{dk}$ are the mean, standard, and skewness of feature values for the k th dimension of MOCC of Q and D , respectively. $\max(\mu_C^{qk}), \max(\sigma_C^{qk}),$ and $\max(S_C^{qk})$, as well as $\min(\mu_C^{dk}), \min(\sigma_C^{dk}),$ and $\min(S_C^{dk})$ are defined as the maximal and minimal values of $\mu_C^{qk}, \sigma_C^{qk},$ and S_C^{qk} among images in database for $C = R, G,$ and B .

Considering CSR's $(f_1^d, f_2^d, \dots, f_{K_2}^d)$ and $(f_1^q, f_2^q, \dots, f_{K_2}^q)$ of Q and D , the image matching distance ∇^{CSR} of Q and D based on CSR is formulated as the following:

$$\nabla^{CSR} = r_2 \sqrt{\sum_{k=1}^n \left(\frac{f_d^k - f_q^k}{\max(f_d^k) - \min(f_d^k)} \right) r_2},$$

Table 4. ACC variation with L and r_2 for $K_2 = 20$

ACC(%) \ r_2 \ L	1	2	3	4	5	10	20	30	40
0.1	67.16	74.98	78.01	80.04	82.06	87.49	90.71	92.82	93.74
0.2	68.72	77.83	81.88	84.91	86.11	89.70	92.82	94.39	95.77
0.3	66.88	76.36	79.76	82.52	83.90	89.14	92.46	94.30	95.03
0.4	61.27	72.31	75.80	78.20	80.22	85.83	91.17	93.19	94.02
0.5	56.85	67.16	71.57	74.43	76.26	82.34	88.50	90.80	92.82
0.6	52.53	62.65	67.53	70.75	72.31	79.02	86.20	88.50	90.25
0.7	49.31	59.52	63.57	66.61	69.18	76.45	83.16	86.11	88.22
0.8	46.54	56.85	60.90	64.31	73.97	81.23	84.45	86.66	88.78
0.9	45.17	54.55	59.15	62.65	65.50	71.94	79.85	83.35	85.65
1	43.42	52.90	57.41	60.72	62.83	70.84	78.58	82.06	84.64
2	36.60	45.35	50.60	53.73	56.76	62.56	71.11	77.83	81.23

where r_2 is a constant; $\max(f_k^d)$ and $\min(f_k^d)$ are the maximal and minimal values among f_k^d 's of all database images.

CSCT image retrieval system combines the MOCC with the CSR to quantize the similarity of Q and D . Using such retrieval system, one can defines the image matching distance $Dist$ between Q and D as:

$$Dist = w_1 \times \nabla^{MOCC} + w_2 \times \nabla^{CSR},$$

where w_1 and w_2 are two given weights. Generally, $Dist$ decreases with increasing similarity of Q and D . Hence, CSCT approach can deliver the image with the minimal $Dist$ from the database.

5 Clustering Based Filter

With Fast advancing applications in multimedia field, image retrieval has been drawn a lot attention due to tremendous various applications in digital library and multimedia information systems. Efficient image retrieval has been always demanded for a database holding a huge amount of images. Image retrieval processes can be speeded up by spending time only on “pre-qualified images”. A fast clustering-based filter thus has been developed to skip a large number of unqualified images.

This clustering-based filter can initially classify all database images into G groups by K-means algorithm based on CSR. The images in the same group have similar CSR. Let $(m_{i1}, m_{i2}, \dots, m_{iK_2})$ be the average of the CSR's of all the images in each group i . $(m_{i1}, m_{i2}, \dots, m_{iK_2})$ is exerted as the respective feature of the group. m_{ij} is the j th value of the respective feature value. m_{ij} is defined as the following:

$$m_{ij} = \frac{1}{n_i} \sum_{k=1}^{n_i} CSR_k[j],$$

where n_i is the number of images in group i and $CSR_k[j]$ is the j th feature value of the k th image in the group.

For given a query image Q , the clustering-based filter initially computes the image matching distance ∇^{CSR} between the CSR of Q and the respective feature of each group, and also selects g groups with the minimal ∇^{CSR} . Then the filter compares Q with each image in those g groups via the corresponding ∇^{CSR} , and directly delivers N_f images in the g groups to CSCT image retrieval system. With such process, cluster-based filter and CSCT image retrieval system are integrated as Fast CSCT image retrieval system through the minimal ∇^{CSR} relative to Q .

Provided that n_δ different pairs (δ_x, δ_y) are assigned to compute the MOCC of the color image, MOCC and CSR of an image contain $3 \times 3 \times K_1$ and K_2 feature values, respectively. Without such filter, it would take time $T_1 = N \times (3 \times 3 \times K_1 + K_2)$ to compute, comparing to $T_2 = N_f \times (3 \times 3 \times K_1 + K_2) + GK_2 + \sum_{i=1}^g \times K_2$ units distance matching time to answer a query with such a filter. $T = T_1 - T_2 = N \times (3 \times 3 \times K_1 + K_2) - N_f \times (3 \times 3 \times K_1 + K_2) + GK_2 + \sum_{i=1}^g n_i \times K_2$. The clustering-based filter divides all database images into G groups using K-means algorithm. For the convenience of analysis, it is assumed that each of the G groups contains equal number of images and N is much larger than N_f , that is, $\frac{gN}{G} = \sum_{i=1}^g n_i$, and $(N - N_f) \approx N$. $T = 9NK_1 + NK_2 - 9N_fK_1 - N_fK_2 - GK_2 - \frac{gN}{G}K_2 \approx 9K_1N + K_2N - K_2(G + \frac{gN}{G})$. Thus, T has the maximal value at $G = \sqrt{gN}$, and $\frac{N(9K_1+K_2)}{K_2} \geq G + \frac{gN}{G}$ leads to $T \geq 0$.

6 Experiments

In this section, the performances of the CSCT-based image retrieval system were evaluated with experiments. There are two sets of database images $SetD = \{I_1^d, I_2^d, \dots, I_{1087}^d\}$ and $SetQ = \{I_1^q, I_2^q, \dots, I_{1087}^q\}$. Each contains 1087 full color images. The images in $SetD$ are employed as the database images and those in $SetQ$ are used as the query images. Some parts of them are drawn out from animations, where each image pair (I_i^d, I_i^q) are randomly picked up from a same animation. Most of the animations were downloaded from the websites <http://www.mcs.hk.edu.tw> and <http://co25.mi.com.tw>. Some other images were downloaded from <http://wang.ist.su.du/IMAGE>. The rest of images were scanned from natural images and trademark pictures. Figure 2 shows some of the query and database images.

In each experiment, every I_i^q is used as the query image. For each query, the system responds to the user L database images with the shortest image matching distances opposite to I_i^q . If I_i^d exists among the L database images, we say the system correctly finds the desired image. Otherwise, the system is considered failed in finding the desired database image. In the following, the accuracy rate of replying a query will be explained with ACC. Hereafter **Space** is referred to the required memory space holding the features of the 1087 database images, and **Time** stands for the total time to execute the 1087 queries.

The purpose of the first and second experiments is to study the influence of MOCC on image querying considering only ∇^{MOCC} is used to measure the

similarity of two images. To investigate the performances of the combinations of (δ_x, δ_y) , the first experiment is designed as K_1 and r_1 are set to 16 and 2. The experimental results were shown in Table 1 and Table 2. The combinations of the horizontal and vertical textures can generate better **ACC** as shown in Table 1. In Table 2, it demonstrates the experimental results that the texture features are extracted at the horizontal resolution different from the vertical resolution. The combination of $(1, 0) + (2, 0) + (0, 1) + (0, 2)$ for (δ_x, δ_y) also results in the best performance. Hence, the combination $(1, 0) + (2, 0) + (0, 1) + (0, 2)$ of (δ_x, δ_y) will be applied in the following experiments.

Table 5. **ACC** variation with L for $K_1 = 16$, $(\delta_x, \delta_y) = (1, 0) + (2, 0) + (0, 1) + (0, 2)$, $r_1 = 0.8$, $r_2 = 0.2$, $K_2 = 20$, $\bar{w}^1 = 0.2$, and $\bar{w}^2 = 0.8$.

L	1	2	3	4	5	10	20	30	40
ACC (%)	78.38	85.92	88.68	90.80	92.00	94.02	95.68	97.61	98.07

In the second experiment, it is to investigate the effect of r_1 in image querying for $K_1 = 16$, (δ_x, δ_y) 's $= (1, 0) + (2, 0) + (0, 1) + (0, 2)$. The experimental results are listed in Table 3. It reveals that a better **ACC** is given as $r_1 = 0.8$.

It was tested that the image querying influence of r_2 in the discernment of ∇^{CSR} in the third experiment. With $K_2 = 20$, ∇^{CSR} only is applied to evaluate the difference between two images. The results of the experiment are tabulated in Table 4. Obviously, there is a better **ACC** obtained at $r_2 = 0.2$.

In the fourth experiment, a probe is designed to evaluate the performances of CSCT image retrieval system. Based on the parameters $K_1 = 16$, $(\delta_x, \delta_y) = (1, 0) + (2, 0) + (0, 1) + (0, 2)$, $r_1 = 0.8$, $r_2 = 0.2$, $K_2 = 20$, $\bar{w}_1 = 0.2$, and $\bar{w}_2 = 0.8$, ∇^{CSR} and ∇^{MOCC} are merged to measure the difference of two images. The experimental results are demonstrated in Table 5. It takes running time 102.125 seconds for 1087 queries.

To carefully analyze the efficiency and the retrieving speed of the fast CSCT image retrieval system, the sixth experiment is carried out using the parameters $K_1 = 16$, $(\delta_x, \delta_y) = (1, 0) + (2, 0) + (0, 1) + (0, 2)$, $r_1 = 0.8$, $r_2 = 0.2$, $K_2 = 20$, $\bar{w}_1 = 0.2$, $\bar{w}_2 = 0.8$, $G = 30$, and $g = 12$. The average accurate rate of 99.36% for I_i^d in the g groups of each query image I_i^q . The average accurate rate of 95.03% for I_i^d in the $N_f = 160$ selected database images. Less than that of normal CSCT-based method, the consumed time is 20.360 seconds in replying 1087 queries in this sixth experiment. Such results confirm that fast CSCT image retrieval system run actually faster at a higher average accurate rate. In addition, it shows that **ACC** increases with higher L values in Table 6.

Table 6. **ACC** variation with L for fast CSCT image retrieval system

L	1	2	3	4	5	10	20	30	40
ACC (%)	74.98	83.35	85.84	87.15	87.80	90.25	92.27	93.28	94.11

In the last experiment, it is to compare the performances of CSCT image retrieval system with those of the system proposed by Huang and Dai [4]. The experiment takes 125.584 seconds in processing 1087 queries. Correlating Tables 5 and 7, CSCT-based image retrieval system is much more efficient than Huang-Dai's approach [6] in terms of **ACC**.

7 Conclusions

Two features, MOCC and CSR, are proposed to characterize a color image for image retrieving approaches. MOCC is used to depict the relationship between the color and texture, while the CSR is employed to illustrate the spatial distribution of the pixels with similar color in an image. Since such image features have individual advantages, both are integrated to form a unique Color-Space and Color-Texture (CSCT) based image retrieval system. The experimental results shows that CSCT approach demonstrate much better **ACC** than that of the system proposed by Huang and Dai [4]. To further increase efficiency of CSCT approach, a clustering based filter is developed to pre-sieve out the most unqualified database images. Furthermore, in terms of efficiency, fast CSCT image retrieval system not only outperformed over Huang-Dai's systems [4], but also over normal CSCT method.

References

1. Y. K. Chan and C. Y. Chen, "Image Retrieval System Based on Color-Complexity and Color-Spatial Features," *The Journal of Systems and Software*, Vol. 71, Issue 1-2, pp. 65-70, 2004.
2. V. N. Gudivada, and V. V. Raghavan, "Design and Evaluation of Algorithms for Image Retrieval by Spatial Similarity," *ACM Transactions on Information Systems (TOIS)*, Vol. 13, No. 2, pp. 115-144, 1995.
3. R. M. Haralick, and L. G. Shapiro, "Computer and Robot Vision," Vol. I, Addison-Wesley, Reading, MA, 1992.
4. P. W. Huang, and S. K. Dai, "Image Retrieval by Texture Similarity," *Pattern Recognition*, Vol. 36, No. 3, pp. 665-679, 2003.
5. S. Liapis, and G. Tziritas "Color and Texture Image Retrieval Using Chromaticity Histograms and Wavelet Frames," *IEEE Transactions on Multimedia*, Vol. 6, No. 5, pp. 676-686, 2004.
6. M. C. Su, and C. H. Chou, "A Modified Version of the K-means Algorithm with a Distance Based on Cluster Symmetry," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 23, No. 6, pp. 674-680, 2001.
7. M. J. Swain, and D. H. Ballard, "Color Indexing," *International Journal of Computer Vision*, Vol. 7, pp. 11-32, 1991.

Generation of Dynamic Heart Model Based on 4D Echocardiographic Images

Michał Chlebiej¹, Paweł Mikołajczak¹, Krzysztof Nowiński²,
Piotr Ścisło³, and Piotr Bała⁴

¹ Department of Information Technology, Institute of Computer Science,
Maria Curie-Skłodowska University,
Pl. M. Curie-Skłodowskiej 1, 20-031 Lublin, Poland
meow@goblin.umcs.lublin.pl

² Interdisciplinary Centre for Mathematical and Computational Modeling,
Warsaw University, Pawińskiego 5a, 02-106 Warsaw, Poland

³ Department of Cardiology, Medical Academy of Warsaw,
02-097 Warszawa, Poland

⁴ Faculty of Mathematics and Computer Science. N. Copernicus University,
Chopina 12/16, 87-100 Toruń, Poland

Abstract. One of the most challenging problems in the modern cardiology is a correct quantification of the left ventricle contractility and synchronicity. Correct, quantitative assessment of these parameters, which could be changed in a course of many severe diseases of the heart (e.g. coronary artery disease and myocardial infarction, heart failure), is a key factor for the right diagnose and further therapy. Up to date, in clinical daily practice, most of these information is collected by transthoracic two dimensional echocardiography. Assessment of these parameters is difficult and depends on observer experience. However, quantification method of the contractility assessment based on strain and strain analysis are available, these methods still are grounded on 2D analysis. Real time 3D echocardiography gives physicians opportunity for real quantitative analysis of the left ventricle contractility and synchronicity. In this work we present a method for estimating heart motion from 4D (3D+time) echocardiographic images.

1 Introduction

Together with techniques based on electrocardiography, ultrasonographic examination of the heart (echocardiography) is one of the most frequent used methods of the heart's examination. Using this modality, vital information about morphology and hemodynamics of the heart could be collected by simply, bedside assessment. Echocardiography, even real time 3D, is relatively inexpensive (when compared to CT or MRI) data acquisition technique. In clinical practice the analysis of the data mainly relies on the visual inspection of the acquired views and on the physicians experience. Such methods lead to a qualitative and subjective assessment without taking into account individual quantitative information included in images. Another problem of the echocardiographic analysis are artifacts from the thorax (e.g. emphysema), which could cause in 5-10% of patients echocardiography is not useful.

To reveal all these vital information and decrease information noise, automated computer-based analysis is highly desirable.

Recently, methods were proposed in the literature for the reconstruction of heart motion from 4D ultrasound images. For the left ventricle segmentation surface based methods (using shape and motion constraints) have been proposed [1] to deal with speckle noise in the echocardiograms. Biomedical models have been also investigated for the modeling of cardiac cycle [2]. In [3], an anisotropic filtering and gradient computation in a cylindrical geometry were used in the model based segmentation approach.

In this work we present a novel approach to describe global left ventricle function from the 3D echocardiographic image sequences. In the first step images are filtered using 4D anisotropic diffusion. After that, non-rigid registration of the 3D time sequence is performed to obtain the description of deformation field. Non-rigidly registered images are used to compute an average 3D dataset. The next phase consists of the shape and texture based segmentation followed by a triangulation step resulting in the 3D surface model. In the final step deformation operator is applied to the surface model in order to recover the time motion of the heart. In the following sections all of the algorithm phases are described in details and applied to the left ventricle.

2 Filtering of the Echocardiographic Time Sequence

The interpretation of the content information in ultrasound images is very challenging task because of the low image resolution and because of the presence of the speckle noise. A number of techniques have been proposed to remove the noise and to improve the ultrasound image quality including median filtering, adaptive weighed median filtering, temporal averaging, temporal dilatation (maximum amplitude writing). However, such techniques often tend to degrade image - displace, blur or round boundaries. They can also suffer from insufficient denoising or large computational cost. In our work we have decided to use computationally efficient filter based on an anisotropic diffusion [4]. The main concept of the anisotropic diffusion in image processing raised from an analogy with fluids diffusion. The fluid concentration can be seen as image intensity I and it is evolving toward an equilibrium state according to the equation:

$$\frac{\partial I(x, y, z, t)}{\partial t} = \text{div}(c(x, y, z, t)\nabla I) \tag{1}$$

where $c(x, y, z)$ is the conductivity coefficient. In the original work authors proposed selection of the conductivity coefficient dependent of the image structure (as the function of the image gradient magnitude $|\nabla I|$):

$$c(x, y, z, t) = g|\nabla I(x, y, z, t)| \tag{2}$$

Different diffusion functions g have been proposed. The most commonly used for the filtering of echocardiographic images is the diffusion function proposed in [5]:

$$g(x, \lambda) = \begin{cases} 1 & x \leq 0 \\ 1 - e^{-\frac{3.315}{(x/\lambda)^4}} & x > 0 \end{cases} \quad (3)$$

where λ is the gradient threshold which defines boundary points (the gradient magnitude values above λ are considered as boundary). This function acts as an edge-enhancing filter with the low diffusion values at the boundary points and with high values in the smooth areas. As the diffusion evolves in time, the magnitude of the gradient at the boundaries is getting higher. Because of that, the value of threshold should increase in every iteration. In our work we use a linear model for the gradient threshold value: $\lambda(t) = \lambda_0 + at$, where λ_0 is an initial value, a is the positive constant and t represents the time step of the single iteration in the diffusion process.

In our work we deal with the time sequence of 3D ultrasound data. Because of that, we have decided to take into account in the diffusion process also temporal consistency of the acquired data. To extend the diffusion algorithm to the fourth dimensional block of data with the time taken as fourth dimension we express Equation (1) in the following form:

$$\frac{\partial I(x, y, z, T, t)}{\partial t} = \text{div}(c(x, y, z, T, t)\nabla I) \quad (4)$$

The results of the 4D filtering of echocardiographic images are shown in the Fig. 1. It may be observed that such filtering drastically reduces the speckle noise and enhances the structure boundaries. The speckle noise may lead to partial disappearing of the image boundaries and then time diffusion may help to recover some of the missing boundary parts.

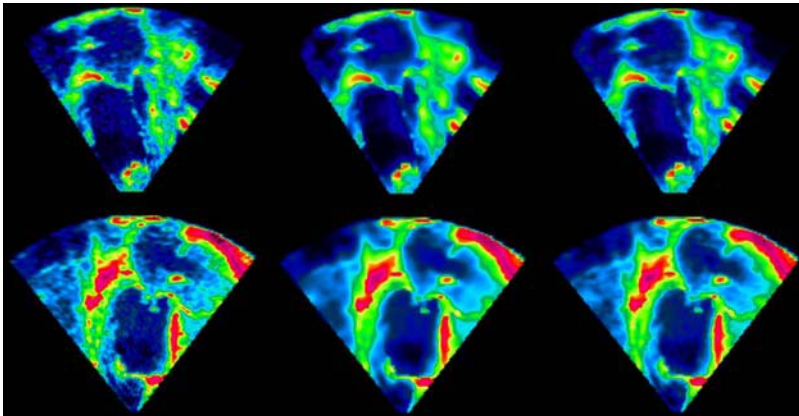


Fig. 1. The 4D anisotropic diffusion in the echocardiographic images of the heart. *Left:* original 3D image frame. *Center* – 3D diffused image ($\lambda_0 = 5.0$, $a = 10$, $\Delta t = 0.05$, 15 iterations). *Right* – 4D diffused image (same parameters).

3 Recovering the Deformation Field

It is important to model the motion of the heart taking into consideration individual patient specific anatomical features. In order to achieve realistic motion we have to extract heart dynamics by studying 3D movement of a corresponding anatomy between the reference frame (at time T_0) and the following frames ($T_1 - T_8$). We recover the transformation that aligns the reference frame with all the other frames by using intensity based 3D volume registration (see Fig. 2). Such approach relies on an elastic transformation which allows to model local deformation of spatial objects. Therefore, it is difficult to describe the local deformation via parameterized transformations. The method of choice is usually FFD (free-form-deformation) method [6] which is commonly used as a powerful modeling tool for 3D deformable objects. The basic idea of FFD is to deform an object by manipulating an underlying mesh of control points. The manipulated lattice determines the deformation function that specifies a new position for each point of the deformed surface. Final and completely combined deformation consists of global transformation (rigid or affine) and local deformation [7]:

$$T(p) = T_{global}(p) + T_{local}(p) \quad \text{where } p = (x, y, z) \quad (5)$$

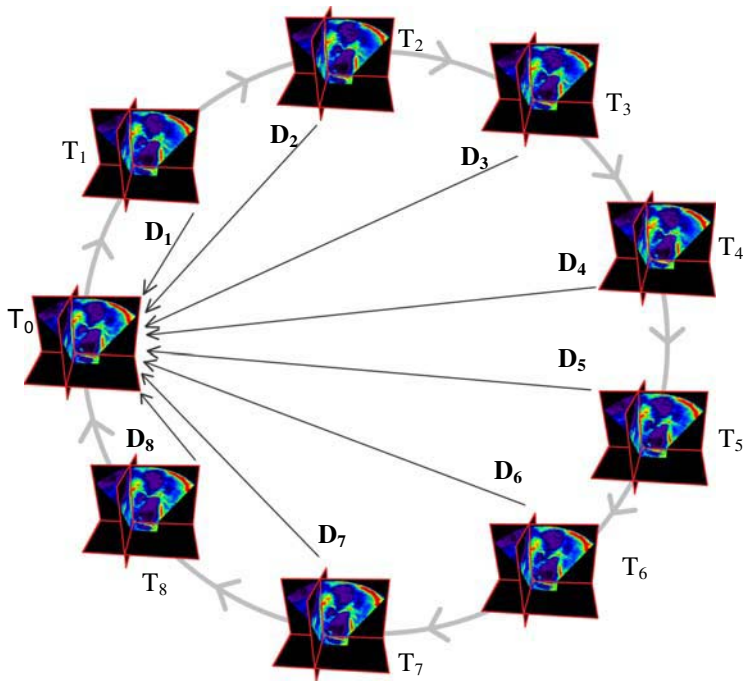


Fig. 2. Registration scheme of the 3D cardiac cycle sequence images $T_1 - T_8$ to the reference frame T_0 . The goal of the proposed method is to recover the deformation field $D_1 - D_8$ using FFD based elastic registration.

In this work, we decided to use FFD model based on a B-splines which have good localization properties. To calculate such deformation, the domain of the object volume is defined as: $\Omega = \{(x, y, z) \mid 0 \leq x \leq X, 0 \leq y \leq Y, 0 \leq z \leq Z\}$,

where X , Y and Z denote object resolution. Let Φ denote a $n_x \times n_y \times n_z$ mesh of control points $\phi_{i,j,k}$ with the uniform spacing. The FFD can be written as the 3D tensor product of the 1-D cubic B-splines:

$$T_{local}(p) = \sum_{i=0}^3 \sum_{j=0}^3 \sum_{k=0}^3 B_i(u)B_j(v)B_k(w)\phi_{i+l,j+m,k+n} \quad (6)$$

where u , v and w are the relative positions of p with respect to the nearest 64 control points and B_i represents the i -th basis function of the cubic B-spline. The number of parameters to be optimized is equal to 3 times number of control points in the lattice. Because of good localization property of B-spline functions optimization procedures can be applied locally. This allows for acceptable running times even for very dense lattices. In our work we use normalized mutual information similarity function [8]:

$$NMI(FI, RI) = \frac{h(FI) + h(RI)}{h(FI, RI)} \quad (7)$$

where RI represents the reference image and FI represents the floating image, $h(FI)$, $h(RI)$ and $h(FI, RI)$ are the single and joint entropies [9]. For the minimization of the selected similarity measure we use the Powell's algorithm [10].

In order to deal with large displacements in the registration process, we use a classical incremental multi-resolution procedure. At the coarsest level (grid size $8 \times 8 \times 8$, data is scaled down by the factor of 8) we can model the maximum allowed deformations. At the final level ($32 \times 32 \times 32$ grid with the full 3D image resolution) we are able to model small deformations to fine-tune the r quality.

After obtaining the 3D frames of the deformation field we are able to describe motion of the whole matter in the volume object. At this point our goal is to define the shape of the object of interest and apply recovered deformation to visualize the motion in the cardiac cycle.

4 Segmentation Procedure

The first step of the segmentation procedure involves noise removal from the original data using time averaging technique (see Fig. 3). The deformation field frames are used to generate new datasets elastically aligned with the reference frame T_0 . After this step an average dataset from the reference frame and all the deformed datasets are created. The noise located in the datasets is smoothed, while the boundaries of the image structures are preserved. When there is no noise correlation between time

frames the process of averaging N frames results in decreasing of noise level \sqrt{N} times.

The segmentation step is performed using an averaged dataset. In our work we decided to use deformable boundary approach for the segmentation procedure. The selected method uses energy function consisted of texture based and shape based terms as proposed in [11]. In this algorithm, starting from an initial estimate (in the presented case we used hand-drawn mask created with 2D ellipse tool), a deformable model evolves under the influence of the defined energy to converge to the desired boundary of an image structure object. The model deformations are efficiently parameterized using the B-spline based Free Form Deformation (see Equation 6).

The texture energy term is calculated using non-parametric Gaussian kernel based method which, in opposite to standard statistical parameters like mean or variance, is more generic and can represent more complex intensity distributions. An initial estimate bounded region Φ_M is used to select the corresponding intensity region of a source image R_M . This region is used to generate 3D texture-intensity energy map (see Fig. 5) which represents the probabilities of the intensity values i being consistent with the model interior using equation:

$$P(i | \Phi_M) = \frac{1}{V(R_M)} \iiint_{R_M} \frac{1}{\sqrt{2\pi\sigma}} e^{-\frac{i-I(x)}{2\sigma^2}} dx \tag{8}$$

where $V(R_M)$ is the volume of R_M and σ is the standard deviation of the Gaussian distribution.

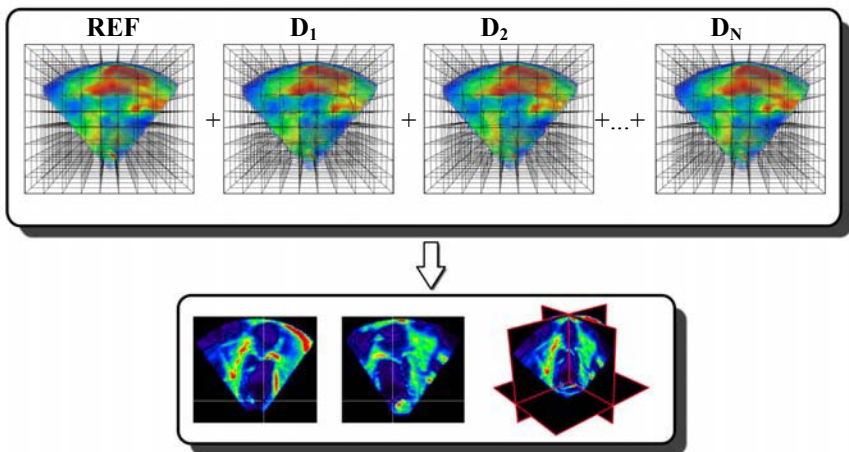


Fig. 3. Time averaging of the reference 3D frame with elastically registered all the other frames. Top: volume rendering of the reference frame and registered data together with the deformation field (represented by deformed wire frame grid). Bottom: averaged dataset (2D cross-sections and 3D slices).

Many different energy functions may be calculated on the basis of texture intensity maps. In our work we have formulated texture energy term E_T as the Shannon's entropy using actual texture map which gets automatically updated while the model deforms.

The shape energy term takes into account gradient information available in the source image. After 3D filtering of the source image (using 3D anisotropic diffusion for edge enhancement purpose) Canny-Deriche's 3D boundary detection filter [12] is applied (see Fig. 4). In the next step 3D Euclidean distance map is generated which assigns to all of the image voxels distance value from the nearest voxel that belongs to the extracted boundaries. The important feature of the generated distance map is that it may help the deforming model to evolve towards the boundaries. The shape energy consists of two terms concerning interior E_I and the boundary E_B of the deformed model. The aim of the interior term is to minimize the sum of squared distances between the implicit shape representation in the model interior Φ_N (which is actually the signed distance calculated using generated distance map with the negative values assigned to all voxels that do not belong to the model) and the underlying distance value Φ_D :

$$E_I = \frac{1}{V(R_M)} \iiint_{R_M} (\Phi_M(x) - \Phi_D(x))^2 dx \tag{9}$$

The role of optimization procedure is to minimize this term – to deform the model along the gradient direction. Such process may result in either shrinking or expanding of the model. Such process is similar to the existence of two way balloon forces included in more sophisticated and time consuming segmentation schemes [13][14][15]. This energy term can attract the deforming model towards the boundaries from far away locations. However it may be insufficient when small unwanted edges are situated inside the model. Introduction of the E_B energy term makes deformation more robust in such cases:

$$E_B = \frac{1}{V(\partial R_M)} \iiint_{\partial R_M} (\Phi_D(x))^2 dx \tag{10}$$

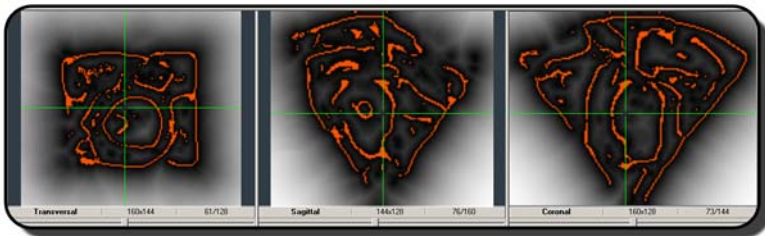


Fig. 4. 2D cross-sections of the Euclidean distance map dataset (brighter intensities represent higher values of the distance measure) together with the 3D edges generated using Canny-Deriche's 3D algorithm

where ∂R_M is the set of the boundary voxels. This term has also one additional advantage, it may prevent leaking of the deforming model through small holes within boundaries. It constrains the model to go along the shortest-geodesic path in the distance map. The complete energy functional is than defined as:

$$E = \alpha E_T + \beta E_I + \gamma E_B \tag{11}$$

where α, β, γ are positive constants which in our approach are selected manually depends on the image content. An example of the described segmentation process of the left ventricle is presented in Fig. 5. As the last step of the segmentation procedure the morphological closing operator to ensure smoothness of the boundary is applied.

5 Motion Reconstruction of the Left Ventricle

After the segmentation procedure we are able to create triangle surface which represents an object of interest. This procedure is followed by mesh smoothing to obtain more realistic looking surface. As the last step the deformation field operator to generate the deformed surface frames is applied. Such approach has an important point-to-point correspondence feature which allows interpolation between deformation field frames in order to obtain smooth motion. Together with the motion visualization we were able to compute some important features of beating heart.

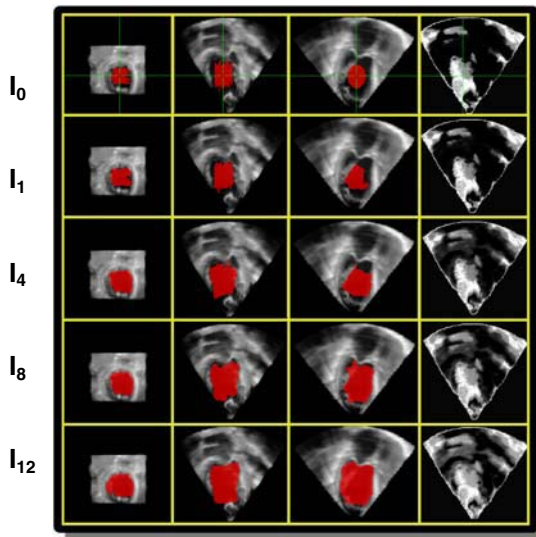


Fig. 5. Segmentation of the left ventricle from echocardiographic images. Algorithm converged to the minimum of the energy functional after 12 iterations. First three columns (from the left) present evolution of deformable segmentation from three different orthogonal perspectives. The last column presents 2D views of the texture-intensity energy map generated using evolving model.

Table 1. Statistical parameters (volume and max displacement) calculated using generated surface frames of the cardiac cycle

	T ₀	T ₁	T ₁	T ₃	T ₄	T ₅	T ₆	T ₇	T ₈
volume[ml]	161.9	180.2	183.9	183.6	182.3	181.1	177.4	177.0	176.3
maxd [mm]	0	4.64	6.53	6.62	7.89	5.95	5.41	4.73	2.63

The deformed in time triangle meshes allowed us to compute changes in volume of the left ventricle (see Table 1). We were also able to localize the regions with the highest deformations as it is presented in the Fig. 6.

6 Conclusions and the Future Directions

In this paper we have proposed an approach of the dynamic heart model generation from the 4D echocardiographic image. We have presented the preliminary results which are very promising. Currently we are working on the improvement of the most crucial stages of the method. All of the algorithms which operate on voxel neighborhood are calculated in Cartesian coordinates. 3D echocardiographic images are generated in the cylindrical or spherical coordinates. This fact should be taken into consideration in the interpolation, filtering or gradient computation. The elastic

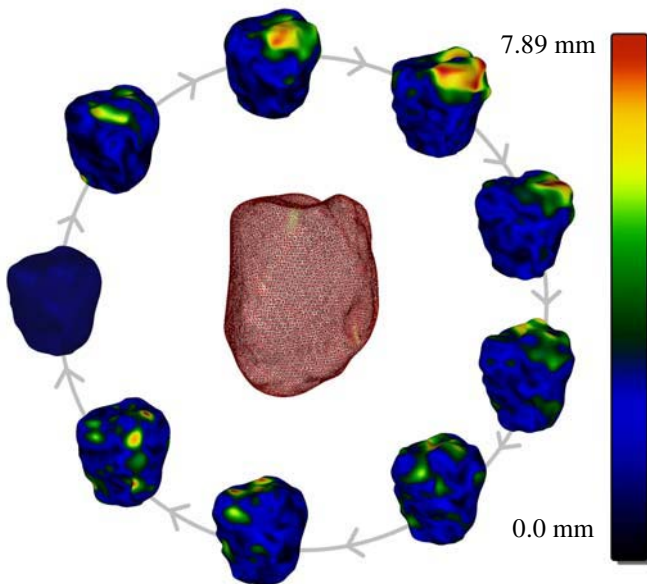


Fig. 6. Reconstructed cardiac cycle of the left ventricle. The diagram presents the deformation in time of the reference surface (visualized also in the center of the diagram in the wire-frame form). Color texture on the frames represent the displacement level of the heart wall.

registration procedure is also extensively investigated. The work on the acceleration of the registration process and further testing of other similarity measures is also in progress. In the described segmentation procedure it is desired to select automatically weights for the energy terms. The definition of the texture energy term needs also to be further investigated.

References

1. Montgant J., Delingette H., Space and time shape constrained deformable surfaces for 4D medical image segmentation., *Medical Image Computing And Computed Assisted Intervention, Lecture Notes on Computer Science*, Vol. 1935., pp. 196-205, Springer Pittsburgh, 2000.
2. Papademetris X., Sinuas A., Dione D., Duncan J., Estimation on 3D left ventricular deformation from echocardiography., *Medical Image Anal.*, 5(1), pp.17-28, 2001.
3. Montgant J, Sermesant M., Delingette H., Malandain G., Ayache N., Anisotropic filtering for model-based segmentation of 4D cylindrical echocardiographic images, *Pattern Recognition Letters*, Vol. 24, pp. 815-828, 2003.
4. Perona P., Malik J., Scale-space and edge detection using anisotropic diffusion, *IEEE Trans. On Pattern Anal. and Mach. Intell.*, Vol.12, No. 7, pp. 629-639, 1990.
5. Weickert J., Anisotropic diffusion in image processing, G. G. Teubner, Stuttgart, 1998.
6. Sederberg T, Parry S., Free form deformation of solid geometric models, *Computer Graphics*, Vol. 20, No.4, pp. 151-160, 1986.
7. Rueckert D., Sonoda L.I., Hayes C., Hill D.L. G., Leach M.O., Hawkes D.J., Non-rigid registration using free-form deformations: Application to breast MR images, *IEEE Transactions on Medical Imaging*, Vol. 18, No. 8, pp. 712-721, 1999.
8. Studholme C., et al., An overlap invariant entropy measure of 3D medical image alignment. *Pattern Recognition*, Vol.32 (1): pp. 71-86, 1999.
9. Shannon C.E., A mathematical theory of communication, *Bell System Technical Journal*, Vol. 27, pp. 2790423 and 623-656, July and October 1948.
10. Press W.H., Flannery B.P., Teukolsky S.A., Vetterling W.T., Numerical Recipes in C, *Cambridge University Press*, second edition, 1992.
11. Huang X., Metaxas D., Chen T., MetaMorphs: Deformable shape and texture models, *IEEE Computer Vision and Pattern Recognition*, Washington, D.C., June, 2004.
12. Monga O., Deriche R., Malandain G., Cocquerez J.P., Recursive filtering and edge tracking: two primary tools for 3D edge detection, *Image and Vision Computing*, Vol. 9 (4), pp. 203-214, August, 1991.
13. Cohen L.D., Cohen I., Finite-element methods for active contour models and balloons for 2-D and 3-D images, *IEEE Trans. On Pattern Analysis and Machine Intelligence*, Vol 15., pp. 1131-1147, 1993.
14. Kass M., Witkin A., Terzopoulos D., Snakes: Active contour models, *International Journal of Computer Vision*, Vol. 1, pp. 321-331, 1987.
15. Paragios. N., Deriche R., Geodesic active regions and level set methods for supervised texture segmentation, *International Journal of Computer Vision*, Vol 46 (3), pp. 223-247, 2002.

Object-Based Image Retrieval Using Dominant Color Pairs Between Adjacent Regions

Ki Tae Park and Young Shik Moon

Dept. of Computer Science and Engineering, Hanyang University, Ansan Korea
Tel.: +82-31-407-8991; Fax.: +82-31-419-1162
{parkkt, ysmoon}@cse.hanyang.ac.kr

Abstract. Most existing methods for content-based image retrieval handle an image as a whole, instead of focusing on an object of interest. This paper proposes object-based image retrieval based on the dominant color pairs between adjacent regions. From a segmented image, the dominant color pairs between adjacent regions are extracted to produce color adjacency matrix, from which candidate regions of DB images are selected. The similarity measure between the query image and candidate regions in DB images is computed based on the color correlogram technique. Experimental results show the performance improvement of the proposed method over existing methods.

1 Introduction

Most of existing content-based image retrieval systems show some good results [1-6]. But in most cases, they use whole images instead of focusing on the regions of interest. Therefore, the systems may produce undesirable retrieval results because of the errors caused by backgrounds. In this paper, we propose an image retrieval method, where an object of interest is used as a query and the retrieval result is candidate regions in DB images where the object exists.

This paper is organized as follows. Section 2 introduces related works. Section 3 describes the proposed method. Experimental results are given in Section 4, and Section 5 concludes the paper.

2 Related Works

Color information in color images is a significant feature for content-based image retrieval. Because color features have very important low-level information, which is insensitive to noises or complexity of background, they have been used for robust retrieval against translation, rotation, and scaling.

One of significant works in color-based retrieval was done by Swain and Ballard who proposed color histogram intersection technique[7], where the similarity measure is the distance between a query image histogram and a DB image histogram. This method has been widely used since it is simple and the computational requirement is low. However, it may produce dome erroneous results since the histogram does not

include any spatial information. To solve this problem, Huang proposed color correlogram method that includes spatial correlation in color information [6]. Even though the performance of this method has been improved, it is inappropriate for partial matching since it computes the similarity using whole images. Das proposed an image retrieval system (FOCUS) to find regions of interest in DB images, which contain the query object [8].

3 Proposed Method

The method proposed in this paper consists of the following steps.

For query image,

- Step1. Segment the image and extract the object of interest
- Step2. Determine dominant color from extracted object
- Step3. Compute color correlogram and construct color adjacency matrix (CAM)

For DB image,

- Step1. Segment the image and extract dominant colors
- Step2. Extract color pairs
- Step3. Determine candidate regions by CAM
- Step4. Compute color correlogram
- Step5. Compute the similarity between query image and candidate regions extracted from DB images using color correlogram

Fig. 1 shows the overall flowchart of the proposal scheme.

3.1 Image Segmentation and Object Extraction

From a given query image including the object of interest, the image is first segmented. Then by selecting the regions of interest, the object is identified. We use the image segmentation algorithm proposed by Demin Wang [9]. This algorithm is known to be an efficient algorithm in terms of computation time and performance. Fig. 2 shows the original image and the segmented image.

To generate the object of interest from the segmented image excluding background, the user selects the regions of interest. Then the selected regions are merged into one region. Fig. 3 shows the image containing the object of interest without background.

3.2 Dominant Color Extraction

The dominant color which is one of MPEG-7 color descriptors is useful when several colors or a specific color sufficiently represent either a whole image or a partial image [10]. In this paper, dominant color is used as a feature to represent each segmented region. The dominant color of a region is defined as the maximum bin of color histogram.

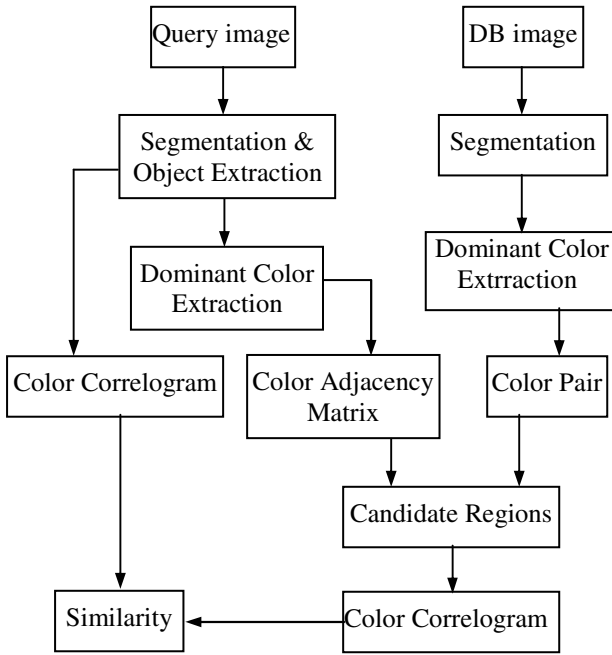


Fig. 1. Overall flowchart



Fig. 2. Segmentation result. (a) Original image, (b) Segmented image.

3.3 Color Adjacency Matrix (CAM)

Objects in images usually have some colorful flat regions adjacent to each other, which produces some spatial information about the object of interest. Examples of those images include the ones in the FOCUS system [8]. We mainly focus on the characteristics of those adjacent regions. Along the boundaries of these adjacent regions, we extract color adjacency information and utilize color pairs which can be extracted from the color adjacency.



Fig. 3. Result of object extraction

In order to extract color pairs, we use 3×3 mask at each pixel. Among the pairs of the center pixel and its neighbors, the pair with the maximum color difference is defined as “color pair”. When the color difference is over a threshold value, it is defined as an “edge”. Color pairs can be identified by computing the color vector angular distance (CVAD) [11,12]. Many researchers have studied the measures based on the angle of a color vector, which produces perceptually admirable retrieval results in RGB domain. Regarding the color vector angular distance it is known that the angular measures are chromaticity-based, which means that they operate primarily on the orientation of the color vector in the RGB space and are robust against intensity changes [13]. Among these measures, we choose vector angle-based distance measure proposed by Androutsos. It is a distance measure based on the angular distance between two vectors. Also, it is a combinational distance measure, which is composed of an angle and magnitude [13]. CVAD measure is shown in equation (1),

$$\delta(\mathbf{x}_i, \mathbf{x}_j) = 1 - \underbrace{\left[1 - \frac{2}{\pi} \cos^{-1} \left(\frac{\mathbf{x}_i \cdot \mathbf{x}_j}{|\mathbf{x}_i| |\mathbf{x}_j|} \right) \right]}_{\text{angle}} \cdot \underbrace{\left[1 - \frac{|\mathbf{x}_i - \mathbf{x}_j|}{\sqrt{3} \cdot 255^2} \right]}_{\text{magnitude}} \quad (1)$$

where \mathbf{x}_i and \mathbf{x}_j is three-dimensional color vector of the center and its neighbor, respectively. The normalization factor of $2/\pi$ in angle portion is attributed to the fact that the maximum angle which can possibly be attained is $\pi/2$. Also, the $\sqrt{3} \cdot 255^2$ normalization factor is due to the fact that the maximum difference vector which can exist is (255,255,255) and its magnitude is $\sqrt{3} \cdot 255^2$. Extracting color pairs using equation (1), we can make the color adjacent matrix (CAM). We utilize not every color pair but some of them. Therefore, we have to choose color pairs to be used as a feature, prior to making CAM. We choose color pairs when the number of corresponding color pairs exceeds a threshold value. The threshold values are determined by experiments. In order to determine color pairs, we use equation (2). As shown in equation (2), the element of each color pair in CAM is assigned 1 or 0.

$$CAM(C_i, C_j) = \begin{cases} 1 & \text{if } N(C_i, C_j) \geq Th \\ 0 & \text{others} \end{cases} \quad (2)$$

Where $N(C_i, C_j)$ is the number of color pairs (C_i, C_j) and Th is a threshold value. Fig. 2 shows how color pairs are extracted and how CAM is constructed by equation (2).

3.4 Candidate Region Extraction

Given color adjacency matrix for the query image, we search for candidate regions in DB image, where the object of interest may exist. After segmenting a DB image, each segmented region is assigned a dominant color. Each pair of adjacent regions are selected as candidate regions if color adjacency matrix of query image with corresponding dominant color pair is equal to 1. Fig. 4 shows how the candidate regions are extracted from DB image.

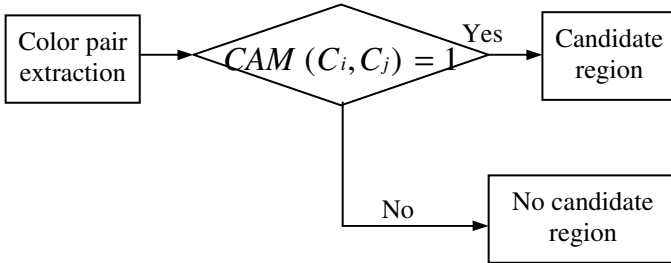


Fig. 4. Candidate region extraction

3.5 Color Correlogram

Among the candidate regions in DB image, the similarity between the query image and each candidate region is computed by using color correlogram [6]. Color correlogram expresses how the spatial correlation of pairs of colors changes with distance. Color correlogram is given by equation (3).

$$\gamma_{ci,cj}^{(k)}(I) \equiv \Pr_{p_1 \in I_c, p_2 \in I} [p_2 \in I_c \mid |p_1 - p_2| = k] \tag{3}$$

$$|p_1 - p_2| \equiv \max\{|x_1 - x_2|, |y_1 - y_2|\}$$

Here I is an $n \times n$ image. Colors are quantized into m colors $c_1, c_2, c_3, \dots, c_m$. For a pixel $p = (x,y) \in I$, $I(p)$ denotes its color. $I_c \equiv \{p \mid I(p) = c\}$. Given any pixel of color c_i in the image, $\gamma_{ci,cj}^{(k)}$ gives the probability that a pixel at distance k away from the given pixel is of color c_j .

3.6 Similarity Measure

To determine the similarity between a query image and DB images, the metric given in equation (4) is computed.

$$|I - I'|_{\gamma, d} = \sum_{i,j \in [m], k \in [d]} \frac{|\gamma_{ci,cj}^{(k)}(I) - \gamma_{ci,cj}^{(k)}(I')|}{1 + \gamma_{ci,cj}^{(k)}(I) + \gamma_{ci,cj}^{(k)}(I')} \tag{4}$$

Where I is the query image, I' is a DB image, and d is the distance between pixels.

4 Experimental Results

For the experiment, FOCUS DB images which include 25 query images are used [2]. We evaluate the performance in terms of object extraction and image retrieval. Fig. 5 shows some query images used in the experiment.



Fig. 5. Some of the query Images

To evaluate the performance of the retrieval, we use the *ANMRR* metric that is the performance measure of MPEG-7 standards for color and texture, which is computed by equation (5) [14].

In equation (4), $NG(q)$ implies the number of images in each category, GTM represents the largest number among $NG(q)$'s, and Q represents the number of query images.

$$ANMRR = \frac{1}{Q} \sum_{q=1}^Q NMRR (q) \quad (5)$$

$$NMRR (q) = \frac{MRR (q)}{K + 0.5 - 0.5 * NG (q)}$$

$$MRR (q) = AVR (q) - 0.5 - \frac{NG (q)}{2}$$

$$K = \min(4 * NG (q), 2 * GTM)$$

$$AVR (q) = \sum_{k=1}^{NG (q)} \frac{Rank (k)}{NG (q)}$$

ANMRR is a normalized measure for the average ranking and the value is always between 0 and 1. The smaller the *ANMRR*, the better the performance.

As shown in Table 1, the average performance of the proposed algorithm has been improved by 12% over DAS method.

Table 1. Performance comparison(ANMRR)

Method	ANMRR
FOCUS	0.313
Proposed Method	0.276

5 Conclusions

In this paper, we proposed an object-based image retrieval method using dominant color pairs. Query image is constructed by selecting regions of interest after the image is segmented. From the segmented query image, we extract dominant color pairs between adjacent regions at the boundary and we compose color adjacency matrix. From DB images, we extract candidate regions by using color adjacency matrix composed from the query image. To measure the similarity between the query image and candidate regions in DB images, the color correlogram technique is used. By Experimental results, it has been shown that errors caused by background colors have been reduced, resulting in the performance improvement over the existing methods.

Acknowledgement

This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

References

1. A. Pentland, R. W. Picard, and S. Sclaroff et al., "Photobook: Tools for Content-based Manipulation of Image Database," *SPIE, Proc. In Storage and Retrieval for Image and Video Databases II*, Vol. 2185, Feb. 1994
2. W. Niblack, R. Barber, W. Equitz, M. Flickner, E. Glasman, D. Petkovic and P. Yanker, "The QBIC Project: Querying Images by Content Using Color, Texture, and Shape," *SPIE*, Vol. 1908, pp. 173-187, 1993
3. W. Y. Ma and B. S. Manjunath, "Netra: A Toolbox for Navigating Large Image Database," *IEEE International Conference on Image Processing*, 1997
4. J. R. Smith and S. F. Chang, "VisualSEEK: A Fully Automated Content-based Image Query System," *Proc. ACM Multimedia*, Boston MA, 1996
5. J. B. Oh, Y. S. Moon, "Content-based Image Retrieval Based on Scale-Space Theory," *IEICE Trans. Fundamental*, June 1999
6. J. Huang, S. R. Kumar, M. Mitra, W. J. Zhu, and R. Zabih, "Image Indexing Using Color Correlograms," *Proc. of the IEEE conference on Computer Vision and Pattern Recognition*, pp. 762-768, 1997
7. M. Swain and D. Ballard, "Color Indexing," *International Journal of Computer Vision*, Vol. 7, No. 1, pp. 11-32, 1991

8. M. Das, E. M. Riseman, and B. Draper, "FOCUS: Searching for Multi-colored Objects in a Diverse Image Database," *Proc. of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 762-768, 1997
9. D. Wang, "Unsupervised Video Segmentation based on Watersheds and Temporal Tracking," *IEEE Trans. on Circuits and System for Video Technology*, Vol. 8, No. 5, pp. 539-546, 1998
10. B. S. Manjunath, J. R. Ohm, V. Vasudevan, A. Yamada, "Color and Texture Descriptors," *IEEE Trans. Circuits and Systems for Video Tech.*, Vol. 11. No. 6, Jun 2001
11. H. Y. Lee, H. K. Lee, and Y. H. Ha, "Spatial Color Descriptor for Image Retrieval and Video Segmentation," *IEEE Trans. on Multimedia*, vol.5, No.3, pp. 358-367, Sep. 2003.
12. D. Androustos, K. N. Plataniotis, and A. N. Venetsanopoulos, "A Vector Angular Distance Measure for Indexing and Retrieval of Color," *Proc. Storage & Retrieval for Image and Video Databases VII*, SPIE-3656, San Jose, USA, pp.604-613, 1999.
13. D. Androustos, K. N. Plataniotis, A. N. Venetsanopoulo, "A Novel Vector-Based Approach to Color Image Retrieval Using a Vector Angular-Based Distance Measure," *Computer Vision and Image Understanding*, vol. 75, pp.46-58, July, 1999.
14. ISO/IEC JTC1/SC29/WG1/ "Core Experiment on MPEG-7 Color and Texture Descriptors," *Doc. N2819, MPEG Vancouver Meeting*, July 1999

Real-Time Vision Tracking Algorithm

Edgar R. Arce-Santana, Jose M. Luna-Rivera,
Daniel U. Campos-Delgado, and Ulises Pineda-Rico

Facultad de Ciencias, UASLP, Av. Dr. Salvador Nava s/n, Zona Universitaria,
C.P. 78290, San Luis Potosi, S.L.P., Mexico
arce@ciencias.uaslp.mx, mlr@ciencias.uaslp.mx,
ducd@ciencias.uaslp.mx,
Ulises.Pineda@postgrad.manchester.ac.uk

Abstract. Real-time object tracking is recently becoming very important in many video processing tasks. Applications like video surveillance, robotics, people tracking, etc., need reliable and economically affordable video tracking tools. Most of current available solutions are, however, computationally intensive and sometimes require expensive video hardware. In this paper, we propose a new object tracking algorithm for real-time video that relies in the combination of a similarity measure with an euclidian metric. This approach infers the trajectory of a moving object by applying a very simple optimization method which makes the tracking algorithm robust and easy to implement. Experimental results are provided to demonstrate the performance of the proposed tracking algorithm in complex real-time video sequence scenarios.

1 Introduction

Real-time vision is an ideal source of feedback for systems that must interact dynamically with the real world. Current applications for real-time vision tracking of moving non-rigid objects range from traditional problems, such as robotic hand eye coordination and robot navigation to more recent areas of interest, such as surveillance, face recognition, user interface, video compression, etc. Most of these tasks are generally involved in very complex environments, making the process a challenge for the vision research community. The main challenge in designing a robust visual tracking algorithm is the inevitable variability in the images of the tracked object over time. Various factors can be responsible for such variations, e.g., changes in the viewpoint or illumination, agile motion, change in shape, object reflectance, or partial occlusions of the target. Under these conditions, therefore, it may be very difficult to detect and track an object in a video sequence or image frames.

This paper presents a simple but robust real-time tracking algorithm based on representing objects through their color statistical distributions. This approach will prove to be robust to environment changes such as partial occlusions, affine transformations [1], variations in illumination, and changes in the camera positions. To track a moving object, identified previously, we use the histogram [2] as the distribution model that will characterize the target object; however, a good approximation depends on the underlying metric that one uses to define the quality of the approximation. The main contribution of this work relies then in the distance expression used to locate the target. This distance combines a similarity measure with an euclidian metric, such distance

combination will prove to yield error surfaces with helpful features. These features will then be exploited to find the next object-target position applying a very simple and fast optimization method. The simplicity of the method proposed here and the experimental results indicate that the suggested tracking algorithm is robust and efficient to several environmental changes. Moreover, this algorithm requires minimal and inexpensive video equipment for its implementation. During the experiments, a basic and inexpensive web-cam that records 20 frames per second was used.

Related research works to the approach presented in this paper include the continuous adaptive mean shift system [3], called CAMSHIFT, which is proposed for face tracking. In [4], Comaniciu et al. proposed a real-time tracking algorithm for non-rigid objects that considers the use of a color histogram to model the target-object. Based on this color histogram, a similarity measure using the Bhattacharya coefficient is performed between the target object and the candidate object distribution. Other related work is presented in [6], where the Kullback-Leibler distance is used to yield the error surfaces in the tracking algorithm; in this work, a trust-region method is applied to solve the optimization problem.

The rest of the paper is organized as follows. The problem formulation and mathematical notation are presented in Section 2. Section 3 introduces the proposed tracking algorithm. The integration and set up of the experiments are discussed in Section 4. Performance evaluation of the tracking algorithm and some results are also presented in Section 4. Finally, some conclusions are drawn in Section 5 with a short remark on future work.

2 Problem Formulation

The primary goal of this work is to track a moving object that may be non-rigid, with different colors and/or texture patterns. It is then considered that an object may have different colors, texture patterns, partially occluded or changing its position by rotating in depth or changes in camera position. In order to capture the characteristics of this complex environment, we make use of a histogram representation of the target object given by its RGB color probability distribution. Following this, the color space is divided into n bins, where a single-valued bin function b is defined by the pixels's RGB values as $b : \mathbf{y} \mapsto \{1, \dots, n\}$ where \mathbf{y} is any pixel's coordinates (x, y) in the image. Thus an object can be represented by its color distribution using a color histogram. To characterize the object of interest inside the scene, we define $A(\mathbf{x})$ as a square area centered at the pixel position \mathbf{x} . The area $A(\mathbf{x})$ represents the target-object in the current frame of a video sequence. Thus the object color probability distribution can be defined as

$$p_{\mathbf{x}}(u) = \sum_{\mathbf{y} \in A(\mathbf{x})} \delta(b(\mathbf{y}) - u) \quad (1)$$

where δ is the Kronecker delta function. Assuming that the target probability distribution does not change in subsequent frames, we can simplify its notation to $p(u)$. In the same way, the probability distribution of an area enclosed by $A(x)$ in subsequent frames is defined as

$$q_{\mathbf{x}}(u) = \sum_{\mathbf{y} \in A(\mathbf{x})} \delta(b(\mathbf{y}) - u). \quad (2)$$

Using the above definition, the tracking problem can be transformed to a search problem where the distance function is given by $f(\mathbf{x}) = D(p, q_{\mathbf{x}})$, where $D(p, q_{\mathbf{x}})$ can be interpreted as a measure of similitude between p and $q_{\mathbf{x}}$. It is important to highlight the fact that such distributions can be seen as vectors in a n -dimensional space. Notice that each component of these vectors denotes the bin-value of the histogram, therefore, it will always be zero or greater than zero. There exist different types of measures to compute similarity between a target distribution and candidate distributions. Among these distance functions are for example, the Kolmogorov-Smirnov (KS) distance [7] defined as $D_{KS}(p, q_{\mathbf{x}}) = \max_u |p(u) - q_{\mathbf{x}}(u)|$, the Bhattacharya (BC) coefficient [6], $D_{BC}(p, q_{\mathbf{x}}) = \sum_{u=1}^n \sqrt{p(u)q_{\mathbf{x}}(u)}$, and the Kullback-Leivler (KL) distance [6], $D(p, q_{\mathbf{x}}) = \sum_{u=1}^n p(u) \log(p(u)/q_{\mathbf{x}}(u))$. Once a distance measure function is obtained, the tracking problem becomes an optimization problem formulated as:

$$\hat{\mathbf{x}} = \arg \min_{\mathbf{x}} f(\mathbf{x}). \quad (3)$$

From (3), it is evident that the performance of a tracking algorithm depends on the distance surface and the optimization method applied.

3 Tracking Algorithm

For tracking a moving non-rigid object in video, detecting the shape and position of the target is the primary task. Since the shape is subject to projections from a 3D space to a 2D image space, objects may suffer of some deformation due, principally, to affine transformations, then it is fundamental to search for a tracking method which must be robust to such transformations. In this section, we propose a novel tracking algorithm based on a hybrid distance function that combines a similarity measure and an euclidian metric. This hybrid distance function aims to provide a similarity measure between two object distributions which can be "robust and efficient" to different changes in the environment.

In what follows, we describe the proposed hybrid distance measure. In order to provide a measure of similarity, we also use the histogram representation but unlike other approaches, the normalized cross-correlation between the target-object histogram and the candidate region histogram is considered. Recall that a histogram can be seen as a vector, therefore, we define the normalized cross-correlation distance as

$$D_1(p, q_x) = \left(1 - \frac{p^T q_x}{\|p\| \|q_x\|}\right). \quad (4)$$

It is important to emphasize that (4) provides a measure that does not depend on the histogram's magnitude. This consideration aims to avoid the problem of scaling, leaving only the *angle* information available in the inner product between two regions' histograms. Therefore, any change in the target-object histogram (vector) magnitude will have little effect in the distance measure defined in (4). Notice that $D_1(p, q_x)$ will be always positive or zero, and will have a minimum value when p and q_x are collinear.

Towards a better understanding of this measure we show the following experiment. It consists on representing an object histogram pattern by a random vector. Aiming

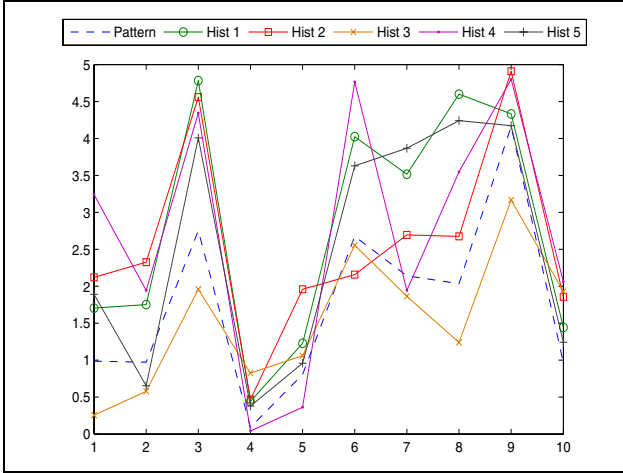


Fig. 1. Pattern and Random Histograms

to emulate the scaling effect and small variations on an object histogram, other five different random vectors are considered with the following characteristics: *i*) each element on each vector is considered to be a random variable with uniform distribution in the interval $[0, 5]$, and *ii*) the random vectors are generated such that the angle, θ_i , between each random vector and the object-histogram vector satisfies that $\cos(\theta_i) > 0.95$, $i = 1, 2, \dots, 5$. Each element of the object histogram is also generated as a uniform random variable with a distribution on $[0, 5]$. An outcome of this experiment is presented in Figure 1. Notice how the shapes of the histograms follow the shape of the object histogram pattern. All vectors having the same angle with the pattern vector, then their distance measure using (4) would yield similar values. These distance values will create a distance surface with undesired flat regions as it will be shown later. Due to these flat regions on the distance surface generated by (4), it can mislead the optimization methods, principally gradient-based methods. Therefore, an extra euclidian distance (ET) term is incorporated in (4) resulting in a new distance function

$$D_2(p, q_x) = \left(1 - \frac{p^T q_x}{\|p\| \|q_x\|}\right) + \lambda \|p - q_x\| \quad (5)$$

where λ controls the contribution of the ET term in (5).

Another consideration that has to be taken into account is the effect yielded by an object that gets close to the camera or it moves away from it. From the histogram viewpoint, these two effects may be interpreted as the representation of two different objects, therefore, to mitigate these effects we define λ to be a parameter that depends on the angle between p and q_x . The final distance measure function can then be rewritten as

$$D_3(p, q_x) = \left(1 - \frac{p^T q_x}{\|p\| \|q_x\|}\right) (1 + \lambda \|p - q_x\|). \quad (6)$$

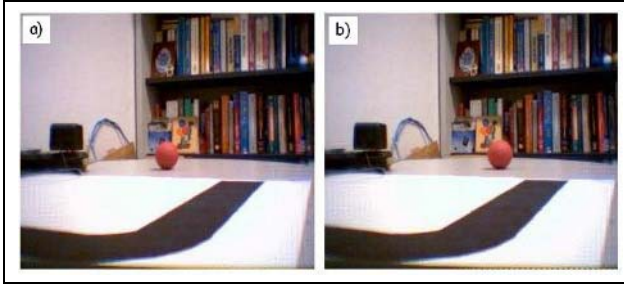


Fig. 2. Ball's location: *a)* initial position and *b)* final position

To compare this new Similarity/Euclidian distance function (SE) with those described in the previous section, the following experiment is carried out. This experiment consists in moving a ball over an area with a homogeneous surface and color changing background, see Figure 2. To run this experiment, the ball's position is captured in two time instants. The initial and final positions are shown in Figure 2 *a)* and *b)* respectively.

Figure 3 shows the surfaces computed using the distance functions KS, BC, KL and the proposed SE distance. The target distribution is set to be the pixels belonging to the area containing the ball. Analyzing these surfaces, it is observed in Figure 3 *a)* that the KS distance presents a non-flat surface around the initial ball's position with many pronounced local-minimal. The characteristics of this surface indicate that finding a global minimum represents a very difficult task due to the fact that an optimization algorithm may get trapped very easily in a local minima. In contrast, the BC and KL distance present many flat regions, making difficult the optimization process to any algorithm based on gradient information, see Figure 3 *b)* and *c)*. In [6] a tracking algorithm is presented based on the KL distance and comparisons are made with the Mean-Shift tracker [4]. In [6] a trust-region optimization method [8] is employed, obtaining, in some cases, similar results that the Mean-Shift algorithm. The principal reason of using this type of optimization methods is due to saddle points yielded by the BC and KL distances, as shown in Figure 3; although these optimization methods can avoid saddle points, the implementation is more complex and requires generally expensive equipment with high frame rate per second. Finally, Figure 3 *d)* presents the surface yielded by the proposed SE distance. The principal characteristics of this surface are that it is smooth and has very few flat regions, compared to the BC and KL distances. This plot also shows a prominent slope toward the region with minimal value, where the maximal correlation exists. Due to these properties, a very easy and fast optimization method may be envisaged to find the target position in subsequent frames.

3.1 Optimization Algorithm

The optimization problem described in the previous section involves to find the global minimum on the surface generated by the SE distance. Since the structure of this particular global optimization problem is too complex to apply analytic optimization approaches, we consider the implementation of the Nelder-Mead (NM) optimization algorithm [9]. Although this algorithm provides a weak asymptotic guarantees, it

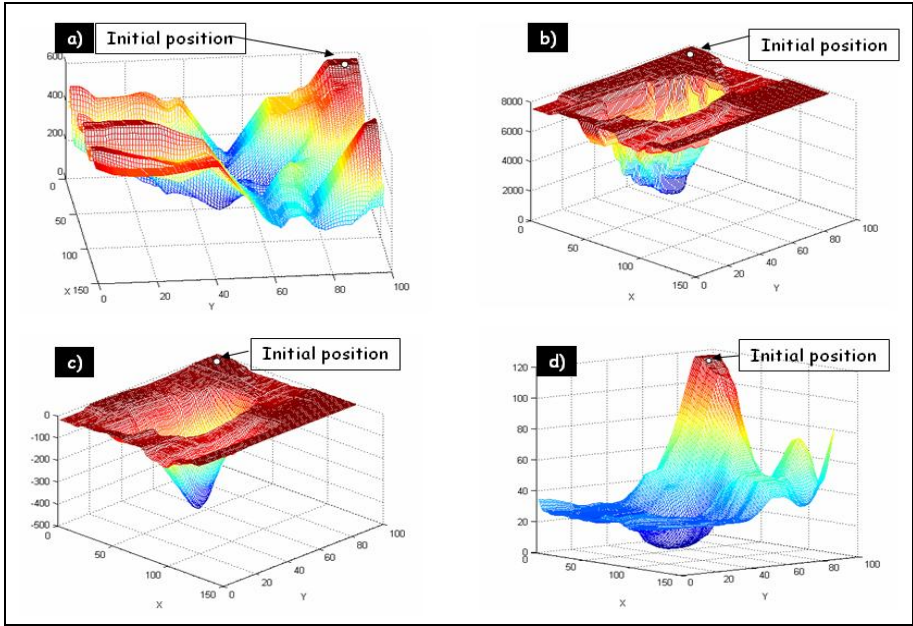


Fig. 3. a) KS, b) KL, c) BC and d) SE distance surfaces

generates a near-optimal solution quickly making the implementation fast and simple. This method attempts to minimize a scalar-valued nonlinear function using only function values, falling in the class of direct search methods. The NM method maintains at each iteration a nondegenerate simplex, a geometric figure in n dimensions of nonzero volume that is a convex hull of $n + 1$ vertices. In our case, the function values are the SE distance which depend on the pixel position $\mathbf{x} = (x, y)$ of a center window $A(\mathbf{x})$, so that a convex hull has only 3 vertices. Each iteration begins with a simplex, specified by its 3 vertices and associated function values, then one or more test points are computed, along with their functions. The iteration terminates with another simplex in which at least a point of the vertices is better or equal, in terms of function values, to the last ones.

The NM algorithm has four main parameters: reflection (ϱ), expansion (χ), contraction (γ), and shrinkage (σ). Typical values of these parameters are: $\varrho = 1$, $\chi = 2$, $\gamma = 1/2$, $\sigma = 1/2$. The outline of a single iteration of the NM algorithm can be summarized as follows:

1. **Order.** Order the $n + 1$ vertices x_i to satisfy that $f(\mathbf{x}_1) \leq f(\mathbf{x}_2) \leq \dots \leq f(\mathbf{x}_{n+1})$.
2. **Reflect.** Compute the reflection point as $\mathbf{x}_r = \bar{\mathbf{x}} + \varrho(\bar{\mathbf{x}} - \mathbf{x}_{n+1})$, where $\bar{\mathbf{x}} = \sum_{i=1}^n \mathbf{x}_i / n$ is the geometric center of a polygon calculated as the average location over n vertices. The worst point is excluded. For simplicity, let's define $f_r = f(\mathbf{x}_r)$ and $f_i = f(\mathbf{x}_i)$ for $i = 1, 2, \dots, n + 1$. If $f_1 \leq f_r \leq f_n$ accept the reflection point \mathbf{x}_r and terminate the iteration.
3. **Expand.** If $f_r \leq f_1$ (the best point in the simplex), compute the expansion point $\mathbf{x}_e = \bar{\mathbf{x}} + \chi(\mathbf{x}_r - \bar{\mathbf{x}})$ and evaluate $f_e = f(\mathbf{x}_e)$. If $f_e \leq f_r$, accept \mathbf{x}_e and terminate the iteration; otherwise (if $f_e \geq f_r$), accept \mathbf{x}_r and terminate the iteration.

4. **Contract.** If $f_r \geq f_n$, the algorithm performs a contraction operation between \bar{x} and the better between \mathbf{x}_r and \mathbf{x}_{n+1} . If $f_n \leq f_r < f_{n+1}$, an outside contraction is performed, *i.e.* $\mathbf{x}_{oc} = \bar{x} - \gamma(\mathbf{x}_r - \bar{x})$ and evaluate $f_{oc} = f(x_{oc})$. If $f_{oc} \leq f_r$, it accepts \mathbf{x}_{oc} and terminate the iteration; otherwise, go to next step (shrinkage).

On the other hand, an inside contraction $\mathbf{x}_{ic} = \bar{x} - \gamma(\bar{x} - \mathbf{x}_{n+1})$ is performed when $f_r \geq f_{n+1}$, then evaluate $f_{ic} = f(x_{ic})$. If $f_{ic} \leq f_{n+1}$, accept \mathbf{x}_{ic} and terminate the iteration; otherwise, go to step 5.

5. **Shrinkage.** Evaluate f at the n points $\mathbf{v}_i = \mathbf{x}_1 + \sigma(\mathbf{x}_i - \mathbf{x}_1)$, for $i = 2, \dots, n + 1$. These points are the new vertices of the simplex in the next iteration.

3.2 Object Tracking Optimization Procedure Via NM Algorithm

Given the color distribution p of the target-object and its pixel position \mathbf{x}_0 in the previous frame, we can use the NM algorithm to solve the search problem formulated in section 2. Therefore, the procedure to get an estimate of the object location in the current frame can be divided into three main steps:

1. Define the vertices of a simplex at the locations \mathbf{x}_0 , $\mathbf{x}_0 - (0, d)^T$, $\mathbf{x}_0 + (d, 0)^T$ where we set the value of d equal to 5 (pixels).
2. Iterate n times the NM-Algorithm, beginning with the simplex defined in step 1, and using as function the SE distance in (6) at the different points of the vertices. After the iterative process is finished, the new target object position is set to be the best vertex of the last simplex found.
3. Set \mathbf{x}_0 the best point found in the last simplex, get the current frame, and go to 1.

4 Real-Time Implementation and Experimental Results

To verify and test the proposed tracking algorithm, some real-time experiments have been conducted. The experiments are carried out using a basic web camera with a maximum frame rate of 20 frame per second (fps). The camera has been connected via an USB port to a PC with a 3.0 GHz Xeon (TM) CPU running under a Microsoft Windows XP operating system. We have implemented all camera interfaces, image processing routines and optimization algorithm using the JAVA language (TM). It is important to highlight that in order to show the simplicity and easy implementation, we have employed a conventional and inexpensive vision equipment. Moreover, our current implementation runs without any code optimization. In order to demonstrate the robustness and efficacy of our approach, we have tested the tracking algorithm with three different scenarios. Figures 4-6 show several key frames from these experiments and the tracking window. Notice that these sequences contain many difficult scenarios which a real-world tracker would likely to encounter. The experiments presented in this section were repeating several times and in all cases they showed the same results.

Tracking a man's face. The first video sequence shown in Figure 4 corresponds to a man moving along of a small office. Figure 4 a) shows the initial tracking point and the following frames (Figure 4 b) to e)) demonstrate the stability of the proposed algorithm

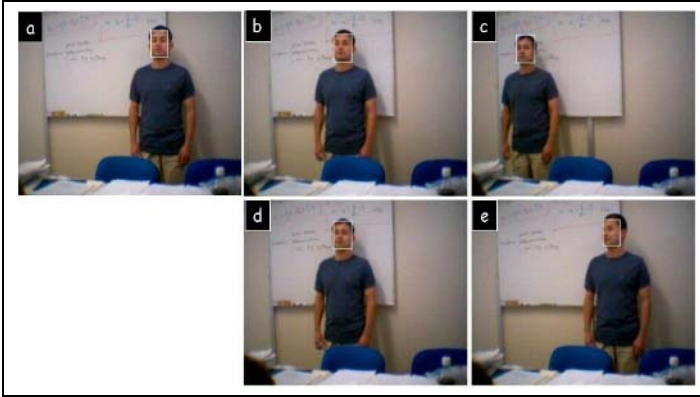


Fig. 4. Human face as target-object

to maintain the tracking of the target-object. Notice that Fig. 4 e) shows a difficult tracking frames when the man turns his head to the right. For this experiment, the RGB space has been divided into $16 \times 16 \times 16$ bins, setting $\lambda = 0.2$ and the tracking window to a 26×36 rectangular area.

Tracking an homogenous object. In a second experiment, a red object controlled by a crane has been set as the target object. The object is set to follow a predetermined trajectory, in any of the (x,y,z) coordinates of a cubic structure, controlled by the crane. The web-cam lens has been placed in front of one of the faces of the crane's structure forming a parallel plane. We have tested the trajectory tracking algorithm by setting a trajectory where the target-object moves closer and away from the camera's position. This effect intends to test the robustness of the algorithm to scale-transformation of the target-object. Figure 5 shows four different frames of the video sequence. It can be seen how the target-object is tracked successfully by the proposed algorithm.

Tracking a car. One last experiment is shown in Figure 6. This experiment consists on tracking a car that moves back and forth to different speeds. The web-cam is set about $1.60m$ above of a flat surface in such a way that all movements can be captured by the camera. The used car has 8 different speeds ranged form 11.2 cm/s to 134.0 cm/s approximately. The main purpose of this experiment is to investigate the robustness of the proposed algorithm as a function of the object's speed. To evaluate the tracking competence of the proposed SE algorithm, the MS algorithm is also implemented and experimental results are compared under the same scenario. The video sequence shown in Figure 6 a) and b) illustrates the performance of the MS tracking algorithm. Figure 6 c) and d) shows the corresponding performance results when the SE tracking algorithm is applied. Results in Figure 6 a) are obtained when the car is moving at the speed of 44.5 cm/s while those obtained in Figure 6 b) are for a speed of 134 cm/s . It is observed from these results that the MS algorithm performs successfully when the car moves at low speed. Increasing the car's velocity has resulted in the MS algorithm to be incapable of tracking the car as the object is lost completely. On the other hand, Figure 6 c) and d) illustrate the capability of the SE algorithm to track the car's trajectory during all the

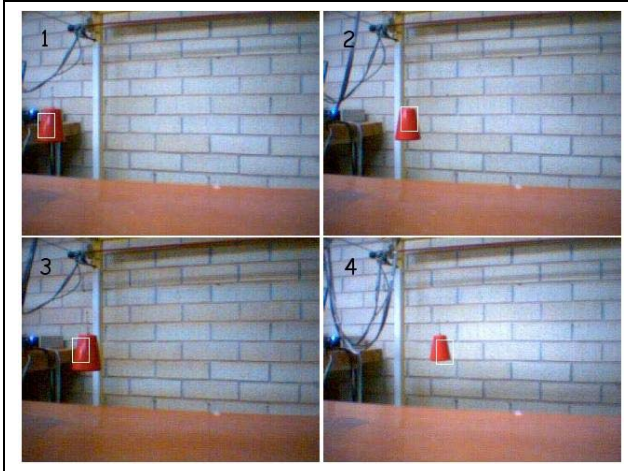


Fig. 5. Tracking a scale-transformed object

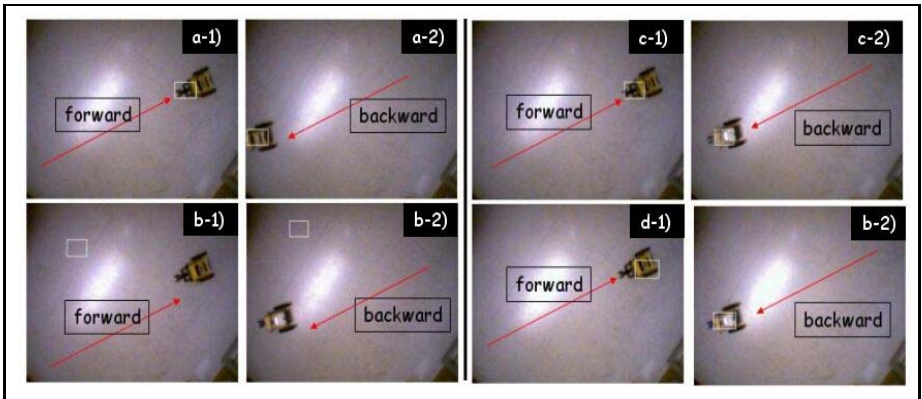


Fig. 6. Results of tracking a car at different speeds using the MS-algorithm (panels *a* and *b*) and SE-algorithm (panels *c* and *d*)

experiment when the car's velocity was either 44.5cm/s or 134cm/s . The same performance has been achieved by repeating the experiment but changing the car's velocity in the range from 44.5cm/s to 134cm/s linearly.

5 Conclusions and Future Work

In this paper, we have introduced a new tracking algorithm based on the histogram information of the target-object and a distance measure (SE distance) composed by two terms: similarity and euclidian. The proposed SE distance function comprises some properties that makes it suitable for real-time object tracking. These properties allow us

the implementation of a simple and fast algorithm for the optimization problem formulated in this paper. For this, we have applied the well-know Nelder-Mead optimization algorithm. A number of experiments have been carried out to test our approach. The results obtained here are encouraging and support our speculation about the applicability of the SE distance function for real-time object tracking. As part of the results, a comparison between the SE and MS tracking algorithms was also performed. This comparison revealed that the proposed algorithm outperforms the MS algorithm as a function of the increment in the object's velocity. Future research focuses on extending the proposed algorithm to the problem of multiple object tracking, and to a further analysis of the critical parameters such as the bin number n or the λ parameter.

Acknowledgement. This research work was supported by Grant PROMEP/103.5/04/1387 and PROMEP/103.5/04/1386.

References

1. E. Trucco: Introductory techniques for 3D computer vision. Prentice Hall, NJ (1998).
2. S.T. Birchfield: Elliptical Head Tracking Using Intensity Gradients and Color Histograms. Proc. Conf. Computer Vision and Pattern Recognition, (1998) 232-237.
3. G.R. Bradski: Computer Vision Face Tracking for Use in a Perceptual User Interface, Intel Technology Journal., (1998)
4. D. Comaniciu, V. Ramesh, P. Meer: Real-Time Tracking of Non-Rigid Objects Using Mean Shift, Proc. Conf. Computer Vision and Pattern Recognition, Vol. 2, (2000) 142-149
5. Tyng-Luh Liu, Hawwann-Tzong Chen: Real-Time Tracking Using Trust-Region Methods, IEEE Trans. on Patter Recognition and Machine Intelligence, Vol. 26, No. 3, (2004) 397-402
6. Hawwann-Tzong Chen, Tyng-Luh Liu: Trust-Region Methods for Real-Time Tracking, IEEE 8th International Conference on Computer Vision , Vol. 2, No. 3, (2001)
7. Chakravarti, Laha, Roy: Handbook of Methods of Applied Statistics, Volume I, John Wiley and Sons, (1967) 392-394.
8. J. Nocedal, S. J. Wright: Numerical Optimization, Springer-Verlang, New York, (1999)
9. Nelder J.A., Mead R.: A Simplex Method for Function Minimization, Computer Journal, Vol. 7, Issue 4 (1965) 308-313.

Efficient Method to Perform Isomorphism Testing of Labeled Graphs

Shu-Ming Hsieh, Chiun-Chieh Hsu, and Li-Fu Hsu

Dep. Information Management,
National Taiwan University of Science and Technology,
Taipei, Taiwan

Abstract. The need to perform isomorphism testing is emerging recently in many application domains such as graph-based data mining for discovering frequent common patterns in a graph database. Due to the complex nature of graph representations, the isomorphism testing between labeled graphs is one of the most time-consuming phases during the mining process. The canonical form of a graph that serves as the isomorphism certificate needs $O(n!)$ to produce for a graph of order n , or $\Theta(\prod_{i=1}^c (|\pi_i|!))$ if vertex invariants are employed to divide n vertices into c equivalence classes with $|\pi_i|$ vertices in each class i . In this paper, we propose a new algorithm to perform isomorphism testing of labeled graphs with worst case time complexity $O(\sum_{i=1}^c (|\pi_i|!))$, in which the product of all $|\pi_i|!$ terms is replaced by the sum of the terms and the asymptotic notation is changed from big theta to big oh. To the best of our knowledge, this proposed model is the latest work that focuses on the dealing of the isomorphism testing of labeled graphs. The result of this algorithm is directly applicable to the fields of graph isomorphism testing for labeled graphs.

1 Introduction

Graphs are suitable for modeling a variety of real-world complex structures with the benefits of being capable of characterizing the spatial, topological, and geometric properties among the objects in the modeled data sets [11]. In many application areas, objects are symbolized as vertices in a graph and the relationships between two objects are represented as edges joining these two corresponding vertices. Furthermore, each vertex and edge is assigned a label to denote the class to which an object belongs and the attributes of relations that held between objects, respectively. In a molecular structure, an atom corresponds to a vertex and a bond between two atoms is represented as an edge. The vertices are assigned labels that stand for the atom types (e.g. C, H) and the labels of edges are the bond types or the relative 3D orientations between a pair of atoms [1][10]. In the geographical information systems (GIS), objects or spatial elements are vertices while the relationships between two objects are edges that hold the information of adjacency, connectivity, and containment [16]. Another example is the field of image retrieval and similarity evaluation, in which vertices denote the recognized objects in an image and edges are the spatial relationships

between pairs of objects. The labels of vertices and edges are the class names to which objects belong and the type of relationships between objects, respectively [7][8][15]. Taking the molecular biology as an example, mining the frequent topological structures in order to identify novel RNAs or protein structures is vital for researchers in this field [1][10]. Finding frequent common chemical substructures are also helpful for toxicologists to classify new toxic substances [9].

The subgraph isomorphism testing problem is known to be an NP-complete problem while it remains an open question that whether the graph isomorphism testing is NP-complete or polynomial solvable [2][6]. Some researchers classified this kind of problems as ISO-complete (isomorphism-complete) problems [6]. Since labeled graphs are polynomial-reducible to *normal graphs*, which are those graphs with no labels but only with vertex identifiers, it remains challenging for the efforts on labeled graphs.

Most of the previous works are dedicated to normal graphs [3][4][5]. Among these efforts, the NAUTY algorithm is known to be one of the fastest algorithms for normal graph isomorphism [11][12][18]. The vertices are divided into several sets with the same vertex invariants, which include the degree of a vertex and the numbers of its neighbors having certain degrees. Then it checks the graph isomorphism between the corresponding subsets of vertices in a brute force manner [5][13]. However, NAUTY does not allow graphs to have edge labels hence it is not applicable to the isomorphism testing of labeled graphs [11][12]. An algorithm named VF2 [4] that improves the data structures employed to make it suitable for matching graphs with large number of vertices and edges. In some kinds of graphs and in graphs of certain orders, it outperforms NAUTY while in other situations it does not. The VF2 algorithm is similar to NAUTY in that they can only be adapted to normal graphs. As for labeled graphs, FSG [11] combines several types of vertex invariants to partition the vertices into equivalence classes. The canonical code of a graph is defined to be the vertex labels followed by the concatenation of the columns of the upper triangular adjacency matrix over all possible permutations of the vertices, where a vertex can only be permuted within the class it belongs. If the vertices of a graph are partitioned into c classes $\pi_1, \pi_2, \dots, \pi_c$, then the number of different permutations need to be considered in order to find the canonical code is $\prod_{i=1}^c (|\pi_i|!)$, which is claimed to be substantially faster than the $n!$ permutations required by the earlier approaches [11]. The length of a candidate code is $\Theta(n^2)$ for a graph with n vertices, hence comparing a pair of candidate codes takes $\Theta(n^2)$ time. Since there are exactly $\prod_{i=1}^c (|\pi_i|!)$ candidates, the total time needed to obtain the canonical code is $\Theta(n^2 \prod_{i=1}^c (|\pi_i|!))$.

In this paper, we propose a new algorithm *CISC* (Class-wise ISomorphism testing with limited baCktracking) to perform the isomorphism testing of labeled graphs. *CISC* combines the benefits of *backtracking* and *dynamic programming* to improve the overall performance. The theoretical worst case time complexity is $O(n \sum_{i=1}^c (|\pi_i|!))$, in which the product of all $|\pi_i|!$ terms is replaced by the sum of the terms and the asymptotic notation is changed from big theta to big oh, compared with $\Theta(n^2 \prod_{i=1}^c (|\pi_i|!))$. For example, if a labeled graph with 20 vertices

is divided into 5 vertex classes with the sizes 3, 5, 6, 4, and 2, the number of all candidate codes is $3! \times 5! \times 6! \times 4! \times 2! (= 69120000)$. The contribution of this work, which will be stated in the following paragraphs, is to substitute the product with summation as upper bound, it becomes $3! + 5! + 6! + 4! + 2! (= 872)$.

The remaining of the paper is organized as follows. Section 2 is the definitions about labeled graphs and proofs of some lemmas of our proposed algorithm. In section 3, we will introduce the algorithm. The discussion about finer partition is included in section 4. Section 5 concludes our work with some remarks.

2 Background and Definition

A *labeled graph* is a graph that the vertices and edges are assigned labels according to the properties they possess. The labels of edges convey the types of relationships between two vertices. Note that the labels of vertices (or edges) are not necessarily different, many vertices (or edges) in a graph can be assigned the same labels. Similar to normal graphs, each vertex of a labeled graph is given a *vertex id*, denoted as v_i or w_i , to recognize a vertex from the others. The vertex *ids* are given in arbitrary and do not possess any further meaning. The labeled graph G in Fig. 1 gives us some examples such as $l(v_2) = B$ and $l(v_2, v_3) = x$, where l is a function that maps every vertex and edge a label.

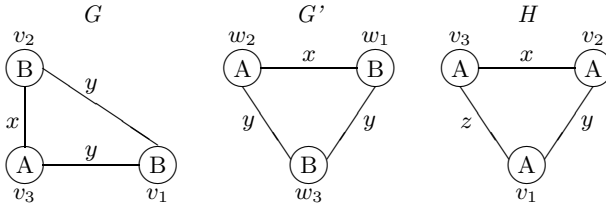


Fig. 1. Labeled Graphs

Two labeled graphs are isomorphic if we can find a one-to-one and onto function between the vertices of these two graphs where the vertex labels, edge labels, and adjacency relations are preserved through the mapping.

Definition 1 (Isomorphism of Labeled Graphs). $G = (V, E, L_V, L_E, l)$ is isomorphic to $G' = (V', E', L'_V, L'_E, l')$, iff there exists a bijective function $f : V \rightarrow V'$ such that: 1. $\forall u \in V, l(u) = l'(f(u))$. 2. $\forall u, v \in V, (u, v) \in E \leftrightarrow (f(u), f(v)) \in E'$. 3. $\forall (u, v) \in E, l(u, v) = l'(f(u), f(v))$.

For example, we can find a bijection f such that $f(v_1) = w_3, f(v_2) = w_1, f(v_3) = w_2$ between graphs G and G' in Fig. 1. Isomorphism is a symmetric relation (also a reflexive and transitive relation), which is denoted as $G \cong G'$. Some approaches employ the canonical codes as isomorphism certificates to determine the isomorphism of two labeled graphs [9][11]. A canonical code is an identifier of a graph such that two graphs are isomorphic to each other if and only if they have the same canonical codes. Canonical codes can be defined by any reasonable representation. For example, it can be the smallest string obtained by concatenating

all the vertex labels with the columns of the upper triangular entries of the adjacency matrices over all possible permutation of vertices [11]. The time complexity to obtain the canonical code of a graph of order n is $O(n!)$. For example, there are $3!$ possible permutations for the 3 vertices in graph H of Fig. 1. The canonical code is obtained by the order (v_2, v_3, v_1) , which corresponding to the canonical code AAxyz. In order to reduce the number of possible permutations, the vertex invariants are popularly employed by many recent works [11]. Vertex invariants are some inherent properties of the vertices that are preserved across isomorphism mappings such as vertices labels and degrees. Vertices with the same values of the vertex invariants will be partitioned into the same equivalence class. If vertices of a graph are partitioned into c classes $\pi_1, \pi_2, \dots, \pi_c$, the time complexity to obtain the canonical code is $\Theta(n^2 \prod_{i=1}^c (|\pi_i|!))$ [11].

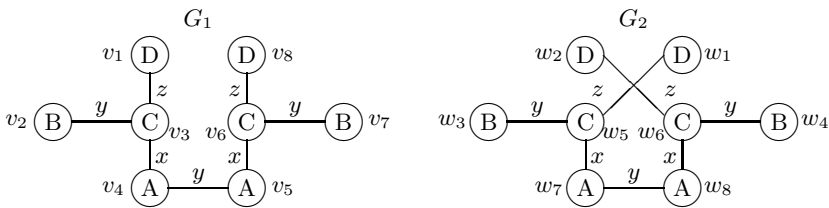


Fig. 2. Two Isomorphic Labeled Graphs

Definition 2 (Vertex Signature). For a vertex v with m neighbors v_1, v_2, \dots, v_m , the signature of vertex v is a string defined as: $sig(v) = l(v)l(v, v_{p(1)})l(v_{p(1)})l(v, v_{p(2)})l(v_{p(2)}) \dots l(v, v_{p(m)})l(v_{p(m)})$, where $p(1), p(2), \dots, p(m)$ is a permutation of $1, 2, \dots, m$, $l(v)$ is the vertex label of vertex v , $l(v_{p(k)})$ is the vertex label of vertex $v_{p(k)}$, $l(v, v_{p(k)})$ is the edge label of edge $(v, v_{p(k)})$. $l(v, v_{p(k)}) \leq l(v, v_{p(k+1)})$ and $l(v_{p(k)}) \leq l(v_{p(k+1)})$ if $l(v, v_{p(k)}) = l(v, v_{p(k+1)})$.

Therefore the signature of a vertex with m neighbors is the vertex label of the vertex followed by m pairs of edge label and vertex label. The vertex signatures of $sig(v_3)$ in G_1 of Fig. 2 is CxAyBzD and AxCyA for $sig(v_4)$. The comparisons of vertex signatures are performed as string comparisons. For a vertex v of degree m , the time to acquire the signature is $O(m \log m)$, which is the time to sort the pairs of edge label and vertex label. The neighbors with larger/smaller vertex signatures of a vertex v are called the larger/smaller neighbors of v . Hence the larger neighbor of vertex v_3 of graph G_1 in Fig. 2 is v_1 , while the smaller neighbors of v_3 are v_2 and v_4 . Also, all the vertices with the same vertex signatures as vertex v are called the peer vertices of v . We can define the graph signature of a graph from vertex signature as follows.

Definition 3 (Graph Signature). For a graph G with n vertices v_1, v_2, \dots, v_n , the signature of G is a string defined as: $Sig(G) = sig(v_{p(1)})sig(v_{p(2)}) \dots sig(v_{p(n)})$, where $p(1)p(2) \dots p(n)$ is the permutation of $1 \sim n$, and $sig(v_{p(k)}) \leq sig(v_{p(k+1)})$, $1 \leq k \leq n - 1$, $sig(v)$ is the signature of vertex v .

The graph signature of graph G_1 in Fig. 2 is the concatenation of $sig(v_4), sig(v_5), sig(v_2), sig(v_7), sig(v_3), sig(v_6), sig(v_1), sig(v_8)$. The upper bound to obtain the graph signature of a labeled graph with n vertices and m edges is $O(n^2 \log n + m \log m)$, which is the time to sort the symbols within each vertex signature and then sort all the vertex signatures. The length of a graph signature is $O(n + m)$, which is the same order of the size of the adjacency list [17]. The equality of two graph signatures is the necessary condition for these two graphs to be isomorphic. Therefore we can employ graph signatures as the first-step filter of isomorphism testing. The performance gain brought by this filter is that with this polynomial-time effort, one can declare the dismissal even the time-consuming matching process has not begun yet. This property is proved as lemma 1 in the appendix.

The relation "equal vertex signature" is an equivalence relation on the vertices of a labeled graph, since it is trivial to see that equality of vertex signatures is reflexive, symmetric, and transitive. Hence the vertices of a graph are partitioned into equivalence classes where all vertices in the same class have the same signatures. We define the ordered partition on a graph as follows.

Definition 4 (Ordered Partition). The vertices of a labeled graph G are partitioned by the vertex signatures into c classes, the ordered partition $\pi(G) = \pi_1(G), \pi_2(G), \dots, \pi_c(G)$ satisfies the following properties :

1. For all vertices $u, v \in \pi_k(G), sig(u) = sig(v), \forall k, 1 \leq k \leq c$
2. For all pairs of vertices $u \in \pi_k(G), v \in \pi_h(G), sig(u) < sig(v)$ if $k < h$

For the vertex signatures defined in definition 2, the ordered partitions on graph G_1 and G_2 of Fig. 2 are $\pi(G_1) = \{\pi_1(G_1) = \{v_4, v_5\}, \pi_2(G_1) = \{v_2, v_7\}, \pi_3(G_1) = \{v_3, v_6\}, \pi_4(G_1) = \{v_1, v_8\}\}$ and $\pi(G_2) = \{\pi_1(G_2) = \{w_7, w_8\}, \pi_2(G_2) = \{w_3, w_4\}, \pi_3(G_2) = \{w_5, w_6\}, \pi_4(G_2) = \{w_1, w_2\}\}$, respectively. Each vertex v belongs to a unique class, which is denoted as $class\#(v)$. The vertices within a class are ordered by their vertex ids. For example, $class\#(v_3) = 3$ and $\pi_{2,2}(G_1) = v_7$ in Fig. 2. We define $\pi_4(G_1)$ as the largest class of the partition $\pi(G_1)$ and $\pi_1(G_1)$ as the smallest class.

Due to the limit of the paper size, the lemmas are stated and proved in the appendix. Lemma 2 states that a vertex of G_1 can only be mapped to a vertex in the corresponding class of G_2 , i.e., the class numbers of vertices are preserved across the isomorphism mappings. Lemma 4 states that for a pair of vertices $(v, w), v \in \pi_k(G_1), w \in \pi_k(G_2), v$ cannot be mapped to w if any larger neighbor v_i of v cannot be mapped to any larger neighbor of w . Lemma 5 reveals that G_1 is isomorphic to G_2 if and only if we can find *local bijections* between each pair of classes $\pi_k(G_1)$ and $\pi_k(G_2)$.

3 The Proposed Algorithm

The key features of the proposed algorithm *CISC* are the following:

1. it compactly encodes the vertex invariants into vertex and graph signatures and performs signature comparisons in linear time;

2. it combines the spirits of backtracking and dynamic programming and limit the backtracking occur only between each pair of corresponding classes, thus achieve the performance to the upper bound of $O(\sum_{i=1}^c (|\pi_i|!))$ instead of $\Theta(\prod_{i=1}^c (|\pi_i|!))$;
3. it uses efficient techniques by which the feasibility testing of two vertices can be conducted by considering only a portion of their neighbors (larger neighbors only), thus reduces the time needed in most practical computations.

3.1 Algorithm *CISC*

CISC employs the graph signatures of two labeled graphs as the *first-step filter* according to lemma 1. The testing process can be immediately terminated and returns a *false* signal when a pair of unequal graph signatures is encountered. Otherwise two ordered partitions according to these graph signatures will be made. The algorithm then tries to find local bijections between each pair of corresponding classes ($\pi_k(G_1)$ and $\pi_k(G_2)$), from the largest classes ($k = c$) to the smallest ones ($k = 1$). From the fact of lemma 5, the testing procedure fails if there exists any pair of corresponding classes between which no bijection can be found. The procedure for finding the local bijection follows the principle of backtracking. During the matching process, the local bijections of larger classes that have already been computed are references. This is the key spirit of *dynamic programming* during the problem solving process [14]. Due to the paper size limit, only the main program and procedure *Class_Test* is listed as below.

Algorithm. *Isomorphism_Test*(G_1, G_2)

Input : two labeled graphs G_1 and G_2

Output : If $G_1 \cong G_2$ return *True*, return *False* otherwise

Begin

1: Calculate the graph signatures of G_1 and G_2

2: **If** *Sig*(G_1) \neq *Sig*(G_2) **Then** return *False* // first-step filter

3: Make ordered partitions $\pi(G_1)$ and $\pi(G_2)$ from *Sig*(G_1) and *Sig*(G_2)

4: **For** *class* $\# \leftarrow |\pi(G_1)|$ **downto** 1 **Do** // the number of classes of $\pi(G_1)$

5: **If** *Class_Test*(*class* $\#$) **Is** *False* **Then** //not all vertices can be mapped

6: return *False*

7: return *True*

End Algorithm

Procedure. *Class_Test*(*class* $\#$)

Input : *class* $\#$: a class number of $\pi(G_1)$

Output : return *True* if $\pi_{class\#}(G_1)$ can be mapped to $\pi_{class\#}(G_2)$

Begin

1: $m \leftarrow$ the number of vertices in the class $\pi_{class\#}(G_1)$

2: *GlobalFlag* \leftarrow *False* //if at least one solution exists

3: Call *DFS_Traverse*(0, m , *class* $\#$) //find all possible mappings

4: return *GlobalFlag*

End Class_Test

The procedure $Class_Test(class\#)$ searches the local state space in a *depth first search* (DFS) style [14] to find all possible local bijective functions between a pair of classes $\pi_{class\#}(G_1)$ and $\pi_{class\#}(G_2)$. The class with the largest $class\#$ is performed $Class_Test$ first. A procedure $Feasibility_Test$ called by $Class_Test$ performs the feasibility testing of the pair of vertices (v, w) , where $v \in \pi_{class\#}(G_1)$ and $w \in \pi_{class\#}(G_2)$ (v and w have the same class number in G_1 and G_2 , respectively). The whole process of feasibility testing includes two phases: *peer test* and *larger – neighbor test*. Peer test is to verify the preservation of adjacency and edge labels for the already matched peer vertices of v (the vertices in the same class as v). Taking an example from Fig. 2, when v_4 in G_1 and w_7 in G_2 are under feasibility testing, we need to perform peer test between each mapped vertices pair such as v_5 in G_1 and w_8 in G_2 . The second phase larger-neighbor test is to assure that every larger neighbor v_i of v can be mapped to a larger neighbor w_j of w in graph G_2 . Since $class\#(v_i) > class\#(v)$ and we start the mapping from the classes with larger class numbers, all the vertices that can be mapped by v_i have already been found. For the vertices pair v_4 and w_7 again, the larger-neighbor test will be performed on the pair v_3 and w_5 since v_3 is a larger neighbor of v_4 and w_7 a larger neighbor of w_5 .

3.2 Correctness Proof

Theorem 1. Algorithm $CISC$ is correct, i.e., 1) if $CISC$ reports that no isomorphism exists, there is indeed no isomorphism. 2) if $CISC$ reports that the isomorphism exists, then the reported function is correct.

Proof:

1) No false dismissal occurs, because:

1. $Class_Test$ will search the whole local state space tree in DFS style if necessary, thus all possible matching solutions between $\pi_i(G_1)$ and $\pi_i(G_2)$ will be verified, and
2. $Feasibility_Test(v, w)$ only considers the larger neighbors of this pair of vertices v and w , since we do not check the possible smaller neighbors, nor the neighbors of neighbors, etc. Hence a promising pair only satisfies necessary constraints.

2) No false alarm occurs because:

1. The preservation of vertex labels is assured since a vertex v in class $\pi_i(G_1)$ can only be mapped to a vertex w in class $\pi_i(G_1)$, while vertices in the corresponding classes have the same vertex labels.
2. The preservation of edge labels is assured. Suppose $v_1, v_2 \in V(G_1)$, $w_1, w_2 \in V(G_2)$, where $f(v_1) = w_1$, $f(v_2) = w_2$, by the reported isomorphism function f . Also suppose that $l(v_1) = l(w_1)$, $l(v_2) = l(w_2)$, but $l(v_1, v_2) \neq l(w_1, w_2)$, then only 3 cases about the class numbers of vertices v_1 and v_2 may exist: (a) $class\#(v_1) = class\#(v_2)$: this case is impossible since *peer test* excludes this possibility. (b) $class\#(v_1) < class\#(v_2)$: v_2 and w_2 must pass the feasibility test before (v_1, w_1) is tested since larger classes are handled earlier. In

feasibility_test(v_1, w_1), if $l(v_1, v_2) \neq l(w_1, w_2)$, then w_1 will not be mapped by v_1 if v_2 is mapped to w_2 , thus $f(v_1) \neq w_1$, which contradicts the assumptions. (c) $class\#(v_1) > class\#(v_2)$: analogous to case (b), which is impossible.

3. The preservation of adjacency relations is assured. The proof is similar to the previous one. Due to the limit of paper size, it is omitted.

3.3 Complexity Analysis

The dominating part of *CISC* is step 4 in the main program, the *Class Test* loop, which is the sum of the time needed to execute *Class Test* on each class. The maximal number of nodes in the local search space tree for a class with $|\pi_i|$ vertices is $|\pi_i|!$. Thus the maximal number of nodes in these c state space trees is $O(\sum_{i=1}^c (|\pi_i|!))$. The work on each node of a search tree is the feasibility testing of a vertex pair (v, w) , where $v \in V(G_1)$ and $w \in V(G_2)$. The feasibility testing is a linear-time work and the reasons are stated as follows. Since feasibility testing is composed of two parts (peer test and larger-neighbor test) as stated above, the procedure peer test needs at most $|\pi_i|$ edge label comparisons, $|\pi_i| < n$. The procedure larger-neighbor test verifies the larger neighbors of vertex v and stops as soon as one of the larger neighbors is not recorded to be mapped to any larger neighbors of vertex w . The number of the larger neighbors of a vertex is at most $n-1$. Therefore, the worst case time complexity is $O(n \sum_{i=1}^c (|\pi_i|!))$.

4 Conclusion

The proposed algorithm *CISC* (Class-wise ISomorphism testing with limited baCktracking) utilizes the specific feature of labeled graphs to compactly encode the vertex invariants into vertex signatures and performs signature comparisons in linear time. It limits the backtrackings occur only within the same partition class, thus achieve the performance upper bound of $O(\sum_{i=1}^c (|\pi_i|!))$ instead of $\Theta(\prod_{i=1}^c (|\pi_i|!))$. The result of *CISC* is directly applicable to those fields that need to perform graph isomorphism testing of labeled graphs such as finding the frequently recurring subpatterns of graph-modeled domains in geographical information systems, bioinformatics, and image retrieval, etc.

References

1. Artymiuk P., Poirrette A., Grindley H., Rice D., Willett P.: A Graph-theoretic Approach to the Identification of Three-dimensional Patterns of Amino Acid Side-chains in Protein Structures, *Journal of Molecular Biology*, 243(2), (1994) 327-344.
2. Chartrand G., Zhang P. (ed.): *Introduction to Graph Theory*, McGraw Hill, New York (2002).
3. Conte D., Foggia P., Sansone C., Vento M.: Thirty Years of Graph Matching in Pattern Recognition, *Int'l Journal of Pattern Recognition and Artificial Intelligence*, 18(3), (2004) 265-298.
4. Cordella L., Foggia P., Sansone C., Vento M.: A (Sub)Graph Isomorphism Algorithm for Matching Large Graphs, *IEEE Tran. Pattern Analysis and Machine Intelligence*, 26(10), (2004) 1367-1372.

5. Foggia P., Sansone C., Vento M.: A Performance Comparison of Five Algorithms for Graph Isomorphism, Proc. of the 3rd IAPR-TC15 Workshop on Graph-based Representation (2001).
6. Gross J., Yellen J.(ed.), Handbook of Graph Theory, CRC Press, Florida (2004).
7. Hsieh S. M., Hsu C. C.: New Method for Similarity Retrieval of Iconic Image Database, Proceedings of 2005 SPIE-IS&T Symposium on Electronic Imaging: Conference on Storage and Retrieval Methods and Applications for Multimedia, Vol. 5682, (2005) 247-257.
8. Hong P., Huang T.: Mining Inexact Spatial Patterns, Workshop on Discrete Mathematics and Data Mining(2002).
9. Huan J., Wang W., Prims J.: Efficient Mining of Frequent Subgraph in the Presence of Isomorphism, University of North Carolina Computer Science Technical Report(2003).
10. Kim N., Shiffeldrim N., Gan H., Schlick T.: Candidates for Novel RNA Topologies, Journal of Molecular Biology, 34(1), (2004) 1129-1144.
11. Kuramochi M. and Karypis G.: An Efficient Algorithm for Discovering Frequent Subgraphs, IEEE Trans. Knowledge and Data Engineering, 16(9), (2004) 1038-1051.
12. McKay B. D.: Nauty Users Guide, <http://cs.anu.edu.au/~bdm/nauty>(2003).
13. McKay B. D.: Practical Graph Isomorphism, Congressus Numerantium, Vol. 30, (1981) 45-87.
14. Neapolitan R. Naimipour, K.: Foundations of Algorithms, D. C. Heath and Company, Massachusetts(1996).
15. Petrakis E., Faloutsos C., Lin K.: ImageMap: An Image Indexing Method Based on Spatial Similarity, IEEE Trans. Knowledge and Data Engineering, 14(5), (2002) 979-987.
16. Theobald D.: Topology revisited: representing spatial relations, Int'l Journal of Geographical Information Science, 15(8), (2001) 689-705.
17. Valiente G.: Trading uninitialized space for time, Information Processing Letters, 92, (2004) 9-13.
18. Washio T., Motoda H.: State of the Art of Graph-Based Data Mining, ACM SIGKDD Exploration Newsletters, 5(1), (2003) 59-68.
19. Yan X., Han J.: gSpan: Graph-Based Substructure Pattern Mining, Proceedings of 2002 IEEE Int'l Conference on Data Mining (2002).

Appendix

Lemma 1. *Given two graph signatures $Sig(G_1)$ and $Sig(G_2)$ of labeled graphs G_1 and G_2 , respectively. G_1 is not isomorphic to G_2 if $Sig(G_1) \neq Sig(G_2)$.*

Proof: we prove this lemma by showing that if G_1 is isomorphic to G_2 , then $Sig(G_1) = Sig(G_2)$. Since $G_1 \cong G_2$, there exists a bijection f that maps each vertex v_i of G_1 to a vertex $f(v_i)$, namely w_i , of G_2 . It is easy to see that $sig(v_i) = sig(w_i)$, because otherwise some of the preservations of edge labels, vertex labels, or adjacency relations must be violated between these two vertices. Since the graph signature of a graph is the string obtained by sorting all the vertex signatures in this graph, these two graph signatures must be equal.

Lemma 2. *Let $\pi(G_1)$ and $\pi(G_2)$ are the ordered partitions of labeled graphs G_1 and G_2 , respectively. If $G_1 \cong G_2$ and f is the isomorphism function, then $class\#(v) = class\#(f(v)), \forall v \in V(G_1)$.*

Proof: From lemma 1 we know that $sig(v) = sig(f(v))$, for all v of G_1 . Since the classes of an ordered partition is in increasing order of vertex signatures and no two classes have the same signatures, it follows that v and $f(v)$ must in the corresponding classes of two partitions $\pi(G_1)$ and $\pi(G_2)$, hence $class\#(v) = class\#(f(v))$.

Lemma 3. *Let $\pi(G_1)$ and $\pi(G_2)$ are the ordered partitions of labeled graphs G_1 and G_2 , respectively. If $G_1 \cong G_2$, then:*

1. $sig(\pi_k(G_1)) = sig(\pi_k(G_2)), 1 \leq k \leq c$, c is the number of partition classes
2. $|\pi_k(G_1)| = |\pi_k(G_2)|, 1 \leq k \leq c$

Proof: let f be the isomorphism function, from lemma 2 we have $class\#(v) = class\#(f(v))$ for all v in G_1 . Therefore vertices in the corresponding classes of two ordered partitions have the same vertex signatures. Furthermore, since f is one-to-one and onto, the numbers of vertices in the corresponding classes of two ordered partitions must be identical.

Lemma 4. *For any vertices $v \in \pi_k(G_1)$, $w \in \pi_k(G_2)$, and a larger neighbor v_i of v (v_i adjacent to v and $class\#(v_i) > class\#(v)$), if v_i cannot be mapped to any larger neighbor of w in graph G_2 , then v is impossible to be mapped to w by any isomorphism function.*

Proof: suppose there is an isomorphism function f that maps v to w and maps v_i to a vertex w_j in G_2 . Vertex w_j is not adjacent to w as assumed. From the definition of isomorphism we have $l(v, v_i) = l(w, w_j)$, which is a contradiction since we know that v_i is adjacent to v but w_j is not adjacent to w . Thus no such isomorphism function f exists. Actually, this lemma holds for all neighbors of v , but if we can find a v_i that is a larger neighbor of v that cannot be mapped, it is by no chance that v can be mapped to w . In other words, each larger neighbor of a vertex v in G_1 can be mapped to a larger neighbor of a vertex w in G_2 is only a necessary condition for v to be mapped to w .

Lemma 5. *Let $\pi(G_1)$ and $\pi(G_2)$ are the ordered partitions of labeled graphs G_1 and G_2 , respectively. If we cannot find a bijection that maps each vertex $v \in \pi_k(G_1)$ to a vertex $w \in \pi_k(G_2)$, for some k , $1 \leq k \leq c$, then G_1 is not isomorphic to G_2 .*

Proof: since no bijection exists between $\pi(G_1)$ and $\pi(G_2)$, there exist at least one vertex $v \in \pi_k(G_1)$ that cannot be mapped to any vertex of $\pi_k(G_2)$. From lemma 2 we know that v cannot be mapped to a vertex in the classes other than $\pi_k(G_2)$. Thus no bijection exists that map v to any vertex of $V(G_2)$, G_1 is not isomorphic to G_2 .

Camera Motion Parameter Estimation Technique Using 2D Homography and LM Method Based on Projective and Permutation Invariant Features

JeongHee Cha and GyeYoung Kim*

School of Computing, Soongsil University, Sangdo 5 Dong, DongJok Gu, Seoul, Korea
pelly@vision.ssu.ac.kr, gykim11@ssu.ac.kr

Abstract. Precise camera calibration is a core requirement of location system and augmented reality. In this paper, we propose a method to estimate camera motion parameter based on invariant point features. Typically, feature information of image has drawback, it is variable to camera viewpoint, and therefore information quantity increases after time. The LM (Levenberg-Marquardt) method using nonlinear minimum square evaluation also has a weak point, which has different iteration number for approaching the minimal point according to the initial values and convergence time increases if the process run into a local minimum. In order to complement these shortfalls, we, first propose constructing invariant features of geometry using similarity function and Graham search method. Secondly, we propose a two-stage camera parameter calculation method to improve accuracy and convergence by using 2D homography and LM method. In the experiment, we compare and analyze the proposed method with existing method to demonstrate the superiority of the proposed algorithms.

1 Introduction

Ubiquitous computing involves every computer being connected, invisible to the user's eyes, always available regardless of time and place, incorporated into our everyday lives and offers an autonomous support for people. Especially, the ubiquitous location-based service (u-LBS), that provides location information of objects such as people and things leads the van of these services, localization technique is an important elementary technology to implement such services. Methods for acquiring location information include using sensors, using vision technology and combining the two approaches. Sensors such as the odometer and the inertial navigation system (INS) yield accurate data only when the inherent error of sensor itself is resolved. If we use the vision technology that recognizes the location with image information, we can get more accurate data than the sensor. However, extracting visual characteristic data for recognition is not an easy task. A typical example of vision-based localization is employing artificial marks to recognize the location. Such application has disadvantages of generating mismatches during camera operation because image feature information is varying according to the camera viewpoint, so must set numerous

* Corresponding author.

assumptions and restrictions [1]. The nonlinear minimization method being used to evaluate the camera's extrinsic factors calculates an optimized solution by minimizing the error. However, the number of iterations for approaching the minimal point varies according to the initial values and the time required for convergence increases if the process runs into a local minimum point [2]. In order to complement these shortfalls, we first propose constructing improved feature models using mathematical tools from projective geometry for identification. Invariant vector in this paper is a characteristic value of corner point unrelated to the camera viewpoint. Secondly, we propose a two-stage calculation method to improve accuracy and convergence by using the information acquired by homography as initial values of the LM method. A block diagram of proposed framework is shown in Fig.1.

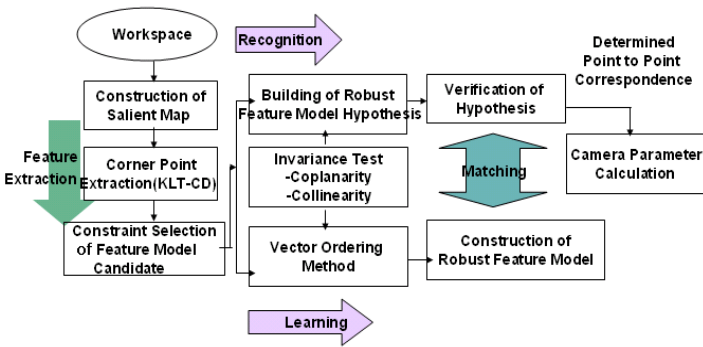


Fig. 1. Block Diagram of Proposed Configuration

2 Methodology

2.1 Cross Ratio, PPIV, Feature Extraction

In order to extract features unrelated to the viewpoint, this paper uses cross ratio of five points on a single plane defined in projective geometry. According to the theorem, when there are five points in a homogeneous coordinate system of a two-dimensional space, if the points exist on a single plane, and three of the five points are not on a same line, cross ratios of two independent projective invariant values exist as shown in Eq. (1) [3].

$$\lambda_1 = \frac{\det(m_{431})\det(m_{521})}{\det(m_{421})\det(m_{531})}, \lambda_2 = \frac{\det(m_{432})\det(m_{512})}{\det(m_{412})\det(m_{532})} \quad (1)$$

$\det(m_{431})$ is the matrix determinant calculated with coordinate data (x, y) of the corner points c_1, c_3, c_4 . Since cross ratio is permutation-sensitive like most projective invariants, we employ the permutation invariant J vector as descriptor since its value is bounded between 2.0 and 2.8, therefore, does not suffer from instabilities due to singularities, and it can provide direct point to point correspondences across matched quintuples. Eq. (3), which indicates each element of the five 2-dimensional invariant

J vectors are calculated with Eq.(2), and it is called *PPIV* (Projective and Permutation Invariant Vector) in geometry [4]. Each of the five points is in a 1:1 mapping relationship with each invariant vector $J^{(i)}$.

$$J[\lambda] = \frac{2\lambda^6 - 6\lambda^5 + 9\lambda^4 - 8\lambda^3 + 9\lambda^2 - 6\lambda + 2}{\lambda^6 - 3\lambda^5 + 3\lambda^4 - \lambda^3 + 3\lambda^2 - 3\lambda + 1} \tag{2}$$

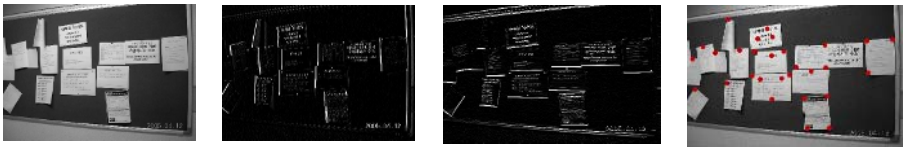
$$J^{(1)} = J[\lambda_1], J^{(2)} = J[\lambda_2], J^{(3)} = J\left[\begin{matrix} \lambda_1 \\ \lambda_2 \end{matrix}\right], J^{(4)} = J\left[\begin{matrix} \lambda_2 - 1 \\ \lambda_1 - 1 \end{matrix}\right], J^{(5)} = J\left[\begin{matrix} \lambda_1(\lambda_2 - 1) \\ \lambda_2(\lambda_1 - 1) \end{matrix}\right] \tag{3}$$

In order to reduce the amount of calculation and create robust feature models, salient map of the image can be used, and the corner points are extracted using the KLT-CD algorithm [5] within the salient region. The salient map is based on the theory that the distinctive area of the image has a higher value than other smooth areas [6]. The KLT-CD algorithm differentiates the image within the region in x and y direction as shown in Eq.(4), multiplies the transposed matrix and adds all the matrix determinants in the region.

$$g = \begin{bmatrix} g_x \\ g_y \end{bmatrix} = \nabla I, \quad gg^T = \begin{bmatrix} g_x \\ g_y \end{bmatrix} \begin{bmatrix} g_x & g_y \end{bmatrix} = \begin{bmatrix} g_x^2 & g_x g_y \\ g_x g_y & g_y^2 \end{bmatrix}, \quad Z = \iint_w \begin{bmatrix} g_x^2 & g_x g_y \\ g_x g_y & g_y^2 \end{bmatrix} w dx \tag{4}$$

$x = (x, y), w: \text{weighting function}$

Since matrix Z contains the pure texture information, analyzing the eigenvalue of Z allows categorization of characteristics. If two of the unique values are large, it signifies that there are corner points to be extracted. The permutation combination is a set of numbers of cases arranged in order by drawing five points from the corner points within the region without duplication. *PPIV* for each permutation combination is calculated using Eq.(1), (2) and (3). Fig.2 displays the image of the process of extracting corner points using the KLT-CD algorithm



(a)original image (b)differential image(x) (c)differential image(y) (d)result image

Fig. 2. Process of Corner Points Extraction

2.2 Learning and Recognition

If the *PPIV* were to be preserved under projective transformation, the first condition is that there must not be three points that exist on a single line because it causes the matrix determinant to be 0, creating a cross ratio of 0 or ∞ . Secondly, the points must be on an identical plane. The restriction of coplanarity stems from the requirement of invariance of the cross ratio. In order to eliminate permutation combinations with three points on a single line, a Grimm matrix [3] was used in experiment. For the

purpose of checking whether the points are on an identical plane, each vector was checked to see if the value was between 2.0 and 2.8. In this paper, we call quintuple points after collinearity and coplanarity test as feature model candidate. The vector ordering techniques [7] was applied to the feature model candidates to extract robust outliers. This approach based on the Euclidean distance from mean invariant vector as Eq. (5), Eq (6). $PPIV_i$ in Eq.(5) is the vector of the i th feature model candidate, where the superscript j in Eq.(6) denotes the j th vector component.

$$PPIV_{mean} = (1/q) \sum_{i=0}^{q-1} PPIV_i, q: \text{feature model candidate}, \tag{5}$$

$$d_i = \sqrt{\sum_{j=0}^4 (PPIV_i^j - PPIV_{mean}^j)^2} \cdot \tag{6}$$

2.3 Matching Using Similarity Function and Graham Search Method

If matching is performed for all feasible blocks by searching the entire salient map, it increases the time complexity as well as the mismatch rate. Therefore, we propose a method for conducting the matching stage for only the blocks with a high degree of similarity between two blocks based on a similarity assessment function. A similarity function R_N uses a correlation equation as shown in Eq.(7).

$$R_N = \frac{\mu_{mn} - \mu_n \mu_m}{\sigma_n \sigma_m} \tag{7}$$

Where μ_n, μ_m denote the mean in N, M, μ_{mn} is the mean intensity value of the pixel-wise product values of the pixels from two window positions, M, N. And $\sigma_n = \mu_{nn} - \mu_n \mu_n$ is the standard deviation in N.

While matching has been performed solely based on the $PPIV$ value in previous studies [8], it is irrational to use only the $PPIV$ value that has instabilities due to noise or small distortions in corner detections. In turn, this study applied the threshold value (0.08). Then a convex hull test was performed using the Graham searching algorithm to filter incorrect matching candidates, and get point- to-point correspondences. Number of points and neighboring relations, corresponding points lie on the convex hull are preserved during projective transformation [9]. Therefore, convex hull test can be additionally used to determine accurate 1:1 correspondence of a feature models. The Graham searching method uses back tracking that makes up for the disadvantages of the conventional method with numerous searching rounds. It assigns candidates to a solution set and finds an optimal solution through back tracking method. Whereas a general algorithm requires an exponential time, Graham searching algorithm only involves a polynomial time since is completely eliminates the solutions not meeting the conditions. Fig. 3 displays the process of seeking points on the convex hull using the Graham algorithm.

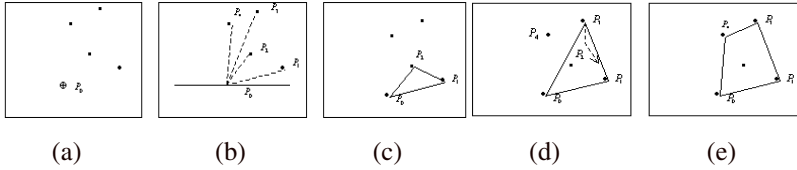


Fig. 3. Search Process of Graham Search algorithm

From the five points, select P_0 with the least y-axis value and the greatest x-axis value as the axis point in Fig.3(a). Align the remaining points around P_0 with the angle with the positive x direction as the key in Fig.3(b). Then as shown in Fig.3(c), consider the three points P_0, P_1, P_2 as the points on the convex hull and add as another point P_3 on the convex hull. In order to verify whether P_2 is a point on the convex hull, check if P_3, P_2, P_1 are in the counter clockwise direction in Fig.3(d). If not, eliminate P_2 on of the three points as a point on the convex hull. In Fig.3 (e), P_4 is again added as a point on the convex hull, the direction of P_4, P_3, P_2 is examined, and P_4 is considered as a point on the convex hull.

From the set of feature model candidates, the most outliers according to Eq.(6) were finally selected as robust feature models. Their graphical representation, along with the corresponding values of the invariant vectors $PPIV_i, 0 \leq i \leq 2$, is given in Fig. 4(left). These three candidates constitute robust feature models. During navigation same scene is viewed from a different vantage-point in Fig. 4(right)). Under a similar procedure coplanar quintuples are extracted and successful matches with reference image are examined. These quintuples constitute the recognized feature models.

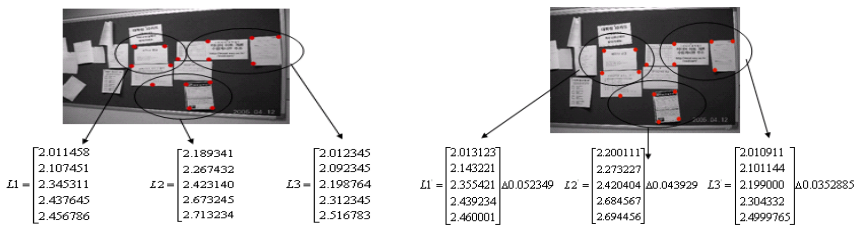


Fig. 4. Robust Feature Model Identified during learning(left) and Recognized Results(right)

Finally, a transformation matrix of two images is calculated using feature model with determined point-to-point correspondence. It is obtained from the solutions of the linear system constituting the eight equations [10].

2.4 Camera Motion Parameter Estimation

This section describes a method for estimation of the camera motion factors using the acquired feature model set.

2.4.1 Coordinate Transformation

Where there is a 2-dimensional image coordinate x, y that corresponds with the 3-dimensional coordinate system under the perspective projection, the image coordinates x', y' according to translation and rotation can be expressed with 8 variables as in Eq.(8). If camera rotation is not substantial and the focal length is large and consistent, the relationship between the 3-dimensional coordinates and the corresponding 2-dimensional image coordinates can be expressed with an affine model as in Eq.(9) [11].

$$x' = \frac{a_1x + a_2y + a_3}{a_7x + a_8y + 1}, y' = \frac{a_4x + a_5y + a_6}{a_7x + a_8y + 1} \tag{8}$$

$$x' = x + \gamma y - \beta f = a_1x + a_2y + a_3, y' = -\gamma x + y + \alpha f = a_4x + a_5y + a_6 \tag{9}$$

Furthermore, the camera rotation data including the focal length (f), tilt angle (α), pan angle (β) and swing angle (γ) can be extracted from the affine factors in Eq.(9).

2.4.2 Initial Value Estimation by Homography

Extraction of the camera motion factors using image can be regarded as a problem of finding a 2-dimensional homography. This is due to the fact that when points on a single plane in a 3-dimensional space are expressed in 2 dimensions under perspective projection, movements of these points are expressed with a 3x3 homography matrix [12]. If the homogeneous coordinates of the reference image is $X = (X, Y, W)^T$, and that of the input image $x = (x, y, w)^T$, and the correspondence relation between the two coordinates is $X \leftrightarrow x$, if the relationship in Eq.(10) is satisfied, there exists a homography matrix M between two images.

$$X = Mx \quad (M = [r_1 \ r_2 \ t]) \tag{10}$$

In the experiment, a homography matrix was calculated using the direct linear transformation algorithm from the correspondence relationship of the four points of the extracted feature models. Assuming that the internal parameters are known, we can obtain the first two column vectors, and the remaining column vectors can be acquired using orthogonality of the camera's rotation matrix R with a cross product ($r_1 \times r_2$) of Eq.(11).

$$R = \begin{bmatrix} r_{11} & r_{12} & r_{13} \\ r_{21} & r_{22} & r_{23} \\ r_{31} & r_{32} & r_{33} \end{bmatrix}, \quad P = [r_1 \ r_2 \ r_1 \times r_2 \ t] \tag{11}$$

Once the rotation matrix R is calculated, the rotation information of each axis is inferred as in Eq.(12).

$$\alpha = \text{atan}\left(\frac{r_{12}}{r_{11}}\right), \beta = \text{asin}(-r_{13}), \gamma = \text{atan}\left(\frac{r_{23}}{r_{33}}\right) \tag{12}$$

However, since the obtained α, β, γ are induced from a periodic function (\sin, \tan), there is the ambiguity of yielding different angles at similar values. Therefore, we use

these data as initial values of the LM algorithm during the experiment to obtain the final solution with improved accuracy and convergence.

2.4.3 Nonlinear Minimizing Method by Levenberg-Marquardt

The LM algorithm is one of the minimization methods using nonlinear minimum square evaluation [2]. If the object function correctly approximated to a localized 2-dimensional function, the Gauss Newton method should be applied. Otherwise, a gradient reduction method is applied. The LM algorithm defines the average square error to evaluate the similarity between the output and the actual output. In turn, if the object function based on the affine model in Eq.(13) is denoted as $\chi^2(a)$, it can be set as Eq.(14).

$$y(x, y, \mathbf{a}) = \begin{bmatrix} u(x, y) \\ v(x, y) \end{bmatrix} = \begin{bmatrix} a_1x + a_2y + a_3 \\ a_4x + a_5y + a_6 \end{bmatrix} \tag{13}$$

$$\chi^2(\mathbf{a}) = \sum_{i=1}^N w_i \left[\frac{y'_i - y(x_i, y_i, \mathbf{a})}{\sigma_i} \right]^2 \tag{14}$$

In Eq.(14), y'_i denotes the i th input feature model, σ_i the i th data variance, and w_i the weight value of 0 or 1. If the object function of Eq.(14) is approximated to the form of a second-order equation for the factor \mathbf{a} using Taylor series, it can be expressed as Eq.(15).

$$\chi^2(\mathbf{a}) \approx r - \mathbf{d} \cdot \mathbf{a} + \frac{1}{2} \mathbf{a} \cdot \mathbf{D} \cdot \mathbf{a} \tag{15}$$

In the above equation, \mathbf{d} denotes the first-order differential matrix of the factor \mathbf{a} for the object function, and \mathbf{D} denotes the Hessian matrix, which is the second-order differential matrix of the factor \mathbf{a} . Furthermore, the factor \mathbf{a} can be calculated with the reverse-Hessian method as in Eq.(16). Conversely, if the above equation cannot be approximated to a second-order equation, it should be resolved with a gradient reduction method as in Eq.(17).

$$\mathbf{a}_{min} = \mathbf{a}_{cur} + \mathbf{D}^{-1} \cdot [-\nabla \chi^2(\mathbf{a}_{cur})] \tag{16}$$

$$\mathbf{a}_{next} = \mathbf{a}_{cur} - const\ ant \times \nabla \chi^2(\mathbf{a}_{cur}) \tag{17}$$

3 Experimental Results

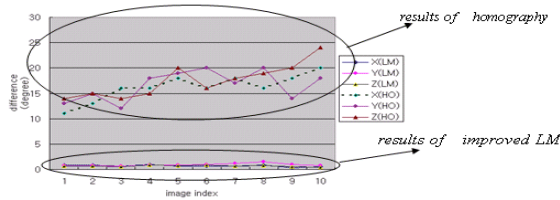
The proposed algorithm has been implemented and experimentally verified in an indoor environment. The image was captures with Nikon Coolpix 3200 and standardized into 640×480 pixels. For the feature models recognition experiment, three robust feature models were extracted from the reference image through learning, and the recognition rate was calculated using 50 input images with different camera views. Table 1 displays the recognition results. CR is the percentage of correct recognitions of robust feature models, and MR (Miss-Recognitions), FP (False-Positives) and FN (False-Negatives) are percentage of incorrect recognitions, recognitions of other feature models as robust models and elimination of robust feature models, respectively.

Table 1. Recognition Results of Feature Model

Feature Model	CR	MR	FP	RN
L1	48(96%)	1(2%)	0(0%)	1(2%)
L2	45(90%)	1(2%)	3(6%)	2(4%)
L3	49(98%)	0(0%)	1(2%)	0(0%)
Total	47.3(94.6%)	0.7(1.4%)	1.3(2.7%)	1(2%)

From the way that comparison of recognition rates using the conventional method and the proposed method of using the similarity function and the Graham search algorithm, the recognition rate of the proposed method was 94.6%, a 1.3% improvement from the conventional method of 93.3%. Furthermore, when the robust feature models were not included, the rate decreased from 2.7% to 2%, indicating that performance had been improved for the proposed method.

Figure 5 compares the accuracies when motion parameter is obtained with the homography matrix and using the improved LM algorithm for 10 different images with known rotation information. The x axis contains index of 10 images used in the experiment and the y axis displays difference between known rotation data and the data acquired from homography and the data obtained by using the improved LM algorithm with homography's results as initial values of LM. Since the rotation information obtained from homography is induced from a periodic function, there is a significant error between the actual rotation data. However, when the LM algorithm is deployed, the result improved substantially.

**Fig. 5.** Accuracy Comparison

4 Discussion

In this paper, we proposed a method for extracting features unrelated to the camera viewpoint to calculate the camera's motion factors. Projective and point permutation invariant vectors have been employed to characterize feature patterns. The method proposed for the motion factor calculation involves making up for the disadvantages inherent in the conventional LM algorithm to improve convergence and accuracy, allowing extraction of optimal camera motion factors. Features used in this paper exist on a coplane, and there are restrictions under indoor environments where there is a geometric model. In turn, there must be continuous studies on extracting features

that is robust to the outdoor noise and without restrictions. Additionally, uncertainty issues due to total or partial occlusions of stored features at recognition need further research.

Acknowledgement

This work was supported in part by IITA through IT leading R&D support project.

References

1. Christian Drewniok and Karl Rohr, "High-Precision Localization of Circular Landmarks in Aerial Images," Proc. 17. Dagm-Symposium, Musterkennung 1995, pp.594-601, Bielefeld, Germany, 13-15. September 1995.
2. Martin T.Hagan and Mohammad B.Menhaj, "Training Feedback Networks with the Marquardt Algorithm", IEEE Transactions on Neural Networks, Vol. 5, No. 6, November 1994.
3. K. Kanatani, "Computational Projective Geometry," CVGIP:Image Understanding Workshop, Washington, DC, pp. 745-753, 1993.
4. Reiner Lenz and Peter Meer, "Point Configuration Invariants under Simultaneous Projective and Permutation Transformations," Pattern Recognition, Vol. 27, No. 11, pp. 1523-1532, 1994.
5. S. Birchfield, "KLT:An Implementation of the Kanade-Lucas-Tomasi Feature Tracker, <http://vision.stanford.edu/~birch/klt/>".
6. Panos E. Trahanias, Savvas Velissaris and Thodoris Garavelos, "Visual Landmark Extraction and Recognition for Autonomous Robot Navigation," Proc. IROS 97, pp. 1036-1042, 1997.
7. V. Barnett, "The Ordering of Multivariate Data," Journal of Royal Statistical Society A, Part 3 139 pp. 318-343, 1976.
8. Vicente, M.A., Gil, P., Reinoso., Torres, F, "Object Recognition by Means of Projective Invariants Considering Corner-Points," Proc. SPIE. Vol. 4570. pp. 105-112. 2002.
9. J.L. Mundy, A. Zisserman, "Geometric Invariance in Computer Vision," MIT Press, Cambridge, MA, 1992.
10. Fishler, M.A. and Bolles, R.C., "Random Sample Consensus: A Paradigm for Model Fitting with Application to Image Analysis and Automated Cartography," Communion ACM, vol. 24, no. 6, pp. 381-395, 1981.
11. Jang SeokWoo, "Shot Transition Detection by Compensating Camera Operations," Soongsil University Press, 2000.
12. Hartley, R. I, Zisserman, A, "Multiple View Geometry in Computer Vision," Cambridge University Press, 2000.

Automatic Generation Technique of Three-Dimensional Model Corresponding to Individual Vessels

Na-Young Lee¹, Gye-Young Kim^{1,*}, and Hyung-Il Choi²

¹ School of Computing, Soongsil University,
Seoul, Korea
white@vision.ssu.ac.kr,
gykim11@ssu.ac.kr

² School of Media, Soongsil University,
Seoul, Korea
hic@computing.ssu.ac.kr

Abstract. We propose a new approach for automatically generating individual vessels to 3D(three-dimensional) model. The modeling process is carried out in two steps. The first step consists of selecting automatically two sets of corresponding feature points between standard and individual vessels. In the second step, 3D model of individual vessels is performed by warping with corresponding feature points. The 3D model of vessels provides patients with better and cleaner visualization without extensive training to understand vessels geometry. It saves reviewing time for physicians since 3D model may be performed by a trained technician, and may also help visualize dynamics of the vessels.

Index term: Angiogram, vessel, feature point, image warping.

1 Introduction

In the late 1970s, quantitative coronary arteriography(QCA) was developed to quantify vessel motion and the effects of drugs on the regression and progression of coronary artery disease[1]. So far, QCA has been the only technique that allows the accurate and reliable assessment of the morphologic changes within the entire coronary vasculature over a certain period of time (regression/progression studies), despite its known limitations [2]. Local QCA evaluations are providing a good accuracy for 2D analyses of stenoses. However, global evaluations of vessel segments or vessel subsystems are not very common. The inaccuracy of visual interpretation of angiograms has been well documented, and has motivated the development of automated methods for quantifying arterial morphology. Accurate descriptions of arterial trees would be useful for quantitative diagnosis of atherosclerosis, for surgical or treatment planning, for monitoring disease progress or remission, and for comparing efficacies of treatments [3].

* Corresponding author.

This paper describes a new method for automatically generating individual vessels to 3D model. 3D model provides many important anatomical measurements that neither are available, nor can be accurately measured in 2D. For example, the projected length of a vessel is shorter in the projected views. Torque and the curvature of vessels are virtually impossible to estimate from 2D views. The 3D model of vessels provides patients with better and cleaner visualization without extensive training to understand vessels geometry. It saves reviewing time for physicians since 3D model may be performed by a trained technician, and may also help visualize dynamics of the vessels.

The structure of the paper is as follows. In Section 2, we describe the two major stages of our algorithm. Experimental results obtained for clinical datasets are discussed in Section 3. Finally, we discuss conclusion in Section 4.

2 Methodology

We propose a new approach for automatically generating individual vessels to 3D(three-dimensional) model. The modeling process is carried out in two steps. The first step consists of selecting automatically two sets of corresponding feature points between standard vessels and individual vessels. In the second step, 3D model of individual vessels is performed by warping with corresponding feature points.

Overall system configuration is as shown in Fig. 1.

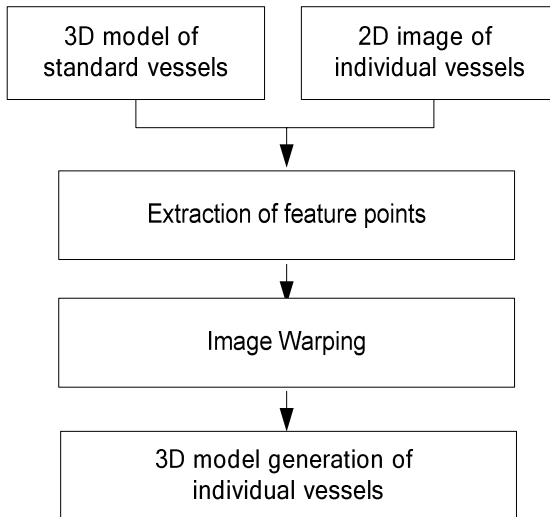


Fig. 1. Overall system configuration

2.1 3D Model Acquisition of Standard Vessels

Coronary arteriography is accomplished by hand-injecting small quantities of radiopaque contrast material (3-5ml) directly into the orifice of each coronary artery

with preformed catheters placed under fluoroscopic guidance [4]. The catheters are inserted into the arterial system either through the brachial artery, the femoral artery, or into the radial artery. Because of the complex structure of the coronary tree, the left coronary system is usually depicted from four to six different angiographic views [direct frontal, left anterior oblique(LAO), right anterior oblique(RAO), and several cranial and caudal projections], and the right coronary system usually from two views(LAO and RAO views) because of its simpler structure. To quantify the 3D model of vessels, the angles of vessel bifurcation are measured with references to LCX, Lt.main, and LAD, as shown in the Table 1. Evaluating the angles of vessel bifurcation from six different angiographic views can reduce the possible measurement error when the angle from a single view is measured.

Table 1. Measured angles of vessel bifurcation from six different angiographic views

	RAO30 CAUD30	RAO30 CRA30	AP0 CRA30	LAO60 CRA30	LAO60 CAUD30	AP0 CAUD30
1	69.17	123.31	38.64	61.32	84.01	50.98
2	53.58	72.02	23.80	51.75	99.73	73.92
3	77.28	97.70	21.20	57.72	100.71	71.33
4	94.12	24.67	22.38	81.99	75.6	69.57
5	64.12	33.25	31.24	40.97	135.00	61.87
6	55.34	51.27	41.8	80.89	119.84	57.14
7	71.93	79.32	50.92	87.72	114.71	58.22
8	67.70	59.14	31.84	58.93	92.36	70.16
9	85.98	60.85	35.77	54.45	118.80	78.93
10	47.39	60.26	34.50	47.39	67.52	34.79
Average	68.67	66.18	33.21	62.31	100.83	62.69
Standard deviation	14.56	29.07	9.32	15.86	21.46	13.06

The Table 1 shows the results of measuring the angles of vessel bifurcation from six different angiographic views for randomly selected ten individuals regardless of gender and age, and the average and standard deviation of each individual's measurements.

The Fig.2 shows the results of generating a 3D model of standard vessels from six different angiographic views.

	RAO30 CAUD30	RAO30 CRA30	AP0 CRA30	LAO60 CRA30	LAO60 CAUD30	AP0 CAUD30
Angiograms						
Model						

Fig. 2. 3D model of standard vessels from six different angiographic views

2.2 Extraction of Feature Points

We used the KLT(Kanade-Lucas-Tomasi) algorithm to extract the feature points from the standard and individual vessels. The standard vessels are projected onto a 2D plane. The basic principle of the KLT is that a good feature is one that can be tracked well, so tracking should not be separated from feature extraction [10]. A good feature is a textured patch with high intensity variation in both x and y directions, such as a corner. Denote the intensity function by $g(x, y)$ and consider the local intensity variation matrix

$$g = \begin{bmatrix} g_x \\ g_y \end{bmatrix} = \nabla I \tag{1}$$

$$gg^T = \begin{bmatrix} g_x \\ g_y \end{bmatrix} \begin{bmatrix} g_x & g_y \end{bmatrix} = \begin{bmatrix} g_x^2 & g_x g_y \\ g_x g_y & g_y^2 \end{bmatrix}$$

$$Z = \iint_W \begin{bmatrix} g_x^2 & g_x g_y \\ g_x g_y & g_y^2 \end{bmatrix} w dx$$

The symmetric 2×2 matrix Z of the system must be both above the image noise level and well-conditioned. The noise requirement implies that both eigenvalues of Z must be large, while the conditioning requirement means that they cannot differ by several orders of magnitude. Two small eigenvalues mean a roughly constant intensity profile within a window. A large and a small eigenvalue correspond to a unidirectional pattern. Two large eigenvalues can represent corners, salt-and-pepper textures, or any other pattern that can be tracked reliably.

In practice, when the smaller eigenvalue is sufficiently large to meet the noise criterion, the matrix Z is usually also well conditioned. This is due to the fact that the

intensity variations in a window are bounded by the maximum allowable pixel value, so that the greater eigenvalue cannot be arbitrarily large.

As a consequence, if the two eigenvalues of Z are λ_1 and λ_2 , we accept a window if

$$\min(\lambda_1, \lambda_2) > T \quad (2)$$

where T is a predefined threshold.

We extracted automatically two sets of corresponding feature points between standard and individual vessels.

2.3 Image Warping

We have warped the standard vessels with respect to the individual vessels. Given the two sets of corresponding feature points, $P = \{p_1, p_2, \dots, p_8\}$ and $Q = \{q_1, q_2, \dots, q_8\}$, 3D model of vessels is performed by warping of the standard vessels. Here, P is a set of feature points in standard vessels and Q is a set of one in individual vessels.

In this work, standard vessels warping is performed by applying the elastic TPS(Thin-Plate-Spline) interpolation function[6] on the two sets of feature points.

The TPS are interpolating functions, representing the distortion at each feature point exactly, and defining a minimum curvature surface between feature points. A TPS function is a flexible transformation that allows rotation, translation, scaling, and skewing. It also allows lines to bend according to the TPS model. Therefore, a large number of deformations can be characterized by the TPS model.

The TPS interpolation function can be written as

$$h(x) = A + \sum_{i=1}^8 W_i K(\|x - x_i\|) \quad (3)$$

Where A are the affine transformation parameters matrices, W_i are the weights of the non-linear radial interpolation function K , and x_i are the feature points. The function $K(r)$ is the solution of the biharmonic equation ($\Delta^2 K = 0$) that satisfies the condition of bending energy minimization.

3 Experimental Results

We simulated the system environment that is Microsoft Windows XP on a Pentium IV 3GHz, Intel Corp. and the compiler used was VC++ 6.0. The image used for experimentation was 512×512 . Each image has a gray-value resolution of 8 bits, i.e., 256 gray levels.

The Fig. 3 shows the results of generating a 3D model of standard vessels from six different angiographic views.

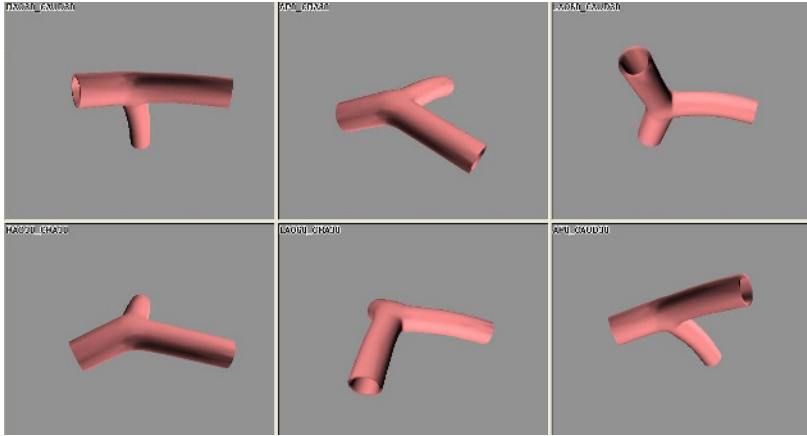


Fig. 3. 3D model of standard vessels in six views

The angiogram shows the different shape of images according to individual vessel. The 3D model of standard vessels is projected onto a 2D plane because angiogram is in 2D. The Fig. 4 shows the result of extracting the feature points by applying the KLT algorithm to the projected standard vessels.

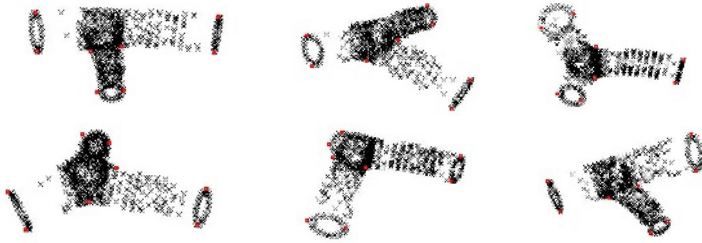


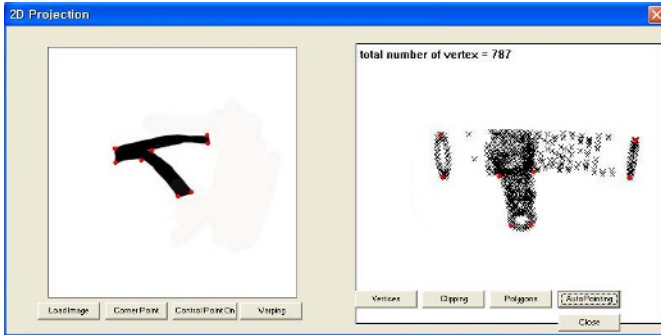
Fig. 4. Feature points automatically extracted from projected standard vessels



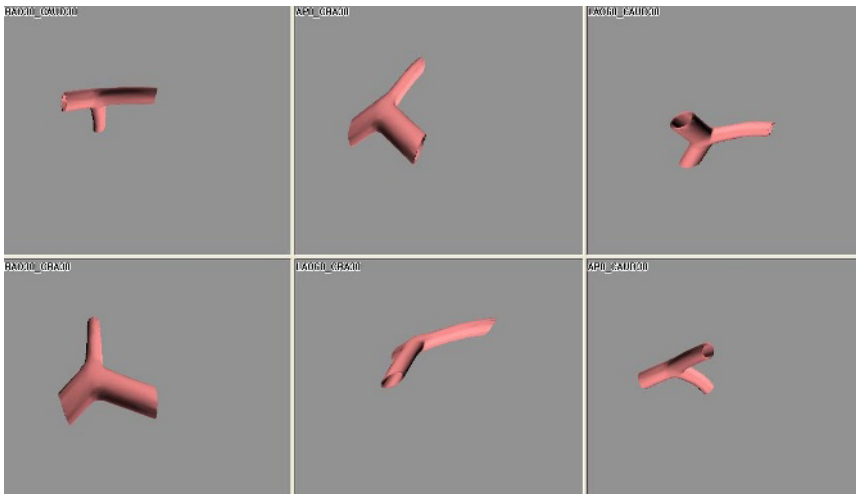
Fig. 5. Feature points automatically extracted from individual vessels

The Fig. 5 shows the result of extracting the feature points by applying the KLT algorithm to the vessels extracted from the angiogram.

The Fig. 6 shows the results of modifying the standard vessels to suit the model of individual vessels using the TPS interpolation function. The Fig.6(a) indicates the result of extracted eight feature points from the standard and individual vessels. And the Fig.6(b) shows the result of generating a 3D model of individualized vessels by inverse projection onto the modified 2D standard model.



(a) Extraction of corresponding feature points from two vessels



(b) 3D model of individual vessels in six views

Fig. 6. Automatic generation result of individual vessels to 3D model

The Fig. 7 shows the results of overlaying the 3D model of standard vessels quantified from the Table.1 data onto the angiograms.

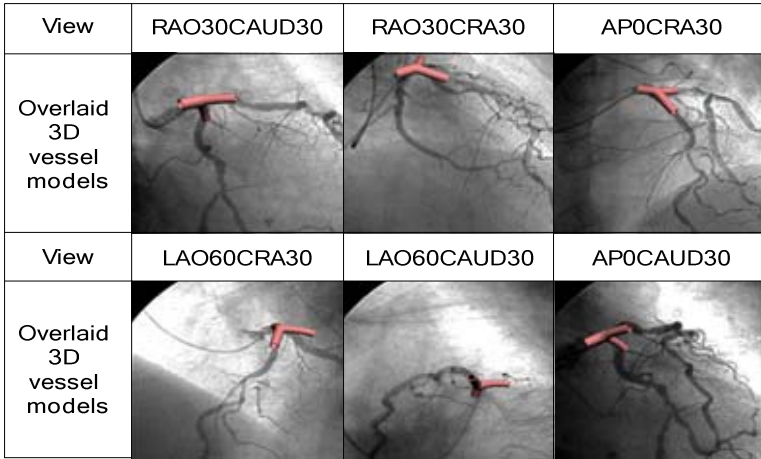


Fig. 7. Overlaid 3D model of standard vessels on six different angiographic views

4 Conclusion

We proposed a simple and effective algorithm to automatically generating of individual vessels model. The 3D model of vessels enables patients to visualize their progress and improvement. Such a model should not only enhance the level of reliability but also provides speedy and accurate identification. In order words, this method can expect to reduce the number of misdiagnosed cases.

Acknowledgement

This work was supported by the Korea Research Foundation (KRF-2004-005-D00198).

References

1. B. G. Brown, E. Bolson, M. Frimer, and H. Dodge, "Quantitative coronary arteriography estimation of dimensions, hemodynamic resistance, and atheroma mass of coronary artery lesions using the arteriogram and digital computation", *Circulation*, vol. 55,(1977) 329-337
2. P. de Feyter, J. Vos, J. Reiber, and P. Serruys, "Value and limitations of quantitative coronary angiography to assess progression and regression of coronary atherosclerosis", in *Advances in Quantitative Coronary Arteriography*(1993) 255-271
3. J. Ross et al., "Guidelines for coronary angiography", *Circulation*, vol.76,(1987) 963A-977A
4. D. Levin, "Clinical overview of cardiac catheterization procedures: Adult diagnostic procedures", in *1998 Categorical Course in Diagnostic Radiology Physics: Cardiac catheterization imaging*,(Oak Brook, IL) (1998) 37-45

5. F.L. Bookstein, Principal warps: thin-plate splines and the decomposition of deformations, *IEEE-PAMI* 11(1989) 567-585.
6. Y. Bentoutou, et. al, "An invariant approach for image registration in digital subtraction angiography", *Pattern Recognition*(2002) 34-48.
7. J. Flusser, T.Suk, Degraded image analysis: an invariant approach, *IEEE Trans. Pattern Anal. Mach. Intell*(1998) 590-603.
8. A. Venot, J.F. Lebruchec, J.C. Roucayrol, "A new class of similarity measures for robust image registration", *Comput. Vision Graph. Image Process*(1998) 176-184.
9. Jianbo Shi, Carlo Tomasi, "Good features to track", *IEEE Conference on CVPR Seattle*(1994) 593-600.
10. Carlo Tomasi and Takeo Kanade, "Detection and Tracking of Point Features", *Carnegie Mellon University Technical Report CMU-CS-91-132*(1991)

Modulating Energy Distribution of Reflected Light Based on Images

Zhanwei Li¹, Guolin Duan¹, Jizhou Sun², Lijuan Sun¹, and Xinran Lv¹

¹ Hebei University of Technology,
Tianjin, China, 300130

stuartzh@public.tpt.tj.cn,
glduan@hebut.edu.cn

² Tianjin University,
Tianjin, China, 300072
jzsun@tju.edu.cn

Abstract. Based on IBMR techniques, this paper study energy distribution of reflection light from object surface and a method is presented to separate elements of specular and diffuse reflection in an image. The ray projected from object surface to images includes diffuse and specular energy distribution. The ray projected from object surface to images includes energy distribution from ambient light, diffuse and specular light. The ray intensity of diffuse reflection or ambient light is irrelevant to viewpoint, but that of specular reflection is relevant to viewpoint and will change with the moving of viewpoint. This paper suppose that the minimal energy of reflection lighting in n corresponding points is energy brought by diffuse reflection and ambient light, so diffuse and specular reflection element are separated.

The separated energy distribution of diffuse light depicts the reflection ability and weight of colors, and that of specular propagation depict the brightness of object surface. Appointed new specular and diffuse ratio to the separated images, scene images with different reflectance properties of the objects surfaces can be obtained, and virtual images with different ratio of energy distribution from specular and diffuse reflection can be reconstructed, furthermore it can be achieve to change the object colors and brightness only based on images.

When rendering images, characteristic of object surface are often adjusted to acquire satisfying visual impression. IBMR techniques have recently received much attention as a powerful alternative to traditional geometry-based techniques for image synthesis. Based on IBMR, this paper present a method to separate energy distribution of diffuse and specular reflection in an image. If re-distributing ratio to the separated images, then the surface characteristic of object in image can be changed, and different impression of images can be obtained.

In the method, inputs are only a few calibrated images, algorithm is simple. Object surface reflection character, geometric model of the scene and the position of lighting are not needed.

Keywords: Image-Based Modeling and Rendering (IBMR), Energy Distribution, Specular Reflection, Diffuse Reflection.

1 Introduction

In image reconstructing, the reflectance properties of object surfaces are often modulated in order to obtain content visual effects. For this reason a number of methods have been introduced to simulate various effects, which increase the realism of generated images. Among these effects are specular reflection and refraction, diffuse inter-reflection, spectral effects, and various others.

The traditional methods for calculating realistic images are Global illumination. Ray tracing follows all rays from the eye of the viewer back to the light sources. Radiosity simulates the diffuse propagation of light starting at the light sources. They are mostly due to the interaction of light with the surfaces of various objects, and are in general very costly to simulate.

The importance of generating realistic images from images has significantly increased during the last few years. But it is difficult to simulate various reflectional effects for images based rendering techniques, because reflection characters of object surface are unknown only from images, so seldom methods are put forward. Image-Based Lighting (IBL) techniques^{[1][2][3]} recover the reflectance properties of all surfaces in a real scene. But geometric model of the scene and the position of lighting are needed in IBL, and its arithmetic is very complicated.

In this paper an image-based rendering method is presented to separate specular and diffuse reflection elements in an image. Appointed new specular and diffuse reflectance ratio to the separated images, scene images with different reflectance properties can be obtained and novel images with different ratio of energy distribution from specular and diffuse reflection can be reconstructed based on IBMR techniques.

The separated energy distribution of diffuse light depicts the reflection ability and weight of colors, and that of specular propagation depict the brightness of object surface. If we re-distribute ratio to the two parts, then it can be achieve to change the object colors and brightness based on images.

2 The Algorithm of Separating Energy Distribution of Specular and Diffuse Reflection^[4]

The goal of global illumination is to compute all possible light interactions in a given scene, and thus obtain a truly photorealistic image. All combinations of diffuse and specular reflections and transmissions must be accounted for.

The ray intensity of diffuse reflection or ambient light (thereinafter for simple we only mention diffuse reflection, refer to the both) is irrelevant to viewpoint (part of constant energy), but that of specular reflection is relevant and will change with the moving of viewpoint (part of non-constant energy). So let

$$C_i(m_i, n_i) = D_i(m_i, n_i) + S_i(m_i, n_i) \quad (1)$$

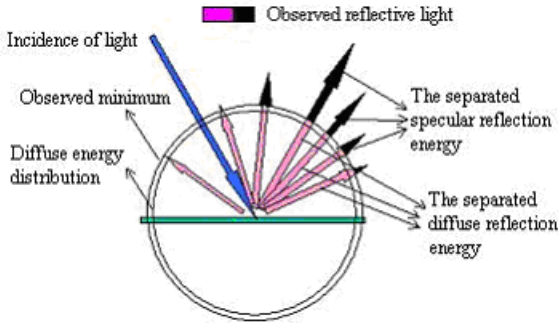


Fig. 1. Sketch map – separating energy distribution of specular and diffuse reflection

Where $i = 1, 2, 3 \dots k$, indicates the image from i^{th} viewpoint, (m_i, n_i) is images coordinate of i^{th} image, $C_i(m_i, n_i)$ is the color of pixel (m_i, n_i) on i^{th} image, $D_i(m_i, n_i)$ is the part of constant energy of the pixel (m_i, n_i) , $S_i(m_i, n_i)$ is the part of non-constant.

The intensity of diffuse reflection remains constant at any viewpoint, so the diffuse reflection energy from k correspondent points (on k images), projected by a space point P on object surface, are constant value, supposed $D(m_p, n_p)$, so let:

$$D_1(m_{1,p}, n_{1,p}) = D_2(m_{2,p}, n_{2,p}) = \dots = D_k(m_{k,p}, n_{k,p}) = D(m_p, n_p) \quad (2)$$

While intensity of specular reflection is variational to different viewpoints, so the energy from k correspondent points are different value, that is:

$$S_1(m_{1,p}, n_{1,p}) \neq S_2(m_{2,p}, n_{2,p}) \neq \dots \neq S_k(m_{k,p}, n_{k,p}) \quad (3)$$

A space point P on object surface project to k images, generate k image points, list k equations:

$$\begin{aligned} C_1(m_{1,p}, n_{1,p}) &= D(m_p, n_p) + S_1(m_{1,p}, n_{1,p}) \\ C_2(m_{2,p}, n_{2,p}) &= D(m_p, n_p) + S_2(m_{2,p}, n_{2,p}) \\ &\dots \dots \dots \\ C_k(m_{k,p}, n_{k,p}) &= D(m_p, n_p) + S_k(m_{k,p}, n_{k,p}) \end{aligned} \quad (4)$$

Camera calibration of intrinsic and extrinsic parameters and finding corresponding points are the base work. The method in [5] is adopted to camera calibration. Scene model can be recovered from scene images and the camera calibration parameters^{[6][7]}. Then the corresponding points on n images can be obtained^{[8][9][10]}.

The k images can be shot by a camera from k viewpoints, so $C_i(m_{i,p}, n_{i,p})$, ($i = 1, 2, 3 \dots k$) are known variable. $D(m_p, n_p)$, $S_i(m_{i,p}, n_{i,p})$, ($i = 1, 2, 3 \dots k$) are unknown variables. In Formula 4, totally there are k equations and $k+1$ unknown variables.

We suppose that the minimal reflection energy in k corresponding points is energy brought by diffuse reflection and ambient light, namely the constant energy part, shows in Figure 1. so the minimal value is $D(m_p, n_p)$ in Formula 4,

$$D(m_p, n_p) = \min(C_1(m_{1,p}, n_{1,p}), C_2(m_{2,p}, n_{2,p}), \dots, C_k(m_{k,p}, n_{k,p})) \quad (5)$$

Thus we obtain $D(m_p, n_p)$, and the unknown variables number in Formula 4 is reduced from $k+1$ to k , then $S_i(m_{i,p}, n_{i,p})$, ($i = 1, 2, 3, \dots, k$) in Formula 4 can be obtained, thus diffuse and specular reflection element are separated. Having computed all the pixels in images, energy distribution of diffuse and specular reflection in k images are separated. It is shown in Figure 2.

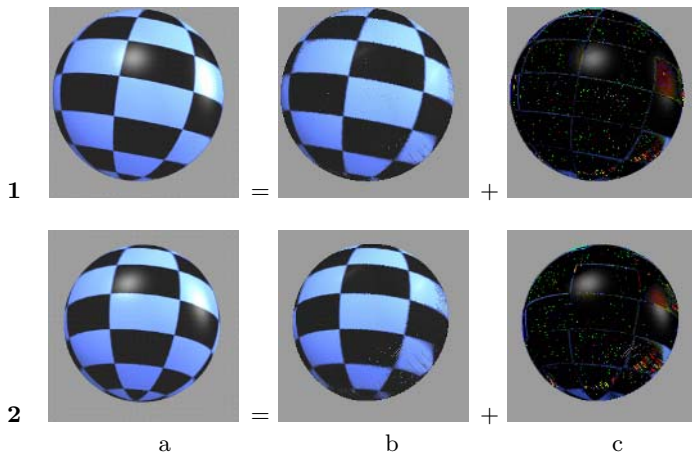


Fig. 2. Figure a are images of input. Figure b and c are images of energy distribution from diffuse and specular reflection, respectively separated from Fig. a.

Figure 2(a) is two of five images shot from five viewpoints. There are two source lights in the scene, so there are two highlight regions on the spherical surface, which lie at middle and right from the Figure 2(a). Figure 2(b) and Figure 2(c) are the separated images from Figure 2(a) using the method we presented above, respectively with energy distribution of diffuse and specular lighting. From Figure 2(c) two highlight regions on the spherical surface are very clear, it show that the energy distribution of diffuse and specular lights are separated on the whole.

In addition, we suppose that the minimal energy value in k corresponding points is the constant value (Figure 1), in fact certain energy from specular reflection must be contained in the minimal value, but it is least in condition of only k images. Although it is impossible to separate the two reflection elements entirely, our method can do its best to separate them with only a few known images. Of course error will be decreased if there are more input images.

3 Analysis of Energy Distribution on the Separated Images

Due to specular reflection, object surface can have a vivid impression. In image reconstructing, the reflectance properties of object surfaces are often modulated in order to obtain content visual effects, but it can not be acquired only from images.

The visual effect of compute-generated images can be adjusted by changing reflectance ratio of specular and diffuse lights. Object surface looks glorious under bigger ratio of specular reflectance, and gloom under less, even coarse if no. Diffuse reflectance refers to material characteristic, such as color and reflectance ability.

The ray from object surface to observer includes ambient light, diffuse light and specular light, which is depicted in Phone illumination model^[11].

$$I = \left[I_a K_a + \sum_i I_i (K_d \cos \theta_i) \right] + \sum_i I_i (K_s \cos^n \alpha_i) \tag{6}$$

Where K_a , K_d , K_s is reflection coefficient of ambient light, diffuse light and specular light. Light source, scene model and viewpoints are determinate on images, so in Formula 6, I_a , I_i , θ_i , α_i , n and K_a are determinate.

Now we respectively multiply coefficient to the separated images, to change the ratio of specular and diffuse energy distribution. Multiply coefficient χ to diffuse energy and γ to specular energy,

$$I_1 = \left[I_a K_a + \chi \sum_i I_i (K_d \cos \theta_i) \right] + \gamma \sum_i I_i (K_s \cos^n \alpha_i) \tag{7}$$

$$= \chi \left[\frac{1}{\chi} I_a K_a + \sum_i I_i (K_d \cos \theta_i) \right] + \gamma \sum_i I_i (K_s \cos^n \alpha_i) \tag{8}$$

Above we merge ambient light to diffuse light, so if we multiply coefficient to it, in fact I_2 is got,

$$I_2 = \chi \left[I_a K_a + \sum_i I_i (K_d \cos \theta_i) \right] + \gamma \sum_i I_i (K_s \cos^n \alpha_i) \tag{9}$$

Above the distinction ΔI between I_1 and I_2 is,

$$\Delta I = I_1 - I_2 = (1 - \chi) I_a K_a \tag{10}$$

Because ambient light $I_a K_a$ generally is weak comparing with diffuse and specular light, its influence to image color is week, so ΔI can be ignored.

Appointed new specular and diffuse reflectance ratio to the separated images, scene images with different reflectance properties can be obtained and novel images with different ratio of energy distribution from specular and diffuse reflection can be reconstructed based on IBMR techniques.

4 Experiment Results

Now we re-distribute ratio to the separated images from Figure 2a(1). In Figure 3, a is the original image[Figure 2a(1)], the other images are result taken different ratio, comparing them with a, the color and brightness of specular highlight on the object are changed respectively.

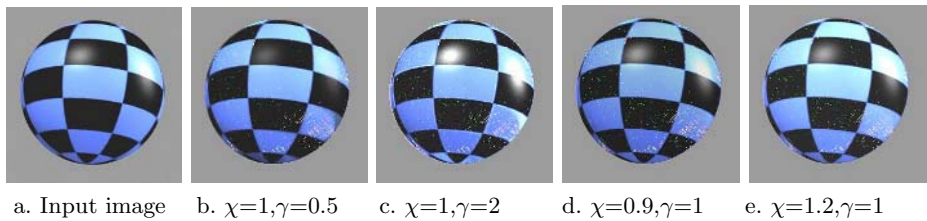


Fig. 3. Images –modulating energy distribution of specular and diffuse light

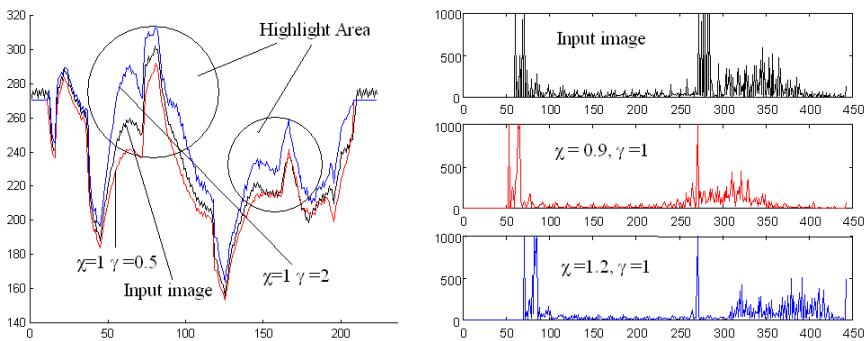


Fig. 4. Image color curve(left) and Image pixels statistics curve(right)

From color curve and pixels statistics curve, let’s analyze the change of the images which are re-distributed energy. The three curves in Figure 4 are respectively color curve of Figure 3(c), input image(Figure 2a(2)) and Figure 3(b). The image color on highlight due to specular reflection changed obviously after modulating the ratio of specular energy distribution. And three curves in Figure 5 are respectively pixels statistics curve of input image, Figure 3(d) and Figure 3(e). The energy of images transferred on the whole after modulating the ratio of diffuse energy distribution.

Above method of modulating the energy distribution is based absolutely on images. Without knowing characteristic of object surface, energy distribution of specular and diffuse reflection are modulated by re-distributing ratio to the separated images.

5 Application and Conclusions

When rendering images, characteristic of object surface are often to acquire satisfying visual impression.

IBMR techniques have recently received much attention as a powerful alternative to traditional geometry-based techniques for image synthesis. Based on IBMR, this paper present a method to separate energy distribution of diffuse and specular reflection in an image. If re-distributing ratio to the separated images, then the surface characteristic of object in image can be changed, and different impression of images can be obtained.

In the method, inputs are only a few calibrated images. Reflection character of object surface, geometric model of the scene and the position of lighting are not needed.

Many techniques have been presented about camera calibration and image based modeling. Different methods are adopted to different kind of scenes. It is a key to accurately find the corresponding points on input images and precisely calibrate the input images when using the method in this paper.

References

1. Yizhou Yu, Paul Debevec, Jitendra Malik, and Tim Hawkins, "Inverse Global Illumination: Recovering Reflectance Models of Real Scenes from Photographs", SIGGRAPH99
2. Sato, Y., Wheeler, M.D., and Ikeuchi, K. "Object shape and reflectance modeling from observation". In SIGGRAPH '97 (1997), pp. 379-387.
3. Ko Nishino, Zhengyou Zhang and Katsushi Ikeuchi. "Determining Reflectance Parameters and Illumination Distribution from a Sparse Set of Images for View-dependent Image Synthesis". in Proc. of ICCV 2001
4. Zhanwei Li, Jizhou Sun, "Separation and Reconstruction of Specular and Diffuse Reflection Images", The First International Conference on Machine Learning and Cybernetics (ICMLC-2002), Beijing, China.
5. Zhengyou Zhang. "A Flexible New Technique for Camera Calibration. Technique", Report of Microsoft Research, 1998 6.
6. Yizhou Yu, "Modeling and Editing Real Scenes With Image-Based Techniques", University of California, Berkeley. 2000 7.
7. Debevec, P. E., Taylor, C.J., and Malik, J. "Modeling and rendering architecture from photographs: A hybrid geometry and image-based approach". In SIGGRAPH '96 (August 1996), pp. 11-20. 8.
8. Paul Debevec, Yizhou Yu, and George Borshukov. "Efficient View-Dependent Image-Based Rendering with Projective Texture Mapping". In 9th Eurographics Rendering Workshop, Vienna, Austria, June 1998 9.
9. Songde Ma, Zhengyou Zhang, "Computer Vision-Computing Theory and Arithmetic Foundation", Science Publication, 1998 10.
10. Yu, Y. and Malik, J. "Recovering photometric properties of architectural scenes from photographs". In SIGGRAPH 98 (July 1998), pp. 207-217. 11.
11. Jianguang Sun, Changgui Yang, Computer Graphics, Qinghua University Publication, p481-485

Aerodynamic Analysis on the Supersonic Separation of Air-Launching Rocker from the Mother Plane

Young Mu Ji¹, Young Shin Kim², Jae Woo Lee¹,
Young Hwan Byun¹, and Jun Sang Park³

¹ Aerospace Engineering, Konkuk University,
Seoul, 143-701 Korea
{ymji, jwlee, yhbyun}@konkuk.ac.kr

² M.I. Tech., 241-3 Jinwi-Myon,
PyungTaek, Kyunggi, Korea
Bored3@hanmail.net

³ Mechanical Engineering, Halla University,
Wonju, 220-712 Korea
jspark@hit.halla.ac.kr

Abstract. A numerical analysis is made of the supersonic separation of air-launching rocket from the mother plane. Three-dimensional Euler equations have been numerically solved to capture details of steady/unsteady flow fields and transient behavior of the launching rocket during separation stage. Various types of interaction between shock and expansion waves are clarified with concomitant effects on the separation process. As extracting important design factors, which have major influences on the stability of separation, a guideline on the design of supersonic air-launching rocket is given.

1. Introduction

1.1 Air-Launching Method

An increasing interest in the dedicated launch system for the small satellites is widely spreading[1]. Studies on the air-launching rocket(ALR) with high thrust, high efficiency, and small weight are going on in diverse areas[2-5]. Typical examples of being successful at present are Pegasus[4] and SpaceshipOne[5], and both of them developed in U.S.A.: the Pegasus is a three-stage solid rocket launched at the altitude 12,000m and the Mach number 0.8. It can launch small satellites to the low altitude orbit. SpaceshipOne is a manned suborbital spacecraft with hybrid rocket motor. It separates at altitude 5,000m from the White Knight, aircraft with two turbofan engines, and climbs to 100km, then dives, glides and lands.

Recently, for several years, the development of supersonic air-launching system including the rocket engine, mission, trajectory and the system design has been performed by the authors[2,3,6]. In those studies, three-stage air-launcher with a hybrid-type rocket as a first stage was designed. Emphasis has been given to the safe and efficient launching. Air-launching method, especially launching at supersonic

speed from the mother plane, has many promising advantages: low satellite delivering cost into the space, use of a higher expansion-ratio than that at ground, a small drag loss during the mission, and no restrictions on the launch site and launch angles[6]. When the ALR launches at supersonic speed, the transonic flow instabilities can be effectively removed. On the other hand, it appears some unstable behaviors caused by the shock interaction between the ALR and the mother plane. Thus, shock interaction phenomena related to aerodynamic forces during the separation should be investigated to guarantee a success of supersonic launching[6].

In this study, the supersonic separation of the ALR from the mother plane and the behavior of the ALR after the separation will be analyzed by the numerical method and investigated the shock-expansion wave interaction between the ALR and mother plane. A guideline for the safe separation will be proposed for the design of supersonic ALR.

1.2 Configuration of the Supersonic Air-Launching Rocket in the Present Study

Mission of the ALR and the preliminary design results are as follows[3]:

- Mother Plane: F-4E Phantom
- TOGW: 1228.9kg
- Total length: 6.5m
- Maximum outer diameter: 0.6m
- Maximum payload: 7.5kg
- Target orbit: 700km circle orbit
- Required velocity: 7503.9m/s
- 1st stage propulsion system: hybrid rocket engine
- 2nd and 3rd stage propulsion system: solid rocket motor

Figure 1 shows a conceptual drawing of the ALR installed on the mother plane, F-4E phantom. Figure 2 shows the control surfaces of the ALR. To secure the tail bump angle for the safe take-off of the mother plane, the ALR has designed as X-shaped 4-control surfaces (fins) of which total area is 0.1887 m².

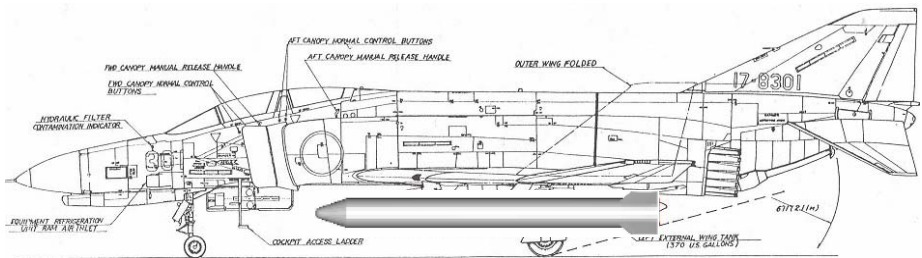


Fig. 1. Schematics of the ALR installed on F-4E Phantom

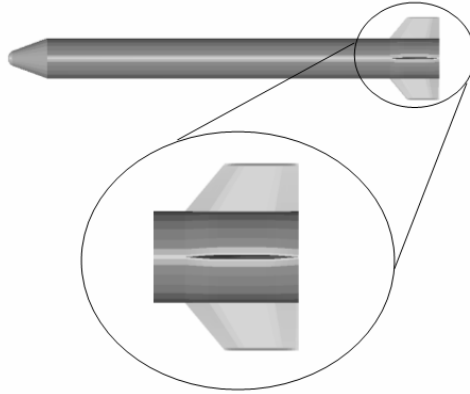


Fig. 2. Control surface shape and location

In this study, the center of gravity is determined by using the TMD (Tactical Missile Design) equation as shown in Eq.(1) [10]. The center of gravity of the ALR is located at 3.51m from the nose.

$$X_{CG} = \sum (X_{\text{subsystem}1} W_{\text{subsystem}1} + X_{\text{subsystem}2} W_{\text{subsystem}2} + \dots) / W_{\text{total}} \tag{1}$$

2 Computational Methods

Three-dimensional compressible Euler equations are solved numerically to investigate the flow field around the mother plane and the ALR. For this work, we employed both of in-house code, AADL3D[11] and the commercial software CFD- Fastran[12]. CFD-Fastran adopted the scheme for spatial difference based on flux vector splitting by Van Leer and MUSCL-scheme to improve accuracy. Minmod limiter is implemented to control oscillatory behaviors of the solution. Time difference terms are treated by fully implicit LU-SGS scheme[12].

In AADL3D, Roe’s FDS(flux difference splitting) scheme is implemented for the spatial discretization with the MUSCL for higher order expansion and fully implicit LU-SGS scheme is used for time integration. Also, the minmod limiter is used to remove solutions with an oscillation[11].

The governing equations for flow fields are as follows

$$\frac{\partial \bar{Q}}{\partial t} + \frac{\partial \bar{E}}{\partial x} + \frac{\partial \bar{F}}{\partial y} + \frac{\partial \bar{G}}{\partial z} = 0 \tag{2}$$

in which

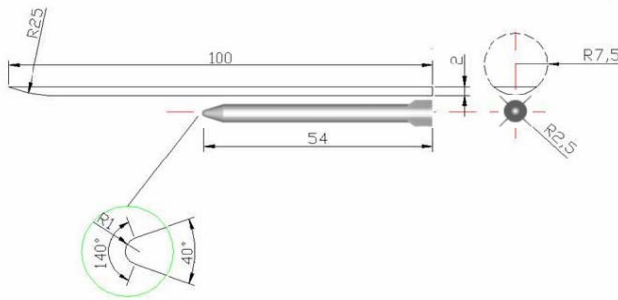
$$\bar{Q} = \begin{Bmatrix} \rho \\ \rho u \\ \rho v \\ \rho w \\ \rho e_t \end{Bmatrix}, \bar{E} = \begin{Bmatrix} \rho u \\ \rho u^2 + p \\ \rho uv \\ \rho uw \\ (\rho e_t + p)u \end{Bmatrix}, \bar{F} = \begin{Bmatrix} \rho v \\ \rho vu \\ \rho v^2 + p \\ \rho vw \\ (\rho e_t + p)v \end{Bmatrix}, \bar{G} = \begin{Bmatrix} \rho w \\ \rho wu \\ \rho wv \\ \rho w^2 + p \\ (\rho e_t + p)w \end{Bmatrix}.$$

For the analysis of unsteady supersonic separation behavior, a six-degree-of-freedom trajectory simulation has performed by which the aerodynamic force and moment on the ALR at each time step are integrated. As time step advances and the ALR moves to a new position, the velocity field and aerodynamic loads are recalculated. Above procedure is recursively continued to reach the drop length at which the ALR is outside the influence of the mother plane, approximately the vertical distance being twice of the rocket length[13].

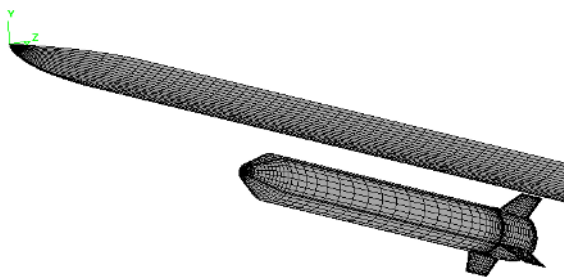
3 Numerical Results of Rocket Separation from the Mother Plane

3.1 Numerical Simulation Model and Grids System

For the numerical analysis of rocket separation from the mother plane, the complete geometry of the ALR located under the simplified mother plane is considered (see Fig. 3). The whole ALR configuration is shown in figure 3.



(a) Rocket arrangement



(b) Surface grid system

Fig. 3. Configurations of the Mother plane and air-launching rocket

After performing several cases of test run together with a grid sensitivity check, three-dimensional body fitted grid system is constructed as in Fig. 3(b), which consists of 15 multi-blocks and overlap structured grids. To enhance the numerical

stability and efficiency, the mother plane of Ogive-cylinder type modified to an infinite length along the downstream direction of the body. In fact, the wake flow does not influence on the upstream flow because the flow is supersonic.

3.2 Analysis Conditions for the Rocket Separation

In order to simulate the ALR separation, initial conditions for the rocket launching are given as follows:

- Launching velocity, M_∞ : 1.5
- Launching altitude: 12,000m
- Free stream pressure: 19399 N/m²
- Free stream temperature: 216.66 K
- Center of gravity, X_{CG} (From Nose): 3.51 m
- TOGW (Take Off Gross Weight): 1241.13 kg
- Moment of Inertia (assuming rigid body), I_{zz} : 4470.9 kg•m²
- Launching angles, (angle of attack, sideslip angle, roll angle): 0°

From the symmetric conditions on the x-z plane, no rolling or yawing movement is allowed.

3.3 Result and Discussions

Figures 4 and 5 show the results of steady-state numerical simulation, which is initial flow field just before the separation of rocket from the mother plane. As shown in Fig. 4, the oblique shock at the nose of the mother plane, and the bow shock around the nose of the ALR are noticeable. As expected, the supersonic free stream induces a strong shock and expansion waves near the fore body of the rocket, and those are reflected on the under-surface of mother plane and go back again and again to the rocket. It is clearly seen in Fig.5 that the reflected shock and the expansion waves wrap around the rocket surface by which a significant pressure change is caused.

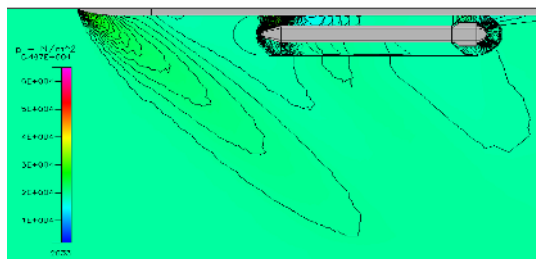


Fig. 4. Steady state pressure contours in the symmetric plane

A localized lower pressure region is noticed near the upper corner of the fore body of the rocket, due to the reflected expansion wave from the mother plane [see Fig. 5(a)]. In a little downstream region, the effect that the fore body shock reflected from the mother plane wraps around the rocket forms relatively high-pressure region

near the lower body of the rocket. This localized pressure difference between the lower ($-90^\circ < \theta < 90^\circ$) and upper half ($90^\circ < \theta < 270^\circ$) surface of the rocket gives rise to initial pitch-up motion during the separation stage. The circumferential angle, θ , around the rocket is defined in Fig. 6.

Above arguments may become clear by plotting the axial distribution of bottom ($\theta = 0^\circ$) and top ($\theta = 180^\circ$) surface. In fig.7, it shows the surface pressure distribution along the axial direction on the rocket surface at various fixed circumferential. Generally, the surface pressure is highest at the nose ($x=0.0$) where nearly normal shock occurs and it decreases very rapidly along the downstream direction because the shock angle, at the same horizontal location corresponding to the concerning rocket surface, inclines [see the pressure distribution over $0 < x < 0.02$]. The trend becomes reverse by the impact of reflected shock from the mother plane [see the pressure distribution over $0.02 < x < 0.1$]. However, the pressure decreases again near the corner turning around the rocket fore-body by the presence of expansion wave, where the flow is somewhat over-expanded [see the pressure distribution over $0.1 < x < 0.15$]. Finally, as over-expansion effect gradually disappears, the pressure monotonically converges to a constant value along the downstream up to fin position [see the pressure distribution over $0.15 < x < 1.0$].

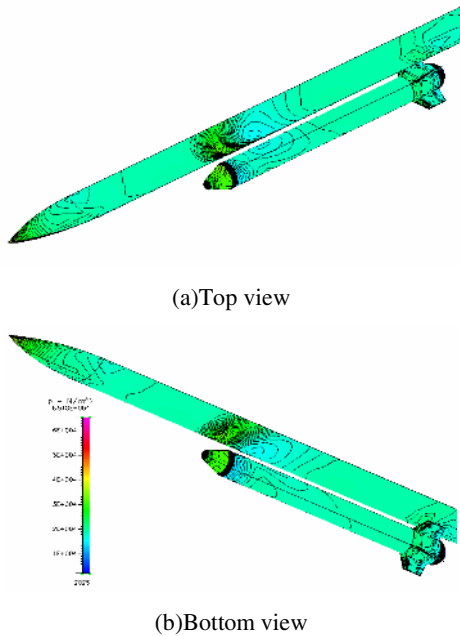


Fig. 5. Pressure contours on the surfaces of mother plane and rocket

In the region $0.02 < x < 0.1$, the shock wave reflected from the mother plane wraps around the rocket body and the wave effect is concentrated at $\theta = 0^\circ$, hence a higher pressure region is formed near the bottom surface ($\theta = 0^\circ$) of the rocket than the top

surface ($\theta = 180^\circ$). The pressure difference between lower pressure top-region and higher pressure bottom-region gives rise to upward-lift of which aerodynamic center is located at a certain position in $0.02 < x < 0.1$, which is far ahead of the center of gravity of the rocket. Therefore, the pitch-up moment is generated at early stage of the rocket separation. In the region $0.1 < x < 0.15$, opposite phenomenon exists but the effect on the resultant moment is very limited due to the smallness of the magnitude of pressure difference and the length of momentum arm from the center of gravity of the rocket.

Pressure increment around the rear-body is mainly due to the presence of the control surfaces (fins). In this region, the pressure difference is negligible so that the contribution of this region on initial pitch-up motion of the rocket is minor.

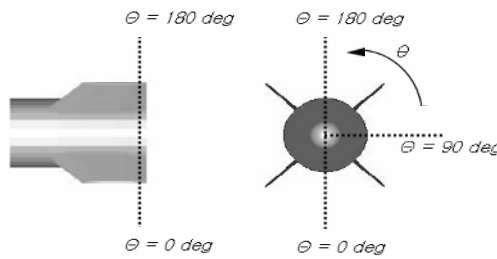


Fig. 6. Definition of circumferential angle θ

Utilizing the result of steady-state analysis as an initial flow condition, numerical computation has done to investigate three-dimensional unsteady separation of the rocket from the mother plane. The computation has been carried out for $t=1.5$ seconds. When $t=1.5s$, the separation distance defined as smallest length between the mother plane and the ALR becomes twice of the rocket length, and all interferences between the mother plane and rocket disappear. To demonstrate two representative cases, i.e., stable and unstable separations, computations have conducted for the cases of rocket body geometry with/without control surface (fin).

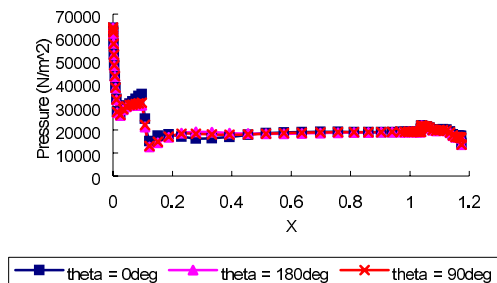


Fig. 7. Surface pressure distributions along the axial direction at $t=0$

In the case of rocket geometry without fin, the rocket undergoes significant pitch-up motion during the separation as shown at Fig. 8. On the surface of under-body near the nose, high-pressure zone is formed at early times, and is broadening to the downstream as time increases. On the other hand, low-pressure zone is rapidly spreading over the whole upper surface as time increases [see the pressure contour at $t=1.5s$ in Fig.8]. By the interaction of surface pressure distribution mentioned above, clockwise pitch-up moment strengthens monotonically as time increases. In this case, there is no recovery force to pitch-down.

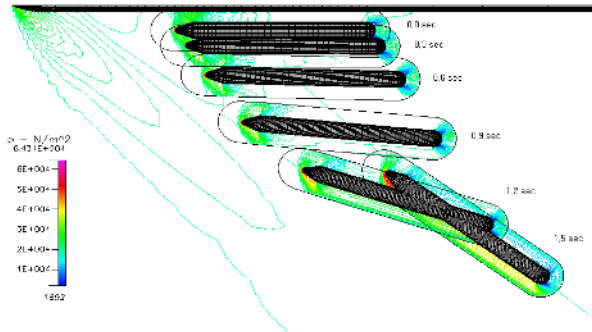


Fig. 8. Pressure contour and transient behavior of the rocket without control surface during separation process

Fig.9 shows time history of the pitch angle in the case of the ALR geometry without fin. A slight pitch-down motion is noticed till to $t=0.4s$ after launching and then the pitch-up moment is generated and the rocket sets in successive nose-up motion after $t=0.4s$. As a result, the rocket motion becomes eventually unstable and is set into the stall behavior at large times.

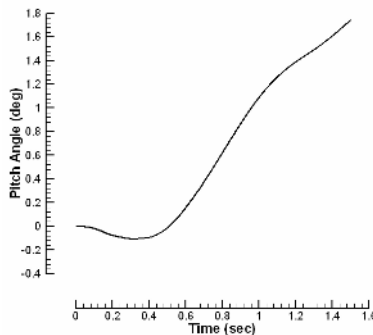


Fig. 9. Time history of the pitch angle in the case of ALR without fin

Figure 10 shows transient motion of the rocket with fin. By the counter action of fin to pitching moment induced by surface pressure distribution near the nose, the

rocket is stably separating from the mother ship, and sustaining a small pitch angle within a proper limitation. The mechanism on stable separation is elucidated in the following reasoning. At the initial state, very small pitch-up moment, due to surface pressure near the nose (nose effect), is forced to the rocket. As time and pitch-up angle increase, fin effect to recover the original positioning of the rocket emerges and this restoring force by fin overwhelms initial pitching-force by the surface pressure distribution near the nose. At those times, the rocket turns into pitch-down motion. As time goes on, one (nose/fin) effect dominates the other (fin/nose) effect alternately. Figure 11 shows the repeating procedure of pitch-up and down motion by restoring pitching moment due to the relative magnitude of nose and fin effects.

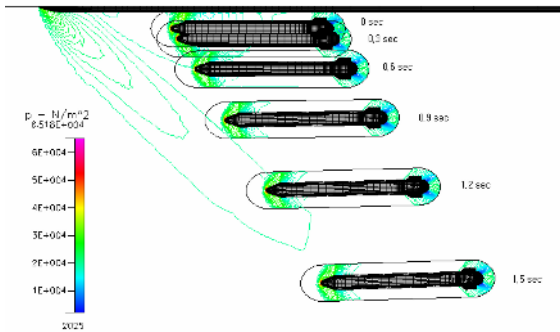


Fig. 10. Pressure contour and transient behavior of the rocket with control surface during separation process

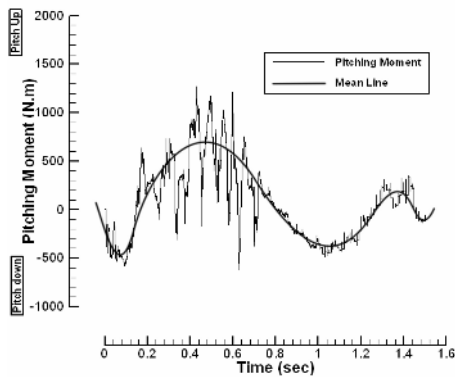


Fig. 11. Pitching moment of the ALR along the time

4 Conclusions

In this study, the supersonic separation of the rocket from the mother plane and the behavior of the rocket after the separation have been investigated.

The shock and the expansion waves generated at the rocket nose are reflected from the mother plane and wrap around the rocket, which results in a significant pressure change on the rocket surface and induces a pitching motion. To demonstrate typical stable and unstable separation processes, two cases of rocket geometry (rocket with/without control surfaces) were investigated:

By the presence of properly designed control surfaces, the pitch-up motion can be stabilized through the competing between destabilizing and stabilizing behaviors, and safe separation is secured.

Acknowledgement

This study has been done in part by the support of grant number R01-2000-000-00319-0 from the Korea Science and Engineering Research Foundation.

References

1. Bang, H.C., Park, H. C.: Status and Future Outlook on Nano-Pico Satellites Development. *J. Korean Soc. Aero. & Space Sci.* 28(5) (2000).
2. Lee, J.W., Park, Jeon, K. S., Roh, W. R.: Mission and Trajectory Optimization of the Air-Launching Rocket System Using MDO Techniques. *AIAA 2002-5492* (2002).
3. Lee, J.W., Park, B.K., Jeon, K.S. Hybrid Air-Launching Rocket System Design through Multidisciplinary Optimization Approach. *ASDL External Advisory Board Review and International Design Symposium*, May (2003) 28-30.
4. Pegasus User's Guide, Orbital Science Corporation, Sept. (1998).
5. Macklin, F. New applications for hybrid propulsion, 39th AIAA/ASME/SAE/ASEE joint propulsion conference, *AIAA 2003-4888* (2003).
6. Donahue, B. Supersonic air-launching with advanced chemical propulsion. 39th AIAA/ASME/SAE/ASEE joint propulsion conference, *AIAA 2003-4888* (2003).
7. Mendenhall, M.R., Lesieutre, T.O., Lesieutre, D.J., Dillenius, M.F.E. Carriage and release aerodynamics of the Pegasus air-launched space booster. *The AGARD FDP Symposium on "Aerodynamics of Store Integration and Separation* (1995).
8. Lasek, M., Sibilski, K. Modeling of External Store Separation. 40th AIAA Aerospace Sciences Meeting & Exhibit (2002).
9. Kim, J.H., Sohn, C.H., Kang, J.H., Kim, M.S. Store Separation Analysis for KT-1 Gun Pod using Wind Tunnel Test and CFD. *Proceedings of the 2003 KSAS Fall Conference* (2003)
10. Fleeman, E.L. *Tactical Missile Design*. AIAA (2001).
11. Lee, J.W., Min, B.Y., Byun, Y.H., Changjin Lee, C. Numerical Analysis and Design Optimization of Lateral Jet Controlled Missile. *21st International Congress of Theoretical and Applied Mechanics*, Aug. (2004).

Effect of Grid Resolution on the Statistics of Passive Scalar in an Injection-Driven Channel

Yang Na¹, Dongshin Shin², and Seungbae Lee³

¹ Corresponding Author, CAESIT,
Dept. of Mechanical Engineering,
Konkuk University,
Hwayang-dong 1, Gwangjin-gu,
Seoul 143-701, Korea
yangna@konkuk.ac.kr

² Dept. of Mechanical Engineering, Hong-Ik University,
Seoul 121-791, Korea
dsshin@wow.hongik.ac.kr

³ Dept. of Mechanical Engineering, Inha University,
Inchon 402-751, Korea
sbaelee@inha.ac.kr

Abstract. Effect of grid resolution on the statistics of passive scalar in a complex shear layer was investigated using a direct numerical simulation technique. The grid resolution in the shear layer which was generated from the interaction of main and injected streams strongly influences the subsequent evolution of the passive scalar. Dissipation, integral length-scale, skewness and flatness factors of the passive scalar are sensitive to the numerical resolution away from the wall where coherent structures grow very rapidly.

1 Introduction

Direct numerical simulation (DNS) resolves all the scales of fluid motion. Conceptually it is the simplest approach and, when it can be applied, it is most accurate and complete in the level of description provided. The drawback of DNS is of course its very large computational cost, and the fact that this cost increases rapidly with the Reynolds number. However, DNS studies have proved extremely valuable in many previous studies in revealing the physics of turbulence and turbulent flows.

For the turbulent flow in an injection-driven channel, an accurate prediction of the flow is of direct importance in many practical applications such as those in combustion chamber and transpiration cooling. Since turbulence plays a critical role in the evolution and dispersion of passive scalar, a better understanding of the flow characteristics will be very useful for the efficient design and operation of various thermal systems.

Even though a significant development has been made to the prediction method of velocity field in wall-bounded channel with transpired walls (Beddini [1]), relatively much less effort has been made in the calculation of passive scalar transport in spite

of its practical importance. Many of earlier investigations had to rely on RANS type approach or relatively simple instrumentations and thus, an inherent limit was imposed in understanding the behavior of turbulent passive scalar field. As the flow situation becomes more complex, the Reynolds analogy between the flow and passive scalar deteriorates further and, thus, the analysis for the passive scalar becomes much more difficult. The present work mainly intended to examine the effect of numerical resolution on the passive scalar transport in complex flow situation. In line with the purpose of this study, a direct numerical simulation technique which gets solutions of governing equations without turbulence model was adopted.

The focus will be restricted to turbulence statistics such as turbulent Prandtl number, turbulent diffusivity and integral length-scale of the passive scalar which are usually hard to obtain directly from the measurements. Even though those statistics will require a significantly long averaging time, an attempt of getting perfectly smooth data by averaging over such a long period of time was not made in the present work. Instead, all the statistics were averaged over a time span which is sufficiently long enough only for up to the second-order statistics on the consideration of computational cost.

A brief description of numerical methodology will be provided in the next section and then, several statistical results will be discussed.

2 Description of Numerical Methodology

2.1 Governing Equations

Assuming that the flow is incompressible, the following non-dimensional equations for velocity and passive scalar were solved on a rectangular, staggered grid (Harlow & Welch [2]).

$$\frac{\partial u_i^*}{\partial x_i^*} = 0$$

$$\frac{\partial u_i^*}{\partial t^*} + \frac{\partial}{\partial x_j^*} (u_i^* u_j^*) = -\frac{\partial p^*}{\partial x_i^*} + \frac{1}{\text{Re}_h} \frac{\partial^2 u_i^*}{\partial x_j^* \partial x_j^*}$$

$$\frac{\partial T^*}{\partial t^*} + \frac{\partial}{\partial x_j^*} (u_j^* T^*) = \frac{1}{\text{Re}_h \text{Pr}} \frac{\partial^2 T^*}{\partial x_j^* \partial x_j^*}$$

All the variables are made dimensionless using an inlet bulk velocity and a half channel height. For convenience, the superscript * will be dropped hereinafter. The governing equations are integrated in time using a semi-implicit scheme. A low storage, 3rd order Runge-Kutta scheme was used for treating convective terms explicitly and the Crank-Nicolson scheme for viscous terms semi-implicitly. All the spatial derivatives are approximated with second order central difference scheme. For more numerical details, see Na [3].

2.2 Computational Details

Three-dimensional, rectangular computational domain consists of a streamwise extent of $26h$ and a spanwise extent of $6.5h$. Here h is the half channel height. The constant wall injection starts along both upper and lower wall from the location of $x/h=13.4$. The strength of wall injection, defined by the ratio of applied wall injection to the inlet bulk velocity, was set to 0.05. This is quite a strong injection and results in a strong acceleration of the flow in the main flow direction to satisfy global mass conservation. Thus, the pressure gradient (which does not appear in the mean concentration equation) is one of important terms in the mean momentum equation budget for the streamwise velocity component. The Reynolds number based on the inlet bulk velocity and a half channel height is 2250.

For the passive scalar, it was assumed that the bottom wall is maintained at a constant temperature (or concentration), $-T_w$, and the top wall at T_w . The Prandtl number was assumed to be 1 so that the working fluid can be thought of as a gas (instead of liquid). In order to prevent the numerical instability for the passive scalar, a widely used QUICK scheme (Leonard [4]) was employed for the convective terms of the passive scalar equation.

The no-slip boundary condition is used along the wall except in a region where constant blowing is applied. The flow is assumed to be homogeneous in the spanwise direction, justifying the use of periodic boundary condition in that direction.

In order to assess the effect of numerical resolution, a series of computations were conducted and the test cases considered in the present paper are summarized in the following table.

Table 1. Test cases performed

Name of test cases	Number of numerical grids
CASE1	$257 \times 129 \times 129 \approx 4.3$ million grids
CASE2	$257 \times 257 \times 129 \approx 8.5$ million grids
CASE3	$513 \times 257 \times 129 \approx 17$ million grids
CASE4	$513 \times 257 \times 257 \approx 34$ million grids

The geometry of the present injection-driven flow contains several regions of non-negligible gradients in the wall normal direction, which requires a very careful distribution of grid spacing. The CASE3 uses a $513 \times 257 \times 129$ grid system and this gives the resolution of approximately $\Delta x^+ \approx 7.5$, $\Delta y_{\min}^+ \approx 0.0056$, $\Delta y_{\max}^+ \approx 1.8$, $\Delta z^+ \approx 7.5$ in terms of wall unit. When 257 grid points are used in the spanwise direction (CASE4), the grid spacing in the spanwise direction becomes 3.8 in wall unit. Judging from the turbulence studies reported in the literature, it can be said that the present resolution is more than good for resolving the simple channel flow at comparable Reynolds number.

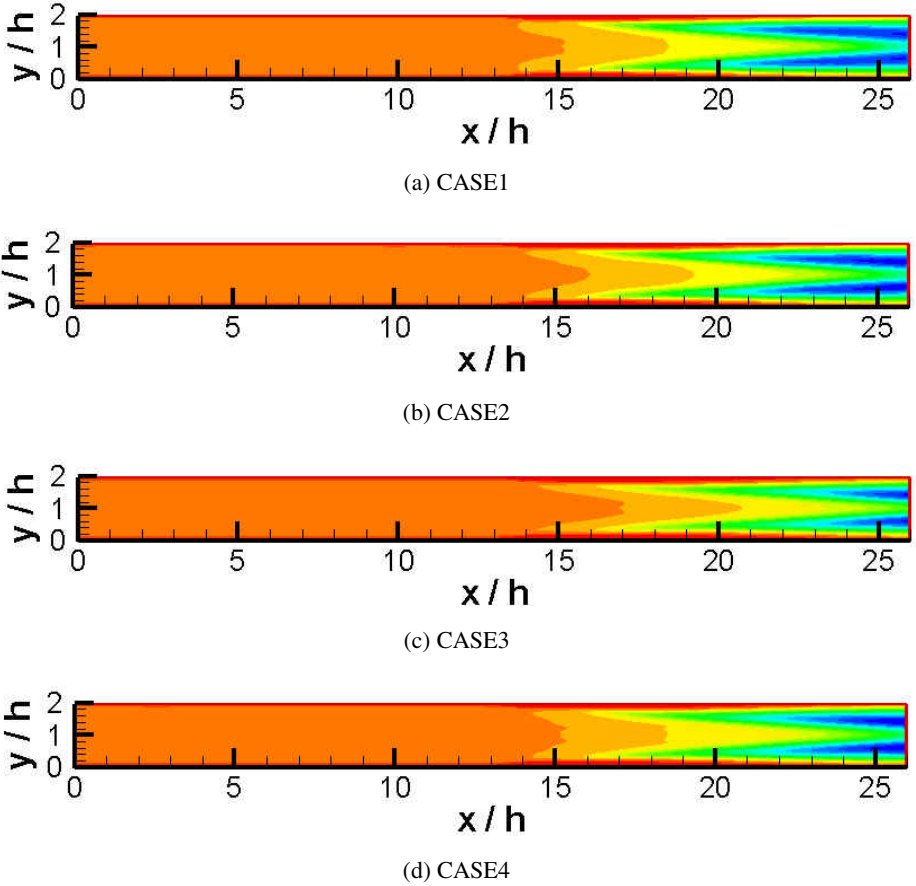


Fig. 1. Comparison of $-\overline{T'v'}$ contours obtained with different resolutions

3 Results and Discussion

The turbulent heat flux in the wall-normal direction is likely to be influenced most by the grid resolution in the shear layer formed in the middle of the channel. A series of contour plots in Figure 1 show the effect of resolution on $-\overline{T'v'}$ in (x-y) plane. Overall behavior is qualitatively similar but it definitely shows the differences especially in the shear layer after $x/h > 15$. However, it can be said that, from an engineering point of view, the resolution of CASE1 is reasonably acceptable in catching the relevant flow physics. .

Turbulent diffusivity and turbulent Prandtl number at $x/h=24$ are compared in Figures 2-3. A non-negligible variation with the numerical resolution is realizable in both figures. Compared with the simple channel flow, turbulent diffusivities are significantly enhanced due to the turbulent activities in the developing shear layer. The turbulent Prandtl number also exhibits a qualitatively different distribution across the

channel. Since new turbulent structures are being generated rapidly in the shear layer, sufficient resolution should be provided to capture the correct growth rate of those structures and thus, the grid resolution is thought to be responsible for the differences seen in these figures.

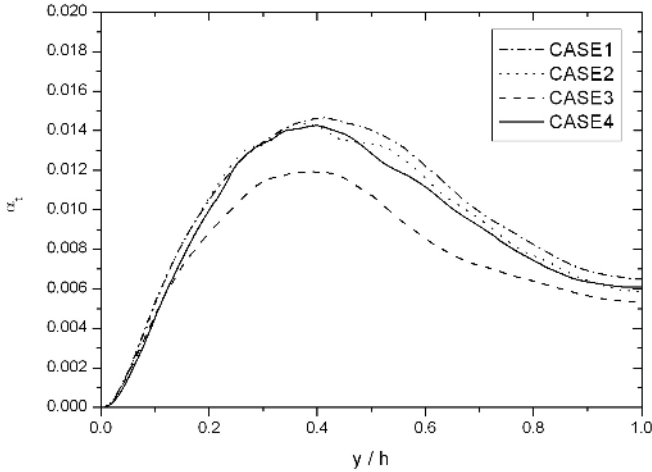


Fig. 2. Distribution of turbulent diffusivity at $x/h=24$

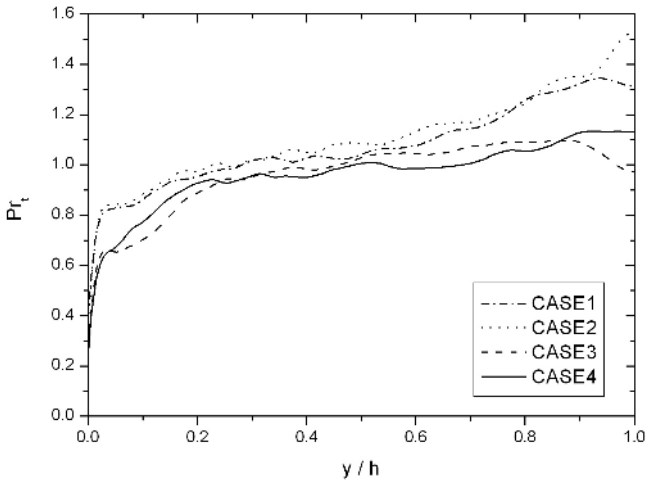


Fig. 3. Distribution of turbulent Prandtl number at $x/h=24$

A similar behavior of resolution-dependence can be seen in the distribution of dissipation of passive scalar. As the resolution gets better, smaller scale motions are better resolved and this results in a higher dissipation rate as shown in Figure 4. In

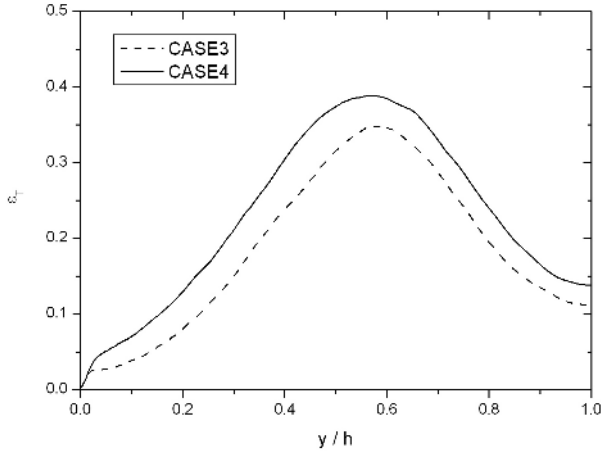


Fig. 4. Dissipation of passive scalar at $x/h=24$

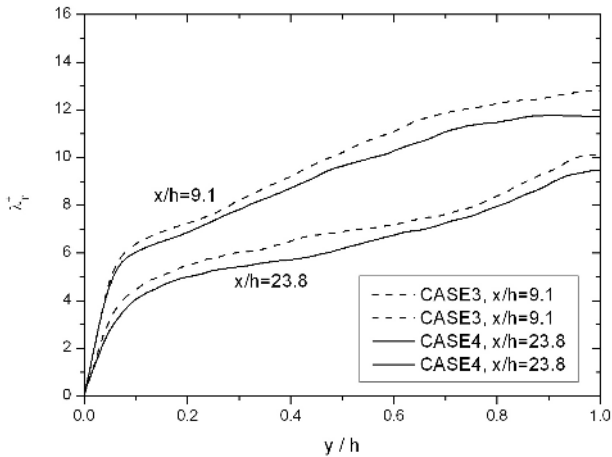
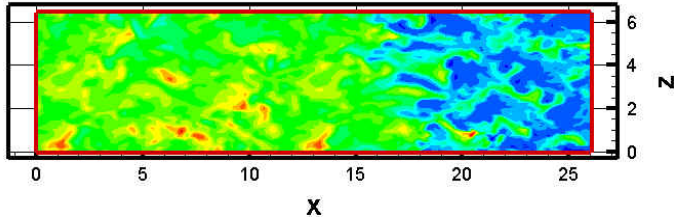
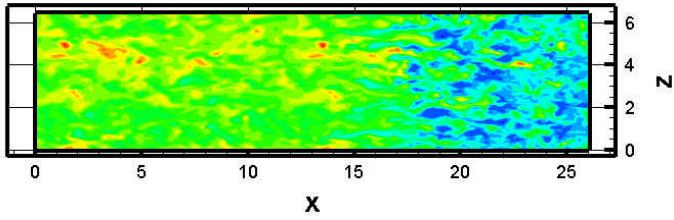


Fig. 5. Integral length-scale of passive scalar

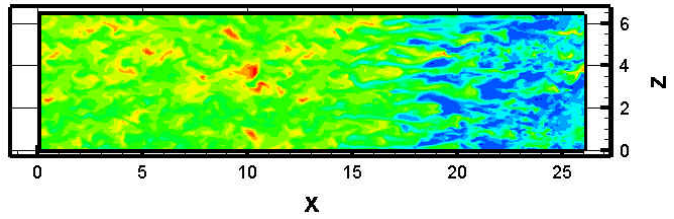
order to understand the turbulence maintenance mechanism, the correct prediction of dissipation is very important. Unfortunately, the simulation with more grid points than CASE4 was not possible due to the prohibitively high computational cost and it is not sure if the further improvement can be obtained with in Figure. Using the information of rms fluctuation and dissipation of passive scalar, one can define the integral length-scale shown in Figure 5. In the shear layer formed in the middle of the channel, the coherent structures which came from the upstream interact with the injected stream originating from the walls. In this process, the existing structures may be broken into smaller ones or smaller scale motions are newly born in this region. This possibility is illustrated in Figure 5. In any case, a better resolution gives a smaller length scales at different locations. This result can be also noticed in Figure 6 where instantaneous passive scalar fields are displayed in $(x-z)$ plane at $y/h=0.43$.



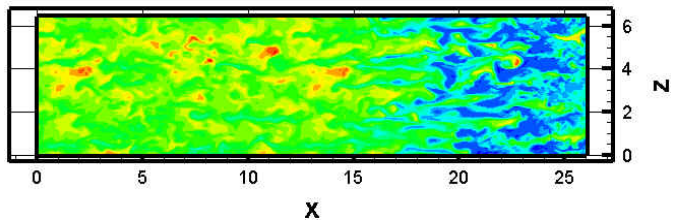
(a) CASE1



(b) CASE2



(c) CASE3



(d) CASE4

Fig. 6. Instantaneous concentration field in (x-z) plane at $y/h=0.43$

Finally, in Figures 7 and 8, skewness and flatness factors at $x/h=24$ obtained from CASE3 and CASE4 are compared. Note that they are calculated from 3rd and 4th order statistics, respectively. Both factors exhibit very high values close to the wall suggesting that the passive scalar is significantly disturbed (or modified by the wall injection). Skewness factor, which is a measure of intermittency, is significantly different from its Gaussian value of zero up to $y/h=0.65$. Flatness factor in the middle of the

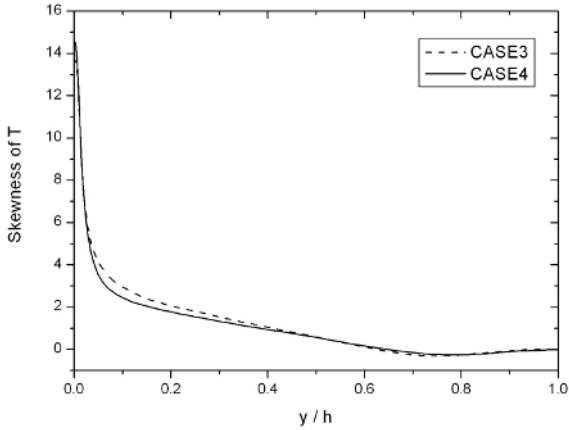


Fig. 7. Skewness factor of passive scalar

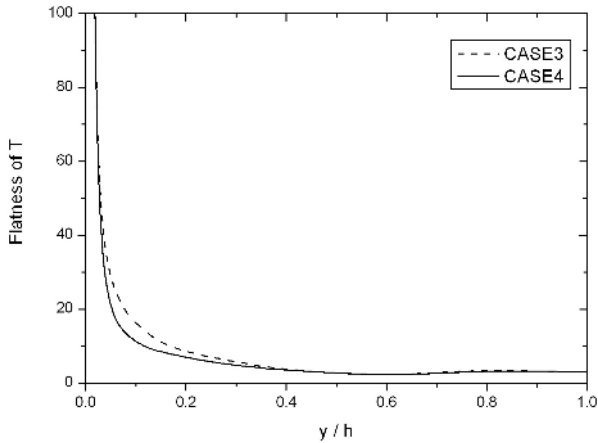


Fig. 8. Flatness factor of passive scalar

channel fluctuates around Gaussian value of 3 similar to the simple channel but it increases very rapidly in the vicinity of the wall. As expected from the previous results, Figures 7-8 show that the higher-order statistics between $0.05 < y/h < 0.4$ are also influenced by the resolution in the developing shear layer.

4 Summary

Direct numerical simulations were performed with different numerical resolutions in the injection-driven turbulent channel which is characterized by non-negligible streamwise inhomogeneity with an objective of analyzing the effect of grid resolution in complex flow situation. In the present configuration, the complexity of the flow came from the shear layer formed by the interaction of main flow with the wall

injection. This inhomogeneity not only renders the computational analysis very expensive but also makes the quality of prediction be influenced by the grid resolution used.

A close investigation of the results suggests that the dissipation and integral length scale of passive scalar are strongly affected by the number of grids. When the resolution is sufficiently high, the turbulent Prandtl number turned out to be rather constant in the outer layer ($y/h > 0.2$). Regardless of the presence of large 2-D roller-type structures, which usually can be observed in the mixing layer, a proper resolution for the smaller scale motions present in the developing shear layer should be guaranteed for the accurate prediction of subsequent evolution of the passive scalar.

Acknowledgement

This work was supported by grant No. R01-2004-000-10041-0 from the Basic Research Program of the Korea Science & Engineering Foundation.

References

1. Beddini, R. A.: Injection-Induced Flows in Porous-Walled Duct, *AIAA J.*, vol. 24, no. 11 (1986) 1766-1772.
2. Harlow, F. H. and Welch, J. E.: Numerical Calculation of Time Dependent Viscous Incompressible Flow of Fluid with Free Surface, *Phys. Fluids*, vol. 8 (1965) 2182-2189.
3. Na, Y.: Direct Numerical Simulation of Turbulent Scalar Field in a Channel with Wall Injection. *Numerical Heat Transfer, Part A* (2005) 165-181.
4. Leonard, B. P.: A Stable and Accurate Convective Modeling Procedure Based on Quadratic Upstream Interpolation, *Comput. Meth. Appl. Mech. Eng.*, vol. 19 (1979), 59-98.

Test of Large Eddy Simulation in Complex Flow with High Schmidt Number

Yang Na^{1,*} and Seungmin Lee²

¹ CAESIT, Dept. of Mechanical Engineering, Konkuk University,
Hwayang-dong 1, Gwangjin-gu, Seoul 143-701, Korea
yangna@konkuk.ac.kr

² Dept. of Mechanical Engineering, Konkuk University,
Seoul 143-701, Korea
minisgood@naver.com

Abstract. Turbulent concentration field with $Sc=50$ was investigated via large eddy simulation. Dynamic mixed model for the passive scalar was tested in a strong shear layer. Both mean and rms eddy diffusivities were shown to be reduced in the middle of the channel as the Schmidt number becomes large. A sudden increase of SGS turbulent Prandtl number in the vicinity of the wall suggests that more careful choice of filter size is required to capture the subgrid-scale dynamics correctly in this region when analyzing high Schmidt number flow.

1 Introduction

Turbulence in fluids is considered as one of the most difficult problems of modern physics. Direct numerical simulation (DNS), known as one of the most accurate and complete analysis tools, is supposed to resolve all the spatial scales of turbulence and naturally it requires an extremely high computational cost. In large eddy simulation (LES), on the other hand, only the dynamics of the larger scale motions are computed explicitly while the effects of small scales are represented by simple subgrid scale (SGS) models. Generally, industrial, natural, or experimental configurations involve Reynolds numbers that are far too large to allow direct numerical simulation and the only possibility then is large eddy simulation.

The literature indicates that significant development has been made for the prediction of a turbulent velocity field, but much less effort has been done in the calculation of passive scalar transport. One of the ingredients in understanding turbulent transport of a scalar between a flowing fluid and a solid surface is to analyze the behavior of the fluctuating concentration field in the diffusive sublayer where almost all of the change of mean concentration or temperature can occur at high Schmidt (Sc) or Prandtl (Pr) numbers. In addition to the fact that the diffusive sublayer lies entirely in the viscous sublayer, a passive interaction of concentration field with coherent structures very close to wall makes the analysis much more difficult compared to the case

* Corresponding author.

of mass transfer at low or moderate Schmidt number and this is reflected in the many controversies of the behavior of mass transfer coefficient. The present work is motivated by the need for the practical methodology for predicting high Schmidt number concentration fields. Among many SGS models available, dynamic mixed model (DMM) proposed by Zang et. al [1] combined with finite difference formulations, which most conveniently uses filters in physical space, was tested in a shear layer resulting from the interaction of main and injected flows.

In several previous LES studies, DMM has been shown to produce better results in a wide range of turbulent flows than the dynamic Smagorinsky model (DSM) of Germano et al.[2]. Even though Calmet & Magnaudet [3] showed the success for the high Schmidt number mass transfer problem with DMM, definitely more evidences in more complex flow situations will be required to assess the feasibility of LES methodology and this motivates the present work.

In the next section, numerical methodology will be briefly explained and then instantaneous and statistical results will be discussed.

2 Numerical Methodology

2.1 Governing Equation

For incompressible flows, the filtered governing equations in a conservative form for the LES of a passive scalar are given as follow:

$$\frac{\partial \bar{u}_i}{\partial x_i} = 0, \tag{1}$$

$$\frac{\partial \bar{u}_i}{\partial t} + \frac{\partial}{\partial x_j} (\overline{u_i u_j}) = -\frac{\partial \bar{p}}{\partial x_i} + \frac{\partial}{\partial x_j} (2\nu \bar{S}_{ij} - \tau_{ij}), \tag{2}$$

$$\frac{\partial \bar{T}}{\partial t} + \frac{\partial}{\partial x_j} (\overline{u_j T}) = \frac{\partial}{\partial x_j} (\alpha \frac{\partial \bar{T}}{\partial x_j} - q_j). \tag{3}$$

where the overbar denotes a grid-filtering operation. The effect of unresolved subgrid scales is represented by the following residual stress tensor τ_{ij} and residual scalar flux vector q_j .

$$\tau_{ij} = \overline{u_i u_j} - \bar{u}_i \bar{u}_j, \tag{4}$$

$$q_j = \overline{T u_j} - \bar{T} \bar{u}_j. \tag{5}$$

All the terms in equations (1)-(3) are resolved except τ_{ij} and q_j which should be obtained through the appropriate LES models. Details of how to integrate governing

equations and to calculate τ_{ij} and q_j using DMM approach are explained in Lee & Na [4] and will not be repeated here.

2.2 Computational Details

The streamwise extent of the computational domain is $26h$ and the spanwise extent is $6.5h$, where h is the half-channel height. In order to provide physically realistic turbulence to the region of main interest with uniform wall injection, a periodic channel (without wall injection) with a length of about $12h$ was placed in front of the region of the injection-driven flow regime.

The Reynolds number defined by the inlet bulk velocity and half-channel height was set to 2250, while Schmidt number (or equivalently, Prandtl number) was set to 50. A total of 129 grids were used in the streamwise direction, 65 grids in the spanwise direction, and 97 grids in the wall-normal direction.

No-slip boundary condition was used at both upper and lower walls except in the region where constant blowing was applied ($x/h > 13$). The strength of the wall injection defined by the ratio of injected velocity to the inlet bulk velocity was set to 0.05. Due to this strong wall injection, the flow experiences a rapid acceleration (or equivalently large convective term) in the main flow direction. For the passive scalar field, the temperature (or concentration) at the wall was set to $-T_w$ and that of the top wall was T_w .

A box filter was applied as both grid and test filters and no explicit filtering was done in the normal direction. The only adjustable parameter of the SGS model is the ratio of filters and the value of 2 was chosen for the present study.

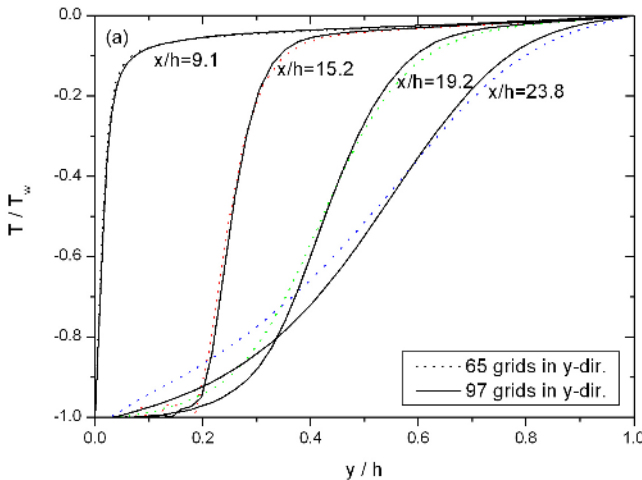


Fig. 1. Mean concentration profiles with two different resolutions

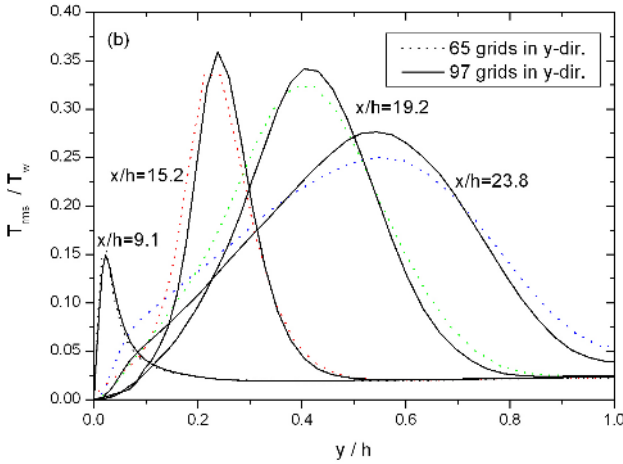


Fig. 2. Concentration fluctuations with different resolutions

3 Results

For the calculation of statistical quantities, averages were obtained over the homogeneous spanwise direction and time of about $40 h/U_b$. This period of time may not be enough for the very smooth higher order statistics but it is sufficient for the purpose of the present study.

The adequacy of the numerical resolution was assessed by examining the mean and root-mean-square (rms) concentration (or temperature) fluctuations at several representative streamwise locations. Figures 1-2 compares the progression of mean and rms fluctuations of temperature profiles. These progressions suggest that profiles deviate significantly from that of lower Schmidt number flows. Since the temperature gradient is extremely large near the wall, a higher resolution gives significant improvement especially in this region. Distribution of concentration (or temperature) fluctuations in the injection-driven region showed sizable departures as well. However, the result at $x/h=9.1$ indicates that a better resolution in the wall-normal direction does not improve the solution in the absence of wall blowing. Thus, a shear layer generated away from the wall requires a higher resolution for the better prediction of concentration field.

In order to understand how the concentration field is modified due to the change of Schmidt number, the present result was compared with that of $Sc=1$ in Figure 3. As shown clearly in the figure, peaks of concentration fluctuations were moved away from the wall. This feature is thought to be directly associated with the growing lifted shear layer that results from the interaction of the main flow with the wall injection. In Figure 4, the instantaneous concentration fields at two different (x - z) planes are presented. At $y/h=0.065$, the streak-like structures are totally disappeared due to the lifted boundary layer.

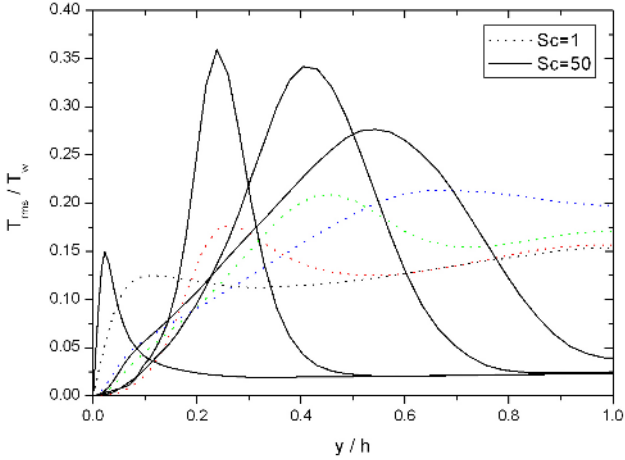


Fig. 3. Comparison of fluctuations with $Sc=1$

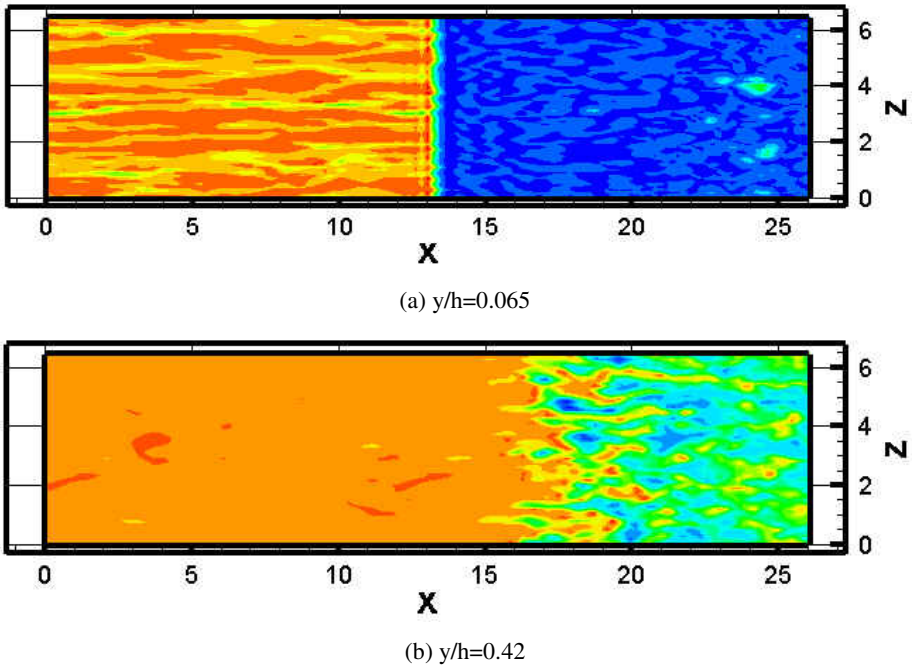


Fig. 4. Instantaneous concentration fields in two $(x-z)$ planes

However, the fact that those structures are present at $y/h=0.42$ suggests that they do not die but just move away from the wall probably due to the action of wall injection.

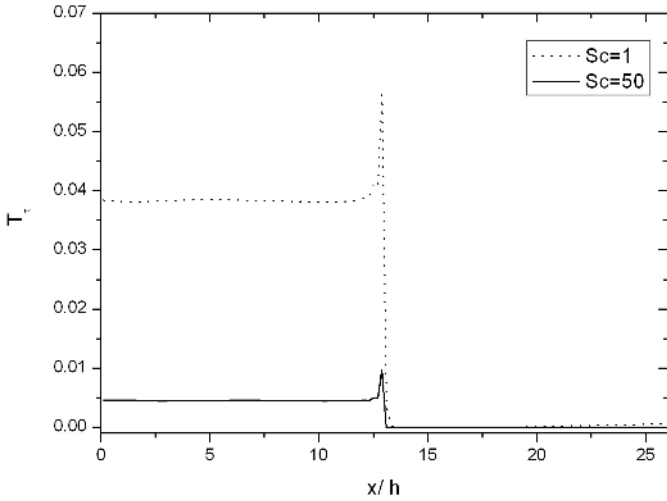


Fig. 5. Distribution of friction temperature

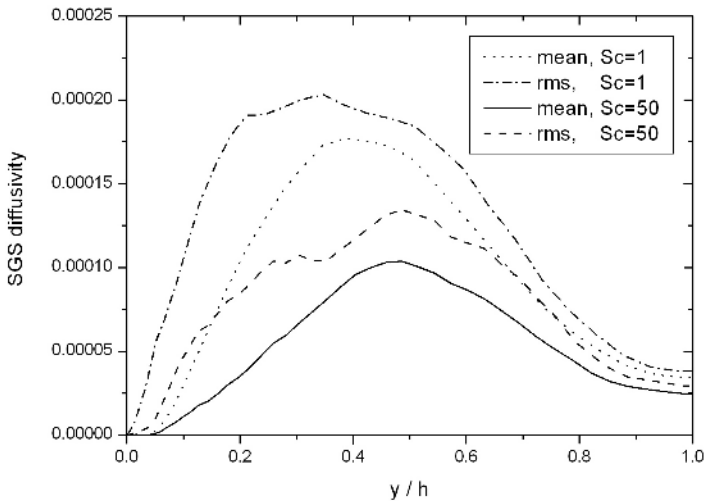


Fig. 6. Comparison of eddy diffusivity

The friction temperature shown in Figure 5 indicates that the concentration boundary layer was totally displaced away from the wall after $x/h=13$ regardless of Schmidt number. The fact that the conduction heat transfer rate (or concentration gradient) at the wall decays faster than the skin friction coefficient (or velocity gradient) implies that hydrodynamic and thermal boundary layers react differently to external forces such as strong wall injection.

Eddy diffusivity at $x/h=24$ are compared for $Sc=1$ and 50 in Figure 6. It is seen that both mean and rms concentration field were reduced throughout the channel. The fact

that a significant variation of the SGS turbulent Prandtl number with Schmidt number was not noticed except in the vicinity of the wall in Figure 7 suggests that eddy viscosity was also reduced due to the higher grid resolution (or higher cutoff wave-number). However, a sudden increase near the wall is worth of notice. This rapid increase of SGS turbulent Prandtl number close to wall is thought to be directly related to an insufficient resolution of thin concentration boundary layer. A concentration field with high Schmidt number is expected to have a very large mean gradient (or equivalently extremely thin boundary layer) and will require a significant grid concentration. Since the present work intends just to test the feasibility of LES for the high Schmidt number, an attempt of using more grid points than 97 in the wall-normal direction was not made.

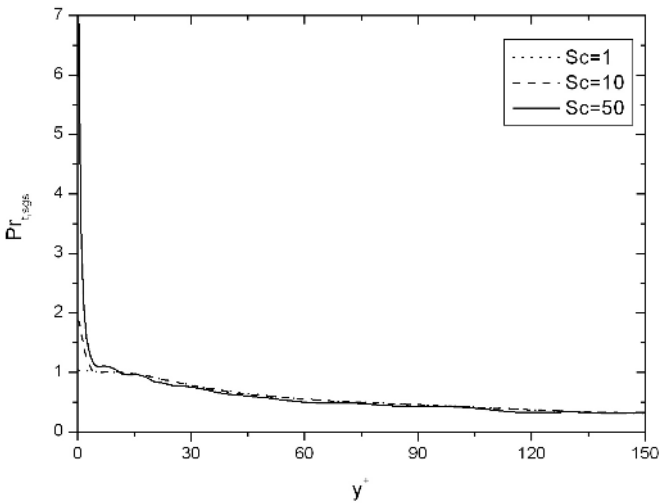


Fig. 7. Comparison of SGS turbulent Prandtl number

4 Summary

The importance of integrated or combined analysis is rapidly growing these days. In many combined studies such as in the present work, an accurate prediction of flow is a prerequisite for the subsequent analysis of heat and mass transfer. Since a passive scalar was assumed here, two-way coupling was not considered this time and the concentration field was assumed not to influence the flow field.

From a practical engineering standpoint, the algorithm of dynamic mixed model of Zang et al. [1] was extended to the prediction of passive scalar and tested in the case of $Sc=50$. To assess the feasibility of the DMM, the model was applied in a strong shear layer generated from the interaction of mean and injected flows. This preliminary test shows the possibility of using DMM for the high Schmidt number flow.

Away from the wall, eddy diffusivity is reduced as the Schmidt number increases. Since the eddy viscosity is unchanged, a lower value of eddy diffusivity results in a

reduced SGS turbulent Prandtl number. However, the reason why the SGS turbulent Prandtl number decreases is not clear. Since high Schmidt number concentration field is associated with a much wider range of length scales than the velocity field, the size of the filter (or cutoff wave-number) for the concentration field is likely to play an important role in the analysis. This issue will be further investigated.

Acknowledgement

This work was supported by Korean Agency for Defense Development under Contract ADD-01-04-01.

References

1. Zang, Y., Street R. L. and Koseff, J. R.: A Dynamic Mixed Subgrid-scale Model and its Application to Turbulent Recirculating Flows, *Phys. Fluids*, A 5, vol. 12 (1993) 3186-3196.
2. Germano, M. , Piomelli, U., Moin P. and Cabot W. H.: A Dynamic Subgrid-scale Eddy Viscosity Model, *Phys. Fluids*, A 3, vol. 7 (1991) 1760-1765.
3. Calmet, I. and Magnaudet, J.: Large Eddy Simulation of High Schmidt Number Mass Transfer in a Turbulent Channel, *Phys. Fluids* 9, vol. 2 (1997) 438-455.
4. Lee, G. and Na, Y.: On the Large Eddy Simulation of Temperature Field Using Dynamic Mixed Model in a Turbulent Channel, *Trans. KSME B*, Vol. 28, No. 10, (2004) 1255-1263.

High-End Modeling and Simulation of Cookoff of HMX-Based Energetic Materials

Jack Jai-ick Yoh

School of Mechanical and Aerospace Engineering,
Seoul National University,
Seoul, 151-742, Korea
jjyoh@snu.ac.kr

Abstract. We present a simple idea to simulate dynamic fracture and fragmentation of a propulsion system exposed to an extreme condition, such as a fire. The system consists of energetic materials confined in a steel cylinder. The strain failure model of the confinement is a modified Johnson-Cook model with a statistical failure distribution. By using the size distribution data of the fragments from the thermal explosion tests, the failure strain distribution can be empirically obtained and then entered into the model. The simulated fracture and fragment sizes are compared with the experimental records.

1 Introduction

In the energetic materials community, there is an interest in using computer simulations to reduce the number of experiments for weapons design and safety evaluation. Models and numerical strategies are being developed for the heating of energetic materials until reaction (cookoff). Munitions exposed to a fire are of great concern. In this case, time scales for behaviour can range from days to microseconds. During the relatively slow heating phase, the response of an energetic materials system is paced by thermal diffusion and chemical decomposition, while the mechanical response is essentially a quasi-static process. As the decomposition reactions accelerate, heat is generated faster than it can diffuse. Product gases are formed and the resulting pressure rises accelerate the energetic and containment material response. The resulting thermal explosion can range in violence from a pressure rupture to a detonation.

A number of investigators have modeled slow cookoff experiments. Chidester *et al.* [1] calculated explosion times for HMX- and TATB-based explosives subjected to varying confinement and thermal environments. Tarver and Tran [2] improved thermal decomposition models for HMX-based plastic bonded explosives and attained reasonable predictions for ignition time using the thermal-chemical code, Chemical TOPAZ. These thermo-chemical models were expanded to include hydro effects, and the earlier models were evaluated against small-scale tests. It was recognized that the models required further development and needed to be benchmarked against well-instrumented cookoff experiments. More recent modeling efforts have focused on wall strain rates as a measure of cookoff violence.

In the modeling work of this study, the process of cookoff is not separated into two regimes. Instead, a single calculation is performed for the heating, ignition, and explosive phases of cookoff. Coupled thermal, mechanical, and chemical models are used during all of these stages to account for effects such as chemical decomposition, burning, thermal expansion, and the closing of gaps. It is seen that the modeling of thermal explosions requires computational tools and models that can handle a wide variety of physical processes and time scales.

We consider the explosive LX-10 which has an HMX base [3]. The LX-10 has a nominal composition of 95% HMX and 5% Viton by weight.

In this paper, we investigate the response of confined HMX-based materials in our Scaled Thermal Explosion Experiment (STEX). The focus is placed on the simulating of fracture and fragmentation of the confinement material, namely AerMet 100 steel. Efforts are made to compare the measured fragment sizes of explosively driven steel pipe. A numerical approach involving variable mass-scaling allows the calculation of coupled thermo-chemical-mechanical results over the widely varying time scales associated with the heating and explosive processes.

2 Experiment

In order to provide a database to test models, the STEX is designed to quantify the violence of thermal explosions under carefully controlled conditions [4]. The cylindrical test, shown in Fig. 1, is designed to provide ignition in the central region of the cylinder. The confinement vessel consists of AerMet 100 with heavily reinforced end caps which confine the decomposition gases until the tube wall fails. A length to diameter ratio of 4:1 is used for which the ID is 4.49 cm and the interior length is 20.3 cm. The wall thickness is 0.3 cm for LX-10, giving an approximate confinement pressure of 200 MPa. Ullage (air space) was included to allow for expansion of the HE without bursting the vessel prior to ignition. The total ullage that is present in the vessel was 8.66% for LX-10.

A feedback control system is used to adjust three radiant heaters to control the wall temperature at location no. 1 of Fig. 1(b). The thermocouples at location nos. 2 and 3

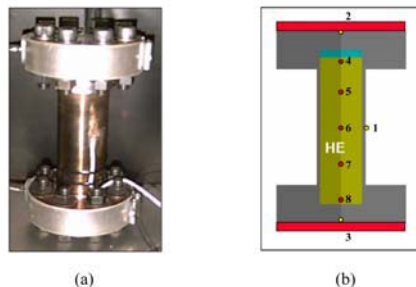


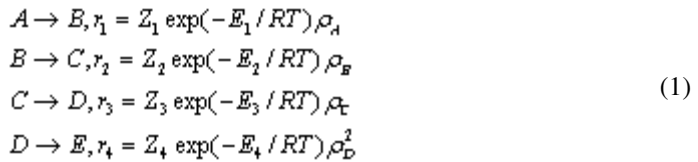
Fig. 1. (a) Photograph of the STEX vessel. (b) Schematic of the model domain.

on the end caps are controlled with separate control loops. The wall thermocouple temperature is increased at 1 C/h until explosion. The lower and upper thermocouples are maintained at 4 and 9 C, respectively, below the wall temperature to provide for ignition near a plane half way between the two end caps. A probe with 5 thermocouples is used to monitor the internal temperature of the HE (see Fig. 1(b)). Two hoop strain gauges were used to measure the radial expansion of the tube at the axial mid-plane.

3 Models

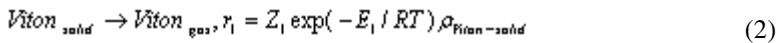
3.1 Chemical model

The four-step, five-species reaction mechanism for HMX is



where *A* and *B* are solid species (β and δ phase HMX), *C* is solid intermediate, *D* and *E* are intermediate and final product gases, respectively. Here r_i is the mass reaction rate, Z_i is the frequency factor, and E_i is the activation energy for reaction *i*. Also ρ_j the mass concentration for species $j = A, B, C, D, E$.

The mechanism for Viton is a single-step, endothermic reaction:



The rate parameters in the above mechanisms for LX-10 are adjusted to fit One-Dimensional-Time-to-Explosion (ODTX) measurements. The values are given in [5].

After the chemical reactions have progressed significantly into the faster regime of cookoff in which changes are occurring on the time scale of the sound speed, a switch is made to a burn front model in which reactants are converted completely to products in a single reaction step. The burn front velocity, *V* is assumed to be a pressure-dependent function, and it takes the form, where *V* is in mm/s and *P* is in MPa.

This change in models is made for several reasons. First the Arrhenius models described above may not apply at the elevated temperatures and pressures of the burn process. The burn rate model is more useful since it can employ measured burn rates as described below. Finally, the computational effort required for the Arrhenius model is prohibitively large as a result of the fine mesh spacing and small time steps required to model the narrow burn front. In contrast, solutions for the burn rate model can be obtained with practical amounts of computation time.

3.2 Thermal Model

The time-dependent thermal transport model includes the effects of conduction, reaction, convection, and compression. The constant-volume heat capacity is constant for each reactant. The thermal conductivities of the solid species A, B and C are taken to be constant, whereas the effects of temperature are included for the gaseous species. The thermal properties for materials A, B and C are reported in [5] and use available measured values for LX-10. The heat capacity, c_v , for gases D and E is assigned the same constant-volume value used in the gamma-law model. The temperature-dependent thermal conductivity is estimated at 1 kbar and $T = 2000$ C using Bridgmann's equation [6] for liquids in which the sound velocity is calculated using results from Cheetah [7].

As for the mechanical model, the discussion is quite involved and the readers are referred to the Refs. [8,9].

3.3 A Modified Johnson-Cook Failure Model for AerMet 100

Simulations of an explosively-driven, steel cylinder were performed using the Johnson-Cook Failure Strain (JCFS) Model. The effects of the heterogeneous microstructure were considered by incorporating Gaussian (spatial) distributions of the JCFS parameters (D_1 in Eqn. 2). The parameters used in the model are listed in Table 1. Fragmenting material motion was considered to be Lagrangian throughout the simulation. The idea is that the failure strain could not be constant in a material else it would fail simultaneously over a dynamically loaded body with infinitesimally small fragments [11].

$$D = \sum \frac{\Delta \epsilon}{\Delta \epsilon_j} \quad (3)$$

$$\epsilon_j = D_1 + D_2 \exp D_3 \frac{-P}{\sigma_y} \quad (4)$$

4 Results

One-dimensional results are not discussed here and the readers are referred to Ref. [5,8,9,10]. Two dimensional simulations are performed for the STEX system LX-10. This system is assumed to be axisymmetric, and a cylindrical wedge was selected for the calculation domain. In Fig. 2, calculated temperatures of the STEX system are plotted versus time, along with measured curves. The measured and calculated temperatures are shown at an internal location (no. 6 in Fig. 1(b)) and the control location (no. 1 in Fig. 1(b)). The predicted and measured internal temperature curves are in good agreement for LX-10, and the predicted explosion temperature (TC no. 1) of 182 C agrees very well with the experimental value of 181.5 C.

Studies were conducted to assess the accuracy of the calculations and the reproducibility of the measurements. The model simulations were repeated with the refined meshes and are numerically accurate to less than a degree. Thus, the model results are numerically accurate and the measurements seem to be reproducible.

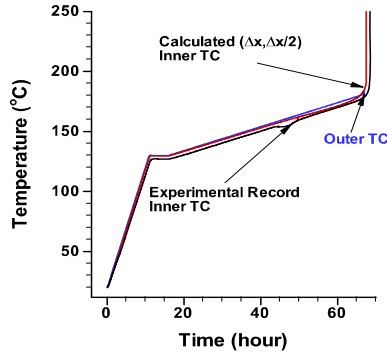


Fig. 2. Prediction of thermal response of confined LX-10

In Figs. 3, calculated vessel wall hoop strain for the STEX system is shown with the measurement over the duration of the tests. The results confirm the accuracy of the hoop strain measurements and the Gruneisen EOS for AerMet 100. Near the ignition point, decomposition gases pressurize the vessel, and measured strains are greater than the empty-vessel results.

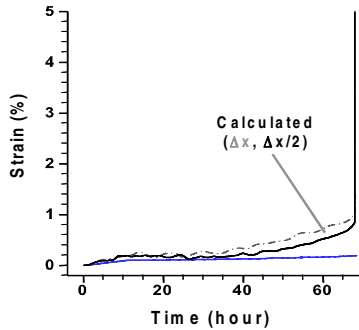


Fig. 3. Experimental and calculated hoop strain records from the slow heating to the thermal runaway phase for LX-10

Figure 4 shows retrieved fragments from the actual STEX run of LX-10. The size distribution varies on the orders of several centimeters. Figure 5 shows three-dimensional numerical simulation of the same system. A distinct fracture pattern is observed and also the size of the unfailed zones (i.e. fragments) is on the order of 1-2 centimeters.



Fig. 4. Retrieved fragments from explosively driven AerMet 100 pipe

Table 1. Parameters used in the current fracture model of AerMet 100 steel

Johnson-Cook Failure Coefficients	
D_1	0.1 +/- 20% standard deviation
D_2	0.156 (Chabildas <i>et al.</i> , 2001)
D_3	0.296 (Chabildas <i>et al.</i> , 2001)

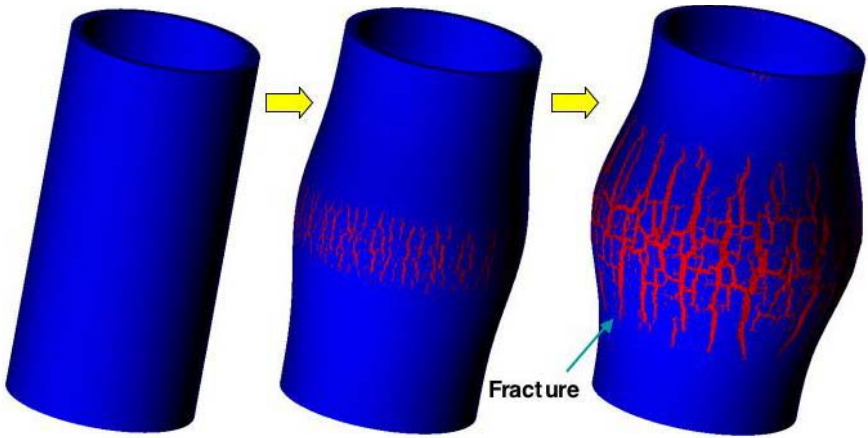


Fig. 5. Crack initiation on outer layer of AerMet 100 steel pipe, loaded at center by HMX spherical deflagration

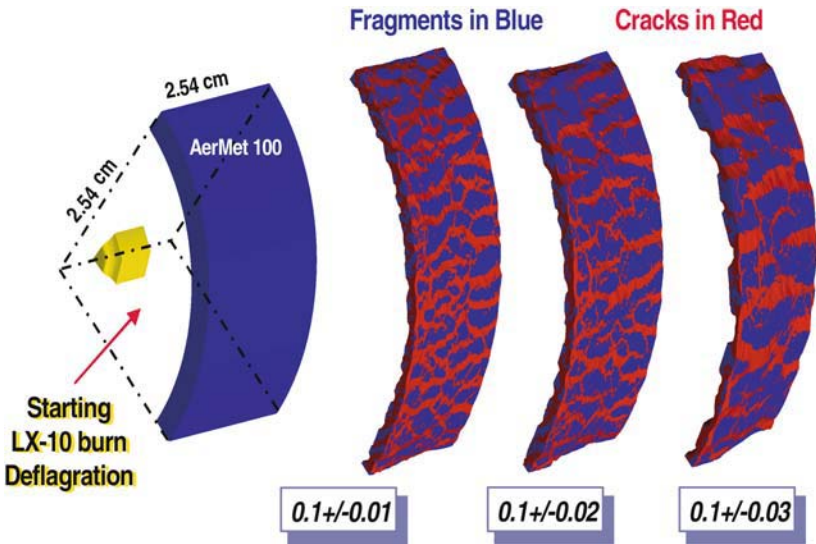


Fig. 6. Variation of D_1 parameter affecting the fragment size of metal pipe

To understand the mechanism of present JCFM, we modified and varied D_1 parameter. The percent deviation of an assumed Gaussian distribution of the parameter is varied from 10, 20, and 30% as shown in Fig. 6. As the width of the bell-shaped distribution increases, the size of the crack (in red) in the simulation increases also. The unfailed zones which we identify as fragments are larger, and their presence is less frequent with increasing distribution width.

5 Conclusions

A numerical investigation was performed to validate the experimental results for the thermally-induced explosion of the HMX-based explosive, LX-10. A particular interest is placed on the modeling of fracture and fragmentation of the AerMet 100 containment of LX-10, upon thermal explosion. A continued effort is needed to build a tool that can confidently address the fragmentation and also the violence of a thermal explosion system.

References

1. Chidester, S. K., Tarver, C. M., Green, L. G., and Urtiew, P. A., "On the Violence of Thermal Explosion in Solid Explosives," *Combustion and Flame*, 110, pp. 264-280, 1997.
2. Tarver, C. M., and Tran, T. D., Thermal Decomposition Models for HMX-based Plastic Bonded Explosives, *Combustion and Flame*, 137, pp50-62, 2004.
3. Meyer, R., Kohler, J., and Homburg, A, *Explosives*, Wiley-VCH, New York, 1993.
4. Wardell, J. F., and Maienschein, J. L., The Scaled Thermal Explosion Experiment, in Proceedings of 12th International Detonation Symposium, San Diego, CA, Office of Naval Research, 2002.
5. Yoh, J. J., McClelland, M. A., Nichols, A. L., Maienschein, J. L., and Tarver, C. M., Simulating Thermal Explosion of HMX-based Explosives: Model Comparison with Experiment, Lawrence Livermore National Laboratory, Technical Report, LLNL-JRNL-210733
6. Holman, J. P., *Heat Transfer*, McGraw-Hill, 1976, pp. 253-254.
7. Fried, L. E., and Howard, W. M., *Cheetah 3.0 Users Manual*, Lawrence Livermore National Laboratory, Livermore, CA, UCRL-MA-117541, 2001
8. Yoh, J. J., McClelland, M. A., Maienschein, J. L. Wardell, J. F., and Tarver, C. M., Simulating Thermal Explosion of RDX-based Explosives: Model Comparison with Experiment, *Journal of Applied Physics*, 97, 8, 2005
9. Yoh, J. J. McClelland, M. A. Maienschein, and J. L. Wardell, "Towards a Predictive Thermal Explosion Model for Energetic Materials," *Journal of Computer-Aided Materials Design*, 10, pp. 175-189, 2005.
10. Yoh, J. J. "Prediction of Thermal Explosion Response of Energetic Materials," Proceedings of the KSAS Spring Conference, 2005, pp.521-524
11. Mott, N. F., *Proc. Roy. Soc. London, Series A*, 189, pp. 300-308, 1947

Multiobjective Optimization Using Adjoint Gradient Enhanced Approximation Models for Genetic Algorithms

Sangho Kim¹ and Hyoung-Seog Chung²

¹ Agency for Defense Development, Yuseong Daejeon, Republic of Korea

² Republic of Korea Air Force Academy, Chungjoo, Republic of Korea

Abstract. In this work, a multiobjective design optimization framework is developed by combining GAs and an approximation technique called Kriging method which can produce fairly accurate global approximations to the actual design space to provide the function evaluations efficiently. It is applied to a wing planform design problem and its results demonstrate the efficiency and applicability of the proposed design framework. Furthermore, to improve the efficiency of the proposed method using adjoint gradients two different approaches are tested. The results show that the adjoint gradient can efficiently replace computationally expensive sample data needed for constructing the Kriging models, and that the adjoint gradient-based optimization techniques can be utilized to refine the design candidates obtained through the approximation model based genetic algorithms.

1 Introduction

The conceptual and preliminary phases of the design of aerospace systems involve searching for either improved or optimal combinations of design variables within large design spaces. Because of the nonlinearities and complex interactions among the design variables and disciplines, realistic high-dimensional multidisciplinary design optimization(MDO) problems are more likely to have multimodal search spaces than single discipline design problems. Typical MDO problems are also multiobjective in nature. Unlike single-objective optimization, multiobjective optimization may result in a set of optimal solutions which represent the trade-off surface between the conflicting criteria. These non-dominated solution points are called Pareto optimal solutions. Once the set of optimal solutions is identified, the designer has the freedom of choosing one solution out of many possible alternatives based on experience, prior knowledge and other criteria or constraints particular to the current design problem. The traditional optimization methods used for single objective optimization has the shortcomings of identifying such Pareto solutions, which result in the need for better global and multiobjective optimization frameworks to fully realize the benefits of conducting MDO.

Genetic Algorithms(GAs), pioneered by John Holland, have recently been gaining much attention as a popular choice for various real-world engineering

problems largely due to their robustness and simplicity. GAs have many advantages that make them suitable for MDO. Because they operate with a population of possible solutions rather than a single candidate, they are less likely to get stuck in a false local minima. Furthermore, a number of Pareto optimal solutions may be captured during one run of GA. They are relatively simple and easy to use and don't require any auxiliary information such as gradients other than the evaluation of the (possibly) multiple objective functions. These merits make GAs very appealing as more reasonable candidate optimization tools for MDO. [1]

One of the biggest drawbacks of GAs, however, is that they require hundreds, if not thousands, of function evaluations to achieve a reasonable improvement within the design space. Thus, the robustness of the method comes with the price of low computational efficiency; therefore, their use is often infeasible for high-fidelity models since the cost of carrying out the necessary function evaluations can be exorbitantly high. The efficiency of GAs has to be improved in some way before they can be truly used in high-fidelity MDO. Given prior work with computationally inexpensive and efficient approximation techniques such as Kriging method, which can produce fairly accurate global approximations to the actual design space, the combination of GAs with these approximation models becomes an obvious approach to overcome the problems of GAs mentioned above. Since the computational cost to estimate the objective function once the approximation model is constructed is almost trivial, the slow convergence rate and the large computational burden to obtain many function evaluations for GA methods are not significant any more.

The Kriging technique has been recognized as an alternative to the traditional Response Surface method in generating approximation models for global and multidimensional optimization. This is due to its abilities to interpolate sample data and to model a function with multiple local extrema. To fully exploit the advantage of the Kriging method, however, a large number of sample data points should be spread out to fill the design space. This can be very costly and even impractical in high-dimensional design optimization using high-fidelity analysis codes. The cost of constructing a Kriging model can be greatly reduced by incorporating secondary information such as values.

The focus of CFD applications has shifted to aerodynamic design since the introduction of control theory to Aerodynamic Shape Optimization(ASO) in transonic flow by Jameson [2, 3] in 1989. This control theory approach is often called the adjoint method, since the necessary gradients are obtained via the solution of the adjoint equations of the governing equations of interest. The adjoint method is extremely efficient since the computational expense incurred in the calculation of the complete gradient is effectively independent of the number of design variables. In fact this method has become a popular choice for design problems involving fluid flow and has been successfully used for the aerodynamic design of complete aircraft configurations [4, 5, 6, 7].

In this work, our intention is to investigate the efficiency and suitability of replacing computationally expensive sample data with the cheaply obtained

gradients through the adjoint method when constructing the Kriging model to be used in multiobjective genetic algorithms. For this purpose, we have chosen the wing planform design problem of Boeing 747 configuration to improve both aerodynamic and structural performances. Another approach of using the adjoint and Kriging methods to improve the overall design process is also proposed and tested, in which the automatic design procedure that uses Computational Fluid Dynamics(CFD) combined with the adjoint gradient-based optimization techniques is utilized to refine the design candidates obtained through the approximation model based genetic algorithms.

2 Implementation

2.1 Overview of Kriging Method

The Kriging technique uses a two component model that can be expressed mathematically as

$$y(\mathbf{x}) = \mathbf{f}(\mathbf{x}) + \mathbf{Z}(\mathbf{x}), \quad (1)$$

where $f(\mathbf{x})$ represents a global model and $Z(\mathbf{x})$ is the realization of a stationary Gaussian random function that creates a localized deviation from the global model [8]. If $f(x)$ is taken to be an underlying constant [9], β , Equation (1) becomes

$$y(\mathbf{x}) = \beta + \mathbf{Z}(\mathbf{x}), \quad (2)$$

which is used in this paper. The estimated model of Equation (2) is given as

$$\hat{y} = \hat{\beta} + \mathbf{r}^T(\mathbf{x})\mathbf{R}^{-1}(\mathbf{y} - \mathbf{f}\hat{\beta}), \quad (3)$$

where \mathbf{y} is the column vector of response data and \mathbf{f} is a column vector of length n_s which is filled with ones. \mathbf{R} in Equation (3) is the correlation matrix which can be obtained by computing $R(\mathbf{x}^i, \mathbf{x}^j)$, the correlation function between any two sampled data points. This correlation function is specified by the user. In this work, the authors use a Gaussian exponential correlation function of the form provided by Giunta, et al. [10]

$$R(\mathbf{x}^i, \mathbf{x}^j) = \exp \left[- \sum_{\mathbf{k}=1}^n \theta_{\mathbf{k}} |\mathbf{x}_{\mathbf{k}}^i - \mathbf{x}_{\mathbf{k}}^j|^2 \right]. \quad (4)$$

The correlation vector between \mathbf{x} and the sampled data points is expressed as

$$\mathbf{r}^T(\mathbf{x}) = [\mathbf{R}(\mathbf{x}, \mathbf{x}^1), \mathbf{R}(\mathbf{x}, \mathbf{x}^2), \dots, \mathbf{R}(\mathbf{x}, \mathbf{x}^n)]^T. \quad (5)$$

The value for $\hat{\beta}$ is estimated using the generalized least squares method as

$$\hat{\beta} = (\mathbf{f}^T \mathbf{R}^{-1} \mathbf{f})^{-1} \mathbf{f}^T \mathbf{R}^{-1} \mathbf{y}. \quad (6)$$

Since \mathbf{R} is a function of the unknown variable θ , $\hat{\beta}$ is also a function of θ . Once θ is obtained, Equation (3) is completely defined. The value of θ is obtained by maximizing the following function over the interval $\theta > \mathbf{0}$

$$-\frac{[n_s \ln(\hat{\sigma}^2) + \ln |\mathbf{R}|]}{2}, \quad (7)$$

where

$$\hat{\sigma}^2 = \frac{(\mathbf{y} - \mathbf{f}\hat{\beta})^T \mathbf{R}^{-1} (\mathbf{y} - \mathbf{f}\hat{\beta})}{n_s}. \quad (8)$$

In order to construct a Kriging approximation the only data required are the function values at a number of pre-specified sample locations. For many computational methods, secondary information such as gradient values may be available as a result of the analysis procedure. Alternatively, the gradient vector can be computed with very little additional cost, as is the case in the adjoint method [11]. Gradient information is usually well cross-correlated with the function values and thus contains useful additional information. The efficiency and accuracy of Kriging models can be greatly improved by incorporating these secondary function values [12].

2.2 Multiobjective Genetic Algorithms

Unlike single-objective optimization where only one optimal solution is pursued, a typical multiobjective optimization problem produces a set of solutions which are superior to the rest of the solutions with respect to all objective criteria but are inferior to other solutions in one or more objectives. These solutions are known as Pareto optimal solutions or nondominated solutions. A genetic algorithm can use the above defined dominance criteria in a straightforward fashion, to drive the search process toward the Pareto front. Due to the unique feature of GAs, which work with a population of solutions, multiple Pareto optimal solutions can be captured in a single simulation run. This is the primary reason that makes GAs highly suitable to be used in multiobjective optimization.

A recent study by Coello[13] proposed a micro-GA based multiobjective optimization utilizing an external file to store nondominated vectors found in previous generations to accelerate the multiobjective optimization procedure. The method implemented additional elitism strategy and adaptive grid-type technique to accelerate the convergence and to keep the diversity in Pareto front. Micro-GAs is a specialized GA that works with a very small population size of usually 3-6 and a reinitialization process. The previous studies showed that micro-GAs achieved a faster convergence rate than simple GAs. In the present research, some of the ideas of Coello's work were adopted to a single objective micro-GA along with the traditional Goldberg's Pareto ranking approach in order to develop an efficient and robust design framework. The authors modified a micro-GA originally developed by Carroll [14] from CU Aerospace for that purpose.

Once fairly accurate global approximation models are constructed with computationally efficient techniques such as the Kriging method, combining them

with GAs becomes an obvious choice to overcome the computational burden presented by GAs. Since the computational cost of estimating the objective function through the approximation models is trivial, the slow convergence rate of GAs leading to many generations and function evaluations to get to the optimal solution would not matter any more.

2.3 Aerodynamic Shape Optimization

In order to find optimum aerodynamic shapes with reasonable computational costs, it is useful to regard the wing as a device which controls the flow in order to produce lift with minimum drag. An acceptable aerodynamic design must have characteristics that smoothly vary with small changes in shape and flow conditions. Consequently, gradient-based procedures are appropriate for aerodynamic shape optimization. One of the main issues affect the efficiency of gradient-based procedures is the actual calculation of the gradient.

A cost effective technique is to compute the gradient through the solution of an adjoint problem, such as that developed in references [2, 3]. The essential idea may be summarized as follows. For flow about an arbitrary body, the aerodynamic properties that define the cost function I are functions of the flowfield variables (w) and the physical shape of the body, which may be represented by the function \mathcal{F} . Then

$$I = I(w, \mathcal{F})$$

and a change in \mathcal{F} results in a change of the cost function

$$\delta I = \frac{\partial I^T}{\partial w} \delta w + \frac{\partial I^T}{\partial \mathcal{F}} \delta \mathcal{F}.$$

Using a technique drawn from control theory, the governing equations of the flowfield are introduced as a constraint in such a way that the final expression for the gradient does not require reevaluation of the flowfield. In order to achieve this, δw must be eliminated from the above equation. Suppose that the governing equation R , which expresses the dependence of w and \mathcal{F} within the flowfield domain D , can be written as

$$R(w, \mathcal{F}) = 0. \quad (9)$$

Then δw is determined from the equation

$$\delta R = \left[\frac{\partial R}{\partial w} \right] \delta w + \left[\frac{\partial R}{\partial \mathcal{F}} \right] \delta \mathcal{F} = 0.$$

Next, introducing a Lagrange multiplier ψ , we have

$$\delta I = \frac{\partial I^T}{\partial w} \delta w + \frac{\partial I^T}{\partial \mathcal{F}} \delta \mathcal{F} - \psi^T \left(\left[\frac{\partial R}{\partial w} \right] \delta w + \left[\frac{\partial R}{\partial \mathcal{F}} \right] \delta \mathcal{F} \right). \quad (10)$$

With some rearrangement

$$\delta I = \left(\frac{\partial I^T}{\partial w} - \psi^T \left[\frac{\partial R}{\partial w} \right] \right) \delta w + \left(\frac{\partial I^T}{\partial \mathcal{F}} - \psi^T \left[\frac{\partial R}{\partial \mathcal{F}} \right] \right) \delta \mathcal{F}.$$

Choosing ψ to satisfy the adjoint equation

$$\left[\frac{\partial R}{\partial w} \right]^T \psi = \frac{\partial I^T}{\partial w} \quad (11)$$

the term multiplying δw can be eliminated in the variation of the cost function, and we find that

$$\delta I = \mathcal{G} \delta \mathcal{F},$$

where

$$\mathcal{G} = \frac{\partial I^T}{\partial \mathcal{F}} - \psi^T \left[\frac{\partial R}{\partial \mathcal{F}} \right].$$

The advantage is that the variation in cost function is independent of δw , with the result that the gradient of I with respect to any number of design variables can be determined without the need for additional flow-field evaluations.

In the case that the flow governing equation is a partial differential equation, the adjoint equation is also a partial differential equation and appropriate boundary conditions must be determined. It turns out that the appropriate boundary conditions depend on the choice of the cost function, and may easily be derived for cost functions that involve surface-pressure integrations. Cost functions involving field integrals lead to the appearance of a source term in the adjoint equation.

The cost of solving the adjoint equation is comparable to that of solving the flow equation. Hence, the cost of obtaining the gradient is comparable to the cost of two function evaluations, regardless of the dimension of the design space.

The formulation of control theory to aerodynamic design problems using the compressible Euler and Navier-Stokes equations as the mathematical model has been fully illustrated in the author's previous works [15, 16].

2.4 Planform Optimization

The shape changes in the wing section needed in order to improve the transonic wing design are quite small. However, in order to obtain a true optimum design, larger scale changes such as changes in the wing planform (sweepback, span, chord, section thickness, and taper) should be considered. Because these directly affect the structural weight, a meaningful result can only be obtained by considering a cost function that accounts for both the aerodynamic characteristics and the weight.

Following the previous works by Leoviriyakit, [17, 18] we redesign both wing section and planform to minimize a cost function including both drag and structural weight terms of the form:

$$I = \alpha_1 C_D + \alpha_2 C_W, \quad (12)$$

where C_W is a dimensionless measure of the wing weight, which can be estimated either from a statistical formula or from a simple analysis of a representative structure, allowing for failure modes such as panel buckling. To estimate the

wing weight, a realistic model should account for both planform geometry and wing loading, but it should be simplified enough that we can express it as an analytical function. An analytical model to estimate the minimal material to resist material and buckling failures has been developed by Wakayama [19]. When shear and buckling effects are small, they may be neglected, resulting in a simplified model developed by Kroo [20]. In his work the wing structure is modeled by a structure box, whose major structural material is the box skin. The skin thickness varies along the span and resists the bending moment caused by the wing lift. Then, the structural wing weight can be calculated based on material of the skin. We follow the analysis developed by Kroo for the present work. Readers can find the detailed description of the wing structure model and the necessary formulation of the adjoint boundary condition using this model in one of the author's previous paper [17].

The wing section is modeled by surface mesh points, and the wing planform is modeled by the design variables shown in figure 1 as root chord (c_1), mid-span chord (c_2), tip chord (c_3), span (b), sweepback (Λ), and wing thickness ratio (t).

The gradient with respect to planform variation can be computed by integrating point-gradients projected in the planform movement direction. In fact, using this planform-gradient information, it has been shown that both drag and structural weight can be improved simultaneously with the use of the steepest descent method [18].

2.5 Flow Solver and Adjoint Solver

The flow solver and the adjoint solver chosen in this work are codes developed by Jameson et al [21, 22, 23]. The flow solver solves the three dimensional Euler equations by employing the JST scheme, together with a multistage explicit time stepping scheme. Rapid convergence to a steady state is achieved via variable local time steps, residual averaging, and a full approximation multi-grid scheme. The adjoint solver uses the similar techniques. In fact much of the software is shared by the flow and adjoint solvers.

3 Results

3.1 Validation of Adjoint Method for Wing Shape and Planform Optimization

Planform-Gradient Accuracy. To verify the accuracy of the aerodynamic and structural gradients with respect to planform variables calculated by the adjoint method, the comparison of the adjoint gradients with the finite-difference

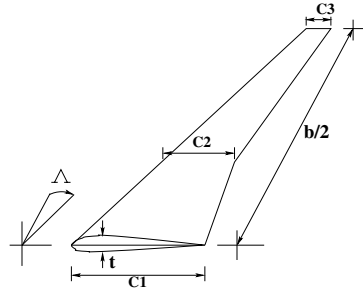


Fig. 1. Simplified wing planform of a transport aircraft

gradients has been performed and presented by Leoviriyakit [18] The case chosen was the Boeing 747 wing fuselage combination at normal cruising Mach 0.85 and a fixed lift coefficient $C_L = 0.45$.

Boeing 747 Wing-Body Configuration Wing Redesign. As a reference point, we first modified only the wing sections to eliminate the shock drag, while the planform of the baseline Boeing 747 was kept unchanged. The total cost function, $I = C_D + 0.07C_W$ has reduced from 0.01435 to 0.01324. The total wing drag was successfully reduced from $C_D = 0.01090$ to $C_D = 0.00985$ and C_W was slightly reduced from 0.0494 to 0.0485.

Boeing 747 Wing Planform Optimization. Boeing 747 Wing Planform Optimization has been performed while the wing sections has also been modified. The total cost function, $I = C_D + 0.07C_W$ has reduced from 0.01435 to 0.01228 in 15 design iteration. This results show that the additional reduction was achieved by including the wing planform optimization in this design.

3.2 Kriging Model-Based Multiobjective Genetic Algorithms(MOGA)

One design cycle of the Kriging-based MOGA were performed. Using a latin hypercube sampling(LHS) technique[24, 25, 26], 29 sample points around the baseline design were selected and the values of their design objectives were assigned by a CFD code. The sample data points are plotted as green asterisks and the baseline design point is shown as a blue star in Figure 2. The locations of sample data points form a Pareto-like distribution. This implies that the baseline design is already close to the optimal Pareto front. This also means that only a small amount of improvement in objective functions values is expected to be achieved. Kriging model was then generated based

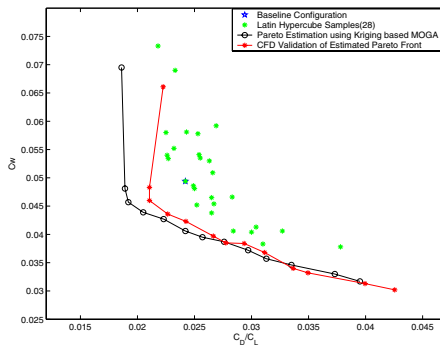


Fig. 2. One design cycle of the Kriging-based MOGA

on the sample data and used for both function evaluations in the MOGA search. The estimated components of the Pareto set from the Kriging-based MOGA search procedure are plotted as black circles whereas the CFD validation results of the Pareto set are shown as red asterisks in the figure. The objective values of the estimated Pareto set from the Kriging-based MOGA and their CFD validation calculations were fairly well matched while some of the values of the drag estimations had discrepancies with their CFD counterparts especially at the lower range of C_D value. We can infer that this discrepancy was resulted

from the lack of sample data points since only 28 samples were used to generate the Kriging model. The accuracy is expected to be improved as more sample points are included. The estimation has produced a number of good design candidates which were all better than the 28 sample points and baseline design. This figure validates the efficiency and accuracy of the Kriging-based MOGA design framework.

The same procedure was repeated to check the applicability of adjoint gradient implementation for generatig Kriging models. At this time, only 12 sample data were used to construct the Kriging model with the supplements of adjoint gradient information at each sample point (total 78 gradients). As shown in Figure 3 the Kriging-based MOGA estimation resulted in a large amount of over-estimation for C_D values; however, the C_W estimations were relatively well matched with the CFD validation data. In addition, the CFD validation results for the gradient enhanced Kriging model case were very close those for the original Kriging model case shown in Figure 2. As the design cycle iterates, the error can be minimized since the trust region of design space also reduces. This result indicate that using adjoint gradient for Kriging model is a valid alternative to improve the efficiency of design process.

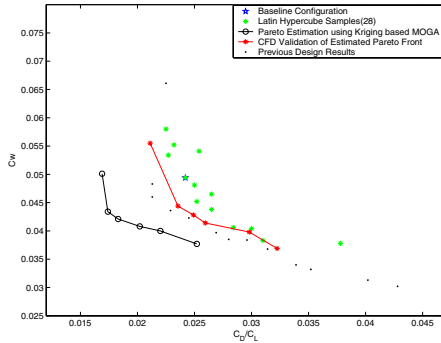


Fig. 3. One design cycle of the Kriging-based MOGA using Adjoint

3.3 Design Refinement Using Adjoint Method

In this design example, the second approach of using the adjoint method to enhance the approximation model-based GAs has been tested. One of the designed configurations provided by GAs was selected as a new base configuration and then the adjoint shape optimization method refined the configuration. Fig. 4 shows the refinement result after 20 design iterations. The total cost function has reduced from 0.01378 (I of the new base configuration) to 0.01211.

4 Conclusions

The applicability and efficiency of using approximation model-based GAs for multiobjective optimization has been demonstrated. A new hybridization strategy implementing adjoint gradient information for the Kriging model construction was proposed and its advantage to reduce the computational cost to collect the required sample data for Kriging model has been validated using a preliminary test case. Another approach of using the adjoint and Kriging methods

Mach: 0.850 Alpha: 2.118
 CL: 0.450 CD: 0.00889 CM:-0.0692 CW: 0.0460
 Design: 20 Residual: 0.9458E-02
 Grid: 193X 33X 33
 Sweep: 36.0789 Span(ft): 206.02
 C1(ft): 52.74 C2: 32.00 C3: 11.93
 I: 0.01211

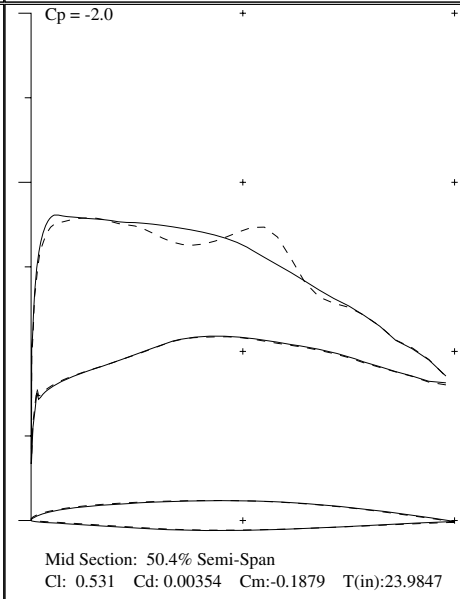
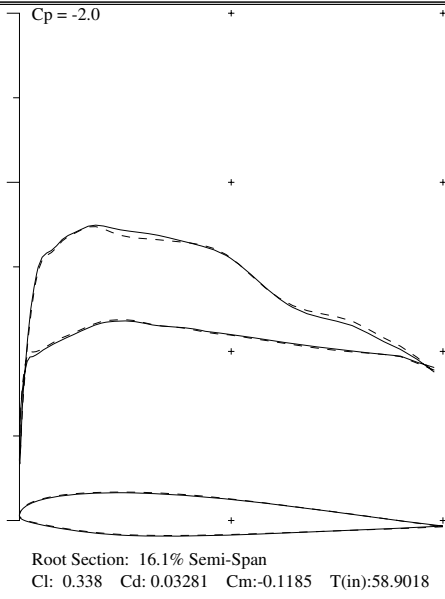
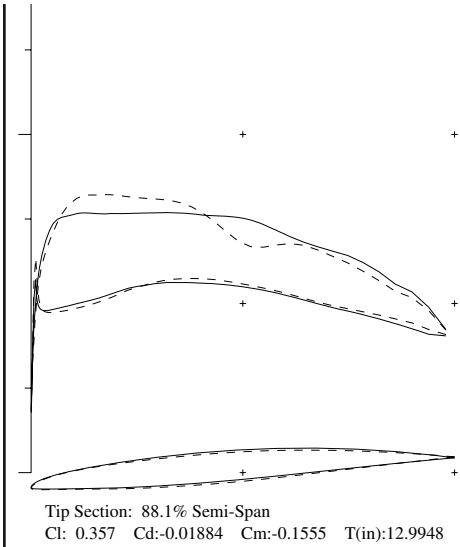
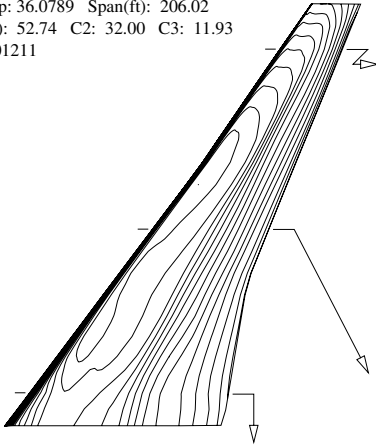


Fig. 4. Solution after 20 adjoint design iterations, Euler drag and wing weight minimization at fixed $C_L = 0.45$, Boeing 747 wing and planform refinement design. Initial C_p : - - -, Redesigned C_p : ——— .

to improve the overall design process is also proposed and tested, in which the adjoint gradient-based optimization techniques is utilized to refine the design candidates obtained through the approximation model based genetic algorithms.

Acknowledgment

Our special thanks go to Professor Antony Jameson, Professor Juan J. Alonso, and Dr. Kasidit Leoviriyakit for their support in the present work.

References

1. Kalyanmoy Deb. An introduction to genetic algorithms. , *SADHANA*, Kanpu Genetic Algorithms Laboratory, Kanpur, India, 1999.
2. A. Jameson. Aerodynamic design via control theory. *Journal of Scientific Computing*, 3:233–260, September 1989.
3. A. Jameson. Optimum aerodynamic design using CFD and control theory. *AIAA paper 95-1729*, AIAA 12th Computational Fluid Dynamics Conference, San Diego, CA, June 1995.
4. J. Reuther, J. J. Alonso, J. C. Vassberg, A. Jameson, and L. Martinelli. An efficient multiblock method for aerodynamic analysis and design on distributed memory systems. *AIAA paper 97-1893*, June 1997.
5. J. Reuther, J.J. Alonso, M.J. Rimlinger, and A. Jameson. Aerodynamic shape optimization of supersonic aircraft configurations via an adjoint formulation on parallel computers. *AIAA paper 96-4045*, 6th AIAA/NASA/ISSMO Symposium on Multidisciplinary Analysis and Optimization, Bellevue, WA, September 1996.
6. O. Baysal and M. E. Eleshaky. Aerodynamic design optimization using sensitivity analysis and computational fluid dynamics. *AIAA paper 91-0471*, 29th Aerospace Sciences Meeting, Reno, Nevada, January 1991.
7. W. K. Anderson and V. Venkatakrishnan. Aerodynamic design optimization on unstructured grids with a continuous adjoint formulation. *AIAA paper 97-0643*, 35th Aerospace Sciences Meeting and Exhibit, Reno, Nevada, January 1997.
8. J. R. Koehler and A. B. Owen. Computer experiments. *Handbook of Statistics, SADHANA*, Kanpu Genetic Algorithms Laboratory, Elsevier Science, New York, 1999.
9. John J. Korte Timothy W. Simpson, Timothy M. Mauery and Farrokh Mistree. Comparison of response surface and kriging models in the multidisciplinary design of an aerospike nozzle. *AIAA paper 98-4755*, 7th AIAA/USAF/NASA/ISSMO Symposium on Multidisciplinary Analysis and Optimization, St. Louis, Missouri, September 1998.
10. A. A. Giunta and L. T. Watson. A comparison of approximation modeling techniques: Polynomial versus interpolating models. *AIAA paper 98-4758*, 7th AIAA/NASA/ISSMO Symposium on Multidisciplinary Analysis and Optimization, St. Louis, MO, September 1998.
11. J. J. Alonso J. Martin and J. Reuther. High-fidelity aero-structural design optimization of a supersonic business jet. *AIAA paper 2002-1483*, 43rd AIAA/ASME/ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference, Denver, CO, April 2002.
12. Edward H. Isaaks and R. Mohan Srivastava. *An Introduction to Applied Geostatistics*. Technical report, Oxfore Univ., 1999.
13. C. A. Coello Coello and G. T. Pulido. A micro-genetic algorithms for multiobjective optimization. Technical report, *Proceedings of the Genetic and Evolutionary Computation Conference (GECCO'2001)* , 2001.

14. D. L. Carroll. Fortran genetic algorithm drive. Technical report, <http://cuaerospace.com/carroll/ga.html>, 2001.
15. K. Leoviriyakit, S. Kim, and A. Jameson. Viscous aerodynamic shape optimization of wings including planform variables. *AIAA paper 2003-3498*, 21st Applied Aerodynamics Conference, Orlando, Florida, June 2003.
16. S. Kim, J. J. Alonso, and A. Jameson. A gradient accuracy study for the adjoint-based navier-stokes design method. *AIAA paper 99-0299*, AIAA 37th Aerospace Sciences Meeting & Exhibit, Reno, NV, January 1999.
17. K. Leoviriyakit, S. Kim, and A. Jameson. Aero-structural wing planform optimization using the Navier-Stokes equations. *AIAA paper 2004-4479*, 10th AIAA/ISSMO Multidisciplinary Analysis and Optimization Conference, Albany, New York, August 30 - September 1 2004.
18. K. Leoviriyakit. *Wing Optimization via an Adjoint Method*. PhD Dissertation, Stanford University, Stanford, CA, December 2004.
19. S. Wakayama. Lifting surface design using multidisciplinary optimization. *Ph. D. Dissertation*, Stanford University, Stanford, CA, December 1994.
20. I. M. Kroo. *A Discrete Vortex Weissenger Method for Rapid Analysis of Lifting Surfaces*. Desktop Aeronautics, P.O. Box 9937, Stanford CA. 94305, Aug. 1987.
21. A. Jameson. Artificial diffusion, upwind biasing, limiters and their effect on accuracy and multigrid convergence in transonic and hypersonic flows. *AIAA paper 93-3359*, AIAA 11th Computational Fluid Dynamics Conference, Orlando, Florida, July 1993.
22. A. Jameson. Analysis and design of numerical schemes for gas dynamics 1, artificial diffusion, upwind biasing, limiters and their effect on multigrid convergence. *Int. J. of Comp. Fluid Dyn.*, 4:171–218, 1995.
23. A. Jameson. Analysis and design of numerical schemes for gas dynamics 2, artificial diffusion and discrete shock structure. *Int. J. of Comp. Fluid Dyn.*, 5:1–38, 1995.
24. R.J. Beckman M.D. McKay and W.J. Conover. A comparison of three methods for selecting values of input variables in the analysis of output from a computer code. Technical report, *SPIE Proceedings : Intelligent Control and Adaptive Systems*, 1979.
25. M. L. Stein. Large sample properties of simulations using latin hypercube sampling. Technical report, *SPIE Proceedings : Intelligent Control and Adaptive Systems*, 1987.
26. Dakota users manual version 3.1. Technical Report *SAND2001-3796*, Sandia National Lab., 2003.

Development of Automated Generation Algorithm for Skipped Surface in Die Design

Sang-Jun Lee¹, Seoung-Soo Lee², Jong-Hwa Kim², and Yoon-Jung Kwon³

¹ Dept. of Automobile, Dongeui Institute of Technology,
Busan, South Korea
leesj@dit.ac.kr

² CAESIT, Konkuk University,
Seoul, South Korea

{sslee, jhkim}@konkuk.ac.kr

³ Dept. of Textile Engineering, Konkuk University,
Seoul, South Korea
yjkwon@konkuk.ac.kr

Abstract. In general the design of exterior panel contains a number of faces composed of surfaces. It makes the design process repetitive and time-consuming task and entails errors or incompleteness such as skipped faces or discontinuity in the result. Furthermore those errors occurred in the design stage cause delay in the die design. In this paper, an algorithm to automate the tedious face work is proposed. The proposed algorithms not only automate the face work but also can reconstruct skipped surfaces or fix the discontinuous faces. The main advantages of the proposed algorithm are reduction of design lead time and to make die design process easier by generating the panel shape from one skin.

1 Introduction

In designing outer panels of an automobile the panels are composed of many faces⁽¹⁾. The individual faces are defined by dividing a surface with neighboring curves. Then a skin is created by assembling those faces. These processes are usually tedious and repetitive tasks and take a lot of time since too many surfaces should be divided into faces. For these reason incomplete design results are passed to the next process with many errors. The common errors are as follows; some surfaces or faces are omitted in the design, there exists discordance of crossed lines among neighboring surfaces, or some discontinuous points^(3,4). These errors should be fixed manually to move on to the next process, die design⁽¹⁾.

In this study an algorithm based on CATIA is proposed to search and restore omitted surfaces and to automate the time spending face design process.

The phase data and geometric data of the elements such as points, lines, faces, and solids are open to the public. Also, the algorithm for developer's correction or reconstruction and some user environment programs for 3D modeling work are released as well. Thus, we decided to develop our algorithm with CATIA⁽⁵⁾.

2 Algorithm for Searching Skipped Surfaces

The procedure to search skipped surfaces in the automotive outer panel design is as follows.

2.1 Defining the Outer Boundary Curve and the Punch Profile in Exterior Panel

- Step 1.** Select a boundary curves.
- Step 2.** Obtain the two end points of the selected curve and then search the curves connected to those end points.
- Step 3.** If more than three curves intersect at one end point, the tangential vectors from each end point are searched and the tangential continuous curve is selected.
- Step 4.** Find end points of newly selected curve and repeat the same procedure until the last end point meet with the other end point of the curve selected in Step 1.
- Step 5.** If those two points does not meet, that means the boundary curve is discontinuous or there are wrong selected curves. In this case, create a circle centered at disconnected end point with radius of 30 mm or 50 mm and inform the designer to select a curve manually and then repeat Step 3 and Step 4.
- Step 6.** If the last two end points meet at a point, the resulting curve would be a closed curve and indicate the curve with red color ⁽⁶⁾.

An example of generated outer boundary curve is shown with thick line in Fig. 1. Also, the blank curve is created in the same way for the punch profile in the panel.

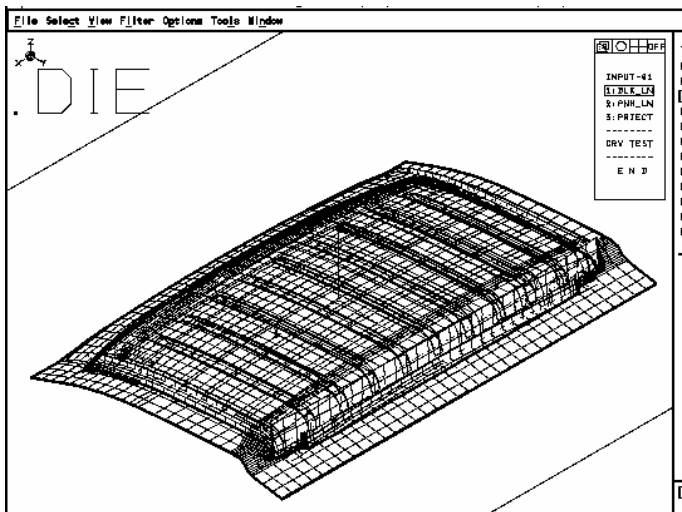


Fig. 1. The Outer Boundary Curve in Roof Exterior Panel

2.2 Searching the Skipped Surfaces

Step 1. Select a face on the outer panel.

Step 2. A boundary curve of the face is searched. If the boundary curve is either the outer boundary curve or punch profile in the panel, skip and search another boundary curve among the elements in 3 dimensional space.

Step 3. Search a neighboring face containing the boundary curve searched in Step 2 by analyzing the logical link among the elements.

Step 4. A skin is generated by connecting neighboring face to the face selected in Step 1.

Step 5. Repeat connecting neighboring faces to form a skin until the skin meets the closed outer boundary curve of the panel⁽⁷⁾.

Fig. 2 shows a skin generated by the above procedure. It has a punch profile to describe the surface of design and skipped surfaces from design department because of the lead time pressure.

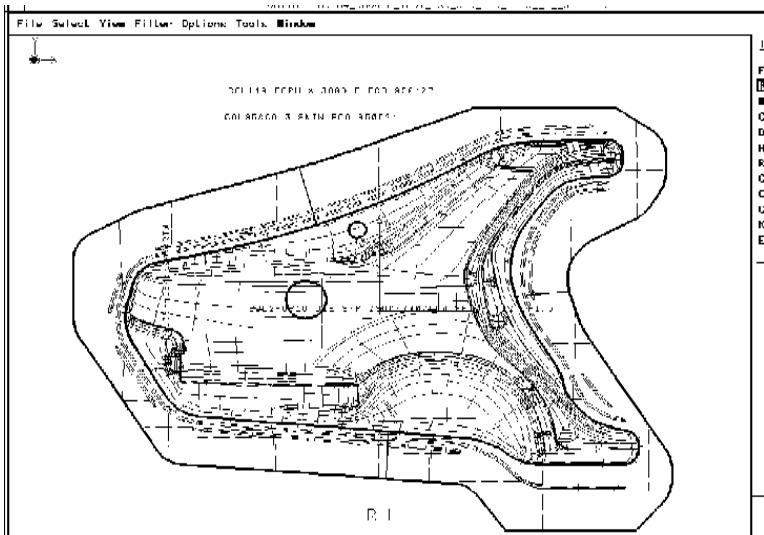


Fig. 2. Searching the Skipped Surfaces in Quarter Outer Panel

2.3 Filling the Skipped Surfaces

Skipped faces are created when only the surface work is performed without face work in design department or when the surface work on panel is skipped.

In the former case, the algorithm described in section 4 is used to generate faces automatically and in the latter case, the algorithm described in section 3 is used to reconstruct the skipped surfaces and then create a skin by connecting the surfaces each other.

3 Algorithm for Reconstructing Surface

This algorithm is to reconstruct a skipped surface from the boundary curves of neighboring faces.

3.1 Determination of Intersected Boundary Curves

In Fig. 3 various shapes of skipped faces in the exterior panel design are shown. Intersecting boundary curves are determined according to the number of neighboring boundary edges on u and v axis.

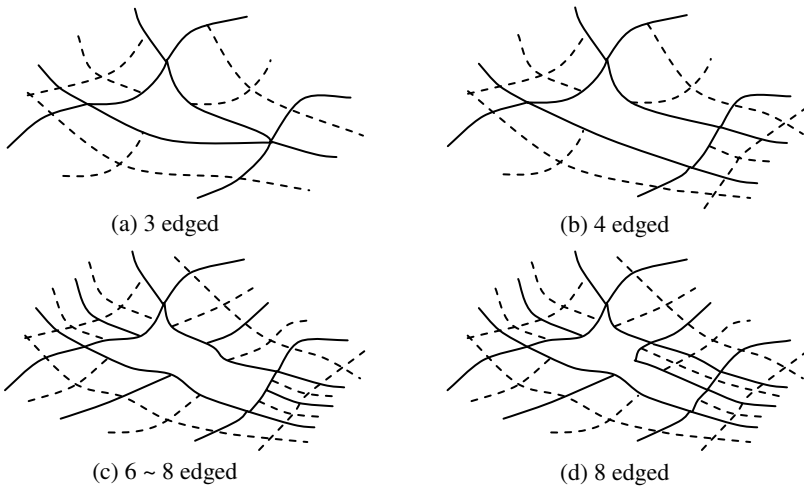


Fig. 3. Various shapes of Skipped surfaces

If the boundary edges are like (c) or (d) in Fig. 3, skipped faces are divided by the Ferguson curve and a patch of skipped face is created by the dividing curves. Fig. 4 shows the skipped face divided by Ferguson curve⁽⁸⁾.

3.2 Reconstructing Surface and Creating Face

Once the intersecting boundary curves are determined, Coons patch is created with tangential vector of neighboring boundary curves and boundary faces as shown in Fig. 5.

If the skipped face has three boundary curves as shown in Fig. 3 (a), the surface will be created by sweeping the profile curve on the u axis along the two trajectory curves on the v axis^(9,10).

The surface created by the above method would be the same shape as the original design in case (a) and (b) in Fig. 3. However, in case (c) and (d) in Fig. 3 the created surface would be different form the original design. But the differences would be very small.

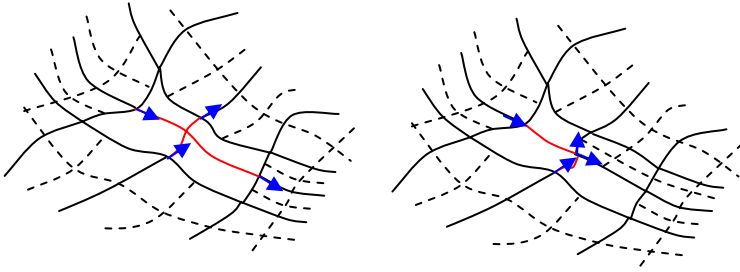


Fig. 4. Examples of skipped face division using the Ferguson curve

Next, the whole surface will be created with the patch.

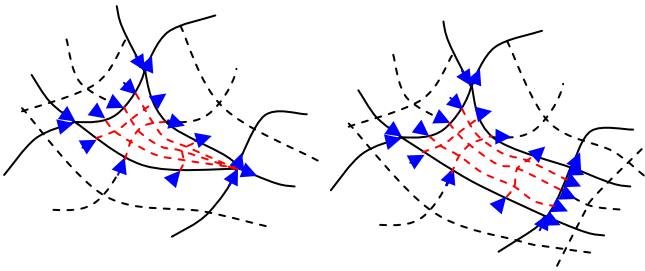


Fig. 5. Generation of Coons patch using the boundary edge and tangent vector

3.3 Algorithm for Continuation of Discontinuity Between Faces

Although an automobile is designed in 3 dimensional space, the design results are displayed in 2 dimension on computer monitor or draft. Thus the skipped faces searched by the automated generation algorithm look like (b) in Fig. 6.

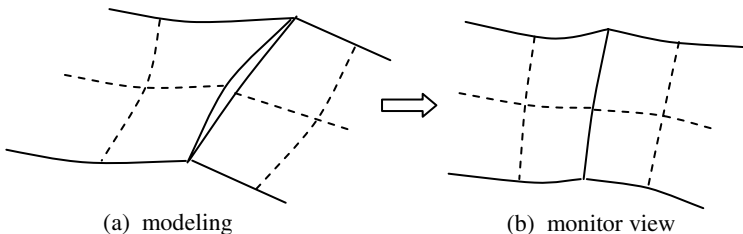


Fig. 6. Discontinuous region between adjacent faces

The following procedure is applied to fix the discontinuities between the faces.

- Step 1.** Select one face among the two adjacent discontinuous faces and divided it into quarter.
- Step 2.** Fill the discontinuous region by generating coons patch with the tangential vector of the boundary curve and the boundary face for the neighboring faces.

4 Face Automated Generation Algorithm

This algorithm is used to generate faces when the panel designer performs only the surface works and leaves the face work undone. The algorithm uses the intersection curves between a surface with unfinished face work and neighboring surfaces with finished face work.

As shown in Fig. 7, the intersection curves between the faces are generated and then the generated intersection curves are trimmed by tracing algorithm⁽¹¹⁾ at the intersection points. Then, generate a face by sewing each surface with the trimmed intersection curves.

The region where the faces are generate is determined by generating iso-parametric curves on each surfaces and check in the number of intersecting points as shown in Fig. 8⁽¹²⁾.

After reconstructing the surfaces, face work is performed to create a skin.

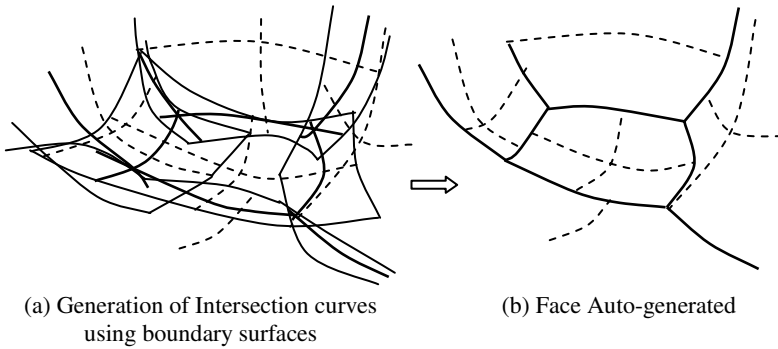


Fig. 7. Face Auto-generation

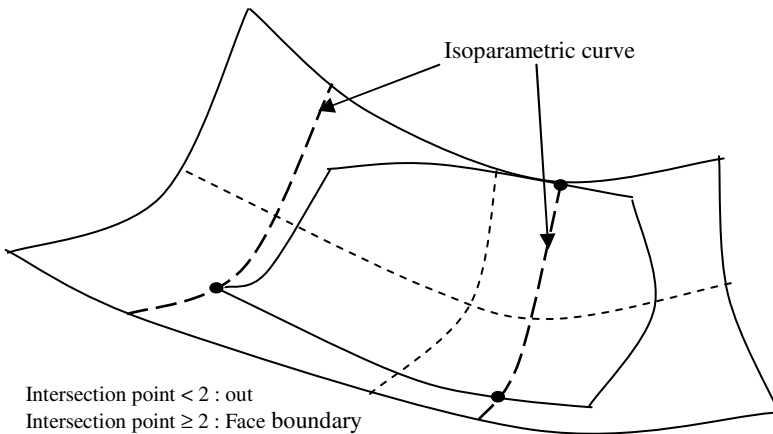


Fig. 8. Scan curve algorithm

5 An Example of Implementing the Proposed Algorithm

In this section, to demonstrate the effectiveness of the proposed algorithm "Auto-Generation Program for Skipped Surface in Die Design" is applied to the surface model of car panel in CATIA environment⁽¹³⁻¹⁵⁾.

The program is implemented on IBM RS/6000 and CATIA Version 4.1.5 with core modeler (CATGEO and CATMSP) is used for graphic software. The program is developed with C++ and IUA for GUI⁽⁴⁻⁵⁾.

The program is applied to the "Front Fender Panel" of a real automobile shown in Fig. 9.

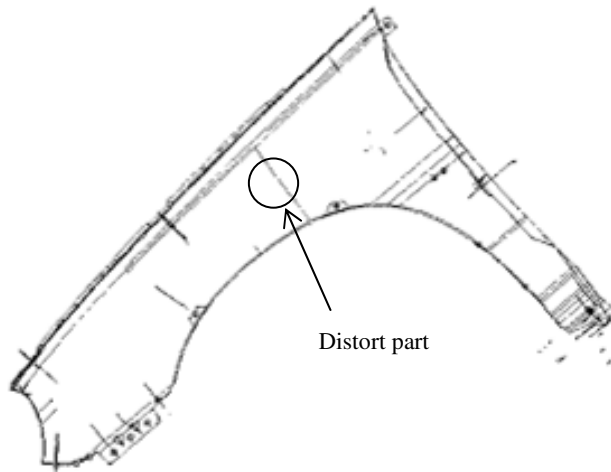


Fig. 9. A Product design shape of Front Fender using CATIA

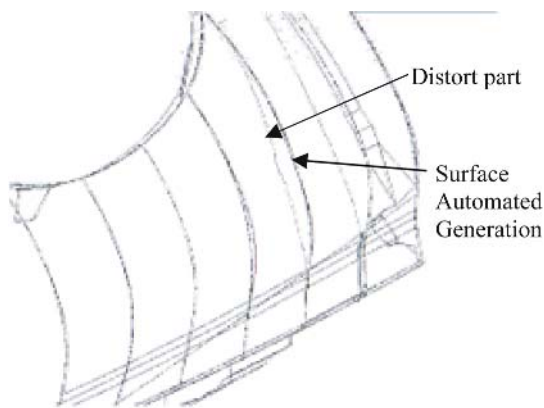


Fig. 10. A Restoration of the original shape in the developed program

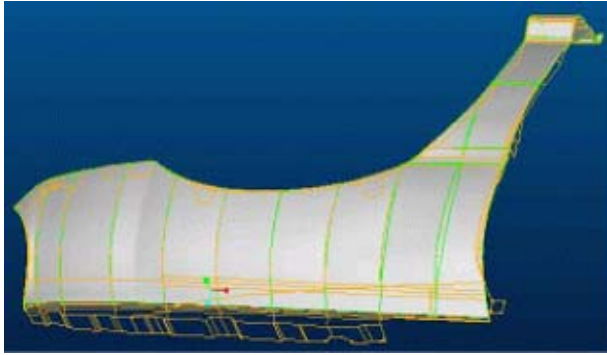


Fig. 11. Result of shape after surfacing process by the developed program

In the panel design there are some surfaces and faces omitted discordance of crossed lines among the neighboring surfaces, or some discontinuous points due to the mistakes of the designers. Fig. 10 shows the regenerated shape using the developed program and Fig. 11 shows the 3D shading results of auto regeneration shape.

6 Conclusion

In this study an algorithm for finding and reconstructing the skipped surfaces is suggested. The proposed algorithm can automate repetitive and time-consuming face work and reconstruct the skipped or discontinuous surfaces on the panel design with a simple program.

In addition the design lead-time can be reduced by automating the time-consuming face work process and the die design process. Also, the next process, die design, becomes easier since the panel is generated as a skin.

References

1. A Editorial Committe in KSAE : Handbook of Automotive Technology - Volume 2 Design, Korean Society of Automotive Engineers (1996) pp. 11-31
2. Paul B. Schubert : Die Methods - Book One and Die Methods - Book Two, Industrial Press Inc. (1966)
3. Jae-Jeong Kim : Learning CAD/CAM with CATIA, Bando Publishers (1998) pp. 115-116 and pp. 263-349
4. Dassault Systems : CATIA V4.1.7 Manuals, IBM CATIA Training Center (1998)
5. Dassault Systems : CATIA Interactive User Access / Geometry Interface / Mathematical Subroutine Package Reference Manuals, Dassault Systems Co. (1995)
6. Tae-Soo Kim, Soon-Kyu Lim, Sang-Jun Lee : A Development of Expert design system for DRAW DIE in Automotive industry, Proceedings of the 10th International IFIP WG 5.2/5.3, International Conference PROLAMAT'98 (1998) pp. 843-855
7. Tae-Soo Kim, Sang-Jun Lee : Development of Expert Design System for TRIM DIE in Automotive Industry, Proceedings of the IASTED International Conference, Intelligent Systems and Control'99 (1999) pp. 55-60

8. Imre Juhász : Cubic parametric curves of given tangent and curvature, Computer Aided Design, Vol. 30, No. 1 (1998) pp. 1-9
9. Cheul-Soo Lee : CAD/CAM - from Shape Modeling to NC Work, Turbo-Tech Publishers (1997) pp. 157-165
10. W-D Ueng, J-Y Lai, J-L Doong : Sweep- surface reconstruction from three-dimensional measured data, Computer Aided Design, Vol. 30, No. 10 (1998) pp. 791-806
11. Kyu-Yeul Lee, Doo-Yeoun Cho and Joong-Hyun Rhim : An Improved Tracing Algorithm for Surface/Surface Intersections, Journal of Ship Technology Research, Vol. 47, No. 3 (2000)
12. Min-Yang Yang and Eung-Ki Lee : Segmentation of Measuring Point Data for Reverse Engineering, Proceeding of Korean Society of CAD/CAM Engineers (1999) pp. 12-17
13. CAD Software : CATIA-Mold and Die Machining Assistant, Dassault System Co. (1996)
14. CAD Software : Computer Aided Die Engineering (CADE), Kelton Graphics Co. (1996)
15. CAD Software : devis-VAMOS, Debis System -haus Industrie (1994)

Development of Requirement Driven Concept Selection Process in Aerospace System

Hyeong-Uk Park¹, Mee-Young Park¹, Seung-Jin Lee¹,
Jae-Woo Lee^{2*}, and Yung-Hwan Byun³

¹ Graduate Research Assistant, Department of Aerospace Engineering

² Associate Professor, Department of Aerospace Engineering,
jwlee@konkuk.ac.kr

³ Department of Aerospace Engineering,
Center for Advanced e-System Integration Technology (CAESIT),
Konkuk University, Seoul 143-701, Republic of Korea

Abstract. A Design Space Model has been developed to find a design requirements by analyzing design sensitivity and by searching for the feasible design region. In addition, the best configuration concept that satisfies the design requirements has been identified using Quality Function Deployment and the Configuration Concept Selection Matrix. These Concept Selection Process can contribute to reduce the time and effort during early design stage.

1 Introduction

In design, the requirement definition and the concept selection are exceptionally influential and therefore need close attention. In the early stage of conventional design process, a designer establishes the design requirements based on market survey or customer needs to sketch various configuration concepts among which the most suitable concept is selected through comparisons and analyses to perform the aircraft concept design. However, whether the results of this process are practically applicable in the design process or not, and how thoroughly they can satisfy the needs of customers have rarely been fully considered. Also, the selection of configuration concepts through comparison-based methods requires considerable time and effort and can be highly influenced by subjective judgments of designers. Thus, not all the configuration concepts selected in this way could be optimal to satisfy the design requirements. Furthermore, not many studies on the feasibility of design requirements and basic configuration concept in the early-stage design process have been done in spite of their great importance.

In this study, we have developed a Design Space Model to reduce the time and effort consumption required for comparisons and analyses and make the identification of design requirements more efficient by analyzing the sensitivity of design variables and marking the applicable design space. In addition, we have established a process to identify the best configuration concept that satisfies the design requirements using

* Corresponding author.

Quality Function Deployment (QFD) and the Configuration Concept Selection Matrix. A regional jet transport with the capacity of 100 passengers was designed as an example and a proof of these processes.

2 Pre-conceptual Design Process

2.1 Best Concept Selection Process

The overall process was roughly divided into three stages: *Requirements Analysis*, *Determination of Feasibility and Design Requirements*, and *Concept Development*. The overall selection process was based on customer requirements and was arranged to specify the design requirements and concepts. Figure 1 shows brief relations and flow of the overall process [1].

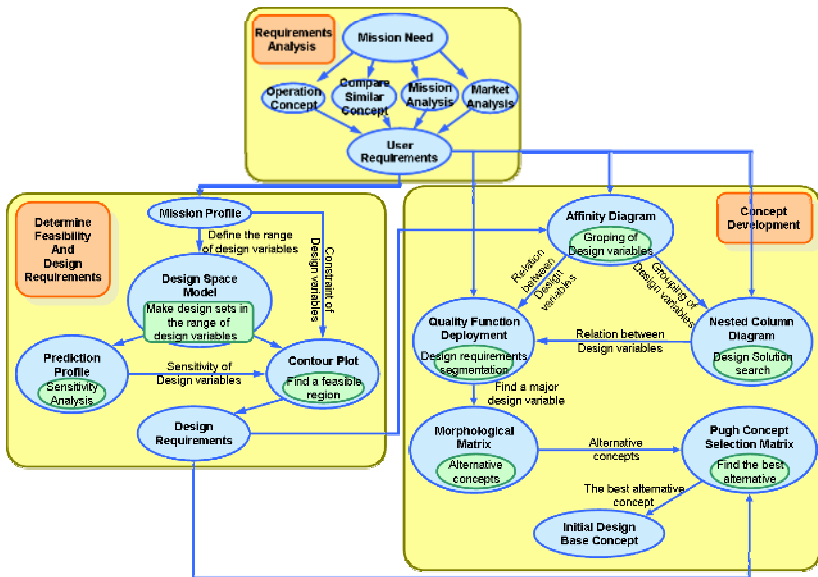


Fig. 1. Pre-conceptual Design Process

2.2 Requirements Analysis

As low-price regional airlines, which are already popular in Europe, North America, and Southeast Asia, have started to emerge in Korea, a regional transport with the capacity of 100 passengers was selected for the design. In order to specify the customer requirements, we counted the number of airlines in each continent, the number of the aircraft(of the kind aforesaid) they possess, and the number of airports located within 2,000km from major cities and estimated the number of aircraft to be sold in 10 years. In result, it was estimated that about 220 aircraft could be sold for five years from mass production [2]. The customer requirements based on this result are:

- Short-distance takeoff & landing
- Large capacities with passenger-favorable aspects
- Low operation and maintenance cost
- Environmental considerations (e.g. noise and gas)
- All-weather capability flights
- Ability to fly outside the Korean Peninsula
(In case of exports and operations after reunification)

Table 1. Forecast Sales of Each Regional Area for 5 years

Area	West Asia	Southeast Asia	Far East Asia	Oceania	The Americas. Canada	Middle South America	Total
Forecast Sale Log	20	50	66	33	45	15	229

2.3 Determination of Feasibility and Design Requirements

2.3.1 Mission Profile

Figure 2 shows the mission of an aircraft to be designed according to the above requirements of customer. This plane are operated by two pilots, two crews. 100 passengers can be accommodated and the maximum payload including these people is 20,500lbs.

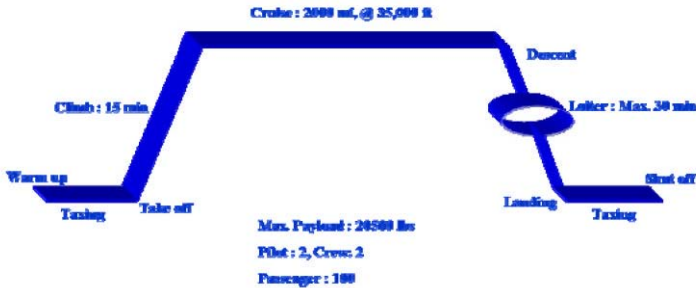


Fig. 2. Mission Profile

The mission profile was considered to extract the major design parameters for each flight phase.

- Takeoff: Takeoff Gross Weight, Takeoff, Field Length, T/W
- Climb: Climb Rate, T/W
- Cruise: Cruising Altitude, Speed, Range, Endurance, L/D, T/W
- Loiter: Loitering Time
- Landing: Landing Field Length, T/W

Above design parameters are applied to the Design Space Model as shown below.

2.3.2 Design Space Model

The design parameters from the Mission Profile were utilized for the sizing code developed for this study. Three-level Full Factorial Method was applied to input variables of the sizing code and 81 different design cases were derived in this way and a Design Space Model was derived that would show interpretations of each case in order to understand the sensitivity of design variables and to mark the applicable range of design. The input variables of Sizing Code and the results are as shown in Table 2 [3, 4].

Table 2. Input & Output parameters of the Sizing Code

Input Data	W/S, T/W, t/c, AR
Output Data	Gross Weight, Empty Weight, Sized Fuel Weight, Designed Wing Loading, CL_MAX for Landing, Required Balanced Take off Field Length, Required Landing Field Length, Stall Speed, Take off Speed, Approach Speed, RDT&E Cost Per Unit

	W/S	T/W	t/c	AR	W ₀	W _e	W _F	CL _{max}	FL _{TO}	FL _{LD}	V _s	V _{to}	V _a	Cost
1	104.0	0.3	0.1	7.0	82570.8	43660.2	17595.6	2.37669	4059.31	3800.51	113.69	125.059	136.262	3.62877E7
2	104.0	0.3	0.1	10.0	78841.4	42513.1	15029.8	2.37669	4059.31	3800.51	113.69	125.059	136.262	3.55104E7
3	104.0	0.3	0.1	13.0	77445.9	42349.2	13806.1	2.37669	4059.31	3800.52	113.69	125.059	136.262	3.53997E7
4	104.0	0.3	0.15	7.0	82912.1	43104.3	18487.3	1.87267	5151.86	4554.26	128.079	140.887	153.508	3.59122E7
5	104.0	0.3	0.15	10.0	78981.0	41874.9	15803.0	1.87267	5151.86	4554.26	128.079	140.887	153.508	3.50769E7
6	104.0	0.3	0.15	13.0	77475.9	41655.4	14525.5	1.87267	5151.86	4554.26	128.079	140.887	153.508	3.49271E7
7	104.0	0.3	0.2	7.0	84912.0	43594.6	19987.4	1.38864	7049.12	5863.16	149.818	164.799	179.562	3.62442E7
8	104.0	0.3	0.2	10.0	80638.2	42228.0	17098.1	1.38864	7049.12	5863.21	149.818	164.799	179.562	3.53174E7
9	104.0	0.3	0.2	13.0	78970.7	41939.2	15728.2	1.38864	7049.12	5863.21	149.818	164.799	179.562	3.51207E7
10	104.0	0.5	0.1	7.0	91554.4	52643.8	17595.6	2.37669	2435.58	3800.51	113.69	125.059	136.262	4.22694E7

Fig. 3. Design Space Model

2.3.3 Prediction Profile

Using the results of each design case from the Design Space Model, a Prediction Profile was prepared. The sensitivity of design variables was investigated using the Prediction Profile to find the major design variables that could influence the design. Then these variables were used as the base axis in Contour Plot. As shown in Fig. 6,

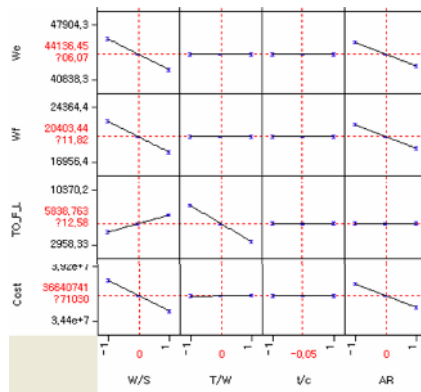


Fig. 4. Prediction Profile

the wing loading (W/S) and the aspect ratio (AR) have the highest sensitivity and are greatly influential in the other design variables [5].

2.3.4 Contour Plot

Based on the results of the Design Space Model and the Prediction Profile, a Contour Plot was prepared. The Prediction Profile was to interpret the sensitivity of design variables, whereas the Contour Plot was used to mark the applicable design space for each condition of restriction. With the two highly sensitive variables used as horizontal and vertical axis respectively, the results can be plotted on a plane. The range of each value in given condition of constraints was indicated by a contour, enabling us to mark the applicable range of design that satisfies all constraints of design variables, or that is not included in any contour. As shown in Fig. 5, the white indication marks the feasible design area within which the conditions that satisfy each design variable are extracted to establish the Design Requirements. If a spot outside the applicable range of design must be included, the applicable range of design need to be adjusted by altering the condition of restriction or replacing high sensitive variables after examining unsatisfactory constraints.

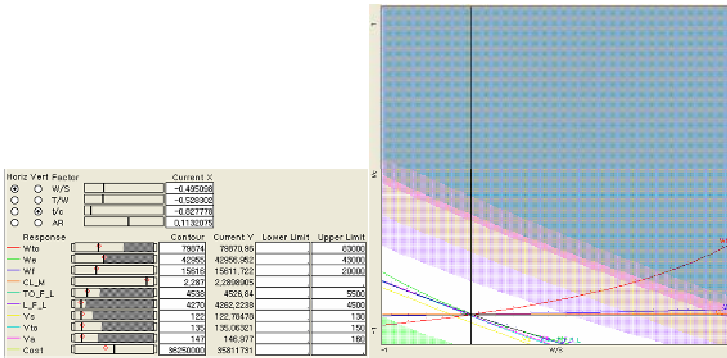


Fig. 5. Contour Plot

2.3.5 Design Requirements

Design requirements are established by identifying design variables in the applicable design range.

The following are the design requirements derived by the procedures afore mentioned:

- Takeoff Gross Weight: Less than 83000 lbs
- Empty Weight: Less than 43000 lbs
- Fuel Weight: Less than 20000 lbs
- Takeoff Field Length: Shorter than 6500 ft
- Landing Field Length: Shorter than 4500 ft
- Stall Speed: Lower than 120 Kts

- Takeoff Speed: Higher than 135 Kts
- Approaching Speed: Lower than 145.0 Kts.

2.4 Configuration Concept Development Process

2.4.1 Affinity Diagram

An Affinity Diagram was prepared to classify the factors indicated in the performance and design requirements. The design requirements were selected on the basis of customer and engineer viewpoints. As for the voice of customer, the factors were classified into airlines, producers, and social requirements; and as for the voice of engineers, the factors were classified into driving force, performance, structure, and aerodynamics.

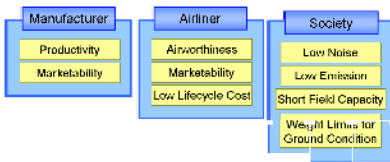


Fig. 6. Voice of Customer

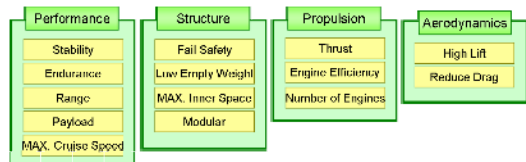


Fig. 7. Voice of Engineer

Based on the initial customer requirements, the subcategories under the voice of customers formed the fundamentals of Nested Column Diagram and Quality Function Deployment (QFD) as shown below. Also, the classifications under the voice of engineers determine the subcategories in Nested Column Diagram and Quality Function Deployment.

2.4.2 Nested Column Diagram

A Nested Column Diagram is a method of searching for the elements that influence a certain factor and the subcategories become the factors or solutions that influence higher categories. In addition, there can be several subcategories under a stage. In this study, the voice of engineer categories that could satisfy the voice of customer categories in Affinity Diagram were connected and the design considerations of each category were connected into subcategories to derive out the design factors that meet the customer requirements. Also, the relations and degree of impact of design variables were analyzed and applied to the construction of QFD.

2.4.3 Quality Function Deployment

A QFD was used to analyze the System Requirements based on the affinity of design factors determined in the Nested Column Diagram. We prepared first and second House of Quality based on the affinity connections in the Nested Column Diagram in order to derive out the configuration and performance factors that often influenced the design requirements and configuration concept as well as a few representative factors needed to analyze the relations between them [6, 7].

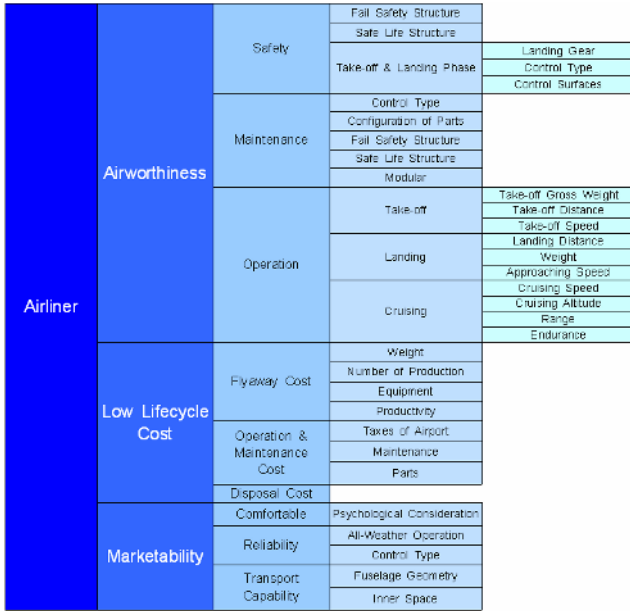


Fig. 8. Nested Column Diagram

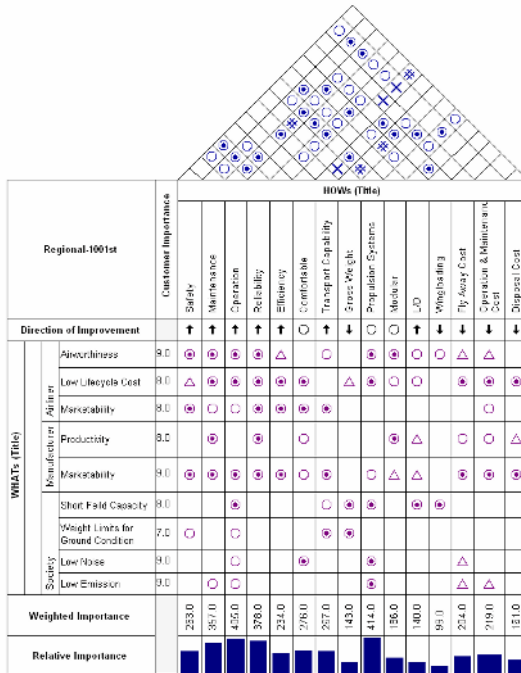


Fig. 9. 1st QFD

2.4.4 Morphological Matrix

• Morphological Matrix

As a result of the Absolute Importance of Second House of Quality, a Morphological Matrix was prepared using the design requirements with high scores. All engine-related categories and all empennage configurations that influence control type and stability from the second House of Quality were considered. (Table 3)

Table 3. Morphological Matrix

Characteristics		Alternatives				
Configuration	Tail Type	Conventional	Cruciform	T-Tail	Canard	Tailless
	Engine Position	Wing		Fuselage		
Control	System Type	Hydraulic		Fly By Wire		Fly By Light
	Control Surfaces	Main Wing			Canard	
Propulsion	Engine Type	Turbo Prop.		Turbo Fan		
	No. of Engine	2		3		4

• Combing Concept

Major configuration concepts from the Morphological Matrix were combined and organized to be compared with basic configuration concepts. (Table 4)

Table 4. Combining Concept Matrix

	Base Line	Concept 1	Concept 2	Concept 3	Concept 4
Tail Type	Conventional	Conventional	Cruciform	Cruciform	T-Tail
Engine Position	Wing	Fuselage	Fuselage	Wing	Wing
Control Sys. Type	Hydraulic	FBL	FBW	FBL	Hydraulic
Control Surfaces	Main wing	Main Wing	Main Wing	Main Wing	Main Wing
Engine Type	Turbo Fan	Turbo Prop.	Turbo Fan	Turbo Prop.	Turbo Fan
No. of Engine	2	4	2	2	3
	Concept 5	Concept 6	Concept 7	Concept 8	Concept 9
Tail Type	T-Tail	T-Tail	Canard	Canard	Tailless
Engine Position	Fuselage	Wing	Fuselage	Wing	Wing
Control Sys. Type	FBW	Hydraulic	FBW	FBL	FBL
Control Surfaces	Main Wing	Main Wing	Main Wing	Canard	Main Wing
Engine Type	Turbo Fan	Turbo Prop.	Turbo Fan	Turbo Prop.	Turbo Fan
No. of Engine	2	2	2	2	2

2.4.5 Pugh Concept Selection Matrix

In Pugh Concept Selection Matrix, the optimal design configuration concept was derived by scoring the design requirement satisfaction level of each configuration. The correlation of high-score categories from the first QFD and nine design concepts subcategorized in the Morphological Matrix were examined. The affinity of each factor was grades as follows:

- + : Indicating Superior Performance (1 point)
- o : Indicating Similar Performance (0 point)
- : Indicating Inferior Performance (-1 point)

Table 5. Pugh Concept Selection Matrix

		Design Concepts									
		1	2	3	4	5	6	7	8	9	10
Design Criteria	Safety	○	+	-	-	+	+	+	-	-	+
	Maintenance	○	-	○	-	○	+	○	+	+	+
	Reliability	○	+	○	+	○	+	○	-	○	-
	Modular Construction	○	-	○	-	○	+	○	○	+	+
	Transport Capability	○	○	○	○	○	○	○	○	○	+
	TAW available	○	-	+	-	+	○	-	○	-	-
	Flying Control	○	+	+	+	○	+	○	+	+	-
	High L/D	○	○	○	○	○	○	○	+	+	+
	+ (plus) Pugh Sums		0	2	2	2	2	5	1	2	4
- (minus) Pugh Sums		0	2	1	2	0	0	1	2	2	2
Concept Rating (+s and -s)		0	0	-1	0	2	5	0	-1	2	2

Final scoring was done by adding the affinity scores of each category. As a result, the design concept No. 7 (T-tail, Fuselage Mounted 2 Engines, Fly by Wire Control System) was chosen to be the most promising configuration which satisfies the customer and performance requirements of this study.

2.4.6 Best Configuration Concept

The design configuration that satisfies the performance and design requirements of this study is shown at Fig. 10.

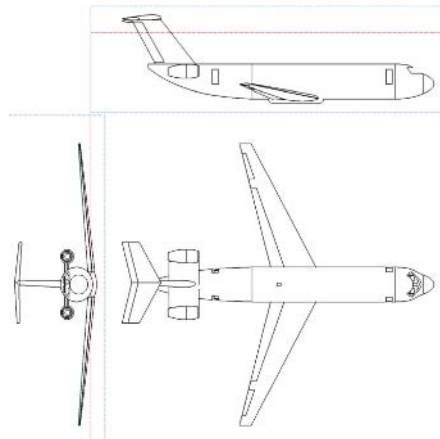


Fig. 11. Selected concept

3 Conclusion

With the requirement-driven Configuration Concept definition procedures that is less susceptible to the designer's subjectivity, we can more reasonably establish the design requirements and design configuration concept which could satisfy the given customer requirements. The process developed in this study is applicable to other types of aircraft and may save much time and effort in early design stage. Various techniques in this study may be replaced by other appropriate tools as needed. In the future, the desirable use of tools for each design issue should be tested and specified and a more flexible process to meet various customer needs should be established to handle uncertainties.

Acknowledgement

This work was supported by grant number R01-2006-000-10744-0 from the Basic Research Program of the KOSEF in 2006.

References

1. Hyeong-Uk Park, Min-Ji Kim, Jae-Woo Lee, Yung-Hwan Byun, "Unmanned Helicopter Conceptual Design by Considering Uncertainty of Requirement", Proceedings of the 2005 KSAS Spring Conference (2005)
2. Aerospace vehicle design project, Def. of Aerospace Eng., Konkuk Univ. (2005)
3. Optimus v5.0, Noesis Solutions Inc. User Manual (2004)
4. JMP v5.0, SAS Institute Inc. User Manual (2002)
5. Andrew P. Baker, The Rule Of Mission Requirements, Vehicle Attributes, Technologies And Uncertainty In Rotorcraft System Design. (2002)
6. QFD Designer 4, Ideacore. (2000)
7. Min-Ji Kim, Mee-Young Park, Jae-Woo Lee, Yung-Hwan Byun, "System Requirement Analysis of Multi-Role Helicopter by Implementing Quality Function Deployment", Korean Council On Systems Engineering Review, Vol. 1, No. 2, (2005) 56-62

A TMO-Based Tele-operation Model: Supporting Real-Time Applications in Grid Environments

Chulgoon Kim¹, Karpjoo Jeong², Hanku Lee^{2,*}, MoonHae Kim³, KumWon Cho⁴, Segil Jeon⁵, Jaehoon Ahn⁶, and Hyunho Ju⁶

¹ Department of Advanced Fusion Technology, Konkuk University, Seoul, Korea
kimchulgoon@ricl.konkuk.ac.kr

² School of Internet and Multimedia Engineering, Konkuk University, Seoul, Korea
{jeongk, hlee}@konkuk.ac.kr

³ College of Information and Communication, Konkuk University, Seoul, Korea
mhkim@konkuk.ac.kr

⁴ Korea Institute of Science and Technology Information
ckw@kisti.re.kr

⁵ BioMolecular Informatics Center, Konkuk University, Seoul, Korea
sgjeon@ricl.konkuk.ac.kr

⁶ School of Computer Engineering, Konkuk University, Seoul, Korea
{jahn, hju}@mclab.konkuk.ac.kr

Abstract. We frequently need to access geographically distributed remote instruments, experimental equipments, databases, human resources with respect to real-time in grid computing environments. In the real world, it is very difficult to implement real-time models in uncontrolled distributed environments and to support well-defined interfaces from real-time systems to external systems. We propose an easy-to-use TMO-based tele-operation model with less strict real-time constraints in grid environments. Using the proposed model, we design and develop a TMO-based tele-operation system for real industrial applications used for construction instruments, space probing instruments, etc.

1 Introduction

With the fast development of grid computing environments, we can access geographically distributed remote instruments, experimental equipments, databases, human resources, high-performance computers, etc, as if accessing local resources from a long distance away. Though this accessibility is very stable and secure, it brings us another side: How are these instruments, devices and data well-synchronized in distributed real-time systems? With conventional programming methods it is very hard to implement real-time models in uncontrolled distributed environments, to design interactions between real-time systems and external systems, and to support well-defined interfaces from real-time systems to external systems.

The main purpose of this paper is to study how to support real-time applications in grid computing environments, to design TMO-based distributed real-time processing

* Author for correspondence: +82-2-2049-6082.

techniques for real industrial applications, and to develop a TMO-based tele-operation model with less strict real-time constraints in grid environments. The proposed TMO-based tele-operation model can be used to control construction instruments, space probing instruments, and tsunami-detecting instruments. For example, a remote engineer can control construction instruments, monitor construction fields, and conference with local engineers from a long distance away using the proposed model in grid computing environments.

In the next section, we discuss related works such as TMO, Distributed Object-oriented Freeway Simulator (DOFS), Real-time CORBA, and Real-time Java. Then, we propose a TMO-based tele-operation model and mention design and implementation issues caused by using TMO in section 3. Section 4 concludes.

2 Related Works

The Time-Triggered Message-Triggered Object (TMO) was established in early 1990's with a concrete syntactic structure and execution semantics for economical reliable design and implementation of RT systems [1, 2, 4, 5]. TMO is a high-level real-time computing object. It is built in standard C++ and APIs called TMO Support Library (TMOSL). Its member functions are executed within specified time windows. TMO is also a high-level distributed computing object. TMOs interact among themselves via remote method calls. Remote method calls are made in forms that are essentially the same as those of calling conventional object methods.

TMO contains two types of methods, time-triggered methods (SpM), which are clearly separated from the conventional service methods (SvM). The SpM executions are triggered upon reaching of the RT clock at specific values determined at the design time whereas the SvM executions are triggered by service request messages from clients. Moreover, actions to be taken at real times which can be determined at the design time can appear only in SpM's. As in other RT object models, the TMO incorporates deadlines and it does in the most general form. Basically, for output actions and methods completions of a TMO, the designer guarantees and advertises execution time-window bounded by start times and completion times. Real-time Multicast and Memory Replication Channel (RMMC) is an alternative to the remote method invocation for facilitating interactions among TMOs. Use of RMMCs tends to lead to better efficiency than the use of traditional remote method invocations does in many applications, especially in the area of distributed multimedia applications which involve frequent delivery of the same data to more than two participants distributed among multiple nodes.

Distributed Object-oriented Freeway Simulator (DOFS) [3] is a freeway automobile traffic simulator conducting with the goal of validating the potential of the TMO structuring scheme supported by the recently implemented TMOSM. DOFS is intended to support serious studies of advanced freeway management systems by providing high-resolution high-accuracy easily expandable freeway simulation. DOFS is also meant to be a foundation for future expansion into a high-fidelity regional traffic simulator which simulates not only freeways but also stop-and-go surface streets. Some of the DOFS's components provide simulation environment. Some of the DOFS's components do monitoring to the environment and share the information each other. Then the system can help the Driver avoiding the traffic road and supply

real-time traffic information. Through this development the developer observed that the programming and debugging efforts were significantly less than the efforts required during earlier development of similar but simpler applications using the conventional object-oriented design or other methods. The TMO scheme brings major improvement in the RT system design and implementation efficiency.

The Real-time CORBA (RT-CORBA) [6] is an optional set of extensions to CORBA to be used as a component of a real-time system. It is designed for applications with hard real-time requirements, such as avionics mission computing, as well as those stringent soft real-time requirements, such as telecommunication call processing. Strict control over the scheduling and execution of processor resources is essential for many DRE applications. Moreover, to allow applications to control the underlying communication protocols and end-system resources, the Real-time CORBA specification defines standard interfaces that can be used to select and configure certain protocol properties. In addition, client applications can explicitly bind to server objects using priority bands and private connections.

The Real-Time Java (RTSJ) [7] is one of Gosling's areas of interest. Real-time systems are found in embedded applications as well as other applications that require a deterministic time behavior. RTSJ includes such features as real-time threads, asynchronous events, interruptible nonblocking I/O (input/output), access to physical memory, scheduling, and timers. One of the concerns of real-time programming is to ensure the timely or predictable execution of sequences of machine instructions. Various scheduling schemes name these sequences of instructions differently. Typically used names include threads, tasks, modules, and blocks. The RTSJ introduces the concept of a schedulable object. Garbage-collected memory heaps have always been considered an obstacle to real-time programming due to the unpredictable latencies introduced by the garbage collector. The RTSJ addresses this issue by providing several extensions to the memory model, which support memory management in a manner that does not interfere with the ability of real-time code to provide deterministic behavior. This goal is accomplished by allowing the allocation of objects outside of the garbage-collected heap for both short-lived and long-lived objects.

3 The Proposed TMO-Based Tele-operation Model

3.1 Architecture

With the fast development of the Internet and grid computing environments, it is no longer necessary for remote instruments, computing resources, and human resources (i.e. engineers and researchers) to be located in the same place and at the same time. Moreover, it is possible for engineers and researchers to access remote instruments and computing resources from a long distance away. However, we need to support real-time controls and the timing characteristics on these geographically distributed, grid-enabled, and real-time applications without pain during the development.

Figure 1 depicts the architecture of the proposed TMO-based tele-operation model. One of the main issues for the proposed model is to apply the easy-to-use TMO to real-time applications that are usually hard to design and implement with conventional programming methods. The proposed model is divided to 3 domains: remote domain, message-handling-service domain, user interface domain.

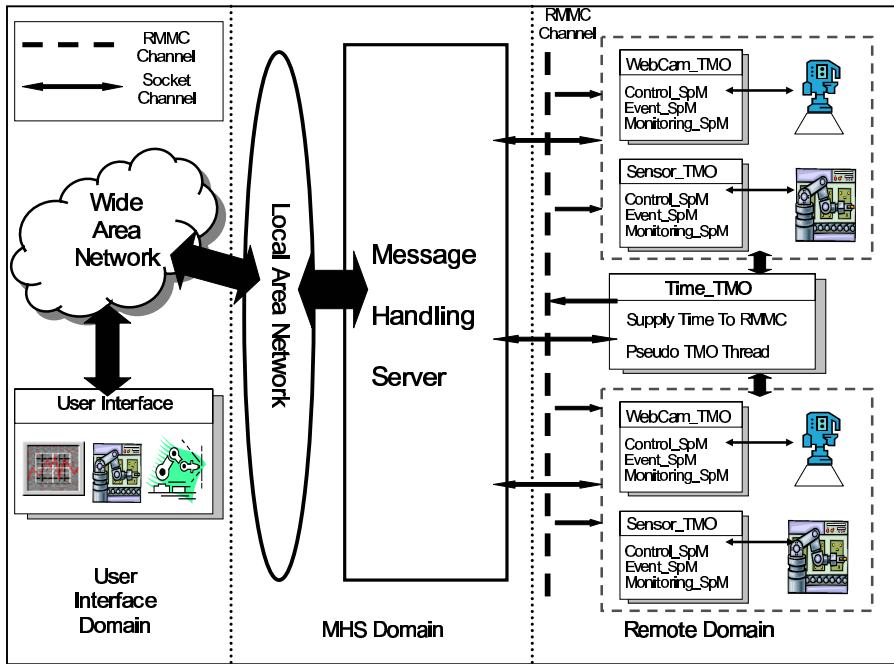


Fig. 1. The Architecture of TMO-Based Tele-Operation Model

The remote domain (RD) is to collect remote data and to monitor remote instruments. RD consists of the Time TMO and working TMOs. The Time TMO gives the timing characteristics to other working TMOs (e.g. WebCam_TMO and Sensor_TMO) via the Real-time Multicast and Memory Replication Channel (RMMC). The video, audio, and sensor data with the timing characteristics are transferred via the socket channel to the message-handling-service domain. The time characteristics supplied by the Time TMO are more suitable to the proposed model than those supplied by the Internet or GPS time services since the Time TMO is closely located to other working TMOs and this locality avoids the network latency that makes it hard to synchronize real-time applications.

The message-handling-service domain (MHSD) is to manage message-handling servers in order to help data communication between UID and RD. MHSD provides the grid-enabled environments based on the TCP/IP-based client/server model and grid applications to handle control-messages between UID and RD to be safely and precisely transferred. MHSD should keep waking up, be started prior to other domains, and wait for control-messages. Servers in MHSD can store a large amount of data from the remote domain and can provide the secure management of data from the remote domain to the interfaces.

Finally, the user interface domain (UID) is to provide user interfaces to check the status of the whole system, to manage incoming and outgoing control-messages

between the client and remote instruments, and to handle real-time information needed for the tele-operation application for the client. This domain is implemented in MFC.

3.2 Implementation

In this section we mention several implementation issues caused by using TMO for the remote domain in detail.

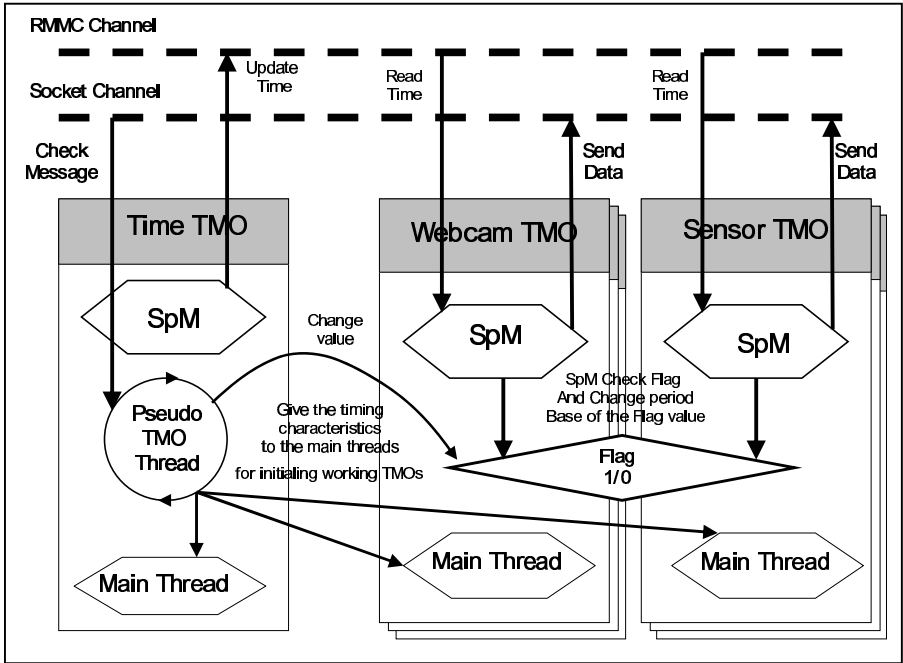


Fig. 2. The Remote Domain: TMO-Based Real-Time Agent framework

Figure 2 represents the basic structure of the remote domain, called TMO-based real-time agent framework for the proposed TMO-based tele-operation system. The real-time agent framework is implemented using TMO toolkit [1]. It consists of the Time TMO and working TMOs (e.g. WebCam_TMO and Sensor_TMO). Moreover, it is basically divided into three services: control-message waiting and processing service, time service, and real-time data processing service.

The control-message waiting and processing service waits for and processes control-messages from UID according to message types using the Pseudo-TMO-Thread. The Pseudo-TMO-Thread is located in the Time TMO and gives the timing characteristics to the main threads for initialing all working TMOs in the remote domain. But The Pseudo-TMO-Thread keeps waking up unlike SpM of TMO periodically wakes

up. Major initialization steps for the TMO-based real-time agent framework are as follows:

1. The Pseudo-TMO-Thread is invoked and checks up the header information of control-messages from MHSD.
2. Each message is classified like WebCamMessage, SensorMessage, etc., and is sent to its designated TMO.
3. Each TMO extracts the timing characteristics from its control-message, initializes its time according to the timing characteristics, and builds up the socket channel among other TMOs.
4. The TMO middleware is activated.
5. The TMO-based real-time agent framework is activated.

The Pseudo-TMO-Thread keeps waking up and getting control-messages from UID. If a control-message is a normal command to control remote instruments, then the Pseudo-TMO-Thread does normal real-time data processing in this service. But if a control-message is a command to scale up or down the whole system in the time dimension, then the Pseudo-TMO-Thread extracts data out of the message, stops the designated SpM for a while, changes the period of the designated SpM, and restarts the designated SpM. When a working TMO needs to process video data, sometimes, the data processing time exceeds the period of SpM for the TMO. It happens because of the network latency or the size of the video data. In this case, the period of SpM should be extended more than the data processing time.

For example, when the network becomes delayed, the data transfer from web cameras becomes delayed as well. To avoid the latency of the whole system because of the latency of the video transfer, the Pseudo-TMO-Thread gets a control-message from UID to change the period of SpM for web cameras from 1 second to 3 seconds. After the network becomes normal, the Pseudo-TMO-Thread gets another control-message from UID to change the period back. This functionality makes the TMO-based real-time agent framework flexible for real-time monitoring.

The time service is served by the Time TMO that is closely located to other working TMOs. The time service synchronizes the timing characteristics of each SpM in working TMOs. The real-time data processing service manages data processing according to the timing characteristics of each SpM and attaches the timing characteristics on video and sensor data. The time service and the real-time data processing service use RMMC that is a real-time communication channel among working TMOs to broadcast common information such as the timing characteristics and memory for working TMOs. RMMC is a good alternative to the Internet or GPS time services since it avoids the network latency that makes it hard to synchronize real-time applications. SpM of the Time TMO periodically (e.g. 200 micro-seconds) updates the timing characteristics of RMMC using its own timing characteristics. Then each SpM reads the timing characteristics of RMMC, attaches it on video, audio, and sensor data, and transfer data to MHSD.

Figure 3 represents a TMO-based tele-operation system based on our proposed model. The TMO-based tele-operation system is a real-time, tele-operation, and tele-monitoring system. Using the system, a remote engineer can monitor construction fields, control construction instruments, and conference with local engineers from a long distance away. In detail, first, a remote engineer monitors the current status of a

designated construction field on his/her computer from a long distance away. Second, the video, audio, and sensor data from the construction field are collected and synchronized by the TMO-based real-time agent framework and transferred via MHSN to the remote engineer. Third, the data are updated and displayed on his/her computer. Finally, the remote engineer can control remote construction instruments by controllers on his/her computer and send control-messages such as scaling up or down the whole system in the time dimension. Using the system, moreover, the remote engineer can chat and talk with local engineers in the construction field.

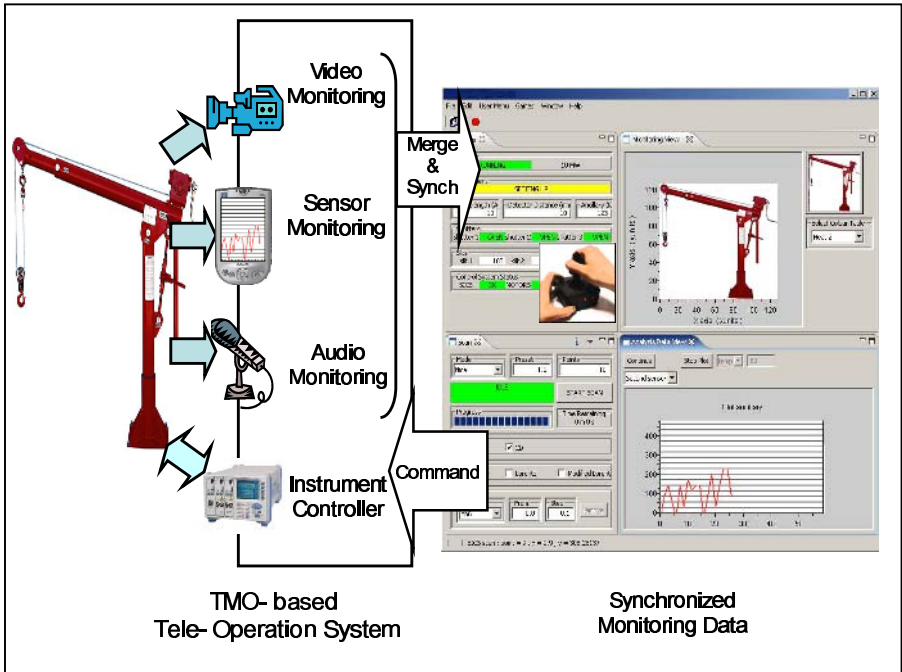


Fig. 3. A TMO-Based Tele-Operation System

3.1 Advantages and Restrictions of the Proposed Model

We experienced several advantages of adapting TMO on the proposed model during implementing a TMO-based tele-operation system.

Developers can highly predict the timing performance using TMO during designing and developing the proposed TMO-based model. Execution of time consuming unpredictable I/O operations such as video outputs, keyboard inputs, etc, can be handled by the Pseudo-TMO-Thread. Each TMO thread designated to instruments are not burdened with these suffering tasks.

Moreover, it is easy to implement and debug TMO nodes. Implementing and debugging of real-time controls and the timing characteristics cause pain during the development of distributed real-time applications with conventional real-time

methods. But all we need to do is to use communication APIs, thread initializing, managing, and terminating APIs, supported by the TMO tool kit.

It is easy to modify and expand the proposed TMO-based model. We often need to scale up or down the whole system in the time dimension. Many modifications could be needed with conventional real-time methods. But all we need to do is to change the scale of the real-time clock of TMO for the proposed TMO-based model.

We experienced some restrictions that TMO-based real-time applications are not suitable to real-time systems handling huge amount of data in a relatively short SpM wakeup period. For example, wind channel experiments in aerospace researches generally need video capturing instruments taking approximately 1,000 photos per second and the size of each photo is approximately 1M bytes. In this case, we can easily scale down the period of SpM (e.g. 10 micro-seconds). But it is impossible to process this amount of video data in time with contemporary hardware and network environments.

Thus, we urge TMO-based real-time applications are suitable to systems with less strict real-time constraints such as construction instruments, space probing instruments, tsunami-detecting instruments, etc, since those instruments product relatively small amount of data in the period of SpM and are not a time-critical decision model.

4 Conclusion

Distributed real-time tele-operation systems are in their infancy because it is very hard to design and implement them with contemporary hardware and conventional programming methods.

We proposed an easy-to-use TMO-based tele-operation model with less strict real-time constraints in grid environments. Using the proposed model, we designed and developed a TMO-based tele-operation system for real industrial applications able to be used in construction fields.

The TMO-based tele-operation model, proposed in this paper, is promising since it provides a sound TMO-based real-time agent framework, cost-effectively resolving the problems caused by conventional programming methods during the development. However, the experimental research and development with the proposed model is at an early stage. Moreover, much more research efforts are needed to develop more stable TMO-based real-time agent framework.

We will adapt the proposed model to develop a tsunami detecting system in the future research.

Acknowledgement

This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment).

References

1. TMOSL_v4.0_manual_draft <http://dream.eng.uci.edu/TMOdownload/>
2. Kim,K.H, "APIs for Real-Time Distributed Object Programming", IEEE Computer,June 2000,pp.72-80
3. K.H.(Kane) Kim, Juqiang Liu, Masaki Ishida and Inho Kim.: "Distributed Object-Oriented Real-Time Simulation of Ground Transportation Networks with the TMO Structuring Scheme" , Proc. COMPSAC '99 (IEEE CS Computer Software & Applications Conf.), Phoenix, AZ, Oct. 1999, pp.130-138.
4. Kim, K.H., "Real-Time Object-Oriented Distributed Software Engineering and the TMO Scheme", Int'l Jour. of Software Engineering & Knowledge Engineering, Vol. No.2, April 1999, pp.251-276.
5. Kim, K.H., "Object Structures for Real-Time Systems and Simulators", IEEE Computer, August 1997, pp.62-70.
6. Douglas Schmidt, Fred Kuhns, "An overview of the Real-time CORBA Specification", IEEE Computer special issue on Object-Oriented Real-time Distributed Computing, June 2000, pp.56-63.
7. Real-Time for Java Experts Group, "Real-time Specification for Java, Version 0.9.2," 29 Mar. 2000, <http://www.rtfj.org/public>.

Design Trade-Offs and Power Reduction Techniques for High Performance Circuits and System

Taikyeong T. Jeong* and Anthony P. Ambler

Department of Electrical and Computer Engineering,
University of Texas at Austin, Austin, TX 78712-1014 USA
{ttjeong, ambler}@mail.utexas.edu

Abstract. This paper presents a novel low power design methodology for dynamic CMOS circuits in order to improve the design trade-off between power and speed. It also discusses a new design methodology of power reduction techniques for high-performance chips. As confirmed through the experiment, we are maximizing the performance of the chip in terms of speed and power. The simulation results of the proposed method are compared and possible improvements and applications are discussed.

1 Introduction

The importance, and amount, of low power and high speed CMOS circuit designs are increasing due to advances in modern semiconductor design technology. These days, low power and high speed circuits are currently becoming more important in the semiconductor area, as well as in the mobile communication field. Methods to improve the power vs. speed trade-off can be considered either at the design process or at the chip-level design integration. Of particular relevance to this research is how power dissipation has increased due to the increasing clock frequency and integration levels of high performance designs. For high performance operation, dynamic CMOS circuits have been used in many high-end processor designs where circuit speed is more important than other design factors [1]. Therefore, the domino logic is inevitable for arithmetic and other circuits involving complex gates with high fan-in and fan-out, in spite of the limitation that its nature consumes high energy [4]. In this paper, we have developed a logic that has low leakage consumption with fast logic characteristics. Using this design methodology, we will present results showing a significant reduction in power consumption; a unique opportunity in the area of logic design.

2 Power and Energy Reduction Techniques

Power dissipation has become the higher priority/leading design constraints, on par with performance. It should be noted that dynamic power dissipation

* T. Jeong is now with the University of Delaware under the research grants of NASA (No. NNG05GJ38G), Newark, DE USA. Tel.: +1-512-786-6402. email: ttjeong@alumni.utexas.net.

is a linear function of the clock frequency; however, simply reducing the frequency would significantly diminish the overall performance [1]. Thus the reduction of clock frequency would be a variable option only in cases where overall throughput of the system can be maintained by other means. Additional dynamic power savings can be achieved by scaling the clock distribution, supply voltage, capacitance, and low power level integration that includes power reduction techniques. Another power problem highlighted by the power reduction is the increase in static power dissipation because of threshold voltages and integration levels. Device threshold voltage is scaling at a lower rate than supply voltage to maintain acceptable sub-threshold characteristics and noise immunity; but, a competing need for high drive current, which depends on $V_{DD} - V_t$, forces lower threshold voltages and higher source/drain leakage currents. Gate leakage currents are also increasing as the oxide under the gate thins [6]. We will demonstrate a new cascaded low power logic design technique (also called, Low Power Domino logic) in the area of power reduction techniques.

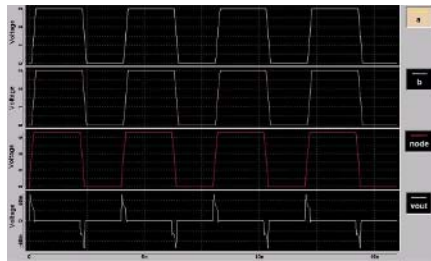
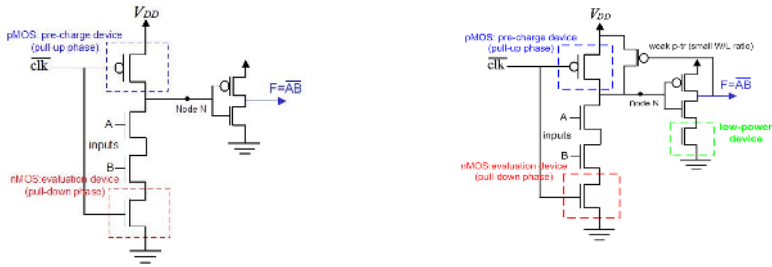


Fig. 1. Waveforms of dynamic circuit implementation

Figure 1 shows a simulated low power circuit waveform, comparing a dynamic circuit with a low power design. Two inputs at the top of the waveform (“a” and “b”) are viewed against the bottom two waveforms, which are associated with the fluctuated output voltage. Conversely, conventional domino logic has a generic node factor (node) and shows a sufficient delay interval from clock to node [5]. It also includes short channel behavior, no latch-up, and fewer mask steps than bulk silicon processing while providing high-speed. To demonstrate the benefit on design methodology, a power efficient logic circuit with interconnection architectures and logic options are demonstrated. Furthermore, a new cascaded low power cell, Low Power Domino (LPD) logic, and its corresponding connections are compared with the original logic.

3 Low Power Design in Dynamic CMOS Circuits

A novel design, the cascaded low power (LPD) cell, is an efficient logic circuit that achieves energy saving through dynamic CMOS circuitry.



(a) A conventional domino logic of latched version (b) A schematic view of low power cell

Fig. 2. A structure of low power domino version for power reduction techniques

A structure of low power domino latched version, which included low power device is shown in Figure 2 (a) and (b), respectively. It should be noted that some logic include pMOS, which has a small W/L ratio and different threshold voltages at the node N. Also, there is sub-threshold and reverse biased leakage in the transistor that we put use a changed threshold voltage [3]. At the end, the output voltage (V_{out}) has a small amount of power saving in standby mode and higher output than conventional logic. After implementation of the proposed design circuit, LPD logic can provide greater power and delay savings than conventional cascade logic. It also includes logic configurations, temperature management, and a power efficiency system. We demonstrate that the proposed circuit is a key design of high-performance design and it appears to be able to get the same performance as existing interconnection networks and still achieve the low-power consumption, i.e., exhibiting high-performance design traits. Figure 3 and 4 show the timing and voltage operations of LPD logic, which is implemented with NAND gates.

During the active mode, LPD logic has the pre-charge device signal which is driven above the supply voltage, the dynamic node that degrades to ground, and the low-power device signal which is driven below the ground. Consequently, when the clock is low, V_{out} is high in standby mode, but the low-power device is a little below the ground line. It occurs because of low leakage and is reduced by an order of magnitude. Although it has a small impact on the logic operation, it highly affects the overall performance. This limitation seems to undermine all the other advantages of the circuit, such as low power dissipation, and sensitivity on noise margin. Furthermore, the leakage during standby mode may be reduced by an order of magnitude with little impact on the active operation speed. In this case, the dynamic node pre-charge phase, rather than being held at V_{DD} , is driven above V_{DD} by either a separate supply voltage or a voltage derived locally. The increased voltage on the gate of the pMOS significantly reduces the leakage through the pMOS and the nMOS discharge devices. At the same time, during the sleep mode, nMOS is driven below the ground V_{SS} rail in a manner similar to the pre-charge pMOS derived voltage limitation. This has demonstrates that

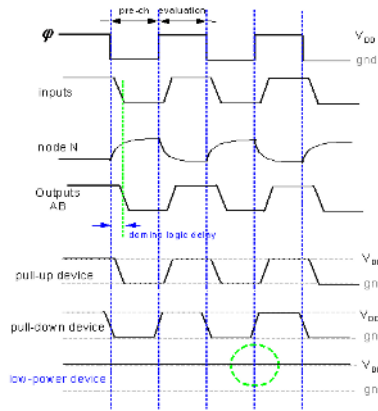


Fig. 3. Timing diagram of low-power domino (LPD) cell in active mode

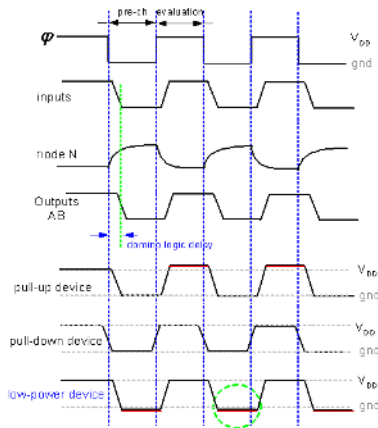


Fig. 4. Timing diagram of low-power domino (LPD) cell in standby mode

a low power device can operate with notable power savings when it has been connected to similar cascaded logic.

4 Simulation and Results

The simulation results from low-power domino (LPD) cascaded logic express significant power/energy savings using these techniques with minimal impact on logic size. In addition, it could be verified in hardware through functional verification of chip design.

Figure 5 shows a detailed comparison of the original logic cells to the low-power domino (LPD) cascade logic cell. It can be observed that there is a trend

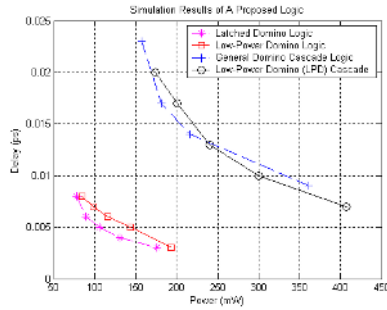


Fig. 5. Final comparison results of low-power domino (LPD) cascaded cell

of power saving on the “Low-Power Domino Cascade” line which overlaps the “General Domino Cascade” line. As power increases past $240mW$, we observe that the LPD logic consumes the same amount of power, while realizing a delay reduction of approximately 18%. On the other hand, considering a fixed delay, we observed a reduction of $25mW$ - $30mW$ power dissipation (see Fig 5). These results confirm that the “Low-Power Domino Cascade” method has an advantage over “General Domino Cascade” method in overall system performance.

5 Conclusions

As modern digital chips and systems become more complex, the implementation of low power and high performance are important design goals. Maximizing the architectural characteristics such as speed and bandwidth, while minimizing power, places an enormous demand on design technology. In this paper, we have introduced a novel design methodology by providing a fast logical propagation method with low power consumption. Furthermore, simulation results of Low-Power Domino (LPD logic) cascade logic design options have demonstrated a savings of static power dissipation. By using the low power dissipation methodology, the lowering of the voltage scaling is not necessary during signal integration. We have also presented the modeling of nonlinear circuits using an adaptive Low-Power Domino (LPD logic) cascade logic design method, which could serve as a better substitute for dynamic circuit design, without losing system performance. Better understanding of the effects of power efficiency can be used to develop accurate low power design methodologies, which can be applied to future design technology. As our design and simulation results have shown, this low power dissipation methodology can be beneficial to a myriad of circuit designs.

Acknowledgment

The author would like to thank the referees for their valuable comments.

References

1. P. Hofstee, N. Aoki, and et. al., "A 1.0 GHz single-issue 64-bit PowerPC processor," *Proc. of ISSCC*, pp. 30-31, 186-187, Feb 1998; pp. 230-231, 1998; vol. 33, pp. 1600-1608, 1998
2. H. Ngo and G. Carpenter, "Low-power phased locked loop concept and system," *27th Annual Int'l. Symp. on Computer Architecture*, pp. 83-94, Vancouver, BC, Canada, Sep 10-14, 2001.
3. T Jeong and A. Ambler, "Power efficiency system for flight application (PESFA) mission: Low power dissipation in digital circuit design for flight application/space communications," *IEEE Tran. on Aerospace and Electronics Systems*, vol 42, 2006
4. F. Herzel, H. Erzgraber, and N. Ilkov, "A new approach to fully integrated CMOS LC-oscillators with a very large tuning range," *CICC*, pp. 573-576, May 2000
5. E. Leobandung, and et. al., "A new approach to fully integrated CMOS LC-oscillators with a very large tuning range," *Proc. of IEDM*, pp. 403-406, Dec 1998
6. N. Zamdmer, and et al, "A 0.13- μm SOI CMOS Technology for Low-Power Digital and RF Applications," *IEEE International Solid-State Circuits Conference (ISSCC'94)*, Washington, 1994

Cavitation Flow Analysis of Axisymmetric Bodies Moving in the Water

Changjin Lee and Doyoung Byun

Dept. of Aerospace Engineering,
Center for Advanced e-System Integration Technology, Konkuk University,
1 Hwayang-Dong, Kwangjin-Gu,
Seoul 143-701, Korea
{cjlee, dybyun}@konkuk.ac.kr

Abstract. This study aims to analyze the turbulent cavitating flow on the axisymmetric bodies moving in the water by using the incompressible two phase flow calculation. A program is developed with a pressure based SIMPLE algorithm and $k-\varepsilon$ turbulent model implemented by wall function. A volume of fraction (VOF) method is used to capture the boundary between fluid and gas phase and the model for bubble production and depletion is also modeled and applied to represent the cavitation phenomena. SIMPLE algorithm is extended to simulate the compressible flow as well as two phase flow. Comparisons of calculation results show very good agreement with previous studies and verify the code validity. For a projectile with a hemispherical head form at the cavitation number (σ) of 0.4, the pressure coefficient C_p agrees pretty well with previous results by Shyy et al. Also another calculation with conical head form at $\sigma=0.5$ provides a good agreement with the results by Kunz et al. After the validation study, effect of cavitation on drag force is investigated. The drag force coefficient on the surface increases at the condition of cavitation.

1 Introduction

It is well known that cavitations are very commonly observed in the flow downstream from screw of ship, around the moving projectile in the water and in the flow with a large pressure gradient. The result of the inception and depletion of cavitation generates unwanted problems during the flow analysis such as pressure oscillations, noise, and structure erosion due to severe pressure oscillation. Also, the inception of cavitation can strongly influence the pressure distribution on the moving bodies. Thus, many studies have been conducted to analyze the characteristics of cavitation flow both in experiments and CFD (computational fluid dynamics). Especially it is also true that the code developments by using CFD technique has been tough tasks due to the inception of cavitation bubble and complicate natures between turbulence and cavitation in two phase flow. And the amorphous boundary between liquid and gas phase should be clearly captured and taken into account as well in the analysis code.

Many efforts has been tried to analyze two phase flow including cavitation bubble by various methods. Shyy et al. [1-3] suggested a pressure-based algorithm in calculating cavitation flow, and Kunz et al. [4-6] calculated super-cavitation flow incorporated with density-based algorithm and preconditioning method in order to account for compressible feature of the flow. Also, they used a volume fraction transport equation to model and to define boundary between liquid and gas phase. In addition, Chen et al. suggested a wake model to include two phase feature in the flow [7-8]. And multi-fluid model was implemented by Owis et al. [9] for cavitation analysis. It should be noted that these researches had been extended the understanding of cavitation phenomena and results to add new applications of hydrofoil, internal flow of venture tube, and etc.

This study aims to develop a CFD program to study the characteristics of cavitation flow around moving body in the water with accounting for compressibility effect of gas phase. The pressure-based SIMPLE algorithm is extended to compressible flow and applied to cavitation flow with volume of fluid(VOF) method.

2 Governing Equations and Modeling

A couple of modeling has been implemented with governing equations; continuity, momentum equations, and volume fraction transport equation in the Cartesian coordinate system. These are in the conservative form as,

$$\begin{aligned} & \frac{\partial}{\partial t} \int_V \rho_m dV + \int_S \rho_m \vec{v} \cdot \vec{n} dS = 0 \tag{1} \\ & \frac{\partial}{\partial t} \int_V \rho_m \vec{v} dV + \int_S \rho_m \vec{v} \vec{v} \cdot \vec{n} dS = \int_S \vec{T} \cdot \vec{n} dS + \int_V \rho \vec{b} dV \tag{1} \\ & \frac{\partial}{\partial t} \int_V \alpha_l dV + \int_S \alpha_l \vec{v} \cdot \vec{n} dS = \int_V (\dot{m}^- + \dot{m}^+) dV \\ \text{where, } & T_{ij} = - \left(p + \frac{2}{3} (\mu + \mu_l) \frac{\partial u_j}{\partial x_j} \right) \delta_{ij} + (\mu + \mu_l) \left(\frac{\partial u_i}{\partial x_j} + \frac{\partial u_j}{\partial x_i} \right) \\ & \rho_m = \rho_l \alpha_l + \rho_v (1 - \alpha_l), \quad \mu_l = \frac{\rho_m C_\mu k^2}{\varepsilon} \\ & \vec{b} = \text{body force} \end{aligned}$$

A mixture density is defined by the linear summation of liquid density and vapor density associated with volume fraction coefficient, α_l .

2.1 Cavitation Modeling

The inception of cavitation in the flow is governed by the interaction of thermodynamic changes associated with phase transformation. So it is appropriate to use the balance of cavitation production and destruction in the flow and each part denotes the evaporation and condensation of liquid generated by various density gradients in the flow. It should be noted that buoyancy and surface tension are generally negli-

gibly small compared to Weber and Froude number effect. The contribution of evaporation and condensation in the flow can be denoted by two empirical constants such as C_{prod} and C_{dest} proposed by Kunz et al. Also, two different constants used in the volume fraction equation can be written as,

$$\begin{aligned} \dot{m}^- &= \frac{C_{dest} \rho_v \alpha_l \text{MIN}[0, p - p_v]}{\rho_l \left(\frac{1}{2} \rho_l U_\infty^2 \right) t_\infty} \\ \dot{m}^+ &= \frac{C_{prod} \rho_v \alpha_l^2 (1 - \alpha_l)}{\rho_l t_\infty} \end{aligned} \tag{2}$$

Here the time scale t_∞ in the volume fraction equation is defined by the ratio of characteristic length to reference velocity (ℓ/U). Also two empirical constants C_{prod} and C_{dest} are 9×10^5 , 3×10^4 respectively and the density ratio between liquid and vapor is assumed as 1000.

2.2 Turbulence Modeling

A conventional turbulence model $k-\epsilon$ was used and table 1 shows coefficients used in the turbulence modeling. And the wall function was used in the flow calculation to account for the interaction between turbulent region and viscous region.

Table 1. Turbulent model coefficients

	C_μ	C_1	C_2	σ_k	σ_ϵ	σ_h	σ_i
k-ε model	0.09	1.4	1.92	1.0	1.3	0.9	0.9

2.3 Numerical Methods

FVM method is the major differencing technique in the numerical calculation. And the collocated grid system can also be used for the allocation of velocity components u , v and dependent variables. The calculation utilizes SIMPLE algorithm and convective terms can be differenced by upwind scheme in the grid system. A generalized equation for governing equations becomes

$$\frac{\partial(\rho\phi)}{\partial t} + \text{div}(\rho\vec{U}\phi) - \text{div}(\Gamma_\phi \text{grad}\phi) = S_\phi \tag{3}$$

After applying FVM to a generalized equation, it becomes

$$\frac{\partial}{\partial t} \int_V \rho\phi dV + \int_S \rho\phi\vec{U} \cdot \vec{n} dS = \int_S \Gamma_\phi \text{grad}\phi \cdot \vec{n} dS + \int_V S_\phi dV \tag{4}$$

where ϕ represents dependent variables, Γ is diffusion coefficient, S_ϕ is source term, S means control surface area, and V is control volume, respectively. Fig. 1 shows a generalized control volume and notations used in the flow analysis.

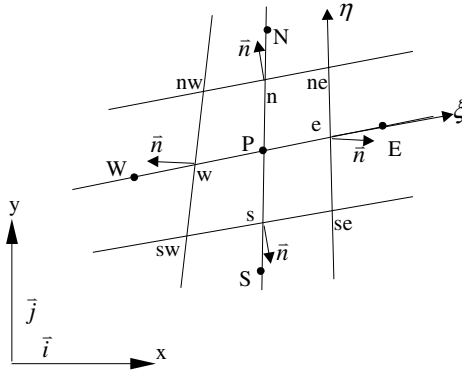


Fig. 1. Schematic of control volume and notations

As shown in the figure, mass flux on surface “e” can be calculated in the collocated grid system as below

$$\dot{m}_e = \int_{S_e} \rho \bar{U} \cdot \bar{n} dS \approx (\rho \bar{U} \cdot \bar{n})_e S_e = \rho_e (S^x u + S^y v)_e \tag{5}$$

And convective flux and diffusion flux of dependent variables are written respectively as,

$$F_e^c = \int_{S_e} \rho \phi \bar{U} \cdot \bar{n} dS \approx \dot{m}_e \phi_e \tag{6}$$

$$F_e^d = \int_{S_e} \Gamma \text{grad} \phi \cdot \bar{n} dS \approx (\Gamma \text{grad} \phi \cdot \bar{n})_e S_e$$

FVM method is popular in calculating flow field associated with collocated grid system. And a SIMPLE [10] algorithm is implemented in this study as one of the FVM scheme for differencing the governing equation. Thus, final difference equation at “p” becomes a simple algebraic equation accounting for the flux balance between four directions and source as,

$$A_P^\phi \phi_P = A_E^\phi \phi_E + A_W^\phi \phi_W + A_N^\phi \phi_N + A_S^\phi \phi_S + b_\phi \tag{7}$$

2.4 Pressure Correction Equation

The solution of pressure and velocity may show an unphysical oscillation due to the use of collocated grid system and should be treated by using interpolation in the momentum equation to avoid oscillation. Below is the difference equation.

$$A_p^{\bar{u}} \bar{u} = \sum A_{nb}^{\bar{u}} \bar{u}_{nb} - V_p (\nabla_d P)_p + b_p \tag{8}$$

It is worth noting that $A_p^{\bar{u}}$ and $A_{nb}^{\bar{u}}$ in the equation are coefficients associated with convective and diffusion terms at center and neighbor cell. Here V_p is a cell volume,

b_p denotes source term. And difference equation can be transformed with corrected pressure as below because of the implementation of predictor-corrector method.

$$A_p^{\bar{u}} \bar{u}^* = \sum A_{nb}^{\bar{u}} \bar{u}_{nb}^* - V_p (\nabla_d P^*)_p + b_p \tag{9}$$

And another interpolation is required to correct velocity components by considering velocity and pressure distribution of neighbor cells. The following relation is the equation for correction.

$$\bar{u}' = \bar{u} - \bar{u}^* = -D_p (\nabla_d P')_p \tag{10}$$

Here D_p is a matrix defined as,

$$D_p = \begin{bmatrix} V_p / A_p^u & 0 & 0 \\ 0 & V_p / A_p^v & 0 \\ 0 & 0 & V_p / A_p^w \end{bmatrix} \tag{11}$$

Also, pressure correction is needed by using continuity equation expressed in terms of corrected velocity.

$$\nabla_d \cdot (\rho D_p \nabla_d P') = \nabla_d \cdot (\rho \bar{u}^*) \tag{12}$$

In the cavitation model, two competitors of production and destruction of cavitation represent density field of the flow which depends on the velocity distribution. Thus, density is coupled with pressure in the two phase flow and the pressure correction equation should be reconsidered in the density calculation. And mass flux can be expressed in terms of corrected velocity, pressure, and density as shown below.

$$u = u^* + u', \quad p = p^* + p', \quad \rho = \rho^* + \rho' \tag{13}$$

$$\rho \bar{u} = (\rho^* + \rho') (\bar{u}^* + \bar{u}') = \rho^* \bar{u}^* + \rho^* \bar{u}' + \rho' \bar{u}^* + \rho' \bar{u}'$$

Here, m and m^* represents the numbers of calculation order. And density correction can be done with the equation as,

$$\rho' = C(1 - \alpha_l) P' \tag{14}$$

Here C is an arbitrary constant and determined by experiences as the order of $O(1)$ since larger value of C makes unstable convergence feature during the calculation.

3 Boundary Conditions and Grid System

The entrance conditions in the calculation include velocity components, and turbulence intensity. And the outlet conditions consist of pressure, velocity, and zero gradient condition. Also, no-slip condition was implemented on the body surface. It should be noted body shapes are both hemispherical and conical head forms used in the experiments conducted by Rouse, and McNown [11]. Fig. 2 and Fig. 3 are grid

systems used for the calculation of hemispherical shape and conical shape, respectively. Each body length for the calculation is ten times of diameter and grid points are concentrated near stagnation and expansion region in order to capture vapor bubble inception.

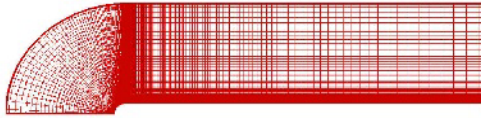


Fig. 2. Grid system for hemispherical shape calculation (170x70)

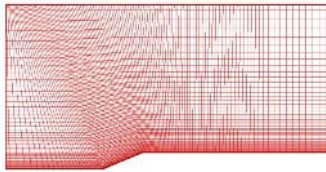


Fig. 3. Grid system for conical shape calculation (120x50)

4 Results

To verify the developed calculation code, numerical calculations are conducted for bodies with hemisphere and cone head at the condition of $Re=1.36 \times 10^5$ for the case without and with cavitation, respectively.

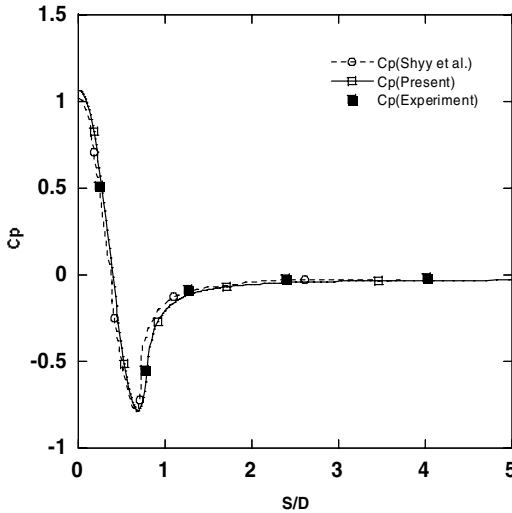


Fig. 4. Calculation result of C_p on the body surface with hemispherical head at $\sigma = 1$

Fig. 4 and Fig. 5 show the comparison of pressure coefficients with results by Shyy[1] and Kunz et al.[5] for the case without cavitation. Pressure distribution along the body surface agrees quite well with experimental results and that by Shyy et al.

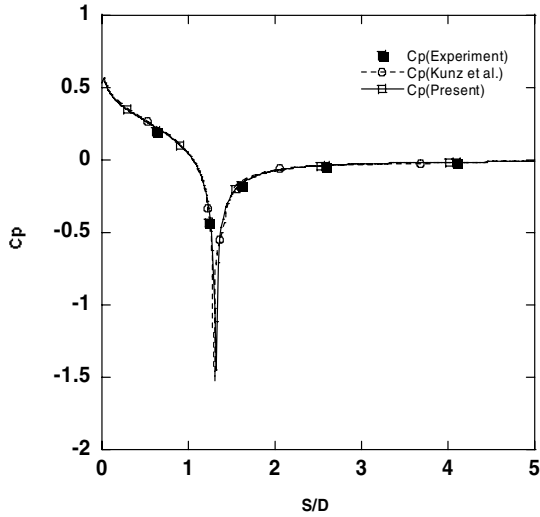


Fig. 5. Calculation result of C_p on the body surface with conical head at $\sigma = 1$

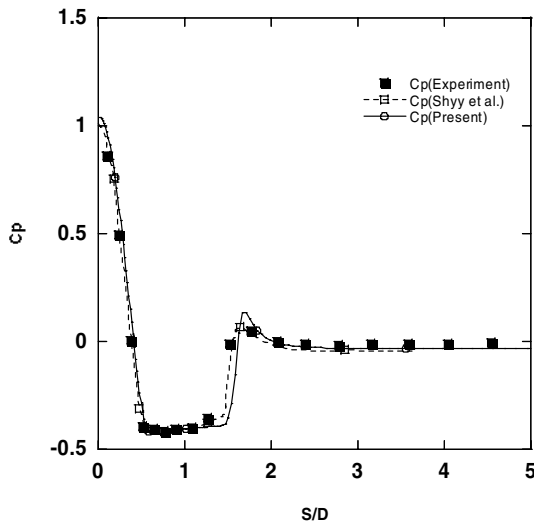


Fig. 6. Calculation result of C_p on the body surface with hemispherical head at $\sigma = 0.4$

Calculations have conducted to predict the inception of cavitation bubble and to predict cavitation reattachment on the surface at the condition of $\sigma = 0.4$ and 0.5 for hemisphere and cone head objects, respectively. Fig. 6 and Fig. 7 show the pressure

coefficients distributions along the surfaces compared with the experimental and the previous results. And it was revealed that pressure coefficient along the surface can predict the cavitation near expansion region and shows a quite good agreement with the experimental results. However, it is found that there is a little undershoot at the cavitation point and overshoot at the reattachment point. This seems to be attributed by the schemes adopted in the calculation; upwind scheme having first order of accuracy.

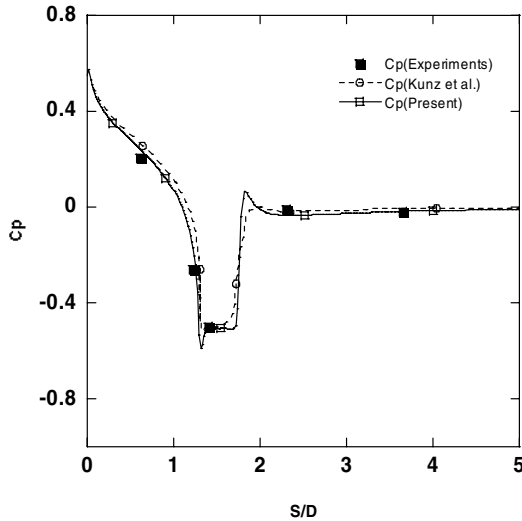


Fig. 7. Calculation result of Cp on the body surface with conical head at $\sigma = 0.5$

Using the developed program, effect of cavitation on drag force is predicted for the hemisphere head object moving at the speed of 25 m/s at the condition of $Re = 6.975 \times 10^6$, $\sigma = 0.638$, vapor pressure = 0.61 kPa, and the ambient pressure 2 atm, respectively. Drag coefficient is 7.6987×10^{-3} which is 5.1% larger than the case without cavitation. Because of the gas bubble on the surface near the head, the pressure drag force increases rather than decrease of the skin friction drag force.

5 Conclusions

A pressure-based method is implemented for cavitating flow computations and single-fluid Navier–Stokes equations with a volume fraction transport equation, are employed. For a projectile with a hemispherical head form at the cavitation number(σ) of 0.4, the pressure coefficient Cp agrees pretty well with previous results by Shyy et al. Also another calculation with conical head form at $\sigma = 0.5$ provides a good agreement with the results by Kunz et al. The drag force coefficient on the surface increases at the condition of cavitation.

References

1. Senocak, I., Shyy, W.: A Pressure-Based Method for Turbulent Cavitating Flow Computations. *J. of Comp. Physics*, 176 (2002) 363-383
2. Wang, G., Senocak, I., Shyy, W., Ikohagi, T., Cao, S.: Dynamics of attached turbulent cavitating flows. *Progress in Aerospace Sciences*, 37 (2001) 551-581
3. Vaidyanathan, R., Senocak, I., Wu, J., Shyy, W.: Sensitivity Evaluation of a Transport-based Turbulent Cavitation Model. AIAA-2002-3184 (2002)
4. Kunz, R. F., Boger, D. A., Stinebring, D. R., Chyczewski, T. S., Gibeling, H. J.: A Preconditioned Navier-Stokes Method for Two-Phase Flows with Application to Cavitation Prediction. AIAA-99-3329 (1999)
5. Kunz, R. F., Boger, D. A., Stinebring, D. R., Gibeling, H. J.: Multi-phase CFD Analysis of Natural and Ventilated Cavitation about Submerged Bodies. FEDSM99-7364, 3rd ASME/JSME Joint Fluids Engineering Conference (1999)
6. Kunz, R. F., Lindau, J. W., Gibeling, H. J., Mulherin, J. M., Bieryla, D. J., Reese, E. A.: Unsteady Three-Dimensional Multiphase CFD Analysis of Maneuvering High Speed Supercavitating Vehicles. AIAA 2003-841, 41st Aerospace Sciences Meeting and Exhibit, January (2003)
7. Chen Y., Heister, S. D.: A Numerical Treatment for Attached Cavitation. *J. of Fluids Engineering*, 116 (1994) 613-618
8. Chen Y., Heister, S. D.: Two-phase Modeling of Cavitated Flows. *Computers & Fluids*, 24 (1995) 799-809
9. Owis, F. M., Nayfeh, A. H.: A compressible Multi-phase Flow Solver for the Computation of the Super-Cavitation over High-speed Torpedo. AIAA-2002-0875, 40th AIAA Aerospace Sciences Meetings & Exhibit (2002)
10. Ferziger, J. H., Peric, M.: *Computational Methods for Fluid Dynamics*. 2nd ed. Springer Verlag, Berlin (1999.)
11. Rouse, H., McNown, J. S.: Cavitation and Pressure Distribution, Head Forms at Zero Angle of Yaw. *Studies in Engineering, Bulletin 32*, State University of Iowa (1948)

Design and Implementation of Semantic Web Search System Using Ontology and Anchor Text*

Nam-deok Cho¹ and Eun-ser Lee²

¹ Chung-Ang University, 221, Huksuk-Dong, Dongjak-Gu, Seoul, Korea
ndcho@softcamp.co.kr

² Soong Information & Media Technology Institute, Soongsil University
eslee1@ssu.ac.kr

Abstract. The World Wide Web has incurred the problem that users are not necessarily provided with the information they want to receive, at a time when the amount of information is explosively increasing. Therefore, W3C (World Wide Web Consortium) proposes the Semantic Web as the new web paradigm to present semantic information and study browser systems that use ontology to perform their tasks. However, these systems do not necessarily provide correct information, particularly when users are trying to show relevant information, or information they are not familiar with. Therefore, the authors of this paper propose that the Semantic WebGraph system should be used to present semantic information, using ontology to query language, and also to show relevant information using Anchor Text in web pages. Such a system forms a Semantic Web base search engine that can get relevant information, as well as information about queried language.

1 Introduction

The World Wide Web, which was introduced by Tim Berners-Lee in 1989, has brought an Internet revolution in the late 20th century. It is extremely convenient, but there has been an explosive increase in supply of information that users do not want to receive. Therefore, the W3C proposes that the Semantic Web be used to help overcome this problem[1]. The Semantic Web is defined to give clear meaning and definition to information exposed in the web, and involves extension of the web so as to enable people to work in cooperation with computers[2][3]. To show semantic information that is well defined for users according to this paradigm a study of a browser system using ontology needs to be achieved[4][6].

However, these systems do not necessarily provide correct information, particularly when users are trying to show relevant information, or information they are not familiar with. In this paper it is proposed that the Semantic WebGraph system be used to show semantic information, using ontology to query language, as well as presenting relevant language using Anchor Text in web pages. Because the Semantic WebGraph shows the relationship between queried and relevant language graphically, users can understand meaning intuitively.

* This work was supported by the Soongsil University Research Fund.

In this paper relevant language does not mean words related to queried language through lexical meaning. Even if meaning does not connect lexically, language can be deemed relevant if language contained in the web page is related to the language being queried. For example, if queried language is "aids", and "sickness" and "hospital" are extracted for relevant language, "sickness" may be only relevant language. But, for the purpose of this paper, "hospital" is also relevant if it is contained in a web page about hospitals which gives information about the symptoms of AIDS and its curative means. Anchor text is an important element for extracting this relevant language. This paper is composed of 5 chapters. Chapter 2 discusses the Semantic Web, Ontology and Anchor Text etc., and chapter 3 describes the design and implementation of the Semantic WebGraph. Chapter 4 shows the results of the Semantic WebGraph along with its estimates, while finally chapter 5 concludes the paper.

2 Base Study

2.1 Semantic Web

Tim Berners-Lee defines the Semantic Web as follows:

"The Semantic Web is an extension of the current web in which information is given well-defined meaning, better enabling computers and people to work in cooperation." [3]

The ultimate purpose of the Semantic Web is to develop the standard of technology that can help computers to better understand web information, and to support semantic search, data integration, navigation and task automation etc. When such things are described in detail the Semantic Web should enable the following work:

- When searching information, the bringing of more correct information.
- Integration and comparison of information from different alloplasm sources.
- Correlation of meaningful descriptive information about certain resources.
- The attachment of detailed information on the web for the automation of web services.

To demonstrate the points that can improve the current web, the hierarchical structure of the Semantic Web is given in Fig. 1 below.

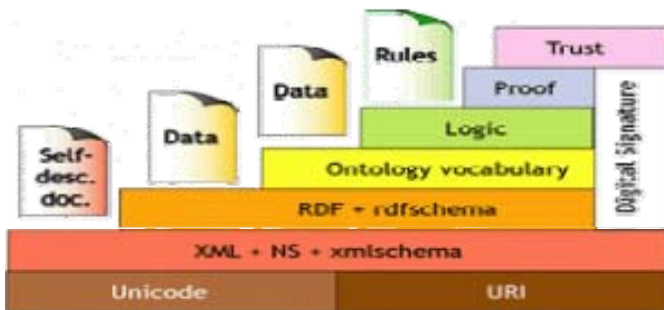


Fig. 1. Hierarchical structure of Semantic Web

The lowest floor of the hierarchical structure consists of a URI (Uniform Resource Identifier) and a Unicode, which addresses the method with which to access the resources of the web protocol. The next floor contains the XML (eXtensible Markup Language) along with the namespace that can define this concept in modular terms. RDF (Resource Description Framework) and RDF schema, describing resources, are located on the next floor. Ontology is located on the fourth floor, and technological elements pertaining to law, logic, proof etc. are located in hierarchies above this.

2.2 Ontology

Gruber defines ontology as follows:

“An ontology is a formal, explicit specification of a shared conceptualization of a domain of interest. ‘Conceptualization’ refers to an abstract model of phenomena in the world by having identified the relevant concepts of those phenomena. ‘Explicit’ means that the type of concepts used, and the constraints on their use are explicitly defined. ‘Formal’ refers to the fact that the ontology should be machine readable. ‘Shared’ reflects that ontology should capture consensual knowledge accepted by the communities.”[7] If this definition is considered in detail it is necessary to view the following sub-components.

Conceptualization: This is an abstracted model to aid thinking. It generally involves the discussion relevant to localized specific fields.

Explicit specification: Defines constraints explicitly, relevant to their form or concept use.

Formal: Machines must be able to understand Ontology, and the existence and standardizations of relevant steps.

Shared: Ontology is a concept that requires all of the group members to display agreeing concerted knowledge that is not necessarily limited to individuals.

Ontology is a very important element that enables knowledge processing, sharing and reuse among web-based application programs. Class classification and definitions of inference rules are included in Ontology. Class classification defines the class and subclass of objects, and the relationship between them. For example, “address” can be defined as a location’s subclass because “address” is a subclass of “location”. Because city codes can be applied only to location, city codes’ subjects must always be the object of the location class.

2.3 Anchor Text

Hyperlink consists of the link (URL) referred to in the web document, and Anchor Text is used to describe simple representations. Between these, Anchor Text does not sensibly describe entirely unrelated substances as information in ways that a web document writer can describe directly in order to provide useful information that a person can directly summarize from a web page. Anchor Text has the following special qualities.

Summarization: Anchor Text has the special quality of being able to summarize the contents or subject of a web document. A third party, who is not necessarily the writer of web documents, is able to describe a web document’s contents more clearly by using Anchor Text, rather than considering the document itself directly.[8][9].

Universality: All general web pages include hyperlink as an essential ingredient. Fundamentally, users can not search web documents if they do not contain hyperlink.

2.4 Related Work

2.4.1 WebGraph

WebGraph is a search engine that can easily search information that users want, using information links between web pages and concept graphs schematized through user's query language[9][10][11]. This search engine introduces concept-based search techniques. Concept-based search is a search method that can extend searches by analyzing the meaning of words and using the concept of word relation. Therefore, this method is similar to a person's thinking, and it can be very effective. Also, this system uses hyperlink information to extract keywords.

2.4.2 MagPie

MagPie is a plug-in program of Internet Explorer. It is a Semantic Web browsing system that shows semantic information using ontology that can speak as the most important element of the Semantic Web. Basically, it is an Active X control program, and when it is consented with a word in a suitable domain, shows semantic information of the words the user wants.[4][5]

3 Design and Implementation

The Semantic WebGraph System consists of an Ontology Maker that creates ontology, a Spider that collects web documents and stores them in databases, and Indexer that extracts keywords on the basis of database contents, keyword indexes and URLs, Query Engines that process query language and relevant language that users want, and Visualization directly to the user (Fig.2).

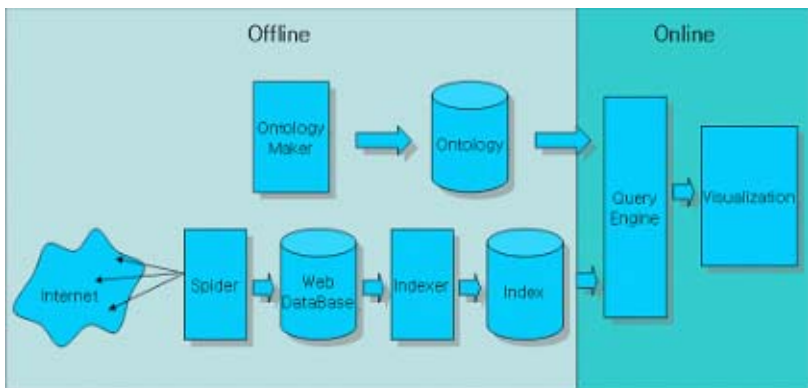


Fig. 2. System Configuration

Whole systems are divided into Off-line Batch Job parts and On-line Processing parts. The Off-line Batch Job part composes ontology in connection with query language, and carries out construction of the index file system in connection with relevant language. The On-line Processing part shows semantic information using ontology

about users' query language or URLs of web page about relevant language using index file system. In this paper our system uses a graph to aid users' visualization.

3.1 Ontology Maker

This is the part that composes ontology. Ontology is used by the background information of query language. That is, users of the web show semantic information by using Ontology that has pre-definitions of query language. Ontology is mainly composed in limited specific domains, and this paper also considers ontology in the medical domain. Ontology is referred to in instances of name and class, and such instances can have more than one representation in terms of vocabulary. For example, where there is an instance called "Cho Nam-Deok" this instance includes "Nam-Deok Cho", "Nam-Deok c" and "C Nam-Deok" ? from an ontological perspective. That is, in the above instance, these expression meanings would be used commonly in Ontology.

3.2 Spider

The Spider's role is to bring storage of the web document to database. Stored information requires the URL of the web document, its title, the sample text (255 letters), and hyper link connection relations. The operation method involves a visit from the URL stored in the database that is connected with hyperlink by way of BFS (Breadth First Search) and collects web documents. Operation environment acts through the Win32 platform and uses MFC. Access is used as the database, and uses the DAO engine.

1. Input URL in queue to begin initially
2. Visit queue's URL by BFS.
3. Store Anchor text of hyperlink by visiting web document.
4. stores in queue if URL of hyperlink is a new thing, and does not store otherwise.
5. Repeat until 2-4 successfully completed.

Fig. 3. Spider Algorithm

3.3 Indexer

It is the program that constructs the index file system for actualizing relevant language searches from databases consisting of web documents and hyper link information. A lot of times frequent joining is required, as well as selection if SQL sentences have been used in the actual search service. Another problem is that a lot of information repetitions occur in the database when saving hyper link information. Therefore, unique indexes are constructed to reduce these. The architecture of this program consists of a URL index along with an index of keywords in an attempt to make the approach to hyperlink information easy and fast. The URL index table extracts

information for the URL when the URL is specified, and this can simply be done by using the hash function. The keyword index table stores information of the keywords' numbers for the whole document, and lists the URLs for the whole document when keywords are given, and it is created by way of the following algorithm.

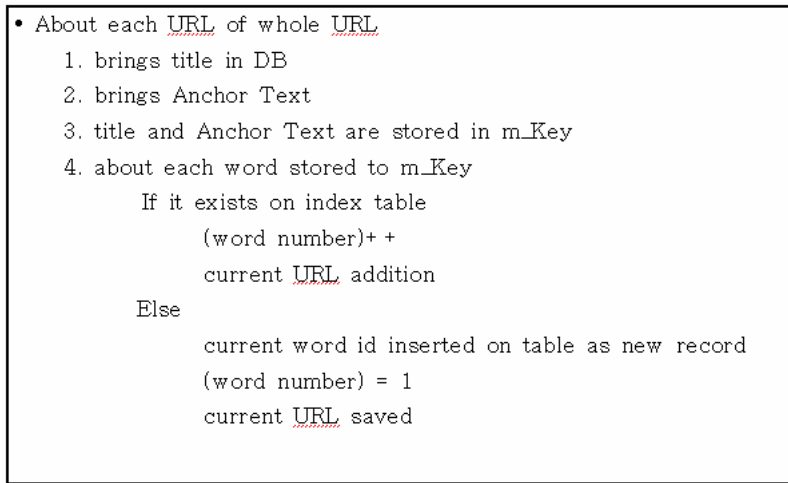


Fig. 4. Indexer Algorithm

3.4 Query Engine

Query Engine is a program that processes query language and relevant language that the user actually wants. It shows information in ontology to show information about query language, and shows URL in an index table to show information about relevant language.

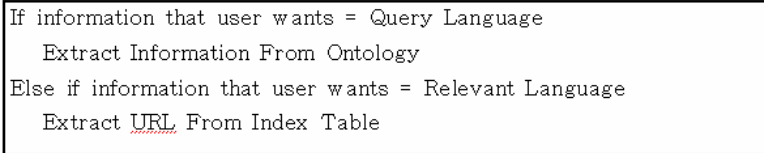


Fig. 5. Query Engine Algorithm

3.5 Visualization

The point of Visualization of this system is the showing of the relation between query language and relevant language, using a graph. Fig. 7 shows, by way of a graph, the relationship between query language, in this case AIDS, and relevant language.

It shows semantic information of referred ontology about the query language, and also show the URL extracted in an index table about relevant language if user would click a certain circle of words by mouse.

4 Result and Estimation

Design and implementation for the Semantic WebGraph system using Ontology and Anchor Text was discussed in the previous chapter. In this chapter the results and estimations of the authors' system will be discussed. Fig. 6 is an example web page from the system. When a user wishes to know medical language regarding “AIDS” the screen (shown below) will use this word as query language.

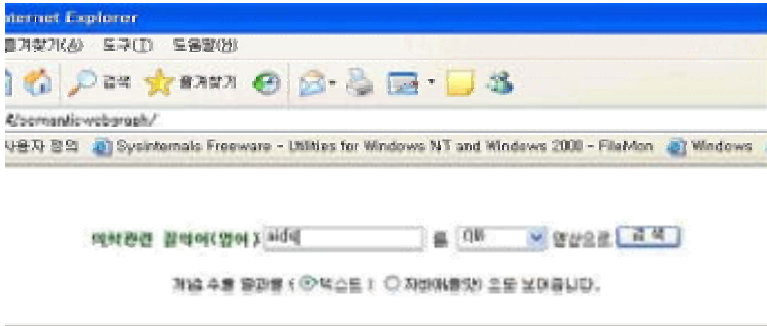


Fig. 6. Screen using a specific word as query language

If the user presses “Search” the query language and relevant language are expressed, as in the graph in Fig. 7. The word in the center of the circle is the query language, and the words surrounding it form the relevant language. The relevant language is formed as keywords, which are extracted in anchor text.

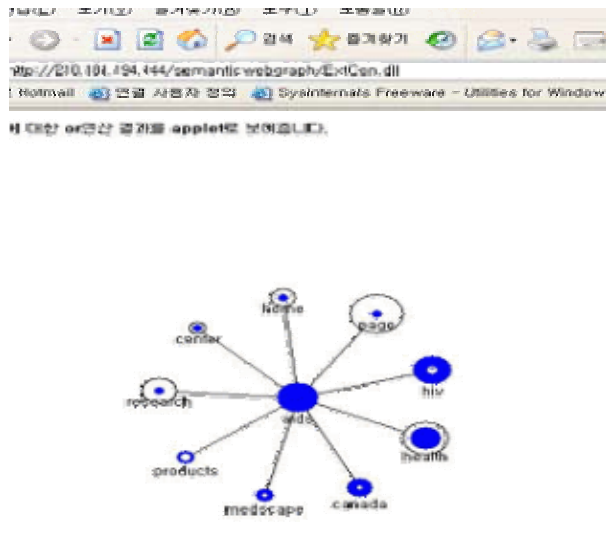


Fig. 7. Result graph when query language is “AIDS”

When the user clicks each circle results are formed, as in Fig. 8. In the upper right corner is the picture showing the semantic information that the user receives when clicking on that part of the query language. The retrieval of this information requires pre-created Ontology. The lower right picture shows the URL that results when the user clicks the circle relating to the relevant language.

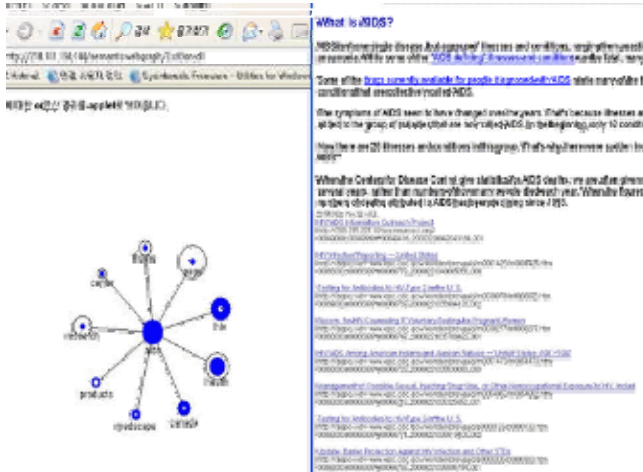


Fig. 8. Final result picture

Thus, this system efficiently shows information that the user wants by providing semantic information about the query language, and the URL of relevant language. Therefore, users can obtain information for the query language and required relevant information, and they are able to get such information even if they lack detailed knowledge about the query language. Fig. 9 shows a chart providing comparisons of other relevant systems.

System	MagPie	WebGraph	Semantic WebGraph
Semantic Information Extract	O	X	O
Relevant Language Search	X	△	O
Visualization	△	O	O
O/S Compatibility	X	O	O

Fig. 9. Chart comparing other systems

The above table indicates that the authors’ system is superior to other systems, and shows that MagPie has the weakness of not having O/S compatibility as a result of it being an Active X program.

5 Conclusion

This paper proposes that the Semantic Web Search System, using Ontology and Anchor Text, be used to overcome the limits of the existing Semantic Web browsing and search system. The authors' system shows information that users can obtain efficiently using a method giving semantic information about query language, and the URL about relevant language. It is shown that users can obtain information for the query language even if they lack knowledge of such language.

Hereafter, by way of research tasks, study of more effective selection of choices of relevant language is needed, along with the drawing of relevant polymorphic graphs.

References

1. <http://www.w3.org/2001/sw/>
2. Tim Berners-Lee, Semantic Web, W3C, <http://www.w3.org/2000/Talks/1206-xml2k-tbl/>, 2000.
3. Tim Berners-Lee, James Hendler, and Ora Lassila, Scientific American article: The Semantic Web, Scientific American issue, May 17, 2001.
4. Dzbor, M., Domingue, J., and Motta, E.: Magpie: Towards a Semantic Web Browser. Proc. of the 2nd Intl. Semantic Web Conf. (ISWC). 2003. Florida, USA
5. Domingue, J., Dzbor, M. and Motta, E.: Magpie: Supporting Browsing and Navigation on the Semantic Web. Proc. of Intl. Conf. on Intelligent User Interfaces (IUI). 2004. Portugal.
6. Quan, Dennis and Karger, David R : How to Make a Semantic Web Browser. In Proceedings International WWW Conference, New York, 2004. USA.
7. Thomas Gruber, A Translation Approach to Portable Ontologies. Journal on Knowledge Acquisition, Vol. 5(2), pp. 199-220, 1993.
8. Sergy Brin, Lawrence Page, The Anatomy of a Large-Scale Hypertextual Web Search Engine", In Proceeding of the 7th International World Wide Web Conference(WWW7), 1998
9. Jun-Young Choi, "Employing Search System by Conceptual Graph using Hyperlink in Internet", Chung-Ang University 90th Master's Thesis, 1998
10. Nam-Deok Cho, "Design and Implementation of Keyword Extraction Algorithm of Search Engine Using Anchor Text and TFIDF", Chung-Ang University 94th Master's Thesis, 2000
11. Sam-il Ko, "Automatic Generation of Concepts in Concept-based Search System", Chung-Ang University 100th Master's Thesis, 2003

Design Progress Management for Security Requirements in Ubiquitous Computing Using COQUALMO*

Eun Ser Lee¹ and Sang Ho Lee²

¹ Information & Media Technology Institute, Soongsil University
eslee1@ssu.ac.kr

² School of Computing, Soongsil University
shlee@comp.ssu.ac.kr

Abstract. This paper estimates the development of a security process in four cases. This paper is intended to help the design lifecycle and progress management in ISO/IEC 15408 (Common Criteria). There are many defects that cause the security requirement problems during the software development. This paper explores the areas of the lifecycle and progress management that remove the security requirements and also manage the schedule and quality problems. For projects in similar domains, it is possible to remove security risk items and to manage progress by using security lifecycle and progress milestone, which can greatly improve the software process.

1 Introduction

The recent advances in information technologies and the proliferation of computing systems and world-wide networks have raised the level of concern about security in the public and private sectors. This concern has been reinforced in the final report of President's Commission on Critical Infrastructure Protection [1] and the associated Presidential Decision Directive 63 (PDD-63) [2]. Security concerns are motivated by increasing use of information technology (IT) products and systems in governments and industries ranging from electronic commerce to national defense. Consumers have access to a growing number of security enhanced IT products with different capabilities and limitations, and should make important decisions about which products provide an appropriate degree of protection of their information.

In order to help consumers select commercial off-the-shelf IT products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace, the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP) to evaluate IT product conformance to international standards. The program, officially known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (Common Criteria Scheme in short) is a partnership between the public and private sectors [3][4].

* This work was supported by Korea Research Foundation Grant (KRF-2004-005-D00172).

This paper provides an analysis of the efficiency of the removal of security requirement risk. Security risk items can also be removed by using security lifecycle and progress milestone, which can greatly improve the software process.

2 Related Works

2.1 ISO/IEC 15408 (Common Criteria, CC)

The Common Criteria (CC), is meant to be used as the basis for evaluation of security properties of IT products and systems. By establishing such a common criteria base, the results of an IT security evaluation will be meaningful to a wider audience [5][6].

The CC is useful as a guide for the development of products or systems with IT security functions and for the procurement of commercial products and systems with such functions. During evaluation, such an IT product or system is known as a Target of Evaluation (TOE). Such TOEs include, for example, operating systems, computer networks, distributed systems, and applications.

The CC defines three types of requirement constructs: package, PP(Protect Profile) and ST(Security Target). The CC further defines a set of IT security criteria that can address the needs of many communities and thus serve as a major expert input to the production of these constructs. The CC has been developed around the central notion of using, wherever possible, the security requirements components defined in the CC, which represent a well-known and understood domain. Figure 1 shows the relationship between these different constructs [1][2].

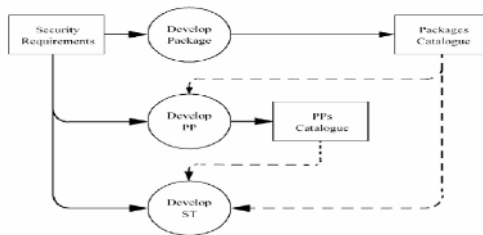


Fig. 1. Use of security requirements

2.2 Protection Profile

Evaluation criteria are most useful in the context of the engineering processes and regulatory frameworks that are supportive of secure TOE development and evaluation. This sub-clause is provided for illustration and guidance purposes only and is not intended to constrain the analysis processes, development approaches, or evaluation schemes within which the CC might be employed [1][2][3].

The CC requires that certain levels of representation contain a rationale for the representation of the TOE at that level. That is, such a level must contain reasoned and convincing argument that shows that it is in conformance with the higher level, and is itself complete, correct and internally consistent. Rationale directly demonstrat-

ing compliance with security objectives supports the case that the TOE is effective in countering the threats and enforcing the organizational security policy.

The CC layers the different levels of representation as described in Figure 2, which illustrates the means by which the security requirements and specifications might be derived when developing a PP or ST. All TOE security requirements ultimately arise from consideration of the purpose and context of the TOE. This chart is not intended to constrain the means by which PPs and STs are developed, but illustrates how the results of some analytic approaches relate to the content of PPs and STs.



Fig. 2. Derivation of requirements and specifications

PP includes the security target and rationale. The contents are as follows:

Table 1. Protection profile items

1	Protection Profile Introduction 1.1 PP Identification 1.2 PP Overview
2	TOE Description
3	TOE Security Environment 3.1 Assumptions 3.2 Threats 3.3 Organizational Security Policy
4	Security Objectives 4.1 Security Objectives for the TOE 4.2 Security Objectives for the Environment
5	IT Security Requirements 5.1 TOE Security Functional Requirements 5.2 TOE Security Assurance Requirements 5.3 Security Requirements for the IT Environments
6	PP Application Notes
7	Rationale 7.1 Security Objectives Rationale 7.2 Security Requirements Rationale

2.3 Security Target

An ST shall conform to the content requirements described in this chapter. An ST should be presented as a user-oriented document that minimizes reference to other material that might not be readily available to the ST user [1][2][3].

The rationale may be supplied separately, if that is appropriate. The contents of the ST are shown in Figure 3, which should be used when constructing the structural outline of the ST. Table 2 describes that contents of the security target.

Table 2. Security target items

1	ST Introduction 1.1 ST Identification 1.2 ST Overview 1.3 CC Conformance
2	TOE Description
3	TOE Security Environment 3.1 Assumptions 3.2 Threats 3.3 Organizational Security Policy
4	Security Objectives 4.1 Security Objectives for the TOE 4.2 Security Objectives for the Environment
5	IT Security Requirements 5.1 TOE Security Functional Requirements 5.2 TOE Security Assurance Requirements 5.3 Security Requirements for the IT Environments
6	TOE Summary Specification 6.1 TOE Security Functions 6.2 Assurance Measures
7	PP Claims 7.1 PP Reference 7.2 PP Tailoring 7.3 PP Additions
8	Rationale 8.1 Security Objectives Rationale 8.2 Security Requirements Rationale 8.3 TOE Summary Specification Rationale 8.4 PP Claims Rationale

2.4 TOE (Target of Evaluation)

The CC contains the evaluation criteria that permit an evaluator to determine whether the TOE satisfies the security requirements expressed in the ST. By using the CC in evaluation of the TOE, the evaluator will be able to make statements about:

- a) whether the specified security functions of the TOE meet the functional requirements and are thereby effective in meeting the security objectives of the TOE;
 - b) whether the specified security functions of the TOE are correctly implemented.
- The security requirements expressed in the CC define the known working domain of

applicability of IT security evaluation criteria. A TOE for which the security requirements are expressed only in terms of the functional and assurance requirements drawn from the CC will be evaluative against the CC. Use of assurance packages that do not contain an EAL shall be justified [1][2][3].

The results of a TOE evaluation shall include a statement of conformance to the CC. The use of CC terms to describe the security of a TOE permits comparison of the security characteristics of TOEs in general.

2.5 MBASE

The difference between failure and success in developing a software-intensive system can often be traced to the presence or absence of clashes among the models used to define the system's product, process, property, and success characteristics [11].

In each case, property models are invoked to help verify that the project's success models, product models, process models, and property levels or models are acceptably consistent. It has been found advisable to do this especially at two particular "anchor point" life cycle process milestones summarized in Table 2 [10][11]. The first milestone is the Life Cycle Objectives (LCO) milestone, at which management verifies the basis for a business commitment to proceed at least through an architecting stage. This involves verifying that there is at least one system architecture and choice of COTS/reuse components which is shown to be feasible to implement within budget and schedule constraints, to satisfy key stakeholder win conditions, and to generate a viable investment business case. The second milestone is the Life Cycle Architecture (LCA) milestone, at which management verifies the basis for a sound commitment to product development (a particular system architecture with specific COTS and reuse commitments which is shown to be feasible with respect to budget, schedule, requirements, operations concept and business case; identification and commitment of all key life-cycle stakeholders; and elimination of all critical risk items) [12][13].

2.6 Ubiquitous Computing

Ubiquitous computing names the third wave in computing, just now beginning. Initially came mainframes, each shared by many users. However, the era of the personal computing is now upon us, and people are forced to stare uneasily at each other across the desktops. However, this era will be followed by that of ubiquitous computing, when technology will recede into the background of our lives [8][9][10].

It is very difficult to incorporate security mechanisms into sensor routing protocols after the design has completed. Therefore, sensor network routing protocols must be designed with security considerations in mind. This is the only effective solution for secure routing in ubiquitous networks.

The contributions of this paper are intended to be as follows:

- (1) Proposed threat models and security goals for secure routing in wireless sensor networks;
- (2) Introduced two novel classes of previously undocumented attacks against sensor networks: sinkhole attacks and HELLO floods;
- (3) Demonstration of how attacks against ad hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks;

- (4) Presented the first detailed security analysis of all the major routing protocols and energy conserving topology maintenance algorithms for sensor networks – described practical attacks against all of them would defeat any reasonable security goals;
- (5) Discussed of countermeasures and design considerations for secure routing protocols in sensor networks

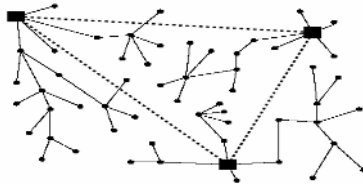


Fig. 3. A representative sensor network architecture

Several risk items are apparent in the connections of the network architecture in Fig.3. These items are to be removed so as to provide a reliable ubiquitous service. Remove of the risk items also provides security of the lifecycle.

3 Theory

Security functions were evaluated using security profiling and security targeting, by way of the ubiquitous method. Evaluation progress was introduced in chapter 2. It should be noted that when evaluation is conducted security requirements focus on the functional. However, the downside of this in terms of security is that defects with often appear in the next stage. Therefore one should refer to the lifecycle to in order to extract and identify the risk factors of the security items. Another problem is that risk factor extraction is a redundant processing job. Furthermore, extraction processing is ambiguous and so firm progress management is required.

This chapter provides identification of risk items and checks the rationale and measurement of total progress management.

3.1 Security Profile Lifecycle

The lifecycle is made by protecting the profiles in order to fulfill the security requirement. The next step is the removal of the redundant risk items. Protection profile progress and identification is as follows:

1. A protection profile developer must be provided to explain the profile of the TOE.
2. Explanation of the TOE must be provided so as to describe its product type and the character of the general IT.
3. The evaluator must have confirmation that the information has satisfied all of the evidence requirements.
4. The evaluator must have confirmation of the explanation of the TOE with regards to quality and consistency.
5. The evaluator must have confirmation of the explanation of the TOE with regards to the relationship of protection profile consistency

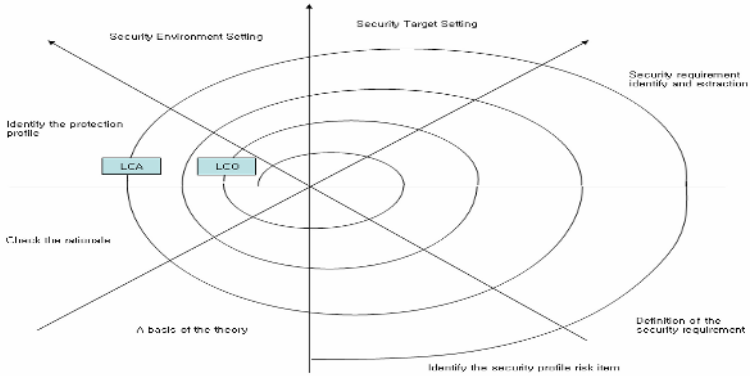


Fig. 4. Ubiquitous lifecycle milestone of the protection profile

This figure shows the activity of the risk item as it is removed from the security requirement during the extraction process. Each of the factors use the repeatable milestone for progress management. Each stage is as follows:

Table 3. Description of the protection profile

Stage	Contents
Identify the protection profile	Identification and analysis the protection target for the extraction of the security requirement.
Security Environment Setting	H/W and S/W, personal element setting for the security.
Security Target Setting	Security requirement Target Setting
Security requirement identification and extraction	Identify and extraction of the security requirement using UML(or other method)
Definition of the security requirement	Definition of the security requirement for system building
Identify the security profile risk item	Identify the security profile risk item at the domain
Basis of the theory	Build of the repeatable lifecycle for the milestone(LCO, LCA)
Checking of the rationale	Check the rationale of the repeatable milestone and risk analysis

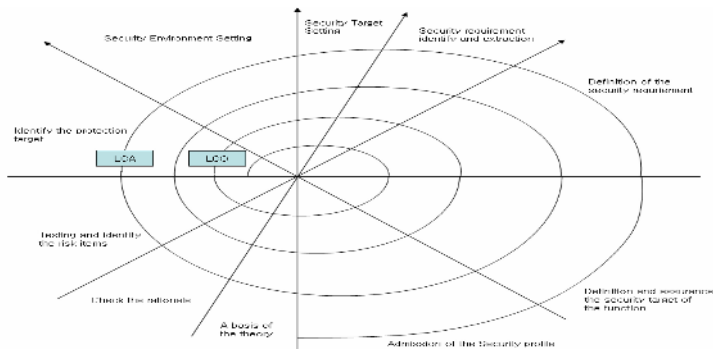


Fig. 5. Ubiquitous lifecycle milestone of the security target

This figure shows provision of the activity of the security requirement extraction of the security target.

Each of the factors use the repeatable milestone (LCO, LCA) for the progress management. Each stage is as follows:

Table 3. Description of the security target

Stage	Contents
Identify the protection target	Identification and analysis the protection target for the extraction of the security requirement.
Security Environment Setting	H/W and S/W, personal element setting for the security.
Security Target Setting	Security requirement Target Setting
Security requirement identify and extraction	Identify and extraction of the security requirement using UML (or other method)
Definition of the security requirement	Definition of the security requirement for system building
Definition and assurance of the function's security target	Definition and assurance of the security target based on the function for the system building
Admission of the Security profile	Admission of the confirmed Security profile at its domain
Basis of the theory	Build of the repeatable lifecycle for the milestone (LCO, LCA)
Checking of the rationale	Check the rationale of the repeatable milestone and risk analysis
Testing and identify of risk items	Testing and identification for the extraction of new risk items.

Use of the milestones (LCO, LCA) is essential for removal of risk and progress management.

The authors of this paper have provided the repeatable cycle based on the milestone element. Progress was checked using the basis of the milestone.

Table 4. Description of the milestone element

Milestone Element	Life Cycle Objectives (LCO)	Life Cycle Architecture (LCA)
Definition of Operational Concept	<ul style="list-style-type: none"> Top-level system objectives and scope System boundary Functional purposes and assumptions Excluded parameters Operational concept Operational environment restrictions and constraints Operational life cycle (responsibility, cycle, address) 	<ul style="list-style-type: none"> Elaboration of system objectives and scope of increment Elaboration of operational concepts to increment
System Prototype(s)	<ul style="list-style-type: none"> Generate user usage scenarios Research and evaluate 	<ul style="list-style-type: none"> Generate range of usage scenarios Research and evaluate
Definition of System Requirements	<ul style="list-style-type: none"> Top-level functions, interfaces, and behavior levels, including constraints and priorities Use cases Stakeholder requirements or scenarios 	<ul style="list-style-type: none"> Elaboration of functions, interfaces, quality attributes, and constraints to be used Order of arrival of IED's to be determined (time) Establish user requirements and their priority
Definition of System and Software Architecture	<ul style="list-style-type: none"> Top-level definition of software architecture Physical and logical architecture Architecture of IED's and its sub-elements Identification of reusable architecture 	<ul style="list-style-type: none"> Elaboration of LCA and increment by increment Physical and logical components, connectors, wiring, and so on CDR's, code entries Component architecture and architectural code choices Multi-structure evolution scenarios
Definition of Life-Cycle Plan	<ul style="list-style-type: none"> Identification of life cycle scenarios Users, scenarios, developers, maintainers Life cycle owner, objects, goals, roles Identification of the tests or progress plan Top-level support, maintenance Top-level WWWVWHH lifecycle 	<ul style="list-style-type: none"> Elaboration of WWWVWHH Life Cycle Operational Capability (LOC) Top-level allocation, identification of key TBD's for later increments
Feasibility Rationale	<ul style="list-style-type: none"> Assessment of life cycle scenarios, its sustainability Use of various measurement, prediction, simulation etc. Elaboration of analysis for multi-forms, models and structures 	<ul style="list-style-type: none"> Assessment of constraints among elements to be used Validation: Use rationale to check on risk management plan and structures

* WWWVWHH: Why, What, When, Who, Where, How, How Much

We are provides that the repeatable cycle based on milestone element. Also, we are checked the progress by the basis of milestone.

Table 5. Setting of the milestone

LCO		↓	LCA	
Cycle 1	Cycle 2	↓	Cycle 3	↓
Determination of top-level concept of operations	Determination of detailed concept of operations	↓	Elaboration of detailed concept of operations by increment, especially IOC	↓
System scope / boundaries / interfaces; top-level requirements	Top-level HW, SW, human requirements	↓	Determination of requirements, growth vector by increment, especially IOC	↓
Small number of feasible candidate architectures (including major COITS, reuse choices)	Provisional choice of top-level information architecture	↓	Choice of life-cycle architecture. Some components of above TBD (low-risk and/or deferrable)	↓
Top-level life cycle responsibilities(stakeholders), process, model, cost/schedule parameters	Make detailed process strategy, responsibilities, cost / schedule allocation	↓	Thorough WWWWEEH plus for IOC; essentials for later increments	↓
Stakeholder concurrence on top-level analysis supporting win-win satisfaction	More detailed analysis supporting win-win satisfaction	↓	Stakeholder concurrence on thorough analysis supporting win-win satisfaction	↓
Top level rationale, including rejected candidate architectures	More detailed rationale underlying system choices	↓	Elaboration of rationale, including risk resolution results	↓

3.2 Calculation of COQUALMO

Lifecycle evaluation compares the number of real defects with the estimated number of defects at each stage of development, using COQUALMO. Defect removal capability was analyzed using risk item management [15].

Table 6. Number of dects introduced

MBASE/Rational Model (Waterfall Model)	Inception (Requirements)	Elaboration (Product Des)	Construction (Development)	Transition	Total
No. of Requirements Defects	130	116	35	-	281
No. of Design Defects		336	201	-	537
No. of Code Defects			809	-	809
TOTAL	130	452	1045	-	1627

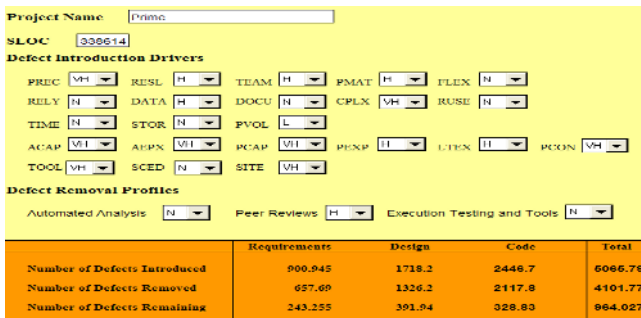


Fig. 6. Calculation of defect number

There were found to be three times the amount of differences between the defect numbers in the real project and that using COQUALMO. Also, such data is required to show 3-4 times such rates of difference in the real project. Therefore, evaluation of the results can be used to estimate defect numbers as follows:

$$1627 \text{ (Real Project)} \times 3.11 \text{ times (approx.)} = 5065 \text{ (COQUALMO)}$$

Defect number estimation uses the COQUALMO algorithm.

4 Conclusion

In this paper a new lifecycle was proposed applicable to the extraction of the security requirement in the ubiquitous stage, along with reliable analysis of relevant requirements. The authors propose not only risk item removal, but also progress management.

In future studies development methodology applicable to the extract of security requirements will be provided.

References

- [1] ISO/IEC 15408-1:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model
- [2] ISO. ISO/IEC 15408-2:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements
- [3] ISO. ISO/IEC 15408-3:1999 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements
- [4] The Report of the President's Commission on Critical Infrastructure Protection CCEB (Common Criteria Editorial Board), Common Criteria for Information Technology Security Evaluation, Version 2.0, May 1998.
- [5] DOD (U.S. Department of Defense), Trusted Computer System Evaluation Criteria, DOD5200.28-STD, December 1985. 1.0, December 1992.
- [6] [ISO96] ISO/IEC Guide 65—General Requirements for Bodies Operating Product Certification Systems, 1996.
- [7] Mark Weiser, "Hot Topics: Ubiquitous Computing" IEEE Computer, October 1993.
- [8] Mark Weiser, "The Computer for the Twenty-First Century," Scientific American, pp. 94-10, September 1991
- [9] Mark Weiser, "Some Computer Science Problems in Ubiquitous Computing," Communications of the ACM, July 1993. (reprinted as "Ubiquitous Computing". Nikkei Electronics; December 6, 1993; pp. 137-143.
- [10] B. Boehm, Software Risk Management, IEEE-CS Press, 1989.
- [11] B. Boehm, A. Egyed, J. Kwan, and R. Madachy, "Developing Multimedia Applications with the WinWin Spiral Model," Proceedings, ESEC/ FSE 97, Springer Verlag, 1997.
- [12] B. Boehm and P. Bose, "A Collaborative Spiral Process Model Based on Theory W," Proceedings, ICSP3, IEEE, 1994. 17

Web Document Classification Using Changing Training Data Set

Gilcheol Park and Seoksoo Kim*

Dept.of Multimedia Engineering, Hannam University,
Daejeon, South Korea
gcpark@hannam.ac.kr

Abstract. Machine learning methods are generally employed to acquire the knowledge for automated document classification. They can be used if a large set of pre-sampled training set is available and the domain does not change rapidly. However, it is not easy to get a complete trained data set in the real world. Furthermore, the classification knowledge continually changes in different situations. This is known as the maintenance problem or knowledge acquisition bottleneck problem. Multiple Classification Ripple-Down Rules (MCRDR), an incremental knowledge acquisition method, was introduced to resolve this problem and has been applied in several commercial expert systems and a document classification system. Evaluation results for several domains show that our MCRDR based document classification method can be successfully applied in the real world document classification task.

1 Introduction

Before computer technology was introduced, people mainly relied on manual classification such as library catalogue systems. In the early stages of the computerized classification development, computer engineers moved this catalogue system into the computer systems. However, as the size of available Web documents grows rapidly and people have to handle them within limited time, automated classification becomes more important. [1,2]

Machine learning (ML) based classifiers have been widely used for automatic document classification and there are various approaches such as clustering, support vector machine, probabilistic classifier, decision tree classifier, decision rule classifier, and so on[3]. But they have some problems when they are applied to real world applications because they capture only a certain aspect of the content and tend to learn in a way that items similar to the already seen items (training data) are recommended (predefined categories) [4]. However, it is difficult to collect well defined training data sets because Web documents (e.g., news articles, academic publications, and bulletin board messages) are continually created by distributed world-wide users and the number of document categories also continually increases.

* Corresponding author. "This work was supported by a grant No. (R12-2003-004-03003-0) from Ministry of Commerce, Industry and Energy".

To manage this problem, the document classifiers should support incremental knowledge acquisition without training data. Though some ML techniques such as clustering techniques [5-7] are suggested as solutions for incremental classification, they do not sufficiently support personalized knowledge acquisition (KA). Document classifiers in the real world should support personalized classification because classification itself is a subjective activity [1]. To be successful personalized document classifiers, they should allow users to manage classification knowledge (e.g., create, modify, delete classification rules) based on their decision. But it is very difficult when users use ML classifiers because understanding their compiled knowledge is very difficult and their knowledge is so strongly coupled with the knowledge of training data sets that it is not easily changed without deliberate changing them. Rule-based approach is a more favorable solution for the incremental and personalized classification task because the classification rules in knowledge base (KB) can be personalized, understood, and managed by users very easily. But rule-based systems are rarely used to construct an automatic text categorization classifiers since the '90s because of the knowledge acquisition (KA) bottleneck problem [3, 8]. We used Multiple Classification Ripple-Down Rules (MCRDR), an incremental KA methodology, because it suggests a way that overcomes the KA problem and enables us to use the benefits of rule-based approach. A more detail explanation will be suggested in section 2. Our research focuses on the personalized Web document classifier that is implemented with the MCRDR method. In section 2, we will explain causes of the KA problem and how MCRDR can solve that problem. In section 3, we will explain how our system implemented in accordance with MCRDR method. In section 4, we will show empirical evaluation, which is performed three different ways. In section 5, we will conclude our research and suggest further works

2 Knowledge Acquisition Problems and MCRDR

KA problems are caused by cognitive, linguistic and knowledge representational barriers [8]. Therefore, the promising solution for the KA must suggest the methodology and KA tools that overcome these problems.

-Cognitive Barrier. Because knowledge is unorganized and often hidden by compiled or *tacit knowledge* and it is highly interrelated and is retrieved based on the situation or some other external trigger, knowledge acquisition is discovery process. Therefore, knowledge often requires correction and refinement - the further knowledge acquisition delves into compiled knowledge and areas of judgment, the more important the correction process becomes [9]. From the GARVAN-ES1 experience, Compton et al [10] provide an example of an individual rule that has increased four fold in size during maintenance and there are many examples of rules splitting into three or four different rules as the systems' knowledge was refined. Compton and Jensen[11] also proposed that knowledge is always given in context and so can only be relied on to be true in that context. MCRDR focuses on ensuring incremental addition of validated knowledge as mistakes are discovered in the multiple independent classification problems [12, 13].

-Linguistic Barrier. Communication difficulties between knowledge engineers and domain experts are also one of the main deterrents of knowledge acquisition. Traditionally, knowledge is said to flow from the domain expert to the knowledge engineer to the computer and the performance of knowledge base depends on the effectiveness of the knowledge engineer as an intermediary [8]. During the maintenance phase, knowledge acquisition becomes more difficult not only because the knowledge base is becoming more complex, but because the experts and knowledge engineers are no longer closely familiar with the knowledge communicated during the prototype phase [11]. Domain knowledge usually differs from the experts and contexts. Shaw[14] illustrates that experts have different knowledge structures concerning the same domain and Compton and Jansen[11] show that even the knowledge provided by a single expert changes as the context in which this knowledge is required changes. For these reason, MCRDR shift the development emphasis to maintenance by blurring the distinction between initial development and maintenance and knowledge acquisition is performed by domain experts without helping the knowledge engineer [13].

-Knowledge Representation Barrier. The form in which knowledge is available from people is different from the form in which knowledge is represented in knowledge systems. The difference between them, called representation mismatch, is central to the problem of KA. In order to automate KA, one must provide a method for overcoming representation mismatch [15]. KA research has been aimed to replace the knowledge engineer with a program that assists in the direct “transfer of expertise” from experts to knowledge bases [16]. Mediating representation facilitate communication between domain expert and knowledge engineer. Intermediate representations provide an integrating structure for the various mediating representations and can form a bridge to the knowledge base[17]. We used *folder structure user interface*, which is largely used for manual document classification in traditional document management application, as *mediating representation method* and *difference lists* and *cornerstone cases* as *intermediating representation*. Folder manipulations are interrelated with the MCRDR KA activities in our system.

3 Real World Web Document Classifier with MCRDR

3.1 Content-Based Load Distribution Server

MCRDR based document classification system is a component of the Personalized Web Information Management System (PWIMS) System. It is implemented with C++ program language based on the MCRDR methodology. It is used to construct both Web document classification and personalized Web portal.

3.2 Folder Structures as a Mediating Representation

The choice of representation can have an enormous impact on human problem-solving performance. The term mediating representation is used to convey the sense of coming to understand through the representation and it should be optimized for human understanding rather than for machine efficiency. It is suggested to improve the KA process by developing and improving representational devices available to the

expert and knowledge engineer. Therefore, it can provide a medium for experts to model their valuable knowledge in terms of an explicit external form [17]. We use traditional folder structures as a mediating representation because users can easily build a conceptual domain model for the document classification by using folder manipulation. Our approach differs from the traditional knowledge engineering approach because we assume there is no mediate person (knowledge engineer). Rather the domain experts or users directly accumulate their knowledge by using KA tools [12].

3.3 Inference with MCRDR Document Classifier

A classification recommendation (conclusion) is provided by the last rule satisfied in a pathway. All children of satisfied parent rule are evaluated, allowing for multiple conclusions. The conclusion of the parent rule is only given if none of the children are satisfied [13]. For example, the current document has a set of keywords with {a, b, c, d, e, f, g}.

1. The system evaluates all the rules in the first level of the tree for the given WL (rules 1, 2, 3 and 5 in Fig. 1.). Then, it evaluates the rules at the next level which are refinements of the rule satisfied at the top level and so on.

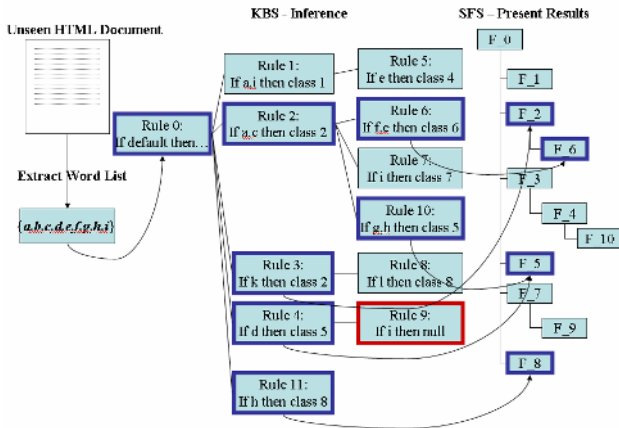


Fig. 1. Inference for the Web document classification

2. The process stops when there are no more children to evaluate or when none of these rules can be satisfied by the WL in hand. In this instance, there exist 4 rule paths and 3 classifications (classes 2, 5, and 6).
3. The system classifies into the storage folder structures (SFS)' relevant nodes (F_2, F_5, and F_6) according to the inference results.
4. When the expert finds the classification mistakes or wants to create the new classifications, he updates the classification knowledge via the knowledge acquisition interface

3.4 Knowledge Acquisition and Intermediate Representation

KA and inference are inextricably linked in the MCRDR method, so some KA steps depend on the inference and vice versa [13]. The KA process consists of the following sub-tasks: 1) initiating KA process, 2) deciding KA method, and 3) validating new rules.

-Initiating KA Process. KA process is initialized by users when they dissatisfy the system's inference result. Kelly suggested that "every construct has a specific range of convenience, which compromise all things to which the user would find its application useful." The range of convenience of each construct defines its extension in terms of a single aspect of a limited domain of events [17]. The users' decision for initializing new KA processes depends on the range of convenience. There are two different kinds of KA initialization: the KA process begins when the system recommends incorrect class or no class and users initiate it (human initiated KA) and users move or copy some pre-classified documents to another folder (system initiated KA).

-Deciding KA Methods. There are three kinds of KA methods: refinement KA, stopping KA, and ground-breaking KA.

- **Refinement KA:** If the user thinks that the current document should be classified into the sub folder (may not exist) of the recommend folder, the user selects (or creates and selects) the sub folder of the folder recommended by the system. The new rule should be added under the current classification rule as the child rule, because it refines current rule. For example, if a certain document that contains keyword "a" and "c", it will be classified into folder F_2 in Fig. 1. But users may want to classify this document to folder F_6 (this folder may not exist when this document classified) because it contains keyword "f" and "e". In this case, the new refinement rule is created under the rule 2 and its conclusion is class 6.
- **Stopping KA:** If the current inference result is obviously incorrect and the users do not want to classify incoming documents into this folder, he/she makes stopping rules with certain condition keyword/keywords. The new stopping rule won't have any recommendation for a folder. For example, if a certain document that contain keyword "d", it will be classified folder F_5 in Fig. 1. But users may not want to classify this document to folder F_2 because it contains keyword "i". In this case, the new rule with condition "i" is added under the rule 4 and its conclusion is "null".
- **Ground-breaking KA:** For example, if a certain document that contains keyword "k", it will be classified folder F_2 in Fig. 1. But domain experts may not want to classify this document to folder F_2 because it contains keyword "h" and they want to make new classification. In this case new rule is added under the root node (e.g. rule 11).

The KA process is initiated by system when users copy or move pre-classified documents to other folder/folders. Its KA method depends on the action types. If the action is moving, the stopping KA and ground breaking KA are needed. For example, if users want to move some documents in F_6 to F_1, they must select keywords that

make stopping rules and ground breaking rules such as “*f*”. In this example, new rule conditions will be “*a*” and “*c*” and “*f*” and “*e*” and “*t*”. If the action is copying, only the ground breaking rule is automatically created by the system. Its condition is the same as the original rule but it has a different conclusion.

-Validating with Cornerstone Case and Difference List. Bain proposed that the primary attributes of intellect are consciousness of difference, consciousness of agreement, and retentiveness and every properly intellectual function involves one or more of these attributes and nothing else. Kelly stated “A person’s construction system is composed of a finite number of dichotomous construct.” Gaines and Shaw suggested KA tools that are based on the notion that human intelligence should be used for identifying differences rather than trying to create definitions. In our system, the experts must make domain decisions about the differences and similarities between objects to validate new rule. Our system supports users with *cornerstone case* and *difference list* [12, 13]. As shown in Fig. 1, an n-ary tree is used for knowledge base (internal schema). MCRDR uses a “*rules-with-exceptions*” knowledge representation scheme because the context in the MCRDR is defined as the sequence of rules that were evaluated leading to a wrong conclusion or no conclusion with existing knowledge base [13]. Though users can see the whole knowledge base (internal schema) in our system, it is not directly used for KA. Instead, MCRDR uses *difference list* and *cornerstone case* for intermediate representation. The documents are used for the rule creation are called “cornerstone cases” and saved with the rules. Each folder may have multiple rules and cornerstone cases. When users make refinement rule or stopping rule, all related rules must be validated but we do not want for users to make a rule that will be valid afterward. Rather we want to present the users with a list of conditions (called “*difference lists*”) to choose from which will ensure a valid rule. The difference between the intersection of the cornerstone cases which can reach the rule and the new case cannot be used [12]. Cases which can be reclassified by the new rule appear in the system. The users may subsequently select more conditions from the different keywords lists to exclude these cases. Any case which is left in this list is supposed to classify the new folder by the new rule. A prior study shows that this guarantees low cost knowledge maintenance [13].

4 Experiment

The goal of our research is to develop personalized Web document classifiers with MCRDR. The experiments are designed to the performance evaluation in the various classification situations. We consider three different cases: 1) document classification without domain change by single user, 2) document classification with domain changes by single user, and 3) document classification within single domain by two users.

-Data Sets. We uses three different data sets: health information domain, IT information domain (English), and IT and finance domain (Korea), which are collected by our Web monitoring system for one month. Table 1 represents the data sets that are used for our experiments.

Table 1. Inference for the Web document classification

Data	Domain	Source	User	Articles
Data Set 1	Health	BBC, CNN, Australian, IntelliHealth, ABC (US), WebMD, MedicalBreakthroughs	1	1,738
Data Set 2	IT (English)	Australian, ZDNet, CNN, CNet, BBC, TechWEB, New Zealand Herald	2	1,451
Data Set 3	IT/Finance (Korean)	JungAng, ChoSun, DongA, Financial News, HanKyeung, MaeKyeung, Digital Times, iNews24	1	1,246

-Results. Classification effectiveness can be usually measured in terms of precision and recall. Generally two measures combined to measure the effectiveness. However, we only use precision measure because our system is a real world application and there is no pre-defined training data set. Fig. 2 shows the experiment’s results. In each figure, horizontal axis represents the cases, left vertical axis represents the precision rates and right vertical axis represents the number of rules.

-Experiment 1. This experiment is performed by a single user without domain changes in the health news domain. The user classified 1,738 articles with 348 rules. Though there are some fluctuations of the precision rate and rule numbers, there exist obvious trends: the precision rate gradually increases and the number of rules gradually decreases as the cases increase. Precision rate sharply increases from starting point to a certain precision level (around 90%) and is very stable after that point. This is caused by the fact that the domain knowledge continually change and as the user knows the domain, the more classification knowledge is needed.

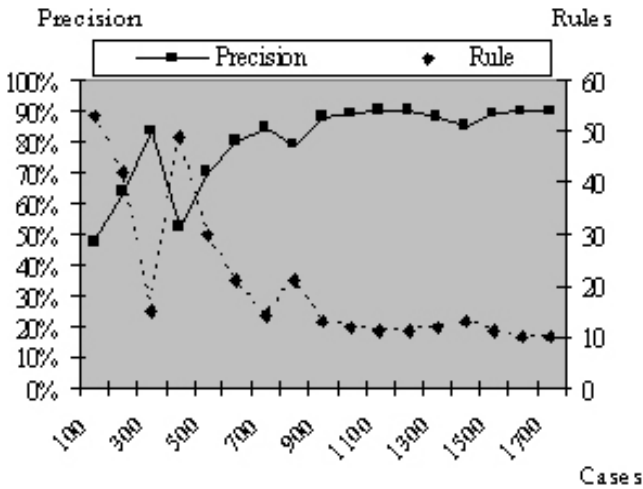


Fig. 2. Classification Result

-Experiment 2. This experiment is performed by a single user in IT and Finance news domain (Korean). Totally, 1,246 articles are classified and 316 rules are created by the users. At first, user classifies IT articles from the business relationship view (e.g. customers, competitors and solution providers). New view point for the domain (technical view) is added when user classifies 550 cases and new domain (finance) added when user classifies 800 cases. When the view point changed, the precision rate went down from 90% to 60% but precision rate recovers around 80% by classifying a small additional amount of cases. When the new domain (financial news) is added to the current domain (IT news), the precision rate sharply decreases to 10% and the rule creation goes up 30 but a very small number of cases is needed to recover 80% precision. This result shows that our document classifier can work efficiently with domain changes.

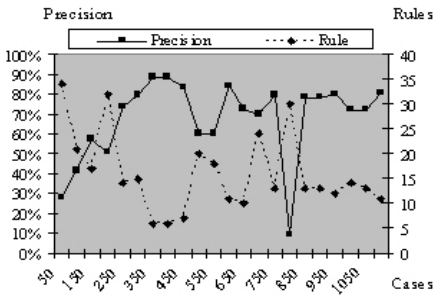


Fig. 3. Classification Result

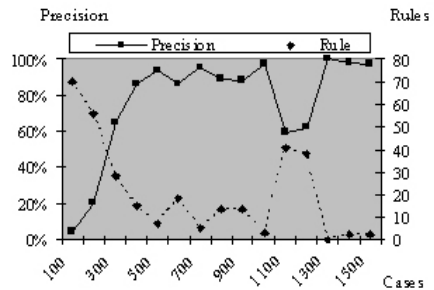


Fig. 4. Classification Results

-Experiment 3. This experiment is performed by two users in the same IT news domain (English). In total, they classified 1,451 articles with 311 rules: User 1 classifies 1,066 articles with 228 rules and user 2 classifies 432 articles with 83 rules. The classification result is shown in Fig. 4. When user 1 classified 500 articles, the precision of classifier reached around 90%. After that point, new rules are gradually created and the precision rate is slightly improved until user 1 classifies 1000. When a different user (user 2) starts to classify, the precision rate sharply down to 60% and many new rules are created. But small articles are needed to get a similar precision rate. This result means that our classifier can be adaptively applied when different users classify.

5 Conclusions

We suggested the MCRDR based document classifier. MCRDR is an incremental KA method and is used to overcome the traditional KA problem. Our classifier used the traditional folder structures as a mediating representation. Users can construct their conceptual document classification structures by using an MCRDR based classifier. In our system, the KA and inference process is inextricably linked, so some KA steps depend on the inference and vice versa. The KA process begins when the classifier

suggest no folder or incorrect folders or users activate some function in folders such as copying or moving some cases. There are three different KA methods – refinement KA, stopping KA, and ground-breaking KA. In the validation process, we used corner cases and difference list as an intermediate representation. Experiment results show that users can create their document classifier very easily with small cases and our system successfully supports incremental and robust document classification. An incremental KA based classification works well in a certain domain where the information continually increases and the creation of training set for machine learning is hard. However, this attitude does not deny the machine learning research works. Rather we view our approach can be a collaborator of machine learning technique. Wada et al. suggest integration inductive learning with RDR, Suryanto and Compton suggest a reduced KA with decision tree. Especially we view our approach can help construct a fine training data set with cost efficiency in the initial stage. Research for the combining incremental KA approach with machine learning techniques will be our further work.

References

1. Pierre, J., Practical Issues for Automated Categorization of Web Pages. 2000.
2. Sullivan, D., Search Engine Size. 2003.
3. Sebastiani, F., Machine Learning in Automated Text Categorization. *ACM Computing Surveys*, 2002. 34(1): p. 1-47.
4. Mladenic, D., Text-learning and related intelligent agents: a survey. *IEEE Intelligent Systems*, 1999. vol.14, no.4: p. 44-54.
5. Wong, W.-c. and A.W.-c. Fu. Incremental Document Clustering for Web Page Classification. in *IEEE 2000 Int. Conf. on Info. Society in the 21st century: emerging technologies and new challenges (IS2000)*. 2000. Japan.
6. Liu, R.-L. and Y.-L. Lu. Incremental context mining for adaptive document classification. in *Conference on Knowledge Discovery in Data. 2002: ACM Press New York, NY, USA*.
7. Charikar, M., et al. Incremental clustering and dynamic information retrieval. in *Annual ACM Symposium on Theory of Computing*. 1997. El Paso, Texas, United States: ACM Press New York, NY, USA.
8. Musen, M.A., Automated Generation of Model-Based Knowledge-Acquisition Tools. *Research Notes in Artificial Intelligence*. 1989, San Mateo, CA: Morgan Kaufmann Publishers, Inc.
9. Lawrence K, L., *Collision-Theory vs. Reality in Expert Systems*. 2nd ed. 1989, Wellswley, MA: QED Information Sciences, Inc.
10. Compton, P., et al. Maintaining an Expert System. in *4th Australian Conference on Applications of Expert Systems*. 1988.
11. Compton, P. and R. Jansen, A philosophical basis for knowledge acquisition. *Knowledge Acquisition*, 1990. vol.2, no.3: p. 241-258.
12. Compton, P., et al., Knowledge acquisition without analysis. *Knowledge Acquisition for Knowledge-Based Systems. 7th European Workshop, EKAW '93 Proceedings*, 1993: p. 277-299.
13. Kang, B.H., P. Compton, and P. Preston, Validating incremental knowledge acquisition for multiple classifications. *Critical Technology: Proceedings of the Third World Congress on Expert Systems*, 1996: p. 856-868.

14. Shaw, M.L.G. Validation in a knowledge acquisition system with multiple experts. in the International Conference on Fifth Generation Computer Systems. 1988.
15. Gruber, T.R., Automated knowledge acquisition for strategic knowledge. *Machine Learning*, 1989. vol.4, no.3-4: p. 293-336.
16. Davis, R., Applications of Meta Level Knowledge to the Construction, Maintenance, and Use of Large Knowledge bases. 1976, Stanford University: Stanford, CA.
17. Ford, K.M., et al., Knowledge acquisition as a constructive modeling activity. *International Journal of Intelligent Systems*, 1993. vol.8, no.1: p. 9-32.

Study on Contents Protection in M-Learning Environment

Jaekoo Song, Mingyun Kang, and Seoksoo Kim*

Dept.of Multimedia Engineering, Hannam University, Daejeon, South Korea
sskim@hannam.ac.kr

Abstract. Examine about M-learning that is e-learning system in wireless internet environment in this treatise, and analyzed DRM technology for contents protection of M-learning environment. In e-learning basically necessary that design about user register, lecture registration, assignment estimation, individual schedule learning and lecture room flat form. Designed about lecture contents service that uses DRM to support Mobile system side in these environment. Therefore, could design MDRM-learning system that emphasize in was lacking contents protection meantime. For front, need more researches about technology connected with DRM and he that emphasize to security of contents education and wireless internet environment, education systems that take advantage of this technology may have to be studied.

1 Introduction

Masie Report and other reports on education technology forecast important progresses in e-learning as follows. First, functions to support teaching and learning will be diversified. Not only the search, access and purchase of contents but also various functions related to learning activities will be provided and, with these functions, organizations such as companies will be able to execute e-learning smoothly through learning platforms. In addition, there are two important factors in the switching of online education from supplementary education to substitute one. One is EPSS (Electronic Performance Support System) through tracking information mentioned above and the other is how to induce individuals to participate in collaborative education. Fortunately, we may be able to measure the outcomes of learning investment accurately by linking personal achievements and organizational ones from e-learning. These progresses can be fully realized when all e-learning tools and contents are based on a set of officially approved industrial standards, which will enable the reuse of contents and compatible technologies. The e-learning market is expanding from school education to reeducation in industrial and public sectors. However, it looks not easy for online education to substitute for all educational practices. In case of the ordinary education market, the prevalent pattern will be the mixture of offline education in classroom and online education.

* Corresponding author. "This work was supported by a grant No. (R12-2003-004-03003-0) from Ministry of Commerce, Industry and Energy".

Even if online teaching is adopted in industrial education, the teaching is generally completed by offline lecture in physical classroom for the reason of collective training. Because enterprises and public institutions usually have reeducation facilities they do not have any problem in executing such a type of education. However, there are many other companies and public organizations without physical facility of education. In order for them to reflect physical features particularly 'the field' in their education, two methods may be feasible. One is mobile learning (M-learning) using devices of high mobility as e-learning tools and the other is so-called blended learning (B-learning) that provides the contents of both offline and online education in e-learning. Combining offline and online, B-learning makes it possible to control field work remotely. For example, when training on a machine or equipment, we can improve the effect of learning using simulations or controlling the machine or equipment in the field remotely. In many cases, occupational reeducation requires the teaching of both theory and practice as well as devices and materials for students' practice. If B-learning is activated, a large number of students can be educated using a small number of machines through remote control. M-learning is meaning in the sense of media expansion. The learning system supporting e-learning was simple learning management system (LMS) in the past but has been expanded to learning contents management system (LCMS) that can upgrade and restructure various learning contents partially. Learning contents management system is a type of management system (CMS) that can distribute contents. If distribution, namely, the publication function is extended, it will enable the delivery of learning contents to mobile devices. With the development of IT technology and the emergence of tablet PC as powerful as desktop PC, mobile devices, which have been limited to the delivery of flash and dynamic 2D multimedia, is overcoming the limitations. Furthermore, mobile computing is activating the wireless Internet. Thus, getting out of fixed Internet environment, e-learning can be executed in the field using the wireless Internet and mobile devices [1~3].

2 Necessity of Contents Protection

With the development of digital contents accelerated by the progress of the wireless Internet, Internet business is booming and online contents providers are supplying a variety of contents stimulating users' interest. These contents are texts as well as multimedia such as music, image and video. Multimedia data are applied to countless areas including Internet broadcasting, education, news, sports, tourist information and experts' consulting, creating new services in the virtual space. Moreover, companies are struggling to move toward knowledge-based management strategies and, to support the transition, are building various systems like KMS, EDMS and PDM and accumulating intellectual assets in the systems. Thank to such efforts, employees become able to share knowledge and find information promptly and conveniently. The government is also accelerating the digitization of information (library informatization by the Ministry of Culture and Tourism, knowledge resource networking project by the Ministry of Information and Communication, etc.). Furthermore, the super-speed information communication network is spreading digital paradigm as a new lifestyle throughout the whole society, and the emergence of digital broadcasting,

digital signature, electronic libraries, electronic books, electronic settlement, electronic payment, etc. is an aspect representing the new paradigm. Compared to traditional analogue ones, digital contents have many advantages in terms of production, processing, publication and distribution but copyright protection for digital products is a critical issue because digital contents can be easily reproduced. Copyright protection in digital paradigm cannot be provided with legal/institutional systems applied to analogue contents. Thus, we need a new legal system for copyright protection as well as technological devices for practical protection of digital contents. In response to the urgent demand, methods for protecting digital contents copyrights and preventing illegal distribution are under development.

MIT selected this type of technologies as one of 10 promising technologies and many researches began to be made on this area as an independent academic discipline. As digital contents business rises as a core next-generation industry, DRM-related R&D and commercialization are essential tasks to be carried out [4~6].

3 DRM

3.1 Key DRM Technologies

Various concepts of technologies are required depending on application area and security level. (1) Encryption technologies: Various encryption technologies are used including encryption, electronic signature and authentication and key distribution to authenticate contents and contents users, enforce transaction and usage rules and confirm transactions and uses (non-repudiation). Before publication, contents are protected safely through packaging. Packed data contain contents, metadata and decryption information. A key used in contents encryption is processed for safe protection so that only the authorized user (or user's system) can access, and generates decryption information. Metadata defines business rules on the distribution and use of contents and the rules are also protected cryptographically to prevent alteration or modification. (2) Key distribution and management: Safe key management and distribution mechanism is required to guarantee the reliability of encryption technology used to protect contents. The biggest characteristic that distinguishes the key management in DRM from other encryption systems is that the key should be kept from all users including the supplier, the distributor and the consumer. DRM key distribution methods can be divided into the symmetric key method and the public key method. In the symmetric key method, load is concentrated on a key distribution server and the server is involved in all contents transactions. On the other hand, the public key method is advantageous in terms of distribution, scalability and interoperability but it requires public key infrastructure (PKI). Therefore, a proper key management mechanism should be selected according to the characteristics of contents and application environment. For example, key management mechanism where load is concentrated on a key distribution server is not desirable if contents are distributed extensively and many role objects are involved in the flow of contents distribution as in the distribution of electronic books and music. (3) TRM (Tamper Resistant Module): A factor that hinders contents protection is that the contents must be decrypted at a moment for use. If the decryption key or decrypted contents are exposed to users in

processing or using the contents, contents may leak out without breaking into the encryption technology. TRM is a software or hardware module like a black box that hides detailed operations and stops its operation if it is modified. In DRM, software reengineering using a debugging tool is prevented by applying TRM technology to modules dealing with information on access rights, keys and decrypted contents. TRM is expected to be used as a key technology determining the safety of DRM system. (4) Digital watermarking: Watermarking technology, which has been spotlighted as one of copyright protection technologies in the last three years, inserts an invisible mark into digital contents as an evidence of ownership. Watermarking has difficulties in finding a profit model because it is applicable only after illegal reproduction has been made and the safety of its algorithm has not been proved. Recently a new soft watermarking technology was commercialized that is used to prevent the fabrication of certificates. Because detection is possible only after an incident has happened, however, the technology is not used widely. Currently watermarks are commonly used in printed documents.(5) Hooking: When an application (e.g. PowerPoint) is executed, it occupies a memory space, uploads necessary functions and controls actions made by the user. If the user makes a specific action (copy & paste, print, save, capture, etc.) the application replaces the address of DLL uploaded to the memory with that provided by DRM solution and controls the functions of the application and, by doing so, controls the use of documents according to the user's access right. This is memory hooking widely used in DRM solutions [1,5,6,7].

4 M-Learning Design Using DRM

MDRM-learning is a system designed to protect contents using DRM technology based on e-learning and M-learning. The structure of MDRM-learning is as in Figure 2.

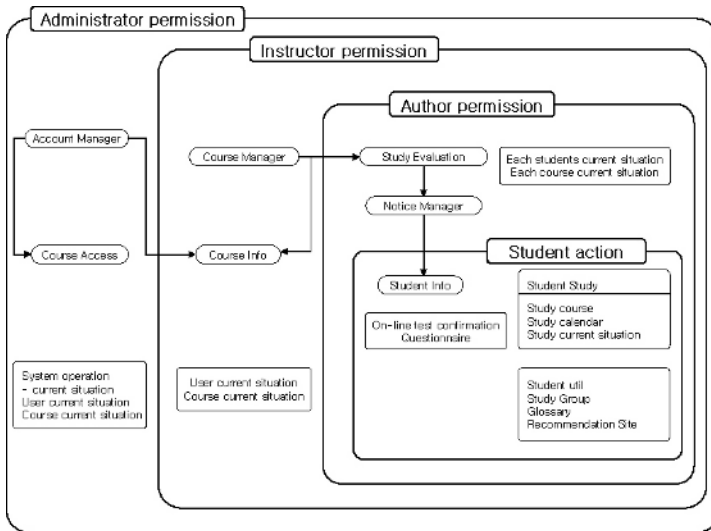


Fig. 2. Structure of MDRM-learning system

Based on the structure above, we designed 12 components and their functions are as in Table 1 and 2.

Table 1. Component function 1

Component	Function
Account Manager	Register a user or a group of users and change information on registered users
Notice Manager	Have multiple bulletin boards and manage notices, lectures, questions and other tasks related to bulletin board management
Report_up	Upload reports, distinguishing managers and learners

Table 2. Component function 2

Study Evaluation	Perform course application, report evaluation, online assessment, questionnaire survey, etc.
Course Manager	Register courses through self-paced method, instructor-led method, etc.
Student Info	Provide students with services such as personal information and mail
Student Study	Show timetables and progress of learning for students' learning management
Student Util	Form study groups and connect to the education broadcasting station
Curriculum Manager	Set curriculums
Course	Register and change students and course managers for each course
Contents Provide	Contents service component based on DRM
Course Access	Register students, lecturers and course managers

4.1 User Registration

MDRM-learning includes additional items to user information so that it can be used by all institutions (companies, schools, etc.) that may execute education. The user data is again divided into data of students, course managers and lecturers and, for the division, we also need information on courses. Course Manager Component transfers Course info to Account Manager Component. Based on the information, the User Connect module connects courses to users. This procedure can be diagrammed as in Figure 3.

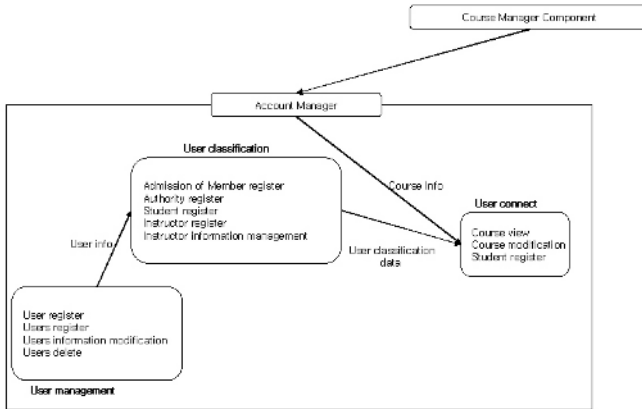


Fig. 3. User registration procedure

4.2 Course Registration

In MDRM-learning, a course can be executed in the self-paced method or in the instructor-led method. In the self-paced method, the learner checks his/her progress and completes learning by having a test for each learning material. In the instructor-led method, learning is made together with the lecturer and activities such as reports and online assessment occur in virtual classroom environment. In addition, teaching plans can be announced by open flow or step by step. Open flow is a tree structure, showing the entire course at once, and the step-by-step method announces teaching plans one by one over a period of time. In order to set lectures, curriculums are defined first and different types of learning are executed. This procedure is as in Figure 4.

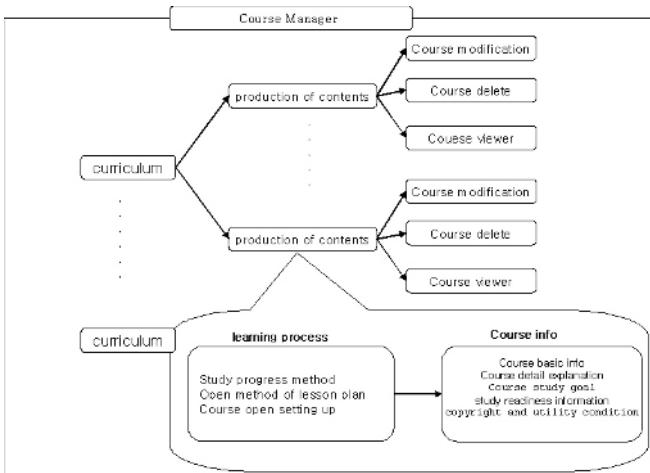


Fig. 4. Course registration procedure

4.3 Report Evaluation

Report_up uses bulletin boards and distinguishes between managers and learners. Learners can upload but can read, modify and delete only what they have uploaded. Managers can access all posted in the bulletin boards. This can be represented as in Figure 5.

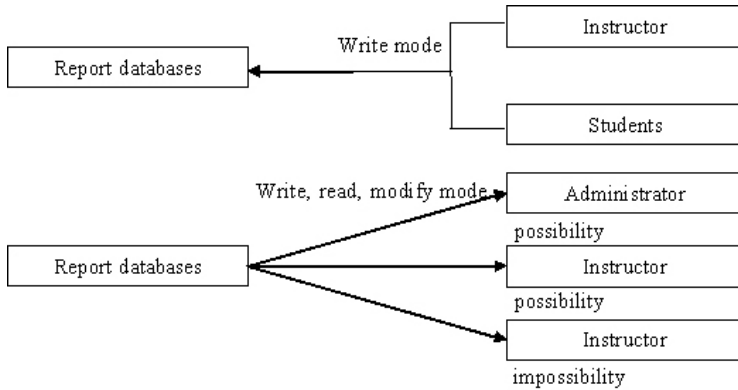


Fig. 5. Report evaluation

4.4 Personal Learning Schedule

This component shows information on currently attending courses and allows learners to make monthly and weekly plans to manage their personal schedule. In addition, this component shows the progress of each course. These functions are represented in Fig. 6.

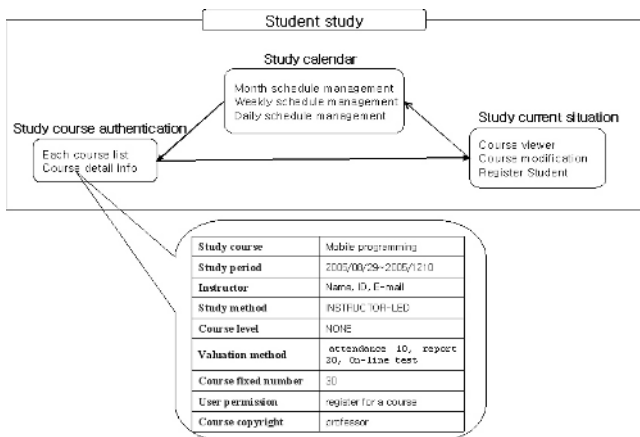


Fig. 6. Personal learning schedule

4.5 Classroom Platform

MDRM-learning was designed to use various bulletin boards and archives for notices related to courses, students' communities and additional learning. These bulletin boards and archives were designed to be created according to the platform set for each course. The basic platform is as in Table 3.

Table 3. Basic course platform

Item	Contents
Home	Contain basic contents of the course and summarize units in tree structure. Learners can choose to attend lectures randomly as they want or in order.
Notice	Show notices related to the course
Report	Submit reports in the course
Discussion room	Students discuss with one another in the course
Archives	Share materials related to the course or necessary in class
Chatting	Students in class can have real-time chatting with one another
Live classroom	Give a real-time video lecture
List	Show the list of students attending the class
Recommended sites	Link sites related to the course

4.6 Course Contents Service Using DRM

This shows the inner structure of DRM contents distribution component. DRM server is largely composed of encryption module, license management module, key management module (SSL module), transaction data management module, etc. and DRM client is composed of license key management module, decryption module, trace response protocol, etc. DRM server includes SSL server, encrypts files from the software encryption code developer, makes license keys and distribute them online. By the request of contents from a client, the server checks if payment has been made, has the encryption module on the Web encrypt the contents, allows download and records the information into the database. Using the information, DRM client manages user license, communicates with SSL client and checks the license. DRM client contains SSL client, which decrypts the encrypted file downloaded from DRM server and certified by the license and sends information on the user's mobile device to the server. Using the mobile device information, the server manages the user. Using the components and their functions listed in Table 1 and 2, we designed MDRM-learning for mobile environment.

5 Conclusions

The development of the wireless Internet and digital contents is activating Internet business and, in this situation, most online contents providers are supplying diverse contents attracting users' attention. These contents include not only texts but also multimedia such as music, images and videos. Various multimedia data are being applied to numerous areas like Internet broadcasting, education, news, sports, tourist information and experts' consulting and creating new services in the virtual space. The present study examined M-learning, which is e-learning system in wireless Internet environment, and analyzed DRM technology for contents protection in M-learning. We planned a MDRM-learning system focused on contents protection, which has been insufficient until now, by designing basic components of e-learning - user registration, course registration, report evaluation, personal learning schedule and classroom platform - as well as course contents service using DRM to support mobile systems in wireless environment. Further research is necessary on DRM and relevant technologies focused on contents security in education and wireless Internet environment as well as on education systems using these technologies.

References

1. "An Empirical Research on Important Factors of Mobile Internet Usage", Ho-young Kim, Jin-woo Kim, The Korea Society of Management Information Systems, Vol.12 No.3, [2002]
2. "A study on mobile DRM system technology in wireless internet service platform" Yong-gyu Lee, master's thesis 2005
3. "Design Strategies for the Tutorial Module to construct Intelligent Tutorings System" Eun-mi Im, master's thesis 1999
4. "Digital Rights Management Candidate Version 2.0", Open Mobile Alliance DRM W/G, 2004
5. "Platform technique of wireless Internet", KTF technique education data, 2003.5
6. Korea Institute of Information Security & Cryptology, "Next a generation network security technique", Korea Information Security Agency, 2002
7. "DRM Content Format Candidate Version 2.0", Open Mobile Alliance DRM W/G. 2004

Design of Security Session Reuse in Content-Based Load Distribution Server*

Seoksoo Kim¹ and Kunhee Han²

¹ Dept. of Multimedia Engineering, Hannam University, Daejeon, South Korea
sskim@hannam.ac.kr

² Division of Information & Communication Engineering,
Baekseok University, South Korea

Abstract. The present study evaluated the performance of security session reuse in a content-based load distribution server. Cluster Web servers, which have a highly expendable structure in response to gradually increasing Web server traffic, have been studied, focused on their scalability, client transparency and high availability. For the latest researches, techniques using an advantage of content - aware request distribution are proposed. And network security is very important. Many information exist which demand information security because development electronic commerce.

1 Introduction

Clustering technology makes a number of servers to process high-capacity services together. A cluster is composed of nodes and a manager. A cluster node processes actual tasks assigned to the cluster. In general, cluster nodes are set up to belong to a cluster. Depending on the role and job of a cluster, software can be specific or general. An example of software performing a specific role is an engineering calculation program mapped to a node, and programs for load balancing like Apache for belong to general software. Like Linux kernel manages the schedule and resources of all processors, the cluster manager manages resources and allocate them to each node. Basically one manager is necessary but sometimes cluster nodes can play the role of cluster manager and, in a large-scale cluster, there can be multiple cluster managers. There are clustering techniques such as HPC, fail-over and load balancing. First, HPC is generally called Linux clustering or Beowulf project.

Beowulf provides a system of high processing capacity by combining the processing capacities of several sub-systems. In the system, which was designed for scientific uses or CPU jobs, only programs made according to API can allocate their jobs to multiple systems [1],[2]. Fail-over is similar to load balancing but there is a slight difference. While all nodes work together in load balancing, backup servers work only when the primary server fails in fail-over.

Modifying load balancing we can implement load balancing and fail-over functions at the same time. Lastly, load balancing is an essential technology for building

* "This work was supported by a grant No. (R12-2003-004-03003-0) from Ministry of Commerce, Industry and Energy".

large-scale websites. This technology puts multiple Web server nodes around and distributes load using the management tool at the center. A characteristic of this technology is that the nodes do not have to communicate with one another. Using load balancing, each node can process requests fittingly to its capacity or load. Or it can process tasks assigned by the cluster manager and this is the content-based load distribution server system proposed in this research [3],[4].

2 Operating Methods of Web Cluster System

Load distribution clustering may operate in one of three ways - direct forwarding, IP tunneling and NAT.

2.1 Direct Routing

When a user accesses a service provided by the server cluster, a request packet forwarded to the virtual IP address (the IP address of the virtual server) is sent to the load distribution server. The load distribution server (LinuxDirector) checks the destination address of the packet and the port number. If the content is coincident with the service of the virtual server, the cluster selects a real server according to the scheduling algorithm and adds a new connection to the hash table recording connections. The load distribution server forwards the packet directly to the selected server. If the incoming packet is corresponding to the connection and the selected server can be identified in the hash table, it is again forwarded directly to the packet. If the server receives the forwarded packet, it finds the address of alias interface or local socket in the packet, processes the request, and returns the result directly to the user. If the connection is released or time is over, the connection is removed from the hash table. The load distribution server simply changes the MAC address of data frame to the selected server and resends it to the LAN. For this reason, the load distribution server and each server should be linked to each other within the same physical segment. Because transmission does not have to be via the load distribution server, it is fast with less overhead.

2.2 IP Tunneling

IP tunneling is also called IP encapsulation, a technology putting an IP datagram into another IP datagram. Using this technology, a datagram forwarded to a certain IP address can be encapsulated and redirected to a different IP address. IP encapsulation is generally used in Extranet, mobile-IP, IP-multicast, tunneled host or network, etc. When a user access a service provided by a server cluster, a request packet forwarded to the virtual IP address (the IP address of the virtual server) is sent to the load distribution server. The load distribution server checks the destination address of the packet and the port number. If the content is coincident with the service of the virtual server, the cluster selects a real server according to the scheduling algorithm and adds a new connection to the hash table recording connections. The load distribution server encapsulates the packet into an IP datagram and forwards it to the real server. If the incoming packet is corresponding to the connection and the selected server can be identified in the hash table, the packet is encapsulated and sent to the selected server.

On receiving the encapsulated packet, the server decapsulates it, processes the request, and return the result to the user according to the routing table of the server. If the connection is released or time is over, the connection is removed from the hash table. In IP tunneling, the load distribution server assigns incoming requests to real servers and replies are sent directly from the servers to the users. As a result, the load distribution server can process more requests and manage over 100 real servers. In addition, the load distribution server can prevent bottleneck in the system. Using IP tunneling, the number of server nodes can be increased significantly. Even if the load distribution server has a 100 Mbps full-duplex network adapter, the maximum throughput of the virtual server can reach 1Gbps. Using the characteristic of IP tunneling, we can build a virtual server of extremely high performance and the technology is particularly suitable for virtual proxy servers. When a proxy server receives a request, it can connect to the Internet, get an object and send it directly to the user. However, IP tunneling must be supported by all the servers.

2.3 NAT(Network Address Translation)

As IPv4 lacks IP addresses and has several problems in security, an increasing number of networks are using private IP (10.0.0.0/255.0.0.0, 172.16.0.0/255.240.0.0, 192.168.0.0/255.255.0.0) that cannot be accessed from the Internet. In order for a host on a private network to connect to the Internet or for the Internet to connect to a host on a private network, it needs NAT (network address translation) function. NAT maps a group of IP addresses to another group. N-to-N mapping is called static NAT and M-to-N (M>N) mapping is called dynamic NAT. Network address port conversion is an extended function to basic NAT, converting multiple network addresses and TCP/UDP ports to a single network address and TCP/UDP port. It is called N-to-1 mapping and used in IP masquerading on Linux. In Linux, a virtual server performs network address port conversion through NAT. Linux IP masquerading code is used and Steven Clarke's port forwarding code is reused. When a user accesses a service provided by the server cluster, a request packet forwarded to the virtual IP address (the external IP address of the load distribution server) is sent to the load distribution server. The load distribution server checks the destination address of the packet and the port number. If the content is coincident with the service of the virtual server according to the rule table of the virtual server, the cluster selects a real server according to the scheduling algorithm and adds a new connection to the hash table recording connections. The destination address and the port of the packet are changed fittingly to the selected server, and the packet is forwarded to the server. If the incoming packet is corresponding to the connection and the selected server can be identified in the hash table, the packet is reformed and forwarded to the selected server. If a response packet comes back, the load distribution server changes the source address and the port fittingly to virtual service. If the connection is released or time is over, the connection is removed from the hash table. If NAT is used and the real server supports TCP/IP, the real server can be concealed completely for higher security but this system has a limitation in scalability. Based on ordinary PC servers, if the number of server nodes is over 20, the load distribution server may have bottleneck. It is because the load distribution server has to change packets whenever they come in and go out.

Let us assume as follows. The average length of a TCP packet is 536 bytes. The delay caused by packet change is 60 μ s (for a Pentium processor, may be shorter with a processor of higher performance), and the maximum throughput of the load distribution server is 8.93Mbytes/s. If the average throughput of a real server is 400Kbytes/s, the load distribution server can schedule 22 real servers [1],[2],[3],[4].

3 Web Cluster System Scheduling Algorithm

Such a load distribution clustering system uses a scheduling algorithm for load distribution. There are several scheduling algorithms as follows.

3.1 Round-Robin Scheduling(RR)

This algorithm simply delivers requests, ignoring all situations including the server and network conditions. This is the simplest and can be efficient if all servers and networks are of the same specification.

3.2 Weighted Round-Robin Scheduling(WRR)

Here, a weight means giving a weight to a specific thing. A weight is given to a specific server so that it processes more requests if the server is superior to others in capacity or can process more requests because of its environment, processing speed for a given type of requests, etc. Using weighted round-robin scheduling, the server does not need to count the number of network connections and can manage a larger number of servers because scheduling overload is less than that in dynamic scheduling algorithm. If the number of requests is large, however, there can be dynamic load imbalance among real servers.

3.3 Least Connection Scheduling(LC)

In least connection scheduling, a new request is directly connected to the server with the least connections. Because this algorithm has to count dynamically the number of actual connections to each server, it is one of dynamic scheduling algorithms. In a virtual server composed of servers with similar performance, big requests do not concentrate on a specific server and, as a result, even a high connection load is distributed very effectively. The fastest server can process more network connections. Therefore, even if the servers in a virtual server vary in processing capacity, they may work very efficiently. In fact, however, the algorithm cannot produce very satisfactory performance because of the TIME_WAIT of TCP. TCP TIME_WAIT is usually two minutes but a website with a large number of connectors may have to process thousands of connections within the two minutes. If Server A has a twice higher processing capacity than Server B, it will face TCP TIME_WAIT after processing thousands of requests. However, Server B just waits until thousands of requests are all processed. For this reason, least connection scheduling can be inefficient in load distribution if the virtual server is composed of servers with different processing capacities.

3.4 Weighted Least Connection Scheduling(WLC)

Weighted least connection scheduling, which is a part of least connection scheduling, can give a performance weight to each real server. A server with a high weight can receive more requests. The virtual server manager can give a weight to each real server. Network connects are allotted based on the number of actual connectors, which is the weight ratio. The base weight is 1. The performance of a cluster system is determined by the scheduling algorithm. Thus, a suitable algorithm should be selected for a system to be built [4],[5],[6],[7].

4 Implementation of Security Session Reuse

This algorithm generates a character string, encrypts it using an algorithm above and transmits it to VS. The encrypted data sent to VS is transmitted to each DPS by the temporary handshake algorithm. The implemented algorithm is as follows.

```

for(i = 0; i < num_chat; i++)
{if(FD_ISSET(client_s[i], &read_fds)){
if((n = recv(client_s[i], rline, MAXLINE, 0)) <= 0)
{removeClient(i);
continue;}
if(strstr(rline, escapechar) != NULL)
{removeClient(i);
continue; }
rline[n] = '\0';
for(p=0;p<1;p++)
{client_s[j]=DES_Decryption(client_d[q]);
for(usenum=0; usenum<reuse; usenum){
for (k=0; k < client1_weighted_num ; k++ )
{send(client_e[q], rline, n, 0);
printf("%s\n", rline);
printf("q = %d\n",j);
} j++;
} q++;
for (k=0; k < client2_weighted_num ; k++ )
{ send(client_e[q], rline, n, 0);
printf("%s\n", rline);
printf("q = %d\n",j);
} j++;
} q++;
for (k=0; k < client3_weighted_num ; k++ )
{ send(client_e[q], rline, n, 0);
printf("%s\n", rline);
printf("q = %d\n",j);
} j++;
} q++;
if (j>4)
{j=1;
q=1;}}}}

```

5 Performance Evaluation

In Figure 1, the clients were given weights 15, 18 and 7 respectively and tested 6 times for a specific length of time, and Figure 2 is the result of applying security session reuse ratios of 0, 10, 20 and 30. In the graphs above, security session reuse ratio was obtained by quantifying the volume of data, to which security sessions were applied. Every time, encrypted data was decrypted in VS, DPS is confirmed, and the data is sent to the DPS. The process is repeated but, with the introduction of reusability, data is decrypted at regular intervals of time or number and transmitted to the corresponding DPS. According to the result of the performance evaluation, the performance of security session reuse went down when weights were small, and it went up when weights were large. Based on the results, security session reuse in an actual content-based load distribution server must reuse sessions in consideration of the service, to which the reuse is applied and appropriate distribution. If traffics allocated to servers are different according to content a low reuse ratio will be desirable, and if they are similar a high reuse ratio will be desirable. However, this result came from data in an artificially crated setting and it may be somewhat different in real environment.

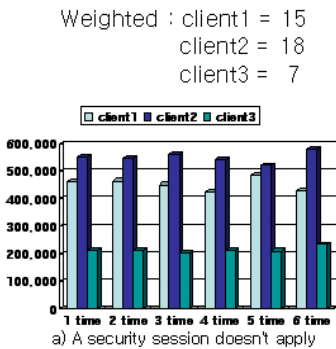


Fig. 1. Performance evaluation 1

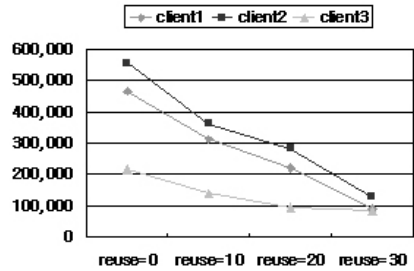


Fig. 2. Performance evaluation 2

6 Conclusion

Cluster Web servers, which have a highly expendable structure in response to gradually increasing Web server traffic, have been studied, focused on their scalability, client transparency and high availability. Recently, researchers on cluster Web servers are paying attention to content-based load distribution that distributes clients' requests among the cluster server nodes according to the type of content or service requested. Due to the characteristic of Web workload, accesses are frequently concentrated on a specific file not the whole files in the site. Using the characteristic, researches on content-based load distribution seek to improve the overall performance of a cluster system through the efficient use of the memory in cluster server nodes. Based on the results, security session reuse in an actual content-based load distribution server must reuse sessions in consideration of the service, to which the reuse is applied and

appropriate distribution. If traffics allocated to servers are different according to content a low reuse ratio will be desirable, and if they are similar a high reuse ratio will be desirable. However, this result came from data in an artificially crated setting and it may be somewhat different in real environment.

References

1. W. Zhang, "Linux Virtual Server for Scalable Network Services," Linux virtura server project,1998.
2. W. Zhang and et al., Linux virtual server project.1998.
3. V.Kumar, A.Grama, and V.N.Rao, Scalable Load Balancing Techniques for Parallel Computers, *Journal of Distributed Computing*, pp.60-79, 1994.
4. T. Schroeder, S.Goddard, and B. Ramamurthy, "Scalable Web Server Clustering Technologies." *IEEE Network*, pp.38-45, 2000.
5. V. S. Pai, M. Aron, G. Banga, M. Svendsen, P. Druschel, W. Zwaenepoel, and E. Nahum, Locality -Aware Request Distribution in Cluster - based Network Server s, In *Proceedings of the 8th Conference on Architectural Support for Programming Languages and Operating System*, San Jose, CA, Oct . 1998.
6. M.Aron, D.Sanders, and P.Druschel, Scalable Content-Aware Distribution in Cluster-based Network Servers. *Proceedings of the 2000 USEMIX Technical Conference*, 2000.
7. V. Pai, M.Aron, G.Banga, M.Svendsen, P.Druschel, W.Zwaenepoel, and E. Nahum Locality Aware Request Distribution in Cluster-based Network Servers. *Architectural Support for Programming Languages and Operating systems* pp 1-12, 1998.

Design of POC System in Ubiquitous Environment

Seoksoo Kim and Gilcheol Park*

Dept.of Multimedia Engineering, Hannam University,
Daejeon, South Korea
sskim@hannam.ac.kr

Abstract. Point of Care system is a medical service system based on wireless communication that creates real-time medical service environment using mobile devices, provides prompt and accurate patient-oriented information service, and improves the efficiency of medical and administrative works in hospital. This paper designs POC system for personal information protection which is available in Ubiquitous Computing environment. POC system design is focused on the scheme for protecting personal information through analyzing the information hazards in Ubiquitous environment. This makes a significant contribution to the medical information service providing people with easy to access services.

1 Introduction

POC system is a medical service system based on wireless communication that creates real-time medical service environment using mobile devices, provides prompt and accurate patient-oriented information service, and improves the efficiency of medical and administrative works in hospital. Combined with the recent development of mobile technology and home networking technology, this system have functions of controlling and monitoring home appliances as well as transmitting video sources to mobile users through multimedia stream server. In this way, the use of mobile technology is expanding its areas [1] particularly in the area of medical service.

The present study was focused on users with mobile terminals on wireless infrastructure in systems providing medical information service as well as on services for protecting medical information provided to the users. Users who receive medical information through their mobile terminals are simply called mobile users.

The development of information communication technology is demanding advanced forms of medical information services in ubiquitous environment and, as a result, medical information services are not limited to medical service providers but are provided directly to patients.

Such a development is mainly thanks to the advancement of wireless networks and terminals, through which mobile users can access the services. For secure service of medical information between mobile users and service providers, the following technologies must be supported.

* Corresponding author. "This work was supported by a grant No. (R12-2003-004-03003-0) from Ministry of Commerce, Industry and Energy".

First, reliable authentication is required between mobile users and the medical information service system. If participants are not identified through authentication between mobile users and the institution providing information service, the service can be modified and is not reliable any more. The present study used two-factor authentication as a safe method of verification between mobile users and a medical information service provider.

Second, medical information needs to be classified according to the type of authorized users. When medical information is sent to a mobile user, the extent of disclosure of the information should be different according to the user's status. This is because the same type of medical information is demanded from various areas and, as a result, the information is exposed to a high risk of disclosure. In this study, we proposed grading mobile users, designed a system that processes information according to user level, and defined XML-based data provided to classified users.

Third, in order to provide medical information to mobile users, we need to design the hospital system that provides the medical information. This study designed a system in connection to EMR (Electronic Medical Record), which is most commonly adopted by hospitals. In addition, we designed according to the recommendation of HL7 (Health Level 7) [2]. In the present dissertation, Chapter 2 analyzed base technologies related to medical information, and Chapter 3 designed POC system for protecting personal information. Chapter 4 drew conclusions and mentioned future research plans.

2 Relevant Researches

2.1 Mobile Service

Mobile service is commonly used in stock exchange, bank service, games, etc. through accessing wireless Internet sites using a mobile terminal. Mobile service is an area of wireless Internet application and is divided into four categories as follows: first, communication services through the exchange of data other than voice call such as electronic mail, SMS (Short Message Service), fax and UMS (Unified Messaging System); second, value-added service of useful information or direct access to useful information such as information search, weather, travel, job offer/job hunting, news, personal information management, game, club and prize competition; third, e-commerce involving the commercial transaction of goods and services such as banking, financing, stock exchange, shopping, ticketing, lotto, auction, joint purchase and image service; and fourth, location providing information like address and telephone number on specific places based on the location of the user's mobile phone such as banks, restaurants, gas stations and medical institutions.

Because mobile services provide various types of information in open environment, it is difficult to protect the information. Mobile policies are being developed with the object of providing users with value-added security service in pure mobile network environment or the environment of interoperation between mobile networks and fixed networks and, by doing so, creating new service models for network operators and safe mobile services for users.

As in Figure 1, a model for mobile security policies is composed of a terminal issuing requests for signals, security gateway negotiating security algorithm and security level with the terminal, a terminal receiving signals, and the AAA (Authentication, Authorization, Accounting) server collecting information on charges for the use of security service.



Fig. 1. Mobile security policy model

2.2 Personal Information in Ubiquitous Environment

'Ubiquitous' means the ability to access the network and get information at any time, in any place and with any device, which is pursued by all newly introduced services today. However, public institutions and companies have not been successful in ubiquitous services. One of the reasons was the difficulty of information protection. In particular, contrary to individuals' will, personal information, which is the biggest issue concerning information protection, is being copied and distributed via all kinds of media though the Internet, various marketing events, diverse communities, and questionnaire surveys. The infringement of personal information is even more serious in ubiquitous environment. Accordingly, it is necessary to analyze the types of infringement of personal information in detail in order to provide medical information in ubiquitous environment in a more secure way. Moreover, in response to possible abuse of personal medical information, security is emerging as a national and legal issue [3]. Personal information can be infringed in various ways and thus it is essential to protect personal information in ubiquitous computing environment. In medical information service as well, information can be infringed, and more various threatening elements exist in wireless network environment [4]. Thus, in POC environment, we need to design a system to protect users' personal information and medical information.

3 POC System Design for Protecting Personal Information

We designed a POC system for protecting personal information in consideration of the following points.

- Support the active discovery and management of mobile terminal resources in wireless environment.
- Make a request for service and return data in a reliable and stable manner.
- Authenticate users safely considering both wired and wireless environment.
- Manage message security using encryption algorithm.

3.1 POC System Structure for the Protection of Personal Information

The POC system for protecting personal information is composed of mobile user application, hospital server system and security system between mobile users and the hospital server system, and its structure is as follows.

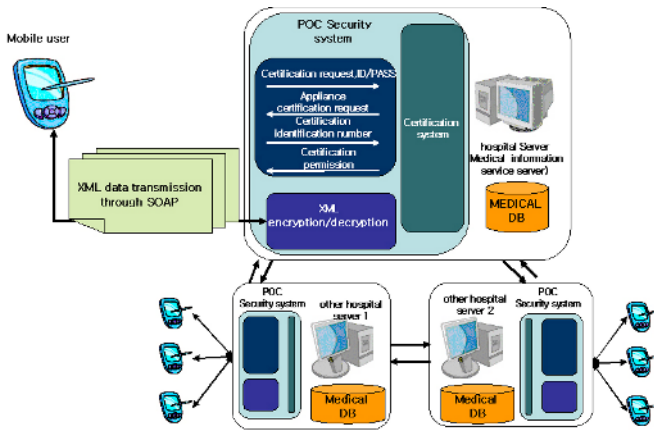


Fig. 2. POC system design for the protection of personal information

In Figure 2, the hospital server system performs the authentication of a mobile user using the patient’s information in the medical database in the server. The medical database has medical information related to the mobile user. The server system uses the authentication system that controls the procedure of authentication. The authentication system keeps the user’s ID and password as well as information to verify the user’s mobile device. In addition, the authentication system identifies the type of the user according to the user classification policy and provides information on XML encryption/decryption. The XML encryption/decryption system encrypts information according to the level of the authenticated user and, at the same time, provides the mobile user with a decryption module. Lastly, the user application manages the connection to the hospital server facilitates information exchange between the server and users. The application must provide user-friendly interface and methods to use so that users can use medical information services conveniently. Besides, it provides encrypted information using SOAP (Simple Object Access Protocol) in order to remove the risk of information leakage when supplying a key for decryption to read information.

3.2 Gradation of Authentication Level

For the efficient management of users, we need to grade users. Gradation is performed through authentication and the contents of provided medical information become different according to the level given to each user. Services provided according to users' level are as follows.

Table 1. Service contents according to the level of mobile users

	Personal information	Request for treatment and information on diseases	Payment	Treatment process	Auxiliary Services (CT, MRI)	Basic Information on the hospital and reservation
1. General clients						■
2. Patients	■	■	■	□	□	■
3. Doctors	■	■		■	■	
4. Assistant staffs	□	□		□	■	
5. Hospital administrators	□		■			■

□: Basic contents ■: Detailed contents

In Table 1, users were classified into five levels - general clients, patients, doctors, assistant staffs, and hospital administrators. A general client is first provided with basic hospital information by the POC system and request medical services through the system. After the first medical service, the client is moved to the level of patient, updating personal information necessary for treatment and provided with detailed information such as required treatments and the name of disease, information such as payment, basic treatment process, incidental procedures such as CT and MRI, and reservation service. A doctor can use all detailed information and medical services related to patients, and is provided with relevant materials useful in treating the patients. An assistant staff can view basic patient information and update and view detailed information generated from his/her work process. Lastly, a hospital administrator is provided with basic patient information as well as information on their payments and reservations. In this classification of services according to mobile user, doctors need to access detailed and various patient information including name, age, the history of family diseases, hospital records, etc. in order to provide accurate medical service. On the other hand, hospital administrators need to access only basic personal information as well as details on payments. By processing and providing information according to information users' level, we can reduce unnecessary disclosure of information. In addition, encryption of necessary information only improves the efficiency of information processing.

3.3 User Authentication Process

The designed POC system uses two-factor authentication to verify users. Two-factor authentication first verifies the user using his/her ID and password and then takes another step of authentication verifying information on the physical device that the user uses to get the information. This method identifies users in a more reliable way. In case of ordinary PDAs or smart phones, the secondary authentication is made without the user's knowledge using the MAC address of the LAN card supporting the wireless Internet. For cellular phones, the user's telephone number registered at the telecommunication company is sent as the authentication number, which is used in the secondary authentication. The former is convenient for users but it may require the additional installment of hardware, and the latter can be implemented easily in the current system but users may feel irritated as they are requested authentication twice.

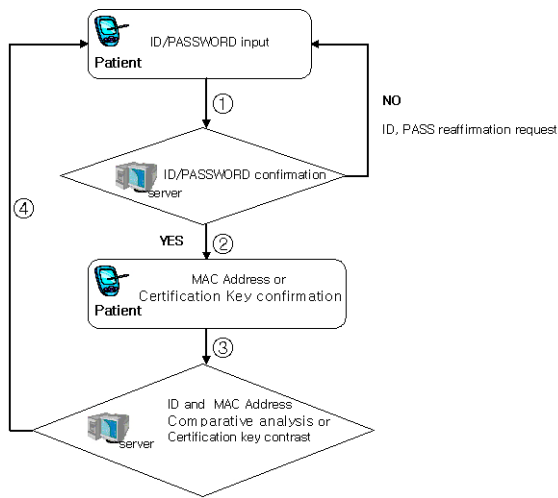


Fig. 3. User authentication process in two-factor authentication system

The proposed POC system takes a process as in Figure 3 for two-factor authentication. The order of authentication is: ① the user requests authentication with ID and password; ② the server verifies the user using the ID and password and requests MAC address of the user's machine or sends the authentication number using the number of a specific telecommunication company; ③ the user resend the MAC address or the provided authentication number to the server; ④ the server compares the MAC address sent by the user with the ID and password verified in the first authentication or confirms the provided authentication number and, based on the result, gives the user the right to access the service. The authentication process is applied to all types of users. Through authentication, each user's level is confirmed and medical information in the medical database is retrieved, updated or changed. Doctors and assistant staffs who lead medical services and hospital administrators

who carry out administrative jobs can use the service conveniently through only the first authentication using fixed terminals provided by the hospital for the internal use of the POC system.

3.4 XML Authentication and Transmission for Information Protection

After authentication, the user is provided with service according to his/her level and the level can change while the user is accessing the service. For general clients, authentication is made by their first use of basic hospital information and the first use of the reservation service. After receiving the first medical service, however, their level is moved up to that of patients and the system must be able to deal with the change of users' level immediately. Thus, after the first medical service, the proposed system provides medical information XML-based and encrypted. That is, the document contains medical information but, for unauthenticated users, it is provided as an encrypted XML-based document. Here, XML encryption methods used by the system are XML Digital Signature [5],[6] and XML Encryption [7].

XML Digital Signature is an XML signature technology recommended as a standard by W3C, expressing existing electronic signatures in XML. Like existing electronic signatures, the technology can put a signature to the whole document. In addition, a signature can be put only to a part of a document using XML transform technology, which enhances reusability. The method of encrypting and authenticating XML itself reduces the load upon the server in the system, and the stability of information can be enhanced by providing documents in the form of contents.

Figure 4 shows the structure expressed in signature elements in an XML electronic document [8]. The structure is as follows.

- Signature.** Parent element in the document with XML electronic signature
- SignatureValue.** Actual value of electronic signature generated using the algorithm defined in SignatureMod
- SignedInfo.** Canonicalization algorithm containing signature algorithm or reference
- CanonicalizationMethod.** Specify algorithm necessary for standardizing XML documents
- SignatureMethod.** Specify algorithm used to generate an actual signature value
- Reference.** Can be included in the signature document or referred to at a different place using ID
- Transforms.** Specify how the signer obtains message digest objects
- DigestMethod.** Specify digest algorithm for generating a digest value
- DigestValue.** Include the digest value generated through DigestMethod
- KeyInfo.** Include information on the key generated by key generator

In order to send verified XML documents, SOAP is used. For the transmission, we need to understand SOAP standards related to security such as message format, encoding, RPC convention, transmission and the properties of message with attached files [9],[10]. SOAP is largely divided into SOAP Envelope containing information on contents inside the message and one who is related to the message, SOAP Encoding Rules that are serialization mechanisms used in exchanging information on data types defined in application programs, and SOAP RPC that is conventions used to express RPC calls and responses to the calls.

```

<Signature ID?><SignedInfo><CanonicalizationMethod/>
  <SignatureMethod/>
  (<Reference URI?>
    (<Transforms>)?
    <DigestMethod><DigestValue>
  </Reference>)+
  </SignedInfo> <SignatureValue> (<KeyInfo>)? (<Object ID?>)*
</Signature>
    
```

Fig. 4. Structure of XML signature

3.5 Provision of Information with the Change of Users' Level

The level of mobile users changes frequently during the process of medical service. At first a user gets hospital information as a general client and uses the reservation system to get medical service. After getting the first medical service, the user's level is moved up to that of patient and this change must be reflected immediately in the system. Thus, the method of information provision with the change of users' level was designed as follows.

Figure 5 shows how to provide information when a user's level has been changed.

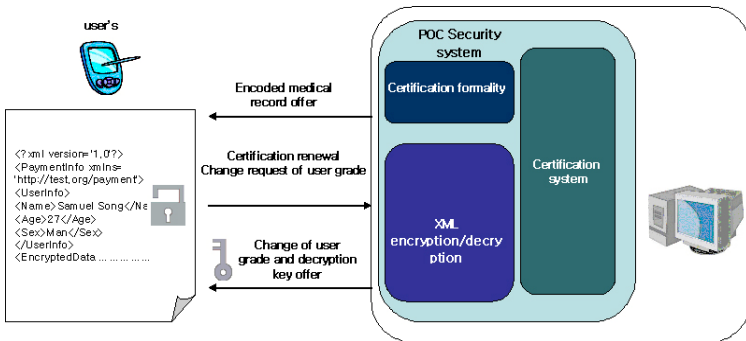


Fig. 5. Provision of information with the change of users' level

When a general client has received a medical service, the XML-based document provided to the client contain the details of the medical service but encrypted. Because the user has not been authenticated, he/she cannot read information on required medical treatments and the name of the disease. To read the encrypted information, the user requests the hospital server to upgrade his/her authentication level. By the request, the server checks the user's information and changes the level. In addition, the server provides an authentication key to the mobile user. The process of changing authentication level between the server and a mobile user must be executable immediately when the user receives and read encrypted information.

4 Conclusions and Future Research Plans

POC system can provide wireless communication technology and medical information effectively at any time and in any place. The usability and the necessity of POC system are getting higher thanks to the rapid spread of mobile terminals and the improvement of terminal performance. The present study designed POC system for the effective provision of medical information service directly to users using wireless terminals in wireless network environment. In addition, we designed a method of personal information authentication and a medical information protection system in the POC system in order to protect information from threatening elements in wireless network environment. In the future, we plan to study systems exchanging medical information through wireless networks. Another research topic is a system that collects information actively in response to the change of situation and manages medical information systematically.

References

1. D. Bushmitch, W. Lin, A. Bieszczad, A. Kaplan, A.Papageorgiou, A. Pakstas, "A SIP-based Device Communication Service for OSGi Framework", Proc. of CCNC 2004 PP.453-458, 5-8 Jan., 2004.
2. HL7, <http://www.hl7.org/Press/20040427b.pdf>
3. Hyun –Cheol Jung "Security of Medical Information System", Korean Information Science Society Vol.16 NO.12, 1998.12
4. Mishra, A.,and rbaugh, W. "An Initial Security Analysis of the IEEE 802.1X Standard", February, 2002.
5. IETF/W3C,"XML-Signature Requirements (Working Draft)," Oct. 1999, <http://www.w3.org/TR/1999/WD-xmldsig-requirements-19991014.html>
6. IETF/W3C, XML-Signature Syntax and Processing (Working Draft), Oct. 2000, <http://www.w3.org/TR/2000/WD-xmldsig-core-20001012/>
7. W3C XML Encryption WG, "XML Encryption Charter," <http://www.w3.org>,2001
8. W3C, "XML-Signature Syntax and Processing", 2002
9. W3C, "SOAP Version 1.2 Part 1 : Messaging Framework", Candidate Recommendation 19 December 2002, <http://www.w3.org/TR/2002/CR-soap12-part1-20021219>
10. W3C, "SOAP Version 1.2 Part 2 : Adjuncts", Candidate Recommendation 19 December 2002, <http://www.w3.org/TR/2002/CR-soap12-part2-20021219>

The Performance Evaluation of OFDM/HL-16QAM System for Optimizing Image Transmission Quality in Wireless Fading

Jae-min Kwak¹, Yang-sun Lee², and Sung-eon Cho³

¹ SoC Research Center, Korea Electronics Technology Institute,
68, Yatap-dong, Bundang-gu, Seongnam-shi, Gyeonggi-do, 463-816, Korea
kjm@keti.re.kr

² Department of Computer Engineering, Mokwon University,
800, Doan-dong, Seo-gu, Daejeon, 302-729, Korea
yslee@mokwon.ac.kr

³ Department of Information Communication, Sunchon National University,
Sunchon-shi, Chonnam, 540-472, Korea
chose@sunchon.ac.kr

Abstract. We have evaluated the performance of an OFDM/HL-16QAM system for achieving high quality image transmission. OFDM/HL-16QAM system has the capability of reliable high speed data service and simultaneous transmission of differentiated two quality of data streams in severe multipath fading channel. For application of image transmission, we have proposed the OFDM/HL-16QAM system adopting fixed length DCT based coding to achieve reasonable image compression rate and obtained the optimal hierarchical modulation parameter maximizing PSNR(Peak Signal to Noise power Ratio) of received still image. Then, it has been shown that the received image quality of the proposed system with optimized hierarchical modulation parameter is better than that of conventional OFDM/16QAM system. From the result, it is found that the proposed system is more effective for mobile multimedia services.

1 Introduction

Recently, there has been an increasing demand for multimedia transmission, such as the transmission of text data, voice and images, in mobile communication systems[1], [2]. In order to provide such multimedia services with high speed transmission and higher bandwidth efficiency, OFDM is expected to be the most appropriate scheme.

In OFDM, transmission is carried out in parallel on the different frequencies [3]-[4]. That is, the entire channel is divided into many narrow band subchannels, which are transmitted in parallel, thereby, increasing the symbol duration and reducing ISI. The carrier spacing is selected such that modulated carriers are orthogonal over a symbol interval. In addition, a guard interval is inserted to combat the frequency selectivity of the channel. Therefore, OFDM is an effective technique for combating against multipath fading and for higher rate transmission over mobile environment [5], [6].

In paper [1], hierarchical transmission system was proposed to transmit still image in mobile communication. The system composed of hierarchical source coder and corresponding channel coder, divides the information into several layers according to their significance, and transmits each layer with different reliability according to their layers. In paper [7], the performance of an image transmission system employing DCT based fixed length coding scheme for achieving reasonable compression rate was evaluated.

In this paper, we propose the OFDM/HL-16QAM system adopting DCT based fixed length coding scheme and show that the system is effective for image transmission by comparing received image quality of OFDM/HL-16QAM system with that of OFDM/16QAM system. Also, the optimum hierarchical parameter maximizing the received image PSNR(Peak Signal to Noise power Ratio) is suggested and the upper bound and lower bound of PSNR achieved by the proposed system are obtained.

This paper is organized as follows. In section 2. the principle of hierarchical 16QAM adopting DCT based fixed length coding is described. Section 3 shows the system model of proposed OFDM/HL-16QAM and the signal representation of the system. In section 4, simulation results are shown and the paper is concluded in section 5.

2 Hierarchical 16QAM with DCT Based Fixed Length Coding

The block diagram of hierarchical 16QAM system is shown in figure 1. After an image source data is divided into subblocks, they are converted to frequency domain by 2 dimensional DCT.

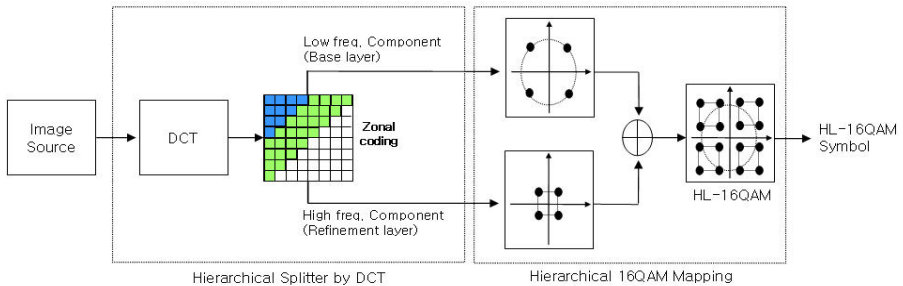


Fig. 1. Block diagram of hierarchical 16QAM system with DCT based fixed length coding

Then, DCT coefficients are quantized, and DCT based fixed length coding is applied for image compression as shown in figure 2 (“lenna” : 256 level monochrome image). By using the bits allocation map in figure 2, where the number in each square shows the number of bits allocated for each DCT quantized coefficient, one subblock image (8x8 pixels, 8 bits per pixel) is compressed (compression rate : 22.27%), and the compressed image results in 30.7[dB] of PSNR. In this paper, these DCT based fixed length coded data are divided again to lower frequency components (base layer) and higher frequency components (refinement layer), then final hierarchical 16QAM mapped output signals which consists of 4 bits are generated.

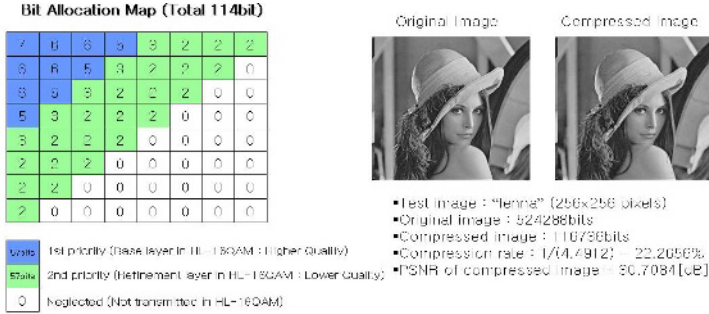


Fig. 2. Bit allocation map and the test image "lenna" (256 level monochrome) with no transmission error

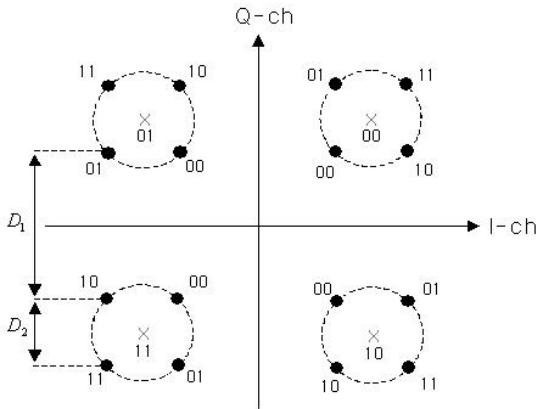


Fig. 3. Constellation diagram of the hierarchical 16QAM

The constellation diagram of hierarchical 16QAM modulation is shown in figure 3. In this figure, D_1 and D_2 are the minimum distance between clusters and the minimum distance within the cluster, respectively. The first two bits determine the one of the four subplanes and the next two bits determine one of the four constellation points within the cluster. In this system, by controlling hierarchical modulation parameter ($\lambda = D_2/D_1$), the performance of each two layered bits can be adjusted. In AWGN channel, the BER(P_{e1}) of base layer and the BER (P_{e2}) of refinement layer are approximately given by [8],

$$P_{e1} = \frac{1}{4} \operatorname{erfc}\left(\frac{\gamma}{4\lambda^2 + 4\lambda + 2}\right) + \frac{1}{4} \operatorname{erfc}\left(\gamma \cdot \frac{4\lambda^2 + 4\lambda + 1}{4\lambda^2 + 4\lambda + 2}\right). \tag{1}$$

$$P_{e2} = \frac{1}{2} \operatorname{erfc}\left(\frac{\lambda^2 \gamma}{4\lambda^2 + 4\lambda + 2}\right), \tag{2}$$

Where γ is the CNR at the receiver front end and $\text{erfc}(\cdot)$ is complementary error function defined by, $\text{erfc}(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty \exp(-t^2) dt$.

Since the hierarchical 16QAM mapping has input bits which is coded by DCT based fixed length coding, it is expected that the reasonable compression rate can be obtained and there may be the optimum hierarchical modulation parameter maximizing the PSNR of reconstructed image at the receiver in fading environments. The PSNR of 256 level monochrome image is defined as [6],

$$PSNR = 10 \log_{10} \frac{255^2}{\sigma_q^2} [dB], \tag{3}$$

Where σ_q^2 is the mean square of the difference between the original and the compressed image.

3 System Model of OFDM System Employing Hierarchical 16QAM

The block diagram of OFDM transmitter employing hierarchical 16QAM is represented in figure 4, where, for simplicity, we have ignored the filters inherent in all communication systems. The N serial hierarchical 16QAM data symbols, spaced by $\Delta t = 1/f_s$ where f_s is the symbol rate and Δt is symbol duration of serial data, are first converted to parallel form by serial-to-parallel (S/P) converter and then modulate N subcarriers.

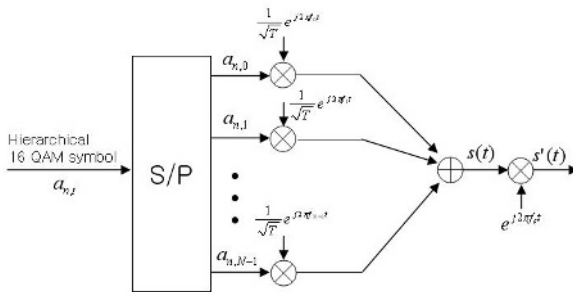


Fig. 4. The structure of OFDM transmitter

They are all added, multiplied by the carrier, and then transmitted to the channel. The subcarrier frequencies are separated by multiples of $1/T$ so that, if signal is not distorted in transmission, the coherent detection of a signal element in any one sub-channel of the parallel system gives no output for the received element in any other subchannel. $s'(t)$ is modulated signal by product operation of $s(t)$ and $e^{j2\pi f_c t}$.

The generated equivalent complex baseband OFDM signal is written as

$$s(t) = \sum_{n=-\infty}^{\infty} \sum_{i=0}^{N-1} \frac{A}{\sqrt{T}} a_{n,i} e^{j2\pi f_i t} p(t - nT_s) . \tag{4}$$

where A is a constant related to the signal power, T_s is the symbol duration, $a_{n,i}$ is the hierarchical 16QAM symbol transmitted to the i-th subchannel in the n-th OFDM symbol interval $[nT_s, (n+1)T_s]$ and f_i is the frequency of the i-th subcarrier. $p(t)$ is a pulse shaping function expressed as

$$p(t) = \begin{cases} 1, & T_g \leq t \leq T_s \\ 0, & \text{otherwise} \end{cases} . \tag{5}$$

where T_g is a guard interval of OFDM signal. The time difference between the symbol period T_s and the guard interval T_g is the effective symbol interval. For orthogonality condition, $f_i = i/T = i/(N\Delta T)$.

The transmitted OFDM signal represented in equation (4) passes through multipath fading channel modeled by two ray model[9]. The simplified impulse response of the fading channel considered in this paper is expressed as [10]

$$h(t) = \delta(t) + b\delta(t - \tau)e^{j\theta} . \tag{6}$$

where the parameters b, τ , and θ are respectively the amplitude, time of arrival, and random phase of delayed multipath components. We assumed that b and τ are constant value but θ is random variable uniformly distributed in $[0, 2\pi)$.

Figure 5 shows the structure of the general OFDM system receiver. At first, the received signal is multiplied by the carrier frequencies, and then passes through a bank of correlators. Finally, the coherently detected symbols are converted to the serial stream by the parallel-to-serial (P/S) converter.

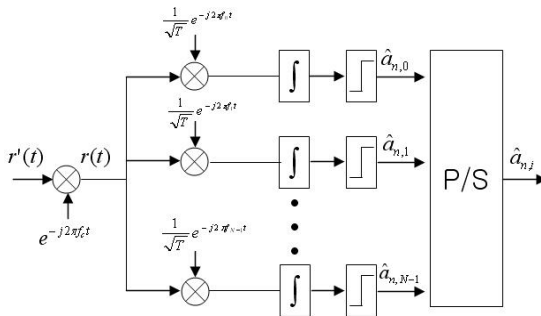


Fig. 5. The structure of OFDM receiver

The received signal after passing through multipath channel is represented as

$$r'(t) = s'(t) * h(t) + n(t) = s'(t) + bs'(t - \tau)e^{j\theta} + n(t), \tag{7}$$

where “*” represents a convolution operation and n(t) is the additive white Gaussian noise with the double sided power spectral density of $N_0/2$. In the first part of the OFDM/HL-16QAM receiver, the signal is down converted to the baseband. The down converted signal is given as

$$r(t) = r'(t)e^{-j2\pi f_c t} = y(t) + n(t)e^{-j2\pi f_c t}, \tag{8}$$

where f_c is the carrier frequency and $y(t)$ is the signal component of $r(t)$ as to be [11]

$$y(t) = \frac{A}{\sqrt{T}} \sum_{n=-\infty}^{\infty} \sum_{i=0}^{N-1} a_{n,i} e^{j2\pi f_c i t} p(t - nT_s) = \frac{Ab}{\sqrt{T}} e^{-j2\pi f_c \tau} e^{j\theta} \sum_{n=-\infty}^{\infty} \sum_{i=0}^{N-1} e^{j2\pi f_c i(t-\tau)} p(t - \tau - nT_s). \tag{9}$$

4 Simulation Results

Figure 6 shows the simulation block diagram of OFDM/HL-16QAM system in two ray multipath fading channel, where the upper path is transmitter and the lower path corresponds to the receiver. After the generated bit streams are first mapped to hierarchical 16QAM symbols and the serial symbol streams are converted to parallel form, zero bits are inserted to this parallel form symbols. Then IFFT block is used to modulate a block of input hierarchical 16QAM symbols onto a number of subcarriers. These modulated parallel data are converted to serial form of symbols, which become OFDM/HL-16QAM signal. In the receiver, signal demodulation process is performed in reverse order of transmitter operation.

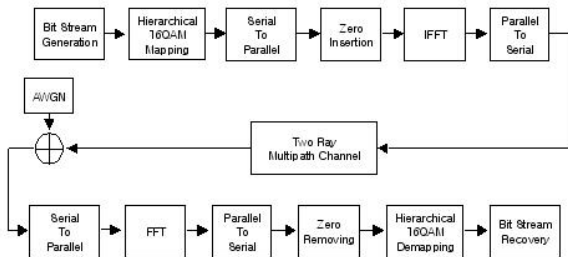


Fig. 6. The structure of OFDM receiver

The system and channel parameter values used for simulation of OFDM/HL - 16QAM system is presented in Table 1. In this simulation, the guard time is not included, so effective OFDM symbol interval is equal to FFT interval at the receiver.

Table 1. Parameters for simulation

Parameters	Values
Modulation Type	Hierarchical 16QAM
Normalized delay (τT)	0.0303 (=31/1024)
Attenuation coefficient(b)	-6dB
Number of subcarriers	64
Hierarchical modulation parameters (λ)	0.1~1.0

4.1 Still Image Transmission

For the simulation of image transmission, we use an image “lenna” shown in figure 2. The bit allocation map for image compression and simulation condition are previously presented in figure 2 and table 1, respectively.

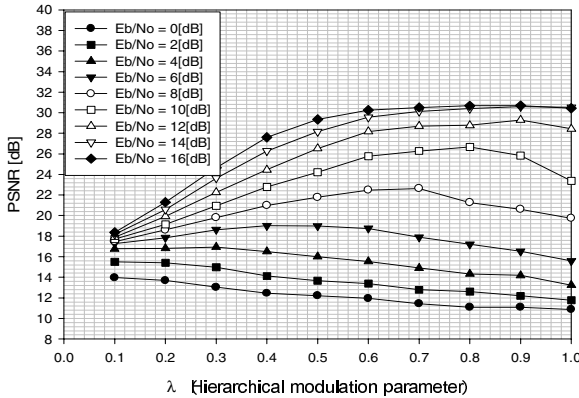


Fig. 7. PSNR performance of the received images according to λ

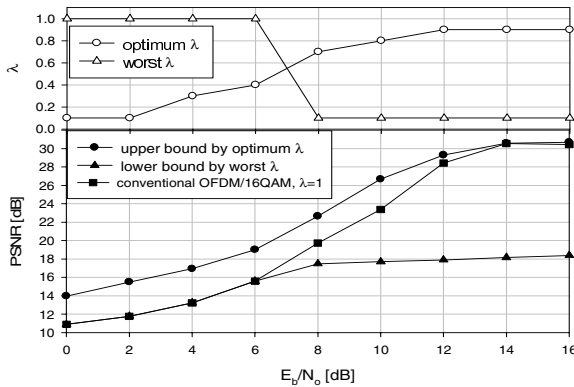


Fig. 8. Upper and lower bound of PSNR according to optimum and worst λ obtained through simulation

Figure 7 shows the PSNR performance which shows instantaneous PSNR performance of the received images of the proposed OFDM/HL-16QAM. It is shown that optimum λ maximizing PSNR exists according to E_b/N_0 value and the optimum λ becomes higher as E_b/N_0 increases. Figure 8 shows the optimum λ and worst λ according to E_b/N_0 and PSNR performance corresponding to optimum and worst case. From the figure, we have found that the proposed system with optimum λ has reasonable gain in PSNR as compared with conventional OFDM/16QAM ($\lambda=1$) system. Especially, the more gain is achieved by the proposed system as E_b/N_0 becomes small.

In figure 9, we have shown examples of simulated image. Figure 9 (a) is the original image and figure 9 (b) is an image compressed by DCT based fixed length coding without transmission error. The bit allocation map is given in figure 2. Figure 9 (c) and (d) are received images of the OFDM/HL-16QAM with optimum λ and conventional OFDM/16QAM ($\lambda=1$) over two ray fading channel.



(a) original image



(b) PSNR=30.71[dB] (no transmission error)



(c) PSNR=26.68[dB] ($\lambda=0.8, E_b/N_0=10$ [dB])



(d) PSNR=23.37[dB] ($\lambda=1.0, E_b/N_0=10$ [dB])

Fig. 9. Example of reconstructed image at the receiver

5 Conclusion

In this paper, we have proposed an OFDM/HL-16QAM system for image transmission. And then, we have evaluated the performance of the system in AWGN and

multipath fading channel. For image transmission, we have proposed the OFDM/HL-16QAM system adopting fixed length DCT based coding, and then obtained the optimum hierarchical modulation parameter maximizing PSNR of received still image. It has been shown that the received image quality of the proposed system with optimized hierarchical modulation parameter is better than that of conventional OFDM/16QAM system. Also, the upper bound and lower bound of PSNR achieved by the proposed system are presented.

Therefore, it is concluded that the proposed OFDM/HL-16QAM system is suitable for mobile multimedia communication demanding multi-reliability of data and high quality image transmission.

Acknowledgment

“This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment)” (IITA-2005-(C1090-0501-0022)).

References

1. Y. Sakamoto, M. Morimoto, M. Okada, and S. Komaki, “A wireless multimedia communication system using hierarchical modulation,” *IEICE Trans. Commun.*, vol. E81-B, no. 12, Dec. 1998.
2. E. K. Wesel, *Wireless Multimedia Communications*, Addison Wesley, 1998.
3. S. B. Weinstein and P. M. Ebert, “Data transmission by frequency- division multiplexing using the discrete fourier transform,” *IEEE Trans. Commun., Tech.*, vol. COM-19, no. 5, pp. 628-634, Oct. 1971.
4. J. A. C. Bingham, “Multicarrier modulation for data transmission : An idea whose time has come,” *IEEE Commun. Magazine*, vol. 28, no. 5, pp. 5-15, May 1990.
5. Richard Van Nee, Ramjee Prasad, *OFDM for Wireless Multimedia Communication*, Artech House, 2000.
6. R. Prasad, *Universal Wireless Personal Communications*, Boston • London: Artech, 1998.
7. K. Ogura, A. Miyazaki, and Y. Akaiwa, “An error resilient still image transmission system for mobile radio communication,” *VTC'04*, vol. 3, pp. 2004-2008, 1999.
8. M. Morimoto, M. Okada, and S. Komaki, “A hierarchical image transmission system for multimedia mobile communication,” *IEICE Trans. Commun.*, vol. E80-B, no. 15, Dec. 1997.
9. N. A. B. Svensson, “On optimum and suboptimum coherent detection of continuous phase modulation on a two-ray multipath fading channel,” *IEEE Trans. Commun.*, vol. 35, pp. 1041-1049, Oct. 1987.
10. M. Sylvain, “Extension of normalized two ray transfer function model to a space diversity line of sight link,” *IEEE Trans. Commun.*, vol. 43, pp. 2271-2280, no. 7 July 1995.
11. W. Hwang and K. Kim, “Performance analysis of OFDM on the shadowed multipath channels,” *IEEE Trans. Consum. Elec.*, vol. 44, no. 4 pp. 1323-1328, Oct. 1987.

Reliable Evaluations of URL Normalization^{*}

Sung Jin Kim¹, Hyo Sook Jeong², and Sang Ho Lee²

¹ School of Computer Science and Engineering,
Seoul National University, Seoul, Korea
sjkim@idb.snu.ac.kr

² School of Computing, Soongsil University, Seoul, Korea
hsjeong@ssu.ac.kr, shlee@comp.ssu.ac.kr

Abstract. URL normalization is a process of transforming URL strings into canonical form. Through this process, duplicate URL representations for web pages can be reduced significantly. There are a number of normalization methods. In this paper, we describe four metrics for evaluating normalization methods. The reliability and consistency of a URL is also considered in our evaluation. With the metrics proposed, we evaluate seven normalization methods. The evaluation results on over 25 million URLs, extracted from the web, are reported in this paper.

1 Introduction

A Uniform Resource Locator (URL) is a string representing a web resource (hereafter, referred to as a “web page”). With a URL, we can access a single web page on the World Wide Web (WWW). A web page can have two (syntactically different) or more URLs with which it can be accessed. Equivalent URLs means those that are syntactically different but represent the same page. The inability to recognize equivalent URLs gives rise to a large processing overhead in web applications; for example, a web crawler repeatedly requesting, downloading, and storing the same page, hence resulting in unnecessary network bandwidth, disk I/Os, disk space, and so on.

URL normalization is a processing of transforming URL strings into canonical form. After normalization, identically transformed URLs are regarded as equivalent URLs. Basically, the URL normalization determines whether two URLs are equivalent prior to access to the corresponding web pages. The term “false positive” is used to mean that non-equivalent URLs are determined as equivalent ones, whereas “false negative” is used to mean that equivalent URLs are determined as non-equivalent ones.

The standard body [1] defined the three types of URL normalizations, namely the syntax-based normalization, the scheme-based normalization, and the protocol-based normalization. The standard normalizations reduce false negatives while strictly avoiding false positives (they never transform non-equivalent URLs into a syntactically identical string). Lee and Kim [6] argued the necessity of extending the standard

^{*} This work was supported by Korea Research Foundation Grant (KRF-2004-005-D00172).

normalization methods and introduced three issues of extended normalizations. Discussed issues are the case sensitivity at the path component, the trailing slash symbol at the path component, and the designation of a default page.

Selecting URL normalization methods to use is dependent on the web applications. Users should take into consideration efficiency and effectiveness of web applications. If effectiveness is more important factor, users have to select the normalization methods that do not cause false positives. On the other hand, if efficiency is more important, users have to select the normalization methods that can reduce the number of duplicate URLs as many as possible.

The goal of this paper is to evaluate normalization methods in a reliable way. We describe four evaluation metrics. First, the URL consistency measures how consistently a URL is used to retrieve the same page during a given time unit. Second, the URL applying rate represents how many URLs are transformed by a URL normalization method. Third, the URL reduction rate represents how many URLs are reduced (how many URLs become same) after a URL normalization method is applied to a set of URLs. Fourth, the true positive rate represents how many URLs are transformed correctly. Finally, with the metrics we propose, we evaluate the standard URL normalization methods. The evaluation was performed on over 25 million URLs, which were extracted from the 20,000 Korean web sites in July 2005.

Our paper is organized as follows. In section 2, URL normalization is discussed. In section 3, we describe the evaluation metrics. Section 4 presents the experimental results, and lastly, section 5 contains the closing remarks.

2 Preliminary Study

2.1 Standard URL Normalizations

A URL is composed of five components: the scheme, authority, path, query, and fragment components. Fig. 1 shows all the components of a URL.

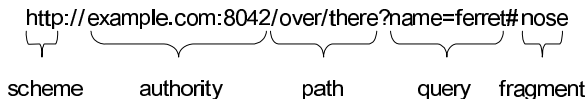


Fig. 1. An example of a URL

The scheme component contains a protocol (here, Hypertext Transfer Protocol) that is used for communicating between a web server and a client. The authority component has three subcomponents: user information, host, and port. The user information may consist of a user name and, optionally, scheme-specific information about how to gain authorization to access the resource. The user information, if present, is followed by a commercial at-sign (“@”) that delimits it from the host. The host component contains the location of a web server. The location can be described as either a domain name or IP (Internet Protocol) address. A port number can be specified in the component. The colon symbol (“:”) should be prefixed prior to the port number. For instance, the port number of the example URL is 8042.

The path component contains directories, including a web page and a file name of the page. The query component contains parameter names and values that may be supplied to web applications. The query string starts with the question mark symbol (“?”). A parameter name and a parameter value are separated by the equals symbol (“=”). For instance, in Fig. 1, the value of the “name” parameter is “ferret”. The fragment component is used for indicating a particular part of a document. The fragment string starts with the sharp symbol (“#”). For instance, the example URL denotes a particular part (here, “nose”) on the “there” page.

A percent-encoding mechanism is used to represent a data octet in a URL component when that octet’s corresponding character is outside the allowed set or is being used as a delimiter of, or within, the component. A percent-encoded octet is encoded as a character triplet, consisting of the percent character “%” followed by the two hexadecimal digits representing that octet’s numeric value. For example, “%20” is the percent-encoding for the binary octet “00100000”, which corresponds to the space character in US-ASCII.

2.2 Standard URL Normalizations

The URL normalization is a process that transforms a URL into a canonical form. During the URL normalization, syntactically different URLs that are equivalent should be transformed into a syntactically identical URL (simply the same URL string), and URLs that are not equivalent should not be transformed into a syntactically identical URL. The standard document [1] describes three types of standard URL normalizations: syntax-based normalization, scheme-based normalization, and protocol-based normalization.

The syntax-based normalization uses logic based on the URL definitions provided by the standard specification to reduce the probability of false negatives. The following three normalizations belong to the syntax-based normalization.

- Case normalization
- Percent-encoding normalization
- Path segment normalization

The hexadecimal digits within a percent-encoding triplet (e.g., “%3a” versus “%3A”) are case-insensitive. The scheme and host component are also case-insensitive. The case normalization transforms all characters within the triplet into upper-case letters for the digits A-F, and transforms characters in the scheme and host components into lower-case letters. For example, “HTTP://EXAMPLE.com” is transformed into “http://example.com/”.

During the percent-encoding normalization, all unreserved characters (i.e., uppercase and lowercase letters, decimal digits, hyphens, periods, underscores, and tildes) should be decoded. For example, “http://example.com/%7Esmith” should be transformed into “http://example.com/~smith”.

The path segments “.” and “..” are intended only to be used within relative references. During the path segment normalization, the path segment “.” and “..” are removed. When “..” is removed, as deemed necessary, the path segment located on the left side of the segment “..” is also removed. For example, “http://example.com/a/b/./../c.htm” is normalized into “http://example.com/a/c.htm”.

The URL normalization may use scheme-specific rules, at additional processing cost (compare with the syntax-based scheme), to reduce the probability of false negatives. Given the “http” scheme, the following normalization can be done. First, the default port number (i.e., 80 for the “http” scheme) is truncated from the URL, since two URLs with or without the default port number represent the same page. For example, “http://example.com:80/” is normalized into “http://example.com/”. Second, if a path string is null, then the path string is transformed into “/”. A URL with a null path string and a URL with a “/” path string represent the same page. For instance, “http://example.com” and “http://example.com/” represent the same page. The former URL is transformed to the latter one. Third, a URL with a fragment and a URL without a fragment represent the same page. For instance, “http://example.com/list.htm#chap1” and “http://example.com/list.htm” represent the same page. During the normalization, the fragment in the URL is truncated. The former URL is transformed into the latter one.

The protocol-based normalization is only appropriate when equivalence is clearly indicated by both the result of accessing the resources and the common conventions of their scheme's dereference algorithm (in this case, redirection is used by HTTP origin servers to avoid problems with relative references). For example, “http://example.com/a/b” (if the path segment “b” represents a directory) is very likely to be redirected into “http://example.com/a/b/”.

2.3 Reliability and Consistency

A URL does not in itself pose a security threat. However, as URLs are often used to provide a compact set of instructions for access to network resources, care must be taken to properly interpret the data within a URL, to prevent that data from causing unintended access, and to avoid including data that should not be revealed in plain text.

There is no guarantee that once a URL has been used to retrieve a web page, the same page will be retrievable by that URL in the future. Nor is there any guarantee that the page retrievable via that URL in the future will be observably similar to that retrieved in the past. The URL syntax does not constrain how a given scheme or authority apportion its namespace or maintains it over time. Such guarantees can only be obtained from the person(s) controlling that namespace and the page in question.

3 Evaluation Metrics for URL Normalization

This section describes four metrics (namely, URL consistency, URL applying rate, URL reduction rate, true positive rate) for evaluating URL normalization. We define the URL consistency metric in order to evaluate normalization methods on consistent URLs. Given a time unit t , a “consistent” URL is referred to as the URL via which the same page has been retrieved during the time unit. Let R_t be the number of download requests during the time unit t . The URL consistency metric is defined as below:

$$\blacksquare \text{URL consistency} = 1 - ((\text{the number of unique pages} - 1) / (R_t - 1))$$

If downloading a web page is unsuccessful, the downloaded page is regarded as the page with null string. For example, suppose that we request a web pages five times for a second, and that the download results are \textcircled{a} , \bullet , \textcircled{b} , \bullet , \textcircled{c} , where black circles means that downloading is unsuccessful and circled characters denote the contents of downloaded page. Then, the URL consistency is $1 - ((4 - 1) / (5 - 1)) = 0.25$.

URL consistency is critical in terms of evaluating URL normalization reliably. Note that once a URL has been used to retrieve a web page, there is no guarantee that the same page will be retrievable by that URL in the future. Hence, when a normalization method is applied to an inconsistent URL, the request results via the original URL and its normalized URL cannot be compared reliably. In other words, even though both the pages that are retrieved via an inconsistent URL and its normalized URL are different, we cannot be sure that the normalization method is incorrect. It is required to evaluate normalization on the URLs with sufficiently high URL consistency values.

Let M_b be the total number of URLs to be handled (or to be collected) before normalization. The URL applying rate represents how many URLs join the normalization. Let N be the number of URLs to which a normalization method is applied. The URL applying rate is defined as below:

- URL applying rate = N / M_b

For example, let us suppose we collect 100 URLs (i.e., $M_b = 100$), such as u_1, u_2, \dots, u_{100} . And, the last ten URLs are normalized into $u_1, u_1, u_{101}, u_{101}, u_{101}, u_{101}, u_{102}, u_{103}, u_{104}$, and u_{105} , respectively. Then, $N = 10$ and the URL applying rate is $(10 / 100) = 0.1$.

When different URL strings could become identical after normalization, users leave only one URL among the identically transformed URLs and throw away the others. Let M_a be the total number of URLs to be handled after normalization. We define the URL reduction rate as below:

- URL reduction rate = $(M_b - M_a) / N$

In the above example, M_a is 95 because 95 URLs (i.e., $u_1, u_2, \dots, u_{90}, u_{101}, u_{102}, u_{103}, u_{104}, u_{105}$) remain after normalization. As a result, the URL reduction rate is $(100 - 95) / 10 = 0.5$. The URL reduction rate shows how many URL strings equal to the others. More precisely speaking, this metric represents the probability that a normalized URL u_x equals to the original forms of the non-normalized URLs (i.e., from u_1 to u_{90}) or the transformed forms (i.e., $u_1, u_{101}, u_{102}, u_{103}, u_{104}, u_{105}$) of the normalized URLs (i.e., from u_{91} to u_{100}).

When an original URL string is transformed into another URL string, the original URL is not used any more. Therefore, when both the pages downloaded with the original and the transformed URLs are different, the original page could be lost. When, those pages are identical, we call the transformation the correct transformation. The true positive rate represents how correctly a normalization method transforms URLs. The true positive rate is defined as below:

- True positive rate = the number of correct URL transformations / N

For example, suppose that nine transformations are correct but one transformation is incorrect. Then, the true positive rate is $(9/10) = 0.9$.

4 Empirical Evaluation

Our experiment was performed in the following procedure. First, the robot [4] was used to collect web pages. Second, we extracted raw URLs (URL strings as found) from the collected web pages. Third, we eliminated duplicate URLs with simple string comparison methods (which will be discussed in more detail later) to obtain a set of URLs that are to be normalized. This step is simply intended to get a set of URLs that are syntactically different with each other, irrespective of URL normalizations. Fourth, relative URLs were transformed into absolute URLs. Fifth, we applied each of the standard normalization methods to the absolute URLs. Sixth, after requesting web pages with the absolute URLs and their normalized URLs, we compare the download results before and after the normalization.

We randomly selected 20,000 Korean sites. The web robot collected 655,645 web pages from the sites in July 2005. The robot was allowed to crawl at most 3,000 pages for each site, and the robot requested web pages within nine hops from the root page of a site. Timeout was set to two seconds. If there were no communication between a web robot and the web server for two seconds, the robot gave up the URL.

From the collected web pages, we were able to extract over 25 million (exactly 25,838,285) raw URLs, where a single URL could be counted many times as long as the URL is founded at many places. For instance, when the string “http://www.example.com/” was found twice on the same page, the number of extracted URLs was counted as two in our experiment.

First, let us see how often raw URLs are found in duplicates on web pages. We considered the following three cases. First, we eliminated duplicates of syntactically identical, raw URLs that are found on the same web page. Second, we eliminated duplicates of syntactically identical URLs starting with the slash symbol (it means that these URLs are expressed as an absolute path) as long as they are found on the same site. Third, we eliminated duplicates of syntactically identical URLs starting with the “http:” prefix. Table 1 shows the numbers of remaining URLs after each elimination method was applied. Note that these simple eliminations of duplicated URLs were able to remove more than a half of all the raw URLs that were found in the beginning.

After transforming relative URLs, in which some components of URL are omitted, into absolute URLs, we obtained 2,329,770 unique absolute URLs. We computed UR

Table 1. Eliminating duplicate URLs

Actions	Number of remaining URLs	Percent of remaining URLs to all the extracted URLs
All extracted URLs	25,838,285	100%
Eliminate the same URLs on a web page	22,757,954	88.1%
Eliminate the same URLs expressed as an absolute path on each site	19,647,693	76.0%
Eliminate the same URLs starting with “http:”	11,046,159	42.8%

L consistencies of the absolute URLs with $R_t = 3$, where t is one second. When we request web pages three times with an absolute URL, three consistency values can be produced by our consistency metric. When the number of downloaded pages is 1, the consistency of the URL is 1 because the same page is downloaded successively (or consistently). When the number of downloaded pages is 3, the consistency is 0 because different pages are downloaded whenever we request. When the number of downloaded page is 2, the consistency is 0.5 (i.e., $1 - ((2 - 1) / (3 - 1)) = 0.5$).

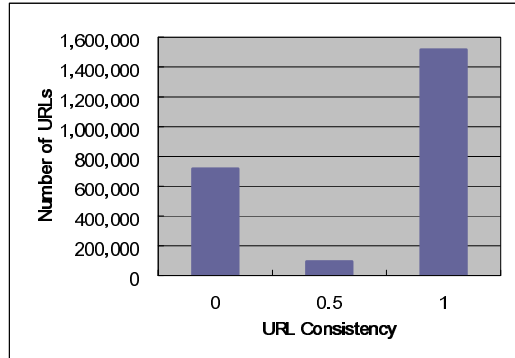


Fig. 2. Distribution of URL consistency

Fig. 2 shows the distributions of the URL consistencies. The X-axis represents the consistency value, and the Y-axis represents the number of URLs whose consistency values corresponds to that of X-axis. About 31% (exactly, 718,038) URLs of the absolute URLs were completely inconsistent (i.e., their consistency values were 0). There were 1,515,522 URLs (approximately, 65% of the absolute URLs), whose consistencies were 1. Only consistent absolute URLs were used for evaluating normalization methods.

We evaluate the seven normalization methods as follows:

- Method 1: Change letters in the scheme component into the lower-case letters
- Method 2: Change letters in the host component into the lower-case letters
- Method 3: Eliminate the default port (i.e., “:80”)
- Method 4: Transform a null path string into the slash symbol
- Method 5: Decode unreserved characters
- Method 6: Eliminate the fragment component
- Method 7: Eliminate the trailing slash symbol

The first six methods (i.e., Methods 1 to 6) are defined in the standard document [1], the last method (i.e., Method 7) is introduced in [1] and [6].

Fig. 3 shows the URL applying rate, URL reduction rate, and true positive rate of the seven normalization methods. The applying rates of Methods 1 to 4 were below 0.01, and those of Methods 5 to 7 were 0.03, 0.12, and 0.03, respectively. The reduction rates of Methods 2, 3, and 7 were below 0.05. Reduction rates of Methods 1

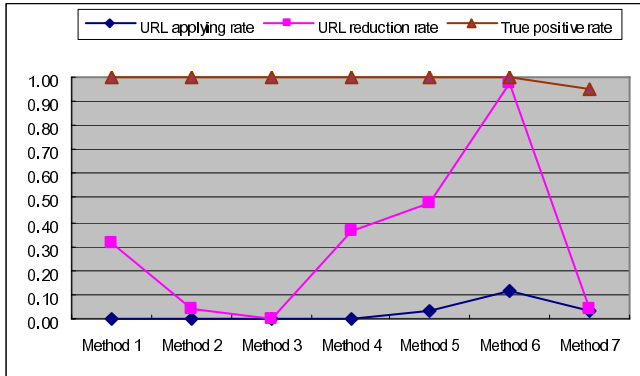


Fig. 3. Evaluation results of the seven normalization methods

and 4 showed that about one third of the URLs that we transform were removed. About half (48.3%) of the URLs to which we applied Method 5 were removed. Most (97.3%) of the URLs to which we applied Method 6 were removed. The applying rate and the reduction rate of Method 6 were relatively very high. The figures showed that 11.7% of the absolute URLs were transformed by Method 6, and 97.3% of the transformed URLs were duplicates. Note that the standard normalizations (Methods 1 to 6) do not cause false positives. The true positive rates of Methods 1 to 6 were 1, and that of Method 7 was 0.95. We learned that approximately 5% of the transformed URLs were wrongly transformed by Method 7 even though the method reduced 5% of the transformed URLs.

5 Conclusion and Future Work

In this paper, we described four metrics for evaluating URL normalization methods. The proposed metrics are summarized in Table 2.

Table 2. Summary of the proposed metrics

Metric	Description
URL consistency	Represent how consistently a URL is used to retrieve the same page during a given time unit
URL applying rate	Represent how many URLs are transformed by a normalization method
URL reduction rate	Represent how many URLs are reduced (how many URLs become identical) after a normalization method is applied
True positive rate	Represent how correctly URLs are transformed

With the metrics proposed, we evaluated seven normalization methods. The first six methods were standard normalization methods and the last method (Method 7) was eliminating the trailing slash symbol. Among 2,329,770 URLs, approximately

65% URLs were consistent URLs. True positive rates of the standard normalization methods were, of course, 1. True positive rate of the seventh method is 0.95, which means that 5% URLs were incorrectly transformed by eliminating the trailing slash symbol. The sixth method (i.e., eliminating the fragment component) exhibited the highest URL applying rate and URL reduction rate values.

In practice, adoption of URL normalization methods has been treated heuristically so far in that each normalization method is primarily devised on a basis of developer experiences. The contributions of this paper include details on the effects of URL normalization, and at the same time, present an analytic way to evaluate URL normalization methods. Our metrics can be used to evaluate not only standard normalization methods but also extended normalization methods to be developed in the future.

Lastly, we would like to mention our future works. First, we plan to devise evaluation metrics measuring the effectiveness of the combinations of the normalization methods. The orders of the normalization methods will be investigated, too. Second, we will study how to find equivalent URLs effectively. Using some information such as page contents, site characteristics, and so on, we can make a mapping table where pairs of equivalent URLs are listed. And then, we normalize URLs not only using the normalization rule but also referring to the mapping table.

References

1. Berners-Lee, T., Fielding, R., and Masinter, L.: Uniform Resource Identifiers (URI): Generic Syntax, <http://gbiv.com/protocols/uri/rfc/rfc2396.html>, (2005)
2. Burner, M.: Crawling Towards Eternity: Building an Archive of the World Wide Web, *Web Techniques Magazine*, Vol. 2. No. 5. (1997) 37-40
3. Heydon, A. and Najork, M., 1999. Mercator: A Scalable, Extensible Web Crawler, *International Journal of WWW*, Vol. 2. No. 4. (1999) 219-229
4. Kim, S.J. and Lee, S.H.: Implementation of a Web Robot and Statistics on the Korean Web, *Springer-Verlag Lecture Notes in Computer Science*, Vol. 2713. (2003) 341-350
5. Kim, S.J. and Lee, S.H.: An Empirical Study on the Change of Web Pages, *Springer-Verlag Lecture Notes in Computer Science*, Vol. 3399. (2005) 632-642
6. Lee, S.H., Kim, S.J. and Hong, S.: On URL Normalization, *Springer-Verlag Lecture Notes in Computer Science*, Vol. 3481. (2005) 1076-1085
7. Shkapenyuk, V. and Suel, T.: Design and Implementation of a High-performance Distributed Web Crawler, In *Proceedings of 18th Data Engineering Conference*, (2002) 357-368
8. Netcraft: Web Server Survey, http://news.netcraft.com/archives/web_server_survey.html, (2004)

Enhanced Misuse Case Model: A Security Requirement Analysis and Specification Model

Sang-soo Choi¹, So-yeon Kim², and Gang-soo Lee³

¹ Korea Institute of Science and Technology Information, Daejeon, 305-806, Korea
choiss@mail.kisti.re.kr

² Chungju National University, Dept. of Computer Science, Chungju, 380-702, Korea
sykim@mail.chungju.ac.kr

³ Hannam University, Dept. Of Computer Science, Daejeon, 306-791, Korea
gslee@mail.hannam.ac.kr

Abstract. An information security system of public or private organization should be developed securely and cost-effectively by using security engineering and software engineering technologies, as well as a security requirement specification (SRS). We present the E-MUC model that is analysis and specification model of security requirement based on UML, and a development process by using E-MUC model. Our approach is based on the paradigm of Common Criteria (ISO/IEC 15408), that is an international evaluation criteria for information security products, and PP which is a common security functional requirement specification for specific types of information security product.

1 Introduction

Awareness of the information security is increasing rapidly along with the development of information-communication infrastructure. Therefore, each organization is constructing and operating information security system. But, many organizations are introducing famous security company's information security products (for example, Firewall or IDS) in order to construct the information security system by finger-counting. Therefore, systematic analysis and specification of security requirements is required to reduce waste of unnecessary budget as well as redundancy of the security function.

In general, software developers are used to UCD (Use case diagram) to analyze and specify of software system. But, UCD is not suitable to analyze and specify of non-functional requirements [1]. Therefore, many researchers are proposed MUC (Misuse case) model to analyze and specify of non-functional requirement (especially, security requirement) [2,3,4,5]. But, these models have several problems as follows:

- These models are focused not actual security requirement but security threats and security mechanisms.
- And, these models do not propose a specific analysis and specify methodology for security requirement.
- Also, these models do not propose criteria to specify security related requirements.

To cope with those problems, we propose the E-MUC (enhanced misuse case) model, that is suitable to analyze and specify of security requirements, and SRS development process by using E-MUC model. Especially, proposed model and process are based on the paradigm of CC [6,7,8], that is an international evaluation criteria for information security products, and Protection Profile (PP) which is a common security functional requirement specification for specific types of information security product. We expect that information security system of organization will be more securely and systematically developed through proposed model and process.

2 Enhanced Misuse Case Model

We develop the E-MUC model that extends UCD and MUC model.

2.1 Definition of Model

E-MUC model is a security requirement analysis and specification model of information security system in a specific organization. Especially, it extends UCD and MUC model as shown in Fig. 1.

E-MUC model consists of seven factors as follows:

- Actor: It is a set of user's role. For example, it is system user of information security system.
- Mis actor: It is a special type of actor that occur misuse case. For example, it is threat agent of information security system. Especially, it marked in reversed (shade) form of actor.
- UC (Use Case): It is a general functional requirement of information security system, or security requirement that is required to reduce analyzed security threat.
- MUC (Misuse Case): It is an action that owner of information security system property does not want to happen. For example, it is security threat. Especially, it marked in reversed (shade) form of UC.
- PUC (Security-Policy Use Case): It is a description about security related policy that is operating in organization. For example, it is a security policy. Especially, it marked in dotted line form of UC.
- SUC (Security Use Case): It is a description about countermeasure of security threat or security policy. For example, it is a security object. Especially, it marked in bold line form of UC.
- SPC (Security Product Case): It is a security product that is produced to reduce analyzed security requirements by organization. For example, it is a certificated Firewall in a CC environment. Especially, it marked in round semicircle quadrilateral.

Also, E-MUC model have seven relations between seven factors as follows:

- Threatens: It means that specific UC is threatened from relevant MUC.
- Demands: It means that specific PUC is required by organization's security related policies.
- Mitigates: It means that specific MUC is mitigated by SUC.
- Effects: It means that specific SUC is influenced from relevant SPC.

- Implements: It means that specific SUC is implemented by relevant UC (especially, security functional requirement).
- Includes: It means that specific UC (especially, functional requirement) or information security system can include relevant UC (especially, security functional requirement).
- Introduces: It means that information security system can introduce or integrate relevant SPC.

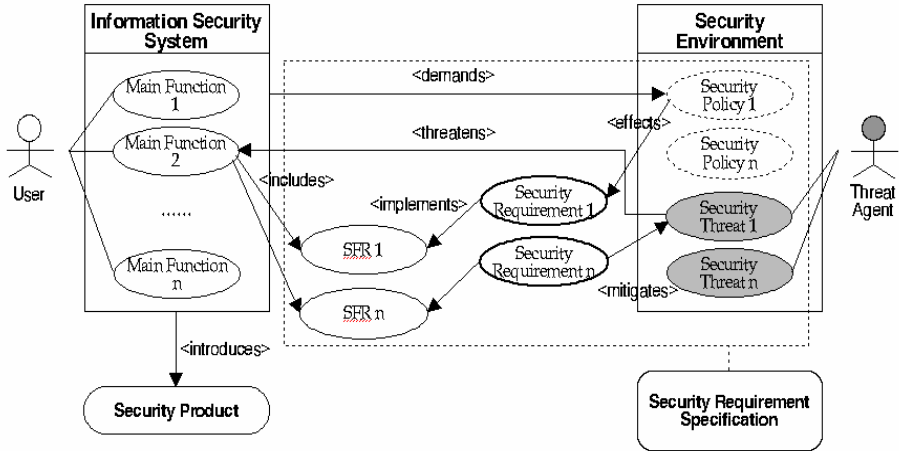


Fig. 1. E-MUC Model

3 Security Requirement Analysis and specification Process

We adapt the paradigm of CC to analyze and specify security requirements as shown in Fig. 2.

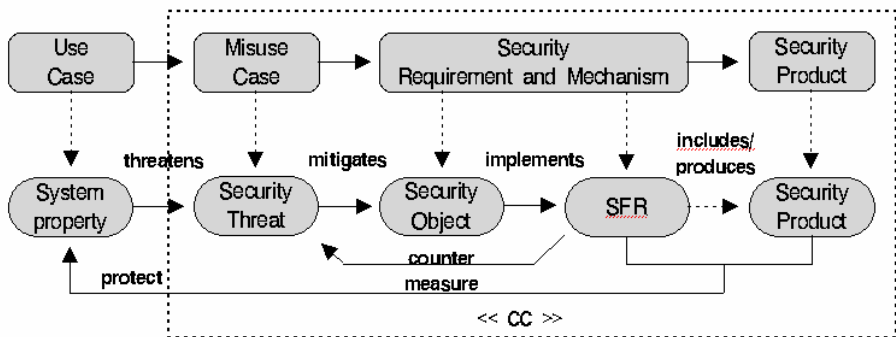


Fig. 2. E-MUC Modeling Process by using paradigm of CC

3.1 Step 1: UC Modeling

Developer performs traditional UC modeling as shown in Fig. 3-(a).

3.2 Step 2: MUC/PUC Modeling

Developer performs MUC modeling to analyzed information security system property and main function. Especially, mis-actor is a threat agent for specific information security system property or main function, and MUC is a threat. It is applied to <threatens> relation between MUC and UC (or information security system property). Also, developer performs PUC modeling to security related policy of organization as shown in Fig. 3-(b). It is applied to <demands> relation between PUC and information security system property.

3.3 Step 3: SUC Modeling

Developer performs SUC modeling to analyzed MUC. Especially, SUC is not security mechanism but security requirement (security objective), that mitigates security threat. It is applied to <mitigates> relation between SUC and MUC. Also, developer performs SUC modeling to analyzed PUC as shown in Fig. 3-(c). It is applied to <effects> relation between SUC and PUC.

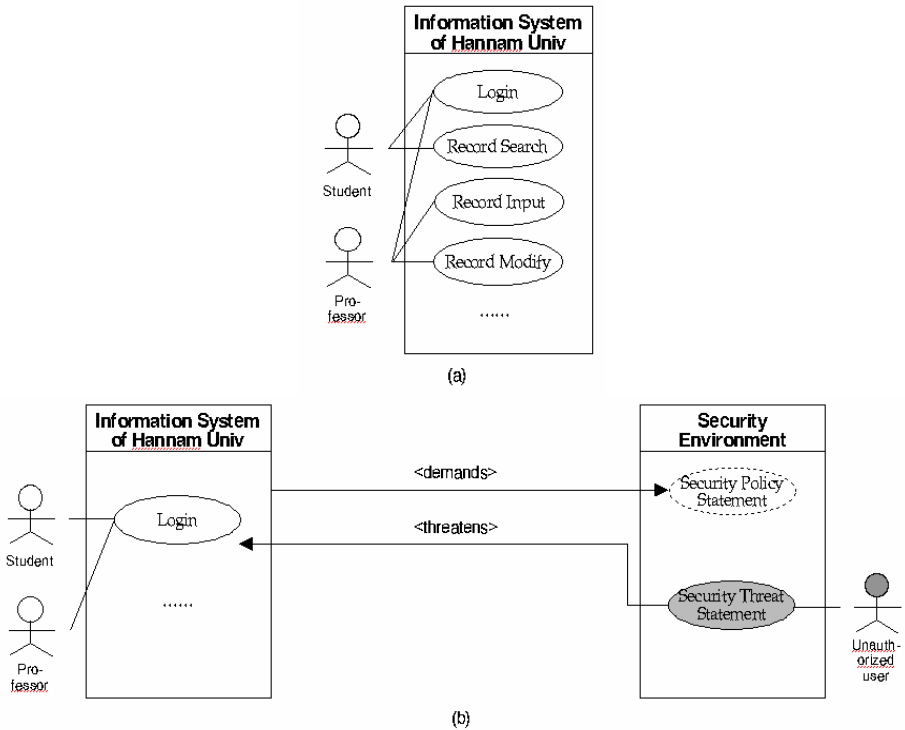


Fig. 3. E-MUC modeling step

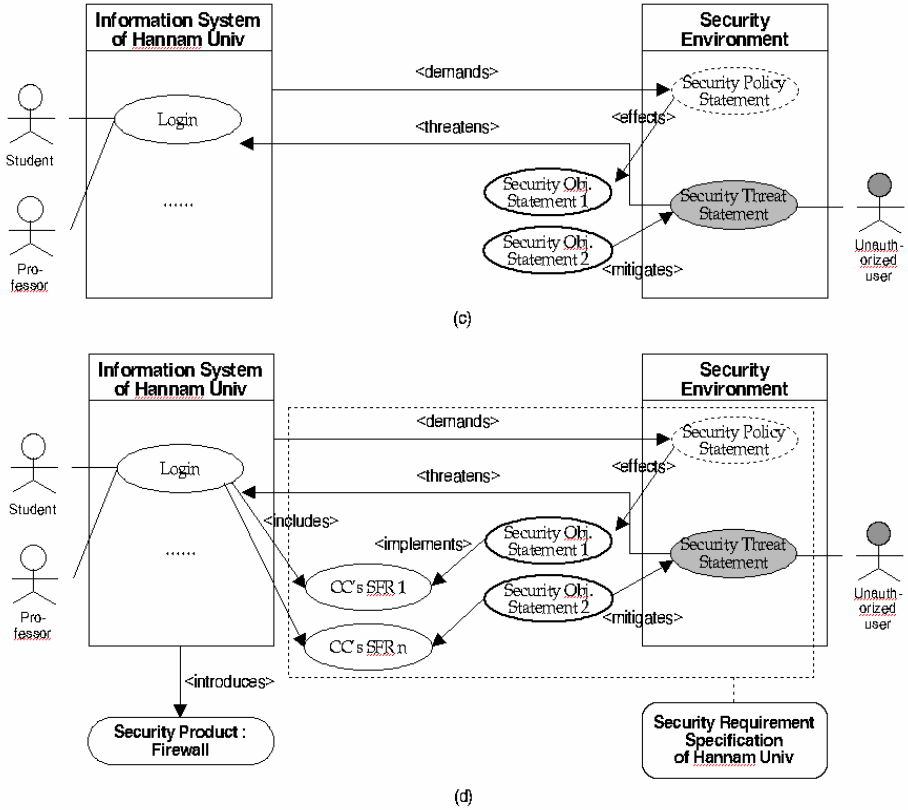


Fig. 3. (continued)

3.4 Step 4: UC Modeling

Developer performs UC (security functional requirement) modeling as shown in Fig. 3-(d). Especially, security functional requirement is a SFR in the CC environment. It is applied to <implements> relation between UC and SUC. Also, there is two way to implement security functional requirements. One way includes security functional requirements in a development process of information security system. Another way introduces information security products that contain relevant security functional requirements. It is applied to <includes> or <introduces> relation in each way.

3.5 Security Requirement Specification Development Tool

In a CC environment, PP is a security requirement specification for specific types of security product. Especially, PP has a very importance role for entire evaluation scheme. Also, SRS concept is very importance role in the C&A (certification and accreditation) environment such as DIACAP [9,10,11,12]. Therefore, we develop

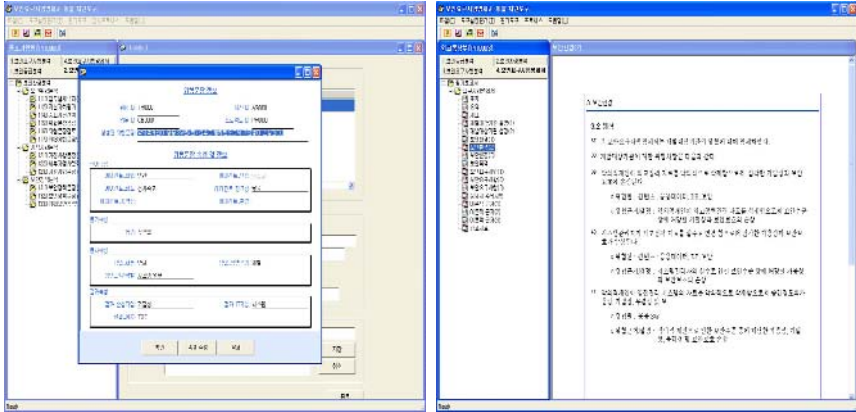


Fig. 4. Some screen shots of SRS-Tool (Korean version)

SRS-Tool that is SRS development supporting tool by using E-MUC model [13]. Especially, SRS-Tool is based on paradigm of CC and CC-Toolbox/PKB. Fig. 4 presents Korean version of SRS-Tool.

4 Analysis and Conclusion

We propose E-MUC model that is based on UC and MUC model and SRS-Tool that is based on CC-Toolbox/PKB. In this section, we present analysis result between our approach and related work.

4.1 Analysis with Related Work

E-MUC model is based on UC and MUC model. Especially, we solve the problems which contained in previous model as follows:

- E-MUC model is focused actual security requirement.
- We propose a specific analysis and specify methodology for security requirement.
- We adapt a paradigm of CC and PP to specify security related requirements.

Table 1 presents main difference between E-MUC model and MUC (UC) model.

Table 1. E-MUC vs. UC and MUC

	UC	MUC (Sindre&Opdahl)	MUC (Alexander)
Target	Functional requirement	Security threat	Security threat
Usage phase	System development	System development	System development
Relation	Includes, extends	Includes, extends, prevents, detects	Includes, threatens, mitigates
Result	Functional requirement	Security threat, security mechanism	Security threat, countermeasure
Contents	-	N/A	N/A

Table 1. (continued)

	AC (McDermott)	SUC (Firesmith)	E-MUC
Target	Security threat scenario	Security requirement	Security requirement (SRS)
Usage phase	System development	System development	System development, Reengineering
Relation	-	-	Threatens, mitigates, implements, includes, demands, effects, introduces
Result	Threat scenario	Security requirement, security mechanism	SRS
Contents	N/A	N/A	CC, PP, CC-Toolbox/PKB

Table 2 presents main difference between SRS-Tool between CC-Toolbox

Table 2. SRS-Tool vs. CC-Toolbox

	CC-Toolbox/PKB	SRS-Tool
Target	PP/ST	PP/ST and SRS
Process	ISO/IEC PDTR 15446	SRS-Process and E-MUC model
Asset analysis	X	O
Classification of Security level	X	O
DB	Threat : 109 Policy : 35 Assumption : 38 Security Objective : 157	Common Threat : 6720 Common Policy : 150 Common Assumption : 213 Security Objective : 489
Generation method of statement	X	O
Security function for tool	X	O
GUI	GUI based on text	GUI based on form
Report form	Self definition	PDF

4.2 Conclusion

In this paper, we present E-MUC model and security requirement analysis and specification process. SRS which is developed through proposed E-MUC model and SRS-Tool can be used to RFP and requirement specification for development of organization’s information security system. Also, we expect that information security system of organization will be developed and constructed securely and cost-effectively by using E-MUC model and SRS-Tool. E-MUC model has the following features:

- Organization can develop easily SRS by itself in accordance with E-MUC model and SRS-Tool.
- Developer can develop systematically SRS by using software engineering, security engineering and security evaluation scheme.
- E-MUC model promotes systematic development of information security system by using standard concept of CC and PP that have history more than 10 years.

Acknowledgement

This work was supported by a grant No.R12-2003-004-01001-0 from 'Korea Ministry of Commerce Industry and Energy' and 'National Security Research Institute'.

References

1. S. Lilly, "Use Case Pitfalls: Top 10 Problems from Real Projects Using Use Cases," Proc. TOOLS-USA'99, pp.174- 183, 1-5, Aug 1999.
2. G. Sindre, A. L. Opdahl, "Capturing Security Requirements through Misuse Cases," Proc. 14th Norwegian Infor-matics Conference (NIK'2001), Tromsø, Norway, pp.26-28, Nov, 2001.
3. I. Alexander, "Misuse Cases - Use Cases with Hostile Intent," IEEE Software, 20, 1 (January-February 2003), pp.58-66.
4. J. McDermott, "Eliciting Security Requirements by Misuse Cases," Proc. 37th Technology of Object-Oriented Languages and Systems(TOOLS-37 Pacific 2000), Sydney, Australia, pp.120-131, 20-23, Nov 2000.
5. Donald G. Firesmith, "Security Use Cases," Journal of Object Technology (JOT), 2(3), Swiss Federal Institute of Technology (ETH), Zurich, Switzer-land, pp.53-64, May/June 2003.
6. CC, Common Criteria for Information Technology Security Evaluation, Version 2.1, CCIMB-99-031, August 1999, http://www.commoncriteria.org/site_index.html.
7. CC, Common Evaluation Methodology, Version 1.0, CEM-99/045, August 1999, http://www.commoncriteria.org/site_index.html.
8. CCRA (Arrangement on the Recognition of Common Criteria Certificates) <http://www.commoncriteria.org>.
9. ISO/IEC 19791, "Information technology - Security techniques - Security assessment of operational systems," 2004. 12.
10. DITSCAP : DoD 5200.40, "Defense Information Systems Certification and Accreditation regulation," 1997.
11. NIACAP, "National Security Telecommunications and Information System Security Instruction," 2000.
12. DIACAP, "The Defense Information Assurance Certification and Accreditation Process," 2002.
13. Sang-soo Choi, Soo-young Chae, and Gang-soo Lee, "SRS-Tool: A Security Functional Requirement Specification Development Tool for Application Information System of Organization," Lecture Notes in Computer Science (LNCS), Vol. 3081, Part2, pp.458-467, May. 2005.

An Analysis of Policy Provisioning Complexity in Accordance with the Application Attributes of the Policy-Based Network*

Hyung-Jin Lim, Moonseong Kim, Dong-Young Lee, and Tai-Myoung Chung

Internet Management Technology Laboratory,
School of Information and Communication Engineering,
Sungkyunkwan University,
Chunchun-dong 300, Jangan-gu, Suwon,
Kyunggi-do, Republic of Korea
{hjlim, mskim, dylee, tmchung}@imtl.skku.ac.kr

Abstract. Since policy-based network technologies emerged themselves, a number of policy-based applications have been tried in the field of communications, which are just independent applications in accordance with policy-based management by each area. Particularly, lots of them were concerned with security and QoS areas. A single policy claims the control of network resources according to relations between network state and its application demand. We attempted to model and evaluate the effect of policy-based applications which were independently applicable to each area on network resources. For the purpose, we defined the complexity, dynamic property and globalization of policy as a matrix affecting its applications, including parameters with influences upon each matrix. Our evaluation results suggest that, in designing a policy-based network, there must be construction factors carefully considered according to their application attributes.

1 Introduction

Policy-based network management (PBNM) is a management skill that defines management policy in the level of businesses and services, and automatically controls networks and services based on the defined policy. It is recommended that the management policy shall be defined with PIM (Policy Information Model) standardized by IETF and DMTF. The policy shall be defined to meet the service requirement of applications as well as the network management area. Therefore, it shall be represented on a basis of recognizable and executable logic that allows a network device to accept, request for and enforce its activities. In order to simulate the abstract policy in conventional equipments, PDP and PEP, which serve as an ANL (Abstract Network Layer) in the network structure, shall be implemented. An automated policy

* This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment).

provisioning structure in accordance with a change in network state shall be required, along with a monitoring structure for the state of a network to which the policy is applied [1~3].

A network provides resources and services, which are requested by application domain, through monitoring and controlling. Together with the attributes of individual application domains, the PBNM structure and the management domain size affect not only the PDP process performance but also the individual policy provisioning performance. Such factors shall be considered to effectively provide the policy according to the network structure and the application attributes. Chapter 2 identified the attributes of conventional network applications by application domains in view of the network management. Chapter 3 described matrices and parameters affecting policy provisioning in application. Chapter 4 presented an evaluation and analysis of each application matrix. Finally, chapter 5 represented the conclusion.

2 Classification and Assumptions

With an increasing demand for leveled-up networking capability along with the appearance of PCs, network size is gradually scaling up from an early Internet setup, e.g., LAN in which multiple consoles were connected with a central server. We identified policy-based network management areas in three typical application cases: QoS Networking Area (QN), Non-QoS Networking Area (NQN) and Non-Networking Area (NN). In the conventional network management area, the QN includes admission control, bandwidth management, and performance monitoring & control, while the NQN includes transport security technologies, with the NN encompassing fault management and address allocation [4~8].

In the application domain and network domain areas, we introduced the following assumptions to evaluate the effect of the policy requirement on the application categories defined in the Section 2.1.

(a) All nodes of a network are assumed to accept the ANL level enabling the policy recognition and enforcement.

(b) The PBNM structure is assumed to have an organic relation with NMS enabling the monitoring of the state of a system and its applied policy.

(c) The policy conflict does not mean just a logical conflict among policies. For example, we used a conflict in which a pre-defined policy could not work on its provisioning when there were no secured resources enough for the performance. For the security policy, we defined that a conflict occurring when the policy of which level was higher than the security requirement.

(d) We considered the static provisioning and the dynamic provisioning. We primarily reviewed the operating performance of the former, and secondarily evaluated the effectiveness of policy adaptiveness when the latter was required [4].

(e) Policy adaptiveness means that the value of a policy attribute is temporarily and properly adjusted within an extent to which a service level in accordance with the current capacity of resources is not surpassed. Generally speaking, the policy conflict is rare under the provisioning environment with the static policy even if it refers to a highly distributed environment.

3 Evaluation of Application Attributes

We selected the following six matrices, presenting their respective measures and weights to evaluate the effect of policy-based applications on the network resources as described in the Section above: Based on related literatures, six matrices, including (1) the complexity of policy structure, (2) the policy priority, (3) the attribute of action, (4) the application area, (5) the action for a positive policy and (6) the action for a negative policy, have been defined as the major factors.

3.1 Complexity of Policy Structure (f_1)

Basic policy structure has the form of “when (state (l)), If (condition (m_k)) then (action (n)),” where l , m_k , n and k , respectively, indicate state, condition, number of actions, and number of attributes comprising the condition.

Verma [10] demonstrated that there was $O(kn^2)$ of complexity in determining the correlation and conflict among policies. However, those results were calculated from the worst case. A mean value shall be obtained for an appropriate evaluation. Therefore a new model in which the correlation and conflict among policies can be determined in a sort algorithm shall be analogized. In the sort algorithm, n policies for each attribute are sorted, where policies with the same attribute of the sorted policies can be resorted. If this is the case, it takes average $O(n \log n)$ to sort n policies, and average $O(kn \log n)$ to further sort k attributes.

3.2 Policy Priority (f_2)

Actions to carry out the policy are generally determined based on their conditions. The policy priority is determined based on various combinations of parameters comprising conditions. We determined the weight of computing cost for the policy priority as shown below:

$$f_2 = \{o_1, o_2, o_3, \dots, o_{\max}\} \quad (\text{Eq. 1})$$

The higher o_x indicates the higher correlation among the priorities. The smaller o_x value in f_4 indicates that the smaller amount of computing cost is required to determine the priorities. For example, a single criterion has a less amount of computing volume than that of the multiple criteria.

The priorities are primarily determined by the order of performance, class, time, specific event and state. The priority determination is a base to solve policy conflicts. Time and priority can be verified under a simple condition of rule. The correlation among policies can be determined by o_x .

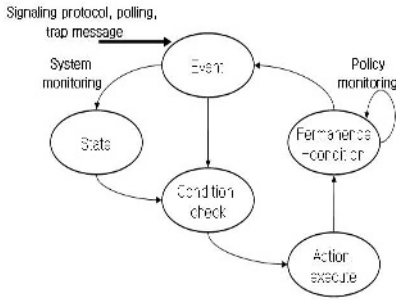


Fig. 1. State Transition Diagram for Policy Process

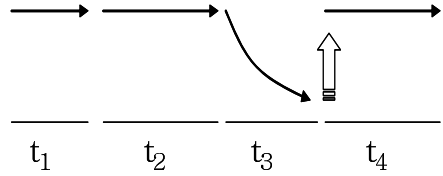


Fig. 2. Adaptive Process of Policy by Monitoring Cycle

3.3 Attribute of Action (f_3)

Actions to carry out a policy are determined by their condition. Fig. 1 shows a state transition diagram for the policy process by the attributes of actions. In the diagram, the precedent conditions include a random combination of system monitoring, state and condition check. The invariant conditions include the precedent conditions plus the performance conditions. The attributes of action represents a random variable f_3 by the precedent or invariant condition as shown below.

$$f_3 = \begin{cases} 0 & \text{precedence} \quad _ \text{condition} \\ 1 & \text{permanance} \quad _ \text{condition} \end{cases} \quad (\text{Eq. 2})$$

Fig. 2 shows the adaptive process of an applied policy by the monitoring cycle. A t_i indicates the interval of monitoring, where a random variable T is time. Linear flows on the top present that the applied policy is positive, and a downward flow at t_3 presents that the policy is negative. The latter flow suggests that the policy application shall be verified to update the invariant condition.

$$E[T] = \bar{\tau}, \forall t_i \in T$$

$$X = \begin{cases} 0 & \text{if } f_3 = 0 \\ |f_2| \bar{\tau} & \text{if } f_3 = 1 \end{cases} \quad (\text{Eq. 3})$$

If defining $E[T] = \int it_i di$, the expectation of a random variable T , by $\bar{\tau}$, $\bar{\tau}$ represents an average interval of monitoring.

3.4 Application Area (f_4)

One policy is basically applied to one node. Since the capabilities of a network has been added to a node, not only its system but also its individual node can request for

consistent policy management for a domain area. Application area varies depending on the application structure of PBNM. For example, all resources for domain shall consistently be administered to meet the QoS of a specific application. Such application attribute requires the ability to meet the SLA required for applications in a network node. For another example, access control policy is applied to the network boundary for perimeter defenses against an external network. The policy applications to all nodes within a domain require computing costs higher than in a single node. Therefore, we defined that weights ranged from 1 to f_2 according to application areas.

$$f_4 \in [1, N). \quad (\text{Eq. 4})$$

3.5 Action for Positive Policy: Factor 5 (f_5)

Policy that meets a specific “condition” in a structure is given access authorization to utilize resources and services. We defined two types of “actions” to be taken when a policy meets a condition: “Access Authorization” and “Resource and Service Utilization”. The resource utilization of a network or system is assigned a higher weight, because the access authorization is given prior to the determination of the resource allocation. We defined the action for a positive policy as shown below:

$$f_5 \in (0, \frac{1}{f_5}) \quad (\text{Eq. 5})$$

The action for a positive policy is defined as ‘0’ for the access authorization, and ‘1’ for the resource utilization. The policy for the resource utilization has a weight higher than that of the access authorization, because the latter is a necessary and sufficient condition for the former.

3.6 Action for Negative Policy: Factor 6 (f_6)

Policy is not executable without satisfying a specific state (1) or condition (m_k). An unmatched condition of access control and user authentication is denied. The minimum resource allocation and the consistency are core factors for the QoS policy, with a determination of policy conflict for its security policy. There are two actions for a negative policy: policy deny and adaptive performance requiring an additional process. We defined the action for a denied policy as shown below:

$$f_6 \in \left(0, \frac{1}{f_6}\right) \quad (\text{Eq. 6})$$

The action for a negative policy is defined as ‘0’ for its deny, and ‘1’ for its adaptive performance in order to assign a weight. You can change the denied policy to the extent necessary to be compatible with the current system state, or solve a possible policy conflict with pre-defined policies. An adaptive performance is employed if a resource state fails to satisfy policy requirements, or if it falls under a policy that doesn’t require such adaptive performance.

4 Analysis of Policy Provisioning Complexity

Network resources shall be appropriately controlled to meet the policy requirements of a specific application. From the existing research results, we considered the following three matrices to simulate the complexity of policy: complexity in determining policy conflict (C), dynamic property of policy (D), and globalization of policy application area (G). We generalized policy requirements with such matrices to identify their application attributes.

4.1 Complexity in Solving Policy Conflict

A policy conflict occurs when the conditions of two or more Policy Rules that apply to the same set of managed objects are simultaneously satisfied, but their actions conflict with each other. Once a policy conflict happens, although it rarely does under a general environment, an execution for a requested policy is denied, or a network administrator should be involved in changing the policy, which overhead is the reason why the current studies concern an adaptive & dynamic policy provisioning. However, those studies concerning such adaptive policy provisioning require detecting and negotiating on a policy conflict. It means that influences due to global conflict detection between domains should be considered if a policy conflict detection is performed, as is the case with our study. Therefore, a complexity in solving policy conflict shall also be considered [9, 10].

The complexity in solving a policy conflict is affected by factors including correlations among policies (i.e., priority) f_2 , the complexity of policy structure f_1 and action attribute f_3 . It is also affected by the time to detect and solve the policy conflict. The running time is determined depending on how to define the correlation among policies. The time to detect the policy conflict is defined as $|f_2| \log |f_2|$. The running time is affected by action attribute f_3 whenever a policy conflict is solved. Equation 7 defines a random variable X of the time to solve a policy conflict based on a invariant condition f_3 , and the running time $|f_1|$ in an event.

$$X = \begin{cases} 0 & \text{if } f_3 = 0 \\ |f_2| \bar{\tau} & \text{if } f_3 = 1 \end{cases} \tag{Eq. 7}$$

The complexity of policy conflict C is expanded as shown below. The probability mass function of action attribute f_3 shall be $P\{f_3: \text{Precedent}\}$ and $P\{f_3: \text{Invariant}\}$.

$$\begin{aligned} C &= |f_2| \log |f_2| + |f_2| + E[X] \\ &= |f_2| \log |f_2| + |f_2| + 0 \cdot P\{f_3: \text{precedent}\} \\ &\quad + |f_2| \bar{\tau} \cdot P\{f_3: \text{invariant}\} \\ &= |f_2| \log |f_2| + |f_2| + |f_2| \bar{\tau} \cdot P\{f_3: \text{invariant}\} \\ &= |f_2| (\log |f_2| + 1 + \bar{\tau} \cdot P\{f_3: \text{invariant}\}). \end{aligned} \tag{Eq. 8}$$

4.2 Dynamic Property of Policy

Policy negotiation and adaptiveness are determined depending on their dynamic property. The dynamic property of policy is defined based on the combination of action attributes for a negative policy (f_6) and action attributes for a positive policy (f_5). The dynamic property (D) is affected by adaptiveness and application area (f_4) [11, 12].

Fig. 3 shows a state transition diagram for a policy process according to dynamic properties of policy. An object (user or device) shall be given an authorization through authentication process prior to the determination about how to utilize resources in a specific application area. In Fig. 3, boxes represent the stage of decision-making. Each box has three modes including access, adaptation and allocation decision until the final policy performance is determined. The adaptation is subdivided into access adaptation and allocation adaptation.

Each circle represents the final performance state achieved by the stage of decision-making. Each state is divided into deny and grant. Each deny is subdivided into access deny and allocation deny, while each grant into access grant and allocation grant.

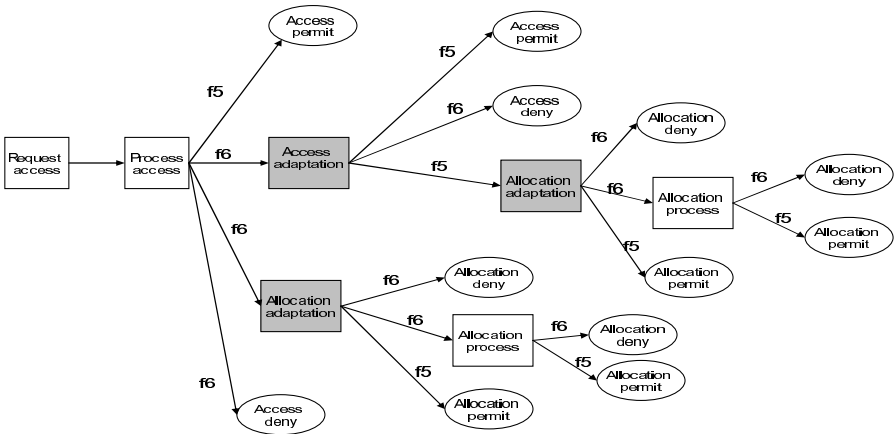


Fig. 3. State Transition Diagram for Policy Process According to Dynamic Property of Policy

Policy negotiation and adaptiveness are determined depending on their dynamic property. The dynamic property of policy can be modulated based on the combination (allocation and access) of action attributes for a positive policy (f_5), action attributes for a negative policy (f_6) and network resource state (v). There are 12 dynamic properties for a policy. Each link represents with f_5 and f_6 , ranging from 0 to 10:

$$f_5, f_6 \in [0, 10] \tag{Eq. 9}$$

The following equation represents the dynamic property weighted by the increasing number of links. The characteristic function χ_j^i with i th flow and j th link is defined as:

$$\chi_j^i = \begin{cases} f_5 & \text{if next node access grant and allocation grant} \\ f_6 & \text{if otherwise} \end{cases} \quad (\text{Eq. 10})$$

The characteristic function I_j^i with i th flow and j th node is defined as:

$$I_j^i = \begin{cases} 1 & \text{if access, adaptation and process} \\ 1 & \text{if allocation, adaptation and process \&} \\ & \text{if next node allocation, deny and grant} \\ 0 & \text{if otherwise} \end{cases} \quad (\text{Eq. 11})$$

where f_1 is consistency requirement. The dynamic property D_j^i with i th flow and j th node is defined as:

$$D_j^i = \chi_j^i + f_1 D_{j-1}^i I_j^i \quad (\text{Eq. 12})$$

where p_i is a probability that one of 12 flows occurs, and \tilde{D}_i is a final value of D_j^i for each i . the expectation of dynamic property D is defined as:

$$D = \sum_i p_i \tilde{D}_i . \quad (\text{Eq. 13})$$

4.3 Globalization of Policy Application Area

The application area is affected by the complexity of policy according to globalization G . The globalization is evaluated based on the total number of nodes maintaining policy consistency N and management area, i.e., the partial number of domain L . A probability that there exist s nodes in t partial domains is as follows:

$$P\{T = t\} = \frac{1}{L^s} {}_L C_t \sum_{i=0}^{t-1} (-1)^i {}_t C_i (t-i)^s, \text{ where } 1 \leq s \leq N \quad (\text{Eq. 14})$$

The expectation $\kappa(s)$ of a random variable T is defined as:

$$E[T] = \kappa(s) = \sum_{t=1}^{\min(L,s)} t P\{T = t\} \quad (\text{Eq. 15})$$

Thus, the globalization G is defined as:

$$G = E[\kappa(s)] = \sum_{s=1}^N \frac{1}{N} \kappa(s) . \quad (\text{Eq. 16})$$

5 Conclusion

In this study, we compared the centralized model and the distributed model of policy-based network management (PBNM), and analyzed the factors affected by its structure and application category. The policy-based network has been introduced in various applications. Thus, each policy provisioning may have different requirements. We analyzed correlations among factors affecting the performance and the nodes to which a policy is applied. The factors, including application area, consistency requirement and network structure, were considered to address the correlations.

A quantitative analysis demonstrated that putatively defined policy attributes were closely correlated with a network state. This study will further be developed to suggest the compatibility of and requirements for a possible application structure for PBNM framework through its quantification in a wider point of view.

References

1. Jude, M., Policy-Based Management: Beyond the Hype, Business Communications Review, March 2001.
2. Kosiur, D., "The Future of Policy-Based Network Management on the Internet", The Burton Group, May 2000.
3. John Strassner, et. al., "Policy-Based network management: solution for the next generation", ELSEVIER, 2004.
4. Emil Lupu, Morris Sloman, et. al., "An Adaptive Policy Based Framework for Network Services Management", Journal of Networks and Systems Management, 2003.
5. Gai, S., et al. "QoS Policy Framework Architecture", draft-sgai-policy-framework-00.txt, February 1999.
6. Corrente, A., et. al., "Policy provisioning performance evaluation using COPS-PR in a policy based network", Integrated Network Management, IFIP/IEEE 8th International Symposium on, March 2003.
7. R. Yavatkar, et. al., "A Framework for Policy-based Admission Control", IETF RFC 2753, January 2000.
8. K.L. Eddie Law, Achint Saxena, "Scalable Design of a Policy-Based Management System and Its Performance," IEEE Communications Magazine, 2003.
9. K. Chan, et. al., "COPS Usage for Policy Provisioning (COPS-PR), IETF RFC 3084, March 2001.
10. Verma, D.C., "Simplifying network administration using policy-based management", Network, IEEE, Volume: 16, Issue: 2, April 2002.
11. K. Yoshihara, M. Isomura, et. al., "Distributed Policy-based Management Enabling Policy Adaptation on Monitoring using Active Network Technology", DSOM '01. IEEE, 2001.
12. Nevil Brownlee, "Traffic Flow Measurement Architecture", IETF RFC2722, Oct. 1999.

Privacy Preserving Unsupervised Clustering over Vertically Partitioned Data*

D.K. Tasoulis^{1,2}, E.C. Laskari^{1,2}, G.C. Meletiou^{2,3}, and M.N. Vrahatis^{1,2}

¹ Computational Intelligence Laboratory, Department of Mathematics,
University of Patras, GR-26110 Patras, Greece
{dtas, elena, gmelet, vrahatis}@math.upatras.gr

² University of Patras Artificial Intelligence Research Center (UPAIRC),
University of Patras, GR-26110 Patras, Greece

³ A.T.E.I. of Epirus, P.O. Box 110, GR-47100 Arta, Greece

Abstract. The exponential growth of databases containing personal information has rendered the task of extracting high quality information from collections of such databases very important. This task is hindered by the security concerns that arise, due to the confidentiality of the data records, and the reluctance of the organizations to disclose their data. This paper proposes a clustering algorithmic scheme that ensures privacy and confidentiality of the data without compromising the effectiveness of the clustering algorithm nor imposing high communication costs.

1 Introduction

Clustering, that is “grouping a collection of objects into subsets or clusters, such that those within one cluster are more closely related to one another than objects assigned to different clusters” [8], is a fundamental process in knowledge acquisition. With the availability of inexpensive storage and the progress of data capturing technology, many organizations have created heterogeneous databases of data, and this is expected to continue. Thus, any knowledge discovery methodology, such as clustering, must take into consideration the distributed and heterogeneous nature of the data. Evidently, clustering rules extracted from a collection of databases tend to reflect globally meaningful results, rather than cognition which is embedded in a particular database.

The scenario of having an individual’s transactions divided among different organizations is common in real life [19]. This raises justifiable concerns among privacy advocates, that may prevent the necessary sharing of data, and hence discourage clustering projects involving more than one organization. Clustering and privacy are therefore, often perceived to be at odds. Clustering results rarely violate privacy as such, since they generally reveal high-level knowledge, rather than disclosing instances of sensitive data. However, the concern among privacy advocates is well founded, as bringing data together to support clustering and

* Partially supported by the “Archimedes” research programme awarded by the Greek Ministry of Education and Religious Affairs and the European Union.

data mining makes in general misuse easier [19]. The problem, therefore is not data clustering *per se*, but the manner in which it is performed. Thus, there is a growing need for the development of methods that have endogenous mechanisms to protect the confidentiality of sensitive data.

Clustering can conform with privacy preserving requirements by satisfying two conditions. Primarily, clustering algorithms need to be applicable without data sharing among the data proprietors; and secondly, no private information must be deducible from the extracted results. If these conditions are met clustering will not compromise privacy and it will contribute to obtaining globally meaningful results. One approach recently investigated is the addition of “noise” to the data before the data mining process [3, 5]. Another approach, restricted to classification, considers how much information can be inferred from the data made available through data mining algorithms, and how to minimize information leakage [3, 10]. Also, the extraction of association rules in horizontally partitioned data, was addressed in [9], while [18] addresses the same problem for vertically partitioned data. Concerning clustering, in [19] an adaptation of the k -means algorithm using several primitives from the secure multi-party computation literature, was proposed. Rather than sharing parts of the original or perturbed data, the authors of [11] suggest to transmit the parameters of suitable generative models, built at each local data site, to a central location that actually performs the clustering procedure. Finally, in [13], privacy preserving hierarchical data clustering methods are introduced using a family of geometric data transformation methods.

In this paper we assume a setting similar with that of [19], in which a number of different sites hold data for different attributes of a common set of entities (vertically partitioned data). The scope of each site is to obtain the clustering result over all its entities, but no site wants to reveal any information about its own attribute values. To this end, based on the recently proposed k -windows clustering algorithm [20], we develop a new algorithmic scheme that prevents the sharing of any meaningful information among the sites involved, results the same output as that obtained by the k -windows algorithm been applied to the unified database, and it does not raise any significant communication cost. Note that it is assumed that there does not exist a malicious site that provides wrong pattern lists in order to force the other sites to provide pattern lists, which can be used to gain information about the data. This assumption can be justified to the extent that the organizations that venture such projects have an established collaboration, rather than a one time partnership. Bad faith in this setting will be punished outside the algorithm.

2 Unsupervised k -Windows Clustering Algorithm

Intuitively, the k -windows algorithm tries to place a d -dimensional window that will contain all patterns belonging to a single cluster; for all clusters present in the dataset [20]. This goal is met by iteratively moving and enlarging the windows. During movement each window is centered at the mean of patterns that

are included in it. This process is iteratively executed as long as the distance between the new and the previous center exceeds the user-defined variability threshold, θ_v . The enlargement process, takes place at each dimension separately. Each range of a window is enlarged by a proportion θ_e/l , where θ_e is user-defined and l stands for the number of previous successful enlargements. Next, the movement process is invoked. Once movement terminates, the proportional increase in the number of patterns included in the window is calculated. If this proportion does not exceed the user-defined coverage threshold, θ_c , the enlargement and movement steps are rejected and the position and size of the d -range are reverted to their prior to enlargement values. Otherwise, the new size and position are accepted. If enlargement is accepted for dimension $d' \geq 2$, then all dimensions d'' , such that $d'' < d'$, undergo enlargement assuming as initial position the current position of the window. This process terminates if it does not result in a proportional increase in the number of patterns included in the window beyond the threshold θ_c .

The unsupervised k -windows algorithm is able to approximate the number of clusters, by applying the k -windows algorithm using a large number of initial windows. The windowing technique of the k -windows algorithm allows for a large number of initial windows to be examined, without any significant overhead in time complexity. Once movement and enlargement of all windows terminate, all overlapping windows are considered for merging. The merge operation is guided by a merge threshold, θ_m . Having identified two overlapping windows, the number of patterns that lie in their intersection is computed. Next, the proportion of this number to the total patterns included in each window is calculated. If the mean of these two proportions exceeds θ_m , then the windows are considered to belong to a single cluster and are merged, otherwise not. All these procedures are illustrated in Fig. 1, where (a) depicts the movement procedure, (b) the enlargement procedure and (c),(d),(e) are the three different instances of the merging procedure. For a comprehensive description of the algorithm and investigation of its capability to endogenously identify the number of clusters present in a dataset, refer to [15]. The unsupervised k -windows algorithm applied in both artificial and real life datasets, has proved to be efficient and effective in obtaining the actual number of clusters present in the dataset and achieving high classification results [17]. A high level description of the algorithm follows.

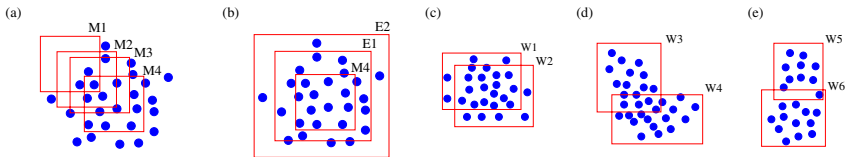


Fig. 1. (a) The movement procedure. (b) The enlargement procedure. (c) Windows that satisfy the similarity criterion of the merging procedure. (d) Windows that satisfy the merging criterion of the merging procedure. (e) Overlapping windows that do not satisfy any of the criteria of the merging procedure.

1. **Set** {the input parameters of k -windows algorithm}.
2. **Initialize** a set W of d -ranges.
3. **Perform** movements and enlargements of the d -ranges in W .
4. **Perform** the merging operation of the d -ranges in W .
5. **Report** the groups of d -ranges that comprise the final clusters.

3 Privacy Preserving Version of the k -Windows Algorithm

In this paper we consider the problem of privacy preserving unsupervised k -windows clustering, which can be formally defined as follows. Let r be the number of different sites, each holding a database with different attributes for the same set of n entities. All sites are interested in clustering through the unsupervised k -windows method the union of their databases, resulting in (a) the number of clusters over the union of data, (b) the final position of the centers of the clusters, and (c) cluster assignment for all points, under the following privacy conditions:

1. All databases are *private*, implying that there will be no disclosing of any database to any other site, or to a third party.
2. There is *minimal necessary information sharing* across the private databases, which means that the result of the clustering algorithm will be obtained without revealing any additional information.

To expose the workings of the proposed algorithmic scheme that enables the application of the k -windows algorithm in this setting, we separately describe each step of the methodology in the following subsections. Subsequently, in Section 4, the security of the scheme and privacy at each step are analyzed.

3.1 Determination of the Initial d -Ranges

The initialization phase requires the mutual agreement of all sites. Specifically, a set of k points that will comprise the centers of the initial d -ranges, should be mutually agreed upon. Each of these points represents a center around which a d -range will be initialized. Having decided on the identities of the patterns that will comprise the initial centers of the d -ranges, the size of the edges of these ranges must be set. The size of each edge can be decided locally; that is, by the site that holds the values for the corresponding coordinate (attribute). As it will be shown below, this information need not be communicated among sites.

3.2 Movements and Enlargements

After the initialization step has been completed for all k d -ranges, each site knows: (a) the coordinates of the centers of the ranges that correspond to the attribute values that it holds; and (b) the size of the edges of the d -ranges for the same coordinates. From this information alone, each site can conclude the set

of points that are enclosed in a particular d -range with respect to the dataset it holds. The complete set of points that are included in the full-dimensional d -range is the intersection of the corresponding sets of all sites. The exact procedure for the computation of the set intersection and its privacy analysis are given in Section 4. This operation for the simple case of two sites, each holding one attribute, is illustrated in Fig. 2. The two dimensional range, Range 1, has as center the point $P1$. Site 1 has decided the size of the edge of Range 1 for attribute 1, while Site 2 has determined the size of the edge for attribute 2. As previously mentioned, this information is private and need not be communicated. Site 1, therefore, concludes that the patterns that are included in Range 1 are $V_1 = \{P1, P2, P3, P4, P5\}$; while Site 2 concludes that for the same Range the enclosed patterns are $V_2 = \{P1, P3, P4, P7\}$. As shown in Fig. 2 the patterns which are included in Range 1 with respect to all dimensions, lie in the intersection of the two sets, $V = V_1 \cap V_2 = \{P1, P3, P4\}$. To obtain the result of the set intersection the parties apply the set intersection protocol for private databases described in Section 4.

Subsequently, the mean of the patterns that lie within each d -range (i.e. the mean value of the d -dimensional points) needs to be calculated. This operation is straightforward as each site can compute the mean for its own coordinates and no information exchange is required. Each site can then update the position of the center of the d -range with respect to the specific coordinates, so as to coincide with the previously computed mean. The process of moving the window is iteratively applied as long as the number of patterns that lie in the d -range is significantly increased as a result of this operation. The stopping criterion for this operation is the user-defined variability threshold, θ_v , that corresponds to the least change in the center of a d -range that renders the re-centering of the d -range acceptable. In this setting, the stopping criterion must be satisfied for all the sites in order to stop the movement process. Once movement is terminated, the d -ranges are enlarged in order to enclose as many patterns as possible from the cluster.

The enlargement process is executed in a similar manner with movement. Since enlargement is considered at each dimension separately, each site can

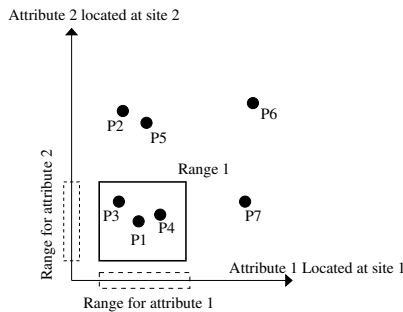


Fig. 2. Determination of points that are included in a d -range, over 2 sites

perform the operation for the coordinate(s) (i.e. attributes) it holds. Once a site has performed enlargement in a particular coordinate the new set intersection is computed for the enlarged d -range. After the enlargement in one dimension is performed, the window is re-centered, through the movement process described above. Once movement terminates, the proportional increase in the number of patterns included in the window is calculated. If this proportion does not exceed the user-defined coverage threshold, θ_c , the enlargement and movement steps are rejected and the position and size of the d -range are reverted to their prior to enlargement values. Otherwise, the new size and position are accepted. If enlargement is accepted for a dimension higher than one, the enlargement process for that d -range is reconsidered for all the lower dimensions (as described in Section 2). This process terminates if enlargement in any dimension does not result in a proportional increase in the number of patterns included in the window beyond the threshold θ_c .

3.3 Merging of the Resulting d -Ranges

To perform the merging operation no information need to be communicated among the sites. Since all the sites know the points that lie inside each window, they can determine the possible overlapping of any two windows. For each pair of overlapping d -ranges, each site can determine the proportion of common points with respect to the total number of patterns included in each window. Comparing this proportion with the threshold, θ_m , it is possible to determine whether the corresponding d -ranges belong to the same cluster.

4 Security and Privacy Analysis

To meet the privacy conditions for the complete algorithmic scheme, i.e., private databases and minimal necessary information sharing across them, it is sufficient to satisfy these conditions during the computation of the set of objects that lie in each d -range query. The computation of this set takes place in two stages. In the first stage each site individually computes the set of objects that lie in a d -range with respect to its attributes. The second stage involves the computation of the intersection of all individually computed sets. The privacy of the first stage is ensured as the computation is private to each site. Thus, only the privacy of the set intersection needs to be investigated.

To perform such a privacy analysis we first need to establish a security model. This is performed through the framework of *secure multi-party computation* [7, 21]. In this contribution we assume the security model to be the *semi-honest* [2, 7]. According to this model, the sites follow the protocol properly with the exception that they can retain a record of all their intermediate computations and received messages, in an attempt to obtain additional information if possible. Under this model, the proposed methodology considers several multi-party set intersections using a secure protocol that involves homomorphic encryptions and hashing [6].

The problem of set intersection of private databases in a multi-party environment is defined as follows. Assume that there are r parties, S_1, \dots, S_r , with corresponding lists of inputs V_1, \dots, V_r from some domain. At the end all parties learn which specific inputs are shared among all databases, without obtaining any additional information. The correspondence to our case is direct.

Considerable effort has been devoted to the development of protocols that address the problem of finding the intersection of two lists while revealing only the intersection. In [12] two solutions to this problem are presented. The first solution requires the oblivious evaluation of n polynomials of degree n , while the second solution requires the evaluation of n^2 linear polynomials, where n denotes the cardinality of the databases. In [2], the problem of two set intersection, intersection size, equijoin and equijoin size are studied using commutative encryptions and hash functions, and secure protocols with low computation and communication costs are provided. In our contribution, we adapt the multi-party protocol introduced in [6]. This protocol involves homomorphic encryption schemes and oblivious polynomial evaluation, it considers a leader party and $r - 1$ client parties and is briefly described in the following steps. Without loss of generality, it is assumed that each list contains l_c inputs. For more details refer to [6].

1. A client party S_i , for $1 \leq i \leq r - 1$, generates a polynomial Q_i of degree l_c whose roots are its inputs, and uses its own public key to homomorphically encrypt the polynomial coefficients. S_i also chooses l_c sets of $r - 1$ random numbers, $\{s_{j,1}^i, \dots, s_{j,r-1}^i\}_{j=1}^{l_c}$, which can be viewed as a matrix with l_c rows and $r - 1$ columns. This matrix is chosen such that the XOR of each row sums to zero. For each column l ($1 \leq l \leq l_c$), the client party encrypts the corresponding shares using the public key of client S_l . Then, it sends all encrypted elements to a public bulletin board (or just to the leader party who acts in such a capacity).
2. For each data item y in his list, the leader S_r prepares $(r - 1)$ random shares $\sigma_{y,l}$, one for each column of the matrix, where $\bigoplus_{l=1}^{r-1} \sigma_{y,l} = y$. Then, for each of the l_c elements of the matrix column representing client S_l , he computes the encryption of $(rn_{y,l} \cdot Q_l(y) + \sigma_{y,l})$ using S_l 's public key and a new random number $rn_{y,l}$. Thus, the leader generates l_c tuples of $r - 1$ elements each. Then, he permutes randomly the order of the tuples and sends the resulting data.
3. Each client S_l decrypts the r entries which are encrypted with its public key, i.e., the l th column generated by S_r , which has l_c items, and the $(r - 1)$ l th columns generated by the clients (also of l_c items). Then, S_l computes the XOR of each row in the resulting matrix, $(\bigoplus_{i=1}^{r-1} s_{j,l}^i) \oplus \sigma_{j,l}$, and sends these l_c results.
4. Each site S_i checks if the XOR of the $(r - 1)$ published results for each row is equal to the value y of its input. If this holds, then $\bigoplus_{l=1}^{r-1} ((\bigoplus_{i=1}^{r-1} s_{j,l}^i) \oplus \sigma_{j,l}) = y$, and y is concluded to be in the list intersection.

The prescribed multi-party set intersection protocol is proved to be correct at evaluating the set intersection and secure with respect to all parties' privacy for the semi-honest model case [6].

Regarding the security control of the multiple queries, the *semi-honest* model on which the above security analysis is based allows the sites to keep a record of all their intermediate computations and received messages, to infer some previously unknown, confidential data about a given entity. Such threats may result in exact, or partial information disclosure [1]. A survey of methods that have been proposed to address the problem of security control for the multiple queries was published [1]. Evaluation criteria of such approaches include security, robustness, suitability and cost. For a more recent survey of such techniques see [4].

5 Complexity Issues

The computational complexity of the algorithm depends on the computational complexity of the range searches. To make this step efficient techniques from Computational Geometry can be employed [14]. All these techniques have in common the existence of a preprocessing stage at which they construct a data structure for the patterns. This data structure allows them to answer range queries in sub-linear time with respect to the size of the database. In this case, however, we must also consider the complexity of the multi-party set intersection protocol. The communication overhead of this protocol is $O(rl_c)$, where r represents the number of sites involved and l_c is the maximum size of each object set. The computation overhead comes up to $O(rl_c^2)$ which can be reduced to $O(r(l_c + l_c \ln \ln l_c))$, through hash-to-bins method described in [6].

6 Discussion and Concluding Remarks

In this paper we present an algorithmic scheme that enables the application of the k -windows algorithm [20] on vertically partitioned data, with privacy. In this setting, the dataset is distributed over a number of sites and each site has information for all the entities, but only for a specific subset of the attributes of each entity. The goal is to cluster the known set of entities without revealing any of the values on which the clustering is based on. The work by Vaidya and Clifton [19] is directly comparable to the proposed setting. In [19] results from secure multi-party computation are employed in order to develop a privacy preserving k -means clustering algorithm. This approach ensures privacy, but imposes a high communication cost of $O(nrk)$, where r represents the number of sites involved, and n the total number of points. The advantages of the proposed approach reside in the clustering procedure per se, as well as, in the privacy preservation. Regarding clustering the k -windows algorithm has the ability to approximate the number of clusters present in a dataset [15, 16], provides high quality results, and has a low algorithmic complexity. With respect to the privacy issues, all privacy conditions are met through the adapted protocols for the semi-honest model. This work can be extended in order to be applicable to heterogeneous database models, as well as, to the case of horizontally partitioned datasets.

References

1. N. R. Adam and J. C. Worthmann. Security-control methods for statistical databases: a comparative study. *ACM Comput. Surv.*, 21(4):515–556, 1989.
2. R. Agrawal, A. Evfimievski, and R. Srikant. Information sharing across private databases. In *Proc. of the ACM SIGMOD International Conference on Management of Data*, pages 86–97, 2003.
3. R. Agrawal and R. Srikant. Privacy-preserving data mining. In *Proc. of the ACM SIGMOD Conference on Management of Data*, pages 439–450. ACM Press, 2000.
4. J. Domingo-Ferrer and J. M. Mateo-Sanz. Current directions in statistical data protection. *Research in Official Statistics*, 1(2):105–112, 1998.
5. A. Evfimievski, R. Srikant, R. Agarwal, and J. Gehrke. Privacy preserving mining of association rules. *Inf. Syst.*, 29(4):343–364, 2004.
6. M. Freedman, K. Nissim, and B. Pinkas. Efficient private matching and set intersection. In *Advances in Cryptology – EUROCRYPT 2004*, 2004.
7. O. Goldreich. *Secure multi-party computation*. Working Draft, Ver.1.4, 2002.
8. T. Hastie, R. Tibshirani, and J. Friedman. *The Elements of Statistical Learning*. Springer-Verlag, 2001.
9. M. Kantarcioglu and J. Vaidya. An architecture for privacy-preserving mining of client information. In C. Clifton and V. Estivill-Castro, editors, *IEEE International Conference on Data Mining Workshop on Privacy, Security, and Data Mining*, volume 14, pages 37–42. Australian Computer Society, 2002.
10. Y. Lindell and B. Pinkas. Privacy preserving data mining. In *Advances in Cryptology, CRYPTO 2000*, pages 36–54. Springer-Verlag, Aug. 20-24, 2000.
11. S. Merugu and J. Ghosh. Privacy-preserving distributed clustering using generative models. In *Third IEEE International Conference on Data Mining*, 2003.
12. M. Naor and B. Pinkas. Oblivious transfer and polynomial evaluation. In *Proc. of the 31st Annual ACM Symposium on Theory of Computing*, pages 245–254, 1999.
13. S. R. M. Oliveira and O. R. Zaane. Privacy preserving clustering by data transformation. In *18th Brazilian Symposium on Databases*, pages 304–318, 2003.
14. F. Preparata and M. Shamos. *Computational Geometry*. Springer Verlag, 1985.
15. D. K. Tasoulis and M. N. Vrahatis. Unsupervised distributed clustering. In *Proc. of the IASTED International Conference on Parallel and Distributed Computing and Networks*, pages 347–351. Innsbruck, Austria, 2004.
16. D. K. Tasoulis and M. N. Vrahatis. Unsupervised clustering on dynamic databases. *Pattern Recognition Letters*, 26(13):2116–2127, 2005.
17. D.K. Tasoulis and M.N. Vrahatis. Novel approaches to unsupervised clustering through the k -windows algorithm. In S. Sirmakessis, editor, *Knowledge Mining*, volume 185 of *Series Studies in Fuzziness and Soft Computing*. Springer Verlag, 2005.
18. J. Vaidya and C. Clifton. Privacy preserving association rule mining in vertically partitioned data. In *The Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pages 639–644. Edmonton, 2002.
19. J. Vaidya and C. Clifton. Privacy preserving k -means clustering over vertically partitioned data. In *The Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2003.
20. M. N. Vrahatis, B. Boutsinas, P. Alevizos, and G. Pavlides. The new k -windows algorithm for improving the k -means clustering algorithm. *Journal of Complexity*, 18:375–391, 2002.
21. A. C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*, pages 160–164, 1982.

Process Development Methodology for U-Integrated Management System

Seong-Man Choi, MalRey Lee, Cheol-Jung Yoo, and Ok-Bae Chang

Dept. of Computer Science & Statistical Information, Chonbuk National University,
664-14, 1Ga, Duckjin-Dong, Jeonju, Jeonbuk, 561-756, South Korea
{sm3099, mrlee, cjyoo, okjang}@chonbuk.ac.kr

Abstract. Existing research expenses management task consists of budget planning, budget draw-up, and exact settlement of budget. Therefore integrated management is needed keenly for certain security, efficient operation and clear execution of research expenses. To reflect these needs, Research Expenses Integrated Management(REIM) has been offered for the application used on mobile by reusing an business application module has been developed in REIM development process. Mobile collaboration component which supports a specialized collaboration process to be adapted for the peculiarities of a mobile machine also has been developed. As a result, it can offer various supportive information for decision making for the establishment of research management policy by reflecting user's requirement in real-time. It can also provide accuracy and prevention of errors to each operation since it can grasp the process of each operation without time and space hindrance through mobile collaboration.

1 Introduction

Competition for information among enterprises is accelerated gradually due to surprising development of network, client/server environment and software technique. Correctness and speediness are needed for the process of data for management of enterprises with this change of the market therefore data warehouse has been developed. The basic of this paper is the need for a system to support decisions regarding research expenses. Research Expenses Integrated Management(REIM) in an enterprise environment has been developed based on need, and to reflect users' requirements to support decisions regarding research expenses, and to promote the efficiency of the budget for research expenses [1, 2].

The REIM development process of the J2ME based is based on the data of an information system of research expenses to supply various decision support information which is needed to establish a budget policy for research expenses. The essential parts of this paper are information retrieval agent and information integration agent [3].

Information retrieval agent finds information for users and information integration agent extracts, transports, transforms and loads data collected by information retrieval agent. Database of an operation system which is managed independently from planning phase of research expenses to exact calculation of the budget including compilation of the budget and operation of the budget is optimized by using the 2 agents. As a result, it can offer various supportive information for decision making for the establishment of

research management policy by reflecting user’s requirement in real-time. It can also provide accuracy and prevention of errors to each operation since it can grasp the process of each operation without time and space hindrance through mobile collaboration.

This paper is organized as follows : Section 2 of this paper is on the study of existing development process and its problems. Section 3 is on UML based development process of the REIM to solve the problems of the existing development process. Section 4 is on the operation process, the operation result and the operation valuation of UML based mobile integrated management system. Section 5 is about conclusion and future works.

2 Related Works

Features and differences of development process of a system which has developed data management system will be discussed in this section [4, 5].

2.1 Inmon Data Management System Process

Inmon data management system process is shown in Figure 1. A incremental and iterative development cycle is essential for development process [4, 5]. It collects data from the host computer which is an operating system at one place and integrates. It extracts, transforms, summarizers and uses the necessary data.

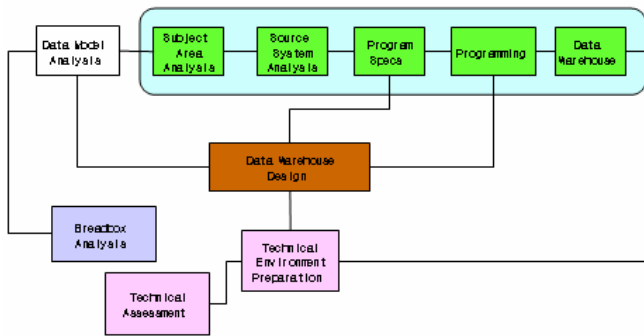


Fig. 1. Inmon data management system process

The development process, shown at Figure 1 is a way of classical development cycle which uses. If a system is developed by using the development process, some parts are overlapped in the development step and causes a problem of a need to go back to the previous step.

2.2 IBM Data Management System Process

IBM data management system process designs infra of technology, and dynamic solution to integrate transaction information through standard feed, and interface

Figure 2. It gives agents the ability to supply advice quickly, and more efficiently to customers, and maintain a close relationship with them [4, 5].

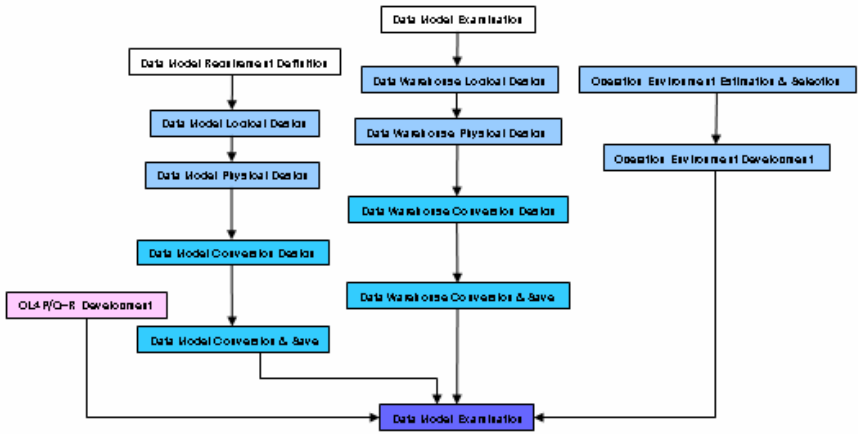


Fig. 2. IBM data management system process

Customer information can be accessed anytime and anywhere through Informix by the development process. As a result, it supplies a better customer service, and reduces time need to make a report largely so it promotes total efficiency.

3 Design of U-Integrated Management System Process

U-integrated management system process in an enterprise environment which is suggested in this paper is incremental and iterative, and it is the biggest feature of UML [6, 7]. It is completed not by one development cycle but by several development cycles Figure 3. Thus the component is getting extended by adding new functions to each development cycle, and the each development cycle repeats. As a result, component begins to develop.

3.1 Planning and Analysis Phase

Planning & analysis phase should be free from any technical and implemental matters. This phase provides knowledge regarding the problem domain, and defines problems which are needed to be solved.

3.1.1 Planning Establishment and Range Settlement

The Process planning of a project and settlement of development range are performed. In other words, problems which should be solved, and things which should be done by the system are confirmed in this task.

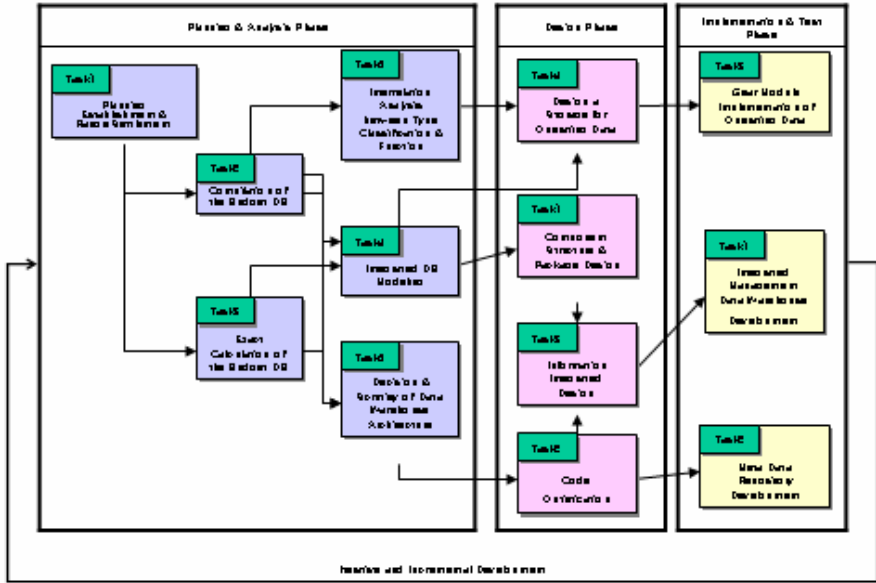


Fig. 3. Design of U-integrated management system process

3.1.2 Compilation of the Budget DB Analysis and Exact Calculation of the Budget DB Analysis

Requirement is analyzed clearly, and data elements are identified in the task of compilation of the budget DB analysis Figure 4.

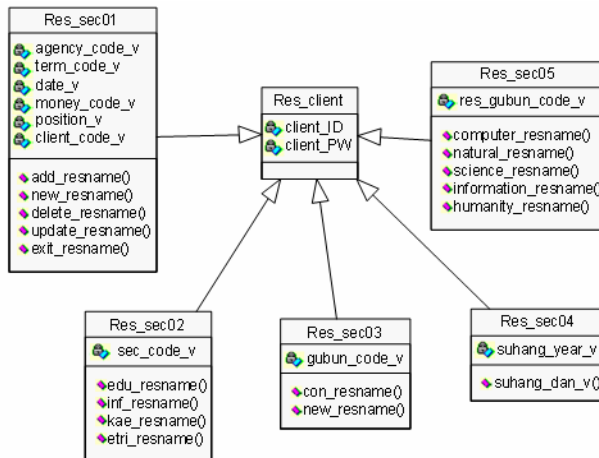


Fig. 4. Compilation of the budget class diagram

Class diagram consists of 6 classes : Res-client class, Res_sec01 class, Res_sec02 class, Res_sec03 class, Res_sec04 class and Res_sec05 class Figure 4. Res_Client class needs id and pw of a person who is in charge of a research. Res_sec01 class has general information of the research with an order organization, operation period and information of research expenses. Res_sec02 class has information which classifies an order organization of a research subject. Res-sec03 class classifies if the research subject is new one or continued one. Res-sec04 class has information of a year and a day which the research is done. Res_sec05 class has information of which field the research belongs to.

3.1.3 Integrated DB Modeling

Integrated DB modeling task is a process to make a data model with budget related data. External data are input through extra modeling process. In other words, integrated DB modeling is made by integrating the result of compilation of the budget analysis DB, and exact calculation of the budget analysis DB Figure 5. Integrated data class diagram consists of ten classes : compilation of the budget class diagram, exact calculation of the budget class diagram, and eight other classes which are needed to perform the research subject.

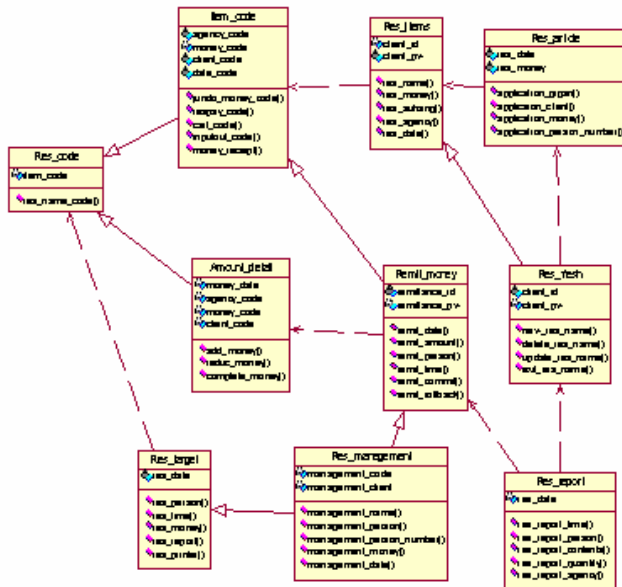


Fig. 5. Integrating of the budget class diagram

3.1.4 Decision and Scrutiny of Data Warehouse Architecture

A task to decide data warehouse architecture which is to be developed based on the result of compilation of the budget analysis DB, and exact calculation of the budget analysis DB is performed at decision and scrutiny of data warehouse architecture task.

Integrated class diagram in step, integrated class diagram of compilation of the budget, and integrated class diagram of exact calculation of the budget are derived to decide data warehouse architecture. Three integrated class diagrams are designed to proceed complicated query to satisfy users' various requirement. Compare and analyze compilation of the budget, and exact calculation of the budget, and integrate the result in the center of the subject which is to be analyzed at decision support system to extract necessary data for decision at integrated class diagram in step Figure 6.

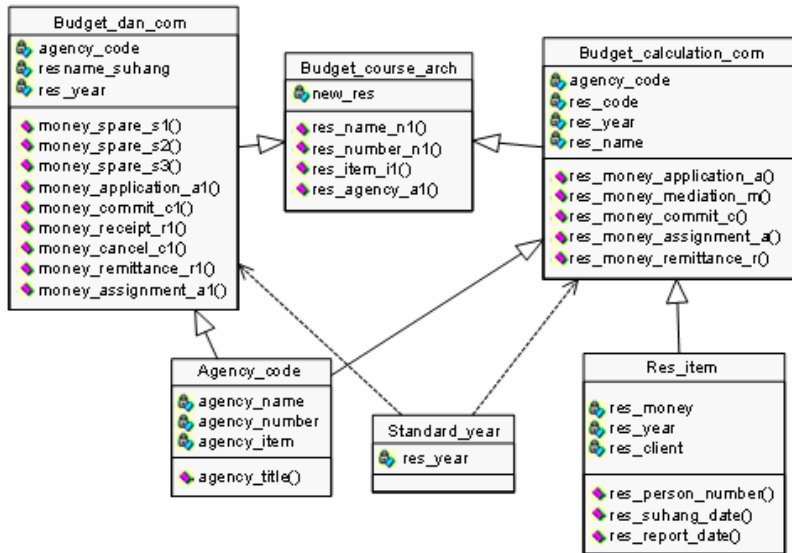


Fig. 6. Integrated class diagram in step

3.1.5 Interrelation Analysis Between Type Classification and Function

A subject is determined for change analysis and prediction analysis of budget management of an information system, and define related data to perform suitable analysis task for the object, and the feature at the task of interrelation analysis between type classification and function.

3.2 Design Phase

Design phase consists of four tasks, and they are performed repeatedly. It is technical extension, and adoption phase of the result of planning & analysis.

3.2.1 Component Structure and Package Design

Describe clearly component interface of components which are identified at compilation of the budget DB analysis, and exact calculation of the budget DB analysis based on integrated modeling defined at previous tasks and design each component.

3.2.2 Code Optimization

The operation is performed with the best instruction code in the given environment to process the operation more quickly by using storage location which has less final execute program at code optimization task.

3.2.3 Information Integrated Design

Extraction, transportation, transformation and loading of data are performed by information integrated agent at information integrated design task [3]. Data are extracted in an operating system, and send them to data warehouse. Data refine task uses ODS(Operational Data Store) which is the middle step store place on the way to the fact table. ODS which has source data makes transformation, and refine task of data easy. As a result, users' requirement change is corresponded quickly, and when there is a problem at the fact table it is recovered quickly.

Data of an existing file are loaded to a temporary table of data warehouse server and data inspection is performed logically at information integrated design phase. When error is removed transform, refine and load the data of the temporary table to a table of integrated data warehouse. The task temporary attribute table is transformed, and generated to load data to MDM(Multi-Dimensional Metadata) of oracle express.

3.2.4 Design of a Storage for Operating Data

Architecture of a storage for operating data is de-signed through the result of interrelation analysis between type classification, and function and integrated DB modeling at design a storage for operating data task.

3.3 Implementation and Test Phase

Implementation & test phase consists of three tasks, and the three tasks are performed repeatedly. Data are extracted, transported, transformed and loaded by information integrated agent at implementation & test phase. It let users access directly to the storage and analyze information with multi-dimension query to perform implementation & test. Final decision on design is made and coding to transform diagram, and specification to programming language construction is performed at implementation phase. Implementation phase is followed by test phase. The purpose of test phase is to find errors which exist at the code.

3.3.1 Integrated Management System Development

Data is extracted and transformed from operating database at integrated management data warehouse development task, and stored at the middle step storage, ODS on the way to the fact table of data warehouse. It is structured to meet users' requirement and change of the fact table.

The model of REIM data warehouse in an enterprise environment which is suggested in this paper uses existing data which are data of planning of the budget DB, compilation of the budget DB, and exact calculation of the budget DB by information

retrieval agent Figure 7. Information retrieval agent uses retrieval engine and finds information which an user wants. Data extraction, data transportation, data transformation and data loading are stored at ODS of integrated database by information integration agent. Data are extracted and stored at data mart of a structure which is suitable for the feature of the task, and analysis task, tendency analysis, and prediction task are performed using OLAP(On-Line Analytical Processing) technique, and data mining technique. Information integration agent let users access, and inspect essential information source, and get rid of unnecessary data for users.

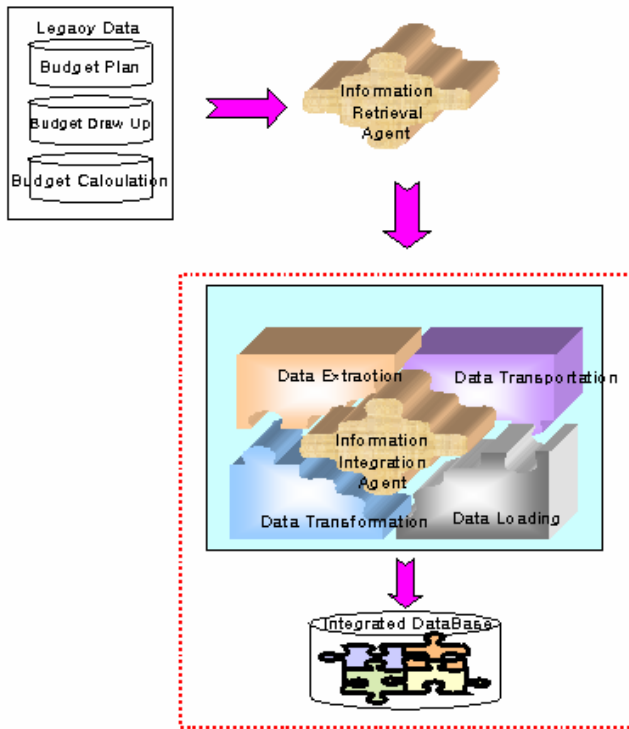


Fig. 7. Design of data warehouse model

3.3.2 Meta Data Repository Development

Users access a repository which stores mass data directly, and meta repository which analyzes, and searches information interactively through multi-dimension query is developed at meta data repository development task.

3.3.3 Gear Module Implementation of Operation Data

Gear module is implemented by multi data mining technique which is suitable for the goal, and the feature at gear module implementation of operating data task.

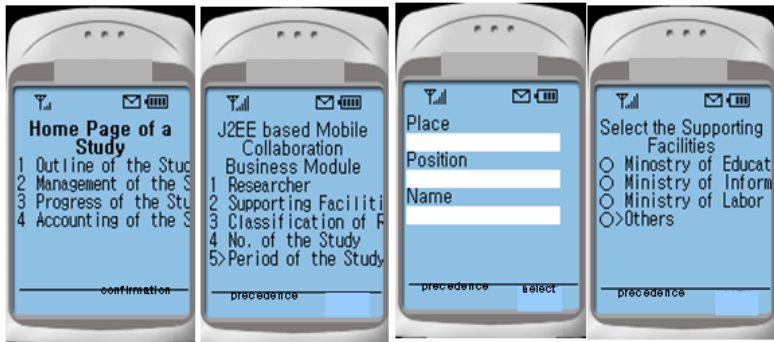


Fig. 9. Performance result of U-integrated management system

4.3 Assessment of U-Integrated Management System Process

The result of comparison between legacy development process, and mobile integrated management system development process of the J2ME based mobile business application is shown at Table 1.

Table 1. Comparison of development process

Process Contents	Immon Development Process	IBM Development Process	REIM Development Process
Construction Contents	Construction	Construction + Operation	Construction + Operation
Construction Danger	High	Low	Low
Use of Tools	Dependent	Dependent	Independent
Feedback	No	Yes	No

5 Conclusion

In this paper is about J2ME based system which has been developed to administrate a study efficiently by applying the existing web application to mobile collaboration business application. As a result the systems which were performed for different purposes are integrated to reduce total performance expenses and let the users join the decision making in real-time. It also makes the operation process of research expenses

clear to support information exchange, plan establishment and analysis work efficiently. The future works are that communications and collaboration should be designed to have application for various environments and visual communication module should be introduced and used.

References

1. Seong-Man Choi, Cheol-Jung Yoo, Ok-Bae Chang, Integrated Management Data Warehouse Development Process of Research Expenses in Enterprise Environment, Journal of KIPS, Vol. 11-D, Num. 1(2004) 183-194
2. Seong-Man Choi, Chang-Mog Lee, Cheol-Jung Yoo, Ok-Bae Chang, Jeong-Yeal Lee, Mobile Collaboration Business Module for Enterprise Application based on J2EE, in Proceedings of The 31th KISS Spring Conference(2004) 367-369
3. Seong-Man Choi, Chang-Mog Lee, Cheol-Jung Yoo, Ok-Bae Chang, Integrated Management Data Warehouse Development for J2ME based on Mobile Business Application, in Proceedings of The 4th Asia Pacific International Symposium on Information Technology(2005) 632-636
4. Theo Huibers, Bernd van Linder, Intelligent Information Retrieval Agents, Microengineering in Optics and Optoelectronics, IEEE Colloquium on(1999) 5/1-5/9
5. Eric Sperley, The Enterprise Data Warehouse: Planning, Building, and Implementation, Prentice Hall PTR, Inc.(1999)
6. Barry Devlin, Data Warehouse : From Architecture to Implementation, Addison-Wesley Longman, Inc.(1996)
7. Rational Software Corp., Unified Modeling Language(UML) Summary(1997)
8. Craig Larman, APPLYING UML AND PATTERNS : An Introduction to Object-Oriented Analysis and Design and the Unified Process, Prentice Hall PTR, Inc.(2002)

A Study on Agent-Based Integrated Security Management System for Managing Heterogeneous Firewall Systems

Dong-Young Lee¹, Hyung-Jin Lim², and Tai M. Chung²

¹ Dept. of Information and Communication MyongJi College, 356-1 HONGEUN3-DONG,
Seodaemun-Gu, Seoul 120-776, Korea
{dylee}@mail.mjc.ac.kr

² School of Information and Computer Engineering,
Sungkyunkwan University, 300 Chun-chun-dong, Changan-Gu,
Suwon City, Kyounggi-Do, Korea
{hjlim, tmchung}@rtlab.skku.ac.kr

Abstract. In this paper, we present the architecture of agent that supports integrated management for firewalls and implemented the prototype of the A-ISMSF(Agent-based Integrated Security Management System for Firewalls). The agent is a component of A-ISMSF consists of web client, integration engine and agents. The design of agent focuses on the scalability to newly introduces or expanded firewall structure so that minimal changes are needed to manage another firewall. An agent initiates with SNMP security MIB, monitors the status of a firewall, and executes control requests from integration engine.

Keywords: Agent, SNMP, Integrated Security Management, Secure MIB, Firewall.

1 Introduction

Network management issues include performance management, fault management, accounting management, configuration management and security management[4, 5]. Even though they are equally important, security management is getting more attention because the recent network community has experienced critical attacks and intrusions. Further, attempts by internal or external crackers who could destroy the network or system are increasing and the consequences are becoming more serious. In fact, the risk of disclosure or misuse of the important information is too risky take for some areas such as national security, personnel, and enterprise's information. In order to protect information and computing resources, various security products such as firewalls and intrusion detection systems (IDS) have been developed[1-3]. However, managing the security systems - particularly various kinds of systems - is not an easy task. Also, users ask for easy and transparent facilities to monitor and control various kinds of security products. Thus, integrated security management for security products has become more important. Over the years, a master-agent paradigm has been accepted as a promising approach for integrated security management. In general, it consists of three components - clients, manager, and agent systems[8]. We have worked on developing the agent-based integrated security management system for managing heterogeneous firewalls(A-ISMSF)[7] to monitor and control various kinds of firewall systems. In this

paper, we present a brief overview of integrated security management architecture and detailed design of firewall agents. The agents perform the control requests from security manager and maintain firewall MIB, and reports monitored status of firewall. Our research focuses on firewalls.

2 Backgrounds

2.1 A-ISMSF Architecture and Operations

We have been developed the agent-based integrated security management system for firewalls, called the A-ISMSF that has an integrated management facility to manage various firewalls such as the SecureShield, the TIS-FWTK, and the ipfwadm. It is consists of three separable parts - client, integration engine, and agent. Figure 1 describes the conceptual architecture of the A-ISMSF.

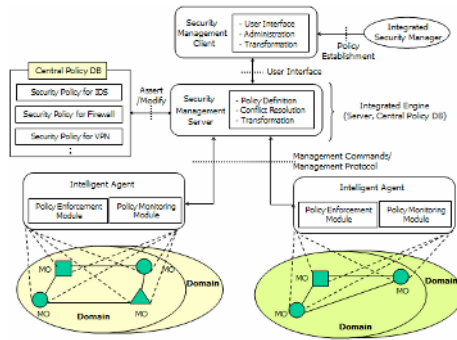


Fig. 1. Conceptual architecture of the A-ISMSF

The client displays conceptual management view of security services to security managers and sends monitoring or control requests to engine using TCP/IP. To interact with user via web browser, the client is implemented using JAVA language. The architecture of A-ISMSF is designed for scalability to support various types of firewalls as well as to accommodate large scaled network environments. It is also expandable for other security products than firewalls such as intrusion detection system (IDS), network virus scanning program (Ex, VirusWall), and other security products. The engine receives and processes requests from clients, and stores status information of security products from agents. It also generates the SNMP messages and dispatches them to the appropriate agents. This process includes spatial and functional assignment of clients request to agents. Spatial assignment selects a security product in an appropriate region while functional assignment selects a kind of security products to perform the request. These assignments process ultimately construct messages that are delivered to agents. The engine also consists of the internal database with five components - the authentication database of users and clients, agent information database, request mapping database, policy database, and the A-ISMSF MIB database. The agents collect data from security products and directly control upon the requests from the engine.

They also provide engine with the A-ISMSF' MIB. The detailed architecture and functions of agent are explained in the following sections. For the interface between agents and engine, the standard network management protocol, SNMP is used and the transmission of control requests, monitored data, and SNMP security MIB data are secured via tunneled communication between agents and engine. Engine-agent interface (EAI) supports data encryption standard (DES) which is one of the cryptographic algorithms recommended in SNMP v3.

2.2 Controlling Methods for Each Firewalls

The methods of configuring firewalls are various and different from each other. For example, policy and other additional configuration change is achieved by console command with appropriate arguments in SecureShield. It includes the embedded HTTP server dedicated to manage configuration web pages and CGI for configuring policies. The console command `ssfdm` is to configure not only the policy but also the various configuration of SecureShield - VPN, NAT, and others[13]. In practice, since the overhead for the agent to communicate with the embedded HTTP server is considerable, the SecureShield agent exploits the console command to reduce overhead. The `ipfwadm` also supports its own console command for configuration[14]. Therefore, the `ipfwadm` agent is able to control `ipfwadm` in the same manner. If a firewall uses console command to configure, the required functionality of agent is the ability to call an external process with arguments for the console command. Figure 2. Describe different configuration methods and required agent functionalities for each firewalls.

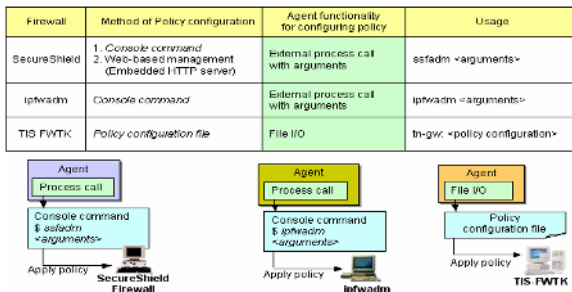


Fig. 2. Controlling methods and required agent functionalities for each firewalls

The agent of SecureShield or `ipfwadm` has this functionality. The TIS-FWTK has separated application gateways for the security services. For example, `tn-gw` denotes telnet gateway, `ftp-gw` denotes the FTP gateway, and so on. The separated application gateways share a common policy configuration file named `netperm-table`. The only way to configure policies in TIS FWTK is to modify the policy configuration file. Each line in the policy configuration file starts a specific keyword which is the name of each application gateway followed by a colon (:) [12]. For example, if the line starts with `tn-gw:`, it specifies the policy for telnet application gateway. In the same manner, we can configure policy for other application gateways. If a firewall application has the policy

configuration file, the agent for the firewall must have the ability to update the file as well as signal to the firewall. That is, the required functionality of agent is file I/O capability. In TIS FWTK, the agent writes policy to netperm-table file. Fortunately, TIS FWTK recognizes the modification to the file and immediately applies new policy. This distinction of the firewall control facilities makes the agents different from other types.

3 Design of the Agent Module for the A-ISMSF

3.1 Two Submodules of MSAF

This section describes the structure of our modularized security agent for firewalls (MSAF). As shown in Figure 3, the agent has two folds - distinct module to focus on its own control facility, and common module identical to all agents. They are application dependent module(ADM) and integrated common module (ICM). The whole external interface of MSAF(modularized security agent for firewalls) is also composed of two parts.

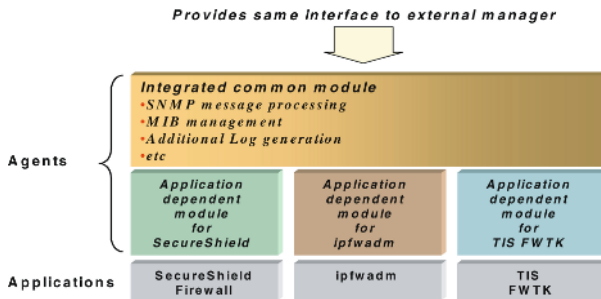


Fig. 3. Conceptual design of MSAF

3.1.1 Integrated Common Module (ICM)

The major functionality of the integrated common module(ICM) is to provide the same control interface to A-ISMSF engine regardless of the types of firewall application that MSAF manages. When the agent is initiated, the A-ISMSF engine is aware of the MIB structure over receiving MIB content. Then upon the arrival of a request from engine for setting or retrieving specific MIB variables, the control operation associated with the request is activated in the firewall application. The architectural design and functions of ICM are identical to all other MSAFs. Therefore, from the view point of A-ISMSF engine, the procedures and arguments for communicating with MSAF are identical except the address of MASF. An additional function of ICM is to manage MIB since the facilities to maintain the MIB are not different among agents.

3.1.2 Application Dependent Module (ADM)

Application dependent module has the function of direct control over individual firewall application. It executes application-dependent operations. Note that different

firewalls from different vendors have specific ways of controlling their security products. As we have seen in the previous page, SecureShield (using console command) and TIS FWTK (modifying netperm-table) have different ways of applying the changes. Thus, ADM is implemented differently in terms of the methods for enforcing policies in each application. All other low-level components of MSAF are hidden to others.

3.2 Detailed Agent Architecture

As shown in Figure 4, MSAF is divided into several sub-modules to increase flexibility, portability and scalability as well as for effective maintenance. Each module in MSAF has its own functionality and communicates each other using function calls. The descriptions of the internal modules are following.

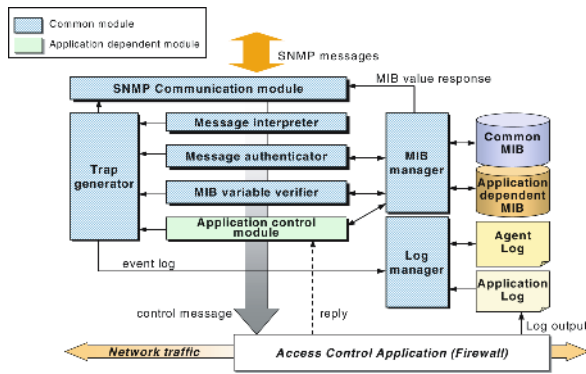


Fig. 4. Detailed architecture of MSAF

- **SNMP Communication module:** SNMP Communication module is responsible for communication with A-ISMSF. The major function is to provide the same SNMP communication interface to the external entity which is the manager. In fact, interface with any external entity is viewed as the above model.
- **Message interpreter:** Message interpreter analyzes received SNMP message, extracts data from the fields of the message, and passes the necessary information to Message authenticator which is described below. If any error occurs while analyzing the message fields, it sends a 'message error' message to the Trap generator.
- **Message authenticator:** Message authenticator executes the authentication process and integration check against received SNMP messages. If authentication fails, message authenticator sends an 'authentication fail' message to the Trap generator.
- **MIB variable verifier:** MIB variable verifier checks if the received SNMP message contains valid MIB variables. Should it detect invalid MIB variables, variable verification error message is sent to the Trap generator under variable names.
- **Application control module:** Application control module executes direct control operations over application. Should it successfully receive the control result, it sends the result to the MIB manager with additional data. Otherwise, it figures out the

possible reason, and passes it to Trap generator with an application control failed message and the reason.

- Trap generator: Trap generator processes all incoming error messages generated by other modules, and generates SNMP trap message. At the same time, it sends an error log message to the Log manager to write into log files.
- MIB manager: MIB manager has the responsibility of managing MIB, and processes requests from each module. It especially, manages two conceptually separated MIBs; Common MIB and Application dependent MIB. Note that they are in the physically same MIB
- Log manager: Log manager records all events generated by other modules and manages firewall application logs.

3.3 Message Processing in the Agent

We divide the message processing in MSAF into two major processes. One is the processing control request which modifies the application policy (i.e. SNMP set-request message). The other is the processing simple retrieval request to get firewall applications information (i.e. SNMP get-request or get-bulk-request message). The operating process of the MSAF messages as shown in Figure 5.

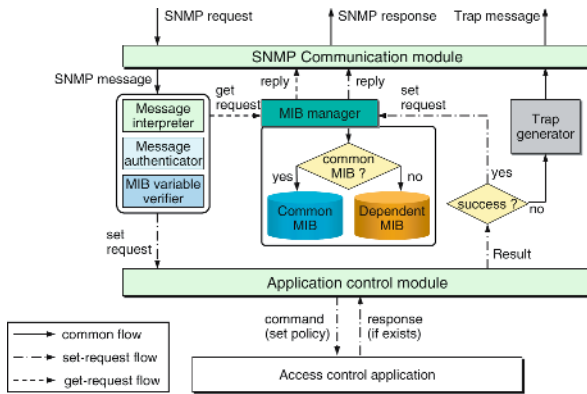


Fig. 5. Message processing in MSAF

First, the SNMP Communication module receives a SNMP message, and it delivers the message to Message interpreter. The message interpreter analyzes the message, divides it into each SNMP message field, and determines the request type. The information needed for authentication is sent to the Message authenticator. If the authentication is succeeded, MIB variables included in the received SNMP message are passed to the MIB variable verifier. If the MIB variables are decided to be valid and the message type is set-request message, then the analyzed message is sent to the Application control module. The Application control module executes modification of policy with information from a message and returns the result of control over application. If the execution result is successful, it sends an 'application control success' message to the MIB manager to set the MIB variables with the requested values.

Otherwise, an application control failed message is sent to the Trap generator with error information, and the Trap generator constructs the SNMP trap message to A-ISMSF engine. To guarantee integrity of MIB variables related to policy, MSAF updates MIB variable after receiving the result of policy applying. If an error occurs while applying policy, the application control module must not send the request for modifying MIB variables. When it is necessary to recover the policy such as firewall restart, the Application control module will reapply policy with MIB values. The last step of the processing is that the get-response message is sent to A-ISMSF engine to report that the requested operation is complete.

4 Prototype and MIB of A-ISMSF

4.1 The OID Tree for A-ISMSF

The management operation using SNMP is accomplished by retrieving or modifying management information. In terms of SNMP, each management information is named an object or object type, and an identifier for each objects is called an object identifier (OID) [4--5]. The model of management information, the allowed data types, and the rules of specifying classes of management information are specified in the SMI v2 (RFC1902). In this document, OIDs are structured in the form of a tree; the OID tree. The OID tree for the A-ISMSF is described in Figure 6.

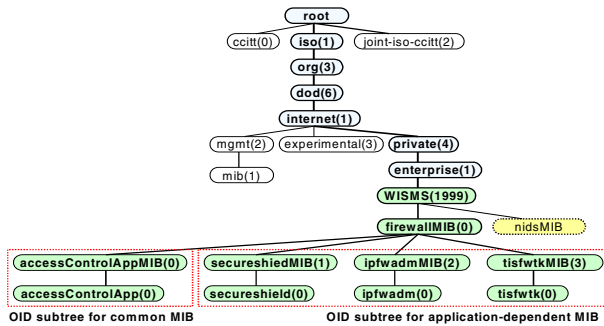


Fig. 6. OID tree for A-ISMSF

We defined the MIB objects of A-ISMSF are temporarily defined under enterprise(4) node of OID tree currently. A-ISMSF is originally the part of the web-based integrated security management system. Therefore, the current MIB for firewall application management, the firewallMIB(0), is defined under the OID named A-ISMSF(1999). We will plan to define additional MIB for A-ISMSF that will manages various network security applications over widely spread network. For example, nidsMIB is reserved for managing network-based intrusion detection system (NIDS).

As we described, the firewallMIB(0) is divided into two major parts; Common MIB and Application dependent MIB. The Common MIB named accessControlAppMIB(0) is common to all MSAF and defined under the node firewallMIB(0). It generalizes the

common functions and information from heterogeneous firewall applications by testing firewall systems in our test environment that is composed of independent small LANs. The OIDs of application dependent MIB are also defined under the firewallMIB(0), and they are named after the name of each firewall applications. They are used for managing functions and information dependent on each application.

4.2 Overview of Common MIB

We classified our common MIB into four different parts and the common MIB of A-ISMSF is depicted in Figure 7.

- **Application information MIB**

Application information MIB objects are used to store static and dynamic information about firewall applications. It contains as depicted the objects in the above slide the name of application, application type, application version, the date application installed, the time application installed, and etc. With these MIB variables, we can view various information about firewall application, check the integrity of application, and monitor its current status.

- **Access control policy table**

Access control policy table is the most significant MIB objects of MSAF. It consists of the policy information of application the agent manages. As a consequence, It is identical to the policy table of applications for each applications. Generally, each firewall applications is various with regard to the methods of managing its policy, but it has the similar characteristics in the consideration of the policy. It is that policy, permit or deny, is decided based on source address, destination address, source port, destination port, protocol, and etc. Access control policy table manages these common factors of policy.

- **Current session table**

Current session table stores the current network session information of the firewall application. We can monitor network session, detect misconfigured policy, and find out the bottleneck of network traffic caused by concentrated service requests through this MIB object. With session information from this table, we can plan further network topology to distribute service requests. When the manager detects the suspicious session information, he should add new policy or install new firewall system.

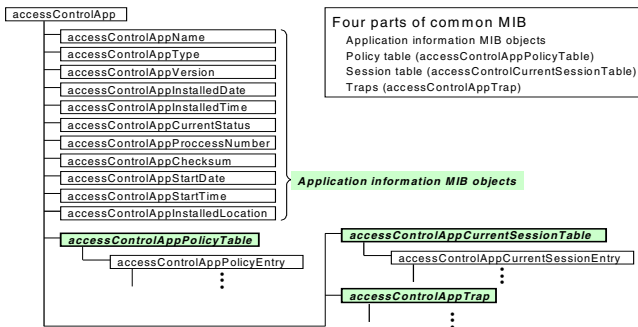


Fig. 7. Common MIB for A-ISMSF

• Traps

Traps are used to notify errors or special events to manager. For example, such special events are application starts working, stop working, status transition of application, the lack of log storage space, administrator logon, the modification of application configuration, it is not a policy, and so forth.

4.3 Prototype of the A-ISMSF

We developed the prototype of the web-based A-ISMSF - the agent-based integrated security management system for managing heterogeneous firewalls to monitor and control various kinds of firewalls through web environments. The management view consists of three parts – topology view, the explainable view of managed firewall and policy table view. The topology view shows the network topology of managed firewalls and the explainable provide the information of the managed firewall to manager. And, the policy table part supports the function to establish the security policy for managed firewall. Figure 8 describes the management view of the A-ISMSF.

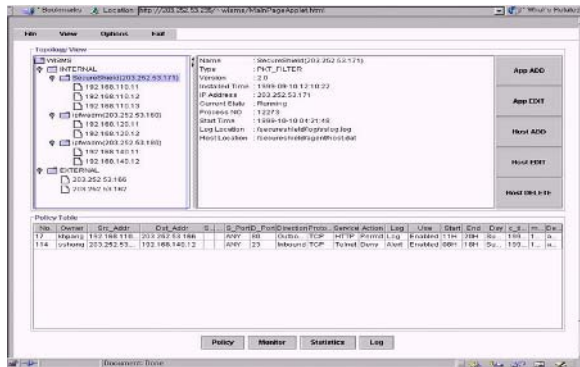


Fig. 8. Management View of the A-ISMSF

5 Conclusion and Future Works

In this paper, we proposed the structure of agent-based integrated security management system for firewalls. It manages the firewalls and designed MSAF - an agent of A-ISMSF. The architecture of MSAF is designed to be scalable to support various types of firewalls as well as to accommodate large scaled network environments. We analyzed the functions of heterogeneous firewalls with our experimental environment. And then, we defined Common MIB and application dependent MIB separately in order to manage an efficient integrated security management system. And also, client-engine Interface (CEI) and engine-agent Interface (EAI) exchange messages using HTTP and SNMP. Each interface is guaranteed secure message s transmission. Finally, we will extend A-ISMS which supporting security systems such as IDS, VPN, and other security systems and resolve the policy conflict problems for managed objects.

References

- [1] William R. Cheswick, Steven M. Bellovin, *Firewalls and Internet Security : repelling the wily hacker*, Addison Wesley, 1994.
- [2] D. Brent Chapman, Elizabeth D. Zwicky, *Building Internet Firewalls*, O Reilly & Associates, Inc., January 1996.
- [3] Chris Hare, *Karanjit Siyan, Internet Firewalls and Network Security - 2nd ed.*, New Readers, 1996.
- [4] William Stallings, *SNMP, SNMP v2, SNMP v3, and RMON 1 and 2 - 3rd ed.*, Addison Wesley, 1999.
- [5] David Perkins, Even McGinnis, *Understanding SNMP MIBs*, Prentice Hall PTR, 1997
- [6] Douglas Hyde, *Web-based Management*, 3Com Corp., Technical report, 1997.
- [7] D. Y. Lee, D. S. Kim, K. H. Pang, H. S. Kim, T. M. Chung, "Web-Based Integrated Security Management System using SNMP", *KNOM Review* Vol. 2, No. 1, April 1999.
- [8] J. Case, K. McCloghrie, M. Rose, S. Waldbusser, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2) , RFC1902, January 1996.
- [9] D. Harrington, R. Presuhn, B. Wijnen, An Architecture for Describing SNMP Management Frameworks , RFC2271, January1998.
- [10] J. Case, D. Harrington, R. Presuhn, B. Wijnen, Message Processing and Dispatching for the Simple Network Management Protocol(SNMP) , RFC2272, January 1998.
- [11] D. Levi, P. Meyer, B. Stewart, SNMP v3 Applications , RFC2273, January 1998.
- [12] TIS Firewall Toolkit Overview, Trusted Information Systems Inc., June 1994.
- [13] *SecureShield Administrator s Guide Version 1.0*, SecureSoft Inc.
- [14] Jos Vos, Willy Konijnenberg, "Linux firewall facilities for kernel-level packet screening", *X/OS Experts in Open Systems BV*, November 1996.
- [15] Iosif G. Ghetie, *Networks and Systems Management : Platforms Analysis and Evaluation*, Kluwer Academic Publishers, 1997.

Optimization of Fuzzy Rules: Integrated Approach for Classification Problems

Yunjeong Kang¹, Malrey Lee¹, Yongseok Lee¹, and Thomas M. Gatton²

¹ School of Electronics & Information Engineering, ChonBuk National University,
664-14, 1Ga, DeokJin-Dong, JeonJu, ChonBuk, 561-756, South Korea

Fax: 82-63-270-3403

mrlee@chonbuk.ac.kr

² School of Engineering and Technology, National University,
11255 North Torrey Pines Road, La Jolla, CA 92037 USA

Abstract. This paper proposes a GA and GDM-based method for removing the unnecessary rules and generating the relevant rules from the fuzzy rules corresponding to several fuzzy partitions. The aim of the proposed method is to find a minimum set of fuzzy rules that can correctly classify all the training patterns. This is achieved by formulating and solving a combinatorial optimization problem that has two objectives: to maximize the number of correctly classified patterns and to minimize the number of fuzzy rules. The fuzzy inference is structured by a set of simple fuzzy rules. In each rule, the antecedent part is made up of the membership functions of a fuzzy set, and the consequent part is made up of a real number. The membership functions and the number of fuzzy inference rules are tuned by means of the GA, while the real numbers in the consequent parts of the rules are tuned by means of the gradient descent method. In order to prove the effectiveness of the proposed method, computer simulation results are shown.

1 Introduction

Many applications of fuzzy reasoning to construct advanced controllers have been reported. Most of these controllers are constituted of a fuzzy model described in the IF-THEN type rules derived from the qualitative knowledge and the experimental know-how of experts or experienced operators. The study of information processing systems based on fuzzy rules has been mainly applied to control problems [1, 2]. The fuzzy rules used in most fuzzy control systems are generally derived from human expert's experience in using of linguistic information. A high non-linear system has undergone many trials and errors and several experiments to acquire proper fuzzy rules. It can provide fuzzy rules by using the numerical information of I/O data, the study of learning, and the study of the neural network and clustering [3, 4]. For classification problems, the automated generation method of fuzzy rules has been proposed by Ishibuchi et al [5, 6]. The generation of fuzzy rules from numerical data for pattern in classification problems consists of two phases: the fuzzy partition of a pattern space into fuzzy subspaces and the determination of a fuzzy rule for each fuzzy subspace. The pattern spaces are divided by a fuzzy grid, and the fuzzy rules are generated in the fuzzy spaces. The performance of a fuzzy classification system based

on fuzzy rules depends on the choice of the fuzzy partitions. If the partition is too coarse, the performance may be low (many patterns may be unclassified). On the other hand, if the fuzzy partition is too fine, many of the fuzzy rules needed may not be generated, because of the lack of training patterns in the corresponding fuzzy subspaces. Therefore the choice of the fuzzy partition is a very important stage. For example, consider the two-class classification problem shown in Fig. 2 where closed circles and open circles denote the patterns in class 1 and class 2, respectively. Because the choice of an appropriate fuzzy partitioning based on a simple fuzzy grid is made more complicated by the difficulty of finding simple fuzzy grid, the concept of distributed fuzzy rules has been proposed in [4,5,8,9,10], where all the fuzzy rules corresponding to several fuzzy partitions were simultaneously employed in a fuzzy classification system. The main drawback to this approach is that the number of fuzzy rules is enormous. If unnecessarily distributed fuzzy rules are removed, and only relevant fuzzy rules are selected, the performance of the selected rule set may become high with a fewer fuzzy rules. This paper proposes a GA [7, 14] and GDM-based [13] method for removing the unnecessary rules and generating the relevant rules from the fuzzy rules corresponding to several fuzzy partitions. The aim of the proposed method is to find a minimum set of fuzzy rules that can correctly classify all the training patterns. This can be achieved by formulating and solving a combinatorial optimization problem that has two objectives: to maximize the number of correctly classified patterns, and to minimize the number of fuzzy rules. A fine fuzzy division can be chosen for a fuzzy classification system with good values. For this, a large number of fuzzy divisions are performed. This method solves the problem of generating a fine fuzzy division but degrades the system efficiency on account of using many of fuzzy rules in inference. In the proposed method, the fuzzy rules corresponding to various fuzzy partitions are simultaneously utilized in the fuzzy inference process. Fuzzy rules are generated from an area with the highest inference errors among those areas which are divided by two membership functions of neighboring antecedent part. The fuzzy inference is structured by a set of simple fuzzy rules. In each rule, the antecedent part is made up of the membership functions of a fuzzy set, and the consequent part is made up of a real number. The membership functions and number of fuzzy inference rules are tuned by means of the GA, while the real numbers in the consequent parts of the rules are tuned by means of the gradient descent method. GA solves problems by using principles inspired by natural selection. That is, they maintain the populations of knowledge structures that represent candidate solutions and then let that population evolve over time through competition and controlled variation [8, 9, 10].

The rest of this paper is organized as follows. In chapter 2, fuzzy reasoning is described. The chapter 3 describes the selecting of fuzzy rules. In chapter 4, simulation results are given and discussed. Finally, the conclusion is presented in chapter 5.

2 Fuzzy Reasoning

This section explains the method used to control the real numbers in the consequent parts of the rules by using simple inference and the gradient descent method. When

the inputs are expressed as x_1, x_2, \dots, x_m , and the output is expressed as y , an inference rule used in simplified fuzzy reasoning can be expressed as [12]

$$\text{Rule } i: \text{ IF } x_1 \text{ is } A_{i1} \dots \text{ and } x_m \text{ is } A_{im} \text{ THEN } y \text{ is } w_i \quad (i=1, \dots, n) \tag{1}$$

where i is the rule number, A_{i1}, \dots, A_{im} are the membership functions of the antecedent part, and w_i is a real number in the consequent part. The membership function $A_{ij}(x_j)$ of the antecedent part is represented by an isosceles triangle as shown in Fig. 1.

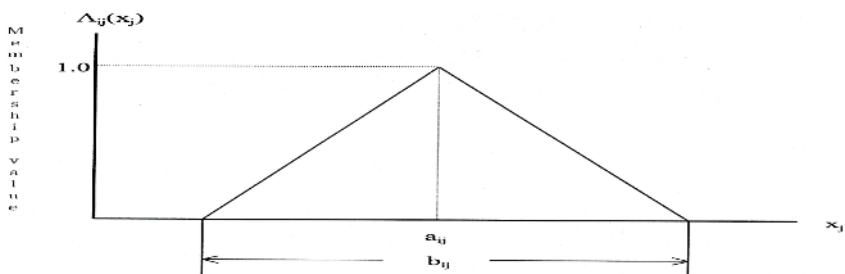


Fig. 1. Membership function of antecedent part

The parameters determining the triangle are the center value a_{ij} and the width b_{ij} . The output of the fuzzy reasoning, y , can be derived from the equations shown below.

$$A_{ij}(x_j) = 1 - \frac{2 \cdot |x_j - a_{ij}|}{b_{ij}} \quad (j = 1, \dots, m) \in [0,1] \tag{2}$$

$$\mu_i = \min\{A_{i1}(x_1), A_{i2}(x_2), \dots, A_{im}(x_m)\} \tag{3}$$

$$y = \frac{\sum_{i=1}^n \mu_i \cdot w_i}{\sum_{i=1}^n \mu_i} \tag{4}$$

where μ_i is the membership value of the antecedent part. This was used as an entity (member of the population) in the genetic algorithms. A real number in the consequent part, w_i , is optimized by using the gradient descent method to provide a local fine tuning mechanism for the GA.

The gradient descent method is used to seek for the vector Z that minimizes an objective function $E(Z)$, where Z is a p -dimensional vector $Z=(Z_1, Z_2, \dots, Z_p)$ of the tuning parameters [11]. In this method, the vector that decreases the value of an objective function $E(Z)$ is expressed as $(-\partial E/\partial Z_1, -\partial E/\partial Z_2, \dots, -\partial E/\partial Z_p)$, and the learning rule is expressed by

$$Z_i(t+1) = Z_i(t) - K * \partial E(Z) / \partial Z_i \quad (i = 1, \dots, p). \tag{5}$$

where t is a number of iterations of learning, and K is a constant. By altering Z according to this learning rule, the value of the objective function $E(Z)$ converges to a local minimum [13].

In the present method, the inference rules are tuned so as to minimize the objective function E which is defined as

$$E = 1/2 * (y - y^p)^2, \tag{6}$$

where y^p is the desirable output data (acquired from specialists). The objective function E represents the inference error between the desirable output, y^p , and the output of fuzzy reasoning, y .

The objective function E consists of the tuning parameter w_i . From Eq. 5, the learning rule of simplified fuzzy reasoning is expressed by

$$W_i(t+1) = w_i - k_w \cdot \partial E / \partial w_i, \tag{7}$$

where the tuning parameter k_w is constant. The learning rule of Eq.7 is to adaptively change the tuning parameters for a direction to minimize the objective function E . Thus, using the learning rule of Eq.7, the tuning parameter of inference rules is optimized to minimize the inference error between the desirable output of y_p and the output of fuzzy reasoning of y .

When repeatedly applying I/O data to the fuzzy rule, we can minimize the object function and acquire a global fitness solution without falling into the local minimum value.

Conventional self-tuning methods need many experiments and trials and errors in order to search for optimal rules. This paper uses a GA and the GDM to acquire the optimal rules.

3 Selecting of Fuzzy Rules

This section explains a method of optimizing the membership function shape and the number of fuzzy inference rules using GAs. The real numbers of the consequent parts of the fuzzy rules are obtained through the use of the gradient descent method. GAs are an optimization technique based loosely on the principles of natural selection. GAs start with a set of encoded parameter strings and an evaluation of the parameter performance corresponding to each string. Then, through the operations of reproduction, crossover, and mutation, the GAs attempt to represent strings into a set. Mutation is added after crossover to expand the region of points that can possibly enter as members of the population. The GAs choose the string with the maximum fitness function $E(s_r)$. Each string is represented as a binary number. A set of string S , called the population, can be represented as

$$s_r = L_{r1}, L_{r2}, L_{rg} \quad (g = 1, \dots, G), \tag{8}$$

$$S = \{ s_1, s_2, \dots, s_R \}. \tag{9}$$

3.1 Generation of Fuzzy Rules

This paper considers the second group in the classification problem shown in Fig. 2. The figure shows examples of generated problem instances by the function of $f(x) = 1/4\sin(2\pi x_1) + x_2 - 0.5$. The pattern space $[0,1] * [0,1]$ is divided into two classes according to the value of the following function $f(x) = 1/4\sin(2\pi x_1) + x_2 - 0.5$. If a

pattern has $f(x) \geq 0$, then x belongs to $G1$. Otherwise, x belongs to $G2$, Closed circles and open circles in Fig.2 represent patterns belong to $G1$ and $G2$, respectively. As learning data, we divided the group numbers of M ($G1, G2, \dots, G_M$) and supposed the pattern number of M ($x_p=(x_{p1}, x_{p2}, \dots, x_{pm}), p=1, 2, \dots, m$). Then each dimension of 2-dimensional pattern space consists of a fuzzy set of the number of k .

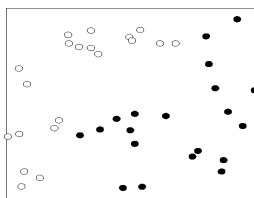


Fig. 2. A classification problem

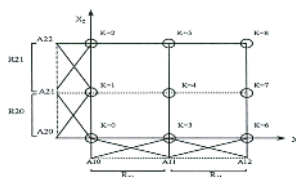


Fig. 3. Examples of fuzzy rule generating regions

[Generation method for fuzzy rules]

[Step 1] Determination of generation of regions for the fuzzy rules.

A rule is generated from the regions with the biggest inference error, after calculated in an each area partitioned by membership functions in neighboring two-antecedent part. Fig.3 shows an example for rule generation regions. The three-membership function in Fig. 3 is a fuzzy set with the input variables x_1 and x_2 . So the nine rules in total specified by the notation of uncolored circles are set. Inference errors are computed and chosen from four areas that are made from R_{10} and R_{11} on x_1 axis and R_{20} and R_{21} on x_2 axis. The region for rule generation is also selected for each input variable.

[Step 2] Generation of the Membership function of the antecedent part

Inference errors are selected from the region having highest error for rule generation. The region for rule generation might be selected for each input variables. A membership function is generated by dividing the region determined by (step 1) into two equal regions by its center value a_{ij} . And then, the membership function number is renumbered in an order of its smallest number. Figure 4 shows an example of the generation of the membership function in the region R_{10} shown in Fig. 2. In the case, three rules specified by a notation \bullet are newly generated.

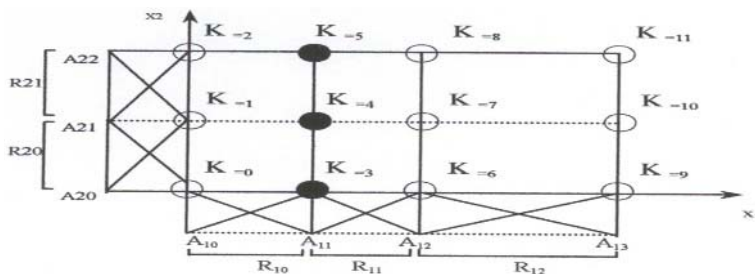


Fig. 4. Example of the generated Rules

[Step 3] Generation of the Real numbers of the consequent part
 Generation is achieved by means of the gradient descent method of eq. 7. The membership functions of an antecedent part are represented in Fig. 5.

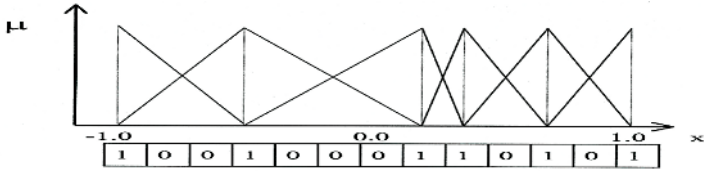


Fig. 5. String representation of membership functions

The binary representations of the membership function consist of strings of “1,” and “0”. A center value appears as “1”, and other appear as “0”. The optimal membership function numbers and its center value toward each input variable x_j are searched by the GA. The fitness $E(s_r)$ which is able to maximize the center value and the number of membership functions are searched for using a GA as follows.

A. A fitness definition

This paper use the learning pattern number $C(s_r)$ while representing the number of patterns that are classified by the rule set in an evaluation function employed for solving a classification problem using the GA. The number of rule sets is defined by $|s_r|$, and the fitness function is defined by the maximum of $C(s_r)$ and minimum of $|s_r|$. The fitness function $E(s_r)$ can be expressed as

$$E(s_r) = \max_r \{ W_c * C(s_r) - W_{s_r} * |s_r| \} \tag{10}$$

B. Definition of a entity

In order to find the optimal solution by using the GA, the entities have to be expressed as strings in order to find an executable solution. In this paper, the number of rules and the membership function are represented by several long strings that are treated as entities.

C. Operations of the GA

This paper uses a simple genetic algorithm employs a GA that extracts the rule by using an eliteness preservation strategy. The GA consists of five basic operations. The following operations are applied to a set of individuals (i.e., the population in a generation) in order to generate a new population in the next generation.

(1) Creation of an initial population

The center values of the membership functions and the widths of the neighboring membership functions are initialized as $a_{ij}=1$ and $b_{ij}=0$, respectively. To evaluate the initial population, the function representing the environment is evaluated for the values encoded in each of the n strings in the initial population $p(0)$.

2) Selection operation

To create the next generation by a crossover operation, a selection probability $P_{sr}(t)$ is represented by

$$P_{sr}(t) = \frac{E(s_r(t))}{\sum_{r=1}^R E(s_r(t))} \quad (11)$$

3.2 Self-tuning Procedure

The procedure to acquire an optimal fuzzy rule using a GA is as follows.

- Step 1: Randomly generate all entities (population) $s_r(t)$, $r=1, \dots, R$ about a initial generation ($t=0$).
- Step 2: Decide the initial real number of the consequent part, using the gradient descent method.
- Step 3: Select two entities $s_i(t)$ and $s_j(t)$ from population $S(t)$ according to selection probabilities $P_{s_i}(t)$ and $P_{s_j}(t)$.
- Step 4: Perform a crossover operation to create a new entity $s_k'(t)$ from the two selected entities.
- Step 5: Perform a mutation operation on a string of an entity $s_k(t)$, using the mutation probability P_m .
- Step 6: Until the new number of entities k , becomes equal to R , repeat from step 3 to step 5.
- Step 7: A new group (population) $S(t+1)=\{s_1'(t), s_2'(t), \dots, s_R'(t)\}$ is generated from step 3 to step 6.
- Step 8: Add 1 to the generation number t , and repeat from step 2 to step 8 until the population S converges. The largest fitness entity in the converged group becomes an optimal solution.

4 Results of Computer Simulations

In this section, a new method is compared with Ishibuchi's method by means of an experiment [4].

4.1 Rule Selection and Pattern Classification by a Fuzzy Grid

A classification problem is applied to Fig. 2. Ishibuchi divided the fuzzy space into subspaces using a fuzzy grid and spaces generating fuzzy rules. Fig. 6 shows the achieved fuzzy division up to six-fuzzy-set in two dimension pattern spaces. If the fuzzy division is small (k is larger), then many patterns may be classified, and many fuzzy rules can be generated, but the performance may be low. On the other hand, if the fuzzy division is large (k is smaller), then many fuzzy rules can not be generated because of the lack of training patterns in the corresponding fuzzy subspaces.

Black area: the rules of the first group (white dots): G1 Gray area: the rules of the second group (black dots): G2

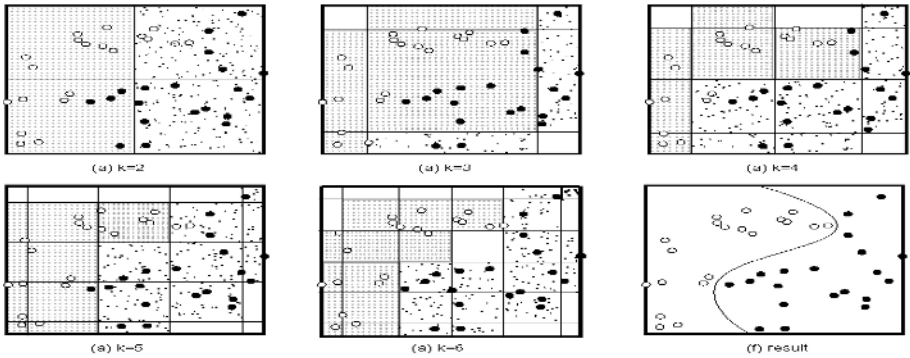


Fig. 6. Generated fuzzy rules and classification results

4.2 Rule Selection and Pattern Classification by GA

A genetic algorithm with the following parameter specifications was applied to the classification problem in Fig. 2.

Population size in each generation(R) : 20 individuals

Stopping Condition(t) : 1000 generation , Mutation Probability(P_m) : 0.01

Length of entity(G) : 13, Value of critical : 1.0×10^{-5}

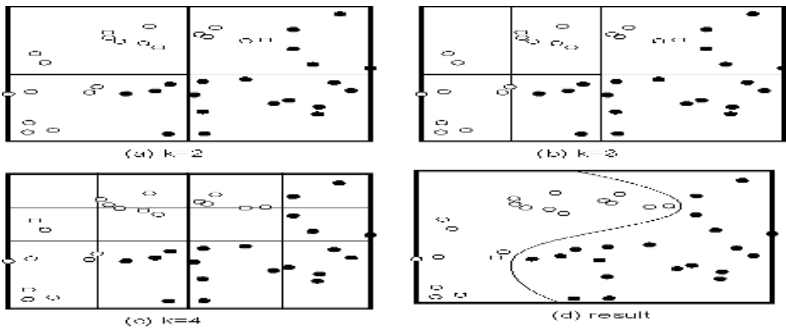


Fig. 7. Simulation results using the proposed method

From the classification results of Fig. 6, when k equals 6, it is possible to see that the whole pattern can be classified. In this case, the total number of rules are 60. The executable numbers of the solution become 1.2×10^{17} . If a GA is applied, then a total of 2000 rules are generated (20 individual *1000 generations). After these values were set, the first population was randomly changed 20 times. Fig. 7 shows the rules created and the classification results by using a numerical value experiment.

In comparing Fig. 6. with Fig. 7, in Fig. 7, the pattern division is accomplished with $k=4$, which is smaller than in Fig. 6. The areas (a)-(c) in Fig. 7 show the fuzzy rules generated by a GA, where (d) is the result of classifying the whole learning pattern. The method was there applied to some searched classification problems as shown in the next section.

4.3 Test Problems

As test problems, five classification problems were selected. In each problem, the pattern space $[0,1]*[0,1]$ is divided into two classes according to the value of the following function $f(x)$. If $f(x) \geq 0$, then x belongs to G1. Otherwise, x belongs to G2.

Problem 1: $f(x) = -1/4\sin(2\pi x_1) + x_2 - 0.5$

Problem 2: $f(x) = -1/3\sin(2\pi x_1) + x_2 - 0.5$

Problem 3: $f(x) = -1/3\sin(2\pi x_1 - 1/2\pi) + x_2 - 0.5$

Problem 4: $f(x) = -|-2x_1 + 1| + x_2$

Problem 5: $f(x) = (x_1 + x_2 - 1)(-x_1 + x_2)$

For each classification problem, 20 problem instances were randomly generated, where each of 10 problem instances has 20 patterns in each class as the given patterns (i.e., as the training patterns). Closed circles and open circles in the given patterns belong to G1 and G2, respectively. These patterns are used for deriving the fuzzy rules in computer simulations. Table 1 shows the usefulness of the suggested method (e. g., in Problem 1).

In the application to the IRIS data, the following biased mutation probability was employed in order to reduce the number of fuzzy rules by the mutation operation: $P_m = 0.01$ for the mutation from $S_r = 1$ to $S_r = -1$, and $P_m = 0.001$ for the mutation from $S_r = -1$ to $S_r = 1$.

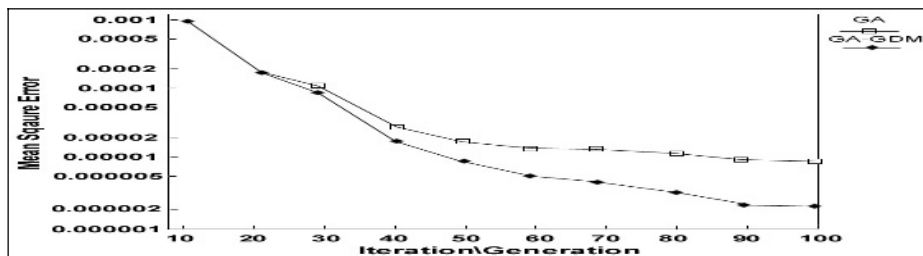


Fig. 8. Results after 100 epochs of learning

5 Conclusion

In this paper, the GA and gradient descent method-based rule generation method has been proposed for finding an appropriate set of fuzzy rules for classification problems. In the proposed method, a GA and gradient descent method were applied to the generation of fuzzy rules generated from numerical data. A combinatorial

optimization problem was formulated for finding a minimum set of fuzzy rules that could correctly classify all the given patterns. The GA and GDM were applied to this problem, and simulation results were shown. However, we had only one among probability values of mutation and took our examination. Future work will involve studying the effects of various probability values on classification problems and apply to similar applications.

References

1. K. H Lee, K. R Oh, Fuzzy Theory and Applications I-II, Hongrung Press, (1991)
2. H. Ichihshi and T. Watanabe : "Learning control system by a simplified fuzzy reasoning model", IPMU'94, Paris-France, July 2-6, (1994) 417-419
3. Shigeo and Ming-Shong Lan: "A method for fuzzy rules extraction directly from numerical data and its application to pattern classification", IEEE Transactions on Fuzzy System, Vol. 3, No. 1, (1995) 18-28
4. H. Ishibuchi, K. Nozaki and H. Tanaka, "Efficient fuzzy partition of pattern space for classification problems." Proc. of the Second International Conference on Fuzzy Logic & Neural Networks (Iizuka, JAPAN), (1992) 671-674
5. H. Illshibuchi, K Nozaki and H. Tanaka, "Distributed representation of fuzzy rules and its application to pattern classification," Fuzzy Sets and Systems, Vol. 52, (1992) 21-32
6. H. Ishibuchi, K. Nozaki and R. Weber, "Approximate pattern classification with fuzzy boundary", Proc. of International Joint Conference on Neural Networks, Vol. 52, (1992) 21-32
7. D. E. Goldberg, Genetic Algorithms in Search, Optimization, and Machine Learning. Addison-Wesley, Reading, Massachusetts, (1989)
8. Thrift P., "Fuzzy logic synthesis with genetic algorithms", Proc. of the 12th International Conference on Genetic Algorithm, San Diego, USA, (1999) 509-513
9. C. L. Karr, "Design of an adaptive fuzzy logic controller using a genetic algorithm," Proc. of the 12th International Conference on Genetic Algorithms, (1999) 450-457
10. Karr C., "Genetic algorithms for fuzzy controllers", AI Expert, February, (1998) 26-33
11. H. Nomura, I. Hayashi and N. Wakami, : " A self-tuning method of fuzzy control by descent method", Proc. of 14th IFSA Congress, Brussels, (2001) 155-158
12. M. Maeda and S. Murakami,: "Self-tuning fuzzy logic controller", Transactions of the society of Instrument and Control Engineers, Vol. 34, No. 2, (1998) 191-197
13. H. B. Carry, "The method of steepest descent for nonlinear minimization problems", Quart. J. Appl. Math., 2, (1994) 258-261
14. D. Park, A. Kandel and G. Langholz, "Genetic-based new fuzzy reasoning models with application to fuzzy control," IEEE Trans.Syst. Man Cybern., Vol. 24, no. 1, (1994) 39-47

A Cooperation Model Using Reinforcement Learning for Multi-agent

Malrey Lee¹, Jaedeuk Lee², Hye-Jin Jeong¹, YoungSoon Lee¹,
Seongman Choi¹, and Thomas M. Gatton³

¹ School of Electronics & Information Engineering, ChonBuk National University,
664-14, 1Ga, DeokJin-Dong, JeonJu, ChonBuk, 561-756, Korea

Fax: 82-63-270-3403

mrlee@chonbuk.ac.kr

² Chosun College of Science & Technology, Korea

³ School of Engineering and Technology, National University,
11255 North Torrey Pines Road, La Jolla, CA 92037 USA

Abstract. In multi-agent systems, the common goals of each agent are established and the problems are solved through cooperation and control among agents. Because each agent performs parallel processes in a multi-agent system, this approach can be easily applied to problems requiring parallel processing. The parallel processing prevents system performance degradation due to local error operation in the system. It also can reduce the solution time when the problem is divided into several sub-problems. In this case, each agent is designed independently providing a relatively simple programming model for solution of the problem. Further, the system can be easily expanded by adding new function agents. In the study of multi-agent systems, the main research topic is the coordination and cooperation among agents.

1 Introduction

The information sources, communication links and agents may not be traced when they are created and disappear. Under this environment, it is difficult to solve problems by using a single agent, which has limited information, computing resources and capabilities [14]. Recently, in order to overcome this difficulty, multi-agent systems have been widely used. In multi-agent systems, agents are equally connected, communicate with each other and control themselves. Multi-agent systems, which are based on distributed artificial intelligence, are able to cooperatively solve problems which a single agent is not able to solve [2,3].

In multi-agent systems, the common goals of each agent are established and the problems are solved through cooperation and control among agents. Because each agent performs parallel processes in a multi-agent system, this approach can be easily applied to problems requiring parallel processing. The parallel processing prevents system performance degradation due to local error operation in the system. It also can reduce the solution time when the problem is divided into several sub-problems. In

this case, each agent is designed independently providing a relatively simple programming model for solution of the problem. Further, the system can be easily expanded by adding new function agents.

In the study of multi-agent systems, the main research topic is the coordination and cooperation among agents. While each agent solves its assignment, it may experience difficulties and confusion due to the local view, multiple goals, distributed information and conflict with other agents. Both coordination and cooperation among agents are necessary to overcome the limitation of each agent, create their own capabilities and knowledge and increase the overall system efficiency. They are also necessary when an agent's behavior is determined by other agents' behaviors. However, the current methodologies for the coordination and cooperation have similar problems because the roles of the agents are fixed and their applications in dynamically-varying open environment are not appropriate.

In this paper a new model for role coordination between agents is proposed in order to improve the currently existing methods. This model modifies its role by using reinforcement learning when the roles of different agents conflict with each other. In chapter 2, reinforcement learning is discussed, and in chapter 3, a new role coordination model is proposed and subsequently applied to an artificial life competition problem in chapter 4. Chapter 5 presents the conclusion for this paper.

2 Coordination Model

2.1 Environment

The parameters that can be varied in the artificial attract system domain are summarized in Table 1.

Table 1. Variable parameters in the artificial attract system domain

- | |
|---|
| <ul style="list-style-type: none"> . Definition of capture, Size and shape of the world, Predator's legal moves . Simultaneous or sequential movement, Visible objects and range . Predator communication . Prey movement |
|---|

The goal of the total agent system is set up through a type of pre-knowledge roles that are carried out by agents, and the sorting of agents' possible actions are specified by the style of actions in each role. Also, the roles to decide their initial roles and to detect conflict between roles are provided as domain knowledge. Therefore, according to the initial role decided by the basis of its pre-knowledge, each agent carries out its role and cooperates with other agents and pre-knowledge when there is conflict with other agents. Reinforcement learning is utilized to carry out the control of its role. Table 2 specifies the pre-knowledge for agents.

Table 2. Pre-knowledge for agents

class	Pre-knowledge
Goal	. a sort of roles to be carried out by each agent
Action	. action type to be carried out to each role
Domain	. a set of rules to automatically role allotment
Knowledge	. a set of rules to detect conflict of roles

The competition environment has a continuous 12*5 lattice structure without any boundary. Initially, the two groups in competition are located arbitrarily at the left or right hand side of the competition environment. If the movement of agents has absolute directions such as east-west-north-south in the competition environment, the results would be sensitive to the initial positions of the groups. Therefore, each agent has directivities of forward, backward, left and right based on its head direction. In the competition environment, there exist only two populations selected for competition, and no obstacles or food. Initial positions of the two competitive populations are sequentially located in the pre-determined lattice. As shown in Figure 2, A and B populations are located at 3-4 and 9-10 columns, respectively. To avoid static behavior pattern due to the initial positioning of the populations, the initial head directions are arbitrarily determined.

2.2 Reward Model

In Reward Model , the artificial organism divides the environment into the friend and the enemy. When the attack to the environment is successful, the reinforcement signal is (+3) in case of the enemy and (-) in case of the friend. This is to balance the reinforcement signal of the enemy's successful attack behavior and the constraint signal of being attacked behavior. In reward model, the default value of reinforcement signal, which was a cause of unnecessary learning, is changed to 0. The constraint signal for behaviors of failed movement or attack is (-1) reinforcement signal. Also, for

Table 3. Reward Model

A sort		Reward Value	
default value		0	
Stop		0	
Movement	Successful	0	
	failed attack	-1	
Attacked	Successful	friend's attack	-1
		enemy's attack	+3
	failed attack	-1	
Being Attacked	One time	-1	
	Two time	-2	
	Three time	-3	

behaviors which induces the attack from the environment, constraint signal of (- number of being attacked) is generated to control the strength of the constraint effect. In reward model , constraint learning for behaviors of failed movement and failed attack is performed. This induces the organism to behave in a more exact and reasonable way. It also induces the artificial organism's attack behavior by eliminating unnecessary reinforcement learning for a simple movement or stop behavior.

(step 1): Initialize reinforcement signal to default value
 (step 2): If (enemy's attack is successful) then reinforcement signal = reinforcement signal +3
 (step 3): If (friend's attack is successful) then reinforcement signal = reinforcement signal -1
 (step 4): If (failed attack) then reinforcement signal = reinforcement signal -1
 (step 5): If (failed movement) then reinforcement signal = reinforcement signal -1
 (step 6): If (being attacked) then reinforcement signal = reinforcement signal -(number of being attacked)

Fig. 1. Computation Algorithm of Reward Model

2.3 Reinforcement Learning Using Q-Learning

The proposed role control model applies the reinforcement learning method using Q-learning , if a conflict of roles occurs [14,15].The reinforcement learning is a learning method that observes system actions, provides appropriate appraisal, and makes desired actions represented in a system. Specially, when Q-learning is utilized as an inferring method of value functions that appraises appropriateness of current status to accomplish a goal on-line, learning is possible without any model for a system to be learned. In the Q-learning method, the mapping between Q-value and state value is searched for using a pair of action and environment state called Q-value. Q-function is utilized for value function. In addition, since it requires only one execution to modify the q-function, the q-learning is advantageous for on line learning. These characteristics of reinforcement learning satisfy many conditions needed for the cooperation between agents in a static environment.

A reinforcement signal represents:

- 1: reward (when a role confliction is resolved)
- 0: punishment (when a role confliction is not resolved)

An agent having received a control signal decides a new role based on the q-function that it keeps, executes the new role, and receives one of the reinforcement signals according to the results of the execution. In learning rule for q-learning to be used in this paper, the q-function is utilized to make a pair with an environment state and an action, and the expected value at the next environment state can be computed without determining all possible actions. If the expected value when an action a is selected at a state s is $Q^*(s, a)$, and the maxim value of $Q^*(s, a)$, is $\max Q^*(s, a)$, then the state value $V^*(s)$ of a state s is computed with following equation as $\max Q^*(s, a)$,:

$$V^*(s) = \max_a Q^*(s, a) \quad (1)$$

And $Q^*(s, a)$ can be represented with a recursive express as:

$$Q^*(s, a) = R(s, a) + \gamma \sum_{s'} T(s, a, s') \max_{a'} Q^*(s', a') \quad (2)$$

Where $R(s, a)$ represents a reward signal value when a state s is transient to s' executing an action. R is a constant value, when the action a is selected, to impose more weight on the effect of current environment. $T(s, a, s')$ is state transition function.

$$Q(s, a) := Q(s, a) + \alpha(r + \gamma \max_{a'} Q(s, a') - Q(s, a)) \quad (3)$$

Where α denotes the learning rate to decide the degree of reinforcement learning, and r represents a value of reinforcement signal in current state.

3 A Method of Automatic Role Coordination

Agents in the role coordination model have the following procedure for performing tasks:

- Step 1: Each agent decides its initial role based on the environment state and the given domain knowledge.
- Step 2: Each agent informs the needs for role coordination while sending coordination signals if its role conflicts with other agents' roles in the observation scope.
- Step 3: Agents receive coordination signals to determine any behavior changes or maintenance of roles according to the value functions.
- Step 4: Each agent performs its work based on the current role.
- Step 5: Each agent self-evaluates the behavior resulting from the previous step, performs reinforcement learning, and revises the value functions, sequentially.
- Step 6: Repeat from step 2 to step 5.

Each agent in the proposed model in this paper always watches its part observation scope and sends coordination signals to corresponding agents if it needs role coordination while checking for conflict with others. Agents receiving the coordination signals change their roles by themselves and compute the values of complement signals according to whether they solve role conflicts or not. With this procedure, reinforcement learning is possible without centralized control for reinforcement signals. Since the goal of the whole system is specified through sorts and the duties of roles, each agent helps the goal to be accomplished by deciding its role and performing the duty of its role. Each agent (or predator) merely performs its predefined duty and doesn't require the evaluation information about the whole system. Thus, the role coordination model using the reinforcement learning proposed in this paper has the advantage of adjusting dynamic environments by coordinating roles through on-line learning if the goals of the agents conflict with each other.

4 Experiments

This chapter describes the emergent behaviors of multi-agents in an artificial attack system. In order to verify the model for the role distribution and control, the model is applied to the pursuit/prey problem. Constraints, such as multiple targets, are modeled and the system to solve these constraints is constructed. The pursuit/prey problem consists of a latticed virtual world, several predators and several prey. The target of the problem is to surround the moving prey by the predators to capture the prey. The virtual world is an infinite space in which the sides are connected. The predator and prey move along the lattice in four directions. Two or more agents cannot be located at the same lattice. The prey moves in an arbitrary direction and 10% slower than the predator. The predators know each other's location. In this experiment, each agent plays as a controller to determine the predator's direction and the problem is solved through cooperation between agents.

The pursuit/prey problem in the experiment basically follows the previous approach. However, instead of arbitrary movement against the prey's behaviors, a more intelligent way of escape, through the movable region is maximized by modifications to model the constraints of movable agents.

The movable region is defined as follows: " Among the points in the virtual world, the number of the points which distance to the prey is shorter than that to the other predators is the movable region, that is, the region where the prey can reach first than that the predators when they start at the same time. Theoretically, all points in the virtual world are to be considered to define the movable region. However, the range of calculation is constrained for some advantages in the actual calculation. To maximize the movable region, it is obtained when the prey moves all four directions. Then the prey moves to the direction which has the largest value. Therefore, the behavior can be more intelligent by considering various possibilities."

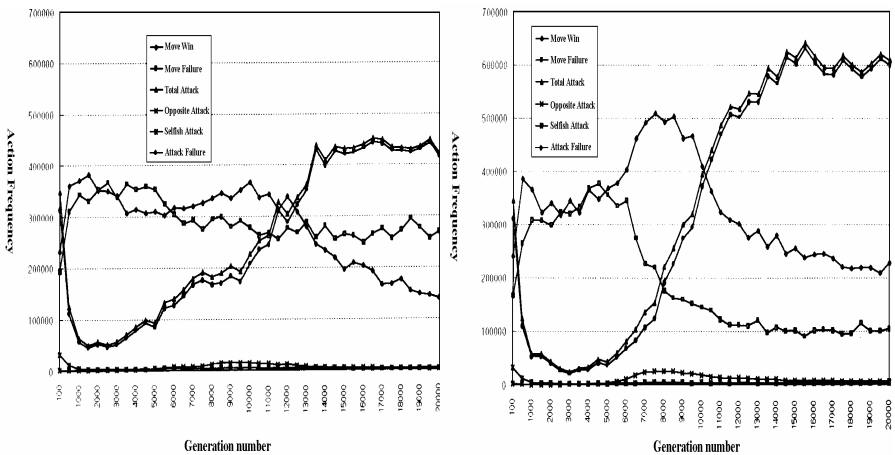


Fig. 2. (a) No Learning Case

(b) Learning Case

5 Conclusion

This paper proposed a role coordination model to resolve the conflicts that can take place between agents in multi-agent systems and applied a modified pursuing problem with this model. In the model, the reinforcement learning has been used to coordinate agents' roles, which function for the agents to cooperate with, although they may have different goals in dynamic environments of the multi-agent systems. Moreover, the validity of the proposed model has been verified by solving the modified pursuing problem. The pursuing problem used in this paper has been modified to include dynamic environments and local observation for multi-agent systems and constraints for multiple goals. However, all of the various components that can be contained in real problems cannot be included. Thus, for future work, further experiments to see if the proposed model can be applied to various applications having a variety of problems should be investigated. In the area of multi-agent system application, further research is needed to subdivide the problems into each agent's role and reduce the dependence of domain knowledge by properly dividing into agents' roles. When the role coordination method is used with reinforcement learning, research about the stability of agent systems is also required, since there is no security to suppress agents that over-issue coordination signals regardless of the environment status

References

1. "Co-ordination in Multi-Agent Systems", Software Agents and Soft Computing, Towards Enhancing Machine Intelligence, concepts and Application, Springer, (1997)
2. Brooks and Maes ed., Artificial Life IV, MIT Press, (1994)
3. Asama et. Al. eds, Distributed Autonomous Robotic Systems I, II, Springer-Verlag, (1994)
4. D. W. Lee, K. B. Sim, "Behavior Learning and Evolution of Collective Autonomous Mobile Robots using
5. Distributed Genetic Algorithms," Proc. of 2nd ASAsian Control Conference, Vol.2, (1997) 675-678
6. Ono, N.; Fukumoto, K., and Ikeda, O.. Collective Behavior by Modular Reinforcement Learning Animate Proceedings of 4th international Conference on Simulation of Adaptive Behavior, (1997) 618-624
7. Yusuke Tanaka and Taketoshi Yoshida "An Application of Reinforcement Learning to Manufacturing Scheduling
8. Problems", IEEE, Vol. 4, (1999) 534-539
9. Pdraig Cunningham and Richard Evans, "Software Agents : A review", (1997)
10. H.S. Nwana, L. Lee and N. R. Jennings, "Co-ordination in Multi-Agent Systems", Software Agents and Soft
11. Computing Towards Enhancing Machine Intelligence, Concepts and Application, Springer, (1997)
12. Peter stone and Manuela Veloso, "Multi-agent Systems: A Survey from a Machine Learning Perspective", Autonomous Robots 8, (2000) 345-382

Development of Network Event Analysis Algorithm Applying Association Rule

Seakjae Han¹ and Wooyoung Soh²

¹ Department of Computer Engineering, Hannam University,
Daejeon, S. Korea
koen@dmdworld.com

² Department of Computer Engineering, Hannam University,
Daejeon, S. Korea
wsoh@neuro.hannam.ac.kr

Abstract. Security threat management system analyzes network status. Network analysis generally gives information about external network status and secures from external attacks by scrutiny of handling internal network. This paper expounds analysis of external network as well as internal network through application of association rule to the network event using data mining method. Essentially Apriori algorithm is used for data mining, yet not suitable for network traffic analysis on real-time. This paper devises and implement network event audit module using the network event association rule algorithm instead of Apriori algorithm.

1 Introduction

To prevent computer emergency against attack and vulnerability, firewall, IDS, etc. are used. Prevention and intrusion are the abilities of the said security system except if it is unknown [1]. Recently, Threat Management System (TMS) [2] shows the network manager the analyzed network events [3] for one of the responses against unknown attack and can also analyze internal network events to know new type of attacks and network procedures.

This paper analyzes network events through application of association rule to the network events using data mining method. Designs and implementation of network event audit module using the new algorithm instead of Apriori algorithm [4][5] is presented.

Composition of this paper is as follows: Chapter 2 confers association rule algorithm. Chapter 3 presents the design and implementation of network events audit module using the new algorithm. Finally Chapters 4 depicts the conclusion.

2 Related Works

2.1 Apriori Algorithm of Association Rule

Data base management systems (DBMSs) have given access to the data stored but they give no analysis of the data. Analysis is required to reveal the hidden

relationships within the data, for instance, for decision support. Size of databases has increased and therefore there is a strong need for automated techniques for automated analysis[6]. Those techniques called data mining and well-known data mining technology is association rule.

Apriori is the most basic and well-known association rule algorithm that locates frequent itemsets in a transactional database. The Apriori algorithm utilizes a simple two-step process; generate frequent itemsets of size k then merge them to generate candidate frequent itemsets of size k+1. The Apriori algorithm takes advantage of the simple Apriori observation that all subsets of a frequent itemset must also be frequent.

Table 1. System environment for development test

Number of purchase	Itemsets
1	{1, 3, 4}
2	{2, 3, 5}
3	{1, 2, 3, 5}
4	{2, 5}

For example, there is database D and let 1st candidate set be C₁, 2nd candidate set is C₂, 3rd candidate set is C₃... nth candidate set is C_n, then we can make a frequent set from C_n.

Let 1st frequent set be F₁, 2nd frequent set is F₂... nth frequent set is F_n.

Table 2 C₁ shows percentages each candidate through scanning from Table 1. Then Table 2 presents F₁ through C₁.

Table 2. Set of candidates C₁ and frequent set F₁

itemset	Frequency (%)
{1}	50%
{2}	75%
{3}	75%
{4}	25%
{5}	75%

itemsets	Frequency (%)
{2}	75%
{3}	75%
{5}	75%

We can make subsets following Table 3 from F₁ and C₂ through scanning D with F1.

Table 3. Set of candidates C_2 and frequent set F_2

itemsets	Frequency (%)		itemsets
{2, 3}	50 %		{2, 3}
{2, 5}	75 %		{2, 5}
{3, 5}	50 %		{3, 5}

Table 4 exemplifies F_2 through C_2 and we finally can make association itemsets {2, 5} through frequent itemsets.

Table 4. Frequent set F_2

itemsets	Frequency (%)
{2, 5}	75 %

3 Implementation and Experiments

3.1 Summary of Network Event Association Rule Algorithm

Threat management system analyzes IP address, port and URL through network traffic usage and packet counts against the new type of attacks and vulnerabilities. This Paper associates with each IP address and port. In this paper, network event items are classified four parts. Because IP address and port are classified source and destination. Therefore network event associations can be made $2^4 = 16$ kinds.

For example, if a lot of same source IP address and destination IP address are associated, then it supposes scan attack. Also if a lot of same source IP address, destination IP address, source port and destination port are associated, then it supposes DoS(Denial of Service) attack. System and development environment for test that algorithm in this paper is below.

Table 5. System environment for development test

CPU	Pentium 4 2.4Ghz(HT)
Memory	512M
HDD	80G
OS	Windows XP Professional
Development tool	Delphi 6

3.2 Network Event Analysis Module Using Apriori Algorithm

For association with network event data, this paper uses representative association rule algorithm Apriori. At this time network event classify source IP, destination IP,

source port and destination port. Since input item is four counts, the number of association rule subset is $2^4 = 16$ counts. Associated rule must make definition of association pattern. For example, if a lot of same IP address and destination IP address can associated, then it supposes scan attack.

In this Paper, network event association rule algorithm uses event count instead support and confidence in Apriori algorithm. IP address and destination port input data item is generated randomly by 10 counts of previous setting data. But, source port input data item is generated randomly by range of 2 bytes. Support count is 30 counts in this test. Even support count was increase or decrease, it was not related in process time by test result.

Fig. 1. is test program with Apriori algorithm.

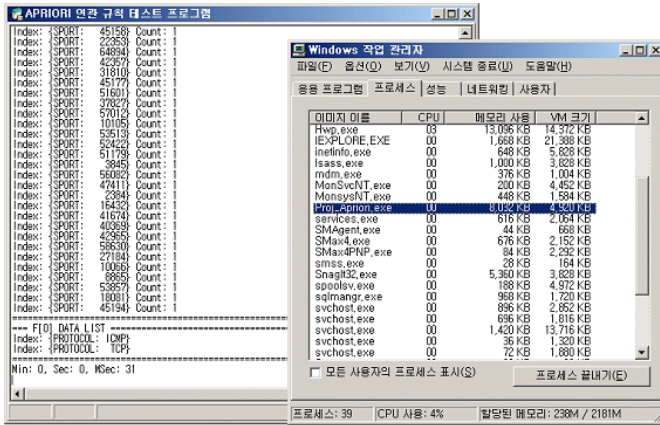


Fig. 1. Using Apriori algorithm with 100 counts of input data

Fig. 1. shows test program using Apriori algorithm with 100 counts of input data. As the results, it takes 0.031 process time and 8 Mbytes of real memory usage and 5 Mbytes of virtual memory usage. Also test program using Apriori algorithm with 1000 count of input data. As the results, it takes 41.843 process time and 44 Mbytes of real memory usage and 41 Mbytes of virtual memory usage. Test program using Apriori algorithm with 10000 counts of input data. As the results, it takes 111.312 process time and 70 Mbytes of real memory usage and 538 Mbytes of virtual memory usage.

If frequent subset is n counts, candidate subset can make $nC_2 = n!/(n-2)!$ counts in test program using Apriori algorithm.

If 1st frequent subset is 100 counts composed by IP address and port are different each other, 2nd candidate subset are $100!/(100-2)! = 100 \times 99$ counts. Also if 2nd frequent subset is 100×99 counts composed by subset are different each other, 3rd candidate subset are $(100 \times 99)!/((100 \times 99) - 2)!$ counts.

So test program using Apriori algorithm require lots of processing time memory usage for candidate subset make. If it use real network events, system will be required processing time memory usage more than test program.

3.3 Proposal New Network Event Association Rule Algorithm

Network event analysis program using Apriori algorithm is impossible on real time.

So, this paper proposes new network event association rule algorithm.

Network event association rule algorithm is accounted frequent subset count and candidate subset in the input time. Network event association rule algorithm makes individual item node. Individual item node has another item node below.

For example when input data is {A, B, C, D}, it makes A, B, C and D node. A node makes B, C and D node. B node makes C and D node. C node makes D node. Individual input item makes node below continuously until item don't have below item. At this time individual item node set accounts count. When 1st input data is {A, B, C, D} and 2nd input data is {B, C, F, G} then below figure shows individual item node set.

A node	A(1) - B(1) - C(1) - D(1) - D(1) - C(1) - D(1) - D(1)
B node	B(1) - C(1) - D(1) - D(1)
C node	C(1) - D(1)
D node	D(1)

Fig. 2. When 1st input data make input item node set lists

Fig. 2. shows when 1st input data make input item node set lists. Node item has individual counts use mark (). A(1) means A item counts is one.

A node	A(1) - B(1) - C(1) - D(1) - C(1) - D(1) - D(1)	➔	A node	A(1) - B(1) - C(1) - D(1) - C(1) - D(1) - D(1)
B node	B(1) - C(1) - D(1) - D(1)		B node	B(2) - C(2) - D(1) - D(1) - F(1) - G(1) - G(1) - F(1) - G(1) - G(1)
C node	C(1) - D(1)		C node	C(2) - D(1) - F(1) - G(1) - G(1)
D node	D(1)		D node	D(1)
			F node	F(1) - G(1)
			G node	G(1)

Fig. 3. When 2nd input data make input item node set lists

When 2nd input data input list, we can see like upper figure. Fig. 3. shows after 2nd input data input, B(2)-C(2)-D(1) item node set is two counts of association rule {B, C}.

3.4 Network Event Analysis Module Using Network Event Association Rule Algorithm

Below figure shows test program using network event association rule algorithm. Test condition is same as Apriori algorithm. Test condition is input data and support count.

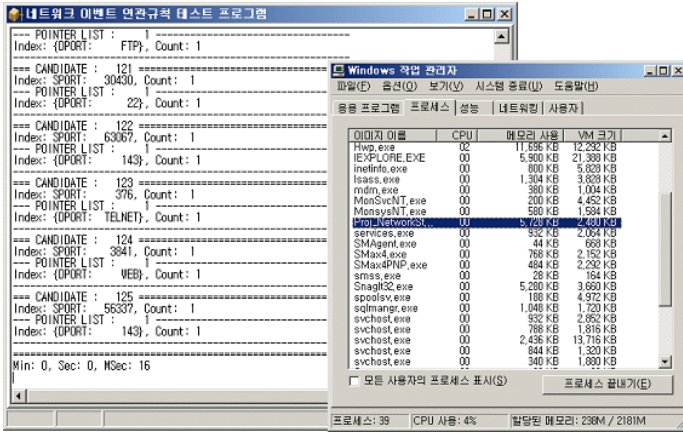


Fig. 4. Using network event association rule algorithm with 100 counts of input data

Upper figure shows test program using network event association rule algorithm with 100 counts of input data. At this time it takes 0.016 process time and 5 Mbytes of real memory usage and 2 Mbytes of virtual memory usage.

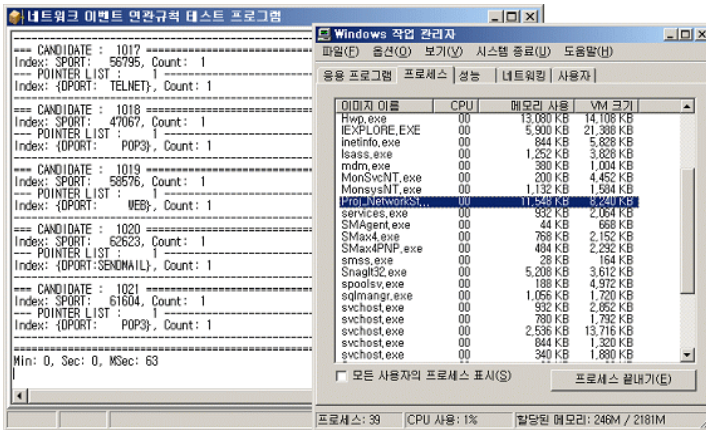


Fig. 5. Using network event association rule algorithm with 1000 counts of input data

Fig. 5 shows test program using network event association rule algorithm with 1000 counts of input data. At this time it takes 0.063 process time and 11 Mbytes of real memory usage and 8 Mbytes of virtual memory usage



Fig. 6. Using network event association rule algorithm with 10000 counts of input data

Fig. 6. shows test program using network event association rule algorithm with 10000 counts of input data. At this time it takes 0.485 process time and 68 Mbytes of real memory usage and 64 Mbytes of virtual memory usage.

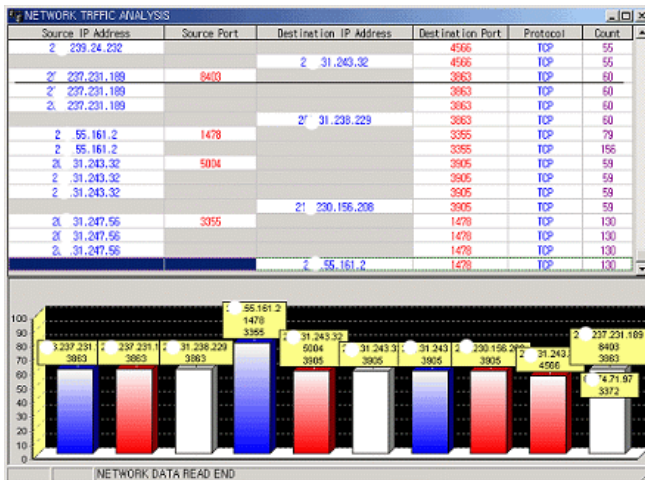


Fig. 7. Network event association rule algorithm with real network event

Upper figure shows program using network event association rule algorithm with real network event. And it process in real time.

Table 6. Performance comparison of Apriori and Network event association rule

Input data counts	Apriori algorithm			Network event association rule algorithm		
	Processing time	Memory(Mbyte)		Processing time	Memory(Mbyte)	
		Real	Virtual		Real	Virtual
100	0.031	8	5	0.016	5	2
1000	41.843	44	41	0.063	11	8
10000	111.312	70	538	0.485	68	64

4 Conclusion

From the network events analysis using data mining method, to prevent against unknown vulnerability and attack, the Apriori algorithm, CPU and memory required high usage, but, the implemented network event association rule algorithm shows excellent result, it can be applied to TMS and other network systems.

References

1. Hyung-Jong Kim, Hong-Geun Kim, Tae-Ho Cho, "Simulation model design of computer network for vulnerability assessment", International Workshop on Information Security Applications (WISA) 2001, Vol.2, pp.203-217.
2. H. Reiser and G. Vogt, "Threat Analysis and Security Architecture of Mobile Agent based Management Systems", Proceedings of NOMS 2000 IEEE/IFIP Network Operations and Management Symposium "The Networked Planet: Management Beyond 2000", Honolulu, Hawaii, USA, April 2000.
3. Myung-Sup Kim, Young J. Won, and James Won-Ki Hong, "Application-Level Traffic Monitoring and Analysis on IP Networks", ETRI Journal, Vol.27, No.1, Feb. 2005, pp.22-42.
4. Maria C. FERNANDEZ, Ernestina MENASALVAS, Oscar MARBAN, "Minimal Decision Rules Based on the Apriori Algorithm", Int. J. Appl. Math. Comput. Sci., 2001, Vol.11, No.3, pp.691 – 704.
5. Ute Ziegenhain, Josef G Bauer, "Triphone tying techniques combining a-priori rules and data driven methods", European Conference on Speech Communication and Technology (EUROSPEECH) 2001, Vol.2, pp.1417-1420.
6. Timo Honkela, "Data Mining and Document Modeling", Neural Networks Research Centre Helsinki University of Technology Tue Aug 5 1997

A New Secure Oblivious Transfer Protocol

Soon-gohn Kim¹ and Heau-jo Kang²

¹ Department of Computer Multimedia Science, Joongbu University,
Daehakro 101, Gumsangun, Chungnam 312-702, Korea
sgkim@joongbu.ac.kr

² Division of Computer Engineering, Mokwon University, 800, Doan-Dong,
Daejeon, 305-729, Korea
hjkang@mokwon.ac.kr

Abstract. In this paper, we proposed two methods in the field of Oblivious Transfer for secret information. One is the interactive method, the other is the non-interactive method. In the first method, we considered the possible situation where one denies what he/she has sent the messages to the other in the process of protocol. To do this we used cryptographic technique for the messages transferred between two mutually distrustful parties. This method has the additional functions that enable to authenticate sender and to protect one's denial of what he/she has sent the messages to the other. In the second method, we proposed non-interactive method for the secure exchange of secret data. Proposed method is based on the difficulty of discrete logarithm problem. The security in proposed method can be chosen as a random number. The traffic amount of proposed method is less than that of the conventional interactive method.

1 Introduction

In the future of information society, computer network will be increased and the amount of information also will be incredibly large. This cryptography technologies will be effectively and broadly applied on all computing areas such as electronic commerce, banking transaction, and trade contact etc. In the future of our information ages, cryptographic protocols will become more important. The application areas of cryptographic protocols are digital-contract signature using concurrent transport protocol for document, an electronic election using multi-party protocols, an electronic cash, coin flipping, asset-comparing protocols, and an applied game protocols, etc.

In order to implement these cryptographic protocols on the distributed environments, it is important to keep the secure communication channels to authorized users, and needs to study an oblivious transfer method to exchange secret information fairly as a cryptographic protocol. This paper analyzes the basic concept of OT protocol to exchange secret information fairly and surveys basic idea of interactive and non-interactive OT protocol. In this paper, we study the oblivious transfer based on discrete logarithm problem proposed by Lein Harn etc. We consider the problems that they did not consider and extend their protocol to have the additional functions. We also presents a new non-interactive type of OT protocol to be verifiable. The traffic

amount of transferring information of the suggested method is less than that of the conventional interactive method.

2 Review of OT

2.1 Basic Concept of OT

In cryptographic protocol, it is very important thing to exchange secret information fairly to each other in many situations. Especially when both people make a signature of an trade contract on the documentation and one of them makes a signature earlier than another, any unexpected things could be happened. To solve this possible problem, there has been a research on fair exchange of secret information. Rabin [12] first introduced the basic idea of OT protocol. It is useful to be basic tool to generally design cryptographic protocol. On the general cryptographic protocol, OT protocol is very useful in case of transferring any information with assuring the secret of encryption.

The following protocol executes in between both people to exchange fairly the secret information. When Alice and Bob each have a m -bit length of secret information, Alice and Bob obviously transfer two secret information by 1-out-of-2 OT. Bob comes to know exactly one of two secret information of Alice. Alice doesn't know that Bob acknowledges any one of Alice's secret information. In the result, it is OT protocol that when Alice transfers a secret information to Bob, Bob can take the secret on the probability $1/2$ and Alice take a half probability of whether Bob takes the Alice's secret. Of course, If Bob takes the secret, Bob comes to know the secret content. OT could be extended on many applications. For an example, it could be considered that Alice transfer just one of the three secrets to Bob. Bob takes a third of probability on just one secret of them and Alice could suppose on a third of probability whether which secret Bob takes.

OT could be classified into three cases following as a general OT on one secret, 1-out-of-2 OT on two secrets and 1-out-of- n OT on n secrets. It is 1-out-of-2 OT that is specially noted. One of them is sent to receiver when a sender has two secret information, S_0 and S_1 . Sender couldn't know whether which secret information a receiver takes. OT is classified into interactive OT(IOT) and non-interactive OT(NIOT) according to a interactive or non-interactive communication. On IOT, it is called "interactive" that their communication is consisted of a few times of interaction between Alice and Bob. On NIOT, not to be interactive each other, there is just communication only from sender to receiver. In this method, the traffic amount of the communication between of them is very little. In real application of OT, overload of transfer by NIOT could be decrease. But since NIOT is dependent on the computational ability of sender and receiver, comparing to IOT, NIOT can be needed for a large computational time.

2.2 Related Work

The problem of the exchange of secrets was first addressed by Rabin[12] and Blum[3,4]. Blum's paper[4] was probably the best known at first. In that paper, the

secret is the factorization of some composite number instead of a single bit or a string of bits. Unfortunately, since the secret of the factorization of a composite number is indeed not a single bit and some linear relationship exists among the exchanged bits, it is shown by Hastad and Shamir[9] that this protocol is not so secure as was claimed. Later, Luby, Micali, and Rackoff[11] proposed a new protocol for the exchange of a single secret bit by flipping a symmetrically-biased coin. Tedrick[13] improved the fairness by exchanging even half a bit and reducing the computational advantage from 2-1 to 5-4[14]. Recently Cleve[6] proposed his controlled gradual disclosure scheme to guarantee that one's confidence of a secret is steadily increasing towards 1 instead of drifting towards 1 by following a random walk.

In general, if the release of a secret is based on the result of flipping two independently identical coins, there may be significant difference in each opponent's knowledge of the other's secret due to the nature of random walk. However, if only one coin, which is biased according to the secrets from two parties, is flipped and the results are observed by two parties, one can infer his/her opponent's secrecy by watching the reaction of his/her opponent. But one thing in common for all of the above schemes is that the security is based on the difficulty of factoring or QRA. The first protocol based on the difficulty of discrete logarithm was proposed by Brickle, Chaum, Damgard, and Graaf[5]. Although, with their protocol one can convince the others that his secrecy of discrete logarithm is within some interval without revealing anything, the exact release of his secret is time consuming unless this problem is transferred to another problem in which security again is based upon factorization.

2.3 VOT Proposed by Lein Harn[8]

Before any data can be transferred between Alice and Bob, they assume that a large prime p , where $p = 4 * p' + 1$, p' is also prime, and $p = 1 \pmod{4}$, and a primitive element, e , of $G(p)$, where $G(p)$ is Galois Field of p , are known to both. Alice chooses her own secret α with $\gcd(\alpha, p-1)=1$ and α is a quadratic non-residue of p , i.e., $\alpha \in \text{QNR}_p$, and submits $A_s = e^{\alpha s} \pmod{p}$ and $A_{1-s} = \alpha^{\alpha} \pmod{p}$, where $s \in \{0,1\}$ and is known only to Alice, to a trusted third party for notarization. From now on, the "secret" in the following protocol refers to α in the notarized value. The problem of whether α , instead of some α' , in this protocol is the real secret of Alice is the same as whether the factorization of N , instead of N' is the real secret of Bob in many other oblivious transfer protocols and this will not be discussed in this paper. After A_0 and A_1 are notarized, Bob start the oblivious transfer by following the steps below:

Step 1. Bob randomly chooses a secret number b with $\gcd(b, p-1) = 1$, and sends to Alice

$$C_1 = A_0^b \pmod{p} \quad \text{or} \quad C_1 = A_1^b \pmod{p}$$

Step 2. Alice computes and sends to Bob

$$C_2 = C_1^{\alpha^{-1}} \pmod{p}$$

Step 3. Bob computes

$$C_3 = C_2^{b^{-1}} \pmod{p}$$

If then $C_3 = e$, Bob knows nothing about Alice’s secret(i.e., Bob loses the game); otherwise Bob checks if

$$A_{s'} = e^{C_3} \pmod p \text{ for } s' = 0 \text{ or } s' = 1.$$

If so, Bob knows Alice’s secret $\alpha = C_3$ (i.e., Bob wins the game). Otherwise, Bob can charge Alice of cheating.

3 Proposed Protocol-I(IOT)

3.1 Extension of Verifiable Oblivious Transfer(VOT)

On the VOT, the conventional protocols have been reviewed on the fact of security, verifiability, and fairness. On the result of analysis, notarized information on sender authentication and refutation protection about the fact that one sent the message could be used to solve a traditional problems, using a digital signature of a public key cryptography system. Those new algorithms are suggested in this paper. We present to design and extend a new IOT.

3.2 Parameters

M_A : message from Alice to Bob

M_B : message from Bob to Alice

$\{p_A, q_A, d_A\}$: Alice’s private key

$\{n_A, e_A\}$: Alice’s public key

$\{p_B, q_B, d_B\}$: Bob’s private key

$\{n_B, e_B\}$: Bob’s public key

R_A : Alice’s digital signature to M_A (encrypted message using Alice’s private key to M_A)

R_B : Bob’s digital signature to M_B (encrypted message using Bob’s private key to M_B)

C_A : encrypted message using Bob’s public key to R_A

C_B : encrypted message using Alice’s public key to R_B

3.3 Proposal of Extended Protocol

Synopsis of Proposed Protocol

(Fig. 1) presents the oblivious transfer protocol using digital signature and notarized information

Alice \rightarrow

$As = e^\alpha \pmod p$	p	$\{n_A, e_A\}$
$A 1-s = \alpha^\alpha \pmod p$	e	$\{n_B, e_B\}$

$s \in \{0,1\}$

	(Alice)		(Bob)
	private key : $\{p_A, q_A, d_A\}$ message : M_A		private key : $\{p_B, q_B, d_B\}$ message : M_B
Step 1		(C_1, C_B, M_B) ←	Select random b, compute C_1 $(\gcd(b, p - 1) = 1)$ $C_1 = A_0^b \pmod p$ or $C_1 = A_1^b \pmod p$ Compute C_B $C_B \equiv (M_B^{d_B} \pmod{n_B})^{e_A} \pmod{n_A}$
Step 2	Decrypt C_B → compute R_B, M_B $M_B \equiv (C_B^{d_A} \pmod{n_A})^{e_B} \pmod{n_B}$ Verify M_B Store R_B Compute C_2 $C_2 = C_1^{a^{-1}} \pmod p$ Compute C_A $C_A \equiv (M_A^{d_A} \pmod{n_A})^{e_B} \pmod{n_B}$	(C_2, C_A, M_A) →	
Step 3			Decrypt C_A → Compute R_A, M_A $M_A \equiv (C_B^{d_B} \pmod{n_B})^{e_A} \pmod{n_A}$ Verify M_A Store R_A Compute C_3 $C_3 = C_2^{b^{-1}} \pmod p$ if $C_3 = e$ then Bob loses else if $C_3 = \alpha$ Bob wins else Bob can charge that A's cheating

Fig. 1. Proposed Protocol

3.4 Protocol Description

The following is the steps of proposed protocol

- When Alice wants to transfer obviously to Bob, digital signature is added to existing protocol.
- When Bob wants to transfer obviously to Alice, the role of each part is symmetrically exchanged.

Step 1

- Bob selects secret number, b, then computes C_1 as following statement.
 $C_1 = A_0^b \pmod p$ or $C_1 = A_1^b \pmod p$
- Bob computes C_B using his private key and Alice's public key.
 $C_B = (M_B^{d_B} \pmod{n_B})^{e_A} \pmod{n_A}$
- Bob transfers (C_1, C_B, M_B) to Alice

Step 2

- Alice computes R_B using her private key to C_B sent by Bob.

$$R_B \equiv C_B^{d_A} \pmod{n_A}$$
 Then Alice computes M_B using Bob's public key.

$$M_B \equiv R_B^{e_B} \pmod{n_B}$$
- Alice compares M_B sent by Bob and M_B computed by herself.
 If two M_B s are identical, stores R_B for protecting Bob's denial of sending. If not, stop the processing of protocol immediately.
- Alice computes C_2 using her secret α .

$$C_2 = C_1^{\alpha^{-1}}$$
- Alice computes C_A using her private key and Bob's public key.

$$C_A \equiv (M_A^{d_A} \pmod{n_A})^{e_B} \pmod{n_B}$$
- Alice transfer(C_2, C_A, M_A) to Bob.

Step 3

- Bob computes R_A using his private key from C_A

$$R_A \equiv C_A^{d_B} \pmod{n_B}$$
 Then Bob computes M_A using Alice's public key.

$$M_A \equiv R_A^{e_A} \pmod{n_A}$$
- Bob compares M_A sent by Alice and M_A decrypted by himself.
 If two M_A s are identical, stores R_A for protecting Alice's denial of sending. If not, stop the processing of protocol immediately.
- Bob computes C_3 , and finishes VOT. $C_3 = C_2^{b^{-1}} \pmod{p}$

3.5 Characteristics of Proposed Protocol

The proposed protocol follows Lein Harn's VOT protocol's properties, and add digital signature. So it has VOT's fairness, verifiability, and security. Two players can not deny the fact that she/he has sent message. But it has poor features about amount of traffic and computation. Table. 1 compares Lein Harn's protocol and proposed protocol.

Table 1. Comparison of Two Protocols

	Lein Harn's protocol	Proposed protocol
Possibility of message exposed	No(O)	No(O)
Possibility of cheating	Much(X)	Few(O)
Certifying of sending message	Impossible(X)	Possible(O)
Possibility of denial of sending	Yes(X)	No(O)
Possibility for settlement of the dispute	Few(X)	Much(O)
Amount of Traffic and computation	Few(O)	Much(X)

(O : good, X : poor)

4 Implementation of NIOT Protocol

4.1 Discrete Logarithm Problem and ElGamal Cryptography

We explain Discrete Logarithm Problem and ElGamal encryption. That is a non-interactive oblivious transfer protocol's mathematical basis in this paper.

Discrete Logarithm Problem is the problem that calculate x , the range $(0 \leq x < p-1)$ to be satisfied

$$y \equiv m^x \pmod p$$

given prime number P , m , $y(0 < m, y < p)$.

The calculation of y , given m , x , p , is calculation of power and able to calculate simply. But Discrete Logarithm calculation does not found executable algorithm by polynomial time and regards as severe problem.

Elgamal cryptography is the encryption algorithm using Discrete Logarithm Problems' difficulty, on prime number p .

Generation of Key

Step 1. Choose big prime number p (the decimal number of more than 100 bytes).

Step 2. Choose g , generation number of Z_n^* (seed number of divisor p).

Step 3. Choose x , one of elements $Z_{p-1} - \{0\}$, and calculate $y = g^x \pmod p$.

Step 4. Open to the public y , g , p as encryption keys, and posses x as secret.

Encryption

Step 1. Accept (y, g, p) encryption key of sending partner by accessing public file

Step 2. Generate random number $k(\in Z_{p-1} - \{0\})$ (update k during encryption time)

Step 3. Encrypt a plaintext $M \in Z_p^*$ following

$$\begin{aligned} c &= (c_1, c_2) \\ &= (g^k \pmod p, My^k \pmod p) \end{aligned}$$

Step 4. Send a ciphertext $c(c_1, c_2) \in Z_p^*$

Decryption

Step 1. Calculate as following using private key x about c received

$$d = c_1^x \pmod p$$

Step 2. Restore M from following expression

$$\begin{aligned} c_2 d^{-1} &= My^k (g^{kx})^{-1} \\ &= M (g^{xk})(g^{kx})^{-1} \\ &= M \pmod p \end{aligned}$$

4.2 NIOT Protocol

Bellare and Micali[1] proposed 1-out-of-2-NIOT using public bulletin. Synopsis of this protocol is as follows

Pre-processing Level

- Center registers prime number $p, g \in Z_p$ and $c \in Z_p$ to public bulletin.
- Bob select private random number x and names $(\beta_0, \beta_1) = (g^x, \frac{c}{g^x})$ or $(\beta_0, \beta_1) = (\frac{c}{g^x}, g^x)$ it, register β_0, β_1 to public bulletin.
- Alice calculates $\beta_0\beta_1 = c$ and confirms that public key of Bob is valid.

Protocol

- regard (p, g, β_0) and (p, g, β_1) as public key of ElGamal, and send S_0, S_1 to Bob
- Alice select arbitrarily.
 $y_0, y_1 \in \{0, 1, 2, \dots, p-2\}$, send $(g^{y_0}, S_0\beta_0^{y_0}), (g^{y_1}, S_1\beta_1^{y_1})$ to Bob
- Bob know discrete algebra about either β_0 or β_1 , therefore Bob can take only one of S_0, S_1 .

5 Proposed Protocol-II(NIOT)

Synopsis of Non-interactive oblivious transfer protocol(NIOT) proposed in this paper is as follows

5.1 Pre-processing Level

- Step 1.** Center registers prime number $p, g \in Z_p$ and $C \in Z_p$ in public directory
- Step 2.** Sender Alice opens discrete logarithms, g^{s_0}, g^{s_1} as secret information to transfer obliviously.
- Step 3.** Receiver Bob select secret random number γ and opens public key,

$$(\beta_0, \beta_1) = ((g^{s_0})^\gamma, c(g^{s_1})^{-\gamma})$$

$$\text{or } (c(g^{s_0})^{-\gamma}, (g^{s_1})^\gamma).$$

5.2 NIOT Protocol Description

Step 1. sender Alice $(p, g\beta_0)(p, g\beta_1)$ regards as public key of Elgamal and encrypt each secret information S_0, S_1 and sends to Bob. That is, sender Alice select $a_0, a_1 \in \{1, 2, \dots, p-2\}$ in random manner and send $(\alpha_1, \alpha_2), (\alpha_3, \alpha_4)$ to receiver Bob.

Here $\alpha_1 = g^{a_0}$, $\alpha_2 = S_0(\beta_0^{a_0})^{S_0^{-1}}$
 $\alpha_3 = g^{a_1}$, $\alpha_4 = S_1(\beta_1^{a_1})^{S_1^{-1}}$

Step 2. Since receiver Bob knows only one of discrete algebra of β_0, β_1 , he can have one of S_0, S_1

$$S_0 = \alpha_2 \alpha_1^{-\gamma} \quad \text{or} \quad S_1 = \alpha_4 \alpha_3^{-\gamma}$$

with decryption of Elgamal

$\begin{aligned} S_0 &= \alpha_2 \alpha_1^{-\gamma} \\ &= S_0(((g^{s_0})^\gamma)^{a_0})^{S_0^{-1}} (g^{a_0})^{-r} \\ &= S_0 g^{\gamma a_0} g^{-a_0 \gamma} \\ &= S_0 (\beta_0^{a_0})^{S_0^{-1}} (g^{a_0})^{-r} \end{aligned}$	$\begin{aligned} S_1 &= \alpha_4 \alpha_3^{-\gamma} \\ &= S_1(\beta_1^{a_1})^{S_1^{-1}} (g^{a_1})^{-r} \\ &= S_1 g^{\gamma a_1} g^{-a_1 \gamma} \\ &= S_1(((g^{s_1})^\gamma)^{a_1})^{S_1^{-1}} (g^{a_1})^{-r} \end{aligned}$
---	--

Step 3. receiver Bob can verify whether $(g^{S_0})^{S_1 C \alpha_1^\gamma \alpha_3^{-\gamma}} = g^{\alpha_2 \alpha_4}$ or $(g^{S_1})^{S_0 C \alpha_1^\gamma \alpha_3^{-\gamma}} = g^{\alpha_2 \alpha_4}$ with secret information received from Alice, that is, from ciphertext $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. And we know this from the following formula

$$\alpha_2 \alpha_4 = S_0 S_1 c (g^{a_0})^r (g^{a_1})^{-r} .$$

6 Conclusions

In this paper, we examined the basic concept of oblivious transfer protocol. And we investigate the interactive oblivious transfer protocol based on discrete logarithm problem proposed by Lein Harn etc. A VOT(Verifiable Oblivious Transfer) protocol is a powerful tool which has the three properties of fairness, verifiability, and security.

We also presented the verifiable interactive oblivious transfer protocol. We proposed a method to extend a VOT using public key cryptography system. We redefined an interactive VOT with RSA public key cryptography system. The structure of our method is similar to the original VOT by Lein Harn etc. The major difference is that our protocol is extended to protect one’s denying what he/she has sent to other in the process of protocol. This method has the additional functions that enable to authenticate sender and to protect denial of what he/she sent message.

This paper reviews the basic concept of non-interactive type of oblivious transfer protocol and presents newly a non-interactive OT protocol. We have proposed a verifiable non-interactive oblivious transfer protocol for the exchange of secrets. The structure of the protocol is similar to that of the original protocol proposed by Bellare and Micali. Their protocols are based on the difficulty of discrete logarithm. Our protocols are also based on the difficulty of discrete logarithm. The secret in their protocol could be chosen as a random number. The security in our protocols also can

be chosen as a random number. The traffic amount of transfer of the proposed method is less than that of the conventional interactive method. In the future, we need to study NIOT protocol with various additional functionality.

References

1. Bellare, M., and Micall, S., "Non-interactive oblivious transfer and applications", *Advances in Cryptology: CRYPTO '89*, (1989) 547-557.
2. Berger, R., Peralta, R., and Tedric, T., "A provably secure oblivious transfer protocol", *Advances in Cryptology : Proc. of EUROCRYPT '84*, (1984) 379-386.
3. Blum, M., "Three applications of oblivious transfer" : 1. Coin flipping by telephone, 2. How to exchange secrets, 3. How to send certified electronic mail, Dept., *EECS*, University of California, Berkeley, Calif. (1981)
4. Blum, M., "How to exchange (secret)keys", *ACM Transaction on Computer System*, Vol. 1, No. 2, (1983) 175-193.
5. Brickle, E., chaum, D., Damgard, I. and van de Graaf, J., "Gradual and verifiable release of a secret", *Advances in Cryptology : CRYPTO '87*, (1987) 156-166.
6. Cleve, R., "Controlled gradual disclosure schemes for random bits and their applications", *Avances in Cryptology : CRYPTO '89*, (1989) 578-588.
7. Harn, L., and Lin, H. Y., "Non-interactive oblivious transfer", *Electronics Letters*, Vol.26, No 10, (1990) 635-636.
8. Harn L. , and Lin H.Y., "An oblivious Transfer Potocol and its Application for the Exchange of Secrets", *ASIACRYPT '91*, (1991) 187-190.
9. Hastad, j., and Shamir, A., "The cryptographic security of truncated linearly related variables", *Proc. of 17th STOC*, (1985) 355-362.
10. Knuth, D., *The Art of Computer Programming*, Vol.2 Addison Wesley, Reading, MA. (1973)
11. Luby, M., Micali, S., and Rackoff, C., "How to simultaneously exchange a secret bit by flipping a symmetrically biased coin", *Proc, 22nd Ann. IEEE Symp. On Foundations of Computer Science*, (1983) 11-21.
12. Rabin, M., "How to exchange secret by oblivious transfer", Harvard Center for Research in Computer Technology, Cambridge, Mass. (1981)
13. Tedric, T., "How to exchange half a bit", *Advances in Cryptology : Proc. of CRYPTO '83*, (1983) 147-151.
14. Tedric, T., "Fair exchange of secrets", *Advances in Cryptology : Proc. of CRYPTO '84*, (1984) 434-438.

Analysis of Security Session Reusing in Distribution Server System

Tai-hoon Kim¹, Seoksoo Kim^{2,*}, Hee-Un Park³, and Myoung-sub Kim¹

¹ San-7, Geoyeo-dong, Songpa-Gu, Seoul, Korea
taihoonn@empal.com

² Dept.of Multimedia Engineering, Hannam University,
Daejeon, South Korea
sskim@hannam.ac.kr

³ Korea Information Security Agency, Seoul, Korea
hupark@kisa.or.kr

Abstract. Web server system researcher's interest in the high performance cluster web server is connected with low cost workstation or PCs by high speed network. For the latest researches, techniques using an advantage of content-aware request distribution are proposed. And network security is very important. Many information exist which demand information security because development electronic commerce. We have the worry about low speed when which a security session is applied in content-aware traffic distribution server system. In this paper, we studied about content-aware traffic distribution server system which a security session reusing is applied.

1 Introduction

The Internet is making rapid progress. Due to the explosive growth of Internet users exceeding the increase of network bandwidth, service requests to Web servers are also growing at a high rate. In response to the rapidly increasing demands for Web services, many researches are being conducted on high-capacity and high-performance Web servers guaranteeing prompt responses and reliable file transmission. If a single server has to process many service requests, its performance cannot be improved significantly. Thus, researchers are studying a technology called Web server clustering that clusters a number of computers and distributes load among them. In its early stage, the Web server clustering technology applied an algorithm distributing load in consideration of load balance but gradually it moved to a load distribution algorithm according to contents [1],[2]. With the development of e-commerce, moreover, data security is being emphasized more than ever. Numerous data are demanding security in the current Web environment. For example, personal information, approval information, file exchange, etc. require security in several aspects and the security of these types of data involves the transmission of encrypted data, authentication process and data checking process, which cause transmission delay [4].

* Corresponding author. "This work was supported by a grant No. (R12-2003-004-03003-0) from Ministry of Commerce, Industry and Energy".

For the improvement of transmission rate, we can reuse security sessions. Thus, the present study implemented Web server cluster environment adopting a load distribution algorithm based on contents, which transmits encrypted data, and examined the relation between content-based load distribution and the reuse of security sessions.

For evaluating the performance of the system, Chapter 2 in this dissertation analyzed Web cluster system, Chapter 3 designed and implemented a content-based load distribution system adopting the reuse of security sessions, and Chapter 4 analyzed the relation between contents and the security session reuse through performance evaluation.

2 Web Cluster System

2.1 Web Cluster System

Clustering technology makes a number of servers to process high-capacity services together. A cluster is composed of nodes and a manager. A cluster node processes actual tasks assigned to the cluster. In general, cluster nodes are set up to belong to a cluster. Depending on the role and job of a cluster, software can be specific or general. An example of software performing a specific role is an engineering calculation program mapped to a node, and programs for load balancing like Apache for belong to general software. Like Linux kernel manages the schedule and resources of all processors, the cluster manager manages resources and allocate them to each node. Basically one manager is necessary but sometimes cluster nodes can play the role of cluster manager and, in a large-scale cluster, there can be multiple cluster managers. There are clustering techniques such as HPC, fail-over and load balancing. First, HPC is generally called Linux clustering or Beowulf project.

Beowulf provides a system of high processing capacity by combining the processing capacities of several sub-systems. In the system, which was designed for scientific uses or CPU jobs, only programs made according to API can allocate their jobs to multiple systems [5],[6]. Fail-over is similar to load balancing but there is a slight difference. While all nodes work together in load balancing, backup servers work only when the primary server fails in fail-over. Modifying load balancing we can implement load balancing and fail-over functions at the same time. Lastly, load balancing is an essential technology for building large-scale websites. This technology puts multiple Web server nodes around and distributes load using the management tool at the center. A characteristic of this technology is that the nodes do not have to communicate with one another. Using load balancing, each node can process requests fittingly to its capacity or load. Or it can process tasks assigned by the cluster manager and this is the content-based load distribution server system proposed in this research [7],[8].

2.2 Web Cluster System Scheduling Algorithm

Such a load distribution clustering system uses a scheduling algorithm for load distribution. There are several scheduling algorithms as follows.

-Round-robin scheduling (RR). This algorithm simply delivers requests, ignoring all situations including the server and network conditions. This is the simplest and can be efficient if all servers and networks are of the same specification.

-Weighted round-robin scheduling (WRR). Here, a weight means giving a weight to a specific thing. A weight is given to a specific server so that it processes more requests if the server is superior to others in capacity or can process more requests because of its environment, processing speed for a given type of requests, etc. Using weighted round-robin scheduling, the server does not need to count the number of network connections and can manage a larger number of servers because scheduling overload is less than that in dynamic scheduling algorithm. If the number of requests is large, however, there can be dynamic load imbalance among real servers.

-Least connection scheduling (LC). In least connection scheduling, a new request is directly connected to the server with the least connections. Because this algorithm has to count dynamically the number of actual connections to each server, it is one of dynamic scheduling algorithms. In a virtual server composed of servers with similar performance, big requests do not concentrated on a specific server and, as a result, even a high connection load is distributed very effectively. The fastest server can process more network connections. Therefore, even if the servers in a virtual server vary in processing capacity, they may work very efficiently. In fact, however, the algorithm cannot produce very satisfactory performance because of the TIME_WAIT of TCP. TCP TIME_WAIT is usually two minutes but a website with a large number of connectors may have to process thousands of connections within the two minutes. If Server A has a twice higher processing capacity than Server B, it will face TCP TIME_WAIT after processing thousands of requests. However, Server B just waits until thousands of requests are all processed. For this reason, least connection scheduling can be inefficient in load distribution if the virtual server is composed of servers with different processing capacities.

-Weighted least connection scheduling (WLC). Weighted least connection scheduling, which is a part of least connection scheduling, can give a performance weight to each real server. A server with a high weight can receive more requests. The virtual server manager can give a weight to each real server. Network connects are allotted based on the number of actual connectors, which is the weight ratio. The base weight is 1. The performance of a cluster system is determined by the scheduling algorithm. Thus, a suitable algorithm should be selected for a system to be built [3],[4],[8].

3 Reuse of Security Session in Content-Based Load Distribution Server

3.1 Content-Based Load Distribution Server

With the spread of e-commerce, the Internet is being used in more diverse ways and demands Web service systems of higher performance. In response to such a demand, cluster Web servers are used. Early cluster Web servers distributed load evenly over the sub-systems but they evolved to systems distributing load differently according to contents. A content-based load distribution system analyzes the contents of service

requested by clients and distributes load based on the result. In this method, a server measures the volume that it can process for a specific type of contents and processes it by weight. That is, requests for a specific target are allocated to a specific Web server using the name of the name of the target.

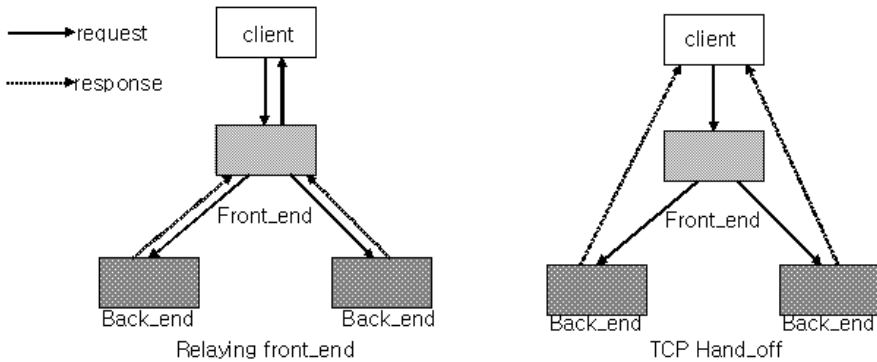


Fig. 1. Mechanism

Because content-based load distribution always distributes requests with the same target name to the same server, the hitting ratio of the main memory cache is improved and the Web server can respond more quickly. In other words, requests are always sent to the server that already has data cached in the main memory. Requests for a specific target are sent to the same server and, by doing so, the hitting ratio is improved and redundancy is reduced. This is the most important characteristic of content-based load distribution. The simplest mechanism for content-based load distribution is the use of a relaying front-end. A HTTP proxy runs at the front-end accommodating clients' connections maintains permanent connections to all back-end nodes. If a request arrives from a user, the proxy allocates a connection to the client according to the load distribution method and forwards the request packet. If a reply comes from the back-end node, the front-end proxy sends it to the client. This method does not need to make a change in the OS kernel of any server in the cluster system and can structure the system simply, but because all response packets from the back-ends to clients are forwarded through the proxy, there is heavy overhead [3]. To avoid bottleneck at the front end caused by overhead, mechanisms such as TCP splicing and TCP hand-off are used. As in Figure 1, TCP splicing shows the same traffic flow as that with the use of a relaying front-end. Different from the use of a relaying front-end, TCP hand-off transmits response from back-end nodes directly to the clients. Due to difference in traffic flow, TCP splicing shows higher scalability than TCP hand-off [9],[10],[11]. Despite the use of TCP hand-off mechanism, the structure of content-based load distribution server using a centralized front-end has a limitation in scalability. In "Scalable Content-aware Request Distribution in Cluster-based Network Servers" [3], the author proved that when the number of back-end nodes is four or more, system performance did not go up any longer due to bottleneck in the load distributor.

3.2 Design of Security Session Reuse in Content-Based Load Distribution Server

Data security is getting more critical. There are innumerable data demanding security in the current Web environment. For example, personal information, approval information, file exchange, etc. requires security in several aspects, and the security of these types of data involves the transmission of encrypted data, authentication process and data checking process, which cause transmission delay. TLS (Transport Layer Security: former SSL (Secure Socket Layer) of Netscape)), which is the service standard providing security sessions, does not guarantee high-speed transmission. In order to create a security session, security keys should be set between the two communication objects. For this, a handshake protocol exists separately and the pre-master secret key used in the protocol is decoded and the master secret key is generated by the server. These processes require a large volume of calculation and lower the transmission performance of the system. For higher transmission rate, accordingly, sessions need to be reused rather than created for each connection. However, not all networks benefit from high session reusability. Figure 2 shows a timing diagram for the handshake protocol.

In cluster environment, excessive session reuse may disrupt load balance, apply too heavy load to a specific server and, in an extreme case, congest the network with traffic. Thus, we need a handshake algorithm that minimizes the slowdown of trans-

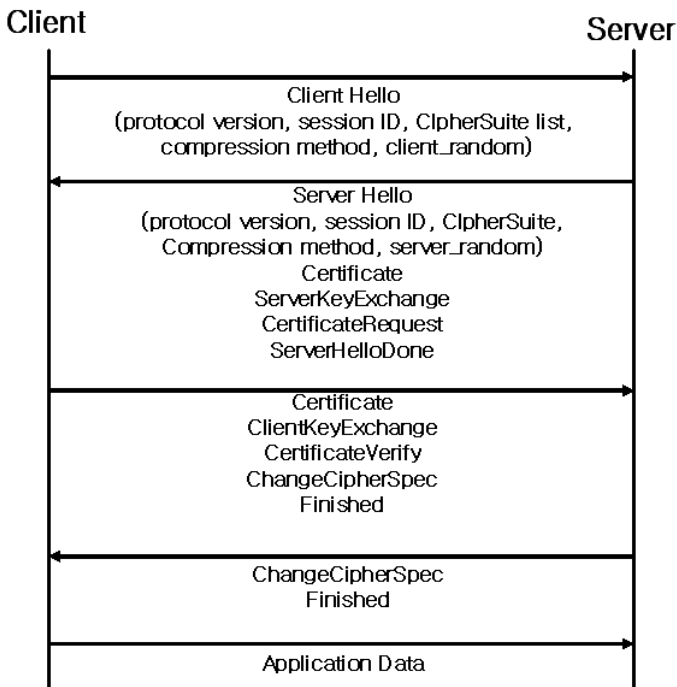


Fig. 2. Handshake timing diagram

mission throughout the entire network by tuning between load balance and security session reuse. Figure 3 shows a simple handshake algorithm for the reuse of security sessions.

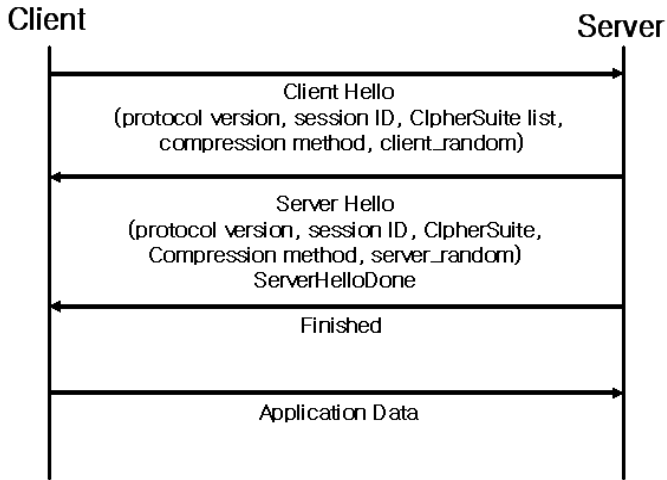


Fig. 3. Simple handshake timing diagram

In this research, in order to evaluate the reusability of security sessions in implementing a content-based load distribution server, we adopted relaying front-end as the mechanism of content-based load distribution and used weighted round robin (WRR) algorithm by giving a weight for content-based load distribution. For applying security sessions, we generated data using DES encryption algorithm at EDCE (Encryption Data Create Equipment) and transmitted the data to DPS (Date Process Server) using the simple handshake algorithm and WRR algorithm at VS (Virtual server) in order to reuse security sessions. This system can be represented in a structure diagram as in Figure 4.

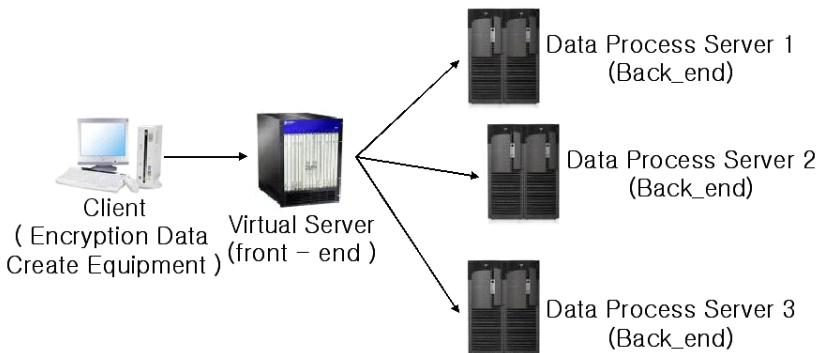


Fig. 4. System structure diagram

4 Performance Evaluation

To evaluate the performance of the implemented algorithm we used Pentium III computers. The Web cluster was built in the NAT method. Data transmission was made to VS using EDCE and from VS to DPS using a switching hub. In order to analyze the data flow, we captured packets using Libpcap on Linux, and represented them in GUI graph using GTK to monitor the packets on xwindow. The graphs in Figure 5 show packet data captured according to the number of experiments and graphs in Figure 6 are data represented in graph. The followings are the result of performance evaluation with changing the values of reuse and weight using the algorithms above. In Figure 5, the clients were given weights 13, 7 and 3 respectively and tested 6 times in 10 minutes, and Figure 6 is the result of applying security session reuse ratios of 0, 10, 20 and 30.

Weighted : client1 = 13
 client2 = 7
 client3 = 3

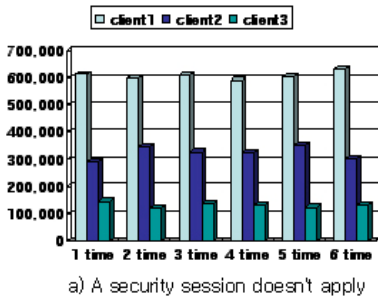


Fig. 5. Performance evaluation 1

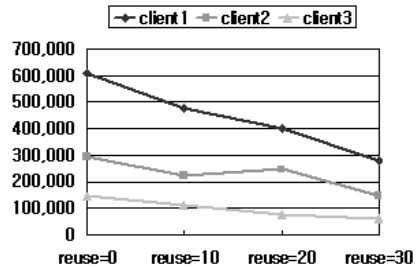


Fig. 6. Performance evaluation 2

In the graphs above, security session reuse ratio was obtained by quantifying the volume of data, to which security sessions were applied. Every time, encrypted data was decrypted in VS, DPS is confirmed, and the data is sent to the DPS. The process is repeated but, with the introduction of reusability, data is decrypted at regular intervals of time or number and transmitted to the corresponding DPS. According to the result of the performance evaluation, the performance of security session reuse went down when weights were small, and it went up when weights were large. Based on the results, security session reuse in an actual content-based load distribution server must reuse sessions in consideration of the service, to which the reuse is applied and appropriate distribution. If traffics allocated to servers are different according to content a low reuse ratio will be desirable, and if they are similar a high reuse ratio will be desirable. However, this result came from data in an artificially crated setting and it may be somewhat different in real environment.

5 Conclusions

The present study evaluated the performance of security session reuse in a content-based load distribution server. Cluster Web servers, which have a highly expendable structure in response to gradually increasing Web server traffic, have been studied, focused on their scalability, client transparency and high availability. Recently, researchers on cluster Web servers are paying attention to content-based load distribution that distributes clients' requests among the cluster server nodes according to the type of content or service requested. Due to the characteristic of Web workload, accesses are frequently concentrated on a specific file not the whole files in the site. Using the characteristic, researches on content-based load distribution seek to improve the overall performance of a cluster system through the efficient use of the memory in cluster server nodes. If security session is applied to a content-based load distribution system, traffic may increase significantly. In order to reduce traffic resulting from security sessions, security sessions should be reused and the reuse should be adjusted appropriately according to content. The present study evaluated the performance of security session reuse simply by reducing the handshake algorithm. However, the reusability of security sessions needs to be studied not only for content-based load distribution algorithm but also for cache algorithm applied to Web pages.

References

1. E. Levy-Abegnoli, A. Iyengar, J. Song, and D. Dias, "Design and Performance of a Web Server Accelerator," IEEE INFOCOM'99, pp.135-143,1999.
2. V. S. Pai, M. Aron, G. Banga, M. Svendsen, P. Druschel, W. Zwaenepoel, and E. Nahum, Locality -Aware Request Distribution in Cluster - based Network Server s, In Proceedings of the 8th Conference on Architectural Support for Programming Languages and Operating System, San Jose, CA, Oct . 1998.
3. M.Aron, D.Sanders, and P.Druschel, Scalable Content-Aware Distribution in Cluster-based Network Servers. Proceedings of the 2000 USEMIX Technical Conference, 2000.
4. V. Pai, M.Aron, G.Banga, M.Svendsen, P.Druschel, W.Zwaenepoel, and E. Nahum Locality Aware Request Distribution in Cluster-based Network Servers. Architectural Support for Programming Languages and Operating systems pp1-12, 1998.
5. W. Zhang, "Linux Virtual Server for Scalable Network Services," Linux virtual server project,1998.
6. W. Zhang and et al., Linux virtual server project,,1998.
7. V.Kumar, A.Grama, and V.N.Rao, Scalable Load Balancing Techniques for Parallel Computers, Journal of Distributed Computing, pp.60-79, 1994.
8. T. Schroeder, S.Goddard, and B. Ramamurthy, "Scalable Web Server Clustering Technologies." IEEE Network, pp.38-45, 2000.
9. D.A. Maltz. and P. Bhagwat, TCP Splicing for Application Layer Proxy Performance, Jurnal of High Speed Networks, pp.225-240, 1999.
10. A. Cohen, S.Rangarajan, and H. Slye, On the Performance of TCP Splicing for URL aware Redirection, Proceedings of the 2nd USENIX symposium on Internet technologies and Systems, 1999

Clustered OFDMA in the Multi-path Fading Channel

Kyujin Lee and Kyesan Lee

Kyunghee Univ., Seochundong, Kihunggu, Youngin-si,
Gyunggi-do, 449-701, Korea
kyujin@khu.ac.kr, kyesan@khu.ac.kr

Abstract. In this paper, we proposed a new modulation and multiplexing technique named Adaptive Spreading Orthogonal Frequency Division Multiple Access (AS-OFDMA). AS-OFDMA might be an efficient system which is more robust against multi-path fading channel. Therefore, the performance of the proposed system is better than the conventional MC-CDMA. Moreover, AS-OFDMA solves the problem of inter code interference. In this paper, we introduce the proposed system and demonstrate the superiority of the proposed system by the computer simulation. We also show the performance comparison between the proposed system and the conventional MC-CDMA technique.

1 Introduction

As the communication technology is developed, the future mobile communication systems are required to be sufficiently flexibility to support a variety of multimedia services such as video, image, picture and data services with high quality.[1] To increase the data rate, we need a more wideband communication technology. However, in the mobile communications, it causes the degradation of performance in the frequency selective fading channel.

A multi-carrier scheme providing high data rate transmission with high frequency utilization efficiency has been proposed for DS/CDMA system based on orthogonal frequency division multiplexing(OFDM), which is a parallel data transmission technique. It is crucial for multi-carrier transmission to have a non-frequency selective fading channel over each sub-carrier.[2],[3],[4] A MC-CDMA is the combination system between OFDM and CDMA, which achieves frequency diversity gain in frequency selective fading channel avoiding inter symbol interference(ISI). Therefore, this is a very effective system. Each carrier in MC-CDMA experiences different fading in the frequency selective fading channel. the frequency diversity gain by de-spreading process can be achieved. Users use same sub-carriers because multiple access technique can be performed by using orthogonal code. Consequently, it makes better frequency efficiency.[5][6][7]

However, in the conventional MC-CDMA, every user uses all the carriers at the same time. As users are increased in the cell, the inter-cell interferences rapidly increased results in degradation of the performance. [8]

To overcome problem of the conventional MC-CDMA system, we proposed the Adaptive Spreading OFDMA.

Adaptive Spreading OFDMA is different to the conventional MC-CDMA. As we mentioned before, all the users transmit data using whole sub-carriers in the conventional MC-CDMA. But the whole sub-carriers are divided by multiple Block unit and it becomes a sub-carrier block set. Adaptive Spreading OFDMA system is spreading by Spreading Factor(SF) for each sub-carrier block set. Therefore, Adaptive Spreading OFDMA gets the frequency diversity gain in frequency selective fading channel avoiding ISI.

The capability of Adaptive Spreading OFDMA is greater than the conventional MC-CDMA, because the whole sub-carriers are splitted into many sub-carreir sets.

As the users are allocated by a block unit, the intra cell interferences are reduced for a block band but not all in band. The proposed system is more effective for Intra cell interference.

2 Channel Model

The principle of multicarrier modulation involves reducing the bit rate of each carrier against the ISI problem and providing high bit rate transmission using a number of those low bit rate carriers. Frequency bandwidth is divided into small ranges and each range is handled by these low rate carrier. Furthermore, an OFDM system transmits different data using several sub-carrier which provide high-rate data transmission and impact on the capacity. Because of the orthogonal overlapping of carriers, an OFDM system can increase bandwidth efficiency. The total bit rate R becomes higher than that of a single carrier R_1 and their relation is given by.[9]

$$R = \frac{2S}{(S + 1)} \times R_1 \quad (1)$$

where S is the number of carriers.

Multicarrier modulation applied to DS-CDMA may be classified into two general cases, depending upon whether time domain or frequency domain is employed. The former is generally called MC-DS/CDMA and the latter is generally called MC-CDMA. The proposed system in this paper belongs to the frequency spreading class. The MC-CDMA and Adaptive Spreading OFDMA system spread the original data in a frequency domain using spreading code. Therefore, MC-CDMA and Adaptive Spreading OFDMA can obtain a frequency diversity effect through despreading since the fading of each subcarrier is different.

Received radio signal is a superposition of delayed and attenuated versions of transmitted signal due to multi-paths. Rayleigh fading model is often a good approximation of realistic channel conditions. The channel model depicted in Fig. 1 is assumed in the paper.

In this model, an 18-path frequency selective Rayleigh fading channel has the exponential decay of the average received power levels with equal interval of $5T_c$ between adjacent paths.

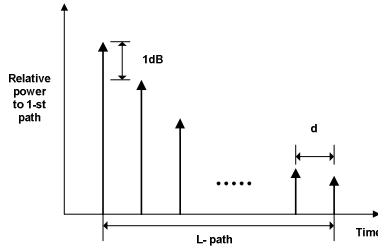


Fig. 1. Exponential Decay Channel Model

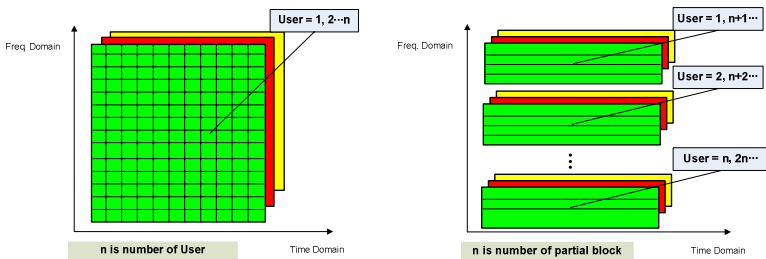
Therefore, the channel model is expressed as[10]

$$\begin{aligned}
 h(t; \tau) &= \sum_{l=0}^{L-1} \xi_l(t) \delta(\tau - \tau_l) \\
 &= \sum_{l=0}^{L-1} \xi_l(t) \delta(\tau - (\tau_0 + ld))
 \end{aligned}
 \tag{2}$$

Where $\xi_l(t)$ is the complex channel gain of the \$l\$-th path and τ_l is the propagation delay of \$l\$-th path.

3 Adaptive Spreading OFDMA System

The conventional MC-CDMA system is illustrated in Fig. 2(a). The MC-CDMA transmitter spreads the original signal using a spreading code over a frequency domain Adaptive Spreading OFDMA as shown in Fig.2 (b) is different to the conventional



(a) Conventional MC-CDMA

(b) AS-OFDMA

Fig. 2. Configuration of MC-CDMA and Adaptive Spreading OFDMA

MC-CDMA. The Adaptive Spreading OFDMA transmit the data using partial band (partial carriers) for user, while all the users transmit data using whole sub-carriers in the conventional MC-CDMA. Adaptive Spreading OFDMA system is spreading by Spreading Factor(SF) for each sub-carrier block set. Therefore, Adaptive Spreading OFDMA achieves the frequency diversity gain avoiding ISI in frequency selective fading channel.

Each data stream is serial-to-parallel(1:M) converted to parallel data ($T = T_b \times M$).

This converted data streams are modulated to each sub-carrier. And the information data are spread in the frequency domain with walsh code that is set of $\{+1, -1\}$. Walsh-code is very suitable for Adaptive Spreading OFDMA system because its cross-correlation value is zero.

MC-CDMA systems have a frequency diversity gain because the data stream is spread over frequency domain. Users share the bandwidth using assigned codes, so many user can use same frequency band with frequency efficiency. However, in the conventional MC-CDMA, as the users increase in the cell, because all the users use the whole carriers, the quantity of intra-cell interferences rapidly increases results in degradation of performance. And the capability of multiple access depends on length of orthogonal code. The maximum user number that can share the band at the same time is $N_u = L_{sf}$, so the capability of multiple access is limited. As the user number increases, the code length is increased. It makes performance degradation because inter-code interference is increased.

The system structure of the adaptive spreading OFDMA transmitter and receiver are shown in Fig.3.

First, each user is assigned to sub-carrier L_{sf} after serial-to-parallel converter. Data streams of assigned user are copied to sub-carriers, and this signals are spread in the frequency domain using walsh code. Copied signal is converted to time domain signal through IFFT. After that, insert Guard interval(GI) to reduce ISI impact and transmit their signals on the wireless channel.

Received signals of adaptive spreading OFDMA system are converted to baseband signals and the guard interval is removed. These signals are converted to sub-carrier components using fast Fourier transform(FFT). The spreading code is multiplied to every sub-carriers in a frequency domain. After the compensation of the fading channel, signals are converted by parallel to serial converter. Finally, converted data is demodulated and detected.

Differently with the conventional MC-CDMA, the proposed system uses a block unit of sub-carriers. In MC-CDMA, data stream is converted to parallel data, but proposed system assigns user to each sub-carrier block. So it achieves a good performance by reducing inter-code interference.

In the case that u users exist in the system, each user in the MC-CDMA system experiences interference from all user but user in the proposed system less interference than MC-CDMA system.

Quantity of reduced interference is $(u * L_{sf}) / \text{carrier}$ (L_{sf} is a length of spread factor). Furthermore, spread code can be reused by a block unit, a maximum user of multiple access is $N_u = L_{sf} * N_b$. So, without increasing spread code, many users share the band

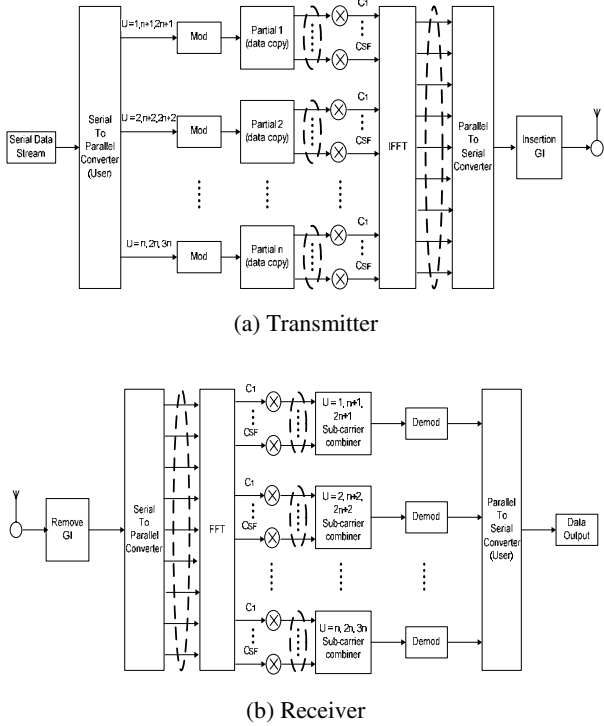


Fig. 3. AS-OFDMA scheme

at the same time. And the proposed system also spread in the frequency domain, we can get the frequency diversity gain.

Packet structure of the proposed system is fig. 4. First 4 symbols are pilot symbol for channel estimation and after pilot symbol, 64 data symbols are located.

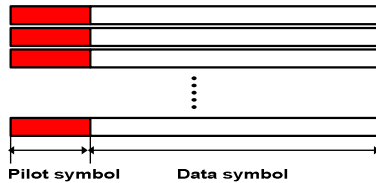


Fig. 4. Packet structure

The number of carrier that transmits same data is L_{sf} (length of spread factor) and the number of user that can access at the same time is also L_{sf} .

$S(t)$ corresponding to the i -th data symbol of the u -th user is follows Then, the transmitted signal become

$$S(t) = \sum_{u=0}^N \sum_{i=0}^{I-1} \sum_{k=0}^{K-1} d_{\beta(u,B)}^u(i) C^{\phi(u,B)}(k) P(t - iT_s) \times e^{j2\pi(K\beta(u,B)+k)\Delta f_{sym}(t-iT_{sym})} \tag{3}$$

where K represents spreading factor, i is data sequence. and u is user index. $\beta(u, B)$ is Block selection function, $\phi(u, B)$ is code reuse function.

$$\beta(u, B) = (u \% B) \quad \text{and} \quad \phi(u, B) = \left\lfloor \frac{u}{B} \right\rfloor \tag{4}$$

B is total number of block. $P(t)$ that represents the pluse shapping function. is written as

$$P(t) = \begin{cases} 1 & -T_g < t < T_g \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

T_{sym} is the OFDM symbol duration with guard time T_g .

If the sample duration is T_s then

$$T_g + T_{sym} = KT_s \quad \text{and} \quad \Delta f_{sym} = \frac{1}{T_{sym} - T_g} \tag{6}$$

is the sub-carrier separation.

At the receiver, received signal is

$$\begin{aligned} r(t) &= \sum_{u=0}^N \int_{-\infty}^{+\infty} S^u(t - \tau) h(\tau; t) d\tau + n(t) \\ &= \sum_{u=0}^N \sum_{i=0}^{I-1} \sum_{k=0}^{K-1} Z_{u,i,k}(t) d_{\beta(u,B)}(i) C^{\phi(u,B)}(k) \\ &\quad \times P(t - iT_{sym}) e^{j2\pi(K\beta(u,B)+k)\Delta f_{sym}(t-iT_{sym})} + n(t) \end{aligned} \tag{7}$$

Where $Z_{u,i,k}(t)$ is the received complex envelope at the $(K_{\beta(u,B)} + k)$ -th sub-carrier of the u -th user.

4 Results

4.1 Simulation Condition

The BER performance is evaluated by computer simulation. Table 1 summarizes the simulation parameters assumed in the paper, and Fig. 2 and Fig. 3 show the structure of MC-CDMA and AS-OFDMA, respectively.

Table 1. Simulation parameters

Number of sub-carriers	128
Short spreading code	Walsh-Hadamard code
Scramble spreading code	Pseudo random sequence
Data modulation	QPSK
Number of data symbol	64
Number of pilot symbol	4
FFT/IFFT length	128
Guard interval	32
Processing gain	16, 32
Channel model	See Section 2.1
Maximum Doppler frequency	5Hz, 25Hz, 50Hz, 100Hz

Fig. 4 shows the packet structure of MC-CDMA and AS-OFDMA. The performance of the propose system was demodulated by computer simulation in a frequency selective Rayleigh fading channel. In particular, a 18-path fading channel model was used in the frequency selective fading channel, as mentioned in Section 2.1 Ideal channel estimation is assumed in this paper. More detailed parameters used in the simulation are shown in Table 1.

4.2 Simulation Results

Fig.5(a) and Fig.5(b) show performance comparison between AS-OFDMA and the conventional MC-CDMA according to maximum doppler shift under the condition of the same process gain and the same user. But here, the capacity is not considered. We can see that AS-OFDMA has better performance than conventional MC-CDMA. From 5(a) and Fig.5(b), we can see that the performance is getting better as the process gain is increasing by the frequency diversity effect.

Fig.6(a) shows BER comparison between AS-OFDMA and conventional MC-CDMA according to maximum doppler shift under the condition of the same process gain and the same system capacity.

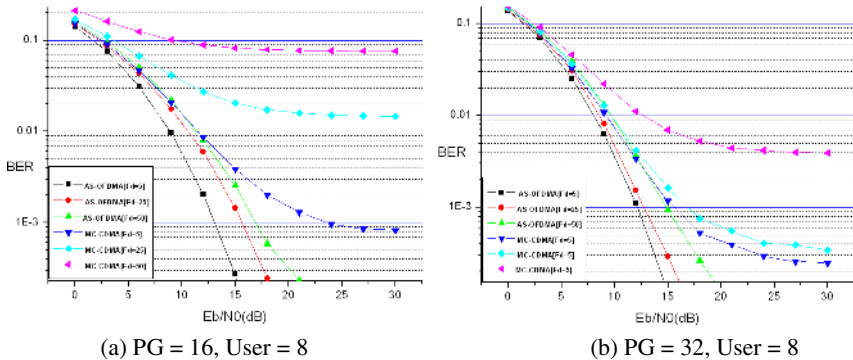


Fig. 5. BER performance comparison between the conventional MC-CDMA and AS-OFDMA

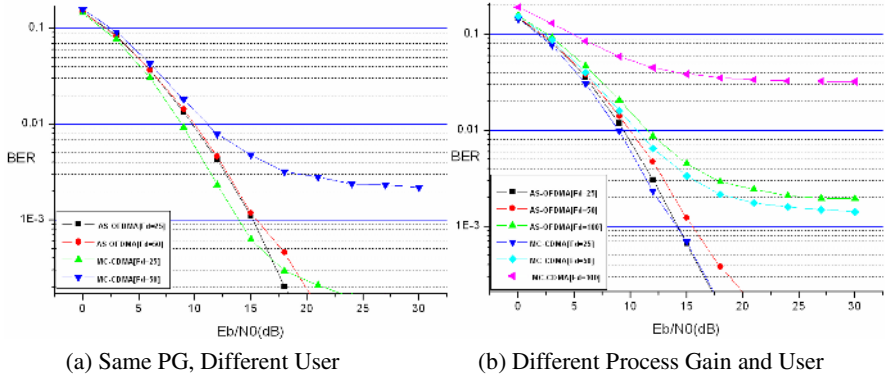


Fig. 6. BER performance comparison between the conventional MC-CDMA and AS-OFDMA. (Same capacity).

Conventional MC-CDMA has 32 process gain, 4 users and AS-OFDMA has 32 process gain, 16 users.

When F_d is 25, from 0dB to 17dB, the performance of conventional MC-CDMA is better than AS-OFDMA. When we compare $F_d=50$ and $F_d=25$, there is no change in AS-OFDMA but there is great performance difference in conventional MC-CDMA.

In Fig.6(b), we compare the BER between AS-OFDMA and the conventional MC-CDMA according to maximum doppler shift under the condition of the different system capacity and the different process gain. The conventional MC-CDMA has 32 process gain, 4 users and AS-OFDMA has 16 process gain, 16 users. There is not much performance gap between two systems. However, the BER performance is rapidly degraded when the doppler shift is 50 and 100. Furthermore, as the E_b/N_0 is getting more increasing the gap is more large.

In 5(a) and Fig.5(b), two systems get frequency diversity gain by using many subcarrier with same data. Because of that, we can see that the process gain is increasing when the performance is getting better. From Fig.5 and Fig.6, We can see that the BER performance of AS-OFDMA is less influenced by the maximum doppler shift than the conventional MC-CDMA.

5 Conclusion

In this paper, Adaptive Spreading OFDMA(AS-OFDMA) system is proposed to achieve the frequency diversity gain avoiding intra cell interference. We compared the BER performance of AS-OFDMA to the conventional MC-CDMA under the Rayleigh fading channel. Performance of these systems is getting better as the process gain is increasing because both of them get the frequency diversity gain. When the maximum doppler shift is small, they have similar performance. However, the maximum doppler shift is high, the performance degradation of the conventional MC-CDMA is rapidly increasing due to the intra cell interference. However, the proposed system is effective for reduction the intra cell interferences. AS-OFDMA has good performance in even the large doppler shift channel condition. It was verified by the

simulation results that the proposed schemes are effective and practical in multi-path Rayleigh fading. The proposed system can achieve the high quality services in the broadband wireless communication channel.

References

1. Richard D. Carsello et.al. : IMT-2000 standard : Radio Aspects. IEEE Personal Communications, pp.30~40, August 1997.
2. S. B. Weinstein and P. M. Ebert. : Data Transmission by Frequency-Division Multiplexing Using the Discrete Fourier Transform. IEEE Trans. Commun. Techn., vol.COM-19,pp.628-634,Oct.1971.
3. J.A.C. Bingham. : Multicarrier Modulation for Data Transmission: An idea whose time has come. IEEE Comm. Mag, pp.5-4, May 1990.
4. R. van Nee and R. Prasad. : OFDM for Wireless Multimedia Communications. Artech House, 2000.
5. Shinsuke Hara, Ranjee Prasad. : Overview of Multicarrier CDMA. IEEE commun. Magazine, pp.126~133, December 1997.
6. S. Hara and Prasad. : Design and performance of multicarrier CDMA system in frequency-selective Rayleigh fading channels. IEEE Trans. On Vehicular Technology, vol.48, no.4, pp.1584~1595, Sept. 1999
7. Michael Schell and Sten Kaiser. : Diversity Considerations for MC-CDMA System in Mobile Communications. Proc. ISSSTA '96, pp.131~135, 1996.
8. Shinsuke Hara and Ranjee Prasad. : Multicarrier Techniques for 4G Mobile Communication. Artech House.
9. E.A sourour and M. Nakagawa. : Performance of orthogonal Multicarrier CDMA in a multipath fading channels. IEEE Trans. Commun., vol.44, no3 pp.356~367, March 1996.
10. M. K. Simon and M. S Alouini. : Digital Communication over Fading Channels, A unified approach to performance Analysis. Jone Wiley & sons, inc., 2002.

Distribution Antenna Diversity System According to Adaptive Correlation Method for OFDM-DS/CDMA in a Frequency Selective Fading Channel

Kyesan Lee and Eunam Huh

Kyunghee Univ., Seochunri, Kihung-eup, Yongin-si, Gyunggi-do, 449-701, Korea
kyesan@khu.ac.kr, johnhuh@khu.ac.kr

Abstract. In this paper, an effective distribution antenna diversity system according to adaptive correlation method for OFDM-DS/CDMA is proposed in the frequency selective fading channel. The combined diversity effect between path diversity of the distributed antennas and frequency diversity of the multi-carrier can be achieved with the proposed system. The proposed system transmits different data using several sub-carriers which are correlated, while, transmitting the same data using several sub-carriers which are de-correlated. It can achieve combined path and frequency diversity gain in a frequency selective fading channel. It provides high data rate services by transmitting the different data using each correlated carrier, and supports good quality by transmitting the same data system with frequency diversity gain is applicable to multimedia service. Thus, the proposed system is sufficiently flexible enough to very support a variety of video, image, voice and data services at a high level of quality.

Keywords: OFDM-DS/CDMA, RAKE diversity, distributed antenna, ISI.

1 Introduction

Recently, mobile communication systems must be flexible enough to support a variety of video, image, picture and data services with high quality [1-3]. As one of the future high wireless communication technologies, The Direct Sequence/Code Division Multiple Access (DS/CDMA) system has been regarded as one of those candidates. It has many desirable features such as fading suppression, immunity against interference, and enhancement of frequency reuse efficiency [3-4].

A DS/CDMA system using distributed antennas has been proposed by Qualcomm for a frequency nonselective fading channel environment such as in indoor wireless communication [3, 5].

A new CDMA application technology for downlink has been a growing interest for the support of high data rate transmission at a high level of quality in mobile communications. A multi-carrier modulation scheme providing high data rate transmission with high frequency utilization efficiency has been proposed for the DS/CDMA system based on orthogonal frequency division multiplexing (OFDM), which is a parallel data transmission technique. It is crucial for multi-carrier transmission to have a non-frequency selective fading channel over each sub-carrier

[6, 7, 10]. Therefore, this OFDM-DS/CDMA (Orthogonal Frequency Division Multiplexing-Direct Sequence/Code Division Multiple Access) system can be considered effective in a frequency selective fading channel environment avoiding ISI (Inter Symbol Interference).

However, a gain in path diversity cannot be obtained by using conventional OFDM-DS/CDMA schemes, because diversity attained by means of the RAKE combining which resolves paths cannot be applied to OFDM-DS/CDMA systems. Therefore a delayed path beyond the guard interval cannot be resolved when we use only FFT (Fast Fourier Transform) modulation.

We use a combined system employing path diversity provided by delayed distributed antennas and frequency diversity from a multi-carrier.

Signals from each antenna are delayed by several chips which can then be combined by using a RAKE receiver at a mobile station which creates diversity. It makes fading from each antenna become more randomized than the conventional systems. It creates uncorrelated signals from each antenna. Therefore we can obtain both the path diversity by means of the RAKE combining method with delayed antennas and the frequency diversity from multi-carrier [12].

We propose an effective distribution antenna diversity system according to adaptive correlation method for OFDM-DS/CDMA in a frequency selective fading channel environment. The proposed system transmits the different data using several sub-carriers which are correlated, and then, the proposed system transmits the same data using several sub-carriers which are de-correlated. It can achieve combined path and frequency diversity in a variable frequency selective fading channel. It provides high data rate services by transmission the different data using each correlated carrier, and achieves high quality by transmitting the same date with multiple antennas. The proposed system is an effective system to achieve multimedia service of high quality according to channel condition.

2 Distribution Antenna Diversity System According to Adaptive Correlation Method

2.1 Base Station Model

We propose a new transmitter diversity systems different data using several correlated sub-carriers, while the proposed system transmits the same data using several sub-carriers which are de-correlated. It can achieve combined path and frequency diversity in a variable frequency selective fading channel. It provides high data rate services by transmitting different data using each carrier, and obtains high quality by transmitting the same data using multiple antennas.

A multi-carrier transmits different data using correlated sub-carriers which provide high-rate data transmission. The proposed system transmits different data on each carrier, which provides an effective system for performing high data rate transmission with efficient frequency utilization such as that required for video, and image. This is because the data rate of the proposed OFDM systems is larger than that of a single carrier system due to the orthogonal overlapping of carriers expressed by equation (1).

On the other hand, the proposed system transmits the same data on a de-correlated carrier. This is an effective scheme for providing a high quality data service in such areas as Internet service which requires low error probability.

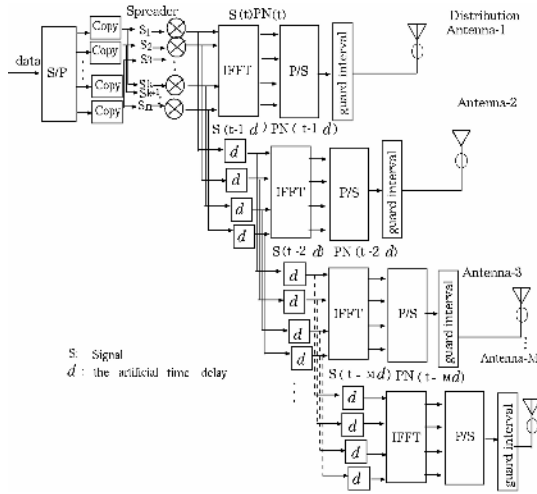


Fig. 1. Base station diagram of the proposed

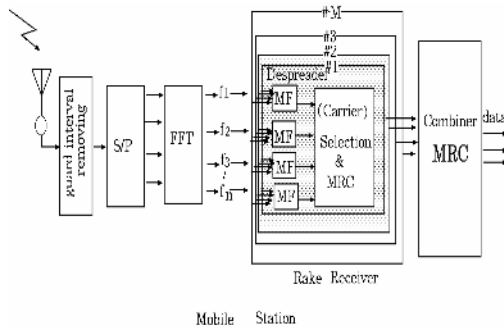


Fig. 2. Mobile station diagram of the proposed system

Binary data bits are assigned to different distribution antennas respectively. The k th user's information signal at the m th distributed antenna can be expressed as

$$b_m^k(t) = \sum_{i=-\infty}^{\infty} b_{i,m}^k P_T(t - iT), \tag{2}$$

where P_T is a rectangular pulse with duration T , and $b_{i,m}^k$ is the binary data of duration T at the i th data interval.

The spreading sequence of the k th user is expressed as

$$a^k(t) = \sum_{j=-\infty}^{\infty} a_j^k \psi(t - jT_c), \tag{3}$$

where a_j^k is the j th chip (± 1) of the k th users, and T_c is the period of the spreading sequence, and $\psi(\cdot)$ is a chip waveform, which in this paper is a rectangular pulse with duration T_c .

A transmitted signal from the m th distributed antenna of the k th user's transmitter is given by

$$s_m^k(T) = \sum_{s=1}^S \sqrt{2P} b_m^k(t - d_m^k) a^k(t - d_m^k) e^{j(w_{s,m}t)}, \tag{4}$$

where w_s is the s th carrier frequency, P is the power of a bit, and b_m^k / T_c is an integer. T_c is the chip period of a spreading sequence.

The orthogonal frequencies $w_{s,m}$ ($s=1,2,3,\dots,S$) are the s th carrier frequencies of the m th antenna and have the relation of

$$w_{s,m} = w_1 + (s - 1)2\pi / T, \text{ where } , s = 1, 2, \dots, S \tag{5}$$

where w_1 is the absolute carrier number.

Fig.1 shows the concept of the proposed system whose base station has multiple antennas with independent fading patterns, and its mobile stations with independent fading patterns, and its mobile stations with single antennas. Several sub-carriers are assigned to each antenna. A set of antennas are fed by a common signal with time delay processing to distinguish signals. Thus, this can makes fading more randomized between the OFDM tones of each antenna than in the conventional system. We can obtain uncorrelated signals from uncorrelated carrier of each antenna; therefore, multipath provides path diversity. The diversity effect of RAKE combining signals delayed by several chips can be obtained by coherent detection at a mobile station.

Fig.1 shows a base station model of the proposed system. The base station transmits different data on near sub-carriers which are correlated such as S_1, S_2, S_3 or S_4, S_5, S_6 . This is why multi-carriers are commonly located in successive frequencies and have high correlations among sub-carriers with one antenna. The same data on the de-correlated carriers are at a great distance from one another, such as in the case of S_1, S_{k+1} or S_2, S_{k+2} . In other words, the S_1 carrier transmits the same data with S_{k+1} , and S_2 does the same data with S_{k+2} because they are de-correlated.

Figure 1 shows that input data are converted from serial to parallel, and are spread in the time domain by PN codes in each carrier. Then the signals of each antenna are

delayed by several chips, and Inverse Fast Fourier Transform (IFFT) is utilized for multi-carrier modulation. The output of IFFT is parallel to serial converted. A guard interval is inserted between the output signals to prevent ISI.

The complex low path impulse response of a channel of the i th user is assumed to be

$$h_k(t) = \sum_{l=0}^{L-1} \beta_l^k \exp(j\tau_{k,l}) \delta(t - lT_c), \tag{6}$$

where l is the number of channel paths, and the path gains $\beta_{k,l}$ are independent identically distributed(i.i.d) Rayleigh random variable (r.v.s) for all k and l , and the angles $\tau_{k,l}$ are i.i.d distributed in $[0,2\pi)$.

2.2 Mobile Station

A received signal of the k th users in MC-DS/CDMA is given by

$$r(t) = \sqrt{2P} \sum_{k=1}^K \sum_{m=1}^M \sum_{l=0}^{L-1} \sum_{s=1}^S \beta_{m,s,l}^k b_m^k(t - d_{m,l}^k - \tau^k) \cdot a^k(t - d_{m,l}^k - \tau^k) e^{j(w_{s,m}t + \phi_{s,m,l}^k)} + n(t) \tag{7}$$

where β_m^k is the path gain due to Rayleigh fading, and τ^k is the propagation delay of the k th user, and $n(t)$ additive white Gaussian noise (AWGN) with two sided power spectral density of $N_0 / 2$, and $\phi_{s,m,l}^k$ is the phase shift, i.i.d. uniformly distributed random variable which takes values in $[0,2\pi)$.

Figure 2 shows a model of the mobile station used by the proposed system. A mobile unit receives the transmitted signals, which are converted from serial to parallel, and FFT is used to demodulate all the carriers, and MRC (Maximal Ratio Combining) diversity is applied by de-correlated signals from M antennas for each carrier at a RAKE receiver. As a result, coherent detection for each carrier is done at a mobile station.

3 Results

The bit error rate (BER) performance of the multiple antenna transmission system utilizing RAKE combining diversity is evaluated as a function of E_0 / N_0 , which is the average received bit energy to noise density ratio of the signal power and the noise power. In Fig.4, signals from each multiple antenna are delayed by several chips to be combined by a RAKE receiver creating artificial paths. Each antenna has four sub-carriers in this scheme.

D.A.R.C (Distributed Antenna system using RAKE Combining) indicates the proposed system. M indicates the number of antennas transmitted at a base station.

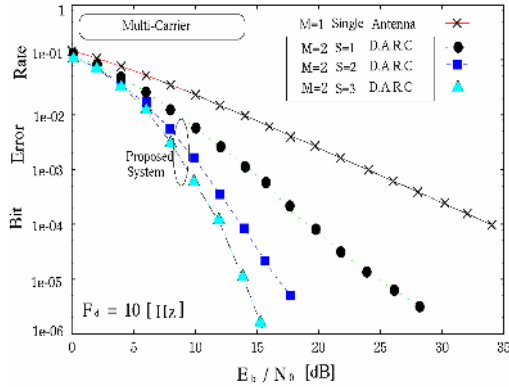


Fig. 3. BER performance of the proposed system

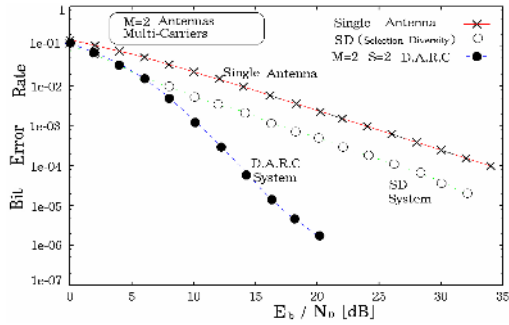


Fig. 4. BER performance of the proposed system

Fig.3 shows that the conventional single antenna system can not obtain better performance compared with the D.A.R.C. system even though the number of carriers increases, its diversity effect is not much achieved. On the other hand, the proposed system can achieve the diversity gain with un-correlated carriers. S=1 means the RAKE combining diversity with only one carrier at all the antennas. S=2 indicates the RAKE Combining diversity with two un-correlated carriers. The proposed system can achieve better diversity gain provided by RAKE Combining with MRC (Maximal Ratio Combining) diversity of de-correlated carriers as well as path diversity.

Fig.4 shows the result of the combined diversity effect between the path diversity and frequency diversity. D.A.R.C.(Distributed Antenna system using RAKE Combining) scheme consisting of 2 antennas and 2 carriers achieves better performance than the SD and the single antenna. Here, SD(Selection Diversity) means that a mobile station selects the antenna receiving the largest power of multi-carrier signal in a selective fading channel. The proposed system is effective in combining carrier and path diversity gain. As a result, the performance of D.A.R.C is better than that of the conventional SD and the single antenna system in Fig.4.

Fig.5 shows the result of BER performance comparison between MRC diversity and carrier selection diversity applied to uncorrelated S carriers of all the antennas. The

proposed system achieves the frequency diversity gain with un-correlated carriers. MRC diversity with un-correlated carriers of the proposed system is better BER performance than that of best carriers selection. The proposed system improves BER performance by combining frequency diversity and path diversity.

Fig. 6 shows the BER performance of the proposed system in multi-users. As mentioned before, SD(Selection Diversity) indicates that a mobile station selects the antenna having the largest power of multi-carrier signals in a selective fading channel. The proposed system is more effective in combining carrier and path diversity gain. We can see from Fig.6 that the performance of the proposed system becomes better than that of the conventional system. The frequency diversity can be achieved by MRC diversity of the un-correlated carriers. Enough low BER performance can be obtained with the frequency diversity gain. However, the proposed system can not achieve BER performance lower than $1e-05$ due to multi-user interference.

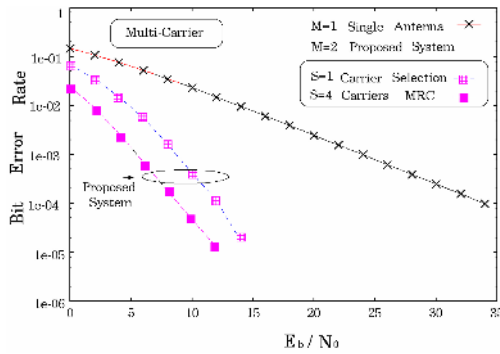


Fig. 5. BER performance of the proposed system

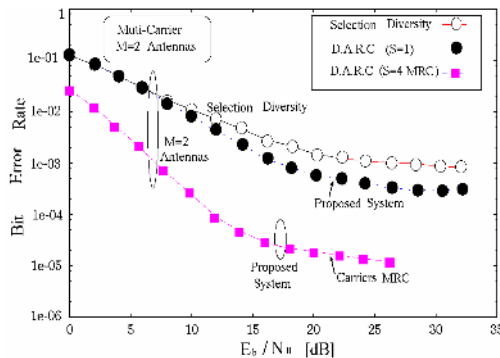


Fig. 6. BER performance of the proposed system

The proposed system fits for data such as Internet copying with low error probability, since it transmits the same data on each correlated carrier.

4 Conclusion

An effective distribution antenna diversity system according to adaptive correlation method for OFDM-DS/CDMA is proposed in the frequency selective fading channel. The proposed system transmits the different data to provide the high data rate using several sub-carriers which are correlated, while it also transmits the same data using sub-carriers which are de-correlated to support the high quality. The de-correlated signals are combined to create the path and frequency diversity effect in a frequency selective fading channel by using a RAKE receiver at a mobile station. It is found that sufficient performance diversity gain of the proposed system can be achieved compared to the other conventional systems. Thereby the proposed system is also effective for data such as Internet which is required with low error probability by transmitting the same data on each de-correlated carrier. The proposed system is flexible enough to support a variety of multimedia services with high quality. It was verified by the simulation results that the proposed schemes are effective, and practical in multi-path Rayleigh fading environment.

Acknowledgment

"This research was supported by the Kyung Hee University Research Fund in 2005"(KHU-20050359).

References

1. R.O LaMaire, A.Krcha, P.Bhagwat and J.Panian.: Wireless LANs and Mobile Networking, *IEEE Commun.* vol.34, no 8, pp. 86-94, Aug 1996
2. G. Yang, K. Pahlavan, and T. J. Holt.: Sector Antenna and DFE Modems for High Speed Indoor Radio Communication, *IEEE Trans. Veh. Tech.*, Vol. 43, No. 4, pp. 925-933, Nov 1994.
3. K. Lee, and M. Nakagawa.: PSAP (Pre-Selected Artificial Path) Diversity System for Indoor DS/CDMA in proc. *IEEE VTC-Fall Conf.*, pp.2672-2676, Oct 1999.
4. Y. Kinugawa, K. Sato and M. Okada.: Frequency and Time Division Multi-carrier Modulation for Indoor Wireless Communication System, *IEICE Trans.*, Vol E77-B., No. 3, pp.396-403, Mar 1994.
5. A. Salmasi, and K. S. Gilhouse.: On the system design aspects of code division multiple access(CDMA)applied to digital cellular and personal communications networks, in proc. *IEEE VTC'*, St, Louis, MO, May 1993.
6. H. Takahashi, M. Nakagawa.: Antenna and Multi-Carrier Combined Diversity System, *IEICE Trans.Com.*, Vol E79-B., No.9, pp.1221-1226, Sep 1996
7. E. A. Sourour, and M. Nakagawa. Performance of Orthogonal Multi-carrier CDMA in a Multi-path Fading Channel, *IEEE Tran. on Com.*, Vol 44, pp.356-367, Mar 1996.
8. K. Lee, and M. Nagakawa.: Adaptive Base Station Sector Antenna Pre-selection Transmitter Diversity using CDMA Forward Link Signal for Indoor Wireless LAN, *IEICE Trans. Com.*, Vol E83-B., No.11
9. K. Lee, M. Nakagawa,.; Distributed Antenna system using RAKE Combining Diversity for a Multi-Carrier DS/CDMA in a Frequency Selective Fading Channel, in proc. *IEEE PIMRC'2000*, London, pp.1490-1294, Sep 2000.
10. Y. Li, J. C. Chuang, and N. R. Sollenberger,.; Transmitter Diversity for OFDM Systems and Its Impact on High-rate Data Wireless Network, *IEEE Journal on Selected Areas in Communication*, Vol 17., No.7, pp.1233-1243, Feb 1999.

MIDAS: Detection of Non-technical Losses in Electrical Consumption Using Neural Networks and Statistical Techniques

Íñigo Monedero¹, Félix Biscarri¹, Carlos León¹,
Jesús Biscarri², and Rocío Millán²

¹ Escuela Técnica Superior de Ingeniería Informática,
Departamento de Tecnología Electrónica, Avda,
Reina Mercedes s/n, 41012 Seville (Spain)
imonedero@us.es

² Endesa, Avda. Borbolla S/N, 41092 Seville (Spain)

Abstract. Datamining has become increasingly common in both the public and private sectors. A non-technical loss is defined as any consumed energy or service which is not billed because of measurement equipment failure or ill-intentioned and fraudulent manipulation of said equipment. The detection of non-technical losses (which includes fraud detection) is a field where datamining has been applied successfully in recent times. However, the research in electrical companies is still limited, making it quite a new research topic. This paper describes a prototype for the detection of non-technical losses by means of two datamining techniques: neural networks and statistical studies. The methodologies developed were applied to two customer sets in Seville (Spain): a little town in the south (pop: 47,000) and hostelry sector. The results obtained were promising since new non-technical losses (verified by means of in-situ inspections) were detected through both methodologies with a high success rate.

1 Introduction

Datamining [1][2] is a computing tool which involves the use of sophisticated data analysis tools to discover previously unknown, valid patterns and relationships in large data sets. Nowadays, datamining is being applied to multiple fields and detection of non-technical losses is one field in which it has met with success recently [3]. A non-technical loss is defined as any consumed energy or service which is not billed because of measurement equipment failure or ill-intentioned and fraudulent manipulation of said equipment. Therefore, detection of non-technical losses includes detection of fraudulent users.

This datamining field involves identifying non-technical losses as quickly as possible once it has been happened. Normally, cases of non-technical loss have to be detected from huge data sets such as the logged data and user behaviour. The workforce is thus not sufficient to analyze these huge data sets and datamining techniques are the only tools which make it possible to study all the data in an acceptable time. The main research and applications in the non-technical losses and fraud detection field have been carried out on credit cards, telecommunications, and computer intrusion

[4][5][6][7]. Thus, for instance, telecommunication non-technical loss can be found in subscriptions where access to a service is obtained, often with false identity details, with no intention of paying. Other kinds of non-technical loss in this field occur from using a service without the necessary authority (for example, using mobile phone cloning) detected by the appearance of unknown calls on a bill. The tools and techniques in these cases involve detecting the users with non-technical loss quickly in order to report them and to recover the lost money.

Not only telecommunication companies and banks have non-technical losses in its users but also electrical companies. However, there is still very little non-technical detection research in electrical companies. Thus, once we have carried out a study of the state of art in this field and we have only found a very few papers [8], being therefore a research topic quite new.

Current methodology work by the electrical companies in the detection of non-technical losses is basically of two kinds. The first one is based on making in-situ inspections of some users (chosen after a consumption study) from a previously chosen zone. The second one is based on the study of the users which have null consumption during a certain period. The main problem of the first alternative is the need for a large number of inspectors and, therefore, a high cost. The problem with the second option is the impossibility of detecting users with non-null consumption (these are only the clearest cases of non-technical losses).

This paper describes a prototype for the detection of non-technical losses which has been developed at the Electronic Technology Department of the University of Seville.

2 Midas Project

MIDAS is the name of a project which developed two methodologies for the detection of non-technical losses, one by means of neural networks and the other by means of statistical techniques. The project was financed by Endesa, the most important electrical company of Spain and one of the most important ones in the world, and by Sadiel which is the most important consulting company of Andalusia and one of the most important ones of Spain. A representation of the stages carried out in the development of the project is shown in Figure 1. Each of the phases shown in the figure are described below:

- 1 Data Selection: The aim of this first phase was the selection from the database of the electrical company of a data set with which to work for the development of the prototype. Specifically, two sets were selected: Hostelry business in the province of Seville and private users in a little town in the south of Seville with a population of about 47,000. The first set was selected for being a traditionally sector of many non-technical losses. On the other hand, the chosen little town was the Sevillian postal code in which the electrical company had registered, through its inspections, the largest number of non-technical loss cases. The non-technical loss files of these users were also collected.
- 2 Query and formatting data: In this second phase the SQL queries were carried out and the data was formatted. Thus, three tables were obtained from the database: one for contracts, one for bills and a third one for files of cases with non-technical

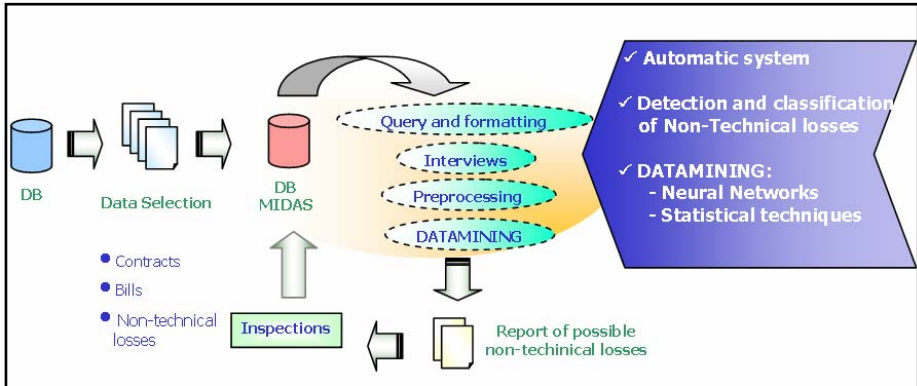


Fig. 1. Phases in the development of Midas

losses. The number of users in each set as well as the number of registered non-technical losses is shown in Table 1. As may be observed, the number of detected cases with non-technical losses was low in relation to the total number of contracts. The three database tables include, for each user, the following fields: bills from the last 4 years (one bill every two months), amount of power contracted and the type of customer (private or the what kind of business), address, type of rate, etc.

Table 1. Analyzed data

Type of customer	Number of Contracts	Cases with Non-Technical Losses
Little town	60048	17
Hostelry business	12879	5

- 3 Interviews: This task involved a number of interviews (exactly five were carried out) with specialized staff of the company for the detection of non-technical losses. In these interviews the different kinds of non-technical loss were studied as well as the various characteristics in the consumption evolution of each of them. This phase was carried out parallel to the two other previous phases.
- 4 Preprocessing: Data was prepared for the mining process in this phase. To this purpose, the entire fields from the tables shown above were studied and two new tables (one for each kind of customer) were generated with a set of fields selected for mining. Specifically, each register in these tables (one for each user) included: the six bills corresponding to the last year's consumption, the power supplied and a non-technical loss sign (the value of this field was 1 if the user had registered some non-technical loss and otherwise the value was 0).
- 5 Datamining (with Neural Networks and Statistical Techniques): These two stages, which were carried out in parallel, involved the data-mining process. The techniques applied were neural networks and a statistical study. Our aim was to try to

obtain results through two different methods in order to obtain two result sources and compare them. The data mining process using these two techniques is described in detail in Sections 3 and 4.

- 6 Reporting possible non-technical losses and inspections: Once the data mining process was carried out, the electrical company would receive reports on customers detected with possible non-technical losses. Finally, the company would study these customers individually to decide on which ones to carry out the inspections. Thus, at the same time, by means of the inspections we could test the validity of the datamining process.

3 Data Mining with Neural Networks

Artificial neural networks are abstract simulations of a real nervous system that contains a collection of neuron units communicating with each other via axon connections. Algorithms based on neural networks are among the most popular data mining techniques used today. In general, neural networks are used when the exact nature of the relationship between inputs and outputs is not known (if the relationship was known, the system could be modeled directly).

There are two types of neural networks depending on the training used: supervised and unsupervised neural networks. Thus, supervised training involves the use of the inputs to come up with an output that can be compared to the given output. On the other hand, unsupervised learning by way of neural network training is unique in that the network is given a set of inputs but no indication of what the output should be. The goal, then, is to have the network itself begin to organize and use those inputs to modify the weights of its own neurons.

We used unsupervised neural networks in our datamining process due to the conditions of our problem. Thus, we had a couple of tables about customers in which we wanted to distinguish users with non-technical losses from users with a normal consumption. It was thus not possible carry out a supervised training since we could not be certain that customers were in the first case (we only had one set of files registered in some inspections). Besides, the total number of non-technical losses registered by the company for this data was very low (only 22 compared with the total number of 72,927 contracts –see Table 1–).

Specifically, we used Kohonen networks (whose structure and working are represented in Figure 2) which provide an objective way of clustering data by utilizing a self-organizing network of artificial neurons. The Kohonen network resembles statistical clustering algorithms as it is capable of finding intrinsic clustering in the input parameter space.

In order to carry out the clustering process, it was necessary to select an adequate set of inputs which would make it possible to characterize the patterns. Thus, after studying the different alternatives, we selected the following inputs as identifiers of customer consumption pattern:

- Maximum: the maximum value of the bills of the previous year.
- Minimum: the minimum value of the bills of the previous year.
- Average: the consumption average of the bills of previous year.

- Difference average: the difference between the average parameter of the customer and the mean of the average parameters of the analyzed customers.
- Consumption coefficient: $(\text{Maximum} - \text{Minimum}) / \text{amount of contract power}$
- Difference average for month N : difference between the consumption in month N and the consumption average for month N of the analyzed customers.
- Difference maximum for month N : difference between the consumption in month N and the consumption maximum for month N of the analyzed customers.

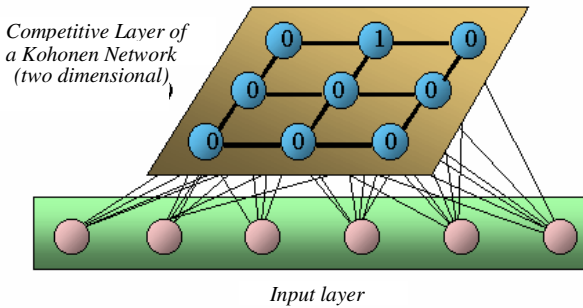


Fig. 2. Kohonen network structure

Once the input parameters had been selected, we designed a process for the detection of non-technical losses based on the search of similarities between the consumption pattern of the registered files and the consumption pattern of database customers. In short, first we carried out a clustering process of the all customers (including the customers with registered non-technical losses). Afterwards, we studied the different clusters in order to identify where the customers with non-technical losses were concentrated. So, in the clusters which were localized, the registered files were identified as possible customers with non-technical losses and we recommended the electrical company to carry out an inspection on them.

In case of hostelry business, we extracted for our analysis the 1,145 customers belonging to the interval of contracted power between 12 and 14 KW. We selected this interval in order to reduce the number of samples because 4 of the 5 files registered by the company belonged to that group. In the case of the little town, we extracted the 46,081 customers of the interval between 12 and 14 KW because 14 of the 17 files of this set were located within that group.

Two Kohonen neural networks were designed for each of the groups studied (hostelry business in the province of Seville and private users in the little town, making for a total of 4 neural networks) in order to carry out the clustering process: The first one was for clustering using parameters which involved, for each customer, an annual calculus of his consumption: Maximum, Minimum, Average, Difference average and Consumption coefficient and the second one was for clustering using the parameters related to monthly consumption: Difference average for month N and Difference maximum for month N .

First, the data was clustered using the first network. Afterwards, in order to reduce the large groups and the number of customer to be inspected, the second network was applied to the data belonging to clusters where the files registered by the electrical company were concentrated. Finally, the resulting groups were studied, that is groups with registered files and, therefore, with customers having a similar consumption pattern.

The two neural networks had 12 neurons and a 4*3 structure and therefore generated 12 clusters for each data set. After training the first network in the case of hostelry business, the registered files were localized into two clusters. The first cluster (cluster *a1*) only had 40 customers whereas the second one (cluster *a2*) had 352. In the case of the little town, the registered files were also localized into two sets (clusters *b1* and *b2*) of 2,520 and 852 customers, respectively. The second neural network was trained on clusters *a2*, *b1* and *b2* (cluster *a1* only had 40 customers) and the registered files were concentrated into an single cluster in each case (clusters *c1*, *c2* and *c3*) of 48, 2,200 and 244 customers, respectively.

Finally, the users of clusters *a1*, *c1*, *c2* and *c3* were identified as customers with possible non-technical losses and we recommended the electrical company to do a specific study for each case and if necessary, to inspect them.

Table 2. Selected study cases using neural networks

Type of customer	Contracts	Selected study cases	Selected rate
Little town	46,081	2,444 (2,200+244)	5.03 %
Hostelry business	1,145	88 (40+48)	7.68 %

4 Data Mining with Statistical Techniques

Outliers are elements in a data set which are grossly different or inconsistent with the remaining data. The statistical method developed for the non-technical losses is based on the detection of outliers, and it provides a general methodology for obtaining a list of abnormal users using only the general customer databases as input. In electrical consumption, outliers can be caused by measurement error or by fraud in customer consumption. But, alternatively, outliers may be the result of inherent data variability. Thus, the detection of outliers and its analysis is an interesting datamining task.

The statistical approach to outlier detection implies the use of a distribution or probability model for the given data set and then identifies outliers with respect to the model using a divergence test. The application of this test requires knowledge of the data set parameters (such as the assumed data distribution), distribution parameters (such as the mean and variance) and, mainly, knowledge of the inherent data variability.

In short, the datamining process involves the following tasks: First, from the two work sets: in the province of Seville and private users in the little town. We normalized these samples erasing the temporary and the local components of the individual

consumption. Thus, we considered the probability distribution of the transformed sample as Gaussian (for the normal operating condition). Afterwards, we calculated and adjusted the threshold of the sample variance. Finally, we used outliers to guide the inspections.

We developed this method working on the set of particular users in the little town, in which we extracted 105 customers with the same contracted power (4 KW) and the same yearly electric consumption (between 0 and 5000 KW).

On the set of selected customers, we carried out a set of calculus for the detection of non-technical losses. The method involved the following steps:

1. Given:
 - A data at a set of spatial location (different customers).
 - Several data acquisitions at each location but spaced in time. It is assumed that all the locations are sampled at the same time but are sampled several times.
2. The operating equation is defined as
3. Follows: $Data\ acquired = Dlt$ where
 - D is the current data point measurement.
 - l is the location of the measurement (number of customers).
 - t is the time of the measurement (this is the time at which all the data is recorded at all locations).
4. The next step is to obtain the average at each time across all locations. This is defined by equation:

$$At = \sum_{l=1}^N \frac{Dlt}{N}$$

where

At is the average of all data at time t , across all locations l

N is the number of locations l

5. It can now be observed, considering the averages and their times, whether there is or not an effect on a change in time. This is something that cannot be seen during an analysis of variance, but which we may see here.
6. The following step was to obtain the differences comparing the data at each location to the average at that time in the following way:

$$Lt = Dlt - At$$

where lt is the difference between the data at each location l and the time t , average.

7. Now the average of the differences lt at each location across time needs to be obtained, that is:

$$\bar{\delta}l = \sum_{t=1}^M \delta lt / M$$

where

$\bar{\delta}l$ is the average of all lt at location l across time t .

M is the number of times averaged.

- In the following step, it is necessary to obtain the differences, comparing each time difference lt , to its average at location l , as shown in equation:

$$\Delta lt = \delta lt - \bar{\delta} l$$

Thus, the values obtained are the residual electrical consumptions after the linear variations in time and space are averaged out.

- The next step was to calculate the standard deviation associated to each customer which is used as a distribution parameter:

$$STD_{\Delta l} = \pm \sqrt{\frac{\sum_{t=1}^6 (\Delta lt - \bar{\Delta} l)^2}{6-1}}$$

where

$$\bar{\Delta} l = \sum_{t=1}^6 \frac{\Delta lt}{6}$$

- Finally, we carried out an outlier analysis (inherent data variability). To do this, we estimated a threshold for STD calculated as the mean of $STD_{1..N}$ multiplied by a constant (1.96 corresponding to a level of significance of 0.05).

$$STD_{\Delta l} = \pm \sqrt{\frac{\sum_{t=1}^6 (\Delta lt - \bar{\Delta} l)^2}{6-1}}$$

Thus, plotting $STD_{1..N}$ and the threshold (Figure 3), we found that 9 customers were outliers.

As mentioned, these outliers can be caused by measurement error or by fraud in customer consumption. But, alternatively, outliers may be the result of inherent data variability. Thus, the following task involved a careful study of these outliers by company staff specialized in non-technical loss detection.

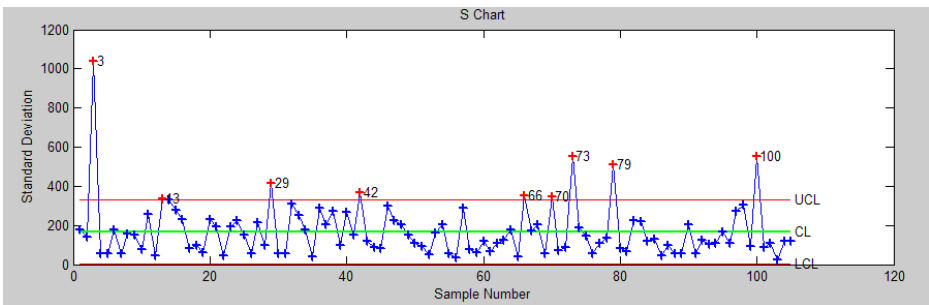


Fig. 3. An STD and threshold representation for the 105 selected customers

Table 3. Selected study cases using statistical techniques

Type of customer	Studied contracts	Selected study cases	Study rate
Little town	105	9	8.57%
Hostelry business	4,047	440	10.87%

5 Results and Conclusions

Once the datamining processes were carried out, the data on the customers detected by both methodologies (neural networks and statistical techniques) as possible customers with non-technical losses, was sent to the electrical company. Thus, some of these cases (selected in order of importance for the company since there was a large number of cases and their study required considerable time) were studied individually and in detail by specialized staff of the company which selected a set of these to be inspected in-situ. The rates of inspections as well as their results are shown in following tables:

Table 4. Datamining results (Neural Networks)

Type of customer	Selected study cases	Cases studied by the company	Cases inspected by the company	Non-technical losses detected
Little town	2,200	5	1	1
Hostelry business	89	27	6	3

Table 5. Datamining results (Statistical Techniques)

Type of customer	Selected study cases	Cases studied by the company	Cases inspected by the company	Non-technical losses detected
Little town	9 (of 105)	6	2	1
Hostelry business	440 (of 4047)	35	15	8

As may be observed in Tables 4 and 5, both methodologies detected cases of non-technical losses: 13 in total. The success rate from the inspections carried out by the company was around 50%. This represents an excellent rate, taking into account that up to that moment the company had carried out the study of a very large number of customers without any previous filtering.

In addition, both methodologies are general and not bound to a particular set or customer type. The whole input information needed is taken exclusively from the general customer database and is currently being integrated into a global system. Finally, we can enumerate three important conclusions for the work described in this paper:

1. We have developed two possible methodologies for the detection of non-technical losses (therefore, including cases of fraud): one by means of neural networks and the other by means of statistical techniques.
2. The company has tested the validity of both (by means of individual studies of the cases detected and by selective inspections in-situ). The resulting success rate of the inspections was around 50%.
3. The work described in this paper is a worldwide original work due to the fact that there is very little research on detection of non-technical losses and fraud detection in electrical consumption.

A possible line of work in the future might be the application of different and more-complex input parameters or other datamining techniques as well as the integration of human expert knowledge in these new techniques in order to improve the results. Therefore, this work is likely to be continued and, in fact, the Electronic Technology Department of the University of Seville and Endesa company are planning a continuation of the studies.

Acknowledgments

We would like to thank the initiative and collaboration of Endesa Company in the person of Mr. Juan Ignacio Cuesta.

References

1. M. Kantardzic, "Data Mining: Concepts, Models, Methods and Algorithms", Ed. IEEE Press, 2003.
2. G. Piatetski-Shapiro, W.J. Frawley, "Knowledge discovery in databases", Ed. AAAI/MIT Press, 1991.
3. Yufeng Kou, Chang-Tien Lu, Sirirat Sinvongwattana, Yo-Ping Huang, "Survey of Fraud Detection Techniques", Proceedings of the 2004 IEEE International Conference on Networking, Sensing & Control, Taiwan, March 21, 2004.
4. J.R. Galván, A. Elices, A. Muñoz, T. Czernichow, M.A. Sanz-Bobi, "System for Detection of Abnormalities and Fraud in Customer Consumption", 12th Conference on the Electric Power Supply Industry, November, 1998, Thailand.
5. R. Wheeler, S. Aitken, "Multiple Algorithms for Fraud Detection", Knowledge-Based Systems 13 (2000) 93–99
6. R. Richardson, "Neural Networks Compared to Statistical Techniques", Computational Intelligence for Financial Engineering (CIFEr), Proceedings IEEE/IAFE, 1997.
7. S. Daskalaki, I. Kopanas, M. Goudara, N. Avouris, "Data Mining For Decision Support on Customer Insolvency in the Telecommunications Business", European Journal of Operational Research 145 (2003), 239–255.
8. José E. Cabral, João Onofre P. Pinto, Edgar M. Gontijo, José Reis Filho, "Fraud Detection In Electrical Energy Consumers Using Rough Sets", 2004 IEEE International Conference on Systems, Man and Cybernetics.

Hyperbolic Voronoi Diagram

Zahra Nilforoushan and Ali Mohades

Faculty of Math. and Computer Sc.,
AmirKabir University of Tech.,
424 Hafez Ave. Tehran, Iran
{nilforoushan, mohades}@cic.aut.ac.ir

Abstract. Voronoi diagrams are among the most extensively studied objects in computational geometry with useful applications in different areas of science. To understand impacts of non-Euclidean geometry on computational geometry, this paper investigates the Voronoi diagram in hyperbolic space specially the one in the Poincaré hyperbolic disk, which is a 2-dimensional manifold with negative curvature. We first prove some lemma in Poincaré hyperbolic disk and then give an incremental algorithm to construct Voronoi diagram.

1 Introduction

Given a set of sites and a distance function from a point to a site, a *Voronoi diagram* can be roughly described as the partition of the space into cells that are the locus of points closer to a given site than to any other site.

Voronoi diagrams have proven to be useful structures in various fields such as astronomy, crystallography, biology etc. [6]. Excellent surveys on the background, construction and applications of Voronoi diagrams can be found in Aurenhammer's survey [3] or the book by Okabe, Boots, Sugihara and Chiu [18]. Naturally the first type of Voronoi diagrams being considered was the one for point sites and the Euclidean metric. Subsequent studies considered extended sites such as segments, lines, curved objects, convex objects, semi-algebraic sets and various distances like L_1 or l_∞ or any distance defined by convex polytope as unit ball [1,5,8,11,12,13,14,15,16]. In [4,19], the Voronoi diagram in upper half-plane has been studied. In this paper, we generalize Voronoi diagrams in the Euclidean space \mathbb{R}^2 into the Poincaré hyperbolic disk, which is a 2-dimensional manifold with negative curvature [17]. From the differential geometry point of view, the curvature of Euclidean space \mathbb{R}^n is zero. So, it is a vital problem to generalize algorithms in \mathbb{R}^n into the Riemannian manifolds with a non-zero curvature.

In section 2 a brief introduction to the Poincaré Hyperbolic disk is given, section 3 comes with the definition of Voronoi diagram in the Poincaré Hyperbolic disk and presents some lemma, in section 4 an algorithm for constructing Voronoi diagram in the Poincaré Hyperbolic disk is given and section 5 is devoted to conclusions.

2 Poincaré Hyperbolic Disk

The *Poincaré hyperbolic disk* is a two-dimensional space which has hyperbolic geometry and negative curvature defined as the disk $D = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 < 1\}$, with hyperbolic metric

$$ds^2 = \frac{dx^2 + dy^2}{(1 - x^2 - y^2)^2} .$$

See [2,9] for details.

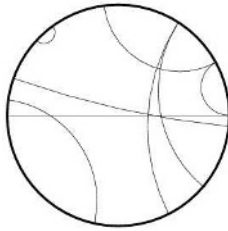


Fig. 1. Poincaré disk and some of its geodesics

The Poincaré disk is a model for hyperbolic geometry in which a *geodesic* (which is like a line in Euclidean geometry) is represented as an arc of a circle whose ends are perpendicular to the disk’s boundary (and diameters are also permitted). Two arcs which do not meet correspond to parallel rays, arcs which meet orthogonally correspond to perpendicular lines, and arcs which meet on the boundary are a pair of limit rays (see figure 1).

A geodesic is expressed as

$$x^2 + y^2 - 2ax - 2by + 1 = 0$$

with $a^2 + b^2 > 1$, or

$$ax = by.$$

Geodesics are basic building blocks for computational geometry on the Poincaré disk. The distance of two points is naturally induced from the metric of D ; consider two point $z_1(x_1, y_1), z_2(x_2, y_2) \in D$, the distance of the two points $d(z_1, z_2)$ can be expressed as

$$d(z_1, z_2) = \int_{\text{the geodesic that connects } z_1 \text{ and } z_2} ds = \tanh^{-1}\left(\left|\frac{z_2 - z_1}{1 - \bar{z}_1 z_2}\right|\right). \quad (1)$$

For a geodesic l , each of the two connected components l^+ and l^- of $D \setminus l$ is called *half-space*.

Lemma 1. *Half-space is a convex set.*

Proof. For given points $z_1, z_2 \in l^+$, suppose l_{z_1, z_2} be the geodesic segment that connects two points z_1 and z_2 . We have to prove that $l_{z_1, z_2} \subset l^+$. Suppose that l and l_{z_1, z_2} are on circles C and C_{z_1, z_2} in the Euclidean plane respectively. Since two circles intersect in at most 2 points and in Poincaré disk it will happen one of the (a) or (b) (See figure 2 for two geodesics), in case (a), therefore there is a diameter which l and l_{z_1, z_2} are in two different side of it. So C and C_{z_1, z_2} do not intersect each other at any point. Hence $l_{z_1, z_2} \subset l^+$. In case (b), there

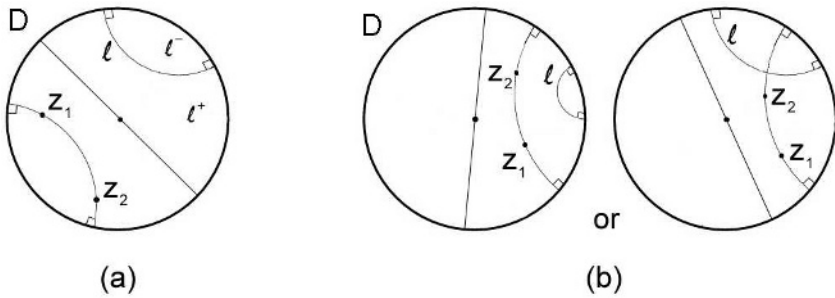


Fig. 2. The position of two geodesics

is a diameter which l and l_{z_1, z_2} are in the same side of it and because of the geodesic's property, the centers of C and C_{z_1, z_2} are in $\mathbb{R}^2 \setminus D$. Therefore, at most one of the intersection is in the D and the other is in the $\mathbb{R}^2 \setminus D$. So $z_1, z_2 \in l^+$ implies that $l_{z_1, z_2} \subset l^+$. The case in which l is a diameter of D , can be proved in a similar way. □

3 Definition of Voronoi Diagram in Poincaré Hyperbolic Disk

Voronoi diagrams are irregular tessellations of the space, where space is continuous and structured by discrete objects. Suppose that the set of n points $P = \{z_1, z_2, \dots, z_n\} \in D$ are given. The *hyperbolic Voronoi polygon* $Vor(z_i)$ for P is defined as follows:

$$Vor(z_i) = \{z \in D \mid d(z, z_i) \leq d(z, z_j) \forall j \neq i\}.$$

The hyperbolic Voronoi polygons for P partition D , which is called *Voronoi diagram in Poincaré hyperbolic disk*. Vertices of hyperbolic Voronoi polygons are called *hyperbolic Voronoi points* and boundaries of Voronoi polygons are called *hyperbolic Voronoi edges* (see figure 3). In fact the Voronoi diagram of a set of points is a decomposition of the space into proximal regions (one for each point). The locus of the same distance from two points is called the *perpendicular*

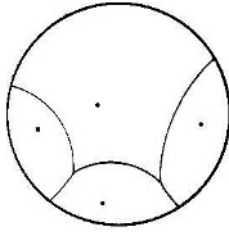


Fig. 3. A Voronoi diagram in D

bisector. In general, any hyperbolic Voronoi edge is the part of a perpendicular bisector. In next lemma, we provide a simple argument for the existence of perpendicular bisector in Poincaré hyperbolic disk.

Lemma 2. *For any two points $z_1, z_2 \in D$, there exist a perpendicular bisector for them in D .*

Proof. We first prove that there exist a geodesic line that maps z_1 to z_2 . We know that there exist a non-Euclidean transform like r that maps z_2 to 0 (the origin of D). Assume $r(z_1) = z'_1$ (See figure 4). Similarly there exist a non-Euclidean transform like s that maps $r(z_1) = z'_1$ to 0. Note that non-Euclidean transform means non-Euclidean reflection with respect to a geodesic line of D . So there is a geodesic line (call l), that reflect with respect to l , maps $r(z_1) = z'_1$ to 0. Since for every non-Euclidean transform like t , t^{-1} is also a non-Euclidean transform, $(s \circ r)^{-1}(l) = \acute{l}$ is a geodesic line of D too that maps z_1 to z_2 . And it can be shown that \acute{l} is the perpendicular bisector of z_1, z_2 . □

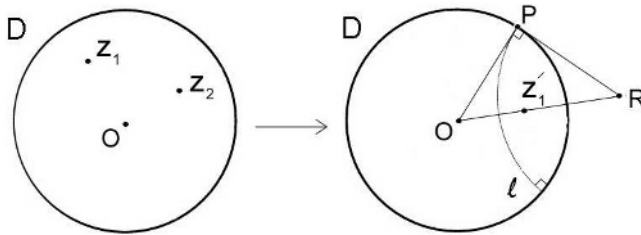


Fig. 4. Figure of lemma 2

A perpendicular bisector in D has the following property.

Lemma 3. *Any perpendicular bisector in D is a geodesic of D .*

Proof. Suppose that two points $z_1(a_1, b_1)$ and $z_2(a_2, b_2)$ in D are given. For any point $X(x, y)$ on the perpendicular bisector of the mentioned points the following equality holds:

$$d(X, z_1) = d(X, z_2).$$

By using formula (1) and solving the equation, we will obtain one of the equation below for perpendicular bisector:

$$x^2 + y^2 - 2\left(\frac{a_1b_2 + a_2b_1}{b_1 + b_2}\right)x - 2\left(\frac{b_1b_2 - a_1a_2 + 1}{b_1 + b_2}\right)y + 1 = 0,$$

$$x^2 + y^2 - 2\left(\frac{a_1a_2 - b_1b_2 + 1}{a_1 + a_2}\right)x - 2\left(\frac{a_1b_2 + a_2b_1}{a_1 + a_2}\right)y + 1 = 0,$$

or

$$[b_1(a_2^2 + b_1b_2 - 1) + b_2(a_1^2 + b_1b_2 - 1)]x = [a_1(a_2^2 + b_2^2 + 1) + a_2(a_1^2 + b_1^2 + 1)]y.$$

And we see that all of these equations are geodesics of D which is mentioned in §2. □

Lemma 4. *Any hyperbolic circle is an Euclidean circle and vice versa.*

Proof. (Sketch of proof) Suppose C is a hyperbolic circle with hyperbolic center c and hyperbolic reduce r . If $c = 0$ (i.e., c is the center of D), then the hyperbolic circle is:

$$\{z \in D \mid d(0, z) = r\} = \{z \in D \mid \tanh^{-1} |z| = r\} = \{z \in D \mid |z| = \tanh r\}$$

and this is an Euclidean circle with center 0 and reduce $\tanh r$. If $c \neq 0$, by using the hyperbolic transform $M(z) = \frac{z-c}{1-\bar{c}z}$ ($z \in D$), c will mapped to 0 and this completes the proof (see [2]). □

Notice that the Euclidean center of the circle is different from the point c . The point c is called *hyperbolic center*. As a result of the above lemma, we obtain the following:

The set of nearest point of P in the Euclidean plane and in the Poincaré hyperbolic disk are the same.

Lemma 5. *The locus of points which have the equal hyperbolic distance from three given points $z_1(a_1, b_1), z_2(a_2, b_2)$ and $z_3(a_3, b_3)$, is a point.*

Proof. It is sufficient to obtain the set of points like $z(x, y)$ which is on the bisector of z_1 and z_2 , z_2 and z_3 , and z_1 and z_3 . From the bisectors formula in lemma 3, the proof will be complete easily. Just notice that the point which is equidistance from given three distinct points in D maybe does not always exist in D , but it certainly exists in \mathbb{R}^2 . □

4 Construction of the Voronoi Diagram in Poincaré Hyperbolic Disk

Our algorithm to construct Voronoi diagram is based on incremental method which is like one proposed initially by [10] in constructing the Voronoi diagram

in the Euclidean geometry, but different in some points. We show that Voronoi diagram in the Poincaré disk can be updated in $O(i)$ -time when a new point is added.

We first explain the algorithm in [10]. Let $S = \{z_1, z_2, \dots, z_i\}$ be a given set of i distinct points. Then we sort them by their (x, y) -coordinate lexicography order. The algorithm proceeds incrementally by adding the point z_{i+1} to $Vor(S_i)$ in each step. Here is the algorithm for making the $Vor(S_{i+1})$ from the $Vor(S_i)$. It consists of the following two steps.

Algorithm. (*Constructing $Vor(S_{i+1})$ from $Vor(S_i)$*)

Step 1: Among the points z_1, z_2, \dots, z_i of the diagram $Vor(S_i)$, find the nearest point to z_{i+1} call $z_{N(i+1)}$. Notice that $z_{N(i+1)} \in \{z_1, z_2, \dots, z_i\}$.

Step 2: Starting with the perpendicular bisector of the segment $z_{i+1}z_{N(i+1)}$, find the point of intersection of the bisector with a boundary edge of $Vor(z_{N(i+1)})$ and determine the neighboring region $Vor_i(P_{N_1(i+1)})$ which lies on the other side of the edge, then draw the perpendicular bisector of $z_{i+1}z_{N_1(i+1)}$ and find its intersection with a boundary edge of $Vor_i(P_{N_1(i+1)})$ together with the neighboring region $Vor_i(P_{N_2(i+1)})$; ... ; repeating around in this way, create the region of z_{i+1} to obtain $Vor(S_{i+1})$. Now by modifying the algorithm above for D , in step 2 we search the hyperbolic Voronoi edge that intersects the perpendicular bisector. When the edge is not infinite edge, we may use the Euclidean algorithm. If the edge is infinite line (the boundary of D is called the *infinite edge*), then use the Procedure below:

Procedure. (for the case that the edge is infinite edge)

Look for a new edge which intersects the perpendicular bisector.

IF the new edge is finite edge

THEN use the new edge and apply the Euclidean algorithm with regarding the edge as starting edge.

ELSE (the new edge is also infinite edge) use the method below.

If the new edge is also an infinite edge, we may locally change the Voronoi diagram, so we treat only the incremental point and the nearest point. We have to repeat the operation of step 2 for all the edges of the hyperbolic voronoi polygon of the nearest point, where each of starting and ending edge of algorithm is the left and the right infinite edge of the found edge (see figure 5).

An important difference between the Poincaré disk geometry and the Euclidean geometry is the existence of more than one lines that pass through a given point and parallel to a given line (see figure 6). Thus we cannot dissolve many degenerate case in the Poincaré disk by the symbolic perturbation (see [7]). Hence we have to use the above Procedure.

Theorem 1. *Voronoi diagram is updated in $O(i)$ -time by using the above algorithm when a new site is added, where i is the number of points.*

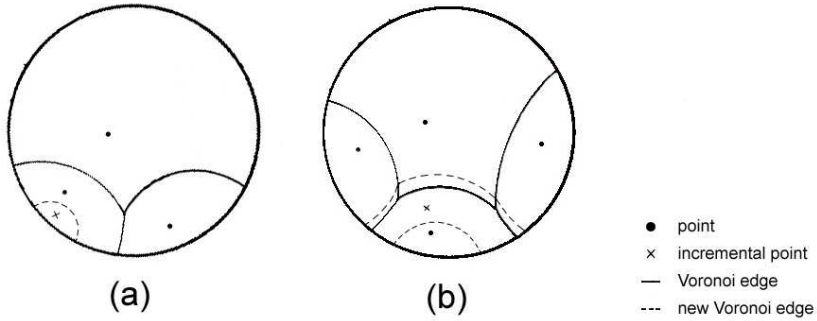


Fig. 5. When the new edge is infinite

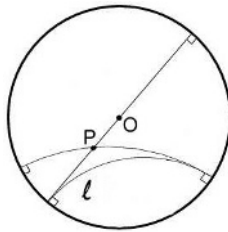


Fig. 6. Two lines pass through a given point P and parallel with line l

Proof. Note that since step 1 of the above algorithm can be done in $O(i)$ -time and step 2 can be done in the linear time with respect to the number of the hyperbolic Voronoi edges. So we have to prove that the number of the hyperbolic Voronoi edges is at most $O(i)$. By considering the dual graph of the Voronoi diagram (Delaunay triangulation), the number of the edge of this graph is same with hyperbolic Voronoi edge. The graph is planar and the vertices are $O(i)$. So, the number of the edges is also $O(i)$. \square

Corollary 1. *For given n point in hyperbolic Poincaré disk, Voronoi diagram can be constructed in $O(n^2)$ time incrementally.*

Proof. Use the above theorem and the fact that

$$\sum_{i=1}^n O(i) = O(n^2). \quad \square$$

5 Conclusion

In this paper we proved some properties about Voronoi diagram in Poincaré hyperbolic disk and gave an incremental algorithm for it. In the future we would generalize this method.

Acknowledgment

We would like to thank professor Abolghasem Laleh for valuable conversations.

References

1. Alt, H., Schwarzkopf, O.: The Voronoi diagram of curved objects. In Proc. 11th Annu. ACM Sympos. Comput. Geom. (1995) 89–97
2. Anderson, J., W.: Hyperbolic Geometry. New York. Springer-Verlag. (1999)
3. Aurenhammer, F., Klein, R.: Voronoi diagrams. In sack. J.R. Urrutia. J. eds: Hand book of Computational Geometry. Elsevier Science publishers B. V. North Holand. Amesterdam. (2000) 201–290
4. Boissonat, J-D., Yvinec, M.: Non-Euclidean metrics, §18.5 in Algorithmic Geometry. Cambridge University Press. (1998) 449–454
5. Chew, L., P., Drysdale, R., L.: Voronoi diagram based on convex distance functions. Proc. 1st Ann. Symp. Comp. Geom. (1985) 235–244
6. Drysdale, S.: Voronoi Diagrams: Applications from Archaeology to Zoology. Regional Geometry Institute. Smith College. July 19. (1993)
7. Edelsbrunner, H.: Algorithms in Combinatorial Geometry. Springer-Verlag. (1987)
8. François, A.: Voronoi diagrams of semi-algebraic sets. Ph.D Thesis. Department of Computer Science. The University of British Colombia. January. (2004)
9. Goodman-Strauss, C.: Compass and Straightedge in the Poincaré Disk. Amer. Math. Monthly. **108** (2001) 33–49
10. Green, P., J., Sibson, R.: Computing Dirichlet Tessellation in the plane. The Computer Journal. **21** (1978) 168–173
11. Karavelas, M.: 2D Segment Voronoi Diagrams. CGAL User and Reference Manual. All parts. Chapter 43. 20 December (2004)
12. Karavelas, M., I., Yvinec, M.: The Voronoi Diagram of Planar Convex Objects. 11th European Symposium on Algorithms (ESA 2003). LNCS **2832** (2003) 337–348
13. Kim, D.-S., Kim, D., Sugihara, K.: Voronoi diagram of a circle set from Voronoi diagram of a point set: 2. Geometry. Computer Aided Geometric Design. **18** (2001) 563–585
14. Koltun, V., Sharir, M.: Polyhedral Voronoi diagrams of polyhedra in three dimensions. In Proc. 18th Annu. ACM Sympos. Comput. Geom. (2002) 227–236
15. Koltun, V., Sharir, M.: Three dimensional Euclidean Voronoi diagrams of lines with a fixed number of orientations. In Proc. 18th Annu. ACM Sympos. Comput. Geom. (2002) 217–226
16. Lee, D., T.: Two-dimensional Voronoi diagrams in the L_p metric. JASM. **27**(4) (1980) 604–618
17. Morgan, F.: Riemannian Geometry: A Beginner's Guide. A K Peters. Ltd. (1993)
18. Okabe, A., Boots, B., Sugihara, K., Chiu, S., N.: Spatial tessellations: concepts and applications of Voronoi diagrams. 2nd edition. John Wiley & Sons Ltd. Chichester. (2000)
19. Onishi, K., Takayama, N.: Construction of Voronoi diagram on the Upper half-plane. In IEICE TRANS. Fundamentals. **E00-X**(2) February. (1995)

Effects of Confinement on Chemical Reaction Equilibrium in Nanoporous Materials

William R. Smith¹, Martin Lísal^{2,3}, and John K. Brennan⁴

¹ Faculty of Science, University of Ontario Institute of Technology,
2000 Simcoe St. N., Oshawa, ON L1H7K4, Canada

william.smith@uoit.ca

<http://science.uoit.ca>

² E. Hála Laboratory of Thermodynamics,
Institute of Chemical Process Fundamentals,
Academy of Sciences of the Czech Republic,
165 02 Prague 6, Czech Republic

lisal@icpf.cas.cz

<http://www.icpf.cas.cz>

³ Department of Physics, Institute of Science, J.E. Purkinje University,
400 96 Ústí n. Lab., Czech Republic

<http://sci.ujep.cz/>

⁴ U.S. Army Research Laboratory, Weapons and Materials Research Directorate,
Aberdeen Proving Ground, MD 21005-5066, U.S.A.

JBrennan@arl.army.mil

Abstract. We present a molecular-level simulation study of the effects of confinement on chemical reaction equilibrium in nanoporous materials. We use the Reaction Ensemble Monte Carlo (RxMC) method to investigate the effects of temperature, nanopore size and capillary condensation on the nitric oxide dimerization reaction in a model carbon slit nanopore in equilibrium with a bulk reservoir. We analyze the effects of the temperature, nanopore width and capillary condensation on the reaction equilibrium with respect to the reaction conversion and fluid structure.

1 Introduction

We now have a fairly good understanding of the influence of confinement on the physical properties of nanophases for simple and moderately complex non-reactive fluids [1, 2]. It is well established, for example, that confinement brings about drastic changes in the thermodynamic properties of non-reactive fluids, such as narrowing the vapor-liquid coexistence curve, lowering the pore critical temperature, increasing the average fluid densities in the pores, and causing the appearance of new types of phase transitions not found in the bulk phase.

In contrast, significantly less is known about the effects of confinement on chemical properties, particularly on chemical reaction equilibria. A chemical reaction confined to a nanosized environment can have a different equilibrium when compared to the same reaction in the bulk phase. For example, the nanopore

phase generally has a higher density than the corresponding bulk phase; from Le Chatelier's principle, this typically results in an increase in yield for reactions in which there is a decrease in the total number of moles across the reaction. Conversely, a drop in yield occurs in reactions when the number of moles increases. Further, some components of the reactive mixture are selectively adsorbed on the solid surfaces, also affecting the reaction equilibrium. Still further, molecular orientations can be strongly influenced by proximity to a solid surface, which can also shift the reaction equilibrium relative to the bulk phase equilibrium. Finally, phase transitions such as capillary condensation are expected to have a strong influence on the reaction conversion in nanopores.

Molecular-level simulation studies of the effects of confinement on reaction equilibria were pioneered by Borówko *et al.* [3, 4] for model reversible reactions in slit pores and by Turner *et al.* [5, 6, 7] for realistic, reversible reactions (nitric oxide dimerization and ammonia synthesis) in carbon micropores and carbon nanotubes. The study by Turner *et al.* [5] was inspired by the experimental work of Kaneko and co-workers [8, 9], who attempted to experimentally measure reaction equilibria in carbon nanopores. More recently, Peng *et al.* [10] simulated chemical reaction equilibria of ammonia synthesis in two porous materials (MCM-41 and pillared clays) and Hansen *et al.* [11] simulated the reaction equilibria of a metathesis reaction system in silicalite-1 pores.

All the above-mentioned simulations mainly focussed on determining the influence of the pore size on the equilibrium reaction conversion. In addition, they also studied the effects of chemical and physical surface heterogeneity on the conversion, as well as the variation of the equilibrium constant across the pore. These authors employed the Reaction Ensemble Monte Carlo (RxMC) simulation technique [12, 13, 14], which enables one to directly simulate the equilibrium properties of chemically reacting systems. The method requires only a knowledge of the intermolecular potentials of the reacting species and their ideal-gas properties, in addition to the system stoichiometry and the overall thermodynamic constraints.

In addition to these simulation and experimental studies, density functional theory (DFT) studies on model dimerization reactions in slit pores have also been performed by Tripathi and Chapman [15]. They studied the effects of the pore size and capillary condensation on the reaction equilibrium. DFT predicts an increase in the reaction conversion due to capillary condensation, with the impact being most significant in smaller pores.

In addition to having been studied previously, the nitric oxide dimerization reaction is interesting for a number of reasons. The reaction is an exothermic, thermodynamically driven reaction in which there is a decrease in the total number of moles. The reaction is important in atmospheric chemistry, as well as in the human body where it regulates blood pressure. Moreover, predicting the effects of confinement on NO dimerization is important to pollution abatement, since activated carbons are commonly used for the removal of nitrogen oxides from auto exhaust and industrial effluent gas streams. From a modeling standpoint, the NO dimerization reaction in carbon slit nanopores is an ideal candidate

reaction to simulate. Carbon nanopores exhibit quite strong solid-fluid interactions [1, 2] and the molecules involved in the reaction, NO and (NO)₂, are simple and easy to model. Due to the NO paramagnetism and (NO)₂ diamagnetism, the composition of the reactive mixture in activated carbons can be measured by magnetic susceptibility [8], providing experimental data for comparison with the theoretical calculations.

2 Reaction Ensemble Monte Carlo

The RxMC method [12, 13, 14] is a powerful simulation tool for studying chemically reacting mixtures. The method only requires knowledge of the intermolecular potentials and the ideal-gas properties of the reaction species that are present. Reactions are simulated by performing forward and reverse reaction steps according to the RxMC algorithm, which guarantees that the reaction equilibrium criteria for a set of R linearly independent chemical reactions involving N species

$$\sum_{i=1}^N \nu_{ji} \mu_i = 0 \quad j = 1, 2, \dots, R \quad (1)$$

are established [16]. In Eq. (1), ν_{ji} is the stoichiometric coefficient of species i in chemical reaction j and μ_i is its chemical potential. The reaction equilibrium condition for our NO dimerization reaction $2\text{NO} \rightleftharpoons (\text{NO})_2$ is

$$\mu_{(\text{NO})_2} - 2\mu_{\text{NO}} = 0 \quad (2)$$

Using the RxMC method, forward and reverse reaction steps are accepted with probabilities

$$\min \left[1, \frac{\Gamma}{V} \frac{N_{\text{NO}} (N_{\text{NO}} - 1)}{N_{(\text{NO})_2} + 1} \exp \left(-\frac{\Delta U}{k_{\text{B}} T} \right) \right] \quad (3)$$

and

$$\min \left[1, \frac{V}{\Gamma} \frac{N_{(\text{NO})_2}}{(N_{\text{NO}} + 1)(N_{\text{NO}} + 2)} \exp \left(-\frac{\Delta U}{k_{\text{B}} T} \right) \right] \quad (4)$$

respectively. In Eqs. (3) and (4), V is the system volume, T is the temperature, k_{B} is Boltzmann's constant, Γ is the ideal-gas quantity defined by

$$\Gamma = \frac{k_{\text{B}} T}{P^0} K \quad (5)$$

N_i is the number of particles of species i , ΔU is the change in the configurational energy U due to forward and reverse reaction attempts and K is the equilibrium constant, typically available in thermochemical tables [17].

Our simulations were carried out at fixed T and P of a bulk reservoir phase in equilibrium with fluid confined to a planar slit nanopore. Reaction steps and standard Monte Carlo displacement moves [18, 19] were carried out in both the bulk and nanopore phases. The simulation requires volume changes for the bulk

phase to maintain the specified pressure, along with species particle interchanges between the nanopore and bulk phases [20] to maintain phase equilibrium for each species. To maintain overall equilibrium, particle exchanges between the phases need only be performed for one species; for convenience, we selected the NO monomer, which is the smaller of the molecules in the reaction [5].

The nanopore consisted of two structureless confining walls separated by a distance H in the z -direction, with periodic boundary conditions applied in the x - and y -directions. The bulk phase was represented by a cubic simulation box with the minimum image convention and periodic boundary conditions. In the case of the nanopore phase, a cut-off equal to half the maximum box size was used, and the long-range correction for the configurational energy was ignored. In the case of the bulk phase, a spherical cut-off radius equal to half the box length was used and the long-range correction for the configurational energy was included [18], assuming that the radial distribution function is unity beyond the cut-off radius.

3 Molecular Model

3.1 Fluid-Fluid Interactions

As in the previous simulation studies of the NO dimerization reaction [5, 13], we used the model proposed by Kohler *et al.* [21] to describe intermolecular interactions in the mixture of NO and $(\text{NO})_2$. The model treats NO as a single Lennard-Jones (LJ) sphere and $(\text{NO})_2$ as a two-site LJ molecule with bond length l equal to the experimental value of 0.2237 nm. For the monomer, the model uses the LJ energy parameter $\varepsilon/k_B = 125.0$ K and the LJ size parameter $\sigma = 0.31715$ nm. The individual LJ parameters for each site in the dimer are the same as those for the monomer. Due to the weak dipole and quadrupole moments, the model neglects electrostatic forces.

3.2 Solid-Fluid Interaction

When simulating equilibrium fluid properties in carbon slit nanopores, it is possible to treat the walls as structureless [1]. In this case, a solid-fluid intermolecular potential is obtained by replacing the sum over solid-fluid particle interactions by a sum of integrals over wall atoms in a given plane. This is a reasonable approximation when the fluid molecule is large compared to the spacing between wall atoms. In graphitic carbons, the C-C spacing between surface carbon atoms is about 0.142 nm, and molecules such as NO ($\sigma = 0.31715$ nm) or $(\text{NO})_2$ ($\sigma = 0.31715$ nm, $l = 0.2237$ nm) feel only a rather small corrugation in the solid-fluid interaction as it moves parallel to the surface. Assuming a LJ potential for the wall atom-fluid interaction and integrating over the interactions with individual carbon atoms in each graphite plane, Steele [22] obtained the 10-4-3 potential for the interaction of a fluid atom with the graphite wall:

$$u_{sf}(z) = 2\pi\varepsilon_{sf}\sigma_{sf}^2\rho_s\Delta \left[\frac{2}{5} \left(\frac{\sigma_{sf}}{z} \right)^{10} - \left(\frac{\sigma_{sf}}{z} \right)^4 - \frac{\sigma_{sf}^4}{3\Delta(z+0.61\Delta)^3} \right] \quad (6)$$

In Eq. (6), z is the distance of the fluid atom from the graphite surface, ε_{sf} and σ_{sf} are the LJ potential parameters for the solid-fluid interaction, $\Delta = 0.335$ nm is the interplanar spacing in graphite and $\rho_s = 114$ nm⁻³ is the number density of carbon atoms. The ε_{sf} and σ_{sf} parameters are obtained from the Lorentz-Berthelot combining rules [18] with the carbon LJ potential parameters $\varepsilon_{ss}/k_B = 28$ K and $\sigma_{ss} = 0.340$ nm. For a slit nanopore of width H , the fluid molecule interacts with both graphite walls, so that the total solid-fluid interaction is given as the sum of $u_{sf}(z)$ and $u_{sf}(H - z)$.

4 Results and Discussion

4.1 Effects of Nanopore Width

We investigated the influence of the nanopore width on reaction conversion by performing two-phase reaction simulations, involving a bulk phase at pressure $P_{\text{bulk}} = 0.16$ bar at reaction equilibrium in equilibrium with an adsorbed phase in a model carbon slit nanopore. Temperatures were varied from 120 K to 160 K. Due to the low value of P_{bulk} , the RxMC simulations showed that the bulk phase behaves as an ideal-gas system and is predominantly monomeric, with about a 0.01 to 0.02 mole fraction of dimers.

Fig. 1 shows the yield of dimers and the average fluid density in the pore for the confined NO dimerization reaction as a function of the nanopore width and temperature. For comparison, the simulation results for the bulk vapor and

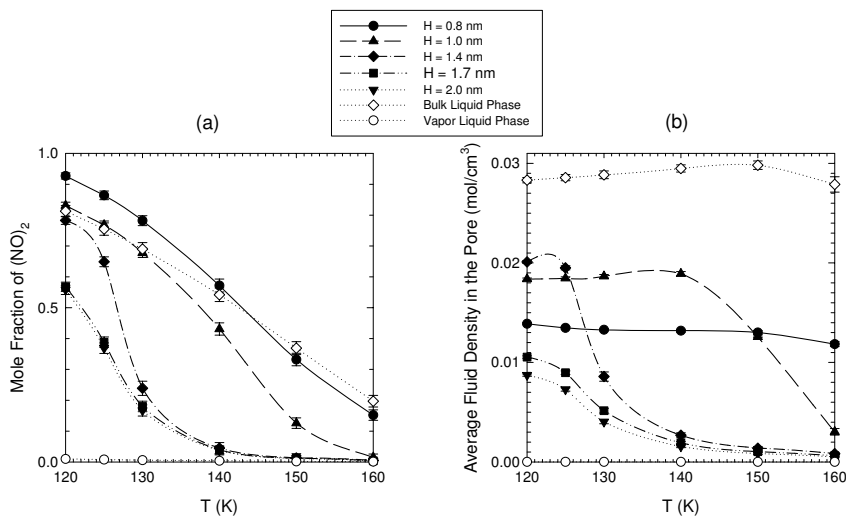


Fig. 1. (a) Mole fraction of $(\text{NO})_2$ dimers and (b) average fluid density as a function of temperature T in the model carbon slit nanopore of various widths H at a bulk pressure of 0.16 bar. For comparison, the simulation results for the bulk vapor and liquid phases are also included. Lines are drawn as a guide to the eye.

liquid phases at $P = 0.16$ bar are included. Fig. 1(a) shows a large enhancement of the equilibrium dimer formation in the nanopores in comparison with the corresponding bulk vapor-phase. The enhancement becomes greater as the nanopore width is reduced. For the nanopores with $H \geq 1.7$ nm, the influence of further increasing H becomes small. The previous studies of Turner *et al.* [5] and Tripathi and Chapman [15] resulted in similar findings.

The enhanced conversion is a result of two phenomena occurring simultaneously in the nanopore phase: (i) the increase in the average fluid density in the pore; and (ii) the preferential adsorption of the $(\text{NO})_2$ dimer on the nanopore surface. The enhanced conversion caused by the higher fluid density in the pore drives the reaction equilibrium towards the formation of more dimers, as seen in Fig. 1. For example, the density of the bulk vapor-phase at $T = 120$ K is about $0.16 \cdot 10^{-4}$ mol/cm³ while the corresponding average fluid density in the nanopores with $H = 0.8$ nm and 2.0 nm is approximately $0.14 \cdot 10^{-1}$ mol/cm³ and $0.87 \cdot 10^{-2}$ mol/cm³, respectively. On the other hand, the average fluid density in the nanopores is substantially lower than the density of the bulk liquid phase, while the reaction conversion in the nanopores with $H = 0.8$ nm and 1.0 nm is comparable with that for the bulk liquid-phase. This behavior is driven by the preferential adsorption of the dimer in the pore phase.

4.2 Impact of Capillary Condensation

Fig. 2 shows the equilibrium yield of dimers and the average fluid densities as a function of P_{bulk} for the $2\text{NO} \rightleftharpoons (\text{NO})_2$ system in nanopores with $H = 2.0$ nm.

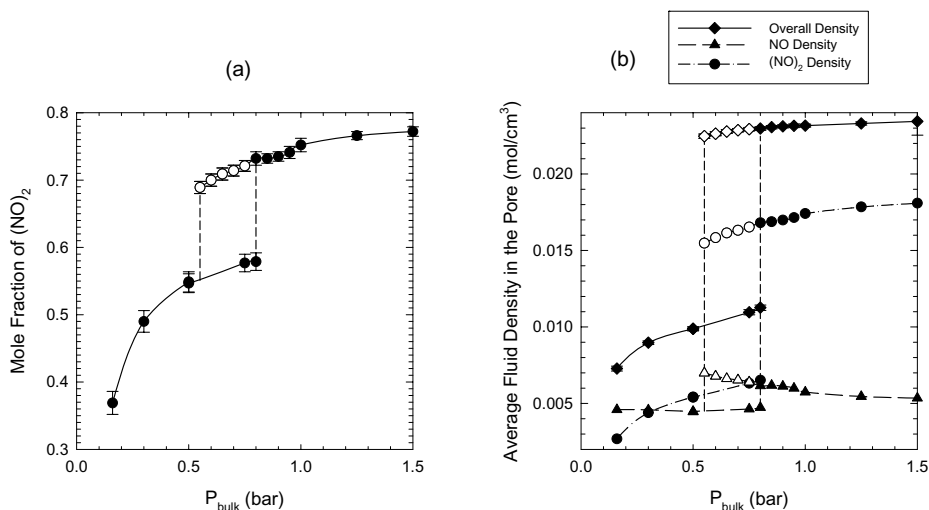


Fig. 2. (a) Mole fraction of $(\text{NO})_2$ dimers and (b) average fluid densities in the pore for the NO monomers and $(\text{NO})_2$ dimers, as a function of bulk pressure P_{bulk} in the model carbon slit nanopore of width 2.0 nm at a temperature of 125 K. Symbols are simulation results of this work and lines are drawn as a guide to the eye. Adsorption and desorption data points are shown as filled and open symbols, respectively.

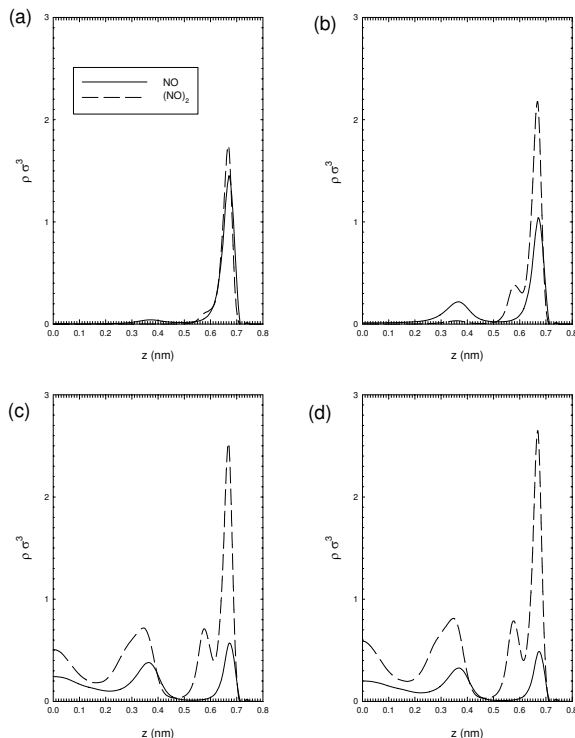


Fig. 3. Profiles of the NO and $(NO)_2$ reduced densities, $\rho\sigma^3$, in the model carbon slit nanopore of width 2.0 nm at a temperature of 125 K and at bulk pressures of (a) 0.30 bar, (b) 0.75 bar (prior to capillary condensation), (c) 0.85 bar (after capillary condensation), and (d) 1.50 bar; z is the distance from the center of the nanopore, which is located at $z = 0$. Due to nanopore symmetry, only half of the fluid density profiles are shown.

We observe a steep vertical rise in the adsorption/desorption isotherms for the dimer mole fractions (Fig. 2(a)) and for the average fluid densities in the pore (Fig. 2(b)) as a result of capillary condensation. Furthermore, hysteresis, widely regarded as a signature of capillary condensation [1], is clearly evident in these isotherms.

Closer inspection of Fig. 2 reveals some very interesting characteristics of the reactive system caused by capillary condensation. First, the reactants and products are in roughly equal proportion prior to capillary condensation, as seen in Fig. 2(a). However, after the onset of capillary condensation, the ratio of dimers to monomers changes to approximately 7:3, reaching a ratio of 8:2 at the highest P_{bulk} considered. Another interesting characteristic is that the increase in the overall average fluid density in the pore as a result of capillary condensation is very non-uniformly distributed between the monomers and the dimers as observed in Fig. 2(b).

The influence of capillary condensation on the structure of the confined reactive mixture of NO/(NO)₂ is elucidated in Fig. 3. Here, we display the profiles of the NO and (NO)₂ densities and simulation snapshots in the nanopore width $H = 2.0$ nm at two bulk pressures prior to capillary condensation, $P_{\text{bulk}} = 0.30$ bar and 0.75 bar (Figs. 3(a) and 3(b)), and at two bulk pressures after the onset of capillary condensation, $P_{\text{bulk}} = 0.85$ bar and 1.50 bar (Figs. 3(c) and 3(d)). Fig. 3 clearly shows the appearance and evolution of subsequent dense (condensation) layers of fluid molecules in the nanopore. The layer positioned around 0.7 nm from the nanopore centre corresponds to the location of the solid-fluid potential minimum. The appearance of these subsequent dense layers is manifested by the presence of additional peaks in the fluid density profiles. For the pre-condensation case $P_{\text{bulk}} = 0.30$ bar (Fig. 3(a)), the onset of another layer of NO molecules between 0.3 nm and 0.4 nm from the nanopore center is evident. Then just prior to capillary condensation, *i.e.* at $P_{\text{bulk}} = 0.75$ bar, this additional NO layer becomes further pronounced, while the onset of an additional layer of (NO)₂ molecules also positioned between 0.3 nm and 0.5 nm from the nanopore centre can be seen in Fig. 3(b). Finally, after capillary condensation, these additional NO and (NO)₂ layers further evolve along with the appearance of layers of NO and (NO)₂ molecules in the nanopore center as seen in Figs. 3(c) and 3(d).

5 Conclusions

The influence of confinement on chemical reaction equilibrium in nanoporous materials was studied in detail by means of the Reaction Ensemble Monte Carlo method for the nitric oxide dimerization reaction in model carbon slit nanopores. The effects of temperature, slit width, and capillary condensation on the reaction conversion and fluid structure have been reported and discussed.

A large increase in the equilibrium dimerization yield in the nanopore phase was found with respect to dimerization in the corresponding bulk phase. The dimerization yield increased by a factor of more than 80 for the smaller nanopores at the lower temperatures and low pressure. The enhanced dimerization is due to the combined effects of the increased fluid density in the nanopore phase and the preferential adsorption of the (NO)₂ dimer in the nanopore. Analogous to the bulk phase behavior, the dimerization yield decreases with increasing temperature. The influence of the bulk phase pressure on the reaction conversion is moderate, unless capillary condensation occurs in the nanopores, in which case it is quite dramatic. Capillary condensation changes the ratio of dimers to monomers from roughly 1:1 prior to capillary condensation to a ratio of 7:3 after capillary condensation. This enhanced dimerization yield is caused by an increase in the overall fluid density in the nanopores. However, this increase is not distributed uniformly between monomers and dimers. There is a significantly larger increase in the average dimer density in the pore than in the average monomer density in the pore upon capillary condensation.

Acknowledgment

This research was supported by the Grant Agency of the Czech Republic (Grant No. 203/05/0725), by the the National Research Programme "Information Society" (Project No. 1ET400720507) and by the National Research Council of Canada (Grant No. OGP 1041). Calculations were carried out in part on the SHARCNET (Shared Academic Hierarchical Computing Network), <http://www.sharcnet.ca>.

References

1. L. D. Gelb, K. E. Gubbins, R. Radhakrishnan and M. Sliwiska-Bartkowiak, *Rep. Prog. Phys.* 62, 1573 (1999).
2. T. J. Bandosz, M. J. Biggs, K. E. Gubbins, Y. Hattori, T. Iiyama, K. Kaneko, J. Pikunic and K. T. Thomson, *Chemistry and Physics of Carbon. Vol. 28* (L. R. Radovic, ed., Marcel Dekker, New York, 2003; pp. 41-228).
3. M. Borówko, A. Patrykiewicz, S. Sokołowski, R. Zagórski and O. Pizio, *Czech. J. Phys.* 48, 371 (1998).
4. M. Borówko and R. Zagórski, *J. Chem. Phys.* 114, 5397 (2001).
5. C. H. Turner, J. K. Johnson and K. E. Gubbins, *J. Chem. Phys.* 114, 1851 (2001).
6. C. H. Turner, J. Pikunic and K. E. Gubbins, *Molec. Phys.* 99, 1991 (2001).
7. C. H. Turner, J. K. Brennan, J. K. Johnson and K. E. Gubbins, *J. Chem. Phys.* 116, 2138 (2002).
8. K. Kaneko, N. Fukuzaki, K. Kakei, T. Suzuki and S. Ozeki, *Langmuir* 5, 960 (1989).
9. Y. Nishi, T. Suzuki and K. Kaneko, *J. Phys. Chem.* 101, 1938 (1997).
10. X. Peng, W. Wang and S. Huang, *Fl. Ph. Equilib.* 231, 138 (2005).
11. N. Hansen, S. Jakobtorweihen and F. J. Keil, *J. Chem. Phys.* 122, 164705 (2005).
12. W. R. Smith and B. Tříska, *J. Chem. Phys.* 100, 3019 (1994).
13. J. K. Johnson, A. Z. Panagiotopoulos and K. E. Gubbins, *Molec. Phys.* 81, 717 (1994).
14. M. Lísal, I. Nezbeda and W. R. Smith, *J. Chem. Phys.* 110, 8597 (1999).
15. S. Tripathi and W. G. Chapman, *J. Chem. Phys.* 118, 7993 (2003).
16. W. R. Smith and R. W. Missen, *Chemical Reaction Equilibrium Analysis: Theory and Algorithms* (Wiley-Interscience, New York, 1982; reprinted with corrections, Krieger Publishing, Malabar, FLA, 1991).
17. J. B. Pedley, *Thermodynamical Data and Structures of Organic Compounds* (TRC Data Series, Thermodynamic Research Center, College Station, Texas, 1994).
18. M. P. Allen and D. J. Tildesley, *Computer Simulation of Liquids* (Clarendon Press, Oxford, 1987).
19. D. Frenkel and B. Smit, *Understanding Molecular Simulation: From Algorithms to Applications* (Academic Press, London, 2002).
20. S. C. McGrother and K. E. Gubbins, *Molec. Phys.* 97, 955 (1999).
21. F. Kohler, M. Bohn, J. Fischer and R. Zimmermann, *Monatsh. Chem.* 118, 169 (1987).
22. W. A. Steele, *The Interaction of Gases with Solid Surfaces* (Pergamon Press, Oxford, 1974).

Multi-channel Estimation in Multiple Antenna MB-OFDM UWB System for Home Entertainment Network

Myung-Sun Baek¹, So-Young Yeo¹, Byung-Jun Jang²,
Young-Hwan You¹, and Hyoung-Kyu Song¹

¹ uT Communication Research Institute, Sejong University, Seoul, Korea

² School of Electrical Engineering, Kookmin University, Seoul, Korea
sabman@sju.ac.kr, yeosoh@sju.ac.kr, bjjang@kookmin.ac.kr,
yhyou@sejong.ac.kr, songhk@sejong.ac.kr

Abstract. The speedy dissemination of digital consumer electronics devices within home and personal area causes increments of multimedia communication and advent of entertainment networking. This feature of communication requires high data-rate transmission. In order to meet the demand, in this paper, a high-speed MB-OFDM system, proposal of 802.15.3a standard for WPAN, employing layered space-time architecture is considered for possible WPAN applications. The MB-OFDM system with multiple antennas increases the transmission rate efficiently with low multiplication operations. With an emphasis on a preamble design for multi-channel separation, we address a channel estimation in MB-OFDM with MIMO antenna system. By properly designing each preamble for multiple antennas to be orthogonal in time domain, the channel estimation can be applied to the MB-OFDM proposal for IEEE 802.15.3a standard in the case of more than two transmitting antennas.

1 Introduction

The speedy dissemination of digital consumer electronics devices within home and personal area, such as digital video disk (DVD) players, MP3 audio players, camcoders, and digital audio and television, causes increments of multimedia communication and advent of entertainment networking. In order to meet consumer's demand for low cost and high performance wireless entertainment network able to support streaming multimedia content and full motion video, ultra-wideband (UWB) technology is selected as a solution for the IEEE 802.15.3a standard [1]. The UWB has attracted considerable interest in the research and standardization communities, due to its promising ability to provide high data rate at low cost with relatively low power consumption [3]. In the standard of IEEE 802.15.3a, the data rate must be high enough (greater than 110 Mb/s) to satisfy a set of consumer multimedia industry needs for wireless personal area networks (WPAN) communication. The standard also address the quality of service (QoS) capabilities required to support multimedia data types [1][2]. The standard is focused on short distance wireless applications, connecting

multimedia devices such as cable/satellite settop boxes, DVDs, digital cameras, digital video recorders, TVs, displays (LCD, DLP, etc) and PCs over distances under 10 meters. So, higher rate and reliable transmission is required to satisfy the condition.

Conventionally, more bandwidth is required for higher data-rate transmission. However, due to spectral limitations, it is often impractical or sometimes very expensive to increase bandwidth. In this case, the scheme using the multiple transmitting and receiving antennas for spectrally efficient transmission is alternative solution [6][7]. Therefore, we apply multiple input multiple output (MIMO) architectures using Bell laboratories layered space-time (BLAST) concepts, which provides significant capacity gain in wireless channels to MB-OFDM system [7]. As an application of the MIMO architecture, a preamble structure for employing BLAST with more than two transmitting antennas is designed to be orthogonal in the time domain, and the channel estimation performance based on an investigated preamble structure is highlighted. The preamble architecture provides a feasible solution of the channel estimation without restoring channel samples corresponding to the number of substantial subcarriers used in data transmission by interpolation. The proposed preamble can be applied to preamble of the MB-OFDM proposal for IEEE 802.15.3a standard.

2 System Model

2.1 MB-OFDM Signaling for WPAN System

In the MB-OFDM system, the whole available ultra wideband spectrum between 3.1-10.6GHz is divided into several sub-bands with smaller bandwidth, whose bandwidth is approximately 500MHz [4][5]. In each sub-band a normal OFDM modulated signal with $K = 128$ subcarriers and QPSK modulation is used. The transmission is not done continually on all sub-bands. Different patterns of sub-band switching is chosen for different users (different piconets) such that the multiuser interference is minimized [4][5].

The transmitted signals can be described using a complex baseband signal notation. The actual RF transmitted signal is related to the complex baseband signal as follows

$$x_{RF}(t) = \text{Re} \left\{ \sum_{s=1}^{S-1} x^s(t - sT_l) e^{j2\pi f_s t} \right\} \quad (1)$$

where $\text{Re}(\cdot)$ represents the real part of a complex variable, $x^s(t)$ is the complex baseband signal of the s -th OFDM symbol and is nonzero over the interval from 0 to T_l , N is the number of OFDM symbols, T_l is the symbol interval, and f_s is the center frequency for the s -th band.

2.2 WPAN System Model with Multiple Antennas

Consider the MB-OFDM system link comprising M transmitting antennas and N receiving antennas. In the multi-antenna MB-OFDM system, antenna responds to each transmitting antenna through a statistically independent fading coefficient. The

received signals are corrupted by additive noise that is statistically independent among the N receivers. Let $\{X_i^s(k) | k = 0, \dots, K - 1\}$ denote the K subcarrier symbols where k and i represent the corresponding subcarrier and transmitting antenna in s -th sub-band, respectively. At the receiver, the output in the frequency domain is

$$\mathbf{R}^s = \mathbf{H}^s \mathbf{X}^s + \mathbf{W}^s \tag{2}$$

where \mathbf{H}^s is an $M \times N$ matrix of propagation coefficient which is statistically independent in s -th sub-band, circularly symmetric complex Gaussian ($CN(0,1)$), and \mathbf{w}^s is an N -dimensional column vector of additive noise whose elements are independent ($CN(0,1)$).

The receiver basically performs the reverse operations of the transmitter. After fast Fourier transform (FFT), the subcarriers are separated for multi-antenna processing.

3 Preamble Design for Multi-antenna MB-OFDM

In this section, assuming that the first step (context sensing) of context-aware action is executed, the multi-channel estimation processing of second step (context acquisition) is described.

In the WPAN system with MB-OFDM, the channel estimation is executed at the all sub-band. Therefore, for marking convenience, the sub-band index s is abbreviated. In the transmitter, the training sequence for the i -th antenna denoted by \mathbf{P}_i for $1 \leq i \leq M$ is designed to be orthogonal in the time domain and is transmitted from each antenna. For the notational convenience, we define an MN -dimensional vector of time-domain for transmitted training sequence as $\mathbf{p} = [\mathbf{p}_1 \mathbf{p}_2 \dots \mathbf{p}_M]^T$ with each element of $\mathbf{p}_i = [p_i(0) p_i(1) \dots p_i(K - 1)]^T$. If we denote \mathbf{P}_1 as a training sequence for the 1-st transmitting antenna, which is an K -dimensional vector with each component of all 1's, the training sequence for the i -th transmitting antenna denoted as \mathbf{P}_i for $1 \leq i \leq M$ is formulated as following rule:

$$\mathbf{P}_i = \mathbf{z}_i \mathbf{P}_1 = \mathbf{F} \mathbf{p}_i \tag{3}$$

where \mathbf{z}_i denotes an $K \times K$ diagonal matrix with each diagonal entry equal to $\exp\{j2\pi k d_i / N\}$ for the frequency-domain index $0 \leq k < N$, \mathbf{F} denotes an $K \times K$ FFT matrix and \mathbf{p}_i is the d_i -th cyclic shifted version of a time-domain, OFDM symbol of the 1-st transmitting antenna denoted as \mathbf{p}_1 .

For the notational convenience, in the following, we define \mathbf{P}_i as an $K \times K$ diagonal matrix given by $\mathbf{P}_i = \text{diag}(\mathbf{F} \mathbf{p}_i)$. For a given number of substantial subcarriers used in data modulation denoted by K , the maximum number of transmitting antennas M can be given by

$$M = \lceil K / \lambda \rceil \tag{4}$$

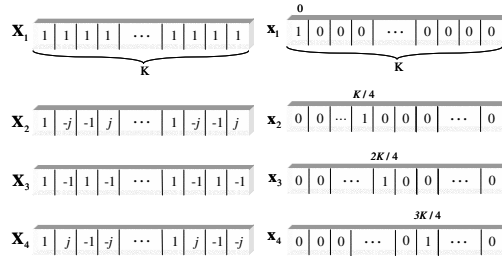


Fig. 1. Example of preamble pattern in the frequency and time domain ($M=4$)

where $\lceil m/n \rceil$ denotes the largest integer not exceeding m/n and λ is total number of channel paths. Considering eqn. (4), the time shift index d_i for each of M multiple transmitting antennas can be designed as $d_i = (i-1)\lceil K/M \rceil$ for $1 \leq i \leq M$, which guarantees each channel impulse response to be orthogonal in the time domain. When a design criterion of $\lceil K/M \rceil \geq \lambda$ is satisfied, the orthogonality is still maintained.

For fast time fading, moreover, a pilot-symbol-added LMMSE channel estimation should be properly designed to give accurate and effective estimation for tracking variations of channels between multiple transmitting antennas and receiving antennas [10]. In the case of four transmitting antennas, from eqn. (3), the preamble pattern in the frequency-domain and time-domain can be depicted as Fig.1.

4 Multi-channel Separation and Channel Estimation

For each transmitting antenna i , we assume that transmitted OFDM symbol goes through a multipath channel before reaching the j -th receiving antenna with the channel impulse response modeled by

$$\mathbf{h}_{ji} = [h_{ji}(0)h_{ji}(1) \cdots h_{ji}(\lambda-1)]^T. \quad (5)$$

If the preamble is carefully designed to satisfy the criteria of eqn. (3) and (4), the convolution terms received at the j -th receiving antenna $\{\mathbf{p}_i \otimes \mathbf{h}_{ji}\}$ are orthogonal in the time domain. After passing through a multipath channel, the received time-domain samples of an OFDM symbol from receiver j can be expressed as

$$\mathbf{r}_j = \sum_{i=0}^M \mathbf{p}_i \otimes \mathbf{h}_{ji} + \mathbf{w}_j = \sum_{i=0}^M \mathbf{c}_{ji} + \mathbf{w}_j \quad (6)$$

where \otimes represents K -point circular convolution, \mathbf{c}_{ji} which is the d_i -th cyclic shifted version of \mathbf{h}_{ji} is given by

$$\mathbf{c}_{ji} = \underbrace{[0 \cdots 0]_{d_i}}_{d_i} \underbrace{[h_{ji}(0)h_{ji}(1) \cdots h_{ji}(\lambda-1)]}_{K} \underbrace{[0 \cdots 0]}_{K-d_i} \quad (7)$$

and $\mathbf{w}_j = [w_j(0) w_j(1) \dots w_j(K-1)]^T$ are independent identically distributed additive white Gaussian noise (AWGN) samples with zero mean and variance of σ_t^2 .

Then, as shown in Fig. 2, by multiplying the received signal \mathbf{r}_j with a vector of a rectangular window function $\boldsymbol{\eta}$ with a size of $U_w = \lceil K/M \rceil$, the received signal \mathbf{r}_j is resolved into an $M \cdot N$ -dimensional received vector with the elements of each shifted channel impulse response from M transmitting antennas plus AWGN samples

$$\mathbf{r}_j' = \boldsymbol{\eta} \mathbf{r}_j = \mathbf{c}_j + \mathbf{w}_j' \tag{8}$$

where $\mathbf{c}_j = [\mathbf{c}_{j1} \mathbf{c}_{j2} \dots \mathbf{c}_{jM}]^T$, $\boldsymbol{\eta} = [\boldsymbol{\eta}_1 \boldsymbol{\eta}_2 \dots \boldsymbol{\eta}_M]^T$ is a vector of a rectangular window function with each component given by

$$\boldsymbol{\eta}_i = \text{diag}(\underbrace{0 \dots 0}_{d_i} \underbrace{1 \dots 1}_{U_w} \underbrace{0 \dots 0}_K) \tag{9}$$

and $\mathbf{w}_j' = [\mathbf{w}'_{j1} \mathbf{w}'_{j2} \dots \mathbf{w}'_{jM}]^T$ with

$$\mathbf{w}'_{ji} = [0 \dots 0 \underbrace{w_{ji}(d_i) w_{ji}(d_i+1) \dots w_{ji}(d_i+U_w-1)}_{U_w} 0 \dots 0]^T \tag{10}$$

Defining \mathfrak{S} being a vector of FFT matrix with the elements of F on its diagonal and assuming perfect synchronization, the FFT output of frequency-domain subcarrier can be expressed as

$$\mathbf{R}_j = \mathfrak{S} \mathbf{r}_j' = \mathbf{P} \mathbf{H}_j + \mathbf{N}_j \tag{11}$$

where \mathbf{P} is a matrix with each element of an $K \times K$ diagonal matrix \mathbf{P}_i on its diagonal, $\mathbf{H}_j = [\mathbf{H}_{j1} \mathbf{H}_{j2} \dots \mathbf{H}_{jM}]^T$ with each component of $\mathbf{H}_{ji} = \mathbf{F} \mathbf{h}_{ji}$, and $\mathbf{W}_j = [\mathbf{W}_{j1} \mathbf{W}_{j2} \dots \mathbf{W}_{jM}]^T$ with the elements of $\mathbf{W}_{ji} = \mathbf{F} \mathbf{w}'_{ji}$.

This estimated multi-channel information can be used for various adaptive techniques such as adaptive modulation, adaptive transmission power control and adaptive beam forming through feedback channel. These adaptive techniques are well adapted to the various user's demands and channel conditions and guarantee the acceptable QoS.

As described earlier, the number of transmitting antennas is selected according to the criterion of eqn. (4) for the given system and channel parameters of K and λ . Unfortunately, if a propagation length λ of exceeds the window size U_w due to incorrectly designed preamble architectures, the estimator results in an additional estimation error. Then, after the window operation according to eqn. (8), in the case of $U_w < \lambda$, the shifted channel impulse response from transmitter i to receiver j defined as \mathbf{c}_{ji} in eqn. (7) can be rewritten by

$$\mathbf{c}'_{ji} = [0 \dots 0 \underbrace{\mathbf{h}'_{ji}}_{d_i} 0 \dots 0]^T \tag{12}$$

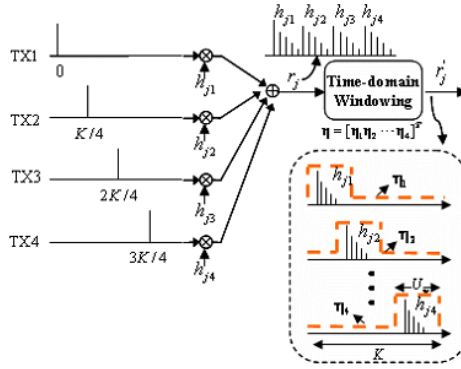


Fig. 2. Windowing process of channel estimation in the case of 4 transmitting antennas at the j -th receiving antenna

where \mathbf{h}'_{ji} is the U_w -dimensional partially overlapped and truncated channel impulse response vector and is given by

$$\mathbf{h}'_{ji} = [h'_{ji}(0) \cdots h'_{ji}(\lambda - U_w - 1) h'_{ji}(\lambda - U_w) \cdots h'_{ji}(U_w - 1)] \quad (13)$$

with $h'_{ji}(l) = h_{ji}(l) + h_{ji-1}(l + U_w)$.

Using eqn. (12) and (13) the received N -dimensional signal vector from transmitter i to receiver j can be expressed as

$$\mathbf{r}'_{ji} = \mathbf{c}'_{ji} + \mathbf{n}'_{ji} = \mathbf{c}_{ji} + \hat{\mathbf{c}}'_{ji-1} - \hat{\mathbf{c}}'_{ji} + \mathbf{w}'_{ji} \quad (14)$$

Where

$$\hat{\mathbf{c}}'_{ji} = [0 \cdots 0 \underbrace{h_{ji}(U_w)}_{d_i} \underbrace{h_{ji}(U_w + 1) \cdots h_{ji}(\lambda - 1)}_{\lambda - U_w} 0 \cdots 0]^T \quad (15)$$

In eqn. (13), two error terms $\hat{\mathbf{c}}'_{ji-1}$ and $\hat{\mathbf{c}}'_{ji}$ are the $\lambda - U_w$ overlapped channel impulse response from transmitter $i-1$ to receiver j with \mathbf{c}_{ji} and the $\lambda - U_w$ truncated channel impulse response from transmitter i to receiver j , respectively.

Finally, in the case of imperfect windowing, the FFT output from transmitter i to receiver j can be given by

$$\begin{aligned} \mathbf{R}_{ji} &= \mathbf{F} \mathbf{r}'_{ji} \\ &= \mathbf{P}_i \mathbf{H}_{ji} + \mathbf{P}_{i-1} \hat{\mathbf{H}}_{ji-1} - \mathbf{P}_i \hat{\mathbf{H}}_{ji} + \mathbf{W}'_{ji} \end{aligned} \quad (16)$$

where $\mathbf{P}_{i-1} \hat{\mathbf{H}}_{ji-1} = \mathbf{F} \hat{\mathbf{c}}'_{ji-1}$, $\mathbf{P}_i \hat{\mathbf{H}}_{ji} = \mathbf{F} \hat{\mathbf{c}}'_{ji}$, and $\mathbf{W}'_{ji} = \mathbf{F} \mathbf{w}'_{ji}$. Then, the least square (LS) estimates of \mathbf{H}_{ji} in eqn. (18) can be obtained by multiplying \mathbf{P}_i^{-1} with \mathbf{R}_{ji} as

$$\tilde{\mathbf{H}}_{ji} = \mathbf{H}_{ji} + \mathbf{P}_i^{-1} \mathbf{P}_{i-1} \hat{\mathbf{H}}_{ji-1} - \hat{\mathbf{H}}_{ji} + \mathbf{P}_i^{-1} \mathbf{W}'_{ji} \quad (17)$$

Based on the eqn. (16), the imperfect windowing gives the covariance matrix of LS estimation as follows

$$\mathbf{Y}_e = E\{\hat{\mathbf{H}}_{ji-1} \hat{\mathbf{H}}_{ji-1}^H\} + E\{\hat{\mathbf{H}}_{ji} \hat{\mathbf{H}}_{ji}^H\} + \frac{1}{\text{SNR}} \mathbf{I}_{N \times N} \quad (18)$$

where $\mathbf{I}_{N \times N}$ is an $N \times N$ identity matrix. Furthermore, the covariance matrix of the LMMSE estimation is given by

$$\mathbf{Y}_e = \mathbf{Y}_h - \mathbf{Y}_{hr} \mathbf{Y}_r^{-1} \mathbf{Y}_{rh} \quad (19)$$

with

$$\begin{aligned} \mathbf{Y}_{hr} &= E\{\mathbf{H}_{ji} \mathbf{R}_{ji}^H\} = E\{\mathbf{H}_{ji} \mathbf{H}_{ji}^H\} \mathbf{P}_i^H - E\{\mathbf{H}_{ji} \hat{\mathbf{H}}_{ji}^H\} \mathbf{P}_i^H \\ \mathbf{Y}_{rh} &= E\{\mathbf{R}_{ji} \mathbf{H}_{ji}^H\} = \mathbf{P}_i E\{\mathbf{H}_{ji} \mathbf{H}_{ji}^H\} - \mathbf{P}_i E\{\hat{\mathbf{H}}_{ji} \mathbf{H}_{ji}^H\} \\ \mathbf{Y}_r &= E\{\mathbf{R}_{ji} \mathbf{R}_{ji}^H\} \\ &= \mathbf{P}_i E\{\mathbf{H}_{ji} \mathbf{H}_{ji}^H\} \mathbf{P}_i^H + \mathbf{P}_{i-1} E\{\hat{\mathbf{H}}_{ji-1} \hat{\mathbf{H}}_{ji-1}^H\} \mathbf{P}_{i-1}^H \\ &\quad + \mathbf{P}_i E\{\hat{\mathbf{H}}_{ji} \hat{\mathbf{H}}_{ji}^H\} \mathbf{P}_i^H + E\{\mathbf{W}_{ji}' \mathbf{W}_{ji}^H\} \\ &\quad - \mathbf{P}_i E\{\mathbf{H}_{ji} \hat{\mathbf{H}}_{ji}^H\} \mathbf{P}_i^H - \mathbf{P}_i E\{\hat{\mathbf{H}}_{ji} \mathbf{H}_{ji}^H\} \mathbf{P}_i^H. \end{aligned} \quad (20)$$

6 Simulation Results and Discussion

To evaluate the multi-channel estimation performance, MB-OFDM system with FFT size of 128, zero padded prefix duration of 32, and guard interval (GI) of 5 is considered in a bandgroup 1 of CM2 UWB channel environment. The frequency and time spreading are not used.

In Fig.3 we plot the BER performance of LMMSE and perfect estimators according to the number of antennas. The performance difference between the LMMSE estimator and perfect estimator becomes similar for high SNR. In low SNR, on the other hand, the performance degradation of the LMMSE estimation for increasing the number of transmitting antennas is observed, which is due to the imperfect symbol cancellation based on the estimated channel information.

The MSE= $E[(\mathbf{H} - \hat{\mathbf{H}})]$ performance of the LMMSE estimator for various values of λ is depicted in Fig. 4. In this figure, the number of transmitting antennas is selected to be 4 according to the criterion of eqn. (4) for given parameters of $K = 128$ and $1 < \lambda \leq 32$, which corresponds to $U_w = 32$, and the curves corresponding to the perfect windowing ($16 < \lambda \leq U_w$) and the imperfect windowing ($U_w < \lambda$) are provided. The SNR gain of the best case of LMMSE estimator encountered $\lambda = 17$ is approximately 2dB, compared to the worst case of LMMSE estimator encountered with $\lambda = 32$.

Fig. 5 shows the effect of imperfect windowing on the MSE performance of both LS and LMMSE estimators for various values of λ and SNR. As a propagation

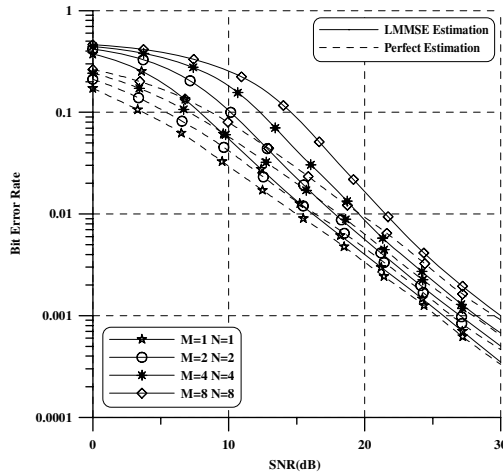


Fig. 3. BER performance of both perfect and LMMSE estimation according to the number of antennas

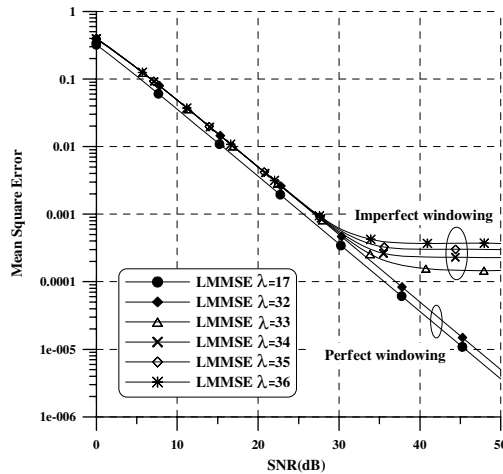


Fig. 4. MSE performance of LMMSE estimator according to the length of the channel impulse response with a selected value of $U_w = 32$ according to $K=128$ and $M=4$

length of λ exceeds the window size of $U_w = \lceil K/M \rceil$ due to imperfect windowing, the MSE of LS and LMMSE estimators increase. Up to SNR=35 (dB), however, the MSE degradation is negligible for some extra channel propagations and there is an irreducible MSE floor for relatively high SNR, which is due to the fact that the estimation error from imperfect windowing is a dominating term at the high SNR.

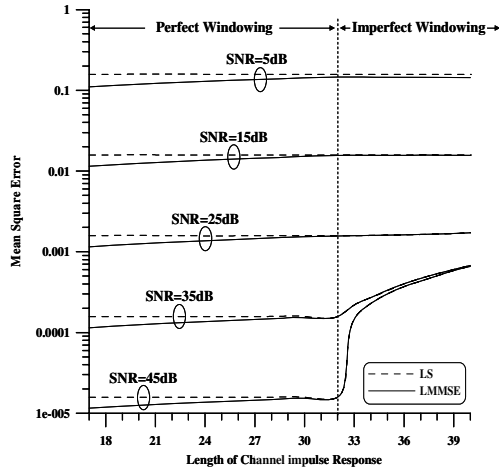


Fig. 5. MSE performance of both LS and LMMSE estimator according to the length L of the channel impulse response with a selected value of $U_w = 32$ according to $K=128$ and $M=4$

6 Conclusions

In this paper, we apply layered space-time architecture to MB-OFDM system based on ultra wideband WPAN for high-rate transmission. In the MB-OFDM system, the transmission rate can be increased efficiently with low multiplication operations by using the multiple transmitting and receiving antennas. Especially, as an application of a layered space-time architecture to MBOFDM system, we provide a new preamble structure and evaluate the channel estimation performance. The investigated preamble structure can estimate the multichannel applied to the MB-OFDM system for IEEE 802.15.3a standard.

Acknowledgement

This work is financially supported by the Ministry of Education and Human Resources Development (MOE), the Ministry of Commerce, Industry and Energy (MOCIE) and the Ministry of Labor (MOLAB) through the fostering project of the Lab of Excellency and is supported by MIC Frontier R&D Program in KOREA.

References

- [1] "IEEE 802.15 WPAN high rate alternative PHY Task Group 3a (TG3a) [Online]". Available: <http://www.ieee802.org/15/pub/TG3a.html>
- [2] E. Saberinia, A. H. Tewfik, "Multi-user UWB-OFDM Communications," *IEEE Trans. Wireless Communications*, vol.1, no.1, pp.127-130, August 2003.

- [3] Qinhua. Li, Leslie A. Rusch, "Multiuser Detection for DS-CDMA UWB in the Home Environment," *IEEE Trans. Wireless Communications*, vol. 20, no. 9, pp. 701-1711, December 2002.
- [4] "Multi-band OFDM Physical Layer Proposal for IEEE 802.15 Task Group 3a," *IEEE802.15-03/268r2*, January 2004.
- [5] E. Saberinia, A. H. Tewfik, C. Kai-Chuan, G. E. Sobelman, "Analog to digital converter resolution of multi-band ofdm and pulsed-ofdm ultra wideband systems," *Proc. CCSP*, vol. 32, no. 22, pp. 787-790, March 2004.
- [6] Y. (G.) Li, Jack H. Winters, and Nelson R. Sollenberger, "Signal detection for MIMO-OFDM wireless communications," *Proc. IEEE int. Conf. Commun*, vol.10, pp.3077-3081, June 2001.
- [7] G. J. Foschini, "Layered space-time architecture for wireless communications in a fading environment when using multi-element antennas," *Bell Labs Technical Journal*, vol. 1, no. 2, pp. 41-59, Autumn 1996.
- [8] T. Marzetta, "BLAST training : Estimating channel characteristics for high-capacity space-time wireless," *Proc. of 37th Annual Allerton Conf.*, pp. 958-966, Monticello, September 1999.
- [9] Q. Sun, D. C. Cox, H. C. Huang, and A. Lozano, "Estimation of continuous flat fading MIMO channel," *Proc. of WCNC2002*, pp. 189-193, March 2000.
- [10] W. G. Jeon, K. H. Paik, and Y. S. Cho, "Two-dimensional pilot-symbol-aided channel estimation for OFDM system with transmitter diversity," *IEICE Trans.Commun.*, vol. E85-B, no. 4, pp. 840-844, April 2002.

Compiler-Optimized Kernels: An Efficient Alternative to Hand-Coded Inner Kernels^{*}

José R. Herrero and Juan J. Navarro

Computer Architecture Dept., Univ. Politècnica de Catalunya,
Barcelona, Spain
{josepr, juanjo}@ac.upc.edu

Abstract. The use of highly optimized inner kernels is of paramount importance for obtaining efficient numerical algorithms. Often, such kernels are created by hand. In this paper, however, we present an alternative way to produce efficient matrix multiplication kernels based on a set of simple codes which can be parameterized at compilation time. Using the resulting kernels we have been able to produce high performance sparse and dense linear algebra codes on a variety of platforms.

1 Introduction

Creation of efficient code has traditionally been done manually using assembly language and based on a great knowledge of the target architecture. Such an approach, however cannot be easily undertaken for many target architectures and algorithms. Alternatively, codes specially optimized for a particular target computer can be written in a high level language [1, 2]. This approach avoids the use of the assembly language but keeps the difficulty of manually tuning the code. It still requires a deep knowledge of the target architecture and produces a code that, although portable, will rarely be efficient on a different platform. Many linear algebra codes can be implemented in terms of matrix multiplication [3, 4]. Thus, it is important to have efficient matrix multiplication routines at hand. The Fortran implementation of Basic Linear Algebra Subroutines (BLAS) [5] is inefficient, and developing efficient codes for a variety of platforms can take a great effort. Consequently, there have been attempts to produce such codes automatically. A new paradigm was created: Automated Empirical Optimization of Software (AEOS). The goal is to use empirical timings to adapt a package automatically to a new computer architecture. PHiPAC [6] was the first such project. Later, the Automatically Tuned Linear Algebra Software (ATLAS) project [7] appeared, which continues to date. Today, ATLAS-tuned libraries represent one of the most widely used libraries. ATLAS uses many well known optimization techniques developed by both linear algebra and compiler optimization experts. However, and despite its name, a great effort has been applied to produce high performance inner kernels for matrix multiplication using hand-coded routines

^{*} This work was supported by the Ministerio de Ciencia y Tecnología of Spain (TIN2004-07739-C02-01).

contributed by some experts. Directory `tune/blas/gemm/CASES` within the ATLAS distribution contains about 90 files which are, in most cases, written in assembler, or use some instructions written in assembler to do data prefetching. Often, one or more of these codes outperform the automatically generated codes. The best code is automatically selected as the inner kernel. The use of such hand-made inner kernels has improved significantly the overall performance of ATLAS subroutines on some platforms. Many processors have specific kernels built for them. However, there exist processors for which no such hand-made codes are available. Then, the performance obtained by ATLAS on the latter platforms is comparatively worse than that obtained on the former.

BLAS routines are usually optimized to deal with matrices of different sizes. One amongst several inner codes can be selected at runtime depending on matrix dimensions. This is very convenient for medium and large matrices of different sizes. When small matrices are provided as input, however, the overhead incurred becomes too large and the performance obtained is poor. There are applications which produce a large number of matrix operations on small matrices. For instance, programs which deal with sparse problems or multimedia codes. In those cases, the use of BLAS can be ineffective to provide high performance.

We are interested in obtaining efficient codes when working on both small and large matrices on a variety of platforms. For these purposes we have created a framework which allows us to produce ad hoc routines which can perform matrix multiplications quite efficiently operating on small matrices. Based on these routines, we have produced efficient implementations of both sparse and dense codes for several platforms. In the following sections we present our approach and comment on the results.

2 Generation of Efficient Inner Kernels for Matrix Multiplication

Our approach relies on the quality of code produced by current compilers. The resulting code is usually less efficient than that written manually by an expert. However, its performance can still be extremely good and sometimes it can yield even better code.

2.1 Taking Advantage of Compiler Optimizations

Compiler technology is a mature field. Many optimization techniques have been developed over the years. A very complete survey of compiler optimization techniques can be found in [8]. The knowledge of the target platform introduced in the compiler by its creators together with the use of well known optimization techniques such as software pipelining, loop unrolling, auto-vectorization, etc., can result in efficient codes which can exploit the processor's resources in an effective way. This is specially true when it is applied to highly regular codes such as a matrix multiplication kernel. Since many platforms have outstanding optimizing compilers available nowadays, we want to let the compiler do the creation of optimized object code for our inner kernels.

2.2 Smoothing the Way to the Compiler

The optimizations performed by the compiler can be favored by certain characteristics of the compiled code. For instance, some loop orders can be more beneficial than others. Some access patterns can be more effective in using memory. Knowing the number of iterations of a loop can help the compiler decide on the application of some techniques such as loop unrolling or software pipelining. We have taken this approach for creating a Small Matrix Library (SML). Basically, we:

- Provide the compiler with as much information as possible regarding matrix leading dimensions and loop trip counts;
- Try several variants of code, with different loop orders or unroll factors.

In addition, in some cases the resulting code can be more efficient if:

- Matrices are aligned;
- All matrices are accessed with stride one;
- Store operations are removed from the inner kernel.

2.3 Creation of a Small Matrix Library

For each desired operation, we have written a set of codes in Fortran. We concentrate on the matrix multiplication since it is one of the most important kernels. Figure 1a shows the performance of different routines for matrix multiplication for several matrix sizes on an Alpha-21164.¹ The matrix multiplication performed in all routines benchmarked uses: the first matrix without transposition (n); the second matrix transposed (t); and subtracts the result from the destination matrix (s). Thus, we call the vendor BLAS routine *dgemm_nts*.

The BLAS routine *dgemm_nts* yields very poor performance for very small matrices getting better results as matrix dimensions grow towards a size that fills the L1 cache (8 Kbytes for the Alpha-21164). This is due to the overhead of passing a large number of parameters, checking for their correctness, and scaling the matrices (*alpha* and *beta* parameters in *dgemm*). This overhead is negligible when the operation is performed on large matrices. However, it is notable when small matrices are multiplied. Also, since its code is prepared to deal with large matrices, further overhead can appear in the inner code by the use of techniques like strip mining.

A simple matrix multiplication routine *mxmlts_g* which avoids any parameter checking and scaling of matrices can outperform the BLAS for very small matrix sizes. Finally, our matrix multiplication code *mxmlts_fix* with leading dimensions and loop limits fixed at compilation time gets excellent performance for all block sizes ranging from 4x4 to 32x32. The latter is the maximum value that allows for a good use of the L1 cache on the Alpha unless tiling techniques are used.

¹ Labels in this figure refer to the three dimensions of the iteration space. However, for all the other figures matrices are assumed to be square and of equal size. In all plots the dashed line at the top shows the theoretical peak performance of the processor.

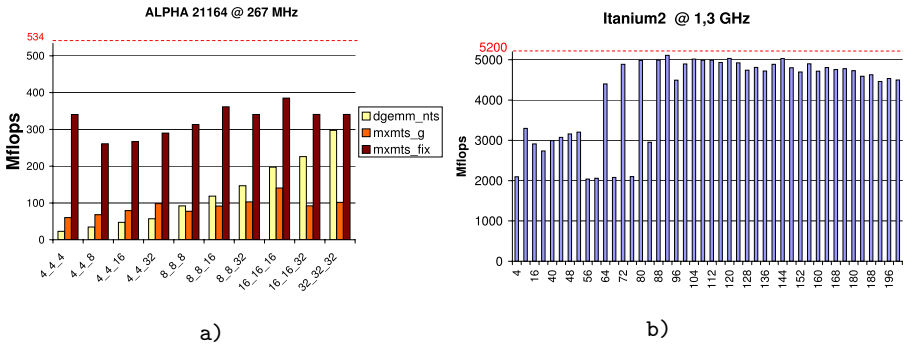


Fig. 1. a) Comparison of performance of different routines for several matrix sizes on an Alpha. **b)** Peak Mflops for SML matrix multiplication routines on an Itanium2.

For a matrix multiplication we have codes with different loop orders (kji , ijk , etc.) and unroll factors. We compile each of them using the native compiler and trying several optimization options. For each resulting executable, we automatically execute it and register its performance. These results are kept in a database and finally employed to produce a library using the best combination of parameters. This process is done automatically with a benchmarking tool [9]. By fixing the leading dimensions of matrices and the loop trip counts we have managed to obtain very efficient codes for matrix multiplication on small matrices. Since several parameters are fixed at compilation time the resulting object code is useful only for matrix operations conforming to these fixed values. Actual parameters of these routines are limited to the initial addresses of the matrices involved in the operation performed. Thus, there is one routine for each matrix size. Each one has its own name in the library. In this paper, however, we refer to any of them as *mxmts_fix*. The best loop order and unroll factor obtained for some matrix dimensions on one processor is not necessarily the best for other matrix dimensions or platforms. Choosing a single code for all cases would result in an important performance loss. We also tried feedback driven compilation using the Alpha native compiler but performance either remained the same or even decreased slightly. Results on the R10000 processor are similar to those of the Alpha with the only difference that the *mxmts_g* performs very well. This is due to the ability of the MIPSpro F77 compiler to produce software pipelined code, while the Alpha compiler hardly ever manages to do so. We conclude that, as long as a good compiler is available, fixing leading dimensions and loop limits is enough to produce high performance codes for very small dense matrix kernels. Further details can be found in [9].

Figure 1b shows the performance of SML matrix multiplication routines for several matrix sizes on an Itanium2 processor. It is interesting to note that the highest performance was obtained for matrix sizes which exceed the capacity of the level 1 (L1) data cache. The reason for this is that on such processor floating-point data never resides in L1 cache but in the upper levels [10]. Table 1

shows the minimum latency for floating-point loads in each cache level for the Alpha 21264 and the Itanium2 processors. The latency of a floating-point load which hits in the Itanium2 level i cache is similar to that of the Alpha level $i - 1$ cache. The Intel Fortran compiler applied the software pipelining technique automatically for tolerating such latency and produced efficient codes. Thus, for our SML matrix multiplication routines on the Itanium2 the best performance was obtained for matrices which exceed the capacity of the L1 data cache.

Table 1. Minimum floating-point load latency when load hits in cache

Cache Level	ALPHA 21264	Itanium2
L1	4	-
L2	13	6
L3	-	13

Originally, we have used this library in a sparse Cholesky factorization based on a hypermatrix data structure [11, 12]. Later we have used it on dense hypermatrix Cholesky factorization and multiplication ($C = C - A \times B^T$).

2.4 Using Hypermatrices to Exploit the Memory Hierarchy

We have used the hypermatrix data structure to adapt our codes to the underlying memory hierarchy. A hypermatrix is a hierarchical data structure with one or more levels of pointer matrices which must be followed to reach a final level of data submatrices. Our code can be parameterized with the number of pointer levels and block sizes mapped by each level.

Sparse Matrices. The application of SML routines to a sparse Cholesky factorization using a hypermatrix scheme has been presented in [13]. Their use improved the factorization efficiency about 12% on a given sparse matrix test suite.

Dense Matrices. The hypermatrix data structure can also be used for dense matrix computations. For the dense codes we follow the next approach: we choose the data submatrix block size according to the results obtained while creating our SML matrix multiplication routine. The one providing the best performance is taken. As seen above, we do this even when the matrix size is too large to fit in the L1 cache. Then, for the upper levels we choose multiples of the lower levels close to the value $\sqrt{C/2}$, where C is the cache size in double words. Such values are known to reduce cache conflicts due to accesses to the other matrices [14].

We found that, for the machines studied, we needed only two levels of pointers for dense operations. On matrix multiplication there is an improvement in the performance obtained when the upper level is orthogonal [15] to the lower. In this way the upper level cache is properly used. The performance improvement is modest, but results were always better than those corresponding to non-orthogonal block forms. On a MIPS R10000 processor we found that our code was outperforming both ATLAS and the vendor BLAS on dense Cholesky

factorization and matrix multiplication. The graph on the left part of figure 2 shows the performance obtained on this platform for a dense Cholesky factorization. The graph compares the results obtained by our code (labeled as HM) with those obtained by routine DPOTRF in the vendor library. Both when upper (U) or lower (L) matrices were input to this routine its performance was worse than that of our code.

We also tried the matrix multiplication operation $C = C - A * B^T$ since this is the one which takes about 90% of Cholesky factorization. The results can be seen in the right part of figure 2. Our code outperformed the DGEMM matrix multiplication routine in both the vendor and ATLAS libraries. We must note however, that ATLAS was not able to finish its installation process on this platform. Thus, we used a precompiled version of this library which corresponds to an old release of ATLAS. These preliminary results encouraged us to work on dense algorithms based on the hypermatrix data structure.

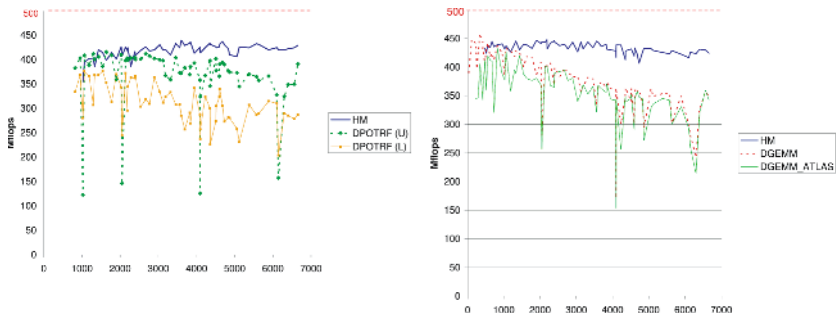


Fig. 2. Performance of dense Cholesky factorization (left) and matrix multiplication (right) on an R10000 processor

We have also compared our dense hypermatrix multiplication and Cholesky factorization with ATLAS DGEMM and DPOTRF routines on two other platforms. On an ALPHA-21264A ATLAS uses hand-made codes specially designed for this platform (Goto BLAS) and outperforms our matrix multiplication code. However, we obtain the same performance as DPOTRF for large matrices. On the Itanium2 our performance got close to ATLAS' both for DGEMM and DPOTRF. It was similar to ATLAS for large matrices. Details can be found in [15].

3 Extension: New Kernels and Matrix Storage

3.1 Generalization of the Matrix Multiplication Codes

We have generalized our matrix multiplication codes to be able to perform the matrix operations $C = \beta C + \alpha op(A) \times op(B)$ where α and β are scalars and $op(A)$ is A or A^t . Actually, we consider $\beta = 1$ since it is more efficient to perform the multiplication of matrix C by β before calling the matrix multiplication kernel

rather than performing this multiplication within it [16]. We allow values of 1 and -1 for α . We parameterize our kernels with preprocessor symbols which are adequately defined at compilation time to determine the type of operation performed. Thus, given a particular loop order and unroll factor, we can produce up to eight kernels: those corresponding to the combinations of transposition of matrices and values of α . The case $C = C + \alpha A^t \times B$ is particularly appealing since it allows accessing all three matrices with stride one. In addition, references to C can be hoisted from the inner loop. Thus, there are no stores in the inner loop. Actually, this is the kernel used in ATLAS. The experiments presented in the rest of the paper refer to this kernel.

3.2 Alignment

Contrary to what happens on other platforms tested, the results obtained for our matrix multiplication routines on an Intel Xeon were initially very poor. This machine allows for vectorization with the SSE2 instruction set [17]. The Intel Fortran compiler can take advantage of them. However, we were getting values around 2300 Mflops, when the theoretical peak for this machine is 4800. By forcing the alignment of matrices to 16, the Intel Fortran Compiler was able to vectorize the code, resulting in a substantial performance increase. The best case is that with $A^t \times B$ which gets a peak performance of 3810 Mflops. Table 2 summarizes these results. On this platform, as on the Itanium2, floating-point loads are not cached in the L1 cache. Thus, the block size automatically chosen (104) targets the L2 cache.

Table 2. Peak Mflops of inner kernel on a Pentium Xeon Northwood

	$A \times B^t$	$A^t \times B$
No align	3334	3220
Align	3457	3810

3.3 Adapting the Codes to the Memory Hierarchy

The use of hypermatrices on dense operations is inefficient both in terms of storage (keeping pointer matrices) and computation (following pointers and recursing through the data structure). The pointer matrices can be avoided for dense operations, keeping only data submatrices. These matrices can be accessed calculating their relative position. We store matrices as a set of submatrices in block major format. We call this scheme TDL in the graphs to refer to the two dimensional layout of data submatrices. In order to use the memory hierarchy we have codes which allow us to do tiling. We have written a code generator which can be used to produce codes with permutations of loop orders. Some of them can behave better than others [18, 19]. For the time being, however, the selection of one of these codes is not automated. We just run some executions and choose the one producing the best results. Block (tile) sizes are again chosen to be multiples of the lower levels close to the value $\sqrt{C}/2$, where C is the cache size in double words [14].

3.4 Results

We present results for matrix multiplication on three platforms. Each of them shows the results of DGEMM in ATLAS, Goto or the vendor BLAS, and TDL using our SML. Goto BLAS [20] are known to obtain excellent performance. They are coded in assembler and targeted to each particular platform. The dashed line at the top of each plot shows the theoretical peak performance of the processor.

For the Intel machines (figure 3) we have included the Mflops obtained with a version of the ATLAS library where the hand-made codes were not enabled at ATLAS installation time. We refer to this code in the graphs as 'nc ATLAS'. We can observe that in both cases ATLAS performance drops heavily. TDL with SML kernels obtain performance close to that of ATLAS on the Pentium 4 Xeon, similar to ATLAS on the Itanium2, and better than ATLAS on the Power4. For the latter we show the Mflops obtained by the vendor DGEMM routine which outperform both ATLAS and TDL (figure 4).

Results for TDL assume matrices already stored in block major format. Although new matrix storage formats have been proposed [21, 22, 23, 24] the matrix will probably need to be transformed from column major order into block major order. We have measured the time necessary to create the three matrices used

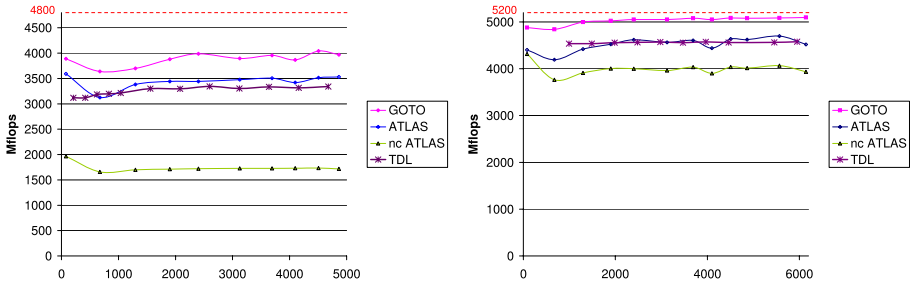


Fig. 3. Performance of dense matrix multiplication on an Intel Pentium 4 Xeon (left) and an Intel Itanium 2 processor (right)

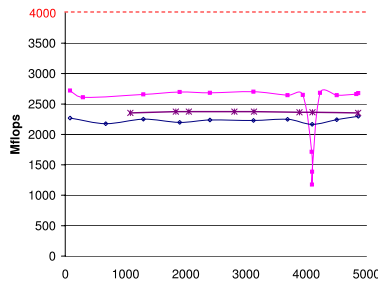


Fig. 4. Performance of dense matrix multiplication on a Power4 processor

in a matrix multiplication. Taking that into account, the performance of TDL drops by about 10% for small matrices, and as low as 1% for the largest matrices tested. The reason for this is that the cost of this transformation is $O(N^2)$ while for the multiplication the cost is $O(N^3)$.

4 Conclusions

Creation of efficient code has traditionally been done manually using assembly language and based on a great knowledge of the target architecture. Such an approach, however cannot be easily undertaken for many target architectures and algorithms. A cheaper approach relies on the quality of code produced by current compilers. The resulting code is usually less efficient than that written manually by an expert. However, its performance can still be extremely good and, in certain cases, it can yield even better code. We have taken this approach for creating our Small Matrix Library (SML). It is important to have data properly aligned and accessed with stride one. Loop orders which allow for the reduction of references to matrices in the inner loop favor performance. Situations where stores can be removed from the inner loop are specially beneficial. The inner kernel can target the first or the second level cache. The latter happens on processors which do not cache floating-point data in the level 1 cache.

The use of a simple two dimensional layout of data submatrices (TDL) avoids the overhead of a hypermatrix data structure, in which pointers have to be followed recursively, resulting in better performance.

Although our approach is not fully automatic as yet, we have been able to test it on several platforms and for many matrix sizes. We have shown that the results obtained on large dense matrices are close to those of hand-written matrix multiplication routines and can outperform ATLAS on some platforms. In addition, our approach can be used to produce efficient kernels for smaller matrix kernels which has been successfully used in a sparse Cholesky factorization. We believe this could also be useful in other types of applications such as multimedia codes.

References

1. Kamath, C., Ho, R., Manley, D.: DXML: A high-performance scientific subroutine library. *Digital Technical Journal* **6** (1994) 44–56
2. Navarro, J.J., García, E., Herrero, J.R.: Data prefetching and multilevel blocking for linear algebra operations. In: *Proceedings of the 10th international conference on Supercomputing*, ACM Press (1996) 109–116
3. Anderson, E., Bai, Z., Dongarra, J., Greenbaum, A., McKenney, A., Croz, J.D., Hammarling, S., Demmel, J., Bischof, C., Sorensen, D.: LAPACK: A portable linear algebra library for high-performance computers. In: *Proc. of Supercomputing '90*, IEEE Press (1990) 1–10
4. Kågström, B., Ling, P., van Loan, C.: Gemm-based level 3 blas: high-performance model implementations and performance evaluation benchmark. *ACM Transactions on Mathematical Software (TOMS)* **24** (1998) 268–302

5. Dongarra, J.J., Du Croz, J., Duff, I.S., Hammarling, S.: A set of level 3 basic linear algebra subprograms. *ACM Trans. Math. Software* **16** (1990) 1–17
6. Bilmes, J., Asanovic, K., Chin, C.W., Demmel, J.: Optimizing matrix multiply using PHiPAC: a portable, high-performance, ANSI C coding methodology. In: 11th ACM Int. Conf. on Supercomputing, ACM Press (1997) 340–347
7. Whaley, R.C., Dongarra, J.J.: Automatically tuned linear algebra software. In: Supercomputing '98, IEEE Computer Society (1998) 211–217
8. Bacon, D.F., Graham, S.L., Sharp, O.J.: Compiler transformations for high-performance computing. *ACM Computing Surveys* **26** (1994) 345–420
9. Herrero, J.R., Navarro, J.J.: Automatic benchmarking and optimization of codes: an experience with numerical kernels. In: Int. Conf. on Software Engineering Research and Practice, CSREA Press (2003) 701–706
10. Intel: Intel(R) Itanium(R) 2 processor reference manual for software development and optimization (2004)
11. Fuchs, G., Roy, J., Schrem, E.: Hypermatrix solution of large sets of symmetric positive-definite linear equations. *Comp. Meth. Appl. Mech. Eng.* **1** (1972) 197–216
12. Noor, A., Voigt, S.: Hypermatrix scheme for the STAR-100 computer. *Comp. & Struct.* **5** (1975) 287–296
13. Herrero, J.R., Navarro, J.J.: Improving Performance of Hypermatrix Cholesky Factorization. In: Euro-Par 2003, LNCS2790, Springer-Verlag (2003) 461–469
14. Lam, M., Rothberg, E., Wolf, M.: The cache performance and optimizations of blocked algorithms. In: Proceedings of ASPLOS'91. (1991) 67–74
15. Herrero, J.R., Navarro, J.J.: Adapting linear algebra codes to the memory hierarchy using a hypermatrix scheme. In: Int. Conf. on Parallel Processing and Applied Mathematics. (2005)
16. Daydé, M.J., Duff, I.S.: The use of computational kernels in full and sparse linear solvers, efficient code design on high-performance RISC processors. In: VECPAR. (1996) 108–139
17. SSE2: (Streaming SIMD Extensions 2 for the Pentium 4 processor) <http://www.intel.com/software/products/college/ia32/sse2>.
18. Gunnels, J.A., Henry, G., van de Geijn, R.A.: A family of high-performance matrix multiplication algorithms. In: International Conference on Computational Science (1). (2001) 51–60
19. Navarro, J.J., Juan, A., Lang, T.: MOB forms: A class of Multilevel Block Algorithms for dense linear algebra operations. In: Proceedings of the 8th International Conference on Supercomputing, ACM Press (1994)
20. Goto, K., van de Geijn, R.: On reducing TLB misses in matrix multiplication. Technical Report CS-TR-02-55, Univ. of Texas at Austin (2002)
21. Gustavson, F.G.: New generalized data structures for matrices lead to a variety of high performance algorithms. In: PPAM. (2001) 418–436
22. Andersen, B.S., Wasniewski, J., Gustavson, F.G.: A recursive formulation of Cholesky factorization of a matrix in packed storage. *ACM Transactions on Mathematical Software (TOMS)* **27** (2001) 214–244
23. Chatterjee, S., Lebeck, A.R., Patnala, P.K., Thottethodi, M.: Recursive array layouts and fast parallel matrix multiplication. In: Proc. of the 11th annual ACM symposium on Parallel algorithms and architectures, ACM Press (1999) 222–231
24. Valsalam, V., Skjellum, A.: A framework for high-performance matrix multiplication based on hierarchical abstractions, algorithms and optimized low-level kernels. *Concurrency and Computation: Practice and Experience* **14** (2002) 805–839

Noise Subspace Fuzzy C-Means Clustering for Robust Speech Recognition

J.M. Górriz¹, J. Ramírez¹, J.C. Segura¹,
C.G. Puntonet², and J.J. González²

¹ Dpt. Signal Theory, Networking and communications,
University of Granada, Spain
gorriz@ugr.es
<http://www.ugr.es/~gorriz>

² Dpt. Computer Architecture and Technology,
University of Granada, Spain

Abstract. In this paper a fuzzy C-means (FCM) based approach for speech/non-speech discrimination is developed to build an effective voice activity detection (VAD) algorithm. The proposed VAD method is based on a soft-decision clustering approach built over a ratio of subband energies that improves recognition performance in noisy environments. The accuracy of the FCM-VAD algorithm lies in the use of a decision function defined over a multiple-observation (MO) window of averaged subband energy ratio and the modeling of noise subspace into fuzzy prototypes. In addition, time efficiency is also reached due to the clustering approach which is fundamental in VAD real time applications, i.e. speech recognition. An exhaustive analysis on the Spanish SpeechDat-Car databases is conducted in order to assess the performance of the proposed method and to compare it to existing standard VAD methods. The results show improvements in detection accuracy over standard VADs and a representative set of recently reported VAD algorithms.

1 Introduction

The emerging wireless communication systems are demanding increasing levels of performance of speech processing systems working in noise adverse environments. These systems often benefit from using voice activity detectors (VADs) which are frequently used in such application scenarios for different purposes. Speech/non-speech detection is an unsolved problem in speech processing and affects numerous applications including robust speech recognition, discontinuous transmission, real-time speech transmission on the Internet or combined noise reduction and echo cancellation schemes in the context of telephony [1, 2]. The speech/non-speech classification task is not as trivial as it appears, and most of the VAD algorithms fail when the level of background noise increases. During the last decade, numerous researchers have developed different strategies for detecting speech on a noisy signal [3] and have evaluated the influence of the VAD effectiveness on the performance of speech processing systems [4]. Most of them have focussed on the development of robust algorithms with special attention on

the derivation and study of noise robust features and decision rules [5, 6, 7, 3]. The different approaches include those based on energy thresholds, pitch detection, spectrum analysis, zero-crossing rate, periodicity measure or combinations of different features.

The speech/pause discrimination can be described as an unsupervised learning problem. Clustering is one solution to this case where data is divided into groups which are related “in some sense”. Despite the simplicity of clustering algorithms, there is an increasing interest in the use of clustering methods in pattern recognition, image processing and information retrieval [9, 10]. Clustering has a rich history in other disciplines [11] such as machine learning, biology, psychiatry, psychology, archaeology, geology, geography, and marketing. Cluster analysis, also called data segmentation, has a variety of goals. All related to grouping or segmenting a collection of objects into subsets or “clusters” such that those within each cluster are more closely related to one another than objects assigned to different clusters. Cluster analysis is also used to form descriptive statistics to ascertain whether or not the data consist of a set of distinct subgroups, each group representing objects with substantially different properties.

2 A Suitable Model for VAD

Let $x(n)$ be a discrete time signal. Denote by y_j a frame of signal containing the elements:

$$\{x_i^j\} = \{x(i + j \cdot D)\}; \quad i = 1 \dots L \tag{1}$$

where D is the window shift and L is the number of samples in each frame. Consider the set of $2 \cdot m + 1$ frames $\{y_{l-m}, \dots, y_l, \dots, y_{l+m}\}$ centered on frame y_l , and denote by $Y(s, j)$, $j = l - m, \dots, l, \dots, l + m$ its Discrete Fourier Transform (DFT) resp.:

$$Y_j(\omega_s) \equiv Y(s, j) = \sum_{n=0}^{N_{FFT}-1} x(n + j \cdot D) \cdot \exp(-j \cdot n \cdot \omega_s). \tag{2}$$

where $\omega_s = \frac{2\pi \cdot s}{N_{FFT}}$, $0 \leq s \leq N_{FFT} - 1$ and N_{FFT} is the number of points or resolution used in the DFT (if $N_{FFT} > L$ then the DFT is padded with zeros). The energies for the l -th frame, $E(k, l)$, in K subbands ($k = 0, 1, \dots, K - 1$), are computed by means of:

$$E(k, l) = \left(\frac{K}{N_{FFT}} \sum_{s=s_k}^{s_{k+1}-1} |Y(s, l)|^2 \right) \tag{3}$$

$$s_k = \lfloor \frac{N_{FFT}}{2K} k \rfloor \quad k = 0, 1, \dots, K - 1$$

where an equally spaced subband assignment is used and $\lfloor \cdot \rfloor$ denotes the “floor” function. Hence, the signal energy is averaged over K subbands obtaining a suitable representation of the input signal for VAD [12], the observation vector at frame l , $\mathbf{E}(l) = (E(0, l), \dots, E(K - 1, l))^T$. The VAD decision rule is formulated

over a sliding multiple observation (MO) window consisting of $2m+1$ observation vectors around the frame for which the decision is being made (l), as we will show in the following sections. This strategy consisting on “long term information” provides very good results using several approaches for VAD such as [8] etc.

3 FCM Clustering over the Observation Vectors

CM clustering is a method for finding clusters and cluster centers in a set of unlabeled data. The number of cluster centers (prototypes) C is a priori known and the CM iteratively moves the centers to minimize the total within cluster variance. Given an initial set of centers the CM algorithm alternates two steps: a) for each cluster we identify the subset of training points (its cluster) that is closer to it than any other center; b) the means of each feature for the data points in each cluster are computed, and this mean vector becomes the new center for that cluster.

This previous clustering technique is referred to as hard or crisp clustering, which means that each individual is assigned to only one cluster. For FCM clustering, this restriction is relaxed, and the object can belong to all of the clusters with a certain degree of membership. This is particularly useful when the boundaries among the clusters are not well separated and ambiguous.

3.1 Noise Modeling

FCM is one of the most popular fuzzy clustering algorithms. FCM can be regarded as a generalization of ISODATA [13] and was realized by Bezdek [14]. In our algorithm, the fuzzy approach is applied to a set of N initial pause frames (energies) in order to characterize the noise space. From this energy noise space we obtain a set of clusters, namely noise prototypes¹. The process is as the following: each observation vector (\mathbf{E} from equation 3) is uniquely labeled, by the integer $i \in \{1, \dots, N\}$, and assigned to a prespecified number of prototypes $C < N$, labeled by an integer $c \in \{1, \dots, C\}$. The dissimilarity measure between observation vectors is the squared Euclidean distance:

$$d(\mathbf{E}_i, \mathbf{E}_j) = \sum_{k=0}^{K-1} (E(k, i) - E(k, j))^2 = \|\mathbf{E}_i - \mathbf{E}_j\|^2 \quad (4)$$

FCM attempts to find a partition (fuzzy prototypes) for a set of data points $\mathbf{E}_i \in \mathcal{R}^K$, $i = 1, \dots, N$ while minimizing the cost function

$$J(\mathbf{U}, \mathbf{M}) = \sum_{i=1}^C \sum_{j=1}^N (u_{ij})^m D_{ij} \quad (5)$$

¹ The word cluster is assigned to different classes of labeled data, that is \mathbf{K} is fixed to 2 (noise and speech frames).

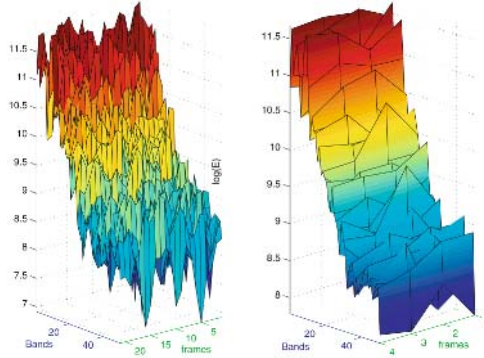


Fig. 1. a) 20 log Energies of noise frames, computed using $N_{FFT} = 256$, averaged over 50 subbands. b) Clustering approach applied to the a set of log-energies using hard decision CM ($C=4$ prototypes).

where $\mathbf{U} = [u_{ij}]_{C \times N}$ is the fuzzy partition matrix, $u_{ij} \in (0, 1)$ is the membership coefficient of the j -th individual in the i -th prototype; $\mathbf{M} = [\mathbf{m}_1, \dots, \mathbf{m}_C]$ denotes the cluster prototype (center) matrix, $m \in [1, \infty)$ is the fuzzification parameter (set to 2) and $D_{ij} = d(\mathbf{E}_j, \mathbf{m}_i)$ is the distance measure between \mathbf{E}_j and \mathbf{m}_i .

Thus, the loss function is minimized by assigning the N observations to the C prototypes with a certain degree of membership in such a way that within each prototype the average dissimilarity of the observations D_{ij} is minimized. Once convergence is reached, N K -dimensional pause frames are efficiently modeled by C K -dimensional noise prototype vectors denoted by \mathbf{m}_c , $c = 1, \dots, C$. In figure 1 we observed how the complex nature of noise can be simplified (smoothed) using a clustering approach (hard CM). The clustering approach speeds the decision function in a significant way since the dimension of feature vectors is reduced substantially ($N \rightarrow C$).

3.2 Soft Decision Function for VAD

In order to classify the second labeled data (energies of speech frames) we use a sequential algorithm scheme using a MO window centered at frame l , as shown in section 2. For this purpose let consider the same dissimilarity measure, a threshold of dissimilarity γ and the maximum clusters allowed $\mathbf{K} = 2$.

Let $\hat{\mathbf{E}}(l)$ be the decision feature vector that is based on the MO window as follows:

$$\hat{\mathbf{E}}(l) = \max\{\mathbf{E}(i)\}, \quad i = l - m, \dots, l + m \tag{6}$$

This selection of the feature vector describing the actual frame is useful as it detects the presence of voice beforehand (pause-speech transition) and holds the detection flag, smoothing the VAD decision (as a hangover based algorithm [7, 6] in speech-pause transition).

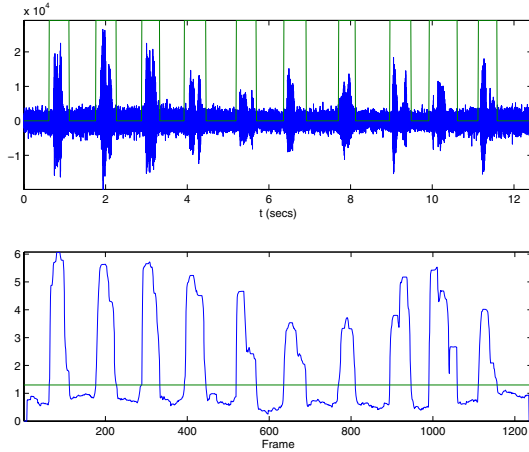


Fig. 2. VAD operation: Top- Decision function and threshold versus frames. Bottom- Input signal and VAD decision versus time.

Finally, the presence of a new cluster (speech frame detection) is satisfied if the following ratio holds:

$$F(l) = \log \left(\frac{1}{K} \sum_{k=0}^{K-1} \frac{\hat{E}(k, l)}{\langle \bar{\mathbf{m}}_c \rangle} \right) > \gamma \tag{7}$$

where $\langle \bar{\mathbf{m}}_c \rangle$ is the averaged noise prototype center and γ is the decision threshold.

The set of noise prototypes are updated in pause frames (not satisfying equation 7)) using the adaptation of the standard FCM, replacing the oldest energy in the noise model, consisting of N samples, by the actual feature vector $\hat{\mathbf{E}}(l)$. The initial prototype matrix $\mathbf{M}(l)$ at decision frame l is the previous one $\mathbf{M}(l - 1)$, and the following update is applied to the fuzzy partition and prototype center matrices:

$$\begin{aligned} u_{ij}^{(t+1)} &= 1 / \left(\sum_{l=1}^C (D_{lj} / D_{ij})^{1/(1-m)} \right) \\ \mathbf{m}_i^{(t+1)} &= \left(\sum_{j=1}^N \left(u_{ij}^{(t+1)} \right)^m \mathbf{E}_j \right) / \left(\sum_{j=1}^N \left(u_{ij}^{(t+1)} \right)^m \right) \\ \text{until } & \|\mathbf{M}^{(t+1)}(l) - \mathbf{M}^{(t)}(l)\| < \epsilon \\ \text{for } & i = 1, \dots, C, \quad j = 1, \dots, N \end{aligned} \tag{8}$$

This sequential adaptation doesn't involve high computational effort although other kind of static adaptation rules could be applied. The algorithm described so far is presented as pseudo-code in the following:

1. Initialize Noise Model:
 - Select N feature vectors $\{\mathbf{E}(i)\}, i = 1, \dots, N$.
 - Compute threshold γ .

2. Apply FCM clustering to feature vectors extracting C noise prototype centers $\{\mathbf{m}(c)\}, c = 1, \dots, C$
3. for $l = \text{init}$ to end
 - (a) Compute $\hat{\mathbf{E}}(l)$ over the MO window
 - (b) if equation 7 holds then $\text{VAD} = 1$
 else Update noise prototype centers $\mathbf{m}(c)$ with equations 8.

Figure 2 shows the operation of the proposed FCM-VAD on an utterance of the Spanish SpeechDat-Car (SDC) database [15]. The phonetic transcription is: “tres”, “nueve”, “zero”, “siete”, “ μ inko”, “dos”, “uno”, “otSo”, “seis”, “cuatro”. We also show the soft decision function and the selected threshold in the FCM-VAD operation for the same phrase.

4 Experimental Framework

Several experiments are commonly conducted to evaluate the performance of VAD algorithms. The analysis is normally focused on the determination of misclassification errors at different SNR levels [7], and the influence of the VAD decision on speech processing systems [4]. The experimental framework and the objective performance tests conducted to evaluate the proposed algorithm are described in this section. The ROC curves are used in this section for the evaluation of the proposed VAD. These plots describe completely the VAD error rate and show the trade-off between the speech and non-speech error probabilities as the threshold γ varies. The Spanish SpeechDat-Car database [15] was used in the analysis. This database contains recordings in a car environment from close-talking and hands-free microphones. Utterances from the close-talking device with an average SNR of about 25dB were labeled as speech or non-speech for reference while the VAD was evaluated on the hands-free microphone. Thus, the speech and non-speech hit rates ($HR1, HR0$) were determined as a function of the decision threshold γ for each of the VAD tested. Figure 3 shows the ROC curves in the most unfavorable conditions (high-speed, good road) with a 5 dB average SNR. It can be shown that increasing the number of observation vectors m improves the performance of the proposed FCM-VAD. The best results are obtained for $m = 8$ while increasing the number of observations over this value reports no additional improvements. The proposed VAD outperforms the Sohn’s VAD [3], which assumes a single observation likelihood ratio test (LRT) in the decision rule together with an HMM-based hangover mechanism, as well as standardized VADs such as G.729 and AMR [2, 1]. It also improve recently reported methods [3, 6, 5, 7]. Thus, the proposed VAD works with improved speech/non-speech hit rates when compared to the most relevant algorithms to date. Table 1 shows the recognition performance for the Spanish SDC database for the different training/test mismatch conditions (HM, high mismatch, MM: medium mismatch and WM: well matched) when WF and FD are performed on the base system [8]. The VAD outperforms all the algorithms used for reference, yielding relevant improvements in speech recognition.

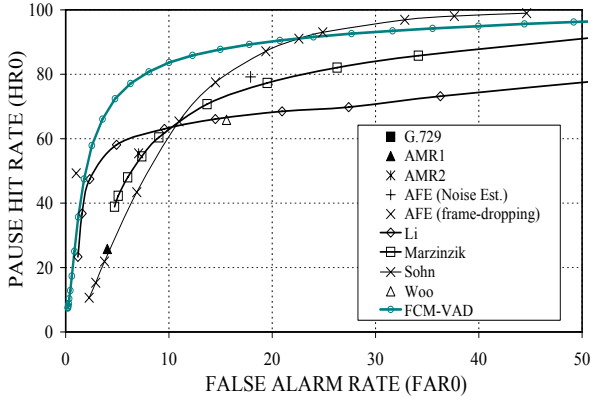


Fig. 3. ROC curves of proposed FCM-VAD in high noisy conditions for $m = 8$, $K = 32$ and $C = 2$ and comparison to standard and recently reported VADs

Table 1. Average word accuracy (%) for the Spanish SDC database

	Base	G.729	AMR1	AMR2	AFE
WM	92.94	88.62	94.65	95.67	95.28
MM	83.31	72.84	80.59	90.91	90.23
HM	51.55	65.50	62.41	85.77	77.53
Average	75.93	75.65	74.33	90.78	87.68
	Woo	Li	Marzinzik	Sohn	FCM-VAD
WM	95.35	91.82	94.29	96.07	96.68
MM	89.30	77.45	89.81	91.64	91.82
HM	83.64	78.52	79.43	84.03	86.05
Average	89.43	82.60	87.84	90.58	91.51

5 Conclusions

A new VAD for improving speech detection robustness in noisy environments is proposed. The proposed FCM-VAD is based on noise modeling using FCM clustering and benefits from long term information for the formulation of a soft decision rule. The proposed FCM-VAD outperformed Sohn’s VAD, that defines the LRT on a single observation, and other methods including the standardized G.729, AMR and AFE VADs, in addition to recently reported VADs. The VAD performs an advanced detection of beginnings and delayed detection of word endings which, in part, avoids having to include additional hangover schemes or noise reduction blocks. Obviously it also will improve the recognition rate when it is considered as part of a complete speech recognition system. The discrimination analysis or the ROC curves are effective to evaluate a given algorithm, the influence of the VAD in a speech recognition system depends on its discrimination accuracy [12]. Thus the proposed VAD improves the recognition rate when it is used as a part of a Automated Speech Recognition (ASR) system.

Acknowledgements

This work has received research funding from the EU 6th Framework Programme, under contract number IST-2002-507943 (HIWIRE, Human Input that Works in Real Environments) and SESIBONN and SR3-VoIP projects (TEC2004-06096-C03-00, TEC2004-03829/TCM) from the Spanish government. The views expressed here are those of the authors only. The Community is not liable for any use that may be made of the information contained therein.

References

1. ETSI, Voice Activity Detector (VAD) for Adaptive Multi-Rate (AMR) Speech Traffic Channels, 1999, ETSI EN 301 708 Recommendation.
2. ITU, A silence compression scheme for G.729 optimized for terminals conforming to recommendation V.70, 1996, ITU-T Recommendation G.729-Annex B.
3. J. Sohn, N. S. Kim and W. Sung, A statistical model-based voice activity detection, 1999, IEEE Signal Processing Letters, vol 16, num 1, pages 1-3,.
4. R. L. Bouquin-Jeannes and G. Faucon, Study of a voice activity detector and its influence on a noise reduction system, 1995, Speech Communication, vol 16, pages 245-254.
5. K. Woo, T. Yang, K. Park and C. Lee, Robust voice activity detection algorithm for estimating noise spectrum, 2000, Electronics Letters, vol 36, num 2, pages 180-181.
6. Q. Li, J. Zheng, A. Tsai and Q. Zhou, Robust endpoint detection and energy normalization for real-time speech and speaker recognition, 2002, IEEE Transactions on Speech and Audio Processing, vol 10, num 3, pages 146-157.
7. M. Marzinzik and B. Kollmeier, Speech pause detection for noise spectrum estimation by tracking power envelope dynamics, 2002, IEEE Transactions on Speech and Audio Processing, vol 10, num 6, pages 341-351.
8. J. Ramírez, José C. Segura, C. Benítez, L. García and A. Rubio, Statistical Voice Activity Detection using a Multiple Observation Likelihood Ratio Test, 2005, IEEE Signal Processing Letters, vol 12, num 10, pages 689-692.
9. Anderberg, M. R. 1973. Cluster Analysis for Applications. Academic Press, Inc., New York, NY.
10. Rasmussen, E. 1992. Clustering algorithms. In Information Retrieval: Data Structures and Algorithms, W. B. Frakes and R. Baeza-Yates, Eds. Prentice-Hall, Inc., Upper Saddle River, NJ, 419-442
11. Jain, A. K. and Dubes, R. C. 1988. Algorithms for Clustering Data. Prentice-Hall advanced reference series. Prentice-Hall, Inc., Upper Saddle River, NJ.
12. J. Ramírez, José C. Segura, C. Benítez, A. de la Torre, A. Rubio, An Effective Subband OSF-based VAD with Noise Reduction for Robust Speech Recognition, 2005, In press IEEE Trans. on Speech and Audio Processing.
13. J. Dunn, A fuzzy relative of the ISODATA process and its use in detecting compact well separated clusters, J. Cybern., vol. 3, no. 3, pp. 32-57, 1974.
14. J. Bezdek, Pattern Recognition with Fuzzy Objective Function Algorithms. New York: Plenum, 1981.
15. A. Moreno, L. Borge, D. Christoph, R. Gael, C. Khalid, E. Stephan and A. Jeffrey, SpeechDat-Car: A Large Speech Database for Automotive Environments, Proceedings of the II LREC Conference, 2000.

Using Box-Muller with Low Discrepancy Points

Tim Pillards and Ronald Cools

Katholieke Universiteit Leuven, Dept. of Computer Science,
Celestijnenlaan 200A, B-3001 Heverlee, Belgium

Abstract. To use quasi-Monte Carlo methods, the integral is usually first (implicitly) transformed to the unit cube. Integrals weighted with the multivariate normal density are usually transformed to the unit cube with the inverse of the multivariate normal cumulative distribution function. However, other transformations are possible, amongst which the transformation by Box and Muller. The danger in using a non-separable transformation is that it might break the low discrepancy structure which makes quasi-Monte Carlo converge faster than regular Monte Carlo. We examine several transformations visually, theoretically and practically and show that it is sometimes preferable to use other transformations than the inverse cumulative distribution function.

1 Introduction

For quasi-Monte Carlo methods, the common approach (see, e.g., [3, 8, 15]) to the approximation of an integral of a function f over \mathbb{R}^d weighted with the multivariate normal density ψ

$$I[f] := \int_{\mathbb{R}^d} f(\mathbf{x})\psi(\mathbf{x})d\mathbf{x} \quad (1)$$

is to transform the integral to the unit cube $I_d := [0, 1]^d$ using the inverse of the multivariate normal cumulative distribution function Ψ

$$I[f] = \int_{I_d} f(\Psi^{-1}(\mathbf{x}))d\mathbf{x} \quad (2)$$

and use a cubature rule of the form

$$Q[f] := \frac{1}{N} \sum_{\mathbf{y}_n \in P_N} f(\Psi^{-1}(\mathbf{y}_n)).$$

Here $P_N \subset [0, 1]^d$ is a low-discrepancy point set with $\#P_N = N$. Several kinds of discrepancy exist. In this article we choose the extreme star discrepancy.

Definition 1. Let \mathcal{Y} be the set of all subintervals of I_d of the form $\prod_{i=j}^d [0, u_j)$, then the star discrepancy is defined as

$$D^*(P_N) := \sup_{U \in \mathcal{Y}} \left| \frac{A(U)}{N} - \text{vol}(U) \right|$$

with $A(U)$ the number of points of P_N inside U .

Using the variation in the sense of Hardy and Krause $V(f \circ \Psi^{-1})$ of a function $f \circ \Psi^{-1} : I_d \rightarrow \mathbb{R}$ as defined in, e.g., [7, 10], it is known that the error of the approximation is bounded by the following theorem.

Theorem 1 (Koksma-Hlawka). *For $f \circ \Psi^{-1} : I_d \rightarrow \mathbb{R}$ a function of bounded variation*

$$|I[f] - Q[f]| = \left| \int_{I_d} f(\Psi^{-1}(\mathbf{x})) d\mathbf{x} - \sum_{\mathbf{y}_n \in P} f(\Psi^{-1}(\mathbf{y}_n)) \right| \leq D^*(P_N) V(f \circ \Psi^{-1}).$$

We refer to [10] for a proof of this classical result and a general introduction on quasi-Monte Carlo methods. Point sequences exist that have a discrepancy of $\mathcal{O}(\log^d(N)/N)$. As the variation does not depend on N this is also the order of convergence for the quasi-Monte Carlo method.

We will first examine several transformations in $2D$. Not only does this make the transformations easier, it also makes it possible to compare the transformed point sets visually. In the following section we introduce the transformations. In Section 3 we compare these transformations theoretically, looking mostly at the variation of f after the transformation. We visually inspect the transformed point sets in Section 4. The point sets should be nicely distributed without gaps or clusters. In Section 5 we present the results of our experiments in two dimensions and we explore the higher dimensional case in Section 6.

2 Transformations

The inverse of the normal distribution function can not easily be evaluated. Several alternatives are known for Monte Carlo methods to generate normally distributed points (see, e.g., [4]). We will examine transformations for the bivariate and multivariate normal density, visually examine the transformed point sets and compare experimental results. Another challenge with integral (2) is that the transformation may introduce singularities and hence an infinite variation which means that we can no longer apply Theorem 1. A way to handle the singularity is to avoid it [7, 12]. Some point sets even have the added bonus of doing this automatically [13].

We will call the transformation which uses the inverse of the cumulative normal distribution “Inverse”. We will also examine two transformations based on the polar transformations by Box and Muller [1] and Marsaglia [9]. For a more elaborate explanation of these transformation see, e.g., [4].

The transformations for Monte Carlo methods are given by

1. Box-Muller ($\mathbf{x} \sim U(I_2)$)

$$T(x_1, x_2) = \sqrt{-2 \log(x_1)} (\cos(2\pi x_2), \sin(2\pi x_2))$$

2. Marsaglia ($\mathbf{x} \sim U(C_2)$)

$$T(x_1, x_2) = \sqrt{\frac{-2 \log(1 - r^2)}{r^2}} (x_1, x_2), \quad (3)$$

where C_2 is the two-dimensional unit ball and $r = \|\mathbf{x}\|_2$. We will use the transformation by Box and Muller and replacing the $U(I_2)$ points by a two-dimensional low discrepancy point set. We call the resulting transformation “Box-Muller”. In [9] Marsaglia mentions that using uniform $[-1, 1]^2$ points and dropping those that fall outside C_2 before using (3) is as easy, as accurate and faster than the transformation by Box and Muller. We will create low discrepancy points in C_2 by generating a low discrepancy point set on I_2 , transforming it to $[-1, 1]^2$ by $I_2 \rightarrow [-1, 1]^2 : (x_1, x_2) \mapsto (2x_1 - 1, 2x_2 - 1)$ and then dropping all points outside the unit ball. On these points, we will use transformation (3). We will call this transformation “Marsaglia”. The transformation by Marsaglia as described in [9] uses $\log(r^2)$ instead of $\log(1 - r^2)$ in (3). However, this transforms the origin to infinity and the border of C_2 to the origin. Using $\log(1 - r^2)$ makes the transformation map the origin to itself and transforms the border of C_2 to infinity.

3 Theoretical Analysis

“Inverse” transforms points which are uniformly distributed over I_d to normal distributed points. As we have seen in the previous section, this is not the only possible transformation. Integral (1) can be transformed by any transformation T given in Section 2 to

$$I[f] = \int_{I_d} f(T(\mathbf{x}))d\mathbf{x}. \tag{4}$$

An important measure of performance is the variation of $f \circ T$. Using the variation $V_{\mathbb{R}^d}$ on \mathbb{R}^d as defined, e.g., in [7], it can easily be proven for a separable transformation T (i.e. $(T(x_1, x_2, \dots, x_d)) = (T(x_1), T(x_2), \dots, T(x_d))$) that $V_{I_d}(f \circ T) = V_{\mathbb{R}^d}(f)$. “Inverse” is a separable transformation and this gives an error bound

$$|I[f] - Q[f]| \leq D^*(P_N)V_{\mathbb{R}^d}(f).$$

The other transformations are not separable.

Another difference comes from the polar character of “Box-Muller”. In two dimensions, if f is a radial function, meaning that $\exists h : f(x_1, x_2) = h(x_1^2 + x_2^2)$, then (4) can be written as

$$\begin{aligned} I[f] &= \int_0^1 \int_0^1 f(\sqrt{-2 \log(x_1)} (\cos(2\pi x_2), \sin(2\pi x_2))) dx_1 dx_2 \\ &= \int_0^1 h(-2 \log(x_1)) dx_1. \end{aligned}$$

And since the one-dimensional projection of a two-dimensional low discrepancy point set is a one-dimensional low discrepancy point set, this essentially reduces the problem to one dimension. We therefore expect “Box-Muller” to perform better for radial or nearly radial functions.

“Marsaglia” uses a cut from I_d to C_d . Cuts that are not parallel to the axes give infinite variation, which may not always be problematic (see, e.g., [2]), but it

means that Theorem 1 is no longer applicable. We therefore expect “Marsaglia” to perform better for functions which go smoothly to zero at infinity in such a way that $f \circ T$ and its derivative is zero at the border of C_2 . Dropping the points outside C_2 also means that for f a constant function, “Marsaglia” will have infinite variation, while for “Inverse” and “Box-Muller” the approximation of a constant function gives an exact result.

4 Visualization

Since

$$\frac{1}{N} \sum_{\mathbf{y}_n \in P_N} f(T(\mathbf{y}_n)) = \frac{1}{N} \sum_{\mathbf{y}'_n \in T(P_N)} f(\mathbf{y}'_n)$$

instead of examining at how a function $f : \mathbb{R}^d \rightarrow \mathbb{R}$ is transformed to $f \circ T : I_d \rightarrow \mathbb{R}$, we can also look at how a low discrepancy point set $P_N \subset I_d$ is transformed to $T(P_N) \subset \mathbb{R}^d$. As a low discrepancy point set on I_d , we choose lattice points since the structure in these points is more obvious than for other low discrepancy sequences.

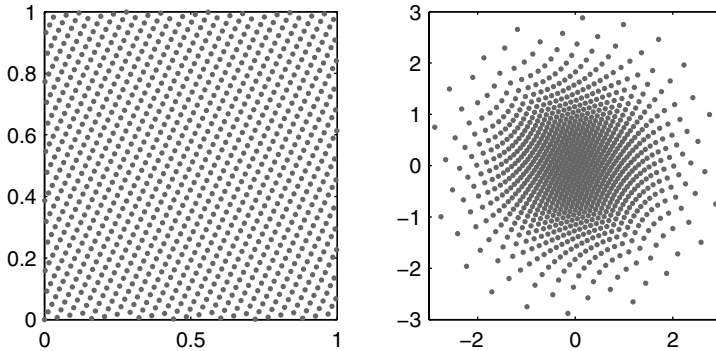


Fig. 1. Lattice points(left). Lattice points transformed with “Inverse”(right).

Fig. 1(left) shows a lattice with 1009 points generated by the fast algorithm in [11]. As can be seen in Fig. 1(right), “Inverse” gives nicely distributed points without clusters or open gaps. “Box-Muller” will use one dimension to determine the radius and one dimension to determine the angle of the new multivariate normal point set. Since the points of a lattice lay on straight lines, it is interesting to see how these lines are transformed by “Box-Muller” into spirals. We can recognize these spirals in the transformed point set (Fig. 2(left)). Looking at the transformed points, we see that they are evenly distributed and that no clusters of points are formed. “Marsaglia” first removes all points outside the unit ball and then expands the radius. We can see hyperbola-like forms in the transformed points (see Fig. 2(right)), but what is more important is that clusters appear at

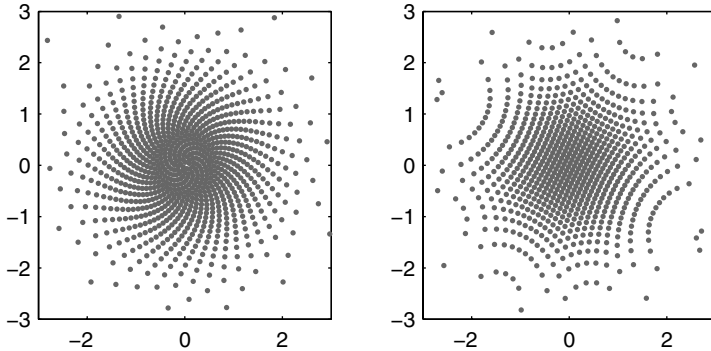


Fig. 2. Lattice points after transformation with “Box-Muller” (left) and “Marsaglia” (right)

the inner sides of these hyperbolas, with gaps in between the hyperbolas. We expect this to affect the performance of the approximation.

5 Two-Dimensional Experiments

We will approximate some integrals (1), combined with the transformations from Section 2, using points from a Sobol’ sequence [14]. We used two functions,

$$f_1(\mathbf{x}) = e^{-(\sin(x_1)+\cos(x_2))^2}$$

weighted with the standard normal density $\psi(\mathbf{x}) = \mathcal{N}(\mathbf{x}, 0, 1)$, and

$$f_2(\mathbf{x}) = \frac{1}{1 + \exp(-\sum_{i=1}^d x_i)} \tag{5}$$

weighted with the normal density $\psi(\mathbf{x}) = \mathcal{N}(\mathbf{x}, 0, \Sigma)$ where Σ is the $d \times d$ covariance matrix with elements

$$\Sigma_{ij} = \sigma_i^2 \quad \text{if } i = j \tag{6}$$

$$= \sigma_i \sigma_j \rho \quad \text{if } i \neq j. \tag{7}$$

For this example $d = 2$ and we choose $\sigma_1 = 1$, $\sigma_2 = 0.5$ and $\rho = 0.5$. This example is a maximum likelihood problem presented in [6]. We first performed a shift on the Sobol’ sequence and calculated the standard error over ten shifts. However, the standard error varied a lot from point to point and this makes the plots difficult to read. That’s why we decided to plot

$$E_{\max}(N) = \max_{n=N, N+1, \dots, 10^6} (\text{stderr}(n)). \tag{8}$$

For both test integrals, we see that the error for “Inverse” and “Box-Muller” is almost equal while “Marsaglia” gives worse results.

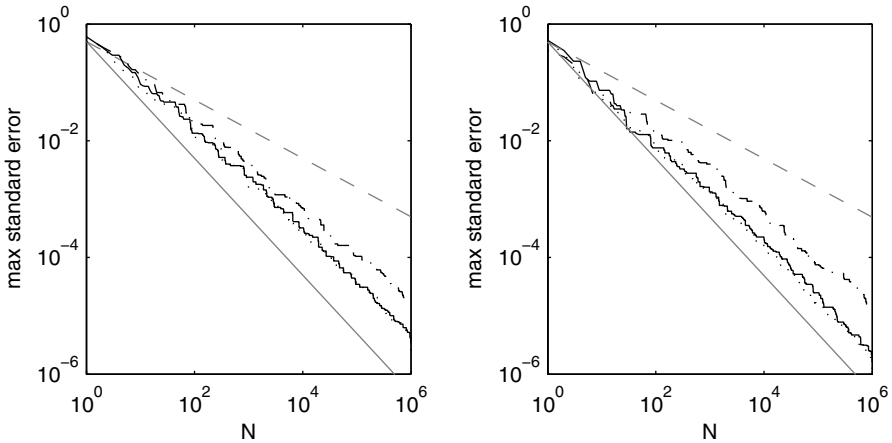


Fig. 3. Convergence of E_{\max} , a maximum over the standard error. Left: $\mathcal{N}(\mathbf{x}, 0, 1)$ with f_1 . Right: $\mathcal{N}(\mathbf{x}, 0, \Sigma)$ with f_2 . Legend: \cdots ="Inverse", $-\cdot-$ ="Box-Muller", $-\cdot-$ ="Marsaglia", gray lines: $-$ = $1/N$, $-\cdot-$ = $1/\sqrt{N}$.

6 Transformations for the Multivariate Normal Distribution

The results in two dimensions suggest that "Box-Muller" and "Inverse" produce the best results. The points are nicely structured without clusters or open spaces between them and the experimental results are also very good. Also theoretically the "Marsaglia" has no benefits compared to "Inverse" and "Box-Muller". Therefore we decided to generalize only "Box-Muller".

"Box-Muller" can be seen as two steps: First generating points on the surface of the ball and then generating the radius (e.g. [5] explains how low discrepancy points can be generated on the surface of a sphere). For multivariate Normal points the radius should be $\text{Gamma}(\frac{d}{2})$ distributed. For d even, two possibilities for generating the radius are the following.

1. Use an approximate inversion of the Gamma distribution. As with the normal distribution, no closed formula exists for the inversion of the gamma distribution but arbitrary precision can be reached although costly. We will call this transformation "GammaInverse".
2. The sum of $\frac{d}{2}$ exponentially distributed points is $\text{Gamma}(\frac{d}{2})$ distributed. For this approach we need a $(d - 1 + \frac{d}{2})$ -dimensional low discrepancy point set. The first $d - 1$ dimensions will be used to generate points on the surface of the ball and the other $\frac{d}{2}$ dimensions will be used to generate the radius. This does increase the dimension of the original problem. We will call this transformation "GammaSum".

Another approach is to generate the points per two dimensions. Starting with d dimensional low discrepancy points, we will transform every pair of dimensions

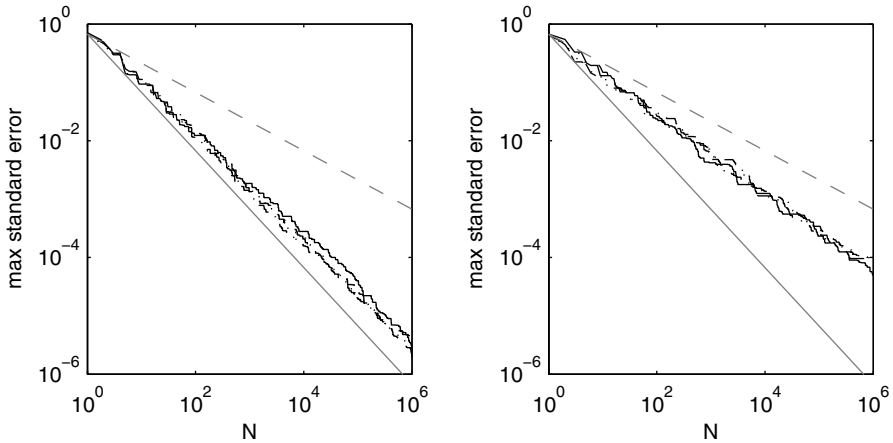


Fig. 4. Convergence of E_{\max} , a maximum over the standard error, for an easy (left) and a hard (right) maximum likelihood problem in ten dimensions. Legend: ---=“Inverse”, —=“Box-Muller”, ···=“GammaInverse”, ·-·=“GammaSum”, gray lines: — = $1/N$, --- = $1/\sqrt{N}$.

with “Box-Muller”. We will call this transformation “Batch”. We illustrate this with two instances from the maximum likelihood problem given in Section 5 with $f(\mathbf{x})$ as in (5) and $\psi(\mathbf{x}) = \mathcal{N}(\mathbf{x}, 0, \Sigma)$ multivariate normal with covariance matrix Σ as in (6-7). The first example uses

$$(\sigma_1, \sigma_2, \dots, \sigma_{10}) = (1.3, 1.9, 1.0, 1.7, 1.2, 1.4, 1.8, 1.1, 1.5, 1.6)$$

and $\rho = 0.9$. Because all σ_i are of the same order and ρ is relatively high, this problem is relatively easy. This can be seen in Fig. 4(left). The convergence order of E_{\max} (see (8)) is almost $1/N$. The second example uses

$$(\sigma_1, \sigma_2, \dots, \sigma_{10}) = (25.6, 1.6, 0.1, 12.8, 0.4, 0.2, 0.8, 3.2, 6.4, 51.2)$$

and $\rho = 0.3$. The large difference in magnitude of the σ_i and the fact that ρ is close to zero, causes the convergence to be closer to $1/\sqrt{N}$ (see Fig. 4(right)). For both experiments the difference in performance between the transformations is negligible. Other experiments with different values for σ and ρ gave similar results.

7 Conclusions

In two dimensions we compared how lattice points are transformed by several transformation often used by Monte Carlo methods, and experimented with some test-functions. “Box-Muller” and “Inverse” both produces nicely distributed points without clusters or open gaps and also perform well for the test-functions. The difference between these transformations is that “Inverse” has

the benefit of being separable while “Box-Muller” is less expensive to compute and reduces the dimension of radial integrals. Cutting off the points from I_d to C_d caused “Marsaglia” to perform worse theoretically, visually and during the experiments. Polar transformations like “Box-Muller” are not nearly as simple in more dimension as they are in two dimensions. We examined three generalizations. Our experiments did not show a significant difference in performance for either transformation. Since “Batch” is the fastest transformation considered, our preference goes to this transformation.

Acknowledgements

This research is part of a project financially supported by the Onderzoeksfonds K.U.Leuven/ Research Fund K.U.Leuven.

References

1. G. E. P. Box and M. E. Muller, *A note on the generation of random normal deviates*, Ann. Math. Stat. 29, pp. 610-611, 1958.
2. M. Berblinger, Ch. Schlier and T. Weiss, *Monte Carlo integration with quasi-random numbers: experience with discontinuous integrands*, Computer Physics Communications, 99 pp. 151-162, 1997.
3. R. Cools, D. Nuyens, *The role of structured matrices for the construction of integration lattices*, submitted.
4. L. Devroye, *Non-uniform random variate generation*, Springer-Verlag, New York, 1986.
5. K.-T. Fang and Y. Wang, *Number theoretic methods in statistics*, Chapman and Hall, London, 1994.
6. J. González, F. Tuerlinckx, P. De Boeck and R. Cools, *Numerical integration in logistic-normal models*, submitted.
7. J. Hartinger, R.F. Kainhofer, R.F. Tichy, *Quasi-Monte Carlo algorithms for unbounded, weighted integration problems*, Journal of Complexity 20(5), pp. 654-668, 2004.
8. C. Lemieux and P. L’Ecuyer, *Efficiency improvement by lattice rules for pricing Asian options*, WSC ’98: Proceedings of the 30th conference on Winter simulation, 1998, IEEE Computer Society Press.
9. G. Marsaglia, T. A. Bray *A convenient method for generating normal variables* SIAM Review 6(3), pp. 260-264, 1964.
10. H. Niederreiter, *Random number generation and quasi-Monte Carlo methods*, volume 63 of *CBMS-NSF regional conference series in applied mathematics*, SIAM, Philadelphia, 1992.
11. D. Nuyens, R. Cools, *Fast component-by-component construction, a reprise for different kernels*, Monte Carlo and Quasi-Monte Carlo Methods 2004 (H. Niederreiter, Harald, D. Talay), pp. 371-385, Springer-Verlag, Berlin, 2006.
12. A. B. Owen, *Quasi-Monte Carlo for integrands with point singularities at unknown locations*, Monte Carlo and Quasi-Monte Carlo Methods 2004 (H. Niederreiter, Harald, D. Talay), pp. 403-418, Springer-Verlag, Berlin, 2006.

13. A. B. Owen, *Halton sequences avoid the origin*, SIAM Review 48. To appear.
14. I. M. Sobol', *On the distribution of points in a cube and the approximate evaluation of integrals*, Zh. Vychisl. Mat. i Mat. Fiz. 7(4), pp. 784-802, 1967.
15. S. H. Paskov, *New methodologies for valuing derivatives*, Mathematics of Derivative Securities (S. Pliska, M. Dempster eds.), pp. 545-582, Cambridge University Press, 1997.

A Fast Integration Method and Its Application in a Medical Physics Problem

Shujun Li¹, Elise de Doncker¹, Karlis Kaugars¹, and Haisen S. Li²

¹ Computer Science,
Western Michigan University
{sli, elise, kkaugars}@cs.wmich.edu
² Department of Radiation Oncology,
University of Florida
haisen@ufl.edu

Abstract. A numerical integration method is proposed to evaluate a very computationally expensive integration encountered in the analysis of the optimal dose grid size for the intensity modulated proton therapy (IMPT) fluence map optimization (FMO). The resolution analysis consists of obtaining the Fourier transform of the 3-dimensional (3D) dose function and then performing the inverse transform numerically. When the proton beam is at an angle with the dose grid, the Fourier transform of the 3D dose function contains integrals involving oscillatory sine and cosine functions and oscillates in all of its three dimensions. Because of the oscillatory behavior, it takes about 300 hours to compute the integration of the inverse Fourier transform to achieve a relative accuracy of 0.1 percent with a 2 GHz Intel PC and using an iterative division algorithm. The proposed method (subsequently referred to as *table method*) solves integration problems with a partially separated integrand by integrating the inner integral for a number of points of the outer integrand and finding the values of other evaluation points by interpolation. The table method reduces the computational time to less than one percent for the integration of the inverse Fourier transform. This method can also be used for other integration problems that fit the method application conditions.

1 The Integration Problem

The intensity modulated proton therapy fluence map optimization is performed based on a (discrete) set of dose values on a three-dimensional grid. The discrete dose is either the dose on grid vertices or the average dose over each voxel. It is well known that using a discrete dose distribution to represent a continuous dose distribution can create aliasing error if the dose grid size is not small enough or, in other words, the spatial sampling resolution is not high enough. An analytical method has been developed to estimate the optimal dose grid size (denoted by h), such that the accuracy of the FMO result is guaranteed during the phase of dose sampling and the superfluous computation is avoided [9]. The method is based on Fourier analysis and the Shannon-Nyquist sampling theorem [6, 3]. According to the theorem, if the dose function $D(x, y, z)$ is effectively band-limited in the Fourier frequency space and the spatial resolution $\frac{1}{h}$ is not high enough, the aliasing error caused by under-sampling is evaluated as

$$\begin{aligned} \Delta_h(x, y, z) &= D(x, y, z) \\ &\quad - \int_{-\frac{1}{2h}}^{\frac{1}{2h}} du \int_{-\frac{1}{2h}}^{\frac{1}{2h}} dv \int_{-\frac{1}{2h}}^{\frac{1}{2h}} dw \tilde{D}(u, v, w) e^{-i2\pi(ux+vy+wz)} \\ &= D(x, y, z) - \iiint_{(u,v,w) \in \mathbb{B}} \tilde{D}(u, v, w) e^{-i2\pi(ux+vy+wz)} dudvdw, \end{aligned} \tag{1}$$

where $D(x, y, z)$ is the 3D dose function, $\tilde{D}(u, v, w)$ is its Fourier transform, and \mathbb{B} is used to denote a cubic box of size $\frac{1}{h}$ centered at the origin of the coordinate system in the frequency space. A value of h is obtained by requiring

$$\frac{|\Delta_h(x, y, z)|}{D(x, y, z)} \times 100\% \leq 2\% \tag{2}$$

for different beam energies (about 50 MeV to 220 MeV).

When the beam is aligned with the dose grid, the Fourier transform of the 3D dose function was obtained as

$$\begin{aligned} \tilde{D}(u, v, w) &= \frac{2}{b} e^{-2\pi^2\sigma_l^2(u^2+v^2)} e^{-2\pi^2\sigma_z^2w^2} \times \\ &\quad \{ pR^{1/p} + [a \cos(2\pi R w) - 2\pi p w \sin(2\pi R w)] \int_0^R t^{1/p} \cos(2\pi w t) dt \\ &\quad + [a \sin(2\pi R w) + 2\pi p w \cos(2\pi R w)] \int_0^R t^{1/p} \sin(2\pi w t) dt \}, \end{aligned} \tag{3}$$

where R is the range of proton beam depending on the initial energy (from 1 cm to 30 cm for clinical application), and $a, b, \sigma_z,$ and σ_l are parameters depending on R and are used to describe the dose model together with p , which is approximately equal to 1.77 [9, 2, 12]. $\tilde{D}(u, v, w)$ oscillates intensively in the w direction. When the beam is at an angle with the dose grid, the orientation can be achieved by rotating the beam an angle θ about the y -axis, then an angle φ about the z -axis. Using polar coordinates, it is well-known in the field of medical imaging that rotating the spatial function rotates the Fourier transform over the same angle [9]. The change of the Fourier transform under the rotation is

$$\tilde{D}(u, v, w) \rightarrow \tilde{D}(\mathbf{R}_{zy}(\varphi, \theta) \cdot \begin{pmatrix} u \\ v \\ w \end{pmatrix}), \tag{4}$$

where

$$\mathbf{R}_{zy}(\varphi, \theta) = \begin{pmatrix} \cos(\varphi) \cos(\theta) & \sin(\varphi) \cos(\theta) & -\sin(\theta) \\ -\sin(\varphi) & \cos(\varphi) & 0 \\ \cos(\varphi) \sin(\theta) & \sin(\varphi) \sin(\theta) & \cos(\theta) \end{pmatrix}. \tag{5}$$

After the rotation, the Fourier transform $\tilde{D}(u, v, w)$ oscillates in each of the three dimensions, which makes the integration extremely computationally expensive. For the case where the beam is aligned with the dose grid, the available programs like Mathematica, MATLAB and Maple can evaluate the integral numerically. Otherwise, they can not handle the problem.

In the practical computation, (1) is rewritten to estimate the upper bound of the aliasing error $|\Delta_h(x, y, z)|$.

$$\Delta_h(x, y, z) = \iiint_{(u,v,w) \notin \mathbb{B}} \tilde{D}(u, v, w) e^{-i2\pi(ux+vy+wz)} dudvdw, \tag{6}$$

where the integration limit is from the cubic box surface to infinity. An upper bound of the aliasing error is

$$\delta_h = \iiint_{(u,v,w) \notin \mathbb{B}} |\tilde{D}(u, v, w)| dudvdw, \tag{7}$$

which is independent of position. The integral is then split into three workable integrals. Observing that $\tilde{D}(u, v, w)$ asymptotically approaches zero rapidly in each dimension (see (3) and Fig. 1(a)), the upper limits of the integral in Eq. (7) are truncated to $3 \times \frac{1}{h}$ in order to avoid integrating over an infinite region.

In [9], one of the integrations was attempted using the adaptive integration method DCUHRE [1]. With a 2 GHz Intel PC, it took about 300 hours to perform 70,000,000 integrand function evaluations to achieve a relative error of 0.1%. A parallel integration library from NAG (Numerical Algorithm Group) was run on 32 CPUs to scan h . This took 2 hours when the relative error tolerance for integration was set to 0.1%. The target of this paper is to find a fast and reliable numerical integration solution so that the computation can be done on a desktop PC.

2 Table Method for the Inner Integrals

We introduce the table method for numerical integration and use it to simplify the calculation of the inner integrals in (3). This method can be applied to a class of integration problems to reduce the dimensionality and the computational time.

2.1 Table Method

The integral of an n -dimensional function $f(x_1, x_2, \dots, x_n)$ over a hyper-rectangular region \mathcal{D} in \mathcal{R}^n is

$$I = \int_{\mathcal{D}} f(x_1, x_2, \dots, x_n) dx_1 \dots dx_n. \tag{8}$$

Under a condition of absolute integrability, this can be rewritten as

$$I = \int_{\mathcal{D}'} f_1(x_1, x_2, \dots, x_i) I_2(u_1, \dots, u_k) dx_1 \dots dx_i \tag{9}$$

where the u 's are functions of the variables of f_1 :

$$\begin{aligned} u_1 &= t_1(x_1, x_2, \dots, x_i), \\ u_2 &= t_2(x_1, x_2, \dots, x_i), \\ &\vdots \\ u_k &= t_k(x_1, x_2, \dots, x_i), \end{aligned} \tag{10}$$

and

$$I_2(u_1, \dots, u_k) = \int_{\mathcal{D}''} f_2(u_1, \dots, u_k, x_{i+1}, \dots, x_n) dx_{i+1} \dots dx_n. \tag{11}$$

A simple example is $u_1 = x_1, u_2 = x_2, \dots, u_k = x_k, (k \leq i)$. There are two extreme cases. If $k = 0$, the integrand $f(x_1, x_2, \dots, x_n)$ can be separated completely as the product of $f_1(x_1, x_2, \dots, x_i)$ and $f_2(x_{i+1}, \dots, x_n)$. In this case, the inner and the outer integrals can be computed independently for most problems. If $k = k, f(x_1, x_2, \dots, x_n)$ cannot be separated. In this case, the table method does not reduce the computational time.

If $k = 1$ and $i > 1$, the inner integral $I_2(u_1)$ is a function of u_1 . A one-dimensional (1D) array of $I_2(u_1)$ for a set of uniformly spaced u_1 can be computed. When computing the outer integral, the value of $I_2(u_1)$ for any u_1 can be approximated by interpolation. The interpolated result can be very accurate if the function $I_2(u_1)$ is well behaved and the size of the array is large enough. Two examples are listed below.

$$\begin{aligned} I' &= \int_0^1 \int_0^1 \sqrt{x_1^2 + x_2} dx_1 dx_2 \int_0^1 \sin(x_2 x_3) dx_3, \\ I'' &= \int_0^1 \int_0^1 \cos(x_1 x_2) dx_1 dx_2 \int_0^1 \frac{x_3}{\sqrt{x_1^2 + x_2^2 + x_3^2}} dx_3. \end{aligned} \tag{12}$$

For I'' , $u_1 = x_1^2 + x_2^2$, thus the range of the table for u_1 is $[0, 2]$.

If $k = 2$ and $i > 2$, the inner integral I_2 is a two-dimensional function of u_1 and u_2 . A two-dimensional array can be generated for interpolation.

If $k = 3$ and $i > 3$, I_2 is a 3D function of u_1, u_2 and u_3 . A uniformly spaced 3D grid is used to obtain the value of I_2 at an arbitrary point in its domain. In order to improve the accuracy, the number of evaluation points of $I_2(u_1, u_2, u_3)$ can be increased, depending on the behavior of the function I_2 .

For a function I_2 of higher dimensions, the table method may be useful in special situations. If $i = 1$ and $k = 1$, the table method does not appear to be useful, because the dimension of f_2 is already n .

The integral I may also be expressed as

$$\int_{\mathcal{D}'} f_1(x_1, x_2, \dots, x_i, I_2(u_1, \dots, u_k)) dx_1 \dots dx_i. \tag{13}$$

(1) is an example of this case.

2.2 Computation of the Inner Integrals

The parameters and numerical results in this article are based on an instance of the computation for $R = 2$ and $R = 30$. The scanning of h was not carried out.

The evaluation of $\tilde{D}(u, v, w)$ is dominated by the computation of the integrals

$$f_{\cos}(w) = \int_0^R t^{1/p} \cos(2\pi wt) dt, \tag{14}$$

and

$$f_{\sin}(w) = \int_0^R t^{1/p} \sin(2\pi wt) dt. \tag{15}$$

In practice, R ($= 1, 2, \dots, 30$) is the index of a loop. The range of w is determined by the integration limits. For a given R , (14) and (15) are functions of w , whose actual values are determined by values of u , v and w , via the rotation represented by (5). As part of a 3D integrand, (14) and (15) are computed repeatedly for the same or different value of w , if we use a traditional integration method. A number of integrals can be computed first and stored in tables. For an arbitrary value of w , if it is in the table, the corresponding integration result is retrieved directly, otherwise, the result can be obtained by interpolation using several (e.g., 6) neighborhood values of w (for a polynomial of degree 5).

The accuracy of the interpolated value depends on the accuracy of the integration results, the number of points in the table, and the behavior of $f_{\cos}(w)$ and $f_{\sin}(w)$. The range of w , which is $[-143, 143]$ is calculated from the ranges of u , v and w . Because of symmetry, we only consider $[0, 143]$. $f_{\cos}(w)$ is drawn for an increasing number of uniformly spaced points w to determine the table size. An interval of 0.001 (143,000 points) is adequate. For a relative error tolerance of 10^{-7} , it took 175 minutes to compute the table for $R = 30$. If 30 tables are needed, for the 30 indexes of R , the tables with the same lower limit 0 and upper limits less than 30 can be generated at the same time with virtually no extra cost, because R is the upper limit of the integral. The tables are saved in files in binary format for later use. Because of the oscillation of $f_{\cos}(w)$ and $f_{\sin}(w)$, a large number of sampling points is needed.

3 Computation Using the Adaptive Method

For 3D problems, there are three cubature rules for the adaptive methods in the parallel integration library PARINT [13]. IRULE_DIM3_DEG11 (a 3D rule of polynomial degree 11), IRULE_DEG9_OSCIL (a general multivariate rule of polynomial degree 9, preferred for oscillatory functions), and IRULE_DEG7 (a general multivariate rule of polynomial degree 7) are from Genz and Malik [7, 8], with refined error estimation techniques from [1]. We chose the 3D rule IRULE_DIM3_DEG11 because it is more efficient than the other two rules for our integration. The univariate rules used for the 1D adaptive methods are from the Quadpack package [11]. The simulation described in this and the next section was carried out on a PC with a 2.4 GHz CPU.

The table method reduced the run time dramatically. For 2,000,000 function evaluations, the table method took 6 seconds, while the method without using it took 1,675 seconds.

For $\theta = 30^\circ$ and $\varphi = 0^\circ$, we used the adaptive method to achieve a relative error of 10^{-3} . It took 266 and 337 seconds with 84,102,067 and 84,032,979 integrand evaluations for $R = 2$ and 30, respectively. We also increased the number of evaluations to 120 million to confirm the stability of the results.

An adaptive method is more efficient when the domain is decomposed along the oscillatory directions. For $\theta = 45^\circ$, $\varphi = 45^\circ$, it is difficult for the program to obtain a relative error of 10^{-3} , although the result is actually accurate enough as verified by the iterated method discussed below.

4 Verification Using the Iterated Method

Because of the oscillatory nature of the integrand, the adaptive method is not very efficient in further improving the accuracy of the integration result of our problem by increasing the number of function evaluations. In addition, when the number of regions in the heap of the program is large, the memory usage must be taken into account.

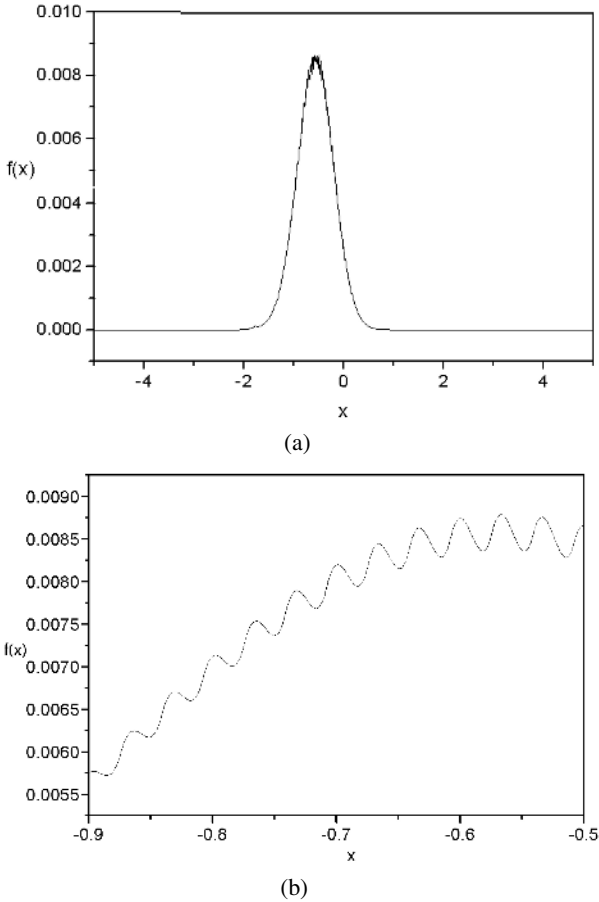


Fig. 1. The other two dimensions are aggregated to have function $f(u)$. (a) The curve is not smooth. (b) No numerical anomaly is found.

An iterated method uses lower-dimensional methods (1D, for example) to solve an integration problem [10, 4, 5]. For low-dimensional problems, it often outperforms other methods for many types of problems. We used a 1D adaptive routine based on a Gauss-Kronrod rule (Gauss 7 points - Kronrod 15 points) for each direction of the 3D function to perform the following simulations.

For an evaluation limit of 1,000 in each direction, the iterated method took more than 10 minutes to obtain a result similar to that of the adaptive method. However the

reported relative error 2.8×10^{-2} is larger than the relative error tolerance of 10^{-3} . For a relative error tolerance of 10^{-4} , the limit was then increased to 10,000 to get a more accurate result. The required accuracy was reached with 5,330,117,925 function evaluations in 6 hours and 26 minutes. This result can be used as a reference for the results of the former computations. If we take the latter result as the correct value, the relative error of the former will be 3.2×10^{-4} , which is less than 2.8×10^{-2} . The actual relative error of the latter should also be less than the reported value, 10^{-4} . A rough estimate can be 10^{-6} .

Because the error estimate of the 1D routine for some functions is too conservative, we proceeded to analyze the result by checking the evaluation points. Fig. 1(a) was drawn for the function $f(u)$ by aggregating (summing up) the integration results of the other two directions (v, w) for 525 points on the x -axis (x is used for u). We can see from the figure that the accuracy of the result is moderate. Fig. 1(b) shows part of 5,000 points on the x -axis of a computation, which indicates that there is no numerical anomaly in this direction.

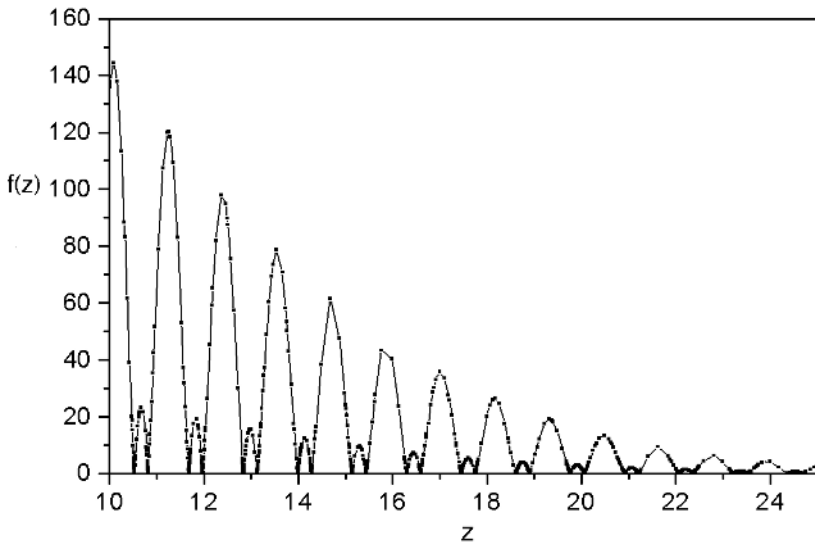


Fig. 2. Integrand function of a fixed point (u, v) as a function of w . Evaluation patterns are shown for the w direction integration.

The iterated method is very efficient for 3D problems. Fig. 2 shows the evaluation points on the z -axis (for w) for a point on the xy (or uv) plane. The oscillation and derivative discontinuities caused according to by (7) make the computation with current automatic routines very inefficient. We can reduce function evaluations by finding the zeros (see Fig. 2) and then integrating it over the regions between the zeros.

The results of this section confirm that the adaptive method is good enough to quickly compute even the difficult cases of the integrals.

5 Summary

We studied the nature of the inner integral for the aliasing error and found a solution to compute the integration effectively. When the variables of an integrand can be partially separated, the table method can be applied to reduce the dimensionality and the computational time. To use this method, the dimension of the problem should be greater than two. It is more efficient for fairly low dimensions. In practice, high-dimensional integrands are usually not easy to separate completely or partially. If the number of variables of the inner integral (not inner integrand) is not small, the size of the array (or the number of integrations of the inner integral) can be very large. Furthermore, the quality of the high-dimensional interpolation cannot be assessed easily.

The table method significantly reduces the computation time of our problem to about 0.37% of the conventional method and thus makes the resolution requirement analysis based on Fourier analysis more feasible for proton therapy fluence map optimization.

We also tested the problem with the iterated method to obtain more accurate results, in order to verify those of the adaptive method. Execution time can be further reduced if we change the 1D adaptive routine, used in the iterated method, to handle the oscillatory behavior and discontinuity of the integrand.

Acknowledgment

The work is supported in part by Western Michigan University and by the National Science Foundation under grant ACI-0203776.

References

1. BERNTSEN, J., ESPELID, T. O., AND GENZ, A. An adaptive algorithm for the approximate calculation of multiple integrals. *ACM Trans. Math. Softw.* 17 (1991), 437–451.
2. BORTFELD, T. An analytical approximation of the Bragg curve for therapeutic proton beams. *Med. Phys.* 24 (1997), 2024–2033.
3. BRACEWELL, R. N. *The Fourier Transform and Its Application*. McGraw-Hill, 1978.
4. DE DONCKER, E., SHIMIZU, Y., FUJIMOTO, J., AND YUASA, F. Computation of loop integrals using extrapolation. *Computer Physics Communications* 159 (2004), 145–156.
5. DE DONCKER, E., SHIMIZU, Y., FUJIMOTO, J., YUASA, F., CUCOS, L., AND VAN VOORST, J. Loop integration results using numerical extrapolation for a non-scalar integral. *Nuclear Instruments and Methods in Physics Research Section A* 539 (2004), 269–273. hep-ph/0405098.
6. DEMPSEY, J. F., AND ET AL. A Fourier analysis of the dose grid resolution required for accurate IMRT fluence map optimization. *Med. Phys.* 32 (2005), 380–388.
7. GENZ, A., AND MALIK, A. An adaptive algorithm for numerical integration over an n-dimensional rectangular region. *Journal of Computational and Applied Mathematics* 6 (1980), 295–302.
8. GENZ, A., AND MALIK, A. An imbedded family of multidimensional integration rules. *SIAM J. Numer. Anal.* 20 (1983), 580–588.
9. LI, H. S., DEMPSEY, J. F., AND ROMEIJIN, H. E. A Fourier analysis on the optimal grid size for discrete proton beam dose calculation. Submitted to Medical Physics.

10. LI, S., DE DONCKER, E., AND KAUGARS, K. On iterated numerical integration. In *Lecture Notes in Computer Science* (Jan 2005), vol. 3514, pp. 123–130.
11. PIESSENS, R., DE DONCKER, E., ÜBERHUBER, C. W., AND KAHANER, D. K. *QUADPACK, A Subroutine Package for Automatic Integration*. Springer Series in Computational Mathematics. Springer-Verlag, 1983.
12. SZYMANOWSKI, H., AND MAZAL, A. E. A. Experimental determination and verification of the parameters used in a proton pencil beam algorithm. *Med. Phys.* 28 (2001), 975–987.
13. PARINT. <http://www.cs.wmich.edu/parint>, PARINT web site.

Payment in a Kiosk Centric Model with Mobile and Low Computational Power Devices*

Jesús Téllez Isaac, José Sierra Camara,
Antonio Izquierdo Manzanares, and Mildrey Carbonell Castro

Universidad Carlos III de Madrid, Computer Science Department,
Avda. de la Universidad, 30, 28911, Leganés (Madrid), Spain
jtellez@gmail, {sierra, aizquier}@inf.uc3m.es,
mildreycc@yahoo.es

Abstract. In this paper we present a protocol for a mobile payment system based on a Kiosk Centric Model (proposed by [2]) that employs symmetric-key operations which require low computational power. Our protocol is suitable for mobile payment systems where the customer cannot communicate with the issuer due to the absence of Internet access with her mobile device and the costs of implementing other mechanisms of communication between both of them are high. However, our proposal illustrates how a portable device equipped with a short range link (such Bluetooth, Infrared or Wi-Fi) and low computational power should be enough to interact with a vendor machine in order to buy goods in a secure way.

1 Introduction

The popularity of m-commerce has increased in the last years thanks to advances in the portable devices and the rapid development of the mobile communication technologies that have allowed people to use mobile telephones or Personal Digital Assistant (PDA) to access the Internet (to read email, browse web pages or purchase information or goods) anywhere and anytime.

Different mobile payment systems have been proposed in the last years, but the one developed by [8] (called 3-D Secure) has become a standard due to its benefits regarding security and flexibility in the authentication methods. This schema allows the authentication of the payer (customer) when she makes an online payment using a debit or credit card. The transaction flow for this scheme is shown in figure 1 where all the main communications links are protected using SSL/TLS and the communication between the issuer/consumer is mandatory.

Despite of the flexibility that 3-D Secure gives to the issuer to choose the authentication method, relationship between payer and issuer is quite strict (although required for Visa's 3D-Secure scheme) and does not allow the use of schemes in which the communication among these parties is not possible due to: 1) the impossibility of the client to connect to Internet from the mobile device

* This work was partially supported by ASPECTS-M Project (Reference Models for Secure Architectures in Mobile Electronic Payments), CICYT-2004.

and 2) the high costs of the infrastructure necessary to implement other mechanisms of communication between the client and the issuer. Most of the mobile payment systems proposed up until now assume the consumer has Internet connectivity through her mobile device, so the restrictions mentioned previously do not represent an important issue. However, it is quite common that the client meets situations in which it is not possible to connect to Internet so it becomes necessary to develop mobile payment systems where the user could use her mobile device as a shopping means, even though she may not have Internet access.

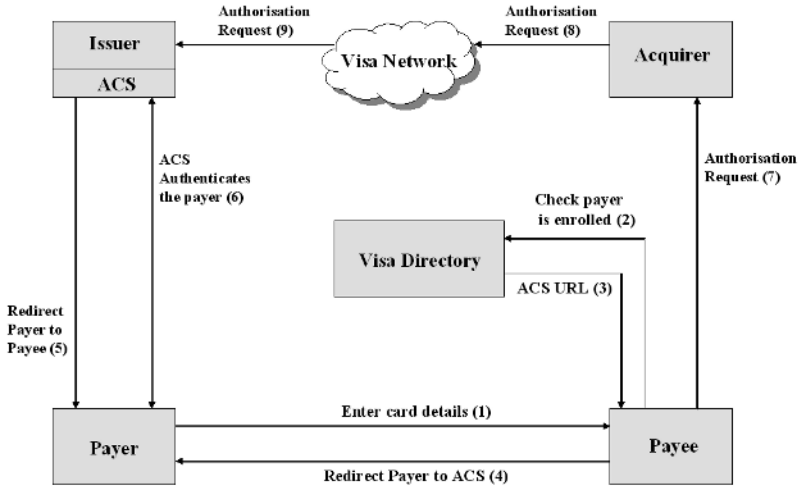


Fig. 1. 3-D Secure transaction [1]

On the other hand, in spite of the wide range of mobile devices available, they all have common limitations [6]: 1) poor computational capabilities, 2) limited storage space and 3) short battery life. These limitations prevent that these devices execute, in an efficient way, computations that require a lot of resources, like those of asymmetric cryptography.

Symmetric cryptography (which employs a shared key between two parties) provides, like asymmetric cryptography, message confidentiality, message integrity and party authentication, and represents an alternative in the construction of secure protocols for mobile payment systems, because symmetric-key operations do not require of a high computational power nor additional communications steps (as happens in protocols based on public-key infrastructure where the public-key certificates have to be verified by a Certificate Authority).

In this paper, we present a protocol (that supports both credit-card and debit-card transactions) for a mobile payment system based on a Kiosk Centric Model (proposed by [2]) which overcomes the limitations mentioned before. Our proposal represents an alternative to the restrictions of mobile payment systems (including Visas 3-D Secure) as for the connection between the client and issuer.

Moreover, it uses symmetric-key operations in all engaging parties to reduce both, the setup cost for payment infrastructure and the transaction cost. Another benefit derived of the using of our proposal is a reduction of all parties computation and communications steps (in comparison with protocols based on public-key infrastructure) that make it suitable for mobiles devices with low computational power.

The rest of this paper is organized as follows: In next section, we survey related work. Section 3 presents the proposed system. In section 4, we analyze the scheme proposed. We end with our conclusions in Section 5.

2 Related Work

In recent years, several studies have been conducted to improve the security of mobile payment systems. Meanwhile, efforts have also been dedicated to unify concepts and scenarios into frameworks that will be useful to develop new electronic payment systems. Research conducted by [2] is an example of a study that unifies many proposed m-commerce usages into a single framework. This research intended to revise the possible range of mobility scenarios, identifying the security issues for each connectivity scenario. As a result, five scenarios were identified and analyzed: Disconnected Interaction, Server Centric Case, Client Centric Case, Full Connectivity and Kiosk Centric Case. The latest has been considered as the starting point in the design of our proposal.

In [9], payment methods are classified according to several standards and analyzed to point out their advantages and drawbacks. Besides, the research also provides a payment process for mobile devices based on pre-payment and accounts. This proposed solutions requirements are low (both on cost and technical capabilities) and it also has high scalability and security properties. However, their methods and processes are not suitable for our proposal, as our goal is to suggest an scheme based on post-payment¹ and symmetric cryptography.

A secure and efficient one-way mobile payment system is proposed in [4]. In their solution the security of the system is based on the intractability of the discrete logarithm problem and the one-wayness of keyed hash function. As opposed to their goal (designing a mobile payment system with minimal complexity using two public key pairs), our solution aims for devising a scheme that relies on symmetric-key operations instead.

The closest work to ours is [5]. Their work proposed a secure account-based payment protocol suitable for wireless networks that employs symmetric-key operations which require lower computation at all engaging parties than existing payment protocols. While this proposal satisfies the majority of our requirements, we have to reformulate their protocol (from now on, SAMPP) to satisfy the requirements of the scheme that we suggest in this work, where the customer never establishes any connection with the bank during the payment transaction.

¹ Mobile payment where the consumer receives the content and consumes it before paying. Credit cards are an example of credit-based payment methods.

As the payment software (also called wallet software) must be sent to the customer by the issuer through the vendor, it becomes necessary the use of techniques to assure that the program received by the client was created and sent by the issuer, and has not been tampered. In order to obtain the protection of the payment software in the aspects mentioned before, two different proposals related to the aforementioned techniques will be detailed in the following paragraphs.

The first work (proposed by [3]) introduced a new approach to watermarking, called path based watermarking, that embeds the watermark, with relatively low cost, in the dynamic branch structure of the program, and shows how error-correcting and tamper proofing techniques can be used to make path based watermarks resilient against a wide variety of attacks. The other work, proposed by [7], describes three techniques for obfuscation of program design: 1) The class coalescing obfuscation, 2) Class splitting obfuscation, and 3) Type hiding obfuscation. The experimental results (applying these obfuscations to a medium-size java program) shows that the run-time overhead, in the worst of the case (class splitting obfuscation), is less than 10% of the total running time of the program.

3 Scheme Proposed

3.1 Notations

- $\{C, V, P, I, A\}$: the set of customer, vendor, payment gateway, issuer and acquirer, respectively.
- ID_P : the identity of party P that contains the contact information of P .
- TID: Identity of transaction that includes time and date of the transaction.
- OI: Order information ($OI = \{TID, h(OI, Price)\}$) where OI and Price are order descriptions and its amount.
- TC: The type of card used in the purchase process (TC=Credit, Debit).
- Stt: The status of the transaction ($Stt = \{Accepted, Rejected\}$).
- TIDReq: The request for TID.
- VIDReq: The request for ID_V .
- $\{M\}_X$: the message M symmetrically encrypted with the shared key X .
- $MAC(X,K)$: Message Authentication Code of the message X with the key K .
- $h(X)$: the one-way hash function of the message X .

3.2 Operational Model

Generally, operational models for m-commerce found in literature involve transaction between two or more entities. Our operational model is composed of four entities: 1) *Customer*: a user who wants to buy information or goods from the vendor and has a mobile device with low computational power and equipped with a built-in display, keyboard (not necessarily with a QWERTY layout), short range link (such Infrared, Wi-Fi or Bluetooth) and capability to execute a java program, 2) *Vendor*: a computational entity (a normal web or an intelligent vending machine) that wants to sell information or goods and with which the user

participates in a transaction, 3) *Acquirer*: the vendor's financial institution, 4) *Issuer*: the customer's financial institution, and 5) *Payment Gateway*: additional entity that acts as a medium between acquirer/issuer at banking private network side and customer/vendor at the Internet side for clearing purpose.

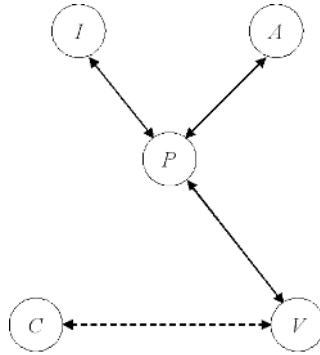


Fig. 2. Operational Model

In figure 2, we specify the links among the five entities of our scheme. Note that there is no direct connection involving the customer and the issuer. Moreover, the connection between the customer/vendor (denoted as the dotted arrow) is set up through a short range link (like bluetooth, infrared or Wi-Fi). On the other hand, interaction among the vendor and the payment gateway (depicted as solid arrow in the scheme) should be reliable and secure against passive and active attacks. Therefore, the connection is supposed to be established through a secure wired channel by using a security protocol like SSL/TLS [4]. Note that the issuer, acquirer and payment gateway operates under the banking private network so we do not concern about connections security among these entities.

The protocol based in symmetric cryptography proposed by [5] is a starting point of our protocol. We reformulated this protocol to satisfy the requirements of that, as stated before, pretends to allow the client to make purchases from its mobile device without connecting itself to Internet.

3.3 Key Generation Technique

Our scheme handles three different sets of shared keys used for encrypt a message symmetrically. Each one is generated off-line in the entity that will store them.

The first set $VPSec_j$, $j = 1, \dots, n$, is generated from the secret $VPSec$ and stored in the vendor and Payment gateway terminals respectively. The other set $CISec_i$ (stored in the customer's device and issuer's terminal, respectively), $i = 1, \dots, n$, is generated from the secret $CISec$. The last set $CVSec_k$ (where $k = 1, \dots, n$) is generated from the secret $CVSec$ and are stored in the customers device and the vendors terminal respectively.

In order to generate the sets of shared keys, we apply a Hash algorithm with one-bit cyclic chain function of a master secret each time a session key is generated [5]. The details are shown as follows:

Generating VPSec_j and CVSec_k

$VPSec_1 = h(1\text{-bit-shift-of-VPSec}), VPSec_2 = h(2\text{-bit-shift-of-VPSec}), \dots,$

$VPSec_n = h(n\text{-bit-shift-of-VPSec})$

$CVSec_1 = h(1\text{-bit-shift-of-CVSec}), CVSec_2 = h(2\text{-bit-shift-of-CVSec}), \dots,$

$CVSec_n = h(n\text{-bit-shift-of-CVSec})$

Generating CISec_i

$CISec_1 = h(1\text{-bit-shift-of-(CDCI,CISec)}),$

$CISec_2 = h(2\text{-bit-shift-of-(CDCI,CISec)}), \dots,$

$CISec_n = h(n\text{-bit-shift-of-(CDCI,CISec)})$

3.4 Detailed Protocols

Our protocol consists of four sub-protocols: Registration, Purchase, Withdrawal and Deposit. Each sub-protocol has the following main functions:

Registration ($C \leftrightarrow V, C \leftrightarrow I$): This sub-protocol involves the customer, the vendor and the issuer. The process starts when the customer shares her credit-and/or debit-card information (CDCI) with her issuer. CDCI contains the long-term secret CISec known only by the customer and her issuer and will be used as an authentication method by the customer in future withdrawals.

In addition, the secret SSWSec is shared between the customer/issuer and will be used as watermark value for the watermarking process at the issuer's side and as software input at customer's side to detect its authenticity.

When the first purchase takes place, V will detect if the wallet software is available in the mobile device. If not, V sends a software request to P , which will forward the request to I . The issuer intends to protect the software against various types of attacks carried away at any moment, following these steps: 1) First, choose one of the obfuscation methods proposed by [7] and apply it to the java code, and 2) Then, apply a watermarking process (proposed by [3]) to the software (using SSWSec as a watermark value and embedded into the software).

Once the software has been prepared, I will forward it to the P , which will send it to V , who will finally send it to C . After C receives the software, she will install it and check its authenticity using the secret SSWSec. If a problem occurs, C could abort the registration sub-protocol or start the process again.

When the software is successfully installed and working, C generates CVSec and send it to V with ID_C and a nonce n encrypted with the session key K , generated by running AKE protocol with V . Then V sends $h(n, CVSec)$ to C as a confirmation of customer's registration. After the sub-protocol has been completed, C and V can generate a new set of CVSec_i by using the same key generation technique. On the other hand, the vendor registers herself to the Payment Gateway and share the secret VPSec.

- 1) $C \rightarrow V$: $\{ID_c, CVSec, n\}_K$
- 2) $V \rightarrow C$: $h(n, CVSec)$

Purchase ($C \leftrightarrow V$): This sub-protocol is carried out between C and V over the wireless channel. The process starts when C sends to V the information necessary to set up the sub-protocol (step 3). After this information exchange ends, C builds up the Payment-script Request with OI and TC . Then, C encrypts it and sends to V where the message is decrypted to retrieve OI .

- 3) $C \rightarrow V$: $ID_C, i, TIDReq, VIDReq$
- 4) $V \rightarrow C$: $\{TID, ID_V\}_{CVSec_i}$
- 5) $C \rightarrow V$: $\{OI, Price, MAC[(Price, TC, h(OI), ID_V), CISec_i]\}_{CVSec_i},$
 $MAC[(OI, Price, ID_C, ID_I), CVSec_{i+1}]$

Note that, although V can decrypt the message using $CVSec_i$, she cannot generate this message since she does not have the necessary $CISec_i$ to construct $MAC[(Price, TC, h(OI), ID_V), CISec_i]$. Thus, any entity of the mobile payment system can ensure that the message is truly sent from C .

Withdrawal ($V \leftrightarrow P$): Withdrawal sub-protocol occurs between V and P through a secure wired channel. V decrypts the message received from C (to retrieve OI), prepares the Withdrawal-script Request (including ID_C , ID_I , and the index i used to identify the current session key in the set of $CISec_i$) encrypted with $VPSec_j$ and then sends it to P .

After the script was received by P , she forwards it to I , adding some information such her identity (ID_P). Here, this script is called Withdrawal-script Request and will be processed by I to approve or reject the transaction.

Once the issuer has processed the request and prepared the Withdrawal-script Response (including Stt), she must send it to P who in turn proceeds to forward to V . The Deposit sub-protocol is activated by P only when the Withdrawal is approved. Otherwise, P assigns the value Discarded to Std .

After the Withdrawal and Deposit sub-protocols are completed, P sends the Withdrawal-script Response to V (including the Deposit-script Response). Then V prepares the Payment-script Response and sends it to C .

- 6) $V \rightarrow P$: $\{MAC[(Price, TC, h(OI), ID_V), CISec_i], j, ID_V,$
 $h(OI), i, TID, Price, ID_C, ID_I\}_{VPSec_j},$
 $MAC[(h(OI), i, TID, ID_C, ID_I), VPSec_{j+1}]$
- 7) $P \rightarrow I$: $MAC[(Price, TC, h(OI), ID_V), CISec_i], i,$
 $h(OI), TID, Price, ID_C, ID_V, h(VPSec_{j+1})$
- 8) $I \rightarrow P$: $Stt, h(Stt, h(OI), h(CISec_i)), \{h(OI), Stt, h(VPSec_{j+1})\}_{CISec_i}$
- 11) $P \rightarrow V$: $\{Stt, \{h(OI), h(VPSec_{j+1})\}_{CISec_i},$
 $h(Stt, h(OI), h(CISec_i)), Std, h(Std, h(OI))\}_{VPSec_{j+1}}$
- 12) $V \rightarrow C$: $\{\{h(OI), Stt, h(VPSec_{j+1})\}_{CISec_i}\}_{CVSec_{i+1}}$

Deposit ($P \leftrightarrow A$): This sub-protocol occurs between the P and A through a secure wired channel when no problems have found at the Withdrawal sub-protocol. Here, the Deposit-script Request is prepared by P who sends it to A

who checks the Price received with the negotiated during the purchase process. If they are matched, the value *Accepted* is assigned to *Std* and the total amount of the *OI* is transferred to the vendor's account. Otherwise, the deposit is refused (the value *Discarded* is assigned to *Std*) and it not represents an excuse for *V* to not deliver the good to *C* because the Withdrawal sub-protocol has been complete successfully. Then, a dispute occurs between *V*, *P* and *A*.

The Deposit-script Response is prepared by *A* and then sent to *P* in order to complete the deposit sub-protocol.

9) **P** → **A**: $ID_p, Price, TID, Stt, h(OI), ID_V, h(VP\text{Sec}_{j+1})$

10) **A** → **P**: $ID_A, Std, h(Std, h(OI))$

After a transaction is completed, each entity of the payment system put in her revocations list, $CV\text{Sec}_i$ and $CISec_i$ to prevent their replay from customer and vendor. In the following purchases, the registration sub-protocol will not occur until the customer is notified to update the secret $CV\text{Sec}$. Thus, when become necessary to renew the secret, the customer runs the Registration sub-protocol to get a new $CV\text{Sec}$. While the secret is not updated, the customer can use other values in the set of $CV\text{Sec}_i$ to perform transactions. To update the $VP\text{SEC}$, the Payment Gateway sends the new secret to the vendor by using an AKE protocol. Finally, to update the $CISec$, the issuer has to add a message with the new secret to the Withdrawal-script Response which will be modified as following:

$$\{h(OI), Stt, h(VP\text{Sec}_{j+1}), NewSecret, h(NewSecret)\}_{CISec_i}$$

4 Analysis

4.1 Comparison with SAMPP

In this section, we present a comparison between SAMPP and ours in order to establish the differences between both protocols.

The major difference between both protocols relies on the operational environment in which they are used. In SAMPP, the mobile device has access to the Internet which allows the client to communicate with the issuer when needed whereas our protocol is based on the idea of the consumer not being able to connect directly to the issuer, in consequence, any information or program that the issuer wants to send to the client, will have to do it through the vendor.

Another difference is the distribution method used with the payment software. While in SAMPP the customer must either download the software from the issuer or receive it by e-mail, in our proposal the wallet software must be sent from the issuer to the consumer through the vendor. This has lead us to the inclusion of security mechanisms (such as code obfuscation and watermarking) that assure the software against several types of attacks.

The third difference worth mentioning can be found in the number of sub-protocols that compose the protocol. SAMPP is composed of two sub-protocols whereas ours it is made up of four sub-protocols. In our protocol, each sub-protocol of the payment process is activated when it is needed (like the deposit

sub-protocol that is activated when the issuer approves the withdrawal) and unnecessary steps are avoided (as happens in SAMPP where the Payment Gateway must send the information to the issuer and the acquirer at the same time even though the withdrawal has not been approved).

The fourth difference can be found in the payment modes allowed by both protocols. In SAMPP, at the moment of the purchase, the client can use only his credit card whereas in ours, credit- or debit-card transactions are supported.

The last difference is the exchange of the secret shared between the client and the issuer (CISec). In the case of SAMPP, at the time of updating the CISec secret, a protocol AKE is used (among client/issuer) whereas in ours, the new secret must be sent inserted in the Withdrawal-script Response.

4.2 Performance

As SAMPP was reformulated to fit our needs, in this section we perform a comparison of both protocols in terms of performance, focusing on the number of cryptographic operations performed by each one (results of this comparison are shown in table 1). We can see that although operational models are different and our proposal is an evolution of SAMPP, the performance of our protocol is the same that of SAMPP.

Table 1. The number of cryptographic operations of SAMPP, and our protocol, respectively

Cryptographic Operations		SAMPP	Ours
1. Symmetric-key encryptions/decryptions	C	4	4
	V	5	5
	P	2	2
2. Hash functions	C	2	2
	V	-	-
	P	-	-
3. Keyed-hash functions	C	2	2
	V	2	2
	P	1	1
4. Key generations	C	2	2
	V	1	1
	P	1	1

5 Conclusions

We have proposed a secure protocol which uses symmetric cryptographic techniques. It is applicable to mobile payment systems where direct communication between the client and the issuer does not exist. Thus, the client takes advantage of the infrastructure of the vendor and payment gateway to communicate with the issuer and purchase securely from her mobile device. Our proposal represents

an alternative to all mobile payment systems where the connection between the client and issuer is mandatory, including Visa's 3-D Secure scheme. Moreover, our scheme illustrates how a portable device equipped with a short range link (such Bluetooth, Infrared or Wi-Fi) and low computational power is enough to interact with a vendor machine in order to buy goods in a secure way

The symmetric cryptographic technique used in our protocol has lower computation requirements at both parties (since no public-key operation is required) and offers the capability of dealing with protocol failures and disputes among parties. Moreover, we have shown that our protocol's performance is about the same than that of SAMPP, although this protocol is used in different operational models. As a result, we state that our proposed protocol allows mobile users to have efficient and secure payment systems even if the communication with the issuer is not possible.

References

1. Al-Meather, M.: Secure electronic payments for Islamic finance. PhD thesis, University of London, (2004).
2. Chari, S., Kermani, P., Smith, S., and Tassiulas, L.: Security issues in m-commerce: A usage-based taxonomy. In *E-Commerce Agents*, volume 2033 of *Lecture Notes in Computer Science*, pages 264-282, Springer-Verlag, (2001).
3. Collberg, C., Carter, E., Debray, S., Huntwork, A., Kececioğlu, J., Linn, C., and Stepp, M.: Dynamic path-based software watermarking. In *ACMSIGPLAN 2004 Conference on Programming Language Design and Implementation 2004*, pages 107-118, ACM, (2004).
4. Ham, W., Choi, H., Xie, Y., Lee, M., and Kim, K.: A secure one-way mobile payment system keeping low computation in mobile devices. In *WISA2002, Lecture Notes in Computer Science*, pages 287-301. Springer-Verlag, (2002).
5. Kungpisdan, S.: A secure account-based mobile payment system protocol. In *ITCC04, International Conference on Information Technology: Coding and Computing*, pages 35-39, IEEE Computer Society, (2004).
6. Lei, Y., Chen, D., and Jiang, Z.: Generating digital signatures on mobile devices. In *18th International Conference on Advanced Information Networking and Applications (AINA 2004)*, pp. 532-535, IEEE Computer Society, (2004).
7. Sosonkin, M., Naumovich, G., and Memon, N.: Obfuscation of design intent in object-oriented applications. In *2003 ACM workshop on Digital rights management (DRM03)*, pp. 142-153, ACM Press, (2003).
8. Visa International: 3-d secure mobile authentication scenarios version 1.0, (2002). [Online], Available: <http://partnernetnetwork.visa.com/pf/3dsec/specifications.jsp>.
9. Zheng, X. and Chen, D.: Study of mobile payments system. In *IEEE International Conference on Electronic Commerce*, pp. 24, IEEE Computer Society, (2003).

Survivable Mechanism for IEEE 802.11 WLAN Improvements

Flavio E. de Deus¹, Ricardo Staciarini Puttini¹, Luis Molinaro¹,
Joseph Kabara², and Luis Javier García Villalba³

¹ Department of Electrical Engineering,
University of Brasilia, Brasília, DF – Brazil
{flavio, molinaro}@nmi.unb.br, puttini@unb.br

² Department of Information Science and Telecommunications,
University of Pittsburgh, Pittsburgh – PA 15260 USA
jkabara@pitt.edu

³ Research Group in Analysis, Security and Systems (GASS),
Department of Computer Systems and Programming (DSIP),
Complutense University of Madrid (UCM),
C/ Profesor José García Santesmases s/n,
Ciudad Universitaria, 28040 Madrid, Spain
javiervg@sip.ucm.es

Abstract. In this paper we propose a mechanism to improve survivability in IEEE 802.11 WLAN. Our approach consists of two main phases: Design and Fault Response. In Design phase, we deal with quantifying, placement and setting up of APs according to both area coverage and performance criteria. In Fault Response phase we consider the reconfiguration of active APs in order to deal with AP fault in the service area. We analyze changes in both power level and frequency channel assignment of the remaining APs, searching for the best configuration during the fault condition. We also propose area coverage and performance metrics to evaluate the effectiveness of the solution for the fault condition, according to the fault tolerance constraints de-fined in the Design phase. Finally, we present an implementation of the proposed techniques¹.

1 Introduction

Wireless local area networks – WLAN, based on the IEEE 802.11 standard [1] are increasingly being considered as the platform of choice for various applications. So, our research addresses the issues surrounding the reliability and survivability of wireless local area networks. To clarify our work we need to specify what kind of AP faults this mechanism can recovery. Initially, we are taking into account the occurrence of failures due to lack of energy to an AP or problems with the wired link to an AP. In particular, we focus on the problem of overcoming these APs failures

¹ This work was supported in part by the CAPES Foundation under grant BEX 2930/03-0. Javier Garcia's work is supported by the Spanish Ministry of Education and Science (MEC) under project TSI2005-00986.

working with reconfiguration of the remaining APs by changing parameters such as power level and frequency channels. Failures regarding to fault on AP functions or slighter problem (e.g., stops forwarding packets) or malfunction can not be detected and solved.

The proposed mechanism is divided in two main phases: Design and Fault Response. The Design phase is based on previous work by C. Prommak et al. [2]. The WLAN design is formulated as a Constraint Satisfaction Problem (CSP) which formally express area coverage and client bandwidth requirements. The solution to the formulated problem is searched allowing for definition of parameter such as: AP quantity, AP placement, AP power level and frequency channel assignment. As a first contribution, we evaluate the definition of additional constraints to the original CSP problem formulated [2], in order to introduce fault tolerance properties in the network design. These constraints consist in limitations on the maximum power level and throughput considered during the network design, allowing for power level and throughput increasing during a fault occurrence.

The second contribution of this paper is the proposal of the mechanisms for the Fault Response phase. Whenever an AP failure is detected, the Fault Response phase is started. A new CSP is formulated and the solution search is initialized with the current configuration of the APs that remain working. The solution is searched from this starting point by relaxing the fault tolerance constraints imposed in the Design phase and restricting the AP quantity and placement parameters. The solution to this modified network design problem aims to provide the best solution possible with the remaining APs, allowing only for soft configuration changes in these elements.

We emphasize that the Fault Response phase can be easily implemented in a centralized Management Station (MS), implemented by software, which polls the AP in the network for detecting failures and remotely sets the new configuration in the active APs after the calculation of the new network design for the fault situation. Both poll and set operations can be easily done by means of SNMP and standard IEEE 802.11 MIB agents, usually found in major supplier's APs. As a last contribution, we present an implementation of this Management Station. In a future work we will address more specific failures improving the fault detection system to cope with more AP failures. This is relevant because the Fault Response phase is dependent to the monitor system to detect and, therefore, overcome failures.

2 Related Work

This section discusses related work in wireless survivability and compares it with our approach. Snow et al. [3] describe reliability and survivability in the context of wireless networks. They describe an "outage index" and perform statistical evaluation of impact of outages. However, their work primarily focuses on proposing end to end connectivity schemes for hybrid cellular overlay networks. Our paper addresses AP failures in WLANs and does not consider an underlying cellular infrastructure.

Haas et al. [4] describe a technique to tolerate the failure of the location database, which is a repository of the locations of mobile stations at the mobile switching centers. Tipper et al. [5-6] present a survivability analysis of Personal Communication Service (PCS) networks; their work identifies several causes of failures in the different wireless network layers, along with metrics to quantify the network

survivability and a simulation model to study the effects of different kinds of failures in a PCS network. The results of their simulation model demonstrate that user mobility can significantly degrade the performance of the network, in the presence of failures. Malloy et al. [7] describe the problems of wireless reliability for PCS networks; their work identifies the causes of failures in the different parts of a PCS network, and proposes a number of solutions to tolerate faults in the different layers.

Dahlberg et al. [8] propose the notion of overlapping coverage areas and dynamic load balancing as a way to overcome infrastructure failures in PCS networks. More recently, Chen et al. [9] describe a scheme for enhancing the connection reliability in WLANs by “tolerating” the existence of “shadow regions” through placement of redundant APs. They present the details of implementing redundancy by making enhancements to the basic 802.11 channel access protocol and demonstrate improvement in connection dependability. Albeit, this scheme works well for improving dependability through redundancy, it deals with “connection” survivability when a user moves from one AP to the shadow regions. Our scheme is not based on redundancy and does not require shadow APs. It focuses on “network” survivability resulting from a network design criterion rather than per user connection survivability resulting from user mobility. There is no redundancy in our approach, avoiding co-channel interference problems [10]. This method provides capacity redundancy which brings us the advantage of preserves the capacity of the system.

3 Design Phase

The task of network planning is to place a sufficient number of APs in a service area. The power level and frequency channel of an AP, together with the environment specific path loss and the antenna radiation pattern, determine the region over which the AP can support traffic demand to/from wireless users. According to capacity analysis of the CSMA/CA protocol used in 802.11 WLANs, the capacity of an AP varies depending on the number of wireless users simultaneously transferring data through the AP [11]. As the number of wireless users actively transferring data through an AP increases, the effective AP capacity decreases. Thus, the number of APs in a service area should be a function of the number of users and the characteristics of their traffic demand [12]. Due to the low cost of the APs, compared to the wireless devices with which they communicate, minimizing the number of the APs is unnecessary. However, over-provisioning the service areas leads to serious system performance degradation due to co-channel interference [10]. Thus, we define that it will be more appropriate and effective work with a design problem that was formulated as a constraint satisfaction problem rather than an optimization problem.

3.1 Demand-Based WLAN Design Model

The demand-based WLAN design prescribes requirements for a finite number of variables with a given set of possible values (called domains) that can be assigned to the variables. Let $G = \{g_1, g_2, \dots, g_c\}$ denote a set of signal test points (STP) representing locations for testing the received signal strength and the signal-interference rate (SIR). Each STP refers to a coordinate in three-dimensional space (x_h, y_h, z_h) , where z_h is

the floor where g_h is located. Let $U = \{d_1^t, d_2^t, \dots, d_m^t\}$ denote a set of demand nodes, where index t indicates the type of sub-area where demand node i is located. The position of demand node i within the service area is denoted by (x_i, y_i, z_i) , where (x_i, y_i) are the coordinates on floor z_i where d_i^t is located. The user activity level (α_i) and the average data rate requirement (R_i) specify the network usage characteristics for the demand node.

The CSP for the demand-based WLAN design model is defined by the triple (V, D, C) , where:

$V = \{n, p_j, f_j, (x_j, y_j, z_j)\}$ denotes a set of variables of the design problem;

$D = \{D_n, D_p, D_f, D_{(x,y,z)}\}$ denotes a set of finite domains associated with each variable; and

$C = \{C1, C2, C3\}$ denotes a set of constraints.

Let $A = \{ap_1, ap_2, \dots, ap_n\}$ denote a set of APs used in the service area, where n is the total number of APs required. Let $ac_j = \{p_j, f_j, (x_j, y_j, z_j)\}$ denote a set of parameters assigned to ap_j for $1 \leq j \leq n$, where p_j denotes the power level assigned to ap_j , f_j denotes the frequency channel assigned to ap_j , and (x_j, y_j, z_j) denotes the coordinate (x_j, y_j) on floor z_j where ap_j is located. $d_{ij}^{t,2}$ is a user association binary variable that equals 1 if demand node $i \in U$ associates to $ap_j \in A$; 0 otherwise. g_{hj} is a signal availability binary variable that equals 1 if STP $h \in G$ can receive a signal from $ap_j \in A$; 0 otherwise. D_n is a set of integer numbers, which are candidate for the number of APs used in the network. D_p is the set of candidate power levels for variable $p_j \in \{P_1, P_2, \dots, P_{\max}\}$. D_f is the set of candidate frequency channels for variable $f_j \in \{F_1, F_2, \dots, F_k\}$. $D_{(x,y,z)}$ is the domain of variable (x_j, y_j, z_j) .

The constraints in the CSP for the demand-based WLAN design model are:

$$C1: r_i^t > R_i, \forall i \in U \quad (1)$$

$$C2: g_{hj}(P_{R_{hj}} - P_{R_{th}}) \geq 0, \forall h \in G, \forall j \in A \quad (2)$$

$$C3: g_{hj}(P_{R_{hj}} - \text{Int}f_{hj} - \text{SIR}_{th}) \geq 0, \forall h \in G, \forall j \in A \quad (3)$$

Constraint C1 (1) ensures that the average data rate available to wireless user i which is a type t user (r_i^t) is greater than the specified user data rate (R_i). The 802.11 capacity model and the user activity pattern correlated with the type of sub-areas where users locate are incorporated in this constraint to estimate the average data rate that the active wireless user can obtain [11, 13].

² In the formulation presented in [2], d_{ij}^t is considered a variable from V instead of a dynamic parameter. Additionally, we require the location of each demand node to be also a STP.

The set of constraints C2 (2) – C3 (3) ensure that the radio signal is available throughout the service region. To assess the signal quality in the service area, the received signal strength and the SIR level are tested at all signal test points (STP’s). The decision variable g_{hj} is equal to one if the received signal strength at the STP h transmitted from the ap_j ($P_{R_{hj}}$ in dBm) and the SIR level with respect to the ap_j (i.e., $P_{R_{hj}} - Intf_{hj}$) meet the received sensitivity threshold (PR_{th}) and the SIR threshold (SIR_{th}) as specified by (2) and (3), respectively; g_{hj} is equal to zero otherwise³.

3.2 Survivability Constraints

We envision a new WLAN design that aggregates survivability properties in order to provide even if not a better service, a minimum connectivity to all user during a failure scenario. Towards this objective we tailored the demand-based WALN design model [2] changing constraints to build our proposed mechanism.

Our approach consists in increasing some constraints to produce a solution that can deal with AP faults. The mathematical formulation for the design model considers both the signal radio coverage requirements and the data rate capacity requirements. Network usage characteristics of WLANs were accounted for by incorporating the correlation between users’ network usage behavior and their locations into the CSP formulation. We change constraints related to the domain of possible power level assignment D_p . Instead of allowing $D_p = \{P_1, P_2, \dots, P_{max}\}$, we introduce a parameter β in this calculation to limit the maximum power level of the APs during network design, in order to create a response range and to make possible our mechanism to act in a failure scenario. Thus, $D_p = \{p_j / p_j \in \{P_1, P_2, \dots, P_{max}\} \text{ and } p_j \leq \beta P_{max}\}$.

Figure 1.(a) shows the modified framework for finding solution to the Design phase CSP. Construction and Frequency Channel Assignment (FCA) steps aim to generate a good starting configuration that provides an estimated number of APs and their initial parameters. The Construction step employs two heuristics: Area Covering Heuristic (ACH) and Demand Clustering Heuristic (DCH). While ACH estimates the number of APs needed to provide radio signal coverage to the service area, DCH places additional AP(s) in those parts of the service area where high traffic volume exists. Together, these two modified heuristics determine the initial locations and power levels of the APs considering the β parameter. The FCA step utilizes simulated annealing to determine the frequency channel assignments of the APs based on AP locations and power levels determined in Construction step.

The Constraint Violation Reduction (CVR) step evaluates the network configuration based on the set of constraints. If any design requirement constraint is violated, the CVR step reduces the constraint violations by adjusting the locations and power levels of the APs by using Tabu search. The CVR step reassigns frequency channels by using the FCA simulated annealing method. If the CVR fails to produce a

³ Although g_{hj} may be equal to one for multiple APs (j), the dynamic parameter d'_{ij} will be equal to one for only one AP. This is required as the demand node can be associated with one and only one AP.

feasible network configuration satisfying all design constraints, the intensification phase revisits good candidate solutions recorded during the CVR step and performs a repairing process for each revisited solution. After the intensification, if a feasible network configuration is still not found, the Add-AP step attempts to solve the problem by installing additional AP(s) in the service area. Running the Design phase we find a survivable solution that matches the needs of the environment and users.

4 Fault Response Phase

In our approach power control offers a simple but powerful response to a failure scenario. The tradeoffs are obvious: reducing the power on a channel can improve performance for other channels by reducing interference, but it can reduce the throughput of the channel by forcing the transmitter to use a lower rate to deal with the reduced signal-to-noise ratio [14]. As a result, we must carefully consider the β % of power level in a Design phase to allow us to work in a Fault Response phase increasing the power level and later reallocating frequency channels if necessary. In practice, the incentives for using power control are complex and we have to distinguish between the techniques that are fully applicable to planned WLAN.

Initially, our mechanism imposes a monitoring phase to detect failures and identify which AP(s) is/are out of service. The process of monitoring the network will also gather information to feed the modified CSP to produce another solution for the failure scenario. At this moment, the solution technique receives all parameters from the remaining APs which will be the initial values to run the CVR phase. However, to manipulate the new variables, we define a new CSP because power level is no longer fixed while APs' position and number are fixed. Such initialization bypasses the Construction and the FCA steps shown in Figure 1.(a). Moreover, starting the solution search from the current assures a solution which implies minimum modifications. Figure 1.(b) illustrates the framework of Fault Response phase.

Inside this context, the CVR step checks the network configuration and start to reduce the constraint violations by adjusting only the APs' power levels and frequency channel reallocation through simulated annealing method. If CVR step cannot find a feasible network, the Intensification step takes place and the best available solution is chosen, even if the network configuration does not satisfy all design constraints, as we can not run an "Add-AP" step to fully solve the constraints.

In the Intensification step, the constrain violation for each candidate solution is evaluated according to a configuration evaluation function (4) which must be minimized. Equation (4) is composed of a weighted combination of two different measures of degree of constrain violations, accomplishing both area coverage and data rate requirements.

$$E_{(solution)i} = w_1M_1 + w_2M_2 \quad (4)$$

where, w_1 = weight factor representing relative importance of radio signal coverage
 w_2 = weight factor representing relative importance of traffic demand coverage

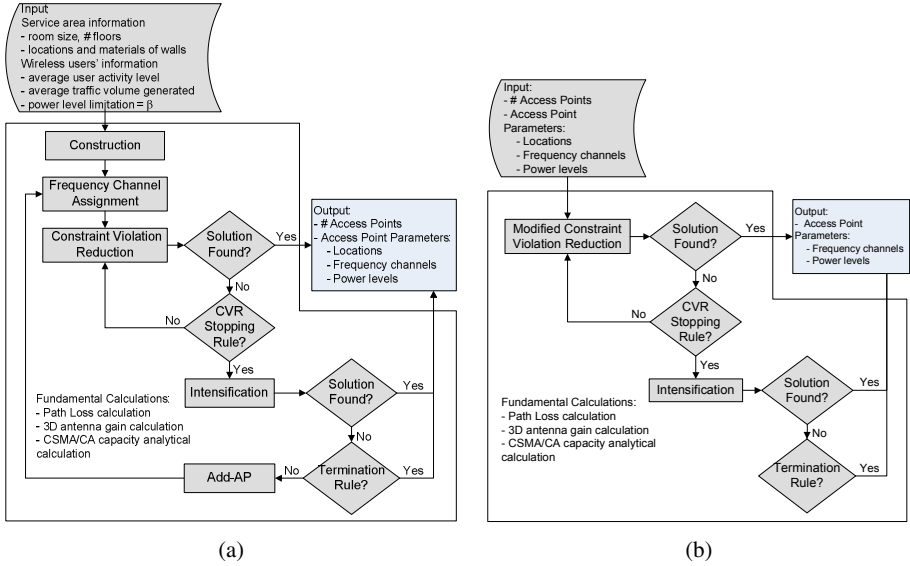


Fig. 1. (a) Framework of the Design phase; (b) Framework of the Fault Response phase

$$M_1 = \frac{1}{2 \sum_{\forall g \in G} w_g} \sum_{\forall g \in G} w_g \left(\max \left(0, \frac{Pr_{th} - Pr_g}{Pr_{th}} \right) + \max \left(0, \frac{SIR_{th} - (Pr_g / Intf_g)}{SIR_{th}} \right) \right) \tag{5}$$

$$M_2 = \frac{1}{\sum_{\forall i \in M} w_i} \sum_{\forall i \in M} w_i \left(\max \left(0, \frac{d_i - r_i^t}{d_i} \right) \right) \tag{6}$$

The first metric (5) concern about the number of users that becomes out of coverage area in a failure scenario and is defined as the ratio between the numbers of users without coverage and the total number of users from the Design phase. Equation (5) measures the ability of users, which were originally associated to the failed AP, to re-associate with another AP after the Fault Response phase. The second metric (6) references the average performance not serviced to the users in the service area during a failure. Let r_i^t denote average data rate available to user i which is type t after the Failure-response phase.

In reaction to a failure, our mechanism is used to select the best-available solution to the failure situation – using a network design criterion – and set the new parameters on the still-working APs. Once the AP(s) in fault is recovered the Fault Response phase is terminated and the previous configuration takes over.

5 Results

The design of WLANs through a demand-based perspective can be accomplished by identification of the individual requirements of wireless users in the service area, represented by demand nodes. This concept allows a designer to precisely describe

the potential number of wireless users and their locations, in order to appropriately place APs and assign users to the APs.

For the results presented in this paper, demand node distributions were created from site surveys and information from the facility staff in each location. Fig. 2 shows the demand node distributions representing prospective wireless users in the service area. The service area considered is the fourth floor of the School of Information Science (SIS4) building at the University of Pittsburgh, spanning an area of 33 x 21 meters. The wireless users are divided in three basic categories, according to average network usage requirements. The average user data rates are taken from observed network usage characteristics [15,16] and are summarized in Table 1.

Table 1. Network Usage Characteristics

User and Sub-area Type	User Activity Level	Average usage data rate (Kbps)
Type 1: Private sub-areas (e.g., staff and graduate student offices)	$\alpha_1 = 0.70$	$R_1 = 460$
Type 2: Public sub-areas for unscheduled activities (e.g., library, student lounges)	$\alpha_2 = 0.60$	$R_2 = 260$
Type 3: Public sub-areas for schedule-based activities (e.g., classrooms, laboratories)	$\alpha_3 = 0.50$	$R_3 = 80$

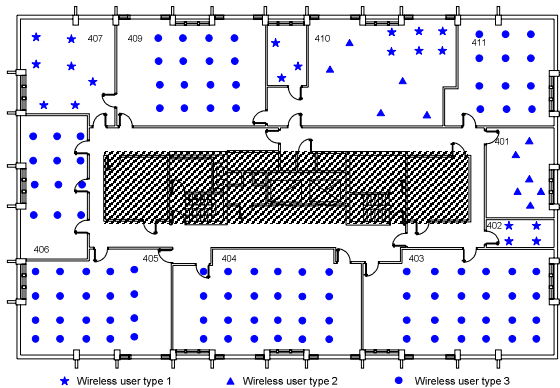


Fig. 2. Demand node distribution for the 4th floor of the School of Information Science

A survivability analysis measures the degree of functionality remaining in a system after a failure, and consists of evaluating metrics that quantify network performance during failure scenarios as well as normal operation. A variety of failure scenarios can be defined, determined by the network component that fails and its location [5]. In WLAN scenarios the main component is the APs.

In order to evaluate the survivability properties of our proposed mechanism, we ran the Design Phase for the SIS4 network service areas with different survivability constraints. We considered useful values of β parameter (e.g. 100%, 85%, 70%, 55% and 40%), which leads to available power levels of commercial APs (e.g. 20, 17, 14, 11 and 8dBm) [17]. Then, we measure the degree of functionality remaining in the

network during an AP failure after reconfiguration by a Fault Response phase run by taking a look in the values of M1 and M2 (Section 4) obtained for each network design, reflecting different values of β parameter. The results are shown in Table 2.

We also found useful to analyze the number of frequency channels changes due to the new configuration for the fault situation. This number is relevant because of the impact on users' activity as users associated to an AP which changes frequency channel assignment may experience a temporary service interruption due to AP reassociation. This is also shown in Table 2 as a normalized metric M3, defined as:

$$M_3 = \frac{1}{n} \sum_{\forall j \in A} t_j \max(0, t_j) \tag{7}$$

t_j is a frequency channel adjust binary variable that equals 1 if $f_j = f'_j$; 0 otherwise. $f'_j \in \{F_1, F_2, \dots, F_k\}$ and denotes the new frequency channel assigned to ap_j in a failure scenario.

According to results presented in Table 2, high levels of β (e.g. $\geq 85\%$) for the Design phase leads to low survivability properties, as there is no power increasing flexibility during an AP fault. For values of $40\% \leq \beta < 85\%$ we were able to find a solution in the Fault Response phase that allows for M1 and M2 $< 3\%$. Finally, variations of M1 and M2 in the scenarios where $\beta = 55\%$ and $\beta = 40\%$ are inexpressive because in the last case although the power increasing flexibility is larger, the SIR tends to be larger too due to the close placement of APs.

Table 2. β Level and its metrics

Design phase		Fault Response phase		
β Level	# of AP	M1	M2	M3
100%	3	0,248	0,213	0
85%	3	0,213	0,181	0
70%	4	0,028	0,018	0,25
55%	5	0,012	0,005	0,40
40%	6	0,008	0,001	0,50

As a preliminary result, we can say that $40\% \leq \beta < 85\%$ are good guesses for the Design phase, but M1 and M2 can be evaluated for different designs and fault conditions in order to establish the best available solution. We have tested our proposed mechanism in more complex scenarios (e.g. multi-floor) and the results lead us to the same β range. This is reasonably expected as we are considering only one AP in failure at a given period of time. We are currently testing multiple AP failures and we intend to present the results for this research in a future paper.

6 Implementation

One of the major characteristics of the proposed solution resides in its ability to deal with currently deployed WLAN networks in concordance with the established IEEE 802.11 standards and related management systems. The *ieee802dot11 MIB* [1]

provides useful variables to access APs configuration (get/set): dot11StationID, dot11CurrentTxPowerLevel, and dot11CurrentChannel.

The use of standard MIB and SNMP allows for a cost-effective implementation of the proposed mechanisms running on centralized platform (Management Station - MS), as illustrated in Fig. 3. In step (1), MS uses SNMP to poll each AP, checking whether they are still connected or not. A simple response-timeout system (e.g. 3 requests without answer) is adopted for fault detection. Whenever a failure is detected, MS start the Fault Response phase calculation (2) to produce a solution which aims to overcome the failure. Then, MS again uses SMNP to set the new configuration to the still-working APs (3). As soon as the new solution reaches a steady state the mechanism gets back to the monitor phase. When the monitor phase identifies that the AP(s) breakdown is solved, the designed solution, stored in MS, is setup again.

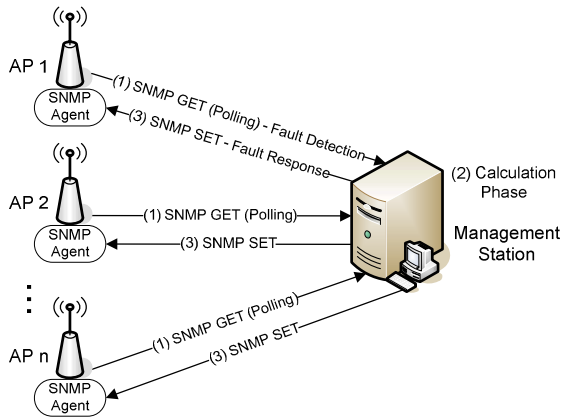


Fig. 3. Fault Tolerance Architecture

7 Conclusions

In scenarios where we could not develop the Design phase (i.e. WLAN already deployed) we can run the Fault Response phase but there will be some limitations because there may not be enough possibilities for power level increasing in order to cope with failure situation as the fault tolerance constraints may not be . Thus, the possibility of raising the power level may not exist in some APs, making the overall results less significant.

This mechanism is based on tradeoffs that are part of the WLAN networks. The wireless medium imposes limits on propagation, interference, throughput, coverage area, and etc. So, applying our mechanism we design a fault tolerance WLAN network which found a balance between over-provisioning and co-channel interference respecting the constraints that we define at first. The power level control helps to manage the interference levels and the cost of this procedure was the throughput. However, work with limited power level brings us spare capacity to deal with bandwidth starvation in failure scenarios. In this direction we can design

survivable WLAN networks adapting the β value and maximize the fault tolerance mechanism over minimum tradeoffs. In addition, our implementation demonstrates that the proposed mechanism is feasible without large costs.

References

1. IEEE Computer Society LAN/MAN Standards Committee. "Part 11: Wireless LAN Media Access Control (MAC) and Physical Layer (PHY) specifications – including ieee802.11-mib, ANSI/IEEE Std 802.11, 1999 Edition (R2003).
2. C. Prommak, J. Kabara, D. Tipper. "Demand-based Network Planning for Large Scale Wireless Local Area Networks". IEEE/ACM First International Workshop on Broadband Wireless Services and Applications (BroadWISE 04) October 2004.
3. A. P. Snow, U. Varshney, and A. D. Malloy. "Reliability and survivability of wireless and mobile networks". IEEE Computer, 33:49–55, July 2000.
4. Z. J. Haas and Y.-B. Lin. "Demand re-registration for PCS database restoration". Mobile Networks and Applications, 5(3):191–198, 2000.
5. D. Tipper, T. Dahlberg, H. Shin, and C. Charnsripinyo. "Providing fault tolerance in wireless access networks". IEEE Communications, 40(1):62–68, January 2002.
6. D. Tipper, S. Ramaswamy, and T. Dahlberg. "PCS network survivability". Mobile and Wireless Communication Networks conference, September 1999.
7. A. Malloy, U. Varshney, and A. P. Snow. "Supporting mobile commerce applications using dependable wireless networks". Mobile Networks and Applications, pp.225–234, July 2002.
8. T. Dahlberg and J. Jung. "Survivable load sharing protocols: A simulation study". ACM/Baltzer Wireless Network Journal, 7:283–296, May 2001.
9. D. Chen, C. Kintala, S. Garg, and K. S. Trivedi. "Dependability enhancement for IEEE 802.11 wireless LAN with redundancy techniques". Proceedings of the International Conference on Dependable Systems and Networks, pp. 521–528, June 2003.
10. J. Kabara, P. Krishnamurthy, and D. Tipper. "Capacity based network planning for wireless data networks". Proceedings IST Mobile Communications Summit, 2001.
11. F. Cali, M. Conti and E. Gregori, "Dynamic tuning of the IEEE 802.11 protocol to achieve a theoretical throughput limit". IEEE/ACM Transactions on Networking, Vol. 8, pp. 785–799, 2000.
12. C. Prommak, J. Kabara, D. Tipper, and C. Charnsripinyo. "Next generation wireless LAN system design". MILCOM 2002. Proceedings, 2002.
13. M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda, "Performance Anomaly of 802.11b". Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, April 2003.
14. A. Akella, G. Judd, P. Steenkiste and S. Seshan, "Self Management in Chaotic Wireless Deployments". Proc. of ACM – MobiCom'05, September 2005.
15. Balazinska and P. Castro. "Characterizing mobility and network usage in a corporate wireless local-area network". International Conference on Mobile Systems, Applications, and Services (MobiSys'03), May 2003.
16. D. Kotz and K. Essien. "Characterizing usage of a campus-wide wireless network," Department of Computer Science, Dartmouth College Technical Report TR2002-423, March 2002.
17. CISCO, "Frequency Band and Operating Channels and Available Transmit Power Settings," in Cisco aironet 1240AG series 802.11 A/B/G AP configuration guide, 2001.

Proposal of a System for Searching and Indexing Heterogeneous Vulnerabilities Databases

Robson de Oliveira¹, Fabio Buiati¹, Luis Javier García Villalba¹, Daniel Almendra²,
L. Pulcineli², Rafael de Sousa Jr.², and Cláudia Jacy Barenco Abbas²

¹ Grupo de Análisis, Seguridad y Sistemas (GASS),

Departamento de Sistemas Informáticos y Programación (DSIP),

Facultad de Informática, Universidad Complutense de Madrid (UCM),

C/ Profesor José García Santesmases s/n, Ciudad Universitaria, 28040 Madrid, Spain

{robson, fabio}@fdi.ucm.es, javiergv@sip.ucm.es

² Universidade de Brasília, Campus Universitário Darcy Ribeiro,

Faculdade de Tecnologia, Depto. de Engenharia Elétrica e Redes de Comunicação,

Laboratório de Redes - sala B1, CEP: 70910-900 - Brasília - DF - Brazil

{danielalmendra, pulcineli}@terra.com.br, desousa@unb.br,
barenco@redes.unb.br

Abstract. This paper describes the project and implementation of a vulnerability search and alert system based on free software. SisBrAV (acronym in Portuguese for Brazilian Vulnerability Alert System), will consist in a spider mechanism that explores several security-related sites for information on vulnerabilities and an intelligent interpreter responsible for analyzing and sorting the relevant data, feeding it into a database. With that information in hands, an email notifier sends out alerts, in Portuguese, about new vulnerabilities to registered clients, according to the operating systems and services run in their environment. In addition to the email notifier, a web server will also be implemented, for systems administrators to perform an on-demand custom search in the vulnerabilities database.

Keywords: Vulnerability Database, Internet spiders, Security Information System, Open Source Solution.

1 Introduction

In a daily basis, a large number of vulnerabilities, which affect a variety of systems and services, are detected. Manufacturers and developers work extensively in order to release, as fast as possible, a patch that fixes the problems found in their products. On the other hand, the hacker community is continually growing, producing malicious codes, exploits and viruses that take advantage of those vulnerabilities very rapidly. With the incredibly large quantity of information that can be found on the Internet today, as well as the increasing number of hacker sites that provide easy access to lots of malicious tools and exploit codes, it is of great importance that every enterprise's systems security team be well advised and informed about what are the threats to their environment and what they can do to avoid them, protecting their systems, services and network quickly and proactively. Even individuals with one or two PCs at home

should be concerned with their system's vulnerabilities, applying the latest patches in their software, avoiding any security problem that may happen.

Existing vulnerability database systems are created and maintained by human administrators, who are responsible for searching, analyzing and evaluating new vulnerabilities everyday, and then updating the database regularly with new entries, in a pretty much manual process. The initial idea of the project depicted in this paper, was that there could be an automatic process of gathering the relevant vulnerabilities information, sorting it according to predefined rules, feeding a database and generating email alerts for specific recipients whose environment could be affected. The solution should be based on free software and should also be portable to many platforms. SisBrAV project is, thus, the result of that idea.

2 Related Issues

Up to this date, in Brazil, there isn't any system such as SisBrAV, which automatically looks for new vulnerabilities and informs the users about them. In the other hand, a large number of security sites can be found in the Internet, and almost all of them have a vulnerability alert section, updated daily, enclosing vulnerabilities for many systems and programs. Thus, information regarding vulnerabilities can be easily accessed through the Internet, but it is very difficult to glimpse which vulnerabilities represent real threats among the large number encountered. So, there is plenty of information, but a lack of simplicity in the process of filtering these pieces of information, in order to keep only in the important ones.

The main challenge in the SisBrAV project is the sorting process, since the system will search for vulnerabilities in many sources, and each of them organizes the information in a particular way. The interpretation of the data collected must be very precise, as well as the sorting process, since the clients must be informed only about the threats to his specific environment. The importance score for each vulnerability must also be precisely assigned, making it possible for the client to assign different priorities when establishing security countermeasures for the vulnerabilities he has been informed about.

Two other elements are also critical for the efficiency of the SisBrAV system: the organization of the vulnerability information and the generation of customized alerts to each client according to his systems and services. The information must be sorted in an accurate but simple manner, and the alerts must be clear and succinct, as well as they must be sent only to the clients whose environment is threatened by the vulnerabilities.

SisBrAV will implement a module for each function it performs. The following section will describe how all these modules work and what functions they perform.

3 SisBrAV Modules

SisBrAV will be consisted of 5 modules. The Vulnerability Search Mechanism (VSM) module will consist in a spider that accesses and indexes many vulnerability documents in several security sites. The Interpreter, Parser and Sorter (IPS) module

will be a program that analyses the data provided from the spider, defining priorities and classifying the entries, according to predefined rules. The Central Database (CDB) module will store all vulnerability data, clients' info and keywords for English-Portuguese translation. The Email Notifier (E-Note) module will alert by email the registered clients about new/updated vulnerabilities specific to each client's environment. At last, the Vulnerability Web Server (VWS) module will be a server, accessible by any registered client, to perform an on-demand, customized vulnerability search in the Vulnerability Database. The details of each module are depicted in the next sections.

3.1 Vulnerability Search Mechanism (VSM)

The vulnerability search and indexing process is made by a spider mechanism. A spider is a program that explores the Internet by retrieving a document and recursively retrieving some or all the documents that are referenced in it. It acts as an untiring human being who follows all links he finds in a web site, and all the links in the subsequent documents he sees. The spider indexes (fully or partially) all the documents that it accesses into a database, which can afterwards be used by a search engine. The spider tool used in SisBrAV will be `htdig`, which is one of the programs that constitute the `Ht://Dig` package (6). `Ht://Dig` is a free web search engine, created in accordance to the GNU (General Public License) rules, and is consisted of many individual programs, like `htdig`, `htdump` and others. The most recent stable version of `Ht://Dig` is 3.1.6, so this will probably be the version implemented in SisBrAV. A brief description of the `htdig` program is necessary, for there are some options which are used in the system, for its best performance and accuracy.

`Htdig` is a spider program (or search robot), which does what is called the "digging" process, retrieving HTML documents using the HTTP protocol, gathering information from these documents and indexing them, creating specific database files which can then be used to perform a search through these documents.

`Htdig` has many options, which are/will be used in the SisBrAV system, either to produce a desired result or for debugging purposes. The `-c <configfile>` option specifies another configuration file instead of the default. Another important option is the `-h <maxhops>` option, used to restrict the dig to documents that are at most `maxhops` links away from the starting document. This option is used every time the initial digging is run, to assure that `htdig` will index only the relevant documents for each site. The `-i` option is used to perform an initial digging. With this option, the old databases are removed, and new ones are created. There are also some options very useful for debugging, such as `-s` and `-v`, used to print statistics about the dig after completion and to set the verbose mode, respectively. For test purposes, one important option is the `-t` option, which tells `htdig` to create an ASCII version of the document database, making it easier to parse with other programs, so that information can be extracted from it for purposes other than searching. It generates the files `db.docs` and `db.worddump`, which formats will be explained later. Finally, the `url_file` argument can also be passed, telling `htdig` to get the URLs to start indexing from the file provided, overriding the default `start_url` in the configuration file.

As said before, when using `htdig` with the `-t` option, it produces two ASCII files, `db.docs` and `db.worddump`. The `db.docs` file contains a series of lines, each of them

relating to an indexed document. The lines contain information such as the document URL, title, modification time, size, meta description, excerpt, and many other useful document information. The `db.wordlist` file has a line for each word found in the indexed documents. Each line in this file contains a word, followed by the document ID where it was found, its location in the document, its weight, number of occurrences, etc. The default configuration file for `htdig` is the file `htdig.conf`. That's where all configuration options for `htdig` (and the other tools, if they are used) are set. Since all of its parameters will probably be left with their default values, this file's content will not be copied in this paper. At first, the security sites indexed by `SisBrAV`'s `htdig` will be the ones listed in the items (5), (7), (8), (9) and (10) in the References section. The number of sites can be (and will be) expanded to a much higher number, but initially only these five sites were chosen. The way `htdig` indexes each site will be almost the same: the only parameter that will differ from one site to another is the number of hops from the starting URL. For example, if `maxhops` is set to 2, `htdig` will index the starting URL, then it will follow all the links in that URL and index all the documents, and finally it will also follow the links in these documents, indexing the documents it finds, and then stop the digging process. Since each site has its way of displaying their documents, the number of hops necessary to gather all relevant vulnerability information will vary from site to site.

To solve this issue, a simple UNIX bash script will be used to read a file that contains lines with an URL and a number (which defines the maximum hops from the initial URL), separated by a TAB. The script will produce different `htdig` commands, according to the number of maximum hops defined. The number of maximum hops for each site is defined by the `SisBrAV` administrators, who inspect the sites and check the number of levels the spider will have to crawl down in order to obtain the maximum amount of relevant information about the vulnerabilities, and the minimum unnecessary information. `Htdig` generates several Berkeley DB type files. These files will then be analyzed by the IPS Module, as explained in the next section.

3.2 Interpreter, Parser and Sorter (IPS)

The IPS Module will probably be written in Java. It will use an heuristics algorithm to perform the content analysis of the data stored in the Berkeley DB files created by `htdig`, in order to feed the Central Database with accurate vulnerability information. The data is parsed and the vulnerabilities are grouped between previously determined, hierarchically distributed classes. At first, the IPS program will perform the sorting process. Initially, it analyses all the entries in the database, to find ambiguous or duplicated information for a same vulnerability. Then, it parses the content of the information, in order to group the vulnerability entries in classes, according to its main aspects: remote/local, type, low/medium/high importance score, etc. It also determines the systems/services in which that vulnerability occurs. If there is more than one entry for the same vulnerability, it correlates all the information found in the entries, to make sure the attributes are set as precisely as possible. For example, if a given vulnerability is issued in three different sites, and one of them scores the vulnerability as of medium importance and the others say its importance is high, the IPS will set this attribute to "high". The hierarchical class tree used to group the vulnerabilities is described in Fig. 1. Each document indexed by the spider in the

VSM module will be related to a specific vulnerability. The IPS module performs the vulnerability sorting process for each document, by following the tree shown in the above figure. Initially, the algorithm determines if the vulnerability is local or remote, according to the information found in the document. It then classifies the vulnerability into a specific vulnerability type, among the predefined types registered in the system, such as Denial of Service, Buffer Overflow, Password Retrieval, Authentication Bypass, etc. Afterwards, an importance score is assigned to the vulnerability. At last, the IPS finds out what operating systems – and their versions – are affected by the vulnerability, and what programs/services – and their versions – are threatened by it. As well as the vulnerability types, there will also be a large list of systems and services (and their respective versions), which IPS will use in the sorting process.

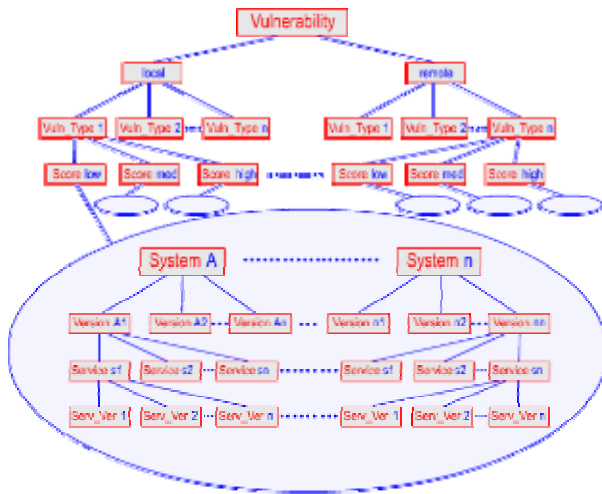


Fig. 1. IPS – Hierarchical Classes Tree

After a given vulnerability is sorted, the IPS checks if there is any other vulnerability with exactly the same characteristics, affecting the same systems/services. If so, it performs a series of tests, to check if both entries refer to the same vulnerabilities. In these tests, other information is analyzed, such as the vulnerability date, the document URL (if the root site is the same, it's probably not the same vulnerability, since a security site must not have duplicated documents for the same vulnerability), and other information. After the vulnerabilities have been classified, the IPS feeds the Central Database with that data. Since the database is not hierarchical, but relational, the IPS will also have to convert the results of the sorting process before actually feeding the Central Database.

3.3 Central Database (CDB)

In order to store all the information regarding vulnerabilities and their attributes, clients' profiles, systems and services data, as well as the English-Portuguese translation data, SisBrAV will have a Central Database. It is most likely that it will be

implemented using a MySQL server, which is GPU compliant, and its architecture will follow the SQL ANSI standard, to guarantee its portability and scalability. The CDB will be divided into three smaller databases, each one storing specific information, although the three of them relate to each other. The first database is the Vulnerability Database, which will contain all the vulnerability information already sorted into defined groups, as seen in the IPS section. The second base is the Client Database, which will keep the client-related data, such as their names, contact information and the systems and software running in their environment. At last, the third database will be the English-Portuguese Translation Database, storing a number of keywords, each one relating to keywords in the other idiom, according to certain parameters. Mostly based on the schema designed by the Open Source Vulnerability Database Team (5), the Vulnerability Database is the most important part of the whole SisBrAV system, for it is the central repository of all vulnerability information. Its structure, which is still being developed, will probably keep the main OSVDB structure, although there will be some changes in certain tables, and other tables will be removed or added. The Vulnerability Database, when fully implemented, will be similar to Fig. 2.

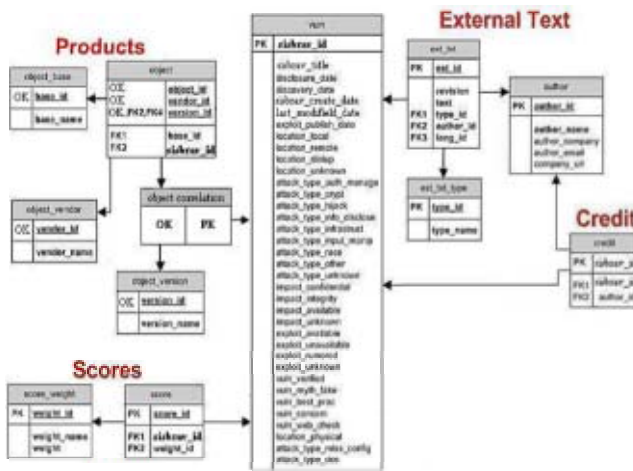


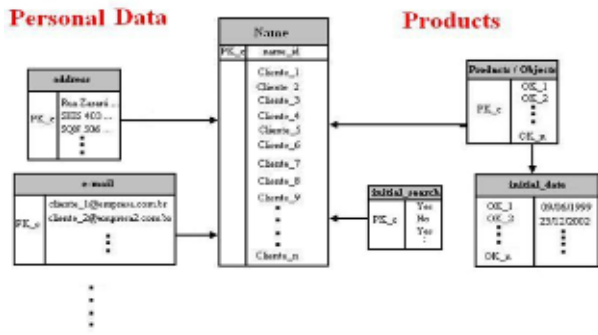
Fig. 2. Vulnerability Database Schema

The External Text section in this database consists in tables that describe certain aspects about a vulnerability. They exist inside the database, but usually describe information that one would use externally to the database. For example, a Solution Description, or a Vulnerability Description is an external text.

The tables in the above schema also deserve some explanation. The vuln table is the main table in the schema. It's where the SisBrAV IDs live. Other information stored in this table includes various dates and vulnerability classification data. The ext_txt_type table defines the types of external texts. For example, Vulnerability Description, Solution Description, Technical Description, Manual Testing Notes. The ext_txt table stores the external text blobs for any type of text that is larger than 1024

characters. Other information stored is the language, type, author, and revision. When the texts are updated/fixed/modified the new text is reinserted into this table and the revision number is incremented. The contributors for anything in the ext_txt table are identified in the author table, making it possible to have a contributor's line to any SisBrAV ID. The authors are used to track the external text authors, as well as the credited researcher of each vulnerability. In the Products section, the object correlation table performs a link between the PK of the vuln table and a key named Object Key (OK). As a result, it is possible for other tables to link to the Products tables without using a PK. The object table binds vendor, base, version and vulnerability together, storing product information. The name object might seem sort of vague, but it means the object that the vulnerability exists within. The object_base table contains product names. For example, Windows, Exchange, Apache, and MySQL are all examples of product names. The object_vendor table contains the vendor names. For example, Microsoft, Sun Microsystems, and Apache Software Foundation are all examples of vendor names. The object_version table contains the version names. For example, 1.0, 2.0, 0.1, XP, 2000, or 95 are all examples of version names. Another crucial table is the score table, used to bind a scoring weight to a vulnerability. It is intended to allow every vulnerability in the database to be associated with one scoring weight. The score_weight table is used to store any type of scoring information needed for scoring calculations. Finally, the credit table adds support for identifying credit for discovering a vulnerability. Instead of storing author like information, a reference to the author table is made, as the data is extremely similar.

The second part of the CDB is the Client Database, responsible for storing all client-related data, involving personal/enterprise identification information, contact emails, products (systems and services) running, etc. Its structure is shown in Fig. 3.



Personal Data section. Contact emails, telephone numbers, addresses and personal/enterprise information, as well as the clients' passwords are entered in this part of the database.

The Name table consists in the main table of the Client Database, containing each client's account ID. All the clients are bound to their products through the Products/Objects table. The initial_date table stores the initial date to search for vulnerabilities, for each product a client registers in the database, while the Initial_search table contains entries that specify if a client is a new registered client in the system (represented by a "Yes" entry) or not ("No"). These entries are used by E-Note, to define if an initial search must be executed or not. At last, the Personal Data tables, such as address, e-mail and others, store client specific information, such as email, telephone numbers, address, personal/enterprise information and login username and password.

The last subpart of the CDB is the English-Portuguese Translation Database, which is still being designed. It will contain a large number of keywords in English and in Portuguese, in addition to semantics and syntax rules, making it possible for the E-Note module to translate the main description of a vulnerability entry to compose a mainly Portuguese email alert.

3.4 Email Notifier (E-Note)

This program will look for updated vulnerability information in the database. After retrieving the information, the program checks, for each registered client, if there are any new/updated vulnerabilities which affect the client's environment. If so, an email message – in Portuguese – is formatted, to inform the client about the new vulnerabilities discovered in his systems and services. This message consists in a brief explanation of the vulnerability, in Portuguese, and one or more links for further information on that issue.

When a client registers in the SisBrAV system, he will have to inform what systems he has and what programs he runs, thus defining the scope of vulnerabilities SisBrAV should be concerned with, when generating alerts to that specific client. Besides that, the client also defines the start date, determining the initial point from which the system should begin the search in the vulnerability database. With that data in hands, E-Note will search in the database only the information that is really necessary for that client, generating a customized email message to him.

The E-Note module will also be written in Java, to guarantee its portability. E-Note is divided in two programs: one program performs the search in the database and the other sends the email alert.

For each new client added in the system, all the data about his systems and services is stored in the clients table, in the SisBrAV database, and a flag is set for this client, with a logical value that represents "NEW". The start date from which he wants to be informed about existing vulnerabilities is also stored in the database clients table.

Every time E-Note is run, it checks if there are any new clients in order to search for all the vulnerability entries that occur specifically in their systems and are newer than the start date defined by the client. It then generates the email alert to those clients, notifying about all vulnerabilities found. Afterwards, the "NEW" flag in the clients' entry in the database is set to a value that stands for "OLD". For existing

clients, the E-Note will simply check if there are new/updated vulnerabilities regarding their systems/services. If so, it generates the email alert for the specific clients whose systems are affected.

Due to the fact that the vulnerability information stored in the database is mainly in English, the vulnerabilities selected by E-Note are also in English. To make it possible for E-Note to generate Portuguese messages, an English-Portuguese translation database will bind English keywords to previously defined Portuguese sentences. E-Note performs, thus, a simple translation in the main vulnerability description. The main aspects – remote/local, high/low importance, etc – of the vulnerability are also translated. For example, if the main description of a vulnerability is “HP-UX DCE Remote Denial of Service Vulnerability”, and its importance is critical, the Portuguese message would be “HP-UX DCE: Vulnerabilidade Remota de Negação de Serviço. Importância: Crítica”. The translation database is in the format described in the previous section.

Along with the main description of the vulnerability, the email also contains links to the sites where that vulnerability is described and discussed.

3.5 Vulnerability Web Server (VWS)

The idea of SisBrAV is not only to inform its users, emailing them alerts about vulnerability issues. The registered clients will also be able to perform a custom search in the Vulnerability Database through the web. With that functionality in mind, the fifth module of SisBrAV will be a Web Server that will handle these web requests. The users will access an authentication site, where they provide their username and password (which are created and informed to him/her during the registering process). If successfully authenticated, they will be redirected to a customized database search page. The site interface is being designed to be friendly and simple, although its security will be fundamental. The web site will probably be based in PHP, due to the fact that this language is very portable, and through its use, the database access can be implemented in a secure and simple manner. The web server chosen for the SisBrAV system was Apache, mainly because it is a multi-platform server, and also because fully supports the web publishing technology which will probably be used (PHP). There are also other technologies which utilization is currently in discussion, such as Java servlets or JSP, because through using it would be easier to integrate the VWS module to the other modules in SisBrAV. XML is also in discussion, since it is another efficient way of implementing the database access from web. If JSP ends up being implemented, Tomcat (which is the servlet container that is used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies, fully integrated with Apache) will also be used.

4 Conclusions

In the current scenario, it is really important for anyone connected to the World Wide Web to protect his/her systems and data against the threats that continually arise. Besides having a nice antivirus tool, a firewall efficiently configured and other security technologies implemented in their network, users and enterprises must keep

all of their Operating Systems, services and other software up-to-date, by applying all their latest patches and fixes. With that in mind, it's of great importance that systems and network administrators be informed quickly about any vulnerability that may be encountered in their systems, so that they can act proactively to build up defense countermeasures to guarantee the security of their environment. SisBrAV will be an important security innovation, since it implements an idea of an automatic vulnerability searching and alerting mechanism, with very little human administration needed. Since it will have many trustable security sites as sources where it will look for vulnerabilities information, SisBrAV will be a very reliable system, extending the horizons of systems and network security. In addition to that features, it is also important to remember SisBrAV, being a Brazilian project, will implement a translation feature in order to produce Portuguese email alerts, so that Brazilian clients will feel comfortable with it. In the future, the language support can be expanded to other idioms. Nowadays, where free software gradually gains space in the software business, a program must support many platforms, so that it can be installed in a variety of systems and interact with different technologies without incurring into stability loss or performance troubles. SisBrAV is being designed using only free software products and platform independent languages, resulting in a solution with great portability and scalability.

Acknowledgements

GASS's work is supported by the Spanish Ministry of Education and Science (MEC) under project TSI2005-00986.

References

1. Deitel, H. M. – Java, Como Programar / H. M. Deitel e P. J. Deitel; trad. Carlos Arthur. Lang Lisboa. – 4.ed. – Porto Alegre: Bookman, 2003.
2. SQL Tutorial. Available from: <http://www.w3schools.com/sql>.
3. PHP/MySQL Tutorial. Available from: <http://www.freewebmasterhelp.com/tutorials/phpmysql>.
4. Portal Java Home Page. Available from: <http://www.portaljava.com/home/index.php>.
5. Open Source Vulnerability Database. Available from: <http://www.osvdb.org>.
6. Ht://Dig Project Home Page. Available from: <http://www.htdig.org>.
7. Internet Security Systems X-force Home Page. Available from: <http://xforce.iss.net>.
8. Cert Knowledge Base. Available from: <http://www.cert.org/kb>.
9. SANS Newsletters. Available from: <http://www.sans.org/newsletters>.
10. Security Focus Home Page. Available from: <http://www.securityfocus.com>.

Performance Analysis of Dynamic Host Isolation System in Wireless Mobile Networks

Hyuncheol Kim^{1,*}, Seongjin Ahn^{2,**}, and Junkyun Choi¹

¹ School of Engineering, Information and Communications University,
119 Munjiro, Yuseong-Gu, Daejeon, Korea, 350-714

pharbor, jkchoi@icu.ac.kr

² Dept. of Computer Education, Sungkyunkwan University,
53 Myungryun-Dong, Jongro-Gu, Seoul, Korea, 110-745

sjahn@comedu.skku.ac.kr

Abstract. Network survivability nowadays has priority over everything for both network design and implementation. The key focus on the network security is securing individual components as well as preventing unauthorized access to network services. Ironically, Address Resolution Protocol (ARP) poisoning and spoofing techniques can be used to prohibit unauthorized network access and resource occupations. Our work deals with simulation of intrusion traffic by explicitly generating data packets that contain ARP spoofing packets. In this paper we report experimental studies of simulation efficiency and network performance of simulated networks using a host isolation system to capture duplicate ARP spoofing attacks. The Virtual Local Area Network (VLAN) based network access control framework proposed in this paper works in parallel with the policy based real-time access control function to make the utmost use of the network resources and to provide a high-quality service to the user.

1 Introduction

Along with development of communication networks, the problem of network security has increasingly become a global challenge. The more access that is provided, the greater is the danger of increased vulnerability for hackers to exploit. Network survivability nowadays has priority over everything for both network design and implementation. Reflecting through these trends, the key focus on the network security is securing individual components as well as preventing unauthorized access to network services [1].

Although Wireless networks are the most popular Local Area Networks (LANs) nowadays, an ignorance of the network security in designing TCP/IP

* This work was supported by grant No. R01-2004-000-10618-0(2005) from the Basic Research Program of the Korea Science & Engineering Foundation. This work was also supported in part by MIC, Korea under the ITRC program supervised by the IITA (IITA-2005-(ITAC1090050200070001000100100)).

** Corresponding Author.

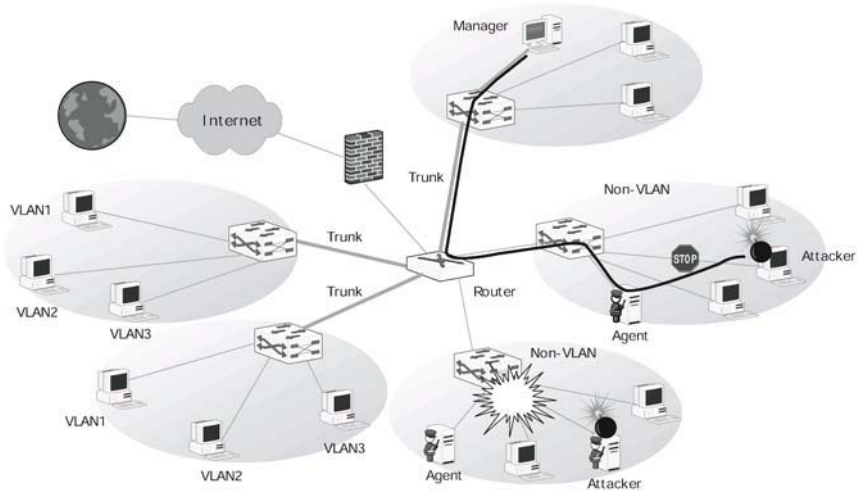


Fig. 1. Duplicate ARP spoofing attack

(Transmission Control Protocol and Internet Protocol) has led important network resources such as servers and hosts to be wasted or damaged. Particularly, IP addresses and Media Access Control (MAC) addresses, limited and important resources, are increasingly misused, which results from its inexperienced and malevolent purposes to cause a security problem or damage the entire networks.

Currently, the major focus on the network security is securing individual components as well as preventing unauthorized access to network services. Ironically, ARP poisoning and spoofing techniques can be used to prohibit unauthorized network access and resource occupations. The protecting ARP which relies on hosts caching reply messages can be the primary method in obstructing the misuse of the network [1][2][3]. However, As shown in Fig.1, traditional host isolation systems that use ARP spoofing can not be applied when attacker use identical IP and MAC address with agent system.

Our research is focused on the studies of network intrusions and their effects on the network in a simulated environment. In this paper we report our experimental results of network performance measures and simulation efficiency of networks under the duplicate ARP spoofing attacks, all simulated using OPNET™.

We also investigate the performance of VLAN-based host isolation system using simulation based on the designed models. In the simulation, a number of traffics are used to study how well host isolation system performs with traffic found in real network environments.

The rest of this paper is organized as follows. The proposed access control system architecture and functional components are described in section 2. Section 3 presents model development issues, and Section 4 analyzes the various performance of the host isolation system using simulation. Finally, Conclusions were drawn in Section 5 about behavior of the proposed isolation control schemes based on analysis of collected statistics.

2 Duplicate ARP Spoofing

2.1 Traditional Host Isolation Scheme

As an IP address is the only one to identify itself, the same IP address cannot be simultaneously used in other equipments. If IP addresses, which are respectively set by hosts in the network, are misused for some inexperienced or malevolent purposes, the security problem could be triggered in the network [4][5].

Wireless local area networks use ARP to resolve IP addresses into hardware, or MAC addresses. All the hosts in the network maintain an ARP cache which includes the IP address and the resolved hardware or MAC addresses. ARP resolution is invoked when a new IP address has to be resolved or when an entry in the cache expires. The ARP poisoning and spoofing attack can easily occur when a malicious user tries to modify the association of an IP address and its corresponding hardware or MAC address by disguising himself of being an innocent host [3].

If a manager want to block a host (B) that uses the specific IP, the Agent system (A) applies the target IP address and the incorrect MAC address to the source address of the ARP Request to transmit an incorrect MAC address to other hosts in the network as the ARP spoofing, when (B) appears a message to give warn against an IP address collision in the network, and other hosts have incorrect MAC address for (B) in the network so that the (B) is disabled while storing the ARP cache.

If a common host (C) requests access to the blocked host (B) in the same network, the Agent (A) checks the ARP Request message to transmit (B)'s ARP Response message to (C). And the (A) Send the ARP request packet that has incorrect MAC address of (B). Then, the ARP cache table is updated in (C) with the incorrect MAC address of (B), which leads to a failure in the communications. Although some hosts has already had a MAC address of the blocked host, the Agent transmits the incorrect MAC address to other hosts through the ARP Spoofing to update the ARP cache table of all blocked hosts in the network.

The Gratuitous ARP checks if there is any other host using its IP address when the host initially boots itself to start the network [6]. A system that uses an unauthorized IP address may cause some problems to other hosts using Gratuitous ARP. For example, a server system of which IP address has already been preoccupied by another system during its rebooting cannot use the network. That is, the IP address may cause severe internal security problems in the network, not from externally [8][9][10].

However, As shown in Fig.1, traditional host isolation systems that use ARP spoofing can not be applied when attacker use identical IP and MAC address with agent system that is called duplicate ARP spoofing.

2.2 Proposed Host Isolation Scheme

To deal with the duplicate ARP spoofing attack, As shown in Fig.2, we proposed VALN-based host isolation system. A VLAN is a logical grouping of end stations

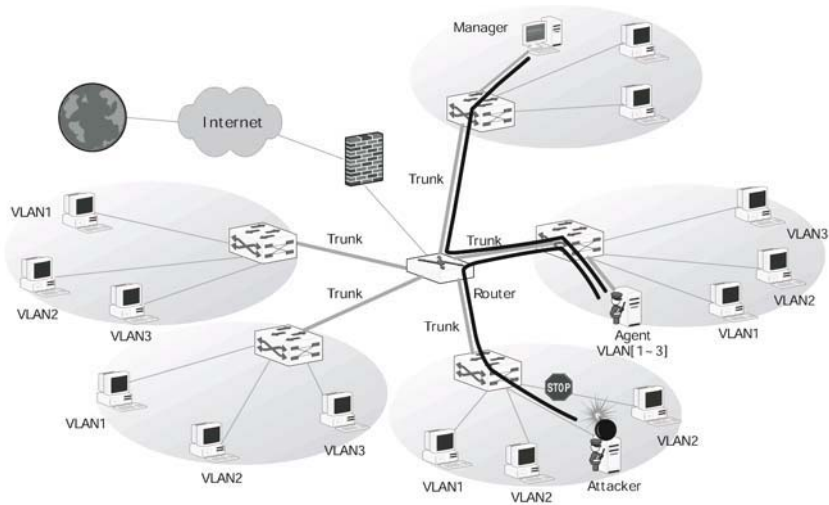


Fig. 2. Proposed VLAN-based host isolation scheme

such that all end stations in the VLAN appear to be on the same physical LAN segment even though they may be geographically separated [7].

End stations are not constrained by their physical location and can communicate as if they were on a common LAN. Because VLAN permit hosts connected to a LAN switch to be grouped into logical groups as a function of some administration strategy, it is very flexible for user/host management, bandwidth allocation and resource optimization.

A host or agent can be a member of the different VLAN simultaneously and temporarily in a multi-netted VLAN. Although multi-netted asymmetric VLAN offers dynamic inter-VLAN connections, VLAN management scheme must have ability to block the host by way of a member host breaks the specific rule, such as illegal behavior and abnormal traffic.

As shown in Fig.2, the agent system need to communicate with multiple VLANs, in which the agent system simultaneously belong to more than one VLAN. All messages are passed to agent system only without damage from manager. Unlike traditional host isolation system, duplicate ARP spoofing attack can be detected by VLAN membership (port) configuration. If attack system is VLAN-unaware device, all frames sent by attack system can only be inserted with the same PVID (port VLAN Identifier) by the switch, thus attack system can't belong to multiple VLANs, and as a result, it can't be accessed by end stations in other VLANs without routers.

3 Model Development

The scenario described above was implemented using OPNET to perform our network security study. Devices used for the tests included VALN-aware switche and generic hubs. For evaluation and analysis of duplicate ARP spoofing, an

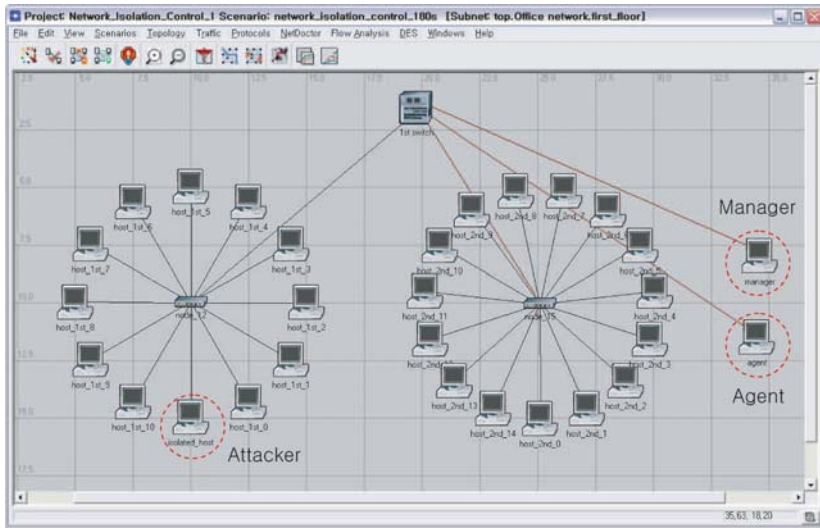


Fig. 3. Network model for duplicate ARP spoofing

extended ARP model and an isolation agent model were designed and implemented in OPNETTM. In order to focus our study in a real life scenario, we researched on a proposal that gave us a comprehensive knowledge about network devices placement and configuration.

3.1 Building Network Models

Fig. 3 shows the OPNETTM model for simulating the duplicate ARP spoofing attack. The network model has been based on a 100 Mbits/s Ethernet LAN and consists of 27 hosts, 1 VLAN-aware switches, 2 hubs, 1 manager, 1 attacker, and 1 agent as shown in Fig. 3. Switch, hosts, hubs, manager and agent nodes are connected by fast ethernet links. The traffic from the sources node to the destinations node is switched through VLAN-aware switch or hubs.

There are 27 hosts arranged into two sub-network in the Fig. 3. Each node in the Fig. 3 is the “generator”, which prepares the packets extracted from the traffic source. Once a packet is ready, it is given to its source host, and from there it will be sent to the destination host through the hub (located at the center of the sub-network).

Since there are 27 distinct IP addresses in the source, the model uses 27 nodes connected to each other through a hub and switch. “isolated_host” (in the left side sub-network) is the “attacker”, and the other nodes are the “victim” of the duplicate ARP spoofing attack.

3.2 Building Process Models

To measure the performance of the proposed host isolation system, a simple node and a process model of agent system were developed. The primary approach to

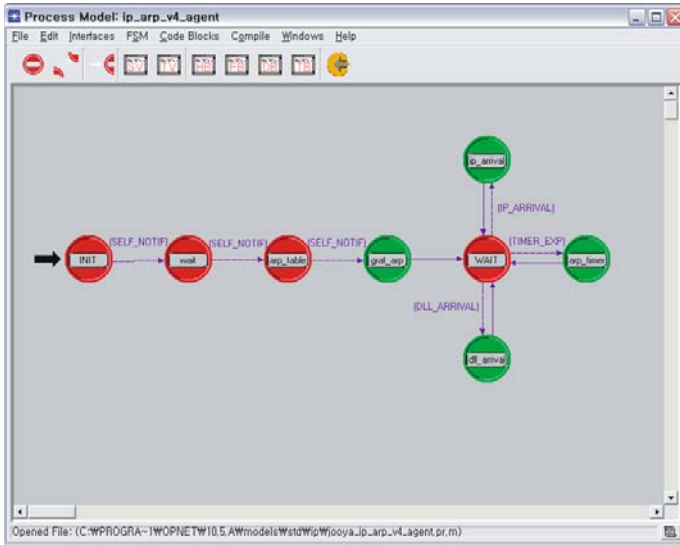


Fig. 4. Process model for duplicate ARP spoofing

the performance analysis of the host isolation model was to build a network topology suitable for such study.

The agent node model has an input and output, performing proposed host isolation operations. Fig. 4 shows the agent node’s process model, comprised of the following states: INIT, WAIT, ARP_TABLE, GRAT_ARP, IP_ARRIVAL, ARP_TIMER, and DLL_ARRIVAL.

INIT state initializes internal data structures. The ARP_TABLE state initialize ARP table of the system. Gratuitous ARP packet is generated when enter the GRAT_ARP state. WAIT state checks if the IP or ARP packet have arrived to it or ARP timers are have expired. If ARP packet has arrived, the DLL_ARRIVAL state updates a ARP table and generates ARP packet. ARP_TIMER state performs aging to update ARP cache.

4 Analysis of Simulation Results

This section presents some results of VALN-aware host isolation scheme simulation that illustrates the impact of host isolation process using ARP spoofing.

On simulating the network to analyze the performance of the proposed isolation scheme several statistics can be collected. These statistics can be collected on the base of per-node or global.

The simulation results are presented in the form of the following graphs:

- End-to-end delay, i.e., the elapsed time for a packet to enter the transport layer at the local host to the time the same packet is forwarded by the transport layer to the application at the remote host.

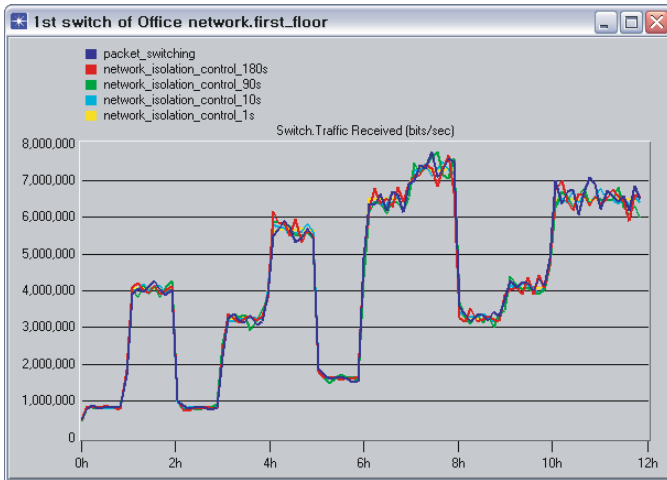


Fig. 5. Network Load

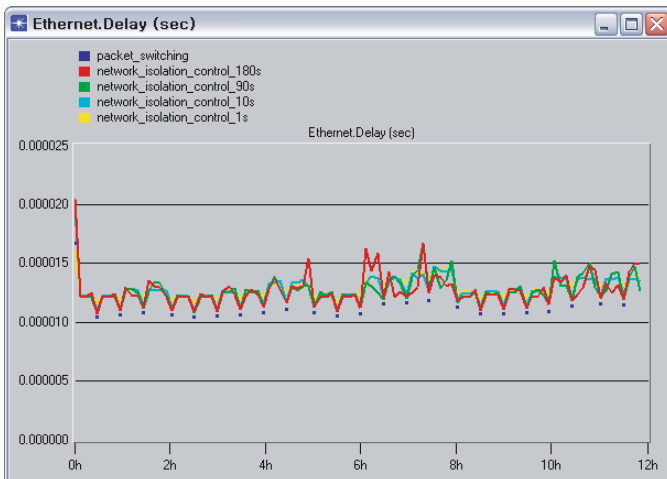


Fig. 6. End-to-end IP packet delay

- Network load, i.e., the total amount of packets that are transferred from source to destination measured with respect to time.

The above parameters depend on the traffic attributes provided to the network. The attributes that control the generating traffic are the inter-arrival time of ARP spoofing packets and the distribution according to which the packet arrivals are spaced out. In the simulation model, the above attributes have been configured so as inter-arrival time equals 1 seconds and the distribution is either exponential or uniform. The exponential distribution emulates the data traffic and the uniform one emulates the real time traffic.

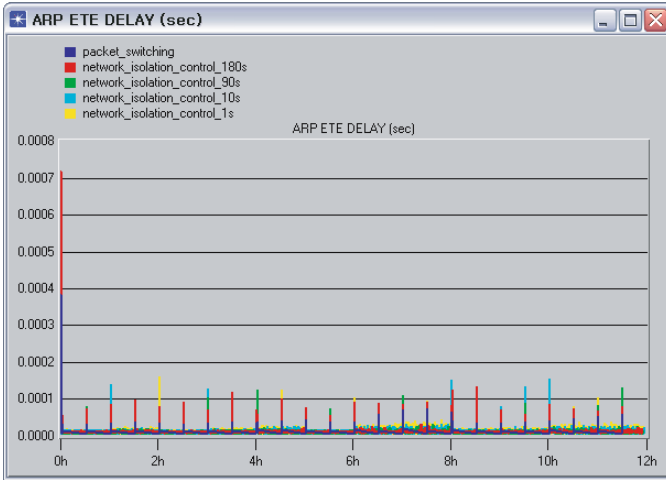


Fig. 7. End-to-end ARP packet delay

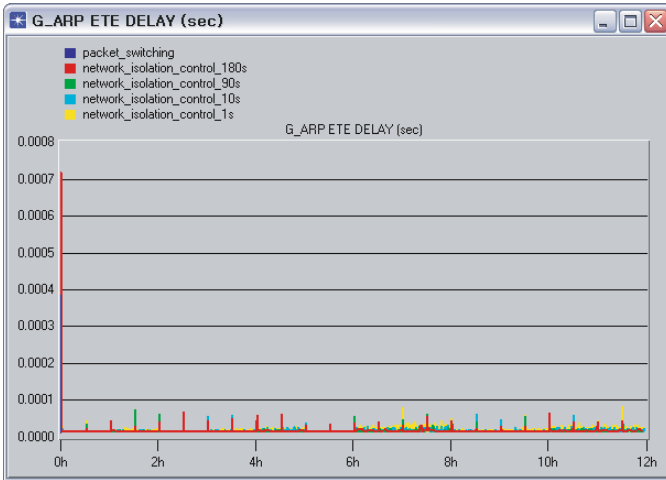


Fig. 8. End-to-end Gratuitous ARP delay

The network traffic pattern is also an important criterion while performing any network or protocol analysis, because the performance or behavioral response of a network or a protocol changes when the traffic packet distribution, attributes of distribution or protocol implementation varies. We have varied these attributes for network analysis, and analyzed the results in different cases.

The obtained results are shown in Fig. 5, Fig. 6, Fig. 7, and Fig. 8. By increasing the number of ARP spoofing packets, we observed a negligible increasing network load. Fig. 5 and Fig. 6 show that an increase in the number of ARP spoofing packets also has an insignificant effect on the mean transfer delay.

Fig. 6, Fig. 7, and Fig. 8 show end-to-end delay of normal packet, ARP packet, and gratuitous ARP packet, respectively. As shown in Fig. 6, Fig. 7, and Fig. 8, end-to-end delay for the proposed isolation scheme has an insignificant effect on the mean transfer delay without regard to the number of duplicate ARP spoofing packets. The reason for these results is based on the mechanisms that the isolation scheme uses one or two fixed size ARP packets.

5 Conclusions

Currently, the major focus on the network security is securing individual components as well as preventing unauthorized access to network services. Ironically, Address Resolution Protocol (ARP) poisoning and spoofing techniques can be used to prohibit unauthorized network access and resource modifications. The protecting ARP which relies on hosts caching reply messages can be the primary method in obstructing the misuse of the network. This paper proposes a network service access control framework, which provides a comprehensive, host-by-host perspective on IP (Internet Protocol) over Ethernet networks security. We will also show how this framework can be applied to network elements including detecting, correcting, and preventing security vulnerabilities.

The purpose of the project was to study and analyze host access control methods using OPNET. We designed two model networks and performed simulation on them in order to understand the working of the duplicate ARP spoofing attack control algorithms and compare their performances. The conclusions we have drawn are based on the parameters we have used in evaluating the performance of the two algorithms and the effectiveness of such parameters in controlling access control.

This study worked upon a system operating under the IPv4 environment, which will come to be needed under the IPv6 that is expected to get its popularity. The same network blocking mechanism as in the IPv4 network can optionally be operated on Internet Control Message Protocol version 6 (ICMPv6). However, the technology allowing the Agent to generate the ICMPv6, not the ARP packet, shall be developed. Upon generating the Neighbor-Advertisement message, the receiving host attempts to direct the new pieces of IP information to the sending host though it does not request the Neighbor-Solicitation message. Thus, the network blocking mechanism can also be applied to the IPv6 environment.

References

1. Hyuncheol Kim, Seongjin Ahn, Sunghae kim, and Jinwook Chung: A Host Protection Framework Against Unauthorized Access for Ensuring Network Survivability, NPC'04, Network and Parallel Computing, Springer-Verlag, Lecture Notes in Computer Science 3222, Oct. (2004) 635–643
2. Wonwoo Choi, Hyuncheol Kim, Seongjin Ahn, and Jinwook Chung: Dynamic Access Control Scheme for Service-based Multi-netted Asymmetric Virtual LAN, ICCSA '05, Computational Science and Its Applications, Springer-Verlag, Lecture Notes in Computer Science 3480, May (2005) 137–145

3. D. Bruschi, A. Ornaghi, et al.: S-ARP: a Secure Address Resolution Protocol, ACSAC '03 (2003) 66–74
4. Hastings, N.E., McLean, P.A.: TCP/IP spoofing fundamentals, Computers and Communications, 1996., Conference Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference (1996) 218–224
5. Ishibashi, H., Yamai, N., Abe, K., Matsuura, T.: A protection method against unauthorized access and address spoofing for open network access systems, Communications, Computers and signal Processing, 2001. PACRIM. 2001 IEEE Pacific Rim Conference (2001) 10-13
6. Bruce McDonald, Taieb Znati, et al.: Comparative Analysis of Neighbor Greeting Protocols: ARP versus ES-IS, SIMULATION '96, Apr. (1996) 71–80
7. D. Ruffen, T. Len, J. Yanacek: Cabletrons SecureFast VLAN Operational Model Version 1.8, IETF RFC 2643, Aug. (1999)
8. WAndrew R. McGee, S. Rao Vasireddy, et al.: A Framework for Ensuring Network Security, Bell Labs Technical Journal, Vol. 8, (2004) 7–27
9. Anirban Chakrabarti, G. Manimaran: Internet Infrastructure Security: A Taxonomy, IEEE Network, Nov./Dec. (2002) 13–21
10. Steven J. Templeton, Karl E. Levitt: Detecting Spoofed Packets, DISCEX03, Vol 1, (2003) 164–175

Meta-model Driven Collaborative Object Analysis Process for Production Planning and Scheduling Domain

Chang Ouk Kim¹, Jun-Geol Baek^{2,*}, and Jin Jun³

¹ Department of Information and Industrial Engineering, Yonsei University,
Sinchon-dong, Seodaemun-gu, Seoul, 120-749, Republic of Korea

² Department of Industrial Systems Engineering, Induk Institute of Technology,
Wolgye-dong, Nowon-gu, Seoul, 139-749, Republic of Korea
jungeol@hanmail.net

³ Department of Computer Science and Engineering, University of Connecticut,
371 Fairfield Road, Storrs, CT, 06269, USA

Abstract. This paper presents a new object-oriented analysis process for creating reusable software components in production planning and scheduling domain. Our process called MeCOMA (Meta-Model Driven Collaborative Object Modeling Approach) is based on three meta-models: physical object meta-model, data object meta-model, and activity object meta-model. After the three meta-models are extended independently for a given production system, they are collaboratively integrated on the basis of an integration pattern. The main advantages of MeCOMA are (1) to reduce software development time and (2) to consistently build reusable production software components.

1 Introduction

Demand of continuous business process re-engineering requires the fundamental rethinking of how information systems are analyzed and designed. It is no longer sufficient to establish a monolithic system for fixed business environments. Information systems which support business processes must be adaptive in nature. One of enabling concepts for the adaptive information system is reusability. Since reusable software components [5] are able to support plug-in-play just like hardware chips, they make it possible for the information system to accommodate the changes of business processes without much modification.

This paper presents a new analysis process for creating such reusable software components in production domain, especially for production planning and scheduling field. Our process is called MeCOMA (Meta-Model Driven Collaborative Object Modeling Approach) and mainly employs object-oriented concepts. To our knowledge, little efforts have been given to object-oriented modeling of high-level production domain, compared with research works toward object-oriented modeling of shop-floor control. In the context of production, most object-oriented models are limited to shop-floor control systems [1][2][9][10][12]. CIM-OSA [6][7] and ARIS

* Corresponding author. Tel: +82-2-950-7606.

[11] are conceptual models that deal with business enterprise. However, the modeling concepts in CIM-OSA and ARIS are also too general to apply for production systems.

Unlike conventional object-oriented methodologies [8], the MeCOMA approach exploits a collaboration scheme of three meta-models: physical object meta-model, data object meta-model, and activity object meta-model. Each of the three meta-models includes invariant conceptual elements with their relationships. It is a mixed approach of top-down method and bottom-up method – the three meta-models are deployed independently for a target production system, after which they are collaboratively integrated on the basis of an integration pattern. Since MeCOMA provides rigorous collaboration pattern, consistent models and components can be derived. The main advantages of the MeCOMA approach are (1) to reduce the software development time and (2) to consistently build reusable production software components.

As far as production system is concerned, two distinguished modeling aspects are discovered compared with business systems such as banks and insurance companies. One is hierarchically recursive structure and the other is coordination task. From the viewpoint of object-orientation, physical production system can be regarded as a recursive structure consisting of layered resources from company at the top level through factories, shops, and cells at the middle levels to machines at the bottom level.

Fig. 1-(a) describes the object-oriented model of the physical structure using composite pattern [4] where constraints are specified inside curly bracket. We use the UML notations [3] to account for object-oriented models. The role of resource is the processing of jobs assigned to the resource. Due to the complexity of planning and scheduling, job at company level is also repetitively decomposed as shown in Fig. 1-(b). Furthermore, Bill-Of-Material (BOM) of end-product has tree form depicted in Fig. 1-(c). Therefore, recursive property can be observed in the structures of physical resources, jobs, and items, respectively.

To make it difficult for modeling this kind of system is that the three recursive structures interact with each other, not being able to analyze them separately. With their coordination behaviors, planning and scheduling activities are carried out. To date, systems that are characterized as the multiple recursive structures with interactions have not been attempted to develop in object-oriented software society.

The decomposition level is dependent on target system. Simple production system may have a company, a factory and several machines. Whereas, complex systems may have several distributed factories, each of them also has shops, many cells in each shop, and several machines in each cell. The objective of this research is to model such various production systems uniformly using the object-oriented meta-models.

We will briefly present a case study in order to assist in understanding of the MeCOMA approach. This system has four physical layers – one company, one factory, two shops, and dozens of machines in each shop. This system manufactures several end-products which are parts of automobiles. From automobile enterprises, the company receives product jobs. Manufacturing plan of each product is prepared using Master Production Schedule (MPS) technique. At factory level, each product plan is exploded to generate part plans using Material Requirement Planning (MRP) technique. According to process plans, parts are scheduled using job shop scheduler at each shop.

The remainder of this paper is organized as follows. Section 2 presents the MeCOMA approach with its application to the case study. Section 3 concludes our research work.

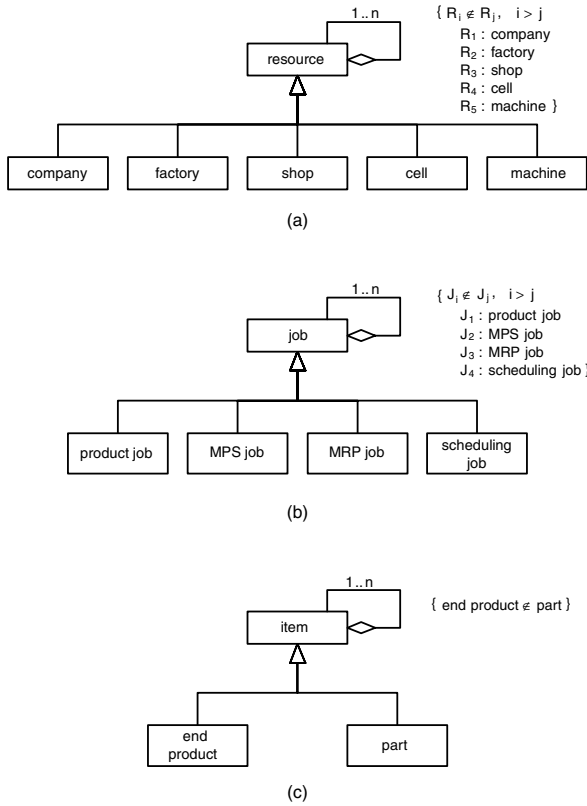


Fig. 1. Recursive structure of (a) resources, (b) jobs, and (c) items

2 The MeCOMA Approach

2.1 Overview

MeCOMA is a meta-model driven process for analyzing the family of production systems in object-oriented way. Here, the meta-model is defined as a set of invariant elements with their relationships. Specifically, MeCOMA is defined as four-tuple:

$$\text{MeCOMA} = \{ \text{PM}, \text{DM}, \text{AM}, \text{CP} \}$$

where, PM – physical object meta-model,
 DM – data object meta-model,
 AM – activity object meta-model,
 CP – collaboration procedure.

PM delineates types of essential real world objects with their relationships, DM classifies production data types, and AM suggests a systematic way of finding production activities. Given a target production system, they are deployed independently, and then integrated using CP which uses an integration pattern.

2.2 Physical Object Meta-model

In this subsection, we will introduce the ontological definition of domain objects required for production planning and scheduling domain. According to dictionary, system is defined as a group of components working together to achieve goals. In the discourse of business organizations, types of components can be categorized as processing entity, processed entity, and coordinator. The goal of this kind of system is to properly engineer the processed entities by the processing entities, while satisfying system constraints. Of the three primary concepts, the role of coordinator is particularly important because they control over the behaviors of the processing entities and processed entities. For each domain, each concept should be specialized.

In the context of production domain, processing units are resources such as companies, factories, shops, cells, and machines, while processed units are items, inventory, resource jobs, and time-phased jobs. The relationships among these objects are shown in Fig. 2-(a). Hereafter, the system consisting of a resource and associated processed objects are called physical system. This system is modeled using the package diagram suggested by UML. A package means a group of semantically related objects.

In Fig. 2-(a), a resource job is a lot of an item that is assigned to manufacturing resource. Ordered products assigned to company and scheduling jobs to shop are typical examples of resource jobs. Due to the complexity of planning and scheduling tasks, a resource job is often divided into several small jobs, each of which is allocated in a fixed time interval. This kind of job is called time-phased jobs. Representative ones are time slot jobs resulting from MPS (Master Production Schedule) and those from MRP (Material Requirement Planning). Resource jobs and time-phased jobs are subclasses of job. Also, as described in Fig. 1, job and item have recursive property. Each item has a set of manufactured product called inventory.

In Fig. 2-(a), two interfaces denoted as hollow circles are linked to resource and resource jobs, respectively. They provide connection points to other physical system – either upper-level system or lower-level system can access the system through the interfaces. On the other hand, the system may need to access others. Dependency relation denoted as dotted line with arrow is used for this possibility. Therefore, three recursive structures in production domain discussed in Fig. 1 can be explained by the recursive structure of the physical system.

One aspect that is not considered in the physical system is the role of coordinator. Virtually, components in production system perform cooperative works under cooperation plans. It is the manager who prepares such cooperation plans. The manager also keeps track of the progress states of the plans, and adjusts them if the actual processing is behind the plans. To take into account this feature in meta-model, the concept of control system is conceived. Fig. 2-(b) shows the control system. It is a logically constructed system embedding a physical system and several sub-control systems.

In the control system, the manager undertakes two important coordination roles – one within its physical system and the other between its physical system and its

sub-control systems. The first role is that the manager generates time-phased jobs for each resource job in its physical system. The second role is that he decomposes the time-phased jobs of its physical system into the resource jobs in the physical systems of the sub-control systems. In general, the manager's roles are performed with the aid of planning or scheduling algorithms. Knowing that the control system is able to comprise its offspring makes the physical object meta-model be flexibly expanded relying upon the structures of target production systems.

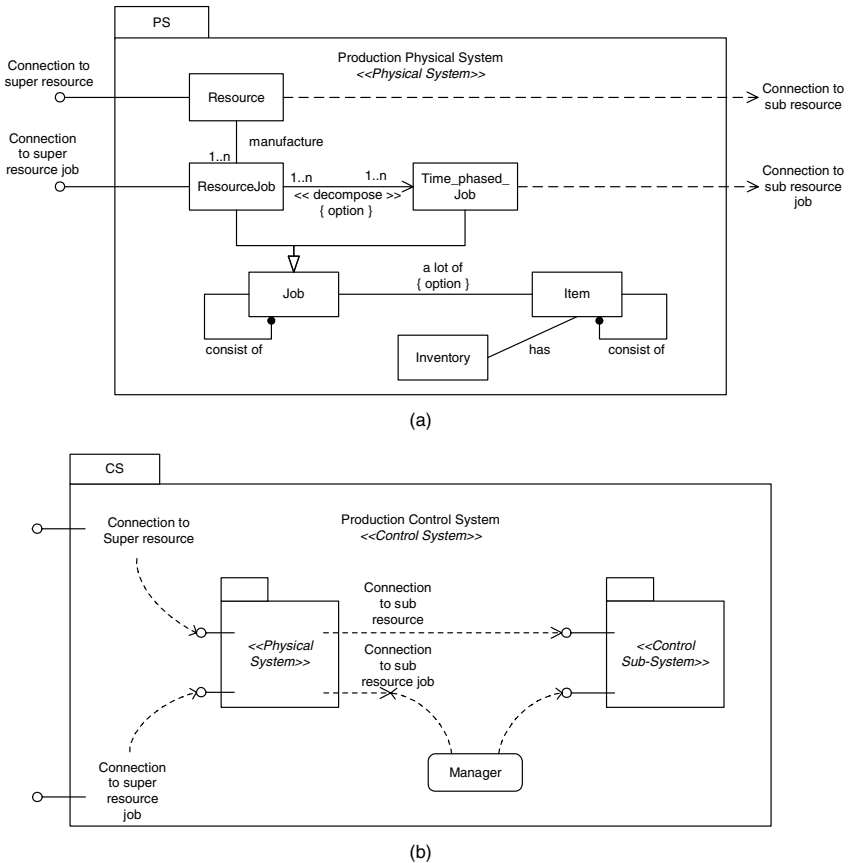


Fig. 2. Physical object meta-model (a) physical system package and (b) control system package

Fig. 3 shows the deployed physical object model for our case study. Note that, in the figure, the shop job in shop PS is not decomposed into time-phased jobs because the shop job is not complex and thus does not require time-phased scheduling such MPS and MRP. The shop job can be directly scheduled on manufacturing machines. The machine CS is the bottom layer in the hierarchy. Therefore, it has no sub control system.

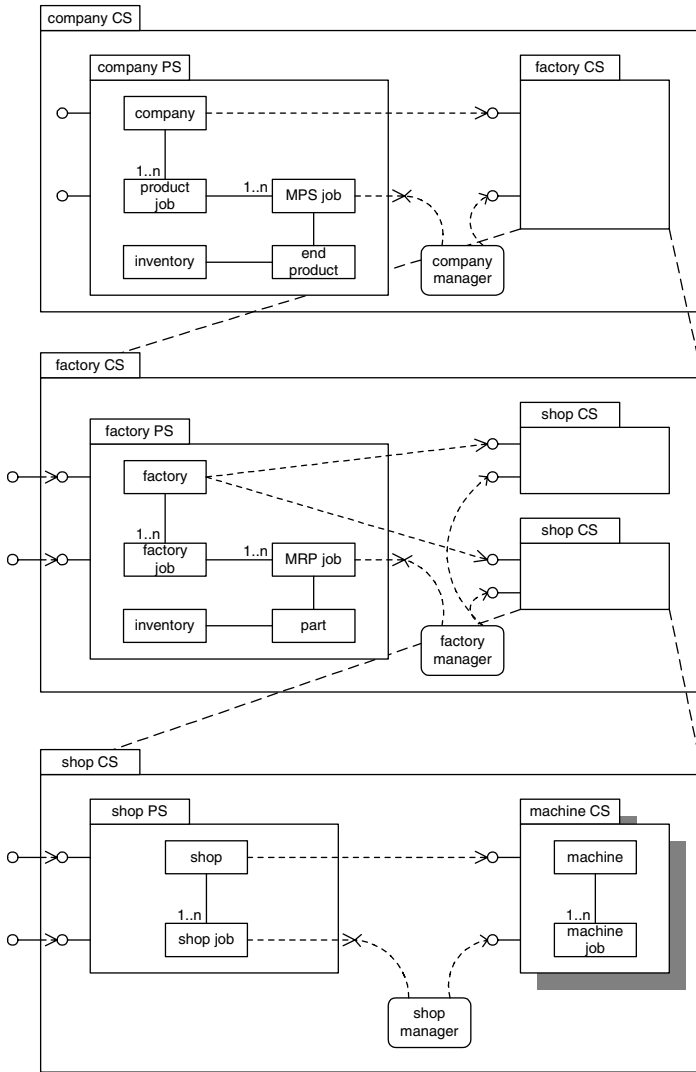


Fig. 3. Deployed physical object model for the case study

2.3 Data Object Meta-model

Associated with each physical object are attributes that describe its properties. In the MeCOMA approach, the attributes are partitioned into semantically related subsets and regard them as individual data objects, because previous experiences tell us that most business information systems define the type of data object as schema and keep the data objects as instantiated tuples of the schema in databases. Hence, it is necessary to analyze business information system coupled with either object-oriented or relational database concept. This idea is realized as data object meta-model in MeCOMA. Fig. 4

shows the data object meta-model. At the first level, the data object meta-model classifies production data into property data objects and relation data objects.

Property data objects express the description, constraints and the current states of physical objects. For instance, item master data object contains descriptive data of item object, resource data object defines the maximum capacity of resource, inventory data object keeps the current level of storage, and so on.

Relation data describe the coordination plans between physical objects. They are further categorized as static data objects and dynamic data objects. In production domain, static data objects imply pre-defined coordination constraints. Of typical are BOM data object that expresses assembly structure among items. Dynamic data objects are coordination data between physical objects. Dynamic data objects are frequently changed by the manager. MPS, MRP, and shop scheduling data are representative ones.

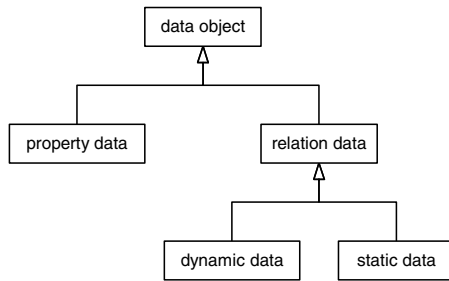


Fig. 4. Data object meta-model

Fig. 5 shows the part of data object model for our case study.

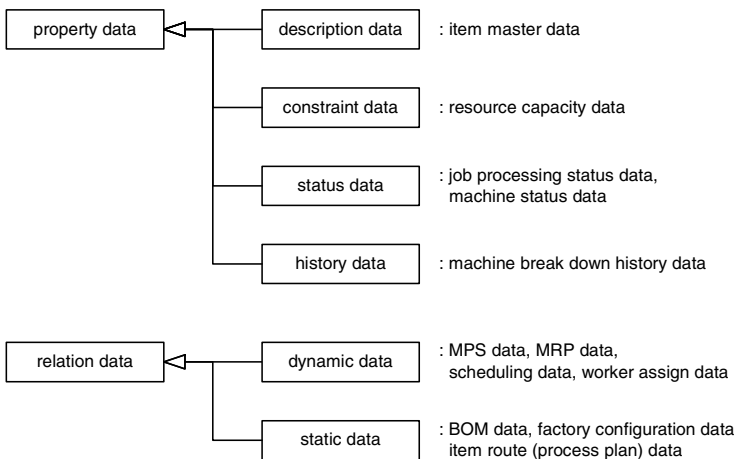


Fig. 5. Part of deployed data object model for the case study

2.4 Activity Object Meta-model

Discovering and representing system activities are the most important step in the analysis of information system. The use case approach [8] is popular one for this purpose. A use case is a narrative, textual description of the sequence of events and activities whereby physical objects with their relationships are derived. This approach does not view use case as an object. Compared with the use case approach, MeCOMA treats activity as an object in that everything that can be conceptualized is object. This fact is reflected in activity object meta-model.

As shown in Fig. 6-(a), an event of interest triggers an activity that can be either operationalized activity or abstracted activity. The former is defined as an activity that only accesses a property data object or a relation data, while the latter is a high-level goal that should be refined until it is materialized by the collaboration of operationalized activities. The refinement is stopped when abstracted activities are realized by operationalized activities.

Operationalized activities are classified into three types: singular activity, social activity, and coordination activity. Singular activity manipulates the property data object of a physical object and is called the operation of the object. Social activity is concerned with behavioral rule associated with human beings. Authorization and confirmation by manager belong to social activities. Coordination activity controls the cooperation of physical objects, so handles dynamic data object.

While the activity refinement step is being progressed, relationships among activities are created. The types of such relationships are depicted in Fig. 6-(b). A parent activity composes more than one child activity. Between them, there exist “AND” composition relationship denoted as dark circle and “OR” composition relationship denoted as hollow circle. Among sibling activities, Parallel and Precede relationships exist. These relationships are dependent on the requirements of production system being explored.

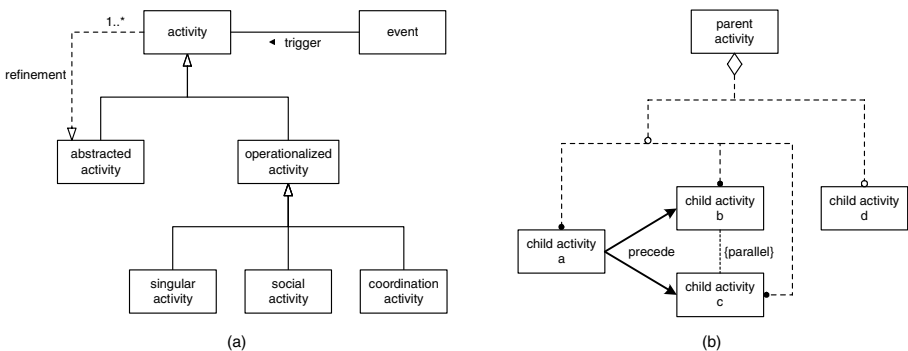


Fig. 6. Activity object meta-model (a) activity object hierarchy and (b) activity relationship

Fig. 7 shows the part of deployed activity object model for our case study. To perform order processing, sub-activity “production planning” is performed before “production execution”. The production planning also has sub-activities MPS, MRP,

scheduling, and purchasing order. Their execution sequence is shown in the figure. The production execution has either manufacturing sub-activity or subcontractor processing sub-activity.

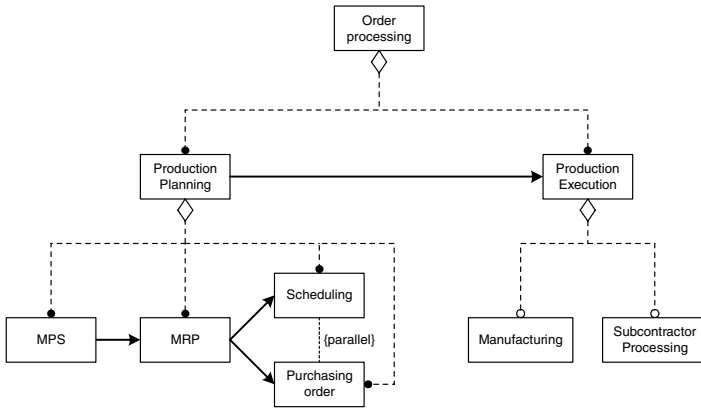


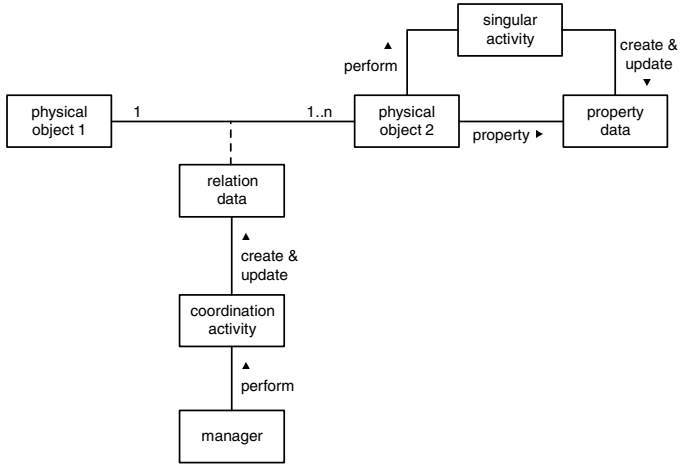
Fig. 7. Deployed activity object model for the case study

2.5 Collaboration Procedure

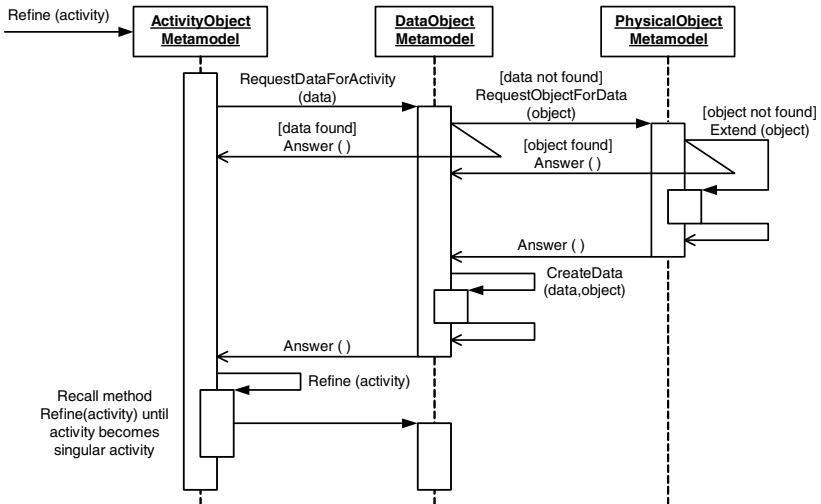
In this subsection, we present an integration method of the three meta-models. Me-COMA puts the same emphasis on the three meta-models. This is materialized through their parallel extensions. Nevertheless, it is necessary to integrate them because they are tightly coupled – activities are done by the cooperation works between physical objects, which are reflected in the data objects related to the physical objects. This fact is illustrated in the integration pattern as shown in Fig. 8-(a).

Associated with each physical object are property data. Between physical objects, there exists a relation data object that specifies their cooperation behavior. According to the type of the relation data object, the cooperation between physical objects is dynamically changed (dynamic data object) or fixed (static data object). Singular activity manipulates a property data object and so is performed by the corresponding physical object. Namely, it will become one of the operations of the physical object at design stage. Manager performs coordination activity and updates associated dynamic data object.

Fig. 8-(b) depicts the collaboration process of the three meta-models using sequence diagram. The meta-models can be expanded concurrently, after which they are synchronized based on the integration pattern. In the collaboration process, data object should be associated with physical objects using the integration pattern. This is also applied between activity object meta-model and data object meta-model. The activity object meta-model requests input and/or output data to the data object meta-model, which is satisfied if such data are declared in the data object meta-model. If not, categorize the data in the data object meta-model and ask the physical object meta-model of associating the data with a physical object or between physical objects. If the physical object meta-model cannot find such object, it should be further unfolded.



(a)



(b)

Fig. 8. Collaboration procedure (a) integration pattern and (b) collaboration process

Fig. 9 shows a part of collaboration procedure for our case study. After parallel extensions of the three meta-models, activity object meta-model requests input and output data of inventory assignment activity to data object meta-model. In this situation, assigned inventory data was not found. Data object meta-model then creates the assigned inventory data object and asks physical object meta-model of the position of the data object. Based on the integration pattern, physical object meta-model associates the data object between resource and inventory. The same procedure is applied to other activities.

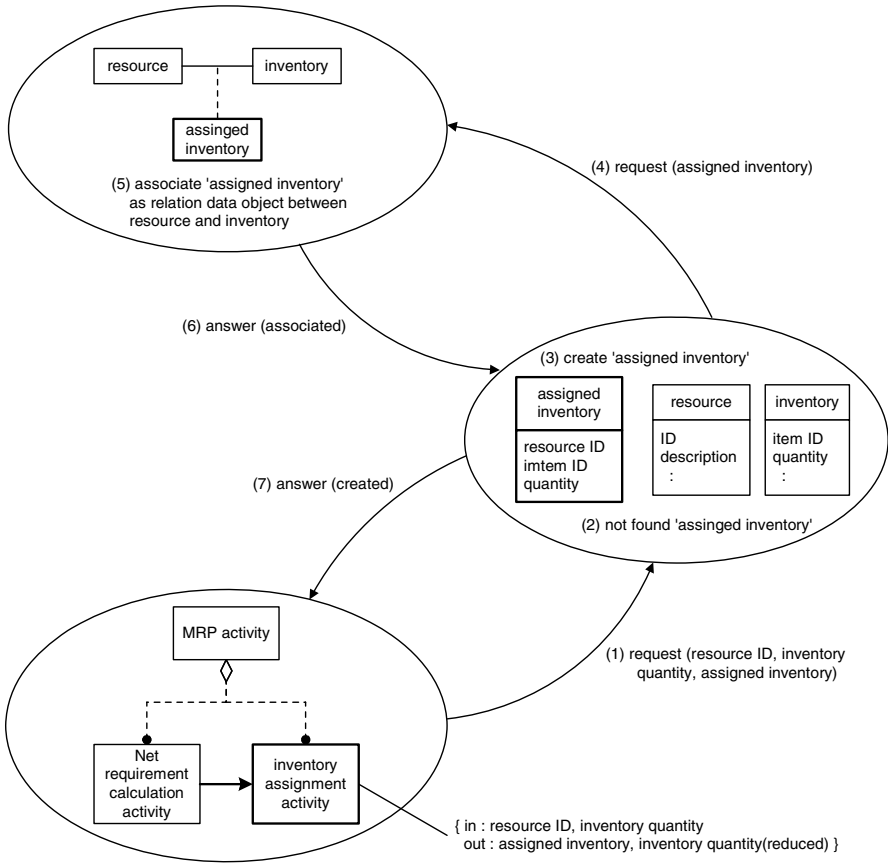


Fig. 9. Collaboration procedure for the case study

3 Conclusion

In this paper, we proposed MeCOMA, an object-oriented way of building hierarchical production planning and scheduling system. We believe that this approach can be used for various types of production system. This was confirmed through an application to a real production company illustrated in this paper. Currently, other cases are also being tested.

References

1. Adiga, S., Object-Oriented Software for Manufacturing Systems, Chapman & Hall, 1993.
2. Doscher, D., and Hodges, R., SEMATECH's experiences with the CIM framework, Communications of the ACM, Vol. 40, No. 10, 82-84, 1997.
3. Eriksson, H.-E., and Penker, M., UML Toolkit, John Wiley & Sons, 1998.

4. Gamma, E., Helm, R., Johnson, R., and Vlissides, J., *Design Patterns – Elements of Reusable Object-Oriented Software*, Addison-Wesley, 1994.
5. Jacobson, I., Griss, M., and Jonsson, P., *Software Reuse: Architecture, Process and Organization for Business Success*, Addison-Wesley, 1997.
6. Jorysz, H. R. and Vernadat, F. B., CIM-OSA part 1: total enterprise modeling and function view, *International Journal of Computer Integrated Manufacturing*, Vol. 3, No. 3-4, 144-156, 1990.
7. Jorysz, H. R. and Vernadat, F. B., CIM-OSA part 2: information view, *International Journal of Computer Integrated Manufacturing*, Vol. 3, No. 3-4, 157-167, 1990.
8. Larman, C., *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and the Unified Process (2nd Edition)*, Prentice-Hall, 2002.
9. Mak, K. L., Wong, S. T. W., and Lau, H. Y. K., An object-oriented rule-based framework for the specification of flexible manufacturing systems, *Computers in Industry*, Vol. 39, 127-146, 1999.
10. Mak, K. L., and Lau, H. Y. K., An object-oriented prototyping tool for automated manufacturing systems, *Computers in Industry*, Vol. 43, 43-60, 2000.
11. Scheer, A.-W., *ARIS – Business Process Frameworks (3rd Edition)*, Springer, 2000.
12. Yalcin, A. and Namballa, R. K., An object-oriented simulation framework for real-time control of automated flexible manufacturing systems, *Computers & industrial engineering*, Vol. 48, No. 1, 111-127, 2005.

Response Against Hacking and Malicious Code in P2P

Wongoo Lee¹, Sijung Kim², and Bonghan Kim³

¹ Korea Institute of Science and Technology Information(KISTI),
Daejeon city, Korea
wglee@kisti.re.kr

² Information Technology Center, ChungJu National University,
ChungJu , Chungbuk, Korea
sjkim6183@hanmir.com

³ Dept. of Computer & Information Engineering, ChongJu University,
Chongju, Chungbuk, Korea
bhkim@cju.ac.kr

Abstract. We have analyzed attacks on and threats to information security, and analyzed information security service in order to provide safe P2P service from these threats. And we have proposed a method to provide information security service studied. It is the method that applies vaccine software to P2P application at peer and designing key distribution protocol to P2P communication environment for confidentiality and integrity.

1 Introduction

P2P(peer to peer) is the service that is provided by technology that connects a person who looks for information with no connection of server computer on the internet to a computer belonged to a person who has information directly in order to share data, and by application the technology. It can search and be provided information directly from the all personal computers. That is how different from established method which has to find out information through search engine on the internet.

However, P2P service is widely open to information security threats by intentional or purposed attack as it transmits data between computers without server. Recently, according to information security industry, it is possible to implant backdoor programs like trojans, backorifice, etc into exchanged files which are serviced in the type of P2P in the country. Unacknowledged user of this can be hacked easily its own computer. When the attacker even finds out the password used on online stock investigation or home-banking, there is a possibility of financial loss. So the problem is getting serious. Also, P2P service is able to convert file extension from document file into MP3 file; therefore, it is possible to draw out the company confidential information in ease. In this case, the chase is almost impossible[1].

Now, there are some P2P hacking tricks published on the famous site related to information security like Security Focus, etc. Therefore, the study is needed to guarantee integrity and confidentiality of P2P network for secure development of P2P service industry. And also the study of prevention on various threats to P2P network and response on that is needed. This paper analyzes information security service

required to transmit various multimedia data safely in P2P. And it also presents key distribution protocols that ensure a response program to hacking in peer and malicious code in order to provide this service, and integrity and confidentiality of the data transmitted.

2 Related Work

The study has been progressing on a P2P system embodiment which considers communication network internationally and on a P2P system embodiment which has no problem with scalability. However there is little study on a method that provides confidentiality and integrity in P2P and response program. This study has been progressing by a few researchers in present. Idota has studied on the field of dangerousness in P2P system, Hiroki has studied on information security threat elements in P2P and information security required, and Paulson, L.D has studied on the kinds and problems of new viruses that targets P2P system. And Simon Kilvington has described threat elements that had happened in real as he mentioned possible threat in P2P networks. The person who has studied on the method for an offer of information security service is Hurwicz and Michael was the one who has introduced the notion of secure data transmission way. Daniel B, Darren G and Navaneeth have dealt with features and advantages of JXTA application for secure P2P programming. William Y and Joseph W have considered the method that can provides secure P2P networking by JXTA. In the field of users' anonymous, Vincent R. Scarlata, Brian N. Levine and Clay S have presented a sharing P2P file system which has anonymous considering responders' anonymity.

3 Information Security Service and Response to in P2P

3.1 Information Security Service in P2P

An organization has to be clear the information security policies that when it opens and shares which data with who or that whether it permits use of PC resources. So, it needs to grasp and check out technical trend of P2P and introduction state of other organization about which P2P software is used inside a post, between posts, between organizations, between user and organization, etc.

Even P2P, new technology, has started from established TCP/IP. A few internet technologies have been chosen to construct to this and it is made of some new functions added there. Therefore, it is important to examine the present internet information security countermeasure by adapting to the features of P2P. Table1 shows specific information security service to vulnerabilities of P2P[2].

3.2 Response on Malicious Code in Peer

User's peer is insecure with no protection on computer malicious code. These malicious attackers achieve an authorization that allows to access to user's computer by the way of deceit by going around imposed restriction which is a simple firewall rule.

Table 1. Security Service and Countermeasure that are requested in P2P

Confidentiality	Technical Countermeasure	<ul style="list-style-type: none"> ✓ File access control ✓ File encryption ✓ Access log management ✓ Personal firewall ✓ Spam mails prevention ✓ Electronic authentication system ✓ Restriction on Installation location of PC using P2P
Integrity	Technical Countermeasure	<ul style="list-style-type: none"> ✓ Traffic control of protocol ✓ Broad-band network maintenance ✓ Application of software retransmission function ✓ Sequential renewal of data ✓ Countermeasure on malicious code
availability	Technical Countermeasure	<ul style="list-style-type: none"> ✓ Employment of parts with high availability ✓ Duplication of hardware ✓ Data backup ✓ Distributed parallel processing ✓ Application of IPv6

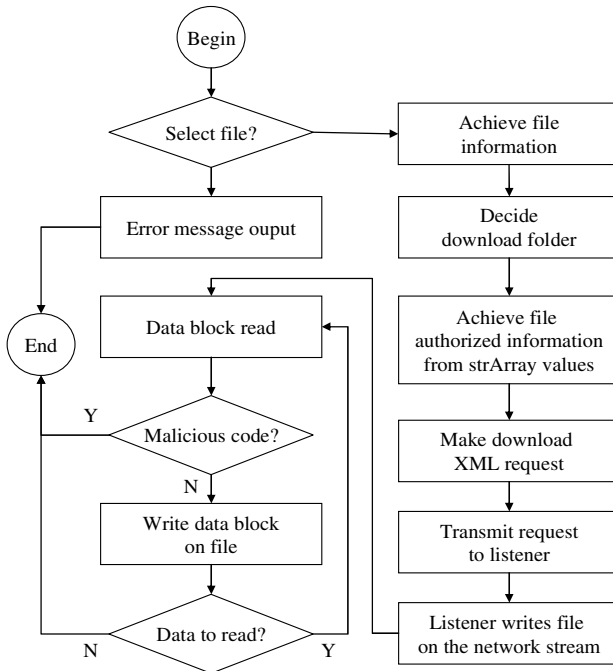


Fig. 1. Applying a malicious code test in a download process

Even if a malicious code invades through various ways, it must be transmitted to user’s computer from exterior. While a malicious code is transmitted through internet, it can be transmitted through user’s floppy disk of local network linkage. Therefore, a firewall is not good enough to protect malicious codes. User needs software that supervises all gates which attacker enters computer interior. A malicious code installs and mutates on its own at the distinguished place. A malicious code grows up by changing application and operating system. Operating system has a potential fault which malicious code can multiply.

The solution is a malicious code software application and finds out update to response it. Update is necessary to prevent established malicious code mutation and new typed malicious code.

Fig.1 shows the location which can apply vaccine program that can examine malicious code to P2P application in the downloading process. User should build a firewall to protect system from inadequate transference or transfer. And also she/he should install malicious code vaccine software to prevent user’s system from malicious code[5][6].

4 An Encryption Key Distributed Protocol Design for P2P

Encryption key distributed protocol meets requirements such as followed so that two concerned parties can trust each other in P2P[4].

- Compatibility

Independent programmers should be able to develop applications by using protocol that can exchange encrypted elements successfully without understanding of others’ codes.

- Scalability

Protocol should be required to provide framework in order to unite new public-key and a large quantity of encrypted methods. This can also prevent a request of generating new protocol and avoids a request of the new information security library.

- Relative Efficiency

Encrypted operation is easy to be an operation with high CPU strength and special public-key. Because of this reason, protocol unites schemes to decrease many linkages and to improve network efficiency.

In this section, it has designed a key distributed protocol to provide confidentiality and integrity to P2P application with server. First, all peers are issued the certificate through user certified procedure when it logs to server at the first time in order to use P2P service. Table2 explains symbols that are used for protocol.

Table 2. Keys used for protocol

Key	description
CEK(Content Encrypted Key)	Encryption-key for confidentiality of content
CHK(Content Hash Key)	Hash-key for integrity
KR	Public-key to transfer CEK
KU	Private-key to get CEK
T	Token for applied peer
CERT	Certificate for applied peer

All peers process log-in procedure like fig.2.

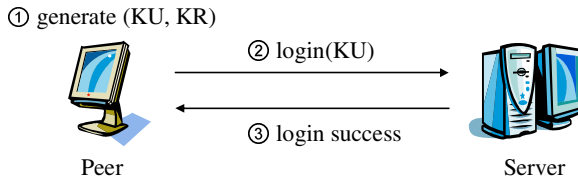


Fig. 2. Log-in Procedures of Peers

- ① All peers generates public keys (KU, KR).
- ② All peers log in the server.
- ③ The server examines whether user is right and responds with a succeed message.
- ④ Peer B transfers a message that searches for specific file name to the server like fig.3.
- ⑤ The server responds usable peers list to according to file name.
- ⑥ Peer B transfers download request file that is located peer A to the server.
- ⑦ The server responds detailed information including IP address, port, A_{KU} of Peer A.

Search-Respond(IP, Port, A_{KU})

- ⑧ Peer B generates token. Token is consisted of random number and timestamp. For the connection of peers, the message is transferred to request files like as followed.

FILE-Request($A_{KU}\{B_{CERT}, B_{KU}, B_T\}$)

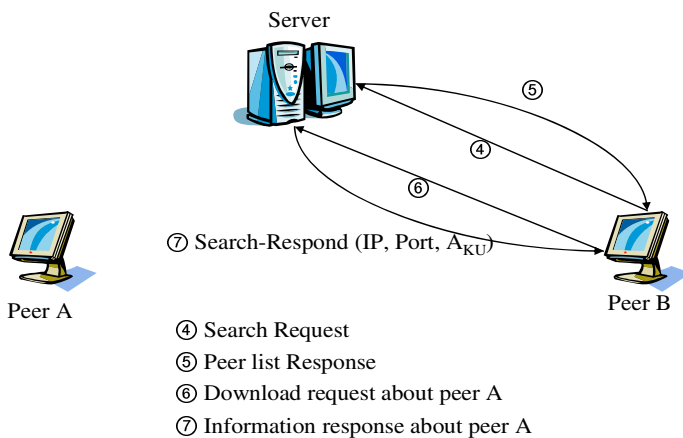


Fig. 3. Peer Search Procedures for a Specific File

which vaccine software is applied to P2P application in peer. Secondly, the method which is to design key distributed protocol for confidentiality and integrity, and applies to P2P communication environment.

The proposed methods are not methods for the perfect P2P information security. Further study needs to embody P2P encryption protocol through proposed design and a P2P application solution united all these dealing plans is needed.

References

1. Hurwicz, Michael, "Peer pressure: Securing P2P networking," Network Magazine, vol.17, no.2, February, 2002.
2. Idota, Hiroki, "The Issues for Information Security of Peer-to -Peer," Osaka Economic Papers, Vol.51, No.3, December 2001.
3. Simon Kilvington, "The dangers of P2P networks," Computer Weekly, Sept 20. 2001.
4. Dana Moore, John Hebler, "*Peer to Peer: Building Secure, Scalable, and Manageable Network*," McGrawHill, 2002.
5. Dreamtech Software Team, "*Peer to peer Application Development: Cracking the Code*," John Wiley & Sons, 2001.
6. Daniel B, Darren G, Navaneeth, "*JXTA: Java P2P Programming*," SAMS, 2002.

Two Efficient and Secure Authentication Schemes Using Smart Cards*

Youngsook Lee, Junghyun Nam, Seungjoo Kim, and Dongho Won**

Information Security Group, Sungkyunkwan University, Korea
{yslee, jhnam, skim, dhwon}@security.re.kr

Abstract. A mutual authentication scheme is a two-party protocol designed to allow the communicating parties to confirm each other's identity over a public, insecure network. Passwords provide the most convenient means of authentication because they are easy for humans to remember. Whilst there have been many proposals for password authentication, they are vulnerable to various attacks and are neither efficient, nor user friendly. In this paper we propose two new password authentication schemes making use of smart cards: the timestamp-based authentication scheme (TBAS) and the nonce-based authentication scheme (NBAS). Both TBAS and NBAS provide many desirable features: (1) they do not require the server to maintain a password table for verifying the legitimacy of login users; (2) they allow users to choose their passwords according to their liking and hence give more user convenience; (3) they are extremely efficient in terms of the computational cost since the protocol participants perform only a few hash function operations; and (4) they achieve mutual authentication between the remote user and the server. In addition, NBAS does not require synchronized clocks between the remote user and the server.

Keywords: Authentication scheme, mutual authentication, password, smart card.

1 Introduction

Authentication schemes are necessary for secure communication because one needs to know with whom he or she is communicating before sending some sensitive information. Achieving any form of authentication inevitably requires some secret information to be established between the communicating parties in advance of the authentication stage. Cryptographic keys, either secret keys for symmetric cryptography or private/public keys for asymmetric cryptography, may be one form of the underlying secret information pre-established between

* This work was supported by the Korean Ministry of Information and Communication under the Information Technology Research Center (ITRC) support program supervised by the Institute of Information Technology Assessment (IITA).

** Corresponding author.

the parties. However, these high-entropy cryptographic keys are random in appearance and thus are difficult to remember by humans, making them inconvenient and costly for use. Eventually, it is this drawback that password-based authentication came to be widely used in reality. Passwords are mostly used because they are easier to remember by humans than cryptographic keys with high entropy.

The possibility of password-based user authentication in remotely accessed computer systems was explored as early as the work of Lamport [12]. Due in large part to the practical significance of password-based authentication, this initial work has been followed by a great deal of studies and proposals, including solutions using multi-application smart cards [5, 15, 10, 14, 6, 17, 16]. In a typical password-based authentication scheme using smart cards, remote users are authenticated using their smart card as an identification token; the smart card takes as input a password from a user, recovers a unique identifier from the user-given password, creates a login message using the identifier, and then sends the login message to the server, who then checks the validity of the login message before allowing access to any services or resources. This way, the administrative overhead of the server is greatly reduced and the remote user is allowed to remember only his password to log on. Besides just creating and sending login messages, smart cards support mutual authentication where a challenge-response interaction between the card and the server takes place to verify each other's identity. Mutual authentication is a critical requirement in most real-world applications where one's private information should not be released to anyone until mutual confidence is established. Indeed, phishing attacks [1] are closely related to the deficiency of server authentication, and are a growing problem for many organizations and Internet users.

The experience has shown that the design of secure authentication schemes is not an easy task to do, especially in the presence of an active intruder; there is a long history of schemes for this domain being proposed and subsequently broken by some attacks (e.g., [7, 3, 4, 13, 9, 17, 16, 11]). Therefore, authentication schemes must be subjected to the strictest scrutiny possible before they can be deployed into an untrusted, open network. In 2000, Sun [14] proposed a remote user authentication scheme using smart cards. Compared with the earlier work of Hwang and Li [10], this scheme is extremely efficient in terms of the computational cost since the protocol participants perform only a few hash function operations. In 2002, Chien et al. [6] presented another remote user authentication scheme which improves on Sun's scheme in two ways; it provides mutual authentication and allows users to freely choose their passwords. However, Hsu [9] has pointed out that Chien et al.'s scheme is vulnerable to a parallel session attack; an intruder can masquerade as a legitimate user by using server's response for an honest session as a valid login message for a fake, parallel session. In this paper, we propose carefully designed two remote user authentication schemes making use of smart cards: the timestamp-based authentication scheme (TBAS) and the nonce-based authentication scheme (NBAS). Our schemes are immune to some

of the most notorious attacks, such as reflection attack, parallel session attack, and replay attack, and any other potential breach of security.

The remainder of this paper is organized as follows. In Section 2, we introduce the timestamp-based authentication scheme TBAS and analyze its security properties. Then, in Section 3, we present the nonce-based authentication scheme NBAS and give a security analysis of the protocol. Finally, we conclude this work in Section 4.

2 A Timestamp-Based Authentication Scheme (TBAS)

In this section we propose a new timestamp-based authentication scheme TBAS that achieves mutual authentication between the remote user and the server. Then we analyze the security of the proposed scheme.

2.1 Description of TBAS

The proposed scheme consists of three phases: the registration phase, the login phase, and the verification phase. The registration phase is done only once when a new user wants to join the system. The login and the authentication phase are performed whenever the user wants to login. A high-level depiction of the scheme is given in Fig. 1, where dashed lines indicate a secure channel, and a more detailed description follows:

Registration Phase. Let x be the secret key of the authentication server (AS), and h be a secure one-way hash function. A user U_i submits his identity ID_i and password PW_i to the server AS for registration via a secure channel. Then AS computes

$$X_i = h(ID_i \oplus x) \quad \text{and} \quad R_i = X_i \oplus PW_i,$$

and issues a smart card containing $\langle R_i, h^* \rangle$ to U_i , where h^* denotes the description of the hash function h .

Login Phase. When U_i wants to log in to the system, he inserts his smart card into a card reader and enters his identity ID_i and password PW_i . Given ID_i and PW_i , the smart card obtains the current timestamp T_1 and computes

$$X_i = R_i \oplus PW_i \quad \text{and} \quad C_1 = h(ID_i, X_i, T_1)$$

Then the smart card sends the login request message $\langle ID_i, T_1, C_1 \rangle$ to the server AS .

Verification Phase. With the login request message $\langle ID_i, T_1, C_1 \rangle$, the scheme enters the verification phase during which AS and U_i perform mutual authentication as follows:

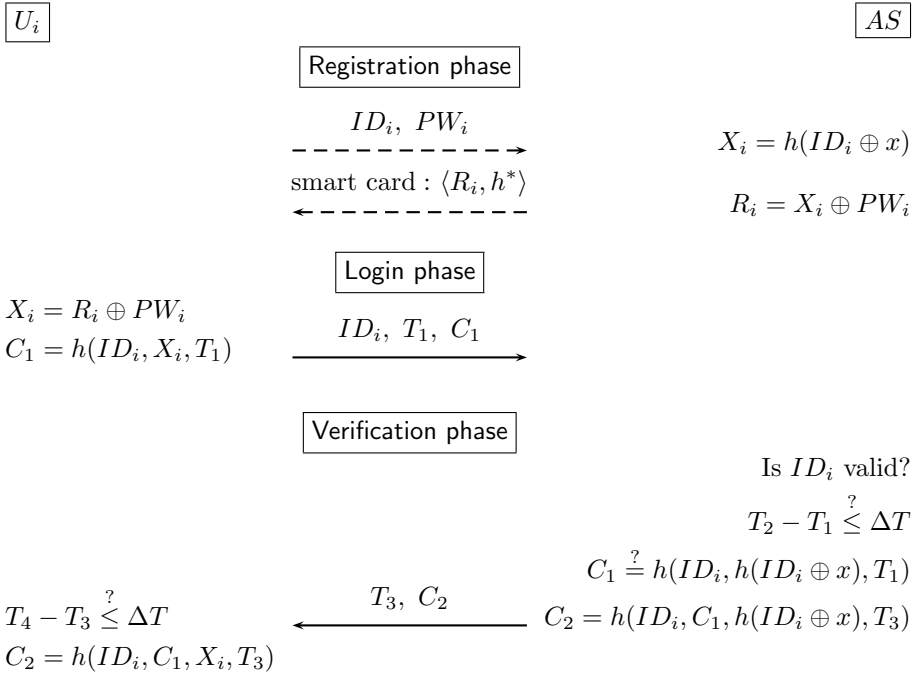


Fig. 1. Timestamp-based authentication scheme

- Step 1.** Upon receiving the message $\langle ID_i, T_1, C_1 \rangle$, the server AS obtains the current timestamp T_2 and verifies that: (1) ID_i is valid, (2) $T_2 - T_1 \leq \Delta T$, where ΔT is the maximum allowed time difference between T_1 and T_2 , and (3) C_1 is equal to $h(ID_i, h(ID_i \oplus x), T_1)$. If any of these is untrue, AS rejects the login request and aborts the protocol. Otherwise, AS accepts the login request.
- Step 2.** AS generates a new timestamp T_3 and computes C_2 as $C_2 = h(ID_i, C_1, h(ID_i \oplus x), T_3)$. AS then sends the response message $\langle T_3, C_2 \rangle$ to U_i .
- Step 3.** After receiving the response $\langle T_3, C_2 \rangle$, user U_i generates a new timestamp T_4 and verifies that: (1) $T_4 - T_3 \leq \Delta T$ and (2) C_2 equals $h(ID_i, C_1, X_i, T_3)$. If both of these conditions hold, U_i believes that the responding party is the genuine server. Otherwise, U_i aborts his login attempt.

TBAS provides many desirable features: (1) it does not require the server to maintain a password table for verifying the legitimacy of login users, (2) it allows users to choose their passwords according to their liking and hence gives more user convenience, and (3) it is extremely efficient in terms of the computational cost since the protocol participants perform only a few hash function operations.

2.2 Security Analysis

We now analyze the security of the proposed scheme TBAS, considering reflection attack, parallel session attack, and replay attack.

Reflection Attack. The basic idea of reflection attack is essentially simple: when an honest protocol participant sends a message to his authenticating party, the intruder eavesdrops or intercepts the message and sends it (or modified version of it) back to the message originator. In our scheme, two authenticators C_1 and C_2 are computed as follows:

$$C_1 = h(ID_i, h(ID_i \oplus x), T_1)$$

and

$$C_2 = h(ID_i, C_1, h(ID_i \oplus x), T_3).$$

This way, it would be impossible for the intruder to mount a reflection attack. The intruder, who wants to impersonate AS to U_i , cannot forge a valid server's response from the login request message $\langle ID_i, T_1, C_1 \rangle$ since C_2 cannot be obtained from C_1 . This is the case because computing C_2 requires the knowledge of the secret value $h(ID_i \oplus x)$ as well as of the public value C_1 . Hence, the scheme TBAS is secure against a reflection attack.

Parallel Session Attack. In this attack, an intruder can masquerade as a legitimate user by using server's response for an honest session as a valid login message for a fake, parallel session [9]. TBAS is also resistant to this kind of parallel session attacks. Even if the intruder eavesdrops on the server's response message $\langle T_3, C_2 \rangle$, she is unable to construct from it (or any modification of it) a valid login request message. This is straightforward since C_1 and C_2 are computed by using different expressions in a way that C_1 cannot be derived from C_2 . Therefore, parallel session attack cannot be applied to our scheme.

Replay Attack. In this attack, an intruder tries to replay messages partly or completely obtained in previous sessions. If an intruder can impersonate a legitimate user through this replay, then the scheme is said to be vulnerable to a replay attack. TBAS also provides protection against replay attacks. Firstly, the server's response for one session cannot be replayed for any other session because each C_2 is tightly bounded to both the server's current timestamp and the user's login request message. This guarantees the freshness of each message from AS . Secondly, the intruder is further prevented from replaying one of user's previous login request messages. This is achieved by letting the server check the validity of the timestamp T_1 used by U_i . However, we note that there seems to be one potential security weakness common to most of existing timestamp-based user authentication schemes. That is, given the time window ΔT , an intruder could impersonate a legitimate user by replaying one of the user's recent login request messages within the time window. The server can detect this kind of somewhat trivial attack, by additional checking that T_1 was not reused by U_i

during the time window of tolerance (i.e., during the time period between T_2 and $T_0 (= T_2 - \Delta T)$). Although most of previously published schemes for remote user authentication do not specify it, we believe that this kind of prevention is implicit in the schemes.

3 A Nonce-Based Authentication Scheme (NBAS)

Most password-based schemes for remote user authentication using smart cards require synchronized clocks between parties in the network. While timestamps are commonly used to detect replay attacks, it is often recommended in practice to avoid relying on their use for security in authentication schemes [2, 7, 8, 3]. To eliminate the need for timestamps, we propose a new remote user authentication scheme NBAS using random numbers called nonces (security issues related to timestamp, counter value, and nonce are well-documented in [3]).

3.1 Description of NBAS

Like TBAS, the nonce-based authentication scheme NBAS consists of three phases: the registration phase, the login phase, and the verification phase. A high-level depiction of the scheme is given in Fig. 2, where a dashed line indicates a secure channel, and a more detailed description follows:

Registration Phase. Let x be the secret key of the authentication server (AS), and h be a secure one-way hash function. A user U_i submits his identity ID_i and password PW_i to the server AS for registration via a secure channel. Then AS computes

$$X_i = h(ID_i \oplus x) \quad \text{and} \quad R_i = X_i \oplus PW_i,$$

and issues a smart card containing $\langle R_i, h^* \rangle$ to U_i , where h^* denotes the description of the hash function h .

Login Phase. When U_i wants to log on to the server, he inserts his smart card into a card reader and enters his identity ID_i and password PW_i . Given ID_i and PW_i , the smart card chooses a random number N_i and computes

$$X_i = R_i \oplus PW_i \quad \text{and} \quad C_i = X_i \oplus N_i.$$

The smart card then sends the login request message $\langle ID_i, C_i \rangle$ to the server AS .

Verification Phase. With the login request message $\langle ID_i, C_i \rangle$, the scheme enters the verification phase during which AS and U_i perform the following steps:

1. Upon receiving the message $\langle ID_i, C_i \rangle$, the server AS first checks the validity of ID_i . If not valid, AS rejects the login request. Otherwise, AS computes $X_i = h(ID_i \oplus x)$ and recovers N_i as $N_i = C_i \oplus X_i$. After that, AS chooses a random number N_s and computes

$$V_s = h(ID_i, C_i, N_i) \quad \text{and} \quad C_s = X_i \oplus N_s.$$

AS then sends the message $\langle V_s, C_s \rangle$ to U_i .

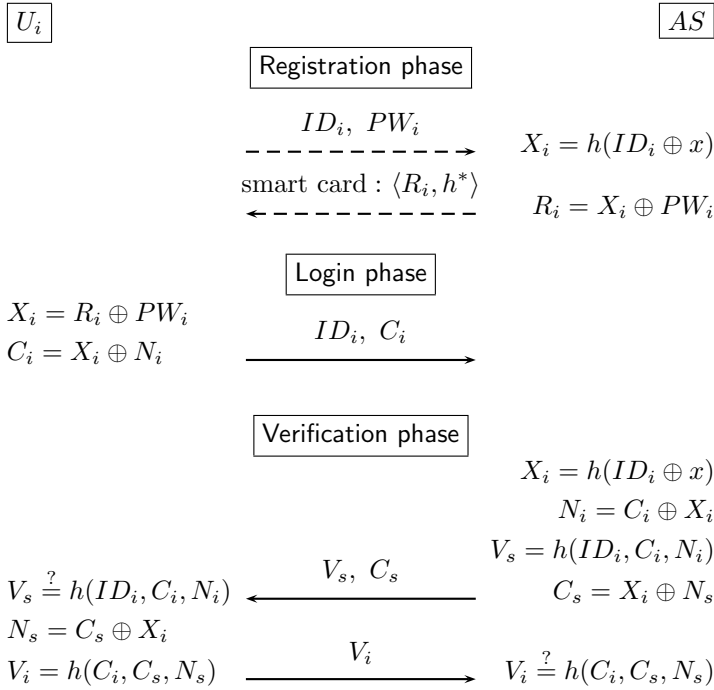


Fig. 2. Nonce-based remote user authentication scheme

2. Having received the message $\langle V_s, C_s \rangle$, the user U_i first verifies that V_s is equal to $h(ID_i, C_i, N_i)$. If the verification fails, then U_i aborts the protocol. Otherwise, U_i believes AS as authentic and recovers N_s as $N_s = C_s \oplus X_i$. After that, U_i computes the response V_i as

$$V_i = h(C_i, C_s, N_s)$$

and sends V_i to the server AS .

3. When AS receives V_i from U_i , it verifies the correctness of V_i by checking that V_i is equal to $h(C_i, C_s, N_s)$. If correct, AS accepts the login request; otherwise, rejects it.

The above-described nonce-based authentication scheme NBAS provides all the advantages of the timestamp-based authentication scheme TBAS. In addition, NBAS no longer requires synchronized clocks between the remote user and the server.

3.2 Security Analysis

We now analyze the security of the proposed scheme NBAS, considering reflection attack, parallel session attack, and replay attack.

Reflection Attack. The intruder cannot impersonate U_i to AS by sending the response V_s (or a modified version of it) of AS back to the server AS . This is because V_s and V_i are computed by using different expressions in a way that one cannot be derived from the other. In the scheme NBAS, the user's response V_i is computed as $V_i = h(C_i, C_s, N_s)$. Since h is a one-way hash function, V_i cannot be obtained without knowing the random nonce N_s . But, V_s is no use in computing N_s since the server's response V_s is computed as $V_s = h(ID_i, C_i, N_i)$; V_s simply does not have any information about N_s . This means that V_i cannot be derived from V_s in any way. Therefore, the scheme NBAS is secure against a reflection attack.

Parallel Session Attack. NBAS is secure against a parallel session attack. An intruder may try to launch an attack by choosing a random number C_E and sending $\langle ID_i, C_E \rangle$ as a login request message. From the server's point of view, C_E is perfectly indistinguishable from C_i of an honest execution since both are simply random numbers. But, upon receiving the message $\langle V_s, C_s \rangle$ from AS , the intruder can go any further with the session since she cannot answer the challenge C_s of AS . An intruder may try to solve this problem by starting a parallel session with AS , posing again as U_i and sending $\langle ID_i, C_s \rangle$ as a login request message. But, the intruder cannot use the server's response to its request C_s in the parallel session as its response to the request C_s from AS in the original session. This is because the server's response and the user's response are computed by using different expressions in a way that one cannot be derived from the other.

Replay Attack. NBAS provides protection against replay attacks. It is impossible for an intruder to impersonate AS to U_i by replaying messages obtained in previous sessions. Since U_i chooses the random nonce N_i anew for each challenge C_i , server's response for one session cannot be replayed for any other session. Following a similar reasoning as above, an intruder is unable to impersonate U_i to AS by replaying any of user's response sent for previous sessions. Hence, NBAS is also resistant to replay attacks.

4 Conclusion

We have proposed two remote user authentication schemes making use of smart cards: the timestamp-based authentication scheme (TBAS) and the nonce-based authentication scheme (NBAS). The primary merit of our schemes is in their simplicity and practicality for implementation on smart cards. The advantages of our schemes can be summarized as follows:

1. The server does not need to maintain a password table for verifying the legitimacy of login users.
2. Users are allowed to choose their passwords according to their liking.
3. The computational cost is extremely low requiring the participants to perform only a few hash function operations.

4. The schemes achieve mutual authentication; i.e., the remote user and the server can authenticate each other.
5. In the scheme NBAS, security does not depend on synchronized clocks shared between the remote user and the server.

We showed heuristically that the proposed schemes achieve the intended security goals against a variety of attacks.

References

1. Anti-Phishing Working Group, <http://www.antiphishing.org>.
2. S. M. Bellovin and M. Merritt, Limitations of the Kerberos authentication system, *ACM Computer Communication Review*, vol. 20, no. 5, pp. 119–132, 1990.
3. R. Bird, I. Gopal, A. Herzberg, P. A. Janson, S. Kutten, R. Molva, and M. Yung, Systematic design of a family of attack-resistant authentication protocols, *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 679–693, 1993.
4. U. Carlsen, Cryptographic protocol flaws: know your enemy, *Proceedings of the 7th IEEE Computer Security Foundations Workshop*, pp. 192–200, 1994.
5. C.-C. Chang and T.-C. Wu, Remote password authentication with smart cards, *IEE Proceedings E - Computers and Digital Techniques*, vol. 138, no. 3, pp. 165–168, 1991.
6. H.-Y. Chien, J.-K. Jan, and Y.-M. Tseng, An efficient and practical solution to remote authentication: smart card, *Computers & Security*, vol. 21, no. 4, pp. 372–375, 2002.
7. W. Diffie, P.C. van Oorschot, and M.J. Wiener, Authentication and authenticated key exchange, *Designs, Codes and Cryptography*, vol. 2, no. 2, pp. 107–125, 1992.
8. L. Gong, A security risk of depending on synchronized clocks, *ACM SIGOPS Operating Systems Review*, vol. 26, no. 1, pp. 49–53, 1992.
9. C.-L. Hsu, Security of Chien et al.'s remote user authentication scheme using smart cards, *Computer Standards and Interfaces*, vol. 26, no. 3, pp. 167–169, 2004.
10. M.-S. Hwang and L.-H. Li, A new remote user authentication scheme using smart cards, *IEEE Trans. on Consumer Electronics*, vol. 46, no. 1, pp. 28–30, 2000.
11. W.-C. Ku, S.-T. Chang, and M.-H. Chiang, Weaknesses of a remote user authentication scheme using smart cards for multi-server architecture, *IEICE Trans. on Communications*, vol. E88-B, no. 8, pp. 3451–3454, 2005.
12. L. Lamport, Password authentication with insecure communication, *Communications of the ACM*, vol. 24, no. 11, pp. 770–772, 1981.
13. G. Lowe, An attack on the Needham-Schroeder public-key authentication protocol, *Information Processing Letters*, vol. 56, no. 3, pp. 131–133, 1995.
14. H.-M. Sun, An efficient remote user authentication scheme using smart cards, *IEEE Trans. on Consumer Electronics*, vol. 46, no. 4, pp. 958–961, 2000.
15. W.-H. Yang and S.-P. Shieh, Password authentication schemes with smart card, *Computers & Security*, vol. 18, no. 8, pp. 727–733, 1999.
16. E.-J. Yoon, W.-H. Kim, and K.-Y. Yoo, Security enhancement for password authentication schemes with smart cards, *Proceedings of the 2nd International Conference on Trust, Privacy, and Security in Digital Business (TrustBus 2005)*, LNCS 3592, pp. 90–99, 2005.
17. E.-J. Yoon, E.-K. Ryu, and K.-Y. Yoo, An Improvement of Hwang-Lee-Tang's simple remote user authentication scheme, *Computers & Security*, vol. 24, no. 1, pp. 50–56, 2005.

Location-Aware Agent Using Data Mining for the Distributed Location-Based Services

Jaewan Lee, Romeo Mark A. Mateo, Bobby D. Gerardo, and Sung-Hyun Go

School of Electronic and Information Engineering, Kunsan National University,
68 Miryong-dong, Kunsan, Chonbuk 573-701, South Korea
{jwlee, rmmateo, bgerardo, blackpc}@kunsan.ac.kr

Abstract. Currently, one of the popular topics of research is location-awareness. Adding this function to location-based services provides necessary information to the user within the location to be aware of the user's position. But some LBS have insufficiencies of providing relevant information to the mobile subscriber. In this research, we proposed a location-aware agent that interacts with the LBS and provides location-aware service by adding a of data mining task. This agent extracts additional information by deploying a mobile agent in the database of LBS and mines the data. To make our approach efficient, we used a data mining method that extracts the relevant information according to the user agent profiles. This enables the proposed system to select information and summarizes the result of location-aware data for the user.

1 Introduction

Location-based services (LBS) are abundant in our society. The improvements of these service provide us a complex system but giving a better services to the user. Jensen [1] discussed some challenges of the location-based services to meet the computing needs of the services. It gives more details on improving the data representation, indexing, and precomputation. The technology or location system used with these services is discussed by Hightower [2] like using GPS, active badges, sensors and others. These issues also help the developer of location-awareness applications to choose a better location system which can be implemented in LBS. There are also many opportunities on LBS that we will be experiencing in the near future as we develop more sophisticated devices.

Location awareness is an evolution of mobile computing, location sensing and wireless technology [3]. A mobile device like PDA can become an information service about the location which is necessary to provide context knowledge of location and other information. For instance, we can configure our PDA for reminders by setting it whenever we are in a specific building or place that has LBS. Before leaving the library, we set the reminder to borrow some books. The reminder activates once the user agent sense that the previous building is out of range or we are already outside the building. Also, other location-aware services can be acquired by using this method.

In this paper, we proposed a location-aware agent integrated with data mining tools to mine the database of LBS. This approach generates location-aware information by mining additional information which was not provided by the LBS. User agent

deploys a mobile agent on the LBS to do the processing of information. The data mining process is provided by features like selecting the user profile for removing unrelated data to improve its performance and efficiency.

2 Basic Concepts

In the location-based services, we discuss various technologies and techniques to provide necessary information. The growth of the LBS becomes an interest of mobile users and opportunity for more information services that can be developed. Accompanied by these developments are increments of distributed hardware and software which become hindrance for providing interoperability to services. Researches show solutions to these problems by using middleware and other techniques. The following subsection will explain some technologies and concepts that were used in our design of the location-aware agent.

2.1 Location-Based Services

Location-based services provide information based on the location of the mobile user. Data storage is necessary in LBS to represent the locations in the world, as well as their attributes and relationships, and the resources available. This database is used for interpreting sensor readings, performing spatial queries and inferences, and triggering actions. In geographic information systems (GIS), the database is usually a geospatial database; in many indoor ubiquitous computing systems, the database may be as simple as a drawing file. In any case, LBS have requirements that challenge traditional data representation systems.

Since location-based services are distributed software and hardware, middleware implementations are proposed [6] [7]. A proposed multi-agent system that manages the location management to solve the problem of the distributed location-based services was presented [6]. The middleware used in the system is based on CORBA implementation. Also, the Middleware [7] uses CORBA that enables the fusion of different location sensing technologies and facilitates the incorporation of additional location technologies as they become available. The requirements of these middleware are certainly large and complex to integrate but would benefit the service providers and mobile users.

2.2 Location-Awareness

Location-awareness is a small part of context-awareness. Context-awareness is the ability of the mobile device to be aware of the users surrounding's physical environment and state. The applications and services using the concept of location-awareness can be developed so that the mobile device can inspect the environment, rather than the other way around. A context-aware mobile device may supply applications with information on location, altitude, orientation, temperature, velocity, biometrics, etc. Location-awareness is only a subset of these concept but powerful on bringing the necessary information.

Location-aware shows awareness of mobile user's current location to provide quick and necessary information. The system consists of location-aware capable mo-

mobile devices that interact with the resources like LBS. The Mobile Shadow [4] is an example of location-based system that uses the concept of location-awareness. It shows the architecture of the location system by presenting the services that can be accessed by the user through user agent. The infrastructure of the system provides supports for proactive location-aware services.

2.3 Data Mining

There are a lot of data mining algorithm that have already introduced to perform efficient data mining to facilitate the processing and interpretation of data. Using data mining enhances the learning of the patterns and knowledge on the distributed databases. Also, data mining is used in location management [10] where the mobility patterns are determined to predict the next location of the mobile user. In the HCARD model [8], proposed an Integrator agent to perform knowledge discovery in the heterogeneous server in the distributed environment. This agent was developed on CORBA for search and extraction of data from heterogeneous servers. Association rules were generated in the study and these can be practically explain for decision making purposes. The research also uses the method of minimizing the operation time by clustering prior to pattern discovery.

3 A Motivation Example for Location-Aware Data Mining

A location-aware service is an additional service of LBS which can inform a mobile user of the current location. The scenario explains a typical situation of a location-awareness. A student has a PDA and user agent software installed named “Jones”. Each establishment or building has LBS and communicates with the mobile device like the student’s PDA. To be reminded before leaving the library, “Jones” was set to alarm and popping a message that the student must borrow a book before leaving the library building. This is a typical example of a location-awareness where the user is informed of knowledge about the location. Moreover, there is still information that can be useful but the LBS or the user agent itself cannot provide this. Here, we say that the user agent sets a reminder to borrow a book but it was informed by the LBS that the book was already borrowed. Probably, the next action of the mobile user will be on his way to exit the library. But the user has interests on other books that he may borrow without knowing. In this case, we can add the data mining process to mine the other books that may interest the user. We give a description on some important user agent profile’s attribute that will be used on the data mining procedure.

Student level: This attribute describe the student level of a user. This input concerns on the level of education that a user currently has. This allows the user agent to have knowledge of the book mostly used for every level of the student.

Interest: The user may be interested in a computer, science and other topics. This attribute collects relative data from the user for providing the interest-level from the context of the location.

4 Framework of Location-Aware Agent

In this study, the researchers' proposed location-based service architecture used CORBA implementation. The protocol used in our architecture is based on the wireless CORBA implementation [9] to support the proposed location-aware agent. Our proposed architecture used PDA or mobile device to deploy the mobile agent of the user agent for providing the location-aware information. We used the compliance of the wireless CORBA specification to acquire the functions of the interoperability of the heterogeneous system by using the CORBA implementation on LBS. Figure 1 illustrates the LBS architecture for our proposed location-aware agent.

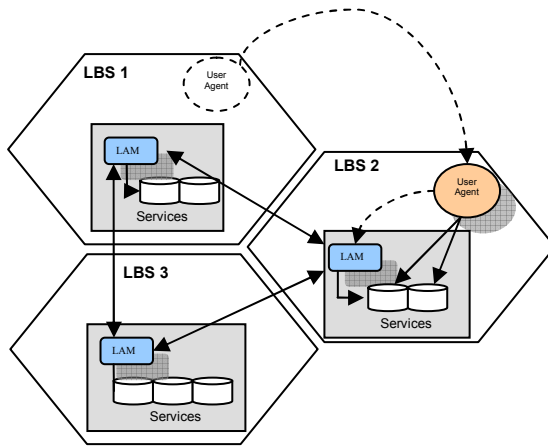


Fig. 1. Location-based service architecture for location awareness agent

In Figure 1, there are three different LBS which provides services to the mobile user. These services are also shared in each LBS which depends on the access privileges. The user agent moves from LBS 1 and after it is in the LBS 2, the location agent manager (LAM) communicates with the user agent and starts its service. The location agent manager is the agent which resides in the LBS, communicates with the user agent through wireless protocol and provides the services to the mobile user. Also, this agent communicates with the other LAM that is in the LBS. The LBS uses the ORB core which provides additional functionality to the heterogeneous system.

4.1 Mobile Agent Middleware for Distributed LBS

Mobile agent-based middleware is one of the issues of research for providing an advanced infrastructure that integrates supports protocols, mechanism, and tools to permit communication to mobile elements. SOMA [11] presented a mobile agent middleware to provide an architecture that integrates supports protocols, mechanism, and tools to permit coordination of mobile agents. In our research, we design the middleware of mobile agent which is integrated in wireless CORBA [9] and having a Java-based platform. The infrastructure of the proposed middleware has a service

layers for designing, implementing, and deploying mobile agent based applications. As shown in Figure 2, our proposed middleware consists of four layers. The mobile agent core services layer consists of communication, migration, naming, security, interoperation, persistence and data mining support. We focus more on the last component which is the data mining support. This additional service is provided to operate the data mining of the mobile agent on the database of LBS.

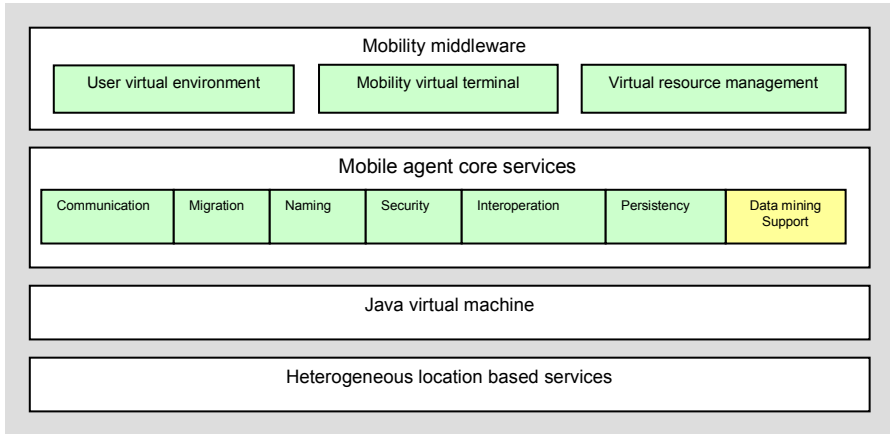


Fig. 2. Proposed mobile agent middleware

Also, these proposed middleware is a compliance to wireless CORBA [9] to support the features of the CORBA environment. The key components in wireless CORBA are Mobile Interoperable Object Reference (Mobile IOR) which is a relocatable object reference, a home location agent which keeps track of the current location of the mobile terminal, an Access Bridge and Terminal Bridge which are the network side end point of the General Inter-ORB Protocol (GIOP) tunnel. The architecture of the wireless CORBA is explained further in [9]. This integration of the middleware provides transparency and simplicity of the services for mobile agent.

4.2 User Agent

The proposed system consists of a single agent which resides on a PDA. The PDA is Java 2 Platform Micro Edition (J2ME) compliance to support the proposed user agent. This agent has the profile of the mobile user and associated with additional role. The user agent represents the virtual personality of the mobile user. Figure 3 is the structure of our proposed location-aware agent. The user agent consists of the user profiles which are student level, interest and address. This agent is integrated in the data mining function and use the user profile for the preprocessing. Additional user profile can be added on the proposed agent.

Figure 3 shows the user agent of a common student. The agent of the LBS communicates with the user agent to provide service to the mobile user. Data mining function will be only triggered if the agent in the LBS accepts the request of the user agent.

User Agent Jones		
Data Mining		
Profile		
Address: Chicago, USA	Interest: Computers	College Stu-

Fig. 3. User profile of mobile agent Jones

This agent also represents the virtual personality of the mobile user. The configuration of other mobile user can be different that may have limited access on the database of LBS. An example of this is a student which will be limited on accessing the database that is prohibited to their given privilege and only administrator features could access the service.

4.3 Mobile Agent Data Mining Procedure

The user agent triggers a location-awareness by deploying a mobile agent at the LBS database and provides the additional information for the location. The security heterogeneous databases of the LBS. Our algorithm has two data mining phases. In Figure 4, the two-phase processes are illustrated. In the first phase, the mobile agent was deployed on the LBS database. The mobile agent does the preprocessing by selecting the attributes that satisfy the user profile’s interest of the mobile user and trimming the data with missing values. This prepares the data to the next phase and to process relevant information before mining. The second phase was processing data on

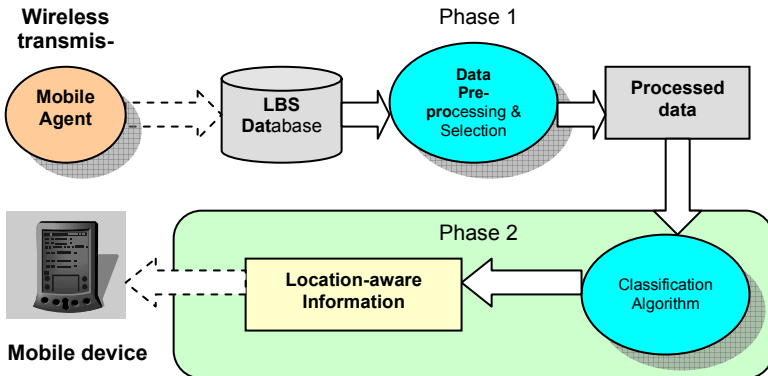


Fig. 4. Proposed two-phase data mining through mobile agent

classification algorithm and creates a decision tree on the information gathered. After the process, the results are returned again to the user agent to inform the mobile user of other interesting information.

5 Location-Aware Data Mining Model

We proposed a framework of the location-aware agent that uses data mining function to provide information awareness of the location. The proposed system used the wireless network via Bluetooth technology for transmission of mobile agent and data. The proposed data mining considers the user profile as the basis of interest to mine the relevant information. Now let us consider the set of user profiles that will be used in the data mining: $P = \{p_1, p_2 \dots p_x\}$. After collecting the user profiles, the mobile agent uses these features to select the relevant attributes of C where it is the raw data from the LBS database. Let D be the set of the selected tuples from C . Equation 1 represent the pre-processing algorithm. The following are the phases of our proposed algorithm.

$$D = \sum_{i=1}^n C\{c_1, c_2, \dots, c_n\} \quad (1)$$

where c_n attribute (value) = p_x (value)

Phase 1. Preprocessing

- a. *User profile selection* – selecting the tuple(s) that satisfy P will be included in D .

Phase 2. Data Mining

- a. *Classification algorithm* – this implements the classification of the data sets of the preprocessed data.
- b. *Decision Tree* – this creates a tree like structure rules based on the classified data sets. This is the last step of our algorithm.

```

INPUT: profile, preprocessdata
OUTPUT: Classification(preprocessdata)

public class Useragent implements MessageListener {
    public void MAdeploy(String[] attributes, String[] values) {
    }
    public void infoReceived(int dest_addr, Message[] msg) {
    }
}

public class MobileAgent implements MessageListener {
    public void Preprocess(String[] profile, String[] val) {
        while(rsData.next())
        {
            if rsData.getObject(profile)=val; AddInfo(rowset)
        }
        Classification(preprocessdata);
    }
    public void infoSend(int dest_addr, Message[] msg) {
    }
}

```

Fig. 5. Location-aware agent and mobile agent data mining algorithm

After the results are acquired, the output of the data mining is sent to the user agent to present the visualize result to mobile user. The sending of message is done in wireless transmission by using Bluetooth. The codes for the location-aware agent and location agent are presented in Figure 5.

6 Experimental Evaluation

The proposed location-aware agent was simulated using the Java and implemented through wireless CORBA. The environment OS platform used here are Windows OS, Red Hat Linux and Sun Solaris 8 to simulate the heterogeneity of the location-based services. The data mining tools were available using the Weka 3 software. After simulating the algorithm on Weka, the classes for classification are inserted in our proposed location-aware agent.

6.1 Results of Data Mining

The experiment for data mining used the scenario given in Section 3. The student searches for books on the database of the library and check its availability. We deployed the mobile agent on the database of a library. The database for our simulation contains 10,000 tuples of transacted data. Each book is presented by the book identification and ordered in classifications like mathematics, computers, social sciences, etc. for example computer books are numbered from 600 to 699. The next attribute is the time it was borrowed. Two cases were used in the experiment. First case, we execute the normal classification and decision tree. This generates 4980 instances and the first 10 are showed in Figure 6. Case 2 is executing our proposed algorithm which has the

Case 1: Classification Tree	Case 2: Classification Tree
BookID = 600: 15 (5.0/3.0)	BookID = 600: 12 (2.0/1.0)
BookID = 601: 13 (5.0/3.0)	BookID = 601: 10 (0.0)
BookID = 602: 16 (7.0/3.0)	BookID = 602: 16 (5.0/1.0)
BookID = 603: 14 (2.0/1.0)	BookID = 603: 16 (1.0)
BookID = 604: 14 (1.0)	BookID = 604: 10 (0.0)
BookID = 605: 10 (0.0)	BookID = 605: 10 (0.0)
BookID = 606	BookID = 606: 8 (7.0/4.0)
totaldays <= 5: 8 (6.0/2.0)	BookID = 607: 10 (0.0)
totaldays > 5: 9 (6.0/2.0)	BookID = 608: 10 (0.0)
BookID = 607: 10 (1.0)	BookID = 609: 12 (2.0/1.0)
BookID = 608: 16 (3.0/1.0)	BookID = 610: 18 (1.0)
BookID = 609: 12 (4.0/2.0)	
BookID = 610: 8 (3.0/2.0)	
Total instances: 4980	Total instances: 190
Correctly classified inst.: 42.47%	Correctly classified inst.: 50.57%

Fig. 6. The results of classification and decision tree algorithm

feature of user profiles to select the relevant data. It generated only 190 instances which summarizes relevant books for the user. This only implies that using our proposed algorithm collects the relevant information and minimizes the processing time.

Figure 6 shows the result of the classification tree algorithm. In the second case, we add the selection of user's interest and provide relevant information. The results show the time it is borrowed and the total number of days it is returned from the day it is borrowed. One interesting part here is that a user can determine the books that are available after data mining from the LBS database. Also, the correctly classified instances from a ten-fold cross-validation of the second case have a higher value than the first case. This is done in Weka if there is no test file specified. This indicates that the results obtained from training data are very optimistic compared with what might be obtained from an independent test set from the same source.

7 Conclusion and Recommendations

In this paper, we proposed a location-aware agent that performs data mining on the heterogeneous LBS to provide additional information awareness. We present the architecture of the location-based services for the proposed agent. The middleware for the proposed agent supports the mobility services on the heterogeneous location-based services. Also, we proposed an algorithm for the data mining by using the user profile to make the information relevant and minimized the processing time.

Our research shows that using the data mining function enhances the location-awareness of the mobile users. There are still more data mining algorithm that can be used to provide the location-aware service. We only presented our experiment on a library database and our future works will test it on other LBS or database that has a location-aware capability.

References

1. Jensen, C.: Research Challenges in Location-Enabled M-Services. Proceedings of the Third International Conference on Mobile Data Management. (2002). pp. 3-7
2. Hightower, J. and Borriello, G.: Location Systems for Ubiquitous Computing. Computer. Vol. 34, Issue 8 (August 2001) pp. 57-66
3. Patterson, C., Muntz, R. and Pancake, C.: Challenges in Location-Aware Computing. IEEE Pervasive Computing. Vol.2, No. 2 (April-June 2003) pp. 80-89
4. Fischmeister, S.: Mobile Software Agents for Location-based Systems. Available at www.old.netobjectdays.org/pdf/02/papers/ws-ages/0934.pdf
5. Want, R., Hopper, A., Falcao, V. and Gibbons, J.: The Active Badge Location System. ACM Transactions on Information Systems, Vol. 10, Issue 1 (January 1992), pp. 91 - 102
6. Mateo, R. M., Lee, J. W. and Kwon, O.: Hierarchical Structured Multi-agent for Distributed Databases in Location Based Services. The Journal of Information Systems, Vol. 14, Special Issue (December 2005) pp. 17-22
7. Ranganathan, A., Al-Muhtadi, J., Chutan, S., Campbell, R. and Mickunas, D.: Middle-Where: A Middleware for Location Awareness in Ubiquitous Computing Applications.

8. Gerardo, B. D., Lee, J. W. and Joo, S.: The HCARD Model using an Agent for Knowledge Discovery. *The Journal of Information Systems*, Vol. 14, Special Issue (December 2005) pp. 53-58.
9. Black, K., Currey, J., Kangasharju, J., Lansio, J. and Raatikainen, K.: *Wireless Access and Terminal Mobility in CORBA*. Available at http://www.omg.org/technology/documents/formal/telecom_wireless.htm.
10. Yavas, G., Katsaros, D., Ulusoy, O., and Manolopoulos, Y.: A Data Mining Approach for Location Prediction in Mobile Environments. *Data & Knowledge Engineering* 54, (2005) pp 121-146.
11. Bellavista, P., Corradi, A., and Stenfalli, S.: *Mobile Agent Middleware for Mobile Computing*. *Computer Journal*. (March 2001) pp. 73-81

An Empirical Development Case of a Software-Intensive System Based on the Rational Unified Process

Kilsup Lee

Dept. of Computer & Information,
Korea National Defense University,
205, Soosaek-dong, Eunpyung-gu,
Seoul, 122-875, Republic of Korea
gislee@kndu.ac.kr

Abstract. The Rational Unified Process (RUP) is a development process which is based on object-oriented, usecase-centric, architecture-centric, and iterative approaches. Most projects for public organizations have adopted waterfall model in software development lifecycle, however, various projects have recently tried to apply an iterative model to minimize risks and to enhance quality of software. But empirical results of software-intensive development based on the RUP are not well known. Therefore, this paper presents process, period, effort and quality factors for a software-intensive system development through the study on the Korean Core Instrumentation System (K-CIS) which has adopted the RUP. We also present the result of comparison between the K-CIS RUP and waterfall model, and lessons learned from the K-CIS case. We believe that our result is useful for establishment of a process and estimation of resource and quality factors for software-intensive systems efficiently.

1 Introduction

As changing into information society, demands on high quality software are increasing rapidly. The methodologies of software development have also advanced by rapid strides. Recently, the object-oriented and component-based methodologies [1], [2], [3], [4] compose a main stream in developing software for large-scale information systems. Also the software development process has made great progress up to the present along methodologies. The waterfall model [5], which develops software in grand, has been used widely in software development, but nowadays it is a trend to use iterative models such as spiral model [5] and Unified Software Development Process (USDP) [6] model in order to reduce risks and to enhance quality of software.

The USDP is a software development process which incorporates object-oriented, usecase-centric, architecture-centric, and iterative approaches. Here, the Rational Unified Process (RUP) [7] is a commercial brand which is more elaborated than the USDP. The lifecycle of the RUP has four phases such as inception, elaboration, construction, and transition, which are composed of iterations. The phases are crossed with process workflows (*i.e.*, business modeling, requirements, analysis and design,

implementation, test, and deployment) and supporting workflows (*i.e.*, configuration management, management, and environment).

The RUP has been applied in various software development projects. Particularly, software-intensive systems include hardware, communication networks, database and their facilities. Often the complexity of a software-intensive system makes it difficult to tailor the RUP and to estimate the proper effort and quality factors. Therefore, this paper presents a tailored process for developing software-intensive systems. Moreover, we have studied on the Korean Core Instrumentation System (K-CIS) for combat training in military area which is a software-intensive system and is developed through the RUP.

The rest of this paper is organized as follows. In section 2, system configuration of generic CIS is explained in brief. In section 3, the system development process of the K-CIS is tailored using the RUP, the C4ISR Architectural Framework (AF)¹ [8], and the Korean Acquisition Process for Defense Automated Information Systems [9]. In section 4, factors on period, effort, and quality for the K-CIS RUP are evaluated through comparison with waterfall model and typical RUP. Finally, we describe concluding remarks in section 5.

2 System Configuration of CIS

Recently, the rapid progress in information technology enables to construct a Combat Training Center (CTC) that provides an environment similar to a real battle field. In

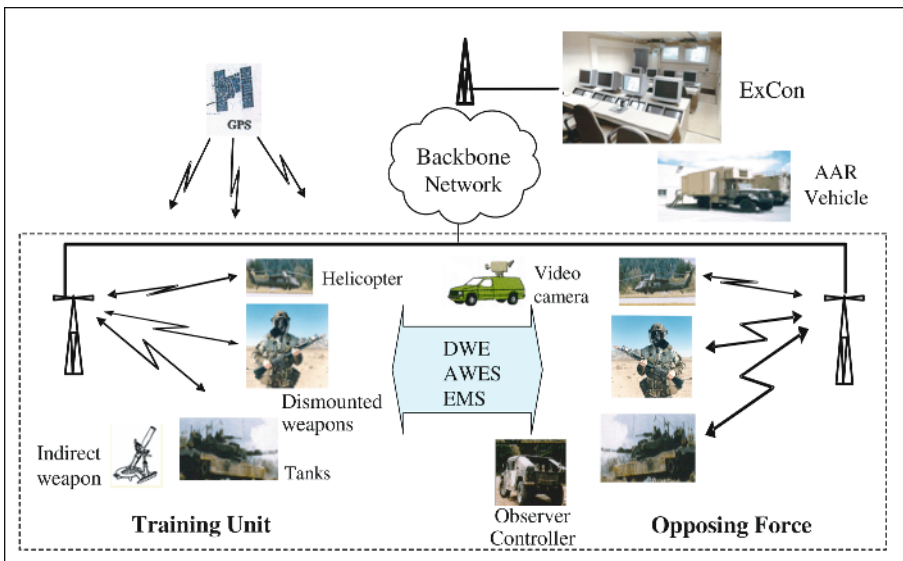


Fig. 1. Configuration diagram of a generic core instrumentation system

¹ Currently, the C4ISR AF has evolved into the Department of Defense Architectural Framework (DoD AF) 1.0.

the CTC, it is possible to exercise in realistic situation and to learn lessons through after action review using the collection and analysis of exercise data. The National Training Center (NTC), the Joint Readiness Training Center (JRTC), and the Getechts Übungs Zentru (GÜZ) are famous sites of CTC, which are running by USA and Germany, respectively. Many other countries including Korea are constructing CTC or considering construction of CTC. [11]

In general, a Core Instrumentation System (CIS) is composed of engagement simulation subsystem, communication networks, exercise control center (ExCon) subsystem, observer controller (OC) subsystem, and after action review (AAR) subsystem. Engagement simulation subsystem simulates weapons of training unit and opposing force through Direct Weapon Engagement (DWE), Area Weapon Effectiveness Simulation (AWES), and Effect Management System (EMS) on fire and damage. DWE and AWES simulate helicopters, dismounted weapons, tanks, and indirect weapon using equipment composed of Global Positioning System (GPS), laser, micro-processors, and radio devices.

Communication networks include a backbone network which consists of an optical network and a microwave network, local area network, and so on. The exercise control center subsystem is composed of workstations, servers, local area networks, exercise management software, and system management software. And the exercise control subsystem is composed of Personal Digital Assistants (PDA's), notebooks, and radio devices. Finally, after the action review subsystem is composed of projection equipments, workstations, and AAR software. Fig.1 shows a configuration diagram of a generic core instrumentation system. Also the system configuration of K-CIS is similar to the configuration shown in Fig. 1.

3 The System Development Process of the K-CIS

Before establishing system development process based on the RUP, we discuss the characteristics of the K-CIS, establishment of process, and efficiency of process. First, the K-CIS is a software-intensive system that is composed of software, hardware, communication networks, facilities, road, and so on. Particularly, software is the core component for integration and interoperation among various components of the K-CIS. The K-CIS software includes exercise control software as user application, system supporting software as commercial off the shelf (COTS), and engagement simulation / communications software as embedded software. Moreover, it has near real time characteristic which engagement data should be reported to the exercise control center subsystem with regular period for simulation of area weapons.

In order to incorporate the RUP into the system development process of the K-CIS, we need to merge workflows of system process such as conceptual development, system requirement analysis, and system design with business modeling workflow of the RUP. Then, we also require combining processes for embedded software and customizing software with the RUP. Moreover, we need to define number of phases, number of iterations, activities, tasks, and artifacts within the RUP. Finally, we need

to evaluate the efficiency of the tailored RUP through comparison with the waterfall model and the typical RUP.

Fig. 2 shows the system development process of the K-CIS which merges the RUP, software development process of MIL-STD-498 [12], and development processes for embedded software and hardware together. The conceptual development has been done using the C4ISR AF that provides Operational Architecture (OA), System Architecture (SA) and Technical Architecture (TA). This method is more detail and specific rather than business modeling workflow of the RUP.

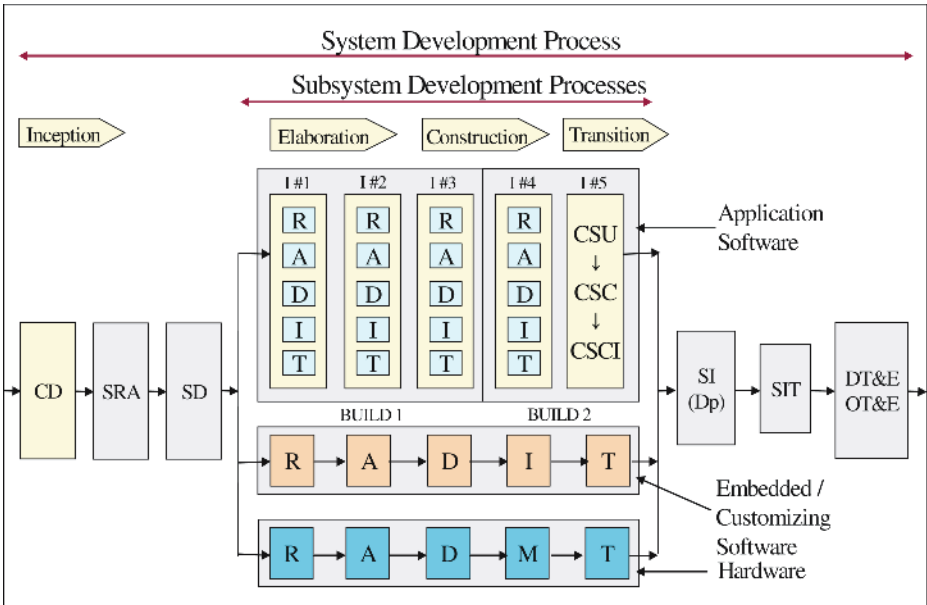


Fig. 2. System development process of the K-CIS. CD (Conceptual Development), SRA (System Requirement Analysis), SD (System Design), I# (Iteration #), R (Requirement), A (Analysis), D (Development), I (Implementation), M (Manufacturing), T (Test), CSU (Computer Software Unit), CSC (Computer Software Component), CSCI (Computer Software Configuration item), SI (System Integration), Dp (Deployment), SIT (System Integration Test), DT&E (Development Test & Evaluation), OT&E (Operational Test & Evaluation).

Moreover, the tailored RUP has two builds and five iterations. Then iteration consists of requirement, analysis, design, implementation, and test workflows. Particularly, iteration 5 is set up for integration of whole software components of the K-CIS. The development processes for embedded software and hardware adopt traditional waterfall model. Deployment workflow is merged into system integration workflow of system process. The workflows, activities, tasks, and artifacts are also presented in Table 1.

Table 1. The K-CIS development process

Workflows	Activities	Tasks	Artifacts
Requirement	Definition of common terminologies		Glossary
	Definition of requirements	Data collection	Software Requirement Specification
		Elaboration of requirements	
	Description of system operation scenarios		System operation scenario
	Definition of usecase model		Usecase specification
Description of architecture usecase view		Architecture usecase view	
Analysis & Design	Analysis of usecase	Drawing sequence diagram	Sequence diagram
		Drawing collaboration diagram	Collaboration diagram
		Drawing class diagram	Class diagram
		Drawing package diagram	Package diagram
	Design of user interface	Drawing user interface diagram	User interface diagram
		Design of user interface layout	User interface layout
		Design of user interface report	User interface report
	Identification of interoperable elements		Interface Req. Specification
Description of architecture logical view		Architecture logical view	
Analysis & Design	Design of usecase	Refinement of sequence diagram	Sequence diagram
		Refinement of collaboration diagram	Collaboration diagram
		Refinement of class diagram	Class diagram
		Refinement of package diagram	Package diagram
	Design of class		Class specification
	Design of subsystem		Subsystem specification
	Design of data model		Table specification
	Definition of deployment model		Deployment diagram
	Description of architecture process view		Architecture process view
	Description of architecture deployment view		Architecture deployment view
Implementation	Description of architecture implementation view		Architecture implementation view
	Structuring component model		Component specification
	Implementation of components		Source code and documentation
Test	Unit test		Unit test plan / report
	Unit system test		Unit system test plan / report
	Integration test		Integration test plan / report

4 Evaluation of the K-CIS Development Process

In this section, we evaluate the K-CIS development process with respect to process and supporting workflows, which come from the RUP [7], through comparison with the waterfall model and the typical RUP. Particularly, we have used the published data in references [2], [5], [7] and the collected data during the K-CIS development.

4.1 Processes Workflows

Process workflows are business modeling, requirements, analysis and design, implementation, and test. Here, we discuss the characteristics of the K-CIS development process with respect to these workflows and integration aspect. Current acquisition process of defense automated information systems [8] has applied the waterfall model implicitly, however, there is no restriction to apply an iterative model in developing software-intensive system. Up to the present, most projects for software-intensive system have adopted the waterfall model.

First of all, we need some tailoring of the RUP to merge with system development process. The waterfall model is considering grand design, but the RUP is based on iterative development. Thus, the RUP is more proper for large-scale software development with incremental and evolutionary approach rather than the waterfall model. This characteristic of the RUP enables ease communications among stakeholders rather than the waterfall model. The result of the tailored RUP is shown in Fig. 2 and its detailed workflows, activities, tasks, and artifacts are shown in Table 1.

In business modeling aspect, the traditional waterfall model begins from requirement stage. But the RUP provides business modeling with 6 scenarios such as organizational chart, domain modeling, and one business with many systems, generic business model, new business, and business process reengineering. However, the K-CIS system development process has adopted the C4ISR AF as its business modeling during conceptual development stage. The concept development stage is a business modeling in the C4ISR AF which has 2 AV (All View) artifacts, 9 OV (Operational View) artifacts, 13 SV (System View) artifacts, 2 TV (Technical View) artifacts. The detailed procedure and artifacts of the C4ISR AF are shown in the reference [9]. Thus, the K-CIS concept development in the C4ISR AF is stronger than the RUP business modeling.

In requirement aspect, the waterfall model is not easy to modify requirements after confirming the requirements. Even though some advanced waterfall model allows modification with feedback to previous states, it is not possible to modify large-scope of requirements. On the other hand, the waterfall model is proper if requirements of a system are definite and can be developed at once. The RUP is easy to complement at next iteration though experience and trial-errors of previous iteration. Therefore, the RUP has advantages when requirements of a system are not clear. But, the RUP has some overheads for managing changes of requirements and their documentation. Meanwhile, these characteristics of RUP can be applied to the remained workflows such as analysis and design, implementation, and test.

In integration aspect, the workflows of waterfall model are performed in sequence with grand design. Each item is tested and its defects are removed along proceeding development. At this time, integration is not easy when there are some defects in an item. The test scope is magnified because it is not verified what defects cause effect to associated items. In the worst case, most associated items should be modified. On the other hand, the iterative model allows incremental development which adds new items to the pre-verified item. Therefore, we can reduce the number of items to be modified. And some critical part of a system can be developed as a prototype at the early stage. Also this prototype can be evolved to whole system.

4.2 Supporting Workflows

In this section, we focus on configuration management, and project management. Particularly, we elaborate project management into risk management and quality management.

First, goal of configuration management is to identify, to evaluate, to decide, and to trace changes of requirements. In general, it is difficult to manage when there are many changes. An iterative development is easier to find defects and to change requirements rather than waterfall model, but is difficult to manage configuration and changes. Any change of a requirement influences activities of analysis, design, implementation, and test; and it requires additional effort to maintain artifacts.

Fig. 3 (a) depicts the number of changes with respect to iterations in the K-CIS case. The data of changes are based on the reports from the meetings of change control board. In iteration #1, there is no change due to developing a pilot within 3 months. But iterations #2 and #3, which are *elaboration* and *construction* phases, shows 60 and 109 changes after holding Software Requirement Review (SRR) and Critical Design Review (CDR) meetings, respectively. We have also found 26 and 29 changes during iterations #4 and #5, which are *construction* and *transition* phases, respectively.

Moreover, Fig. 3 (b) depicts the number of defects found with respect to iterations. It shows small numbers below 200 at iterations #1, #2, and #3, but it increases rapidly up to 1026 at iteration #4. The reason is that many defects are found during the integration of configuration items. However, the number of defects at iteration #5 shows the small numbers below 200. We can observe some points from these two figures. For instance, we can see that the changes at the iteration #3 cause the K-CIS system to produce many defects at the iteration #4.

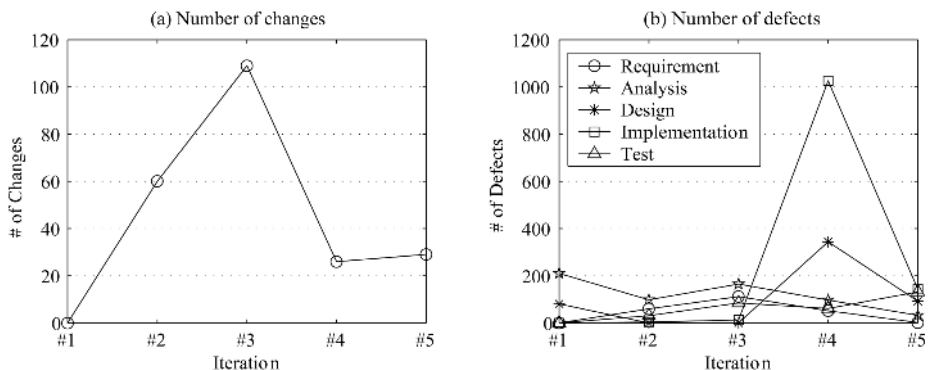


Fig. 3. Changes and defects with respect to iterations

Second, risks in software development are managed by control activities. In waterfall model, it is possible to identify impact of risk exactly after finishing test. Thus, we need more efforts to mitigate risks found at last phases than iterative model. In the K-CIS case, we have identified risks with respect to project area at initial stage and have provided a risk management plan. At iteration 1, we have developed a pilot

project to train beginners and people who are familiar with waterfall model. Then, we have assigned core parts with high risks to iteration 2 so as to reserve lead time in case of failures in development. Next, we have prepared a step-wise integration plan. Finally, we have identified new risks, impacts and possibilities of risks continuously aligned with quality management activities.

Third, with respect to quality management we take a look at aspects of period (Month), effort (Man Month), lifecycle model, and defects. First of all, Table 2 presents the ratio of period and effort assigned with respect to lifecycle models. The K-CIS RUP model shows a mixed form of waterfall and typical RUP at inception and elaboration phases. However, about 50% of period and efforts at the construction phase moves to the transition phase. This particular phenomenon can be explained by activities of the system process which are requested by the acquisition procedure of the K-CIS. As a result, we need to assign more period and efforts to transition phase, when severe acquisition procedure is expected.

Table 2. The ratio of period and efforts assigned with respect to lifecycle models

Phase	Waterfall Model [5]		Typical RUP [7]		K-CIS RUP	
	Period (M)	Efforts (MM)	Period (M)	Efforts (MM)	Period (M)	Efforts (MM)
Inception	13	5	10	5	13	4
Elaboration	20	20	30	20	25	24
Construction	55	60	50	65	25	33
Transition	12	15	10	10	37	35

Table 3 presents the ratio of period and effort assigned with respect to software size, KSLOC (Kilo- Source Lines of Code). The K-CIS RUP has taken 47 months for whole system development and 30 months for software components only. Here, the period of the K-CIS, 30 months, is similar to the period of the typical RUP, 28 months, and the increment of 17 months comes from the system development process. The efforts 1,752 MM (Man Month) of the K-CIS case are similar to ones of the typical RUP. But the efforts of the K-CIS are similar to those of the waterfall model if we subtract the efforts, 380 MM from the acquisition procedure of the K-CIS. This fact notes that we need some time to migrate from a waterfall model to an iterative model.

Table 3. The ratio of period and efforts assigned with respect to software size

Kilo-SLOC	Waterfall Model [5]		Typical RUP [7]		K-CIS RUP	
	Period (M)	Efforts (MM)	Period (M)	Efforts (MM)	Period (M)	Efforts (MM)
450	40	1,466	28	1,890	47	1,752

Meanwhile, the typical RUP requires more effort rather than the waterfall model. Its cost for incremented efforts is rewarded by high quality of software. Table 4 presents the number of defects found with respect to lifecycle models. In general, defects are found by activities of artifact review, joint review, validation, verification,

test, audit, and process assessment. In Table 4, The K-CIS RUP shows a low number of defects at requirement workflow. It is due to application of the C4ISR AF instead of the business modeling of RUP. Even the total number of defects is the smallest among alternatives, the defects are found at last workflows such as implementation and test. This fact notes that the participants of the K-CIS project are not familiar with the K-CIS RUP.

Table 4. The number of defects found with respect to lifecycle models

Workflow	Waterfall Model [5]	Typical RUP [7]		K-CIS RUP
		Iter. (2-4)	Iter. (5-10)	
Requirement	4.2	3.2	2.4	0.5
Analysis	3.1	2.5	3.7	1.3
Design	1.1	1.1	2.2	1.2
Implementation	1.0	2.1	3.5	5.9
Test	9.4	8.9	11.8	8.9

5 Concluding Remarks

In this paper we have studied on an interactive development using the RUP to a software-intensive system. We have chosen the K-CIS RUP case and have compared with the waterfall model and the typical RUP model. As the main results, the K-CIS RUP includes some changed processes with respect to tailoring with system processes; the concreteness of workflows, activities, tasks, and artifacts; and the business modeling from those of the typical RUP. Moreover, the K-CIS process also shows some strength in adaptability to large-scale systems, communications among stakeholders, and the flexibility of requirement changes rather than those of the waterfall model. However, the K-CIS process shows some weakness in configuration management and documentation rather than those of the waterfall model.

Meanwhile, we have taken seven lessons learned from the K-CIS case. First, the RUP can be merged with legacy system development process well with some modifications. Fig. 2 shows an example of merging the RUP, the C4ISR AF, and system development process together. Second, it needs some tailoring activities, tasks, artifacts to meet specific business characteristics. Third, the C4ISR AF may reduce the number of defects than business modeling of RUP. We can see the number of defects from requirement workflow in Table 4. Fourth, an iterative model is superior to a waterfall model in risk mitigation and reuse of experiences from previous iterations, and shows large number of changes at elaboration and construction phases as shown in Fig.3.

Fifth, we need a strategy to relate step-wise interface test with quality management activities in order to mitigate risks and to improve quality of final product. Sixth, we require adjustment of period and efforts for construction and transition phases of the RUP when the RUP is merged with a system development process under an acquisition manager's control. The K-CIS RUP case in Table 2 shows that about 50% of assigned period and efforts at the construction phase has moved to the transition phase. Seventh, when we migrate from a waterfall model to an iterative model at the

first time, we may simply repeat the waterfall model, because we are lacking at know-how on the integration and the distribution of efforts. As a result, the efforts for defect correction are increased as shown in Table 3.

Finally, we believe that the result of our work is useful for establishing system development process with the RUP, when public organizations are intended to acquire software-intensive systems.

References

1. Dennis, A., Wixom, B.H., Tegarden, D.: Systems Analysis and Design with UML 2.0 - An Object-Oriented Approach. 2nd ed., Wiley, (2005)
2. Braude E.: Software Engineering - An Object- Oriented Perspective. Wiley, (2001)
3. Sterling Software, Inc.: Sterling Software Component-Based Development Method. (available with COOL:Spex and COOL:Gen products), <http://www.sterling.com>, (2005)
4. Cheesman, J., Daniels, J.: UML Components - A Simple Process for Specifying Component-Based Software. Addison-Wesley, New York, (2001)
5. AEW Services: The Role of the Project Life Cycle (Life Span) in Project Management. AEW Services, Vancouver, BC, (2003)
6. Jacobson, I., Booch, G., Rumbaugh, J.: The Unified Software Development Process. Addison-Wesley, (1999)
7. Philippe K.: The Rational Unified Process - An Introduction. 2nd ed., Addison Wesley, (2000)
8. MND: Directive on National Acquisition Management Process - Automated Information System. Directive, No. 727, Ministry of National Defense, (2003)
9. C4ISR AWG: C4ISR Architecture Framework. Ver. 2.0, (1997)
10. DoD: DoD Architecture Framework. Ver. 1.0, (2003)
11. TRADOC: Operational Concept Description of Core Instrumentation System. Korea Advanced Combat Training Center, (1999)
12. DoD: Software Development and Documentation. MIL-STD-498, (1994)

Color Preference and Personality Modeling Using Fuzzy Reasoning Rule

Am-Suk Oh¹, Tae-Jung Lho², Jang-Woo Kwon³,
and Kwang-Baek Kim⁴

¹Dept. of Multimedia Engineering,
Tongmyoung Univ. of Information Technology, Korea
asoh@tit.ac.kr

²Dept. of Mechatronics Engineering,
Tongmyoung Univ. of Information Technology, Korea
tjllho@tit.ac.kr

³Dept. of Computer Engineering,
Tongmyoung Univ. of Information Technology, Korea
jwkwon@tit.ac.kr

⁴Dept. of Computer Engineering,
Silla University, Korea
gbkim@silla.ac.kr

Abstract. Human ability to perceive colors is a very subjective matter. The task of measuring and analyzing appropriate colors from colored images, which matches human sensitivity for perceiving colors has been a challenge to the research community. In this paper we propose a novel approach, which involves the use of fuzzy logic and reasoning to analyze the RGB color intensities extracted from sensory inputs to understand human sensitivity for various colors. Based on this approach, an intelligent system has been built to predict the subject's personality. The results of experiments conducted with this system are discussed in the paper.

1 Introduction

Color perception by an individual involves attaching a label denoting the color in order to categorize the perceived color. Human beings rely on color for a variety of reasons including recognizing color of the traffic signal while driving. However, human beings also regard it as an aesthetic issue when it comes to color perception for choosing the colors for their clothing, furniture and objects that surround them. The choice often reflects their personality. It is often difficult to label these colors exactly by using a finite number of categories like, red, blue green etc.

Human eye contains rods, which identify black & white, and three types of color cones, which are sensitive to blue, green and red. By combining the cone type's relative light intensities, color is perceived by the human brain. Combined response of cones is called the Eye Luminous Efficiency. Differences in individual's visual sensitivity results in different color perception by each human being. Psychologists have linked people's preference for colors with their personalities [1][2].

Computer monitors display a wide range of colors by assigning real values to the intensity of red, green and blue (RGB) colors and then fusing them. Number of bits is used to represent intensity of each color, hence if 2 bits are used only two values (black and white) can be represented. As the number of bits is increased more gray levels can be represented, which can result in providing excellent color saturation. However, the task of perception involves categorizing into color classes. If a single label is attached to the given pixel intensity value there is a high likelihood of making an error. This paper uses fuzzy logic and reasoning to determine the most appropriate linguistic label to the color selected from the given color palate in order to minimize the error.

The entire process of applying fuzzy logic in this paper contains the following steps:

- Step 1 : Define fuzzy sets
- Step 2 : Relate observations to fuzzy sets
- Step 3 : Define fuzzy rules
- Step 4 : Evaluate each case for all fuzzy rules
- Step 5 : Combine information from rules
- Step 6 : Defuzzify results.

2 Human Eye Color Sensitivity and Perception

Many researchers [3][4][5] have studied the color sensitivity of the human eye. Bjorstadt has used a variety of survey methods to study color sensitivity and human ability to perceive color. The study investigates [6] the relationship between color preference and the personality of the perceiver. According to the study, people who perceive yellow and red color and prefer warmer colors demonstrate a tendency to be “stimulus-receptive”. People who prefer warm colors are usually very active, straightforward and tend to be reasonable rather than confrontational by nature. They can be easily distracted, tend to give up easily and not struggle, and display strong emotions. On the other hand, people who prefer cold colors, i.e. green and blue, tend to be “stimulus-selective”. Table 1 shows the relationship between color preference and personality.

3 Dealing with Sensitivity Using Fuzzy Logic

3.1 Membership Function for Colors

The first task is to define fuzzy sets corresponding to high, low and intermediate values. An advantage of the fuzzy approach is that we don't have to define each possible level [7][8]. Intermediate levels are accounted for as they can have membership on both the high and low fuzzy sets[9]. For these the fuzzy sets we assume the membership function shown in Fig 1.

For each R, G, and B color values set memberships (Low, Low Medium, High Medium and High) are selected using a triangle type membership function and calculated using the intensity range. Based on the intensity value, membership value for each of the four fuzzy sets is calculated.

Table 1. Relationship between color preference and personality

Color preference	Personality
White	These people tend to be very self-conscience and behave based on how other people will perceive their actions. They tend to lack self-confidence and are often reluctant to express their own preferences.
Black	They tend to be unhappy, lack self-confidence and self-esteem, and are prone to dwell.
Gray	These people are not happy unless they are with other people and assisting them with their problems. They have great loyalty to country and home. They are independent, cautious, and prefer comfort to glamour. They are neat and fashionable.
Yellow	They tend to be intellectuals. They are definitely extrovert and likely, if crossed, to "roar like a lion." They are very generous, forthright, and open with people. People preferring yellow have a strong spiritual or metaphysical interest.
Orange	They are full of enthusiasm and look for adventure. Their ideas are unique. Their strong determination helps them carry through any plan of responsibility.
Brown	They see the good in all people. They have a very logical mind. They are understanding as well as firm. Their quick adaptability is a great asset.
Pink	They seem to be always dissatisfied. They usually do not express their own opinion.
Red	They tend to be extrovert, full of vigor and vitality. They are of youthful mind, which aspires to freedom of movement.
Green	They are usually kind, generous, and loyal. They are inclined to be methodical and you have great determination
Sky blue	They are stubborn. They are sensitive and conscientious.
Blue	They are very sensitive and have a tendency to be moody. Introvert by nature.

if $C \leq 45$ then $\mu_{Low}(C)=1$
 else if $C > 45$ and $C \leq 81$ then

$$total = \left(\frac{95 - C}{50} + \frac{C - 31}{50} \right)$$

$$\mu_{Low}(C) = \frac{C - 31}{50} \times \frac{1}{total}$$

$$\mu_{LM}(C) = \frac{95 - C}{50} \times \frac{1}{total}$$
 else if $C > 81$ and $C \leq 109$ then

$$\mu_{LM}(C) = 1$$
 else if $C > 109$ and $C \leq 145$ then

$$total = \left(\frac{159 - C}{50} \times \frac{1 - 95}{50} \right)$$

$$\mu_{LM}(C) = \frac{C - 95}{50} \times \frac{1}{total}$$

$$\mu_{HM}(C) = \frac{159 - C}{50} \times \frac{1}{total}$$
 else if $C > 145$ and $C \leq 173$ then

$$\mu_{HM}(C) = 1$$
 else if $C > 173$ and $C \leq 209$ then

$$total = \left(\frac{223 - C}{50} + \frac{C - 159}{50} \right)$$

$$\mu_{HM}(C) = \frac{C - 159}{50} \times \frac{1}{total}$$

$$\mu_{High}(C) = \frac{223 - C}{50} \times \frac{1}{total}$$
 else if $R > 209$ then $\mu_{High}(R) = 1$

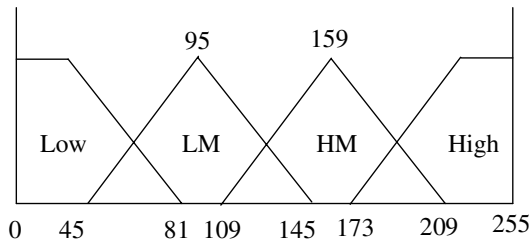


Fig. 1. Membership function for each color based on the color intensity

Fig. 1 shows the fuzzy membership functions for each color based on the color intensity using 8-bit representation, i.e. range of 0-255. Table 2 shows the interval for each fuzzy set membership function. H represents high function range, HM represents

medium high function range, LM represents the next lower function range, and L represents the lowest function range.

Table 2. Intervals for the fuzzy membership function

Fuzzy membership class	Intensity interval
Color frequency low.(L)	[0,81]
Color frequency little low.(LM)	[45,145]
Color frequency little high.(HM)	[109,209]
Color frequency high.(H)	[173,255]

3.2 Define Decision Rules for Color Information

First the intensity values for each color (red, blue and green) are obtained and the membership value for H, HM, LM, and L fuzzy sets is calculated using the function shown in Fig. 1.

Table 3. Rule of color reasoning

Color Preference	R	G	B	Membership Degree
White	H	H	H	H
	HM	HM	HM	HM
Black	L	L	L	H
	LM	LM	LM	HM
Gray	LM	LM	LM	H
	HM	HM	HM	H
Yellow	H	H	L	H
	HM	HM	L	HM
Orange	H	HM	L	H
	H	LM	L	HM
Brown	LM	LM	L	H
	HM	LM	L	HM
Pink	H	HM	HM	H
	H	LM	HM	H
Red	H	L	L	H
	H	LM	LM	HM
Green	L	H	L	H
	LM	H	LM	HM
Sky blue	LM	HM	H	H
	HM	HM	H	HM
Blue	L	L	H	H
	LM	LM	H	HM
Purple	HM	L	H	H
	HM	LM	H	HM

Now we must define the decision rules. These rules are defined in simple language terms. There are no decisions to be made about breakpoints. There are no decisions to be made about the functional form of the relationships. The rules can be understood at a common sense level. At the same time these rules result in specific and repeatable (same inputs gives same output) results. Table 3 shows the decision rules that relate the color to the fuzzy set membership value for the RGB color. It is possible to assign numerous different color categories. However, only 12 color categories are chosen for the fuzzy reasoning rules.

3.3 De-fuzzinification to Obtain Precise Color

Next step is to draw inference using the rules shown in Table 3. In this case, we want to relate the observations to the rules. We are interested in what degree an observation has membership in the fuzzy set associated with each rule. The following memberships need to be evaluated as follows:

$$\begin{aligned} \mu_{R_i}(R_m G_m B_m, Y_m) &= \min(\mu_R(R_i), \mu_G(G_i), \mu_B(B_i), \mu_Y(Y_i)) \\ \mu_T(m_i) &= \max(\min(\mu_R(R_i), \mu_G(G_i), \mu_B(B_i)), \mu_Y(Y_i)) \end{aligned} \tag{1}$$

For logical "and" operations using fuzzy sets the resulting membership functions are defined as the minimum of the values of the memberships on the component sets. If the rule has "or" operations the maximum of the memberships would be used. Further these memberships can be used to define a fuzzy set for the outcomes of the rules. Specifically, the membership of an observation on the rules fuzzy set becomes the maximum membership of the outcomes fuzzy set.

In this paper we use the Max-Min method to determine the membership of an observation. In step 5 combinations are performed. The task is to define one fuzzy set for the outcome considering all the rules and the values for a specific observation. One way to do this is take the maximum of the score for the membership function defined for each rule. In this paper, the composite score is determined using center of gravity method. The composite score X is calculated using equation below.

$$X = \frac{\sum(x_i \times \mu_i)}{\sum x_i} \tag{2}$$

In this phase, linguistic meaning is assigned to each pixel in the set using a fuzzy inference operation. To do this we first combine the results from all rules into the outcome fuzzy set and then transform this composite fuzzy set to a crisp number. Table 4 shows the final result of color evaluation using defuzzification.

Table 4. The final color evaluation

Final color	Evaluation range
As membership value is low crisp value is 0	$0 \leq X < 0.4$
To result of inference for membership value is highest color intensity	$0.4 \leq X \leq 1.0$

4 Experimental Analysis and Results

In order to embody color sensitivity using Fuzzy theory, experiments were carried out using Visual C++ 6.0 on an IBM PC with a Pentium TV CPU. Fig. 2 shows the screen capture of a window designed using an image editing program for providing a range of color options to the user. The user chooses the color by clicking on the color palate provided in that window. Note that a large variety of colors are available to the user to choose from. After the user selects the color from the variety of options, fuzzy logic and reasoning approach discussed in this paper is applied and the nearest matching color is determined. Fig. 3 shows the screen capture where a user has chosen a color from the palate (on the left). On the right the nearest match chosen by our approach is shown in Fig. 3.

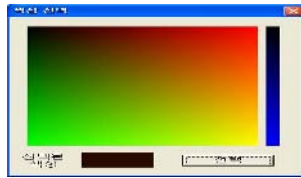


Fig. 2. Screen capture of the computer application showing the color palate

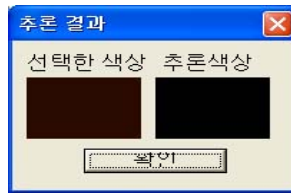


Fig. 3. Screen captures showing the color chosen by the user and the color match obtained by the fuzzy intelligent

Fig. 3 here shows selection of optional black level color, RGB(41,11,1) by the user on the left. On the right the fuzzy logic and reasoning analysis result shows the value RGB (0,0,0). Based on the color value obtained by fuzzy logic and reasoning analysis Fig. 4 shows the result based on the research of Bjurstadt.

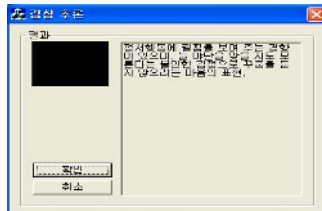


Fig. 4. Screen captures displaying the color preference and the personality of user

5 Conclusion

We have discussed a fuzzy logic based approach for assigning linguistic labels to a variety of color combinations. An intelligent system has been designed which displays a color palate to the subject. The subject chooses the color of his preferences and based on the fuzzy reasoning algorithm system performs computations. Finally, the color preference is linked by the system to subject's personality based on existing psychological studies. Results of experiments with this system demonstrate its success.

References

1. Lee, K. S. and Chung, H. M.: The Emotions Inference Using Differential of Symbolic Multiple Valued Logic Functions. Proceedings of KFIS Fall Conference, Vol. 12. No. 2. (2002) 493-496
2. Weiner, B.: The Emotional Consequences of Casual Ascriptions. The 17th Annual Carnegie Symposium on Cognition, (1994) 185-209
3. Fabo, B.: The Psychology of Color. Dong-A Publications, (1985)
4. Deborah, T. S.: The Psychology of Color and Design. Tein Publications, (1996)
5. Color Psychology, <http://simri.netian.com/>.
6. Pluchik, R.: Emotion. A Psycho Evolutionary Synthesis, (1980)
7. Lee, H. J., Kim, B. S., Kang, D. H. and Kim, K. B.: Recognition of Emotion Based on Simple Color using Physiological Fuzzy Neural Networks. Proceedings of Korea Multimedia Society, Vol. 6. No. 1. (2002)537-540
8. Yasuhiro K. and Naotoshi, S.: An analysis of emotions by using fuzzy reasoning. 13th Fuzzy Symposium, (1997) 4-6
9. Kim, B. K., Kim, B. Y. and Cho, J. H.: Self-Directed Learning using Fuzzy Grade Sheets. International Journal of KIMICS, Vol. 2. No. 2. (2005) 97-101

The Development of Reliability Verification Tool of RFID Tag for Effective Product Control Systems

Ki-Uk Kim¹, Hyun-Suk Hwang², Bong-Je Kim¹, Su-Hwan Jeong¹,
and Chang-Soo Kim^{1,*}

¹ PuKyong National University,
Dept. of Computer Science, Korea
dawnlion@daum.net, kbj0430@pdj.hs.kr,
tony6666@nate.com, cskim@pknu.ac.kr

² PuKyong National University,
Institute of Engineering Research, Korea
hhs@mail11.pknu.ac.kr

Abstract. Radio Frequency Identification (RFID) systems, which are the important technology to identify objects using tags, readers, and sensors, have been used in many applications. Recently, the performance evaluation of RFID systems is required to construct effective RFID systems as the development of RFID systems increases. However, most existing researches are limited to systematic factors related to RFID hardware systems. Therefore, we propose the environmental factors affecting on the performance of RFID systems and verify the reliability of RFID systems through defined factors. For doing the evaluation, we construct a prototype of product control RFID system and simulate our system with the proposed factors. As the results, we describe the factors to construct effective RFID systems.

1 Introduction

Radio Frequency Identification (RFID) is the technology for executing individual identification using Radio Frequency. The RFID is important for Ubiquitous Computing Environment, and much of the research has dealt with expectations of economic effects attained from RFID technology in Korea, America, Japan and elsewhere [18]. Research into the RFID system is classified into hardware and software systems. In the hardware development, most of the research focuses on the RFID tag and reader [14] and RFID software systems in fields of library control [2], airport [20], entrance exit management system [15], transportation [10], postal system [1], and product control system [17].

As the applications mentioned above, RFID systems have been actively used in many parts. Especially, product control processes, which are a common part in real business fields, have been constructed using 13.56 MHz RFID systems [22]. However, there are some restrictions in using RFID systems in actual field of the

* Corresponding author.

product control because of the cost of RFID tag [19], tag collision [9], performance [21], and security [8]. Especially, the performance of RFID equipment such as tags and readers is an important consideration in constructing RFID systems. For example, how the system performs as different variations of the distance between the reader and tags, tag location, and multi-tag, and how the system performs in different environments such as sensors and conveyor’s speed [5]. Therefore, it is essential that reliable verification tool to evaluate performance of RFID systems must be provided to apply the RFID systems to real fields in a rapid time frame.

In this paper we propose the factors and methods for performance evaluation in RFID systems. In order to verify the RFID systems, we composed of two parts. At the first part, we will implement a RFID system on a real-time product control process which is manufactured as a prototype system for simulations of a RFID system in our laboratory [16][13]. Next, we will test our system as factors affecting on the performance of RFID systems with the various kinds of RFID Tags.

This paper is organized in the following manner. In the next section, we describe the features of RFID system and common factors affecting the RFID systems in previous research. In Section 3, we present the architecture of a RFID system, and propose the factors for reliable verification. We address the results of experiment, and finally, we summarize this research and describe future work.

2 RFID Systems

2.1 The RFID Features

RFID systems consist of two main components, RFID tags which are attached to the object to be identified and are perceived as the data carriers, and RFID readers, which can read tags by sensors [6]. RFID systems have different features as frequency. Especially, the 13.56MHz frequency is used in the most active fields because the tags are relatively cheaper, and these features are shown in table 1. The 13.56MHz RFID systems are usually used in automation of productions and product control systems [23].

Table 1. The Features of 13.56MHz RFID Systems

The Features	Contents
Reading Distance	< 60cm
Operation Mode	Passive
Application Field	Product Control Process, Transportation Card, Baggage Control
Identification Speed	Low Speed
Read/Write Function	Available

Data in RFID tags can be written and read. This regulation follows the ISO 15693 standard [12] and is shown in Fig 1. The data is written in the area of defined data blocks. RFID systems have advantages to write to tags and to reuse them [3].

Block : 8 byte

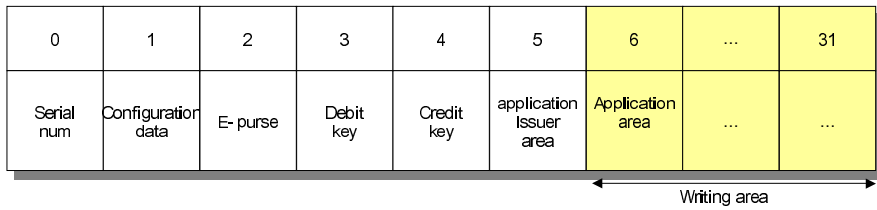


Fig. 1. Data Block of RFID Tag

2.2 Factors Affecting the RFID System Performance

As mentioned in the earlier section, it is limitations that the current RFID systems are dependent on the environmental factors such as speeds, distances, and temperatures of devices. The research about factors affecting the verification of RFID systems are of a growing interest, and some of the research has proposed several factors as shown table 2.

Table 2. Related Works

Authors	The Factors	Frequency	Features
Floerkemeier[7]	<ul style="list-style-type: none"> - arrangement of tag - tag detuning - collision with other device - affecting on metal/water 	13.56MHz	Design improvement
Inoue [11]	<ul style="list-style-type: none"> - arrangement of tag - distance between tag/reader - moving speed of tag - collision with other device 	13.56MHz	Systematic approach
Daniel [4]	<ul style="list-style-type: none"> - distance between tag/reader - affecting on metal/water - identification rate of material 	900MHz	The first performance evaluation test

Floerkmeier [7] and Inoue [11] proposed the problems of RFID and tried to improve the reliability through a systematic approach. However, the study does not present the performance results of various tags. The research aim of RFID Alliance Lab [4] is to provide the performance evaluation of RFID system on the 900MHz systems.

The factors affecting the RFID systems in most research are tag location, collision problem and tag speed.

3 Architecture for Verification of RFID Systems

We present the architecture of RFID systems and factors to verify the performance the systems.

3.1 RFID Verification System Architecture

The architecture of the verification tool of RFID system is shown in Fig 2. We developed a method to verify a product control RFID system and developed the verification tool using the system. The RFID system consists of the start client, the Web service, database system, and the end client. The start clients read product information such as type, color, size, serial number and save the information to a tag. Web services process values required from clients by connecting to the database systems. The end clients confirm the actual products and display the information on a screen in a control line by reading RFID tag. The line information as the type of products will be set up before the system is started.

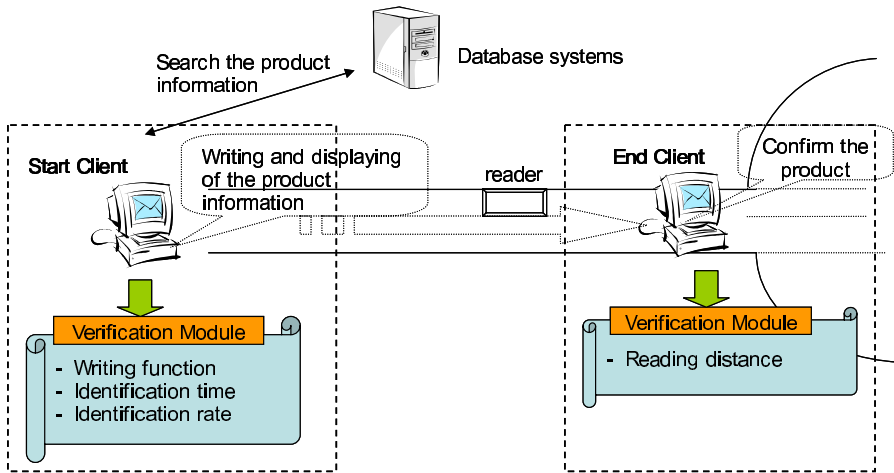


Fig. 2. Architecture of the RFID System

Start Client. Client systems read the product information from database systems and a tag serial number by a tag reader. The general procedures of start client modules are as follows.

- (1) The workers login to RFID product control system with defined login-id and line number.
- (2) Tag is loaded onto the products.
- (3) The information of products is read from database systems.
- (4) The employees make sure the information is accurate.
- (5) When the contents of products happen to be modified, they will be change into other types of products.
- (6) The changed item will record on the database systems
- (7) The product serial number is recorded in the RFID Tag.

End Client. End clients confirm product information and classification according to products features. The sensor in end clients helps the identification of products. The I/O card control system distributes the products and a packing spot that categorizes the products before wrapping according to feature of products.

- (1) The sensor recognizes the production through RFID tag.
- (2) The product information is displayed on the screen.
- (3) The products are classified by classifier according to a signal whether the product information is exact or not.

Verification Module. We verify the performance of RFID tags. The performance evaluation is performed in the four factors which are identification time, identification multiple tags, distance between tags and readers, and writing ability of tags. The experiment of the distance factor is preformed in the end clients and other factors are experimented on the client module.

3.2 Factors of Reliability Verification

We use the two kinds of tag, the Pico tag system of A company which operates at 13.56MHz based on the ISO 15693 standard[12] for RFID. The specifications of tested RFID tags are in table 3. We experimented with the factors of reading distances, identification time, identification rate, and writing ability.

Table 3. Tested RFID Tags Descriptions

Features	Pico Tag
Standard Protocol	ISO 15693
Carrier Frequency	13.56MHz
Reading Distance	70cm – 1.5m
Anti Collision	50 chips/s
Type of Tags	Card type & Film type
EEPROM Memory Size	8 byte block
Communication Speed	26kbps

Table 4. Verification Factors

Factors	Variable	Experiment Criterions
Identification Speed	Identification time per one tag	- Number of test tag : from 1 to 20 - Arrangement of tag: 4*4 metrics
The rate of Identification	The number of tags	- Number of tag : from 1 to 20 - Arrangement of tag: 4*4 metrics
	The distance between tags and reader	- Location of tag : middle of reader - Number of tag : one per one time - The distance: 0.1 - 20cm
Durability	The number of writing	- The size of writing data : 8 byte - Number of test tag : one tag at a time

The factors affecting the verification are divided into three parts, which are total identification time, the distance of reading success, and writing ability as shown table 4.

4 Verification Results

4.1 Method of Reliability Verification

We describe the reliability verification method and how the verification performs in Fig. 3.

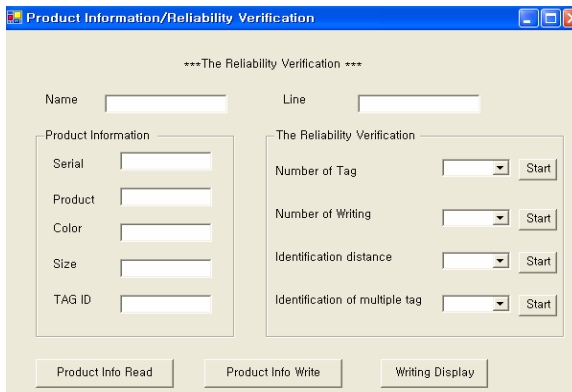


Fig. 3. Reliability Verification Tool

Number of Tag. We verified the collision problem. We select a number of the tags from 1 to 20 in regular sequence. The return values are the total identification time.

Number of Writing. We verified how many writings are possible. The data of 8 bytes size are written in the tags, and we checked the return values, which are the number of writing success tags.

Identification Distance. We checked how many tags were identified as varied distances, which were measured from 0.5cm to 20cm.

Identification of Multiple Tags. We also verified the collision problem. We arranged the tags of shape of 4*4 metrics as increasing from 1 to 25 tags.

4.2 Results of Reliability Verification

We present the results of reliability verification. This research used two kinds of RFID tags, which are card types and film types. Fig. 4 shows the results of verification data. In Card type tag, the average identification time per one tag is 41.34(ms), and the other type is 48.41(ms). As a result, we know card type tags are better than film ones in identification average time.

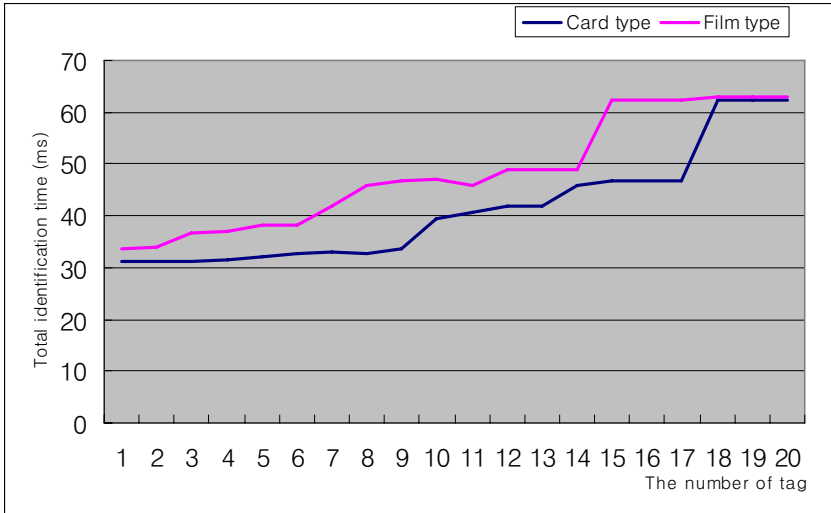


Fig. 4. Identification Time according to the Tag Number

Fig. 5 shows the results of identification rates of multiple tags. The identification rate until 6 tag is about 90%. However, the identification performance drops in more than 6 tags after 13 tags identification rate fall to 50%. In case of Card type tag, the performance is under 25% in more than 14 tags, but the Film type is under 25% from 19 tags. Hence, we discover the number of tags used in real-time product control is suitable about 6 tags, and we can recommend the card type tag than film type tag if tags are identified immediately.

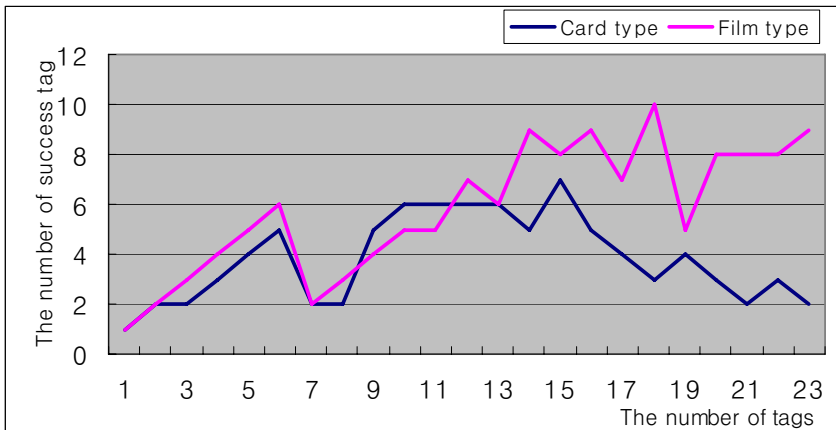


Fig. 5. Identification Rate of Multiple Tags

Fig. 6 shows how RFID tags can be identified in some distances. We have verified 20 tags according to distance points. The results represent that the best distance of Card type tag is from 0.5 to 14.5 (cm), and Film type is suitable in 4.5 (cm). The results shows the distances between readers and tags can be suitable to 14 cm in card type tags.

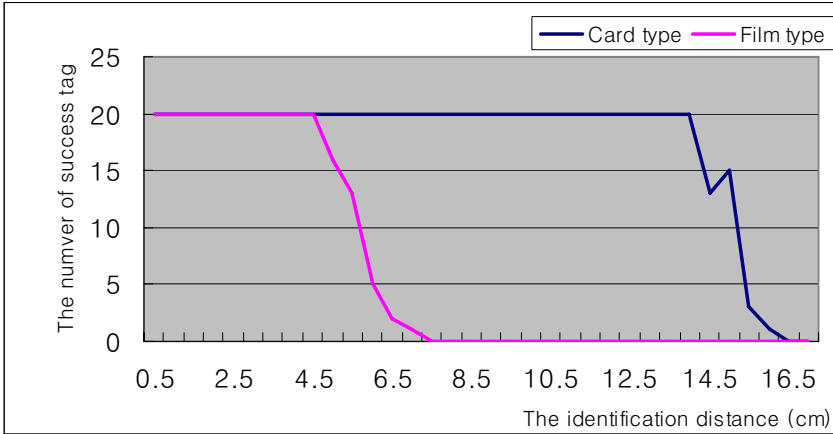


Fig. 6. The Reading Distance

Fig. 7 shows how many data is written in a tag. We have saved size the data of 8 bytes repeatedly and checked how many the writing works are successful each case. We know that the Card type tags are strong until writing to about 30 times, and Film type tag is strong until 10 times. The average error rate to writing works is about 0.36 in the card type. Hence, we can recommend the use of card type tags in case tags needs writing works, and the cards are unstable in writing after using the tag for 30 times.

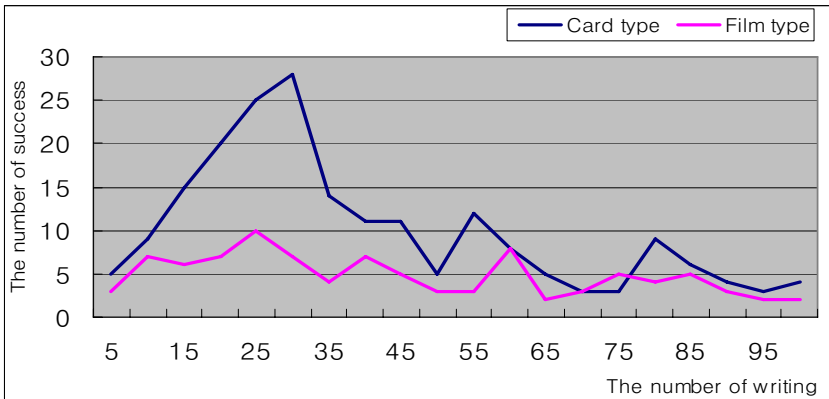


Fig. 7. Writing Ability

5 Conclusion

In this paper, we proposed the factors affecting the performance evaluation and verified the reliability verification of RFID Tag using 13.56MHz RFID system. To verify the RFID systems, we implemented the production control system and we tested it by using different tags. We discovered that the number of tags used in real-time product control is suitable for 6 tags, and we can recommend the card type tag rather than the film type tag if tags are identified immediately. Also, we know from the results that the card type tags are stable in 14 cm in distance distances and 1 to 30 times in writing ability.

Our future works are as follows. In this research, we have tested product of one vendor and two kinds of tags. We need verification of various vendors of RFID systems to provide effective performance evaluation. Also, we must add the some factors affecting the interference between tags and packing material.

References

1. Bak,M., Jung,U., Jin,B.,Lee,Y., KimmH.: Practical use of RFID technology for improvement of the Postal Service. Journal of Electronic and Telecommunications Research Institute. Vol 16. No 6. (2001) 153-162
2. Che,J., Son,J., Oh,D., Kang,B., Bak,S,: Development of a Book Retrieval System using RFIDs and Wireless Teriminals. Proceedings of the Korea Multimedia Society Conference (2003) 1035-1038
3. Clinton,S.:A Global SAW ID Tag with Large Data Capacity. IEEE Ultrasonics Symposium (2002) 65-69
4. Daniel,D., RFID Alliance Lab: A Performance Analysis of Commercially Available UHF RFID Tags Based on EPCGlobal's Class 0 and Class 1 Specifications. <http://www.rfidalliancelab.org/r1exc/title.html>
5. De, P., Basu,K., Das,K.: An Ubiquitous Architectural Framework and Protocol for Object Tracking using RFID Tags. Proceedings of the First Annual International Conference on Mobile and Ubiquitous System. (2004) 1-9
6. Finkenzeller, K.: RFID Handbook. John Willey & Sons Inc. (2003)
7. Floerkemeier,C., Lampe,M.: Issue with RFID usage in ubiquitous computing applications. Pervasive Computing Second International Conference , LNCS No.3001 (2004) 188-193
8. Gao,X.,Xiang,Z.,Wang, H.,Shen,J.,Huang,J.,Song,S.:An Approach to Security and Privacy of RFID System for Supply Chain. Proceedings of IEEE International Conference on E-Commerce Technology for Dynamic E-Business (2004)
9. Hartmann,P.,Brown,J.,Claiborne,W.: Anti-Collision Methods for Global SAW RFID Tag System. Proceedings of IEEE International Ultrasonics Symposium IEEE (2004) 805-808
10. Hightower,J., Borriello,G.: Location System for Ubiquitous Computing. IEEE. Vol.34, No 8 (2001)
11. Inoue,S.,Hagiwara,D.,Yasuura,H.:A Systematic Approach for the Reliability of RFID System. TELCON 2004 IEEE Region 10 Conference. (2004) 183-186
12. ISO/IEC JTC1/SC31, <http://usnet03.uc-council.org/sc31>, (2005)
13. Jeong, S. H., Hwang, H.S. ,Kim,C. S.:The Development of Component Modules of RFID Tag Application for Product Control Systems, Proceedings of the Korea Multimedia Society Conference, Vol. 8, No. 2 (2005) 135-139

14. Jeong,S.: A study on RFID technology and policy 2004, National computerization agency in korea (2004) 1-285
15. Jung,T., Kim,H., Lee,S., Kim,C., : Design and Implement of Entrance and Exit Management System Using RFID. Proceedings of the Korea Multimedia Society Conference (2005) 739-742
16. Kim,K.,Jeong,T.,Lee,S.,Kim,C.,Hwang,H.,Jeong,S.: The Implementation of the Real-Time Product control System using RFID Tag. Proceedings of the 12th KSII FALL Conference,Vol.6, No.2 (2005) 331-336
17. Kim,K., Kim,N,: The Development of a good warehouse Management systems based on Ubi Computing using RFID. Proceedings of the Korea Intelligent information system society Conference (2004) 204-208
18. Kim,S., Bak,S.: A industry trend and development prospect RFID/USN of RFID/USN, ETRI Journal vol. 20. (2005) 43-54
19. Lee,J.:The Chipless Technology. Proceedings of the Korea electromagnetic engineering society Conference. Vol 15, No.2 (2004) 54-63
20. Mccoy,T., Bullock, R., Brennan,P.: RFID for airport security and efficiency. Signal Processing Soutlions for Homeland Security 2005. (2005)
21. Penttila, K.,Sydanheimo,L.,Kiviloski,M.: Performance development of a high-speed automatic object identification using passive RFID technology. Proceedings of the 2004 IEEE International Conference on Robotics & Automation (2004) 4864-4868
22. Ryoson,H.,Goto,k.,Ueno,M.,Kikuchi,A.,Shimpuku,Y.: 13.56MHz RFID Device and software for mobile system. Consumer Communication and Networking Conference (2005) 241-244
23. Steve,C.,Thomas,V.:Optimization of inductive RFID Technology for Product Management. Proceedings of the 2001 IEEE International Symposium (2001) 82-87

Avoidance of State Explosion Using Dependency Analysis in Model Checking Control Flow Model

Sachoun Park and Gihwon Kwon

Department of Computer Science, Kyonggi University,
San 94-6, Yiui-Dong, Youngtong-Gu, Suwon-Si, Kyonggi-Do, Korea
{sachem, khkwon}@kyonggi.ac.kr

Abstract. State explosion problem is a major huddle in model checking area. The model described in the temporal model checking is mainly control flow model. The *f*FSM is a model for describing the control flow aspects in PeaCE(Ptolemy extension as a Codesign Environment), which is a hardware/software codesign environment to support complex embedded systems. *f*FSM, like a Statecharts, supports concurrency, hierarchy and global variables. But due to lack of their formality, we defined step semantics for this model and developed its verification tool in the previous work. In this paper, we present the model reduction technique based on dependency analysis to avoid the state explosion problem. As a result, the model, which couldn't be verified before applying the technique, is verified.

Keywords: State explosion problem, Dependency analysis, Model reduction, Model checking.

1 Introduction

Control flow model like a Finite State Machine (FSM) is widely used in specifying system behavior. The PeaCE[1] is the Hardware/software codesign environment to support complex embedded systems. The specification uses synchronous dataflow (SDF) model for computation tasks, extended FSM model for control tasks and task-level specification model for system level coordination of internal models (SDF and FSM).

The *f*FSM is another variant of Harel's Statecharts, which supports concurrency, hierarchy and internal event as Statecharts does. Also it includes global variables as memories in a system. This model is influenced from STATEMATE of i-Logix inc.[2] and the Ptolemy[3] approaches. But the formal semantics of *f*FSM was not defined. The absence of a formal semantics caused problems such as confidence for simulation, correctness of code generation, and validation of a system specification. In the previous work, in order to solve those problems we defined step semantics of *f*FSM and we developed simulation and verification tool, Stepper, by means of the formal semantics, which was defined by flatten model of *f*FSM. SMV model checker was used in verification part, so this tool had a translation module from flatten *f*FSM into input language of SMV. In our tool, to be convenient for user to check some

* This work was supported by grant No.(R01-2005-000-11120-0) from the Basic Research Program of the Korea Science & Engineering Foundation.

important properties, those are automatically generated. According to the users' choice in the property window, one of six properties can be checked. Built-in properties are such as unused components, unreachable guards, ambiguous transitions, deadlock, divergent behaviors, and race condition violation[4].

However, because of the use of variables in *f*FSM model, the state explosion problem occurs. Therefore, in this paper, to overcome the problem, we introduce model reduction technique into the Stepper, which is focusing on components of the model that are referred to in the property to be checked via dependency analysis. This technique is sometimes known as *cone of influence* which syntactically decrease the size of the state transition graph. Chan showed effective results of the model checking of Statecharts model using this technique[5]. Lind-Nielsen[6] proposed dependency analysis on the HSEM(Hierarchical State Event Model) to perform the compositional model checking. We attempted to apply these techniques to *f*FSM model to tackle the state explosion problem. Through experimental results, we show that the Stepper is improved on the scalability and give that system consisted of loosely coupled components is very effective in model checking.

The rest of the paper is structured as follows. In the next section, we overview the reduction technique so called cone-of-influence. In Section 3, we show reduction technique with dependency analysis in the control flow model. The experimental results present in section 4, and then we conclude the paper in section 5.

2 Background

Cone of influence technique attempts to decrease the size of the control flow model by focusing on the variables of the system that are referred to in the properties for model checking. In this chapter, we will summarize the cone of influence abstraction explained in [7].

Let V be the set of variables of a given synchronous circuits, which can be described by a set of equations: $v_i' = f_i(V)$, for each $v_i \in V$, where f_i is a boolean function. Suppose that a set of variables $V' \subseteq V$ are of interest with respect to the required property. We want to simplify the model by referring only to these variables. However, the values of variables in V' might depend on values of variables not in V' . Therefore, we define the cone of influence C for V' and use C in order to reduce the description of the model. The cone of influence C of V' is the minimal set of variables such that

- $V' \subseteq C$
- If for some $v_i \in C$ its f_i depends on v_j , the $v_j \in C$.

We will next show that the cone of influence reduction preserves the correctness of specifications in Computation Tree Logic(CTL) if they are defined over variables (atomic propositions) in C .

Let $V = \{v_1, \dots, v_n\}$ be a set of Boolean variables and let $M = \{S, R, S_0, L\}$ be the model of a synchronous circuit defined over V where,

$S = \{0,1\}^n$ is the set of all valuation of V .

$$R = \bigwedge_{i=1}^n [v_i' = f_i(V)].$$

$$L(s) = \{v_i \mid s(v_i) = 1 \text{ for } 1 \leq i \leq n\}, S_0 \subseteq S.$$

Suppose we reduce the circuit with respect to the cone of influence $C = \{v_1, \dots, v_k\}$ for some $k \leq n$. The reduced model $\hat{M} = (\hat{S}, \hat{R}, \hat{S}_0, \hat{L})$ is defined by

$$\hat{S} = \{0,1\}^k \text{ is the set of all valuations of } \{v_1, \dots, v_k\}$$

$$\hat{R} = \bigwedge_{i=1}^k [v_i' = f_i(V)]$$

$$\hat{L}(\hat{s}) = \{v_i \mid \hat{s}(v_i) = 1 \text{ for } 1 \leq i \leq k\}$$

$$\hat{S}_0 = \{(\hat{d}_1, \dots, \hat{d}_k \mid \text{there is a state } (d_1, \dots, d_n) \in S_0 \text{ such that } \hat{d}_1 = d_1 \wedge \dots \wedge \hat{d}_k = d_k\}$$

Let $B \subseteq S \times \hat{S}$ be the relation defined as follow:

$$((d_1, \dots, d_k), (\hat{d}_1, \dots, \hat{d}_k)) \in B \Leftrightarrow d_i = \hat{d}_k \text{ for all } 1 \leq i \leq k$$

According to the proof in [7] B is a bisimulation between M and \hat{M} . Thus, $M \equiv \hat{M}$. As a result, we can obtain the following theorem:

Let f be a CTL formula with atomic proposition in C . Then $M \models f \Leftrightarrow \hat{M} \models f$.

3 Reduction of Control Flow Model

In this section, we explain our reduction method with below example. Figure 1 shows f FSM of mole game, where a player can hit the moles which move up and down after he/she inserts the coin. This game is a kind of reflex game. Whenever the player hit the risen mole, the score increase. During a time unit, presented *time* event, player can hit one mole once.

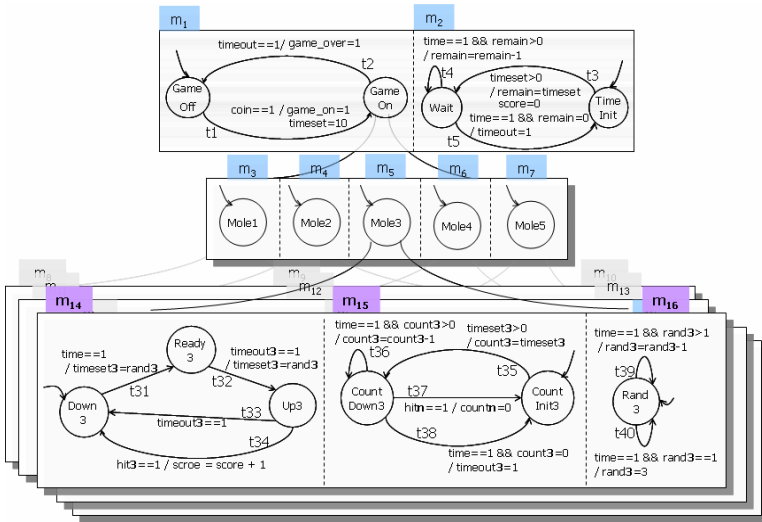


Fig. 1. f FSM model of mole game

3.1 Syntax of Control Flow Model

To explain the reduction technique, we define flatten machine of *fFSM*. There exit events, global variables, states, and transition. *I*, *O*, and *IT* are sets of input events, output events, and internal events, respectively.

Definition 1 (*fFSM*). $fFSM = (I, O, IT, M, \gamma, V)$, where *I*, *O*, *IT* are set of events, *V* is a set of global variables, and $M = \{m_1, \dots, m_n\}$ is the set of *simple FSM*. Let $\Sigma = \bigcup_{i=1}^n S_i$ be the set of all states in *M*, hierarchical relation γ maps a state to the set of machines which belong to the state: $\gamma: \Sigma \rightarrow 2^M$.

The hierarchical function γ has three properties: there exist a unique root machine, every non-root machine has exactly one ancestor state, and the composition function contains no cycles. Let $sub: \Sigma \rightarrow 2^\Sigma$, and $sub(s) = \{s' \mid M_i \in \gamma(s) \wedge s' \in S_i\}$ is another function to relate between a super state and its sub states. sub^+ denotes the transitive closure of *sub* and sub^* denotes the reflexive transitive closure of *sub*.

Definition 2 (*Simple FSM*). $m_i = (S_i, s_i^0, T_i, scr_i)$

1. $S_i = \{s_i^0, s_i^1, \dots, s_i^n\}$ is the finite set of states of m_i ,
2. s_i^0 is a initial state,
3. T_i is the set of transition of m_i , and a transition $t \in T_i = (s, g, A, s')$ is composed of source and target states $s, s' \in S_i$, guarding condition g which is Boolean expression, and set of actions *A*,
4. $scr_i: S_i \rightarrow 2^{Script}$ is a function to map a set of script into a state.

Guards that include variables and events have the following minimal grammar.

$$G ::= true \mid \neg G \mid G_1 \wedge G_2 \mid e < Exp \mid e = Exp \mid v < Exp \mid v = Exp$$

$$Exp ::= n \mid v \mid Exp_1 \bullet Exp_2,$$

where *n* is an integer constant, $v \in V$ is a global variable, $\bullet \in \{+, -, \times, / \}$ represents a set of binary operators.

3.2 Dependency Analysis in Control Flow Model

Although this example is a small, however it has 20 events and 18 variables, which cause state explosion during model checking. So we focused the feature of this model and found out that the relationship among moles is loosely coupled. Actually if we want to check any properties about the *mole3*, there is no need to concern with other moles, because the behavior of the *mole3* is not affected by other moles. In order to verify the model reduced by means of only components referred in a property, we defined dependency between components in a given model, where the component is one of machine, event, and variable, because each component is translated by one variable in SMV input language according to translation rules mentioned in previous works[4], we can say that this reduction technique preserves the correctness of properties written CTL if they are defined over variables (atomic propositions)

corresponding to components referred in properties. In this subsection we will explain how to generate dependency graph of given \mathcal{J} FSM model.

Definition 3 (Dependency Graph). Dependency graph is consist of set of nodes N and set of links L . N is a set of all components of given model and when m is a simple machine, $e \in \mathcal{IOU\mathcal{I}T}$ is an event, $v \in V$ is a variable, L is a set of the dependency relation defined as follows:

1. Machine m depends on machine m' if m is defined in a sub-machine of m' . Machine m depends on event e or variable v if there is at least one guard in m that has a syntactic reference to e or v .
2. Event e depends on machine m if there is at least one occurring e in m . Event e depends on event e' or variable v if e' or v is used a guard to occur e . Event e depends on variable v if e is used an action and there is a syntactic reference to v in the right-hand side of the assignment of the action.
3. Variable v depends on machine m if there is at least one assignment to v in m . Variable v depends on event e or variable v' if e or v' is used a guard to update v and v is used in the right-hand side of the assignment to v .

Below figure 2 shows a generated DG by means of Definition 3 about machine m_1 and m_2 in Figure 1. DG is obtained by fixed point calculation from components referred in properties to be checked. Machine m_1 and m_2 do not directly depend on each other, but through events *timeset* and *timeout* depend on each other implicitly.

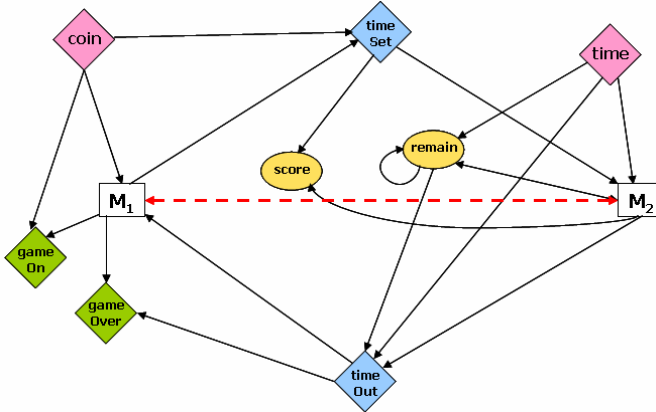


Fig. 2. Dependency graph of m_1 and m_2 in Figure 1

3.3 Correctness of Specification in Reduced Model

With the DG, if we want to check about the machine m_2 , then events *gameOn* and *gameOver* may not be used to translate the model into SMV. This technique is a kind of *cone of influence* mentioned in previous chapter. Due to our translation rule, each component in DG corresponds to variable in SMV and variables in SMV are implicitly represented by Boolean variables. So we regard the component as some

Boolean variables like variables in synchronous circuits. It is proved in [7] that the cone of influence preserves the correctness of specifications in CTL if they are defined over variables (atomic propositions) corresponding to components referred in properties. According to the proof, since the original model M and the reduced model M' are bisimulation relation, for any CTL formula ϕ written in referred components in a given property, $M \models \phi \Leftrightarrow M' \models \phi$.

4 Experimental Results

4.1 Verification on Reduced Model

Using simulation, ambiguous transitions was found machine m_{15} in Figure 1. The event trace is $\langle \{coin\}, \{time\}, \{time\}, \{time\}, \{time\}, \{time, hit_3\} \rangle$. It means that when the first rising the third mole, if player hits the mole, then in state the *CountDown3*, transition t_{36} and t_{37} are executed simultaneously, that is ambiguous transitions. But, by original model, we cannot terminate the verification procedure in Stepper. To overcome this state explosion problem, we apply the reduction technique based on DG explained in previous section, like figure 3. So we can detect this error within 8.25 second and 159027 BDD size. However, the trace generated by model checking is not the same by simulation. The result trace is $\langle \{coin\}, \{time\}, \{time, hit_3\} \rangle$. It means that there exist serious flaw in the mole game f FSM.

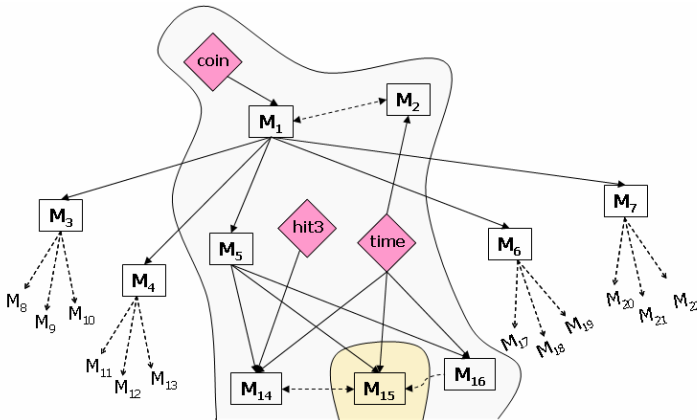


Fig. 3. Selected machine for verifying ambiguous transitions in m_{15}

4.2 Correction of the Model Error

The model error is that when still the control is in *Ready3* state, if player hits the third mole, since the model react the event hit_3 , t_{36} and t_{34} are executed simultaneously, but it is just a model error, that is ugly model, not any semantic error. Even though there is a little concern of observation, we can understand that the machine m_5 becomes stuck after that trace. However, through the detection of local deadlock, this error is not detected by semantic analysis because eventually when the super state of machine

m_5 is transferred, the stuck situation is forced to be resolved by semantics. In this case, like Figure 4, designer must modify the model.

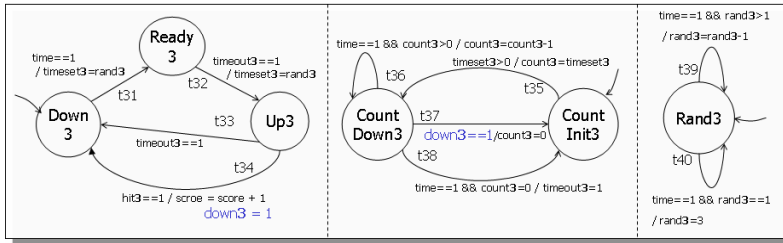


Fig. 4. Modified sub-model under the machine m_5

5 Conclusions

The f FSM is a model for describing the control flow aspects in PeaCE(Ptolemy extension as a Codesign Environment), which is a hardware/software codesign environment to support complex embedded systems[1]. We defined step semantics for the control flow model and developed its verification tool in the previous work[4]. In this paper, in order to avoid the state explosion problem, we introduce the model reduction technique based on dependency analysis[5,6,7]. As a result, the model, which couldn't be verified before applying the technique, is verified.

Now we are interesting in applying this reduction technique to software model checking. Because software model used in model checking is one of control flow model and its size is huge.

References

1. D. Kim, "System-Level Specification and Cosimulation for Multimedia Embedded Systems," Ph.D. Dissertation, Computer Science Department, Seoul National University, 2004.
2. iLogix: <http://www.ilogix.com/>
3. <http://ptolemy.eecs.berkeley.edu/>
4. S. Park, K. G. Kwon, and S. Ha, "Formalization of f FSM Model and Its Verification," in the Proceedings of the ICESSE, LNCS 3820, Springer, pp.361-372, 2005.
5. W. Chan, "Symbolic Model checking for Large software Specification," Dissertation, Computer Science and Engineering at University of Washington, 1999.
6. J. B. Lind-Nielsen, "Verification of Large State/Event Systems," Ph.D. Dissertation, Department of Information Technology, Technical University of Denmark, 2000.
7. E. M. Clarke, O. Grumberg and D. Peled, Model Checking, MIT Press, 1999.
8. J. Lind-Nielsen, H. R. Andersen, H. Hulgaard, G. Behrmann, K. J. Kristoffersen, K. G. Larsen, "Verification of Large State/Event Systems Using Compositionality and Dependency Analysis", FMSD, pp. 5-23, 2001.
9. E. M. Clarke, W. Heinle, "Modular translation of Statecharts to SMV," Technical Report CMU-CS-00-XXX, CMU School of Computer Science, August 2000.

Design and Implementation of Web Usage Mining System Using Page Scroll*

IL Kim¹, Bong-Joon Choi, and Kyoo-Seok Park

Dept. of Computer Engineering, Kyungnam University,
Masan, Kyongnam, Korea
{clinicagent, sizzler}@korea.com,
kspark@kyungnam.ac.kr

Abstract. A web browser of a limited size has difficulty in expressing on a screen information about goods like an Internet shopping mall. Page scrolling is used to overcome such a limitation in expression. For a web page using page scrolling, it is impossible to use click-stream based analysis in analyzing interest for each area by page scrolling. In this study, a web-using mining system is presented, designed, and implemented using page scrolling to track the position of the scroll bar and movements of the window cursor regularly within a window browser for real-time transfer to a mining server and to analyze user's interest by using information received from the analysis of the visual perception area of the web page.

1 Introduction

A lot of methods including log analysis based web data mining, eye tracking, and mouse tracking are being used to evaluate interest in web pages.

A series of processes for collecting, accumulating, and analyzing data to evaluate interest require enormous capital in constructing a relevant system. Unfortunately, additional human resources and time have been necessary in collecting and accumulating data efficiently through the system constructed. In particular, there are many researches in web data mining based on log analysis, which provides convenience in information collection and includes usage information for all visitors. For an Internet shopping mall, it is difficult to express all information about goods through a web browser of a limited size.

To overcome such a limitation, page scrolling is used to identify it; in this case, however, the existing log based analysis may not be useful in analyzing interest in information a user wants.

Based on user interface environment, a web is not real space that users can feel directly with their hands but virtual one that they may feel indirectly through an input device such as a keyboard or a mouse. Therefore, it can be said that actual interaction between interface and a user occurs through an input device of PC.

In this paper, we present a web usage mining model using page scrolling to collect the position of the scroll bar of a web browser and movements of a window cursor

* This research has been funded by the Kyungnam University Masan, Korea (2005).

regularly, transfer the results to the mining server in real time, and analyze the visual recognition area of the relevant web page and captured images and collected data through the mining server. This paper has the following construction. Relevant researches in Chapter 2 consider how to segment pages based on visual recognition and analyze the recognition rate by web page areas and web usage mining; Chapter 3 designs this web usage mining system using page scrolling. Chapter 4 implements the web usage mining system using page scrolling; Chapter 5 draws conclusions and presents subjects for a future study.

2 Related Work

2.1 Web Usage Mining

Visitor search behaviors are recorded in a web server log file, along with information on user IP address, date and time of accessing a web page, how to request, URL of the page accessed, protocol being used in transferring data, status codes, the number of bytes transferred, and so on[4].

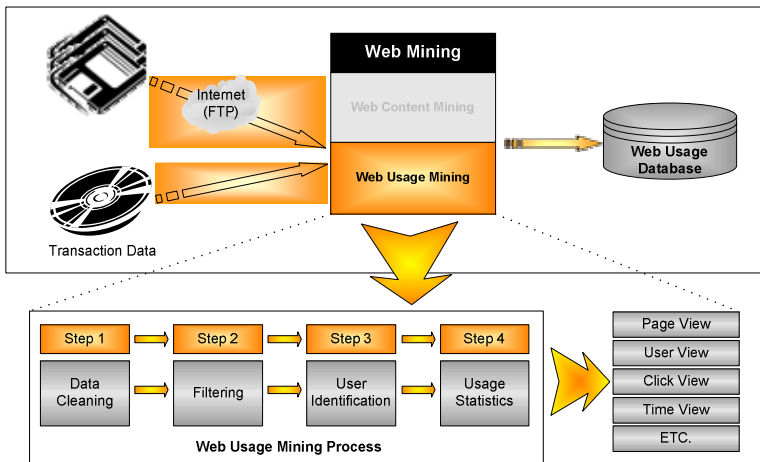


Fig. 1. Web Usage Mining Process

Figure 1 shows web mining processing for user behaviors using log files.

In a data cleaning process, information on visitor behaviors recorded in a log file was parsed to extract information such as IP address, time of connection, and requested pages. Filtering aims to remove information unnecessary for visitor search behaviors, such as image, by using the information cleaned.

User identification aims to track accurate information on visits by using information about a visitor's IP address, the amount of time for maintaining session, and the browser being used and that about log-in. Statistical visitor information, such as

statistical visit date and time, the number of visits, the revisit rate, the browser being used, and OS being used, was extracted and analyzed from multiple viewpoints of page, user, click-stream, and time series[2].

2.2 Recognition of Common Areas in a Web Page Using Visual Information

Figure 2 shows the areas segmented by Milos Kovacevic to designate an interest area and analyze the recognition rate by web page areas: H (Header) for 200 pixels at the top of the web page, F (Footer) for 150 pixels at its bottom, LM (Left Menu) for 15 percent on the left, RM (Right Menu) for 15 percent on the right, and C (Center) for the remaining area[3].

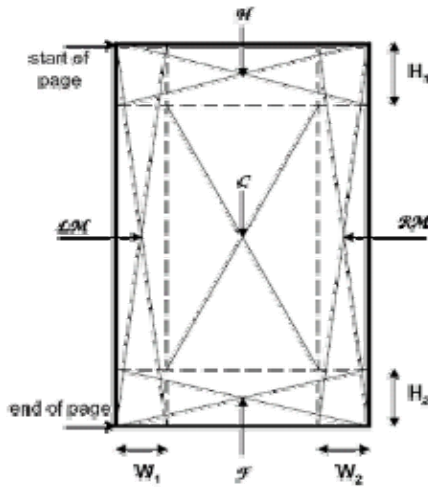


Fig. 2. Position of areas of interest in a page

Table 1 shows the results from the test Milos Kovacevic implemented for the recognition rate by interest areas: 59 percent for H, 70 percent for F, 79 percent for LM, and 81 percent for RM. Thus, the recognition rate was low at the top and bottom of the web page and there was no significant difference in the rate between LM and RM.

Table 1. Recognition rate by interest areas

	H	F	LM	RM	Overall
Not recognized	25	13	6	5	3
Bad	16	17	15	14	24
Good	10	15	3	2	50
Excellent	49	55	76	79	23

2.3 Vision-Based Page Segmentation

People use a web browser to explore a web page, which is provided in two-dimensional expression of many visual blocks segmented by lines, blanks, image, color, and so on. As a page segmentation method based on visual recognition, which was presented by Deng C., VIPS simulates how people understand web page layout through their visual recognition capacity, and uses a document object model (DOM) structure and visual information repetitively to extract visual blocks, ultimately detecting visual segmentation elements, constructing a content structure, and thus extracting a content structure based on visual recognition[5, 8].

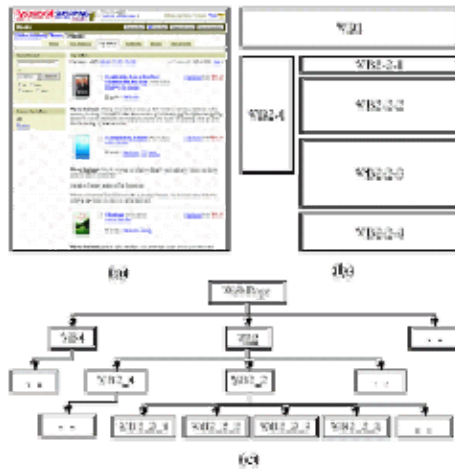


Fig. 3. The layout structure and vision-based content structure of an example page

Figure 3 shows a content structure based on visual recognition for a sample page, detecting visual blocks as in Figure 3(b) and expressing the content structure as in Figure 3(c), thus reflecting the semantic structure of the page[5].

3 Web Usage Mining System Using Page Scroll

3.1 Web Usage Mining System Using Page Scroll

A web site visually provides various multimedia contents (web contents), such as text, image, audio, and moving pictures, which are inserted in a web page as in Figure 4. The monitor being most frequently used now has the resolution of 1024×768 pixels; by using this monitor to execute a web browser, the maximum 995×606 pixel web page can be expressed on the web browser. In Figure 4, a 788×1375 pixel web page is actually shown; here, the browser, which is 995 pixels in width, is enough to express 788 pixel information, thus showing no horizontal scroll bar but a vertical scroll bar is shown to express the remaining information as it is 606 pixels in length and not enough to express 1375 pixel information[8].



Fig. 4. Exposure of web page

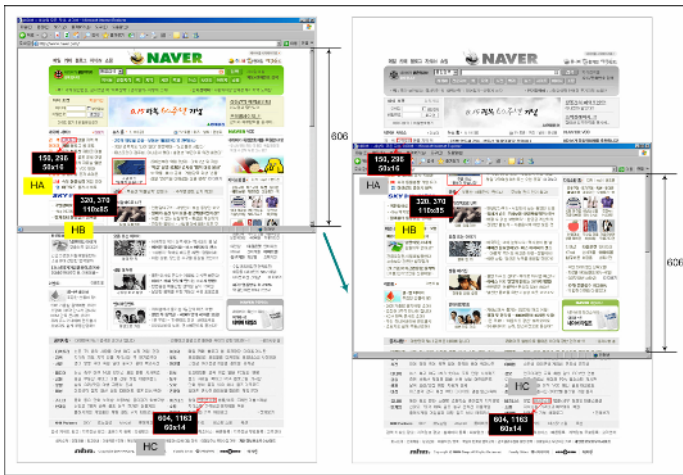


Fig. 5. Exposure or non-exposure of information on a web page

Figure 5 shows exposure or non-exposure of information provided on a web page by the scroll bar of the web browser; with HA, HB, and HC for expression areas of hyperlink included in a web page, the first scene had HA and HB exposed but HC unexposed while the second scene had HB exposed only partially but HA and HC unexposed.

Therefore, it is necessary to analyze the exposure and recognition rate for each web page area by the position of the vertical scroll bar.

This web usage mining system using page scrolling is composed of a vision-based usage mining (VUM) server for performing mining and a user activity collector (UAC) for collecting web user activities as in Figure 6. The VUM server has the functions of visually analyzing a web page, or the target of mining, and of analyzing information on user activities collected via UAC.

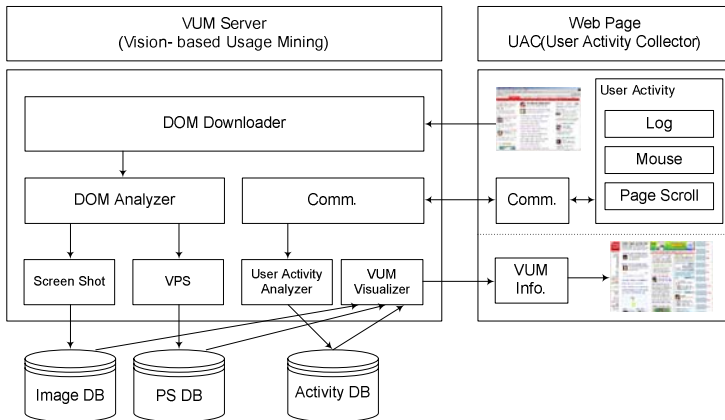


Fig. 6. Web Usage Mining System Using Page Scroll

The process of visually analyzing a web page, or the target of mining, is as follows. First, it downloads a web page, expresses it visually in DOM, and then analyzes information on the position and size of visual expression of web contents included in the web page by the DOM analyzer in pixels. With the analysis of information on the position and size, it generates an area segmented visually by vision-based page segmentation (VPS), generates image for web screen and areas through screen capture, and then inserts UAC into the web page. UAC downloaded in the web browser collects information on a web page, a window cursor, and user activities including page scrolling regularly and transfers it to the VUM server through a communication module.

A user activity analyzer (UAA) in the VUM server analyzes information on web page log and user activities and stores it in database.

The VUM visualizer visualizes information on visual analysis and user activities and provides it in the web page mode.

3.2 Usage Information Collection and Analysis

This usage information collection and analysis system cannot operate by the existing usage information collection method, or web server log file analysis, or by the log information collection method using java script, or simple click-stream. In addition to information on click-stream, it is therefore necessary to collect information on user behaviors such as the position of the window cursor and that of the scroll bar of the web browser and send it to the analysis system for analysis. Figure 7 shows the work flow for collecting and analyzing user information.

User information collection consists of two stages according to the properties of the web.

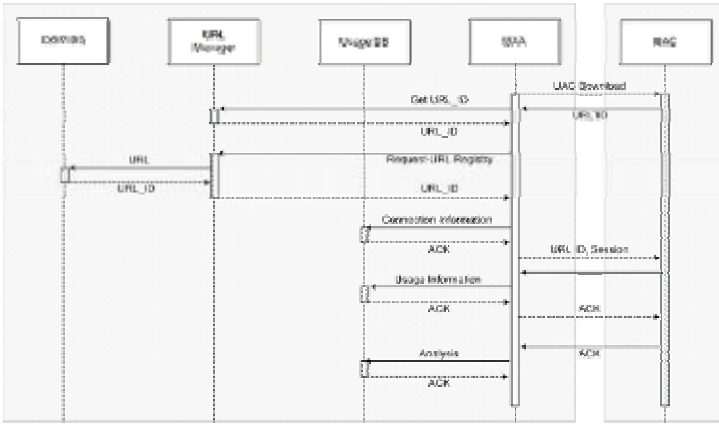


Fig. 7. Work-flow for collecting and analyzing user information

At the first stage, when a user connects a web page, the user information collection module inserted in the web page is executed, consequently sending information on web page connection and collecting that on the usage type. After receiving information on web page connection, the usage information analyzer analyzes the information, stores it in usage database, and assigns URL ID and a session to it. Table 2 shows information on web page connection to transfer; Table 3 shows log data transferred. At the second stage, information on the usage type is collected and transferred at the designated sampling interval. After receiving information on the usage type, the usage information analyzer analyzes the information and stores it in the usage database.

Table 2. Information on web page connection to transfer

	Type	Example
IP	String	127.0.0.1
URL	String	/Interest/49.html
Referrer URL	String	/Interest/Interest.htm
Time	Date	2005-6-15/13-57-7.858
Time Zone	Integer	-9
Screen Resolution(Width)	Integer	1280
Screen Resolution(Height)	Integer	1024
Browser Size(Width)	Integer	1272
Browser Size(Height)	Integer	915
Colors	Integer	16
Etc.	String	cookie=y,java=y,history=0

Table 3. Example of log data

```
url=/Interest/49.html,referrer=http://www.eyerank.com/Interest/Interest.htm,time=2005-6-15/13-57-7.858,zone=-9,sw=1280,sh=1024,bw=1272,bh=915,color=16,cookie=y,java=y,history=0
```

Table 4 shows the collected information on the usage type; Table 5 shows the transferred information on the usage type. The sampling interval of 0.1 second was used in collecting information on the usage type. In transferring usage type information being collected every 0.1 second by the usage information analyzer, a package of 10 or 20 sampling data is transferred due to a great amount of traffic.

Table 4. Usage Data Type

	type	ex.
URL ID	Integer	1
Sampling ID	Integer	1
Scroll Position of Browser	Integer	240
Cursor Position of Window(X)	Integer	449
Cursor Position of Window(Y)	Integer	340

Table 5. Example of usage type information

```
url=0&MT=T1S0X449Y340T2S0X449Y340T3S0X449Y340T4S0X449Y340T5S0X449Y340T6S0X449Y340T7S0X449Y340T8S0X449Y340T9S0X449Y340T10S0X449Y340
```

4 Implementation

This web usage mining system using page scrolling used 0.1 second, or a half of the optimum interval of 0.2 to 0.3 second being used by L. Granka's eye tracking analysis[6], as the interval for collecting information on user activities, and its implementation environment is as shown in the following table.

Table 6. H/W Environment

	OS	CPU	RAM	HDD	
H/W #1	Windows 2003 Server	P-IV 3.6GHzx2	6GB	74GBx4 (RAID 0+1)	DB-Server (MySQL 4.0)
H/W #2	Windows 2003 Server	P-IV 3.6GHzx2	6GB	74GBx2	Web-Server (IIS 6.0)
H/W #3	Windows XP Professional	P-IV 3.0GHzx1	1.5GB	120GB	Client

In this study, we designed and implemented a system to analyze visual recognition areas of a web page and to collect the position of the scroll bar of the web browser and that of the window cursor and a mining system to analyze the results. Figure 8 shows the results of collecting and analyzing 957,103 pieces of user behavior information on

22,199 page views for a user who connected a web page. Exposure time was analyzed in seconds per vertical pixel, with the maximum exposure area around 391 pixels, which was exposed for 21,717 seconds; the average click rate was analyzed by classifying the Y position, among hyperlink exposure positions, in 100 pixels. The exposure time for an area included in the first scene of the web browser is relatively longer than that for an area included in the second scene; the closer to the bottom, the shorter exposure time; and the click rate is also proportional to exposure time.

And the analysis of information on user activities through page scrolling makes it possible to make detailed exposure analysis on the web page; it is therefore easy to determine what area of the page is most exposed to a user. Figure 9 shows the results



Fig. 8. Exposure time and Click-Through



Fig. 9. Interest on visually segmented areas

from the analysis of interest through the analysis of exposure time and that of window cursor activities on visually segmented areas.

5 Conclusion

In this study, we designed and implemented a web usage mining system using page scrolling to collect the position of the scroll bar of a web browser and movements of a window cursor regularly, transfer the results to the mining server in real time, and analyze the visual recognition area of the relevant web page and captured images and collected data through the mining server. Many existing data collection and analysis methods are based on frequency using page view, Hits, algorithms, and so on. Based on simple click events that occur in a web browser, these methods have a limitation of analyzing records on a user's information reference.

To overcome such a limitation for the existing analysis methods, this system discovered user activities within a web browser, used the position of page scrolling and that of the cursor to measure interest in a web page, used information on scrolling in a long page and that on window cursor coordinates not used for web usage mining, and thus could analyze the user's interest in the web page accurately. The web usage mining system using page scrolling should be applied to Internet shopping malls to standardize the techniques of analyzing interest in goods, along with further researches in a web-based business process.

References

1. Yang, T. and Zhang, H., HTML Page Analysis Based on Visual Cues, In 6th International Conference on Document Analysis and Recognition(ICDAR 2001), Seattle, Washington, USA, 2001.
2. Chang-Doo Lee, Bong-Jun Choi, Zoo Gang, IL Kim, Kyoo-Seok Park, "A Study on Detection Technique of Bookmarking using Favicon in Web Browser", Proceedings of International Conference on East-Asian Language Processing and Internet Information Technology 2002, EALPIIT2002, Korea Information Processing Society, pp.427-433, 2002.01.
3. Milos Kovacevic, Michelangelo Diligenti, Macro Gori, Marco Maggini, Veljko Milutinovic, "Reconition of Common Areas in a Web page Using Visual Information: a possible application in a page classification", Proceedings of the 2002 IEEE International Conference on Data Mining (ICDM 2002), pp. 250-257, 2002
4. Youn-Hong Jung, iL Kim, Kyoo-Seok Park, Design and Implementation of an Interestingness Analysis System for Web Personalization & Customization, Journal of Korea Multimedia Society, Vol. 6, No. 4, July 2003, 707-713.
5. D. Cai, S. Yu, J. -R. Wen, and W. -Y. Ma, VIPS: a vision-based page segmentation algorithm, Microsoft Technical Report, MSR_TR-2003-79, 2003.
6. L. Granka, T. Joachims, and G. Gay, Eye-Tracking Analysis of User Behavior in WWW-Search, Poster Abstract, Proceedings of the Conference on Research and Development in Information Retrieval (SIGIR), 2004.
7. Bong-Joon Choi, IL Kim, Yong-Won Shin, Kwang-Hyung Kim, Kyoo-Seok Park: A Study of Link-Competition in a Hyperlinked Environment. International Conference on Internet Computing 2004: 339-344
8. IL Kim, Kyoo-Seok Park, "Vision Based Web Usage Mining", Proceedings of The 2005 International Symposium on Multimedia Applications in Edutainment(MAEDU2005), pp.18-21, 2005.

A Security Architecture for Adapting Multiple Access Control Models to Operating Systems^{*}

Jung-Sun Kim¹, SeungYong Lee², Minsoo Kim³,
Jae-Hyun Seo³, and Bong-Nam Noh^{1,**}

¹ Dept. of Computer Science, Chonnam National University, Korea

² Linux Security Research Center, Chonnam National University, Korea

³ Dept. of Information Security, Mokpo National University, Korea
{cybersun, birch}@lsrc.jnu.ac.kr,
{phoenix, jhseo}@mokpo.ac.kr, bbong@jnu.ac.kr

Abstract. In this paper, we propose a new security architecture for adapting multiple access control models to operating systems. As adding a virtual access control system to a proposed security architecture, various access control models such as MAC, DAC, and RBAC are applied to secure operating systems easily. Also, the proposed was designed to overcome the deficiencies of access control in standard operating systems, makes secure OS more available by combining access control models, and apply them to secure OS in runtime.

1 Introduction

We can approach individual's computer and network that is linked in all over the world and use information everywhere at home or office at any time by fast development of computer technology recently. Sensitive data is opened to a lot of unauthorized users or disclosed in open state in attack by development of technology. Security technology of firewall, intrusion detection system and encryption mechanism etc. was developed for safe sharing of information and safe protection of information, and these protected network or servers' information. However, it is difficult to cope with latent security vulnerability such as application bug and insider's attack and authorization abuse and misuse, because these security technology operates in application level. Also, it has fundamental limit that does not protect oneself if system is hacked. Therefore, new security technology such as secure operating system needs to solve these problems.

Secure operating system is implementation of TCB (Trusted Computing Base) that supports security function of authentication and encryption etc. to protect system from illegal activity caused by security vulnerability in operating system. Secure kernel that offers base of secure operating system is implementation of reference monitor and it offers access control. Access control is process that decides whether access that

^{*} This work was supported (in part) by the Ministry of Information & Communications, Korea, under the Information Technology Research Center (ITRC) Support Program.

^{**} Correspondent author.

happened within system is suitable or not. Reference monitor at access occurrence judges whether access decision is right to security rule drawing necessary information from subject and object [9,10]. Security policy for access control is MAC (Mandatory Access Control), DAC (Discretionary Access Control), RBAC (Role Based Access Control) [2] etc., and those are used to be standard that classifies secure operating system by its properties. Research about access control security architecture of secure operating system has been developed to maximize efficiency of access control by separating policy enforcement part and policy. Also, access control security architecture of secure operating system has characteristics of kernel independence of access control that separates access control function from kernel and flexibility of access control that can apply various access control models.

In this paper, we propose a new access control security architecture which is added virtual access control system so that it can apply various access control policy and can support flexibility and kernel independence of access control between physical kernel and logical access control policy. Therefore, the proposed security architecture can apply new access control policy as well as well-known access control policy such as MAC, DAC and RBAC to security kernel easily, and offers advantage that can change access control policy or replace it dynamically.

2 Related Work

Research about security architecture for access control has been studied for a long time based on reference monitor and was applied to many Secure or Trusted Operating Systems. This section describes work specifically related to generic access control frameworks.

The challenge of providing a highly general access control framework has been previously explored in the Generalized Framework for Access Control (GFAC)[8] and the Flask architecture[7]. These two architecture have been implemented as patches for Linux kernel by the RSBAC[3] and the SELinux[4,11] projects. The Medusa DS9[12] project has developed its own general access control framework and implemented it in Linux. Domain and Type Enforcement (DTE) provides support for configurable security policies, and has also been implemented in Linux[5]. The LOMAC[6] project has implemented a form of mandatory access control based on the Low Water-Mark model in a Linux loadable kernel module. The Linux Security Module (LSM)[1] project has been created to develop a common set of kernel hooks that can support the needs of all of the Linux security projects.

As LSM seeks to support a broad range of existing Linux security projects, it does not provide particular access control architecture such as Flask or the GFAC to support the greatest flexibility. And LOMAC was not designed to provide flexibility in its support for security policies. The Flask architecture and the GFAC separate policy including decision from enforcement and can support a variety of security policies. Also, the Medusa DS9 project is similar to SELinux and RSBAC at a high level in that it is also developing a kernel access control architecture that separates policy from enforcement.

3 The Proposed Access Control Security Architecture

In this chapter, we explain an access control security structure added VACS (Virtual Access Control System). The main aim for the proposed was to produce a flexible and effective access control system by adding some special mechanism for existing Linux access control mechanisms. To achieve this goal, we make VACS which is similar to VFS (Virtual File System). Therefore, it enables a policy administrator to apply access control models quickly and simply in underlying systems as the VFS does. And, the proposed security architecture supports dynamic policy loading and changes as VACS addresses atomic policy changes between several well-known or new security models such as MAC, DAC and RBAC.

3.1 The Proposed Security Architecture

The proposed is consisted of 3 components of SA (Security Agent), SM (Security Manger) and SCM (Security Control Mediator) as in Figure 1. SA is a module which requests policy decision and enforces policy as its decision. SM decides an access decision about request from SA. And SCM analyzes and controls the access result and it logs an event. This architecture permits a clear distinction between components that make decisions and enforce them. SA acts independently of SM that makes decisions, and loaded access control mechanisms can use the underlying infrastructure.

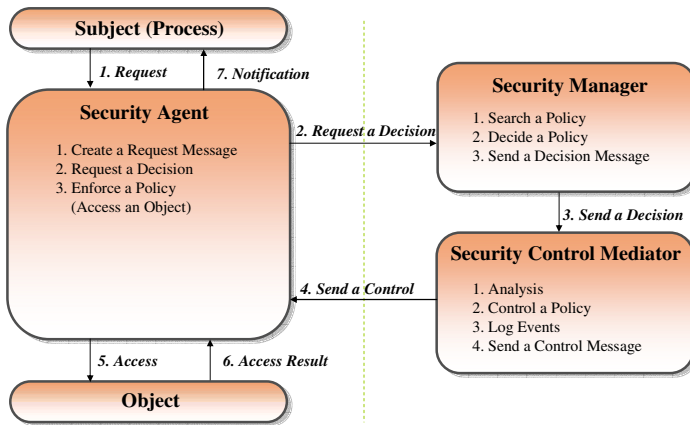


Fig. 1. The Proposed Security Architecture for Access Control

The proposed uses basic security context which is represented by subject, object and action's triple like $\langle S, O, A \rangle$ to identify access request and make decisions about it. Subjects are the users and the processes within a computer system, and objects are many kinds of entities which are represented as files particularly directories, devices, memory and others. Also, subjects and processes can serve as objects. The actions are operations that subjects perform upon objects according to the type of objects. For an example, a subject can perform *append*, *create*, *execute* operations on file objects.

Access control processing of the proposed involves a number of steps as follows: (1) The subject calls a system function to request access to an object. Then, SA gets some system information, such as the user ID, the process ID, the action type, and ID of the target object, and makes the Request Message which is consisted of basic security context before calling the decision module. (2) SA requests decision to SM about the request. Then, SM searches the proper access control mechanisms and makes a decision to that request. (3) SM sends a decision to SCM. Then, SCM analyses the decision and other related information, and it controls the invoking process if needed. And then, it logs some events and makes the control message including decision. (4) SCM sends a control messages to SA. Then SA enforces the decision according to the control message. (5) If the control message includes grant then SA accesses the object, if not returns an access error to the process. (6) SA receives an access result from the object. (7) And then, SA passes the result and control back to the invoking process.

3.2 Security Agent

SA requests decision to SM about access from the subject and performs action for object according to access control results from SCM. As in Figure 2 this module has 3 functions such as *ContextMaker*, *RequestRM* and *ReceiveCM*. *ContextMaker* identifies subject, object and action, and it makes request message including the basic security context like $RM(Subject, Object, Aaction)$. After making a request message, *RequestRM* sends it to SM. And then *ReceiveCM* waits the control message including decision and control information from SCM. Finally, in case of granted SA enforces the decision by accessing the object and notifies the access result to the invoking process. If not, it stops system call and passes control back to the invoking process.

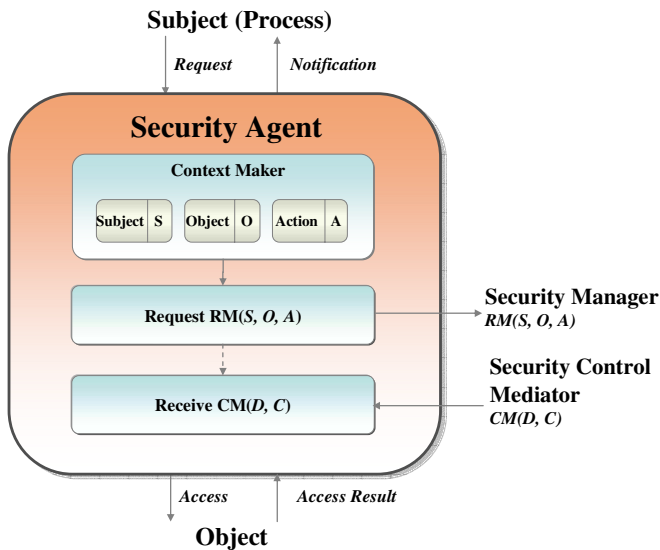


Fig. 2. The Architecture of Security Agent

3.3 Security Manager

SM makes decisions about access requests according to decisions of access control mechanisms which are loaded as loadable kernel modules by policy administrator. After making a decision, SM passes the result to SCM for next processing. This module is consisted of two parts, which are VACS (Virtual Access Control System) Layer and *SendDM* function as in Figure 3. VACS Layer receives the Request Message and searches proper access control mechanism from registered access control mechanisms. And then, it makes a decision with selected access control mechanisms. The decision has three types of values such grant, deny and undefined. After making a Decision Message including decision and other information, *SendDM* sends it to SCM. Decision Message is consisted of basic security context from Request Message, access decision information, and policy information obtained from access control mechanism, and it is represented by *DM* (*Subject, Object, Action, Decision, Policy*).

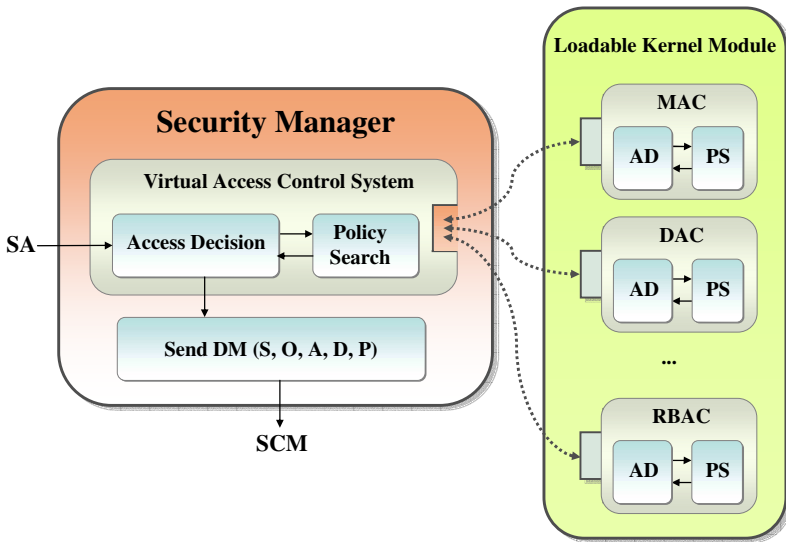


Fig. 3. The Architecture of Security Manager

The VACS is an abstraction of an access control implementation. It provides a consistent interface to multiple access control mechanisms such as MAC, DAC and RBAC. This consistent interface allows the user to view the access control mechanism on the running system as a single entity even when the access decision is made up of a number of diverse access control mechanisms.

The process between VACS and access control mechanisms is as follows. First, access control models are implemented to LKM (Loadable Kernel Modules) which are loaded by policy administrator in runtime. As in Figure 3, MAC module, DAC module and RBAC module are loaded. And then, they are used and managed with VACS interfaces which are shown in Table 1. Kernel achieves access control service through the VACS interfaces such as *access_decision*, *policy_search* and others

corresponding to each access control mechanism's implemented functions at access control service requested. However, because VACS does not support the function of verifying the loaded kernel module, policy administrator must be careful in loading the access control mechanisms.

Table 1. Interfaces of the Virtual Access Control System

API's Name	Description
register_vacs	registers access control mechanism to kernel
unregister_vacs	unregisters access control mechanism from kernel
init_vacs	initializes the data structure of VACS
get_vacs	gets the pointer of register access control mechanism
set_vacs	sets the current access control mechanism
init_policy	initializes the data structure of access control mechanism
release_policy	releases the data structure of access control mechanism
access_decision	makes a decision about access request
policy_search	searches the policy about access request
get_sscontext	gets the security context of a subject
get_oscontext	gets the security context of a object
set_policy	sets the policy of access control mechanism
get_policy	gets the policy of access control mechanism

The VACS has some data structures such as `vacs_policy_list`, `vacs_current_policy`, `vacs_policy_count` and other variables. Also, it includes principal data types such as `vacs_policy_list_t`, `vacs_policy_t`, `vacs_policy_ops_t`, etc. Examples of some data structures and `access_decision` interface are follows.

Examples of `vacs_policy_ops_t`, `vacs_policy_t` data structure, and `access_decision` interface

```

struct vacs_policy_ops_t {
    int      (*init_policy) (void);
    int      (*release_policy) (void);
    decision_t (*access_decision) (struct rm_t *rm);
    ...
};
struct vacs_policy_t {
    int      id;
    char      name[MAX_POLICY_NAME];
    struct vacs_policy_ops_t *ops;
    ...
};
decision_t access_decision(struct rm_t *rm){
    decision_t decision = D_GRANT;
    struct policy_t *policy = vacs_policy_list;
    while(policy != NULL){
        decision &= policy->ops->access_decision(rm);
        policy = policy->next;
    }
    return decision;
}

```

The following example is an `access_decision` function for MAC access control mechanism which is implemented to LKM. The *dominates* function is the implementation of relation *dom* (\leq) defined in MAC. Subject can read object if and only if subject dominates object, and subject can write object if and only if subject is dominated by object. Before making a decision, *verify* function checks whether basic security context is valid or not. Then, it checks the relation *dom* between subject and object. Logical operation is mapped to defined system call in `action_map` function.

Example of an Access Decision function for MAC access control mechanism

```

decision_t access_decision(struct rm_t *rm)
{
    decision_t d = D_DENY;
    if(!verify(rm->s, rm->o, rm->a)) return(D_UNDEFINED);
    if(dominates(rm->s, rm->o)&& action_map(rm->a, READ))
        return(D_GRANT);
    if(dominates(rm->o, rm->s)&& action_map(rm->a, WRITE))
        return(D_GRANT);
    return d;
}
    
```

3.4 Security Control Mediator

SCM analyzes and controls the decision of SM, and it consists of *Controller*, *Analyzer*, *Logger* and *SendCM* as in Figure 4. *Analyzer* analyzes related information to subject, object and action and judges whether SM’s decision is valid or not. *Controller* controls related process and user according to the result of *Analyzer*, and creates a control message *CM(Decision, Control)*. *Logger* logs some information such as access request time, subject, object, action, process, decision, control, policy etc. according to it’s configuration for administrators. *SendCM* sends the control message to SA.

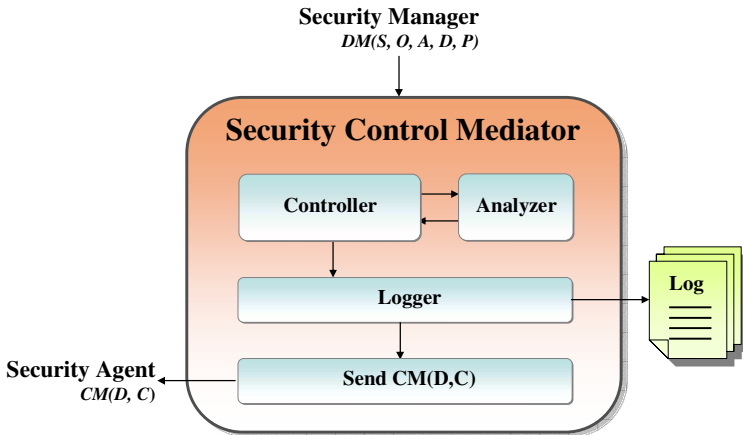


Fig. 4. The Architecture of Security Control Mediator

4 Experiments

In this chapter we explain experiment results of performance and stability tests in the Linux system where the proposed security architecture is implemented. The performance analysis is achieved by the lmbench tools[14], and the stability analysis is taken by the LTP (Linux Test Project) tools[13]. We compare the performance and stability of the base Linux with those of a system where the proposed security architecture is implemented.

Our experiment system equips Intel Xeon™ CPU 3.06 GHz, 1 GB RAM memory, 512KB cache and Fast Ethernet, and the kernel has been patched to kernel 2.6.13 version. The performance experiment measures bandwidth and latency rate of processes, memory, files and network. And the stability experiment tests the stability of system calls and kernel modules.

4.1 Performance Results with the Lmbench Tools

The performance experiment results by the lmbench tools are shown in Table 2 and Table 3. Table 2 shows the performance degradation of 0.14% ~ 36.09% according to the experiment comparing the base Linux with the proposed security architecture. The whole performance is not deteriorated in case of the PIPE's latency rate that shows the biggest overhead. However it shows the overhead of 1.39% ~ 58.88% in case of applying policies in the proposed security architecture. The most degradation occurs in processing policy mechanisms implemented by Linux kernel modules.

Table 2. Performance Results of lmbench system call tests (μ s)

Test items	Base 2.6.13	Proposed Arch.	Proposed + MAC	Proposed + RBAC	Proposed + MAC + RBAC
Simple syscall	0.1314	0.1321	0.1336	0.1371	0.1434
Simple stat	1.7653	1.7684	1.8588	1.8700	1.9893
Simple open/close	2.1328	2.3645	2.6520	2.5278	2.9055
Select on 10 fd's	0.6675	0.6684	0.6768	0.6695	0.6942
Select on 10 tcp fd's	0.7089	0.7206	0.7366	0.7208	0.7418
Signal handler overhead	1.6052	1.6577	1.6931	1.6261	1.7328
Protection fault	0.6766	0.6844	0.6865	0.6852	0.7166
Pipe latency	4.9534	6.7415	7.6765	7.5030	7.8703
Process fork + exit	182.6	198.6	218.2	202.4	220.6
Process fork + execve	586.2	601.6	739.8	675.2	743.8
Process fork + /bin/sh -c	1761	1795	2138	1956	2149
File/usr/tmp/XXX (KB/s)	49589	48300	49882	49257	49075

In case of executing /bin/sh, the proposed architecture shows the overhead of 1.93% compared with base 2.6.13. In case of applying MAC, RBAC and MAC+RBAC, it shows the overhead of 21.41%, 11.08% and 22.05% respectively.

Table 3. Performance Results of lmbench context switch tests (number of process = 64, μ s)

Test target	OK	4K	8K	16K	32K	64K
Base kernel 2.6.13	4.10	7.00	9.01	12.41	18.21	30.44
Proposed	4.15	7.01	9.19	12.44	18.36	30.45
Proposed + MAC	4.78	7.45	9.85	12.90	19.26	31.65
Proposed + RBAC	4.81	7.58	9.88	12.97	19.43	31.71
Proposed + MAC + RBAC	4.98	7.64	9.98	13.21	19.56	31.86

Table 3 shows context switch results measured according to data segment sizes. It shows that the context switch overhead of the proposed architecture is less than about 2% compared with base kernel 2.6.13. And it shows that the proposed architecture applied with MAC+RBAC has the overhead of 4.6% ~ 21.4%.

4.2 Stability Results with the LTP Tools

We have tested the stability of the proposed architecture with test items such as file system, direct IO, memory administration, IPC durability and scheduler durability using the LTP tools. The LTP tools pass absurd argument values to relevant system calls and decide whether a test success or not with suitable error codes and return values. Table 4 describes stability results using LTP tools. The values of relevant items in Table 4 mean failure rate (the number of failed tests/ the number of total tests). And, the number of total tests is different according to Linux kernel version.

Table 4. Stability Results of LTP tests

Test items	Base kernel 2.6.13	Proposed	Proposed +MAC	Proposed +RBAC	Proposed +MAC+RBAC
system call	3/687	3/687	3/687	3/687	3/687
NPTL	0/1	0/1	0/1	0/1	0/1
file system	0/55	0/55	0/55	0/55	0/55
direct IO	0/28	0/28	0/28	0/28	0/28
memory	0/21	0/21	0/21	0/21	0/21
pipe	0/8	0/8	0/8	0/8	0/8
scheduler	0/3	0/3	0/3	0/3	0/3
pty	0/3	0/3	0/3	0/3	0/3
math library	0/10	0/10	0/10	0/10	0/10

Table 4 shows that 3 system call tests fail among 687 on the target systems such as base kernel, the proposed architecture and others. The 3 failed system calls are madivse02, ioperm02 and fcntl23, and the number followed in the system call names corresponds to the number of test that was achieved by the LTP tools. For the example of the fcntl23 system call test, it means that the 23rd fcntl system call test of the LTP tools fails on the test target systems. Therefore, the proposed security architecture needs supplementation about failed system calls such as madivse, ioperm and

fcntl, but it guarantees the stability of other system calls equally with base Linux kernel 2.6.13. Also, the proposed architecture guarantees the stability of kernel modules because it passes all basis kernel module tests that correspond to file system, memory administration and scheduler durability test etc.

5 Conclusions

In this paper, we have explained a security architecture that has been studied until recently, and we present a new access control architecture for applying multiple access control models to secure operating systems. Also, we have designed VACS and applied it to the proposed security architecture. Therefore, the proposed access control architecture separates policies from enforcement and provides the flexibility of access control. The VACS layer abstracts the features of most access control mechanisms, so that other parts of the kernel can access the access control mechanism without knowing what kind of access control mechanism is in use. Finally, it demonstrates that the performance overhead and the stability of the proposed security architecture are suitable to be used in Linux systems.

References

1. Morris, J., Smalley, S., Korah-Hartman, G.: Linux Security Modules: General Security Support for the Linux Kernel. USENIX Security Symposium, Aug (2002).
2. Ferraiolo, D. F., Sandhu, R., Gavrilu, S., Kuhn, D. R., and Chandramouli, R.: Proposed Standard for Role-Based Access Control. ACM Transactions on Information and Systems Security, Vol. 4. No. 3. Aug (2001) 224-274
3. Ott, A.: The Rule Set Based Access Control (RSBAC) Linux Kernel Security Extension. 8th Int. Linux Kongress, Enschede (2001)
4. Loscocco, P., and Smalley, S.: Integrating Flexible Support for Security Policies into the Linux Operating System. In Proceedings of the FREENIX Track 2001 USENIX Annual Tec. Conference, June (2001)
5. Hallyn, S. and Kearns, P.: Domain and Type Enforcement for Linux. In Proceedings of the 4th Annual Linux Showcase and Conference, Oct (2000)
6. Fraser, T.: LOMAC - Low Water-Mark Integrity Protection for COTS Environments. In Proceedings of the 2000 IEEE Symposium on Security and Privacy, May (2000)
7. Spencer, R., Smalley, S., Loscocco, P., Hibler, M., Andersen, D. and Lepreau, J.: The Flask Security Architecture: System Support for Diverse Security Policies. In Proceedings of the Eight USENIX Security Symposium, Aug (1999) 123-139
8. Abrams, M. D., Eggers, K. W., Padula, L. J. L. and Olson, I. M.: A Generalized Framework for Access Control: An Informal Description. In Proceedings of the Thirteenth National Computer Security Conference, Oct (1990) 135-143
9. Pfleeger, C. P., Pfleeger, S. L.: Security in Computing. PRENTICE HALL (2002)
10. Gollmann, D.: Computer Security. John Wiley & SONS (1999)
11. Mcgarty, B.: SELINUX: NSA's Open Source Security Enhanced Linux. O'REILLY (2005)
12. Medusa DS9 project. <http://medusa.fornax.org>
13. The Linux Test Project. <http://ltp.sourceforge.net>
14. The Lmbench Project. <http://lmbench.sourceforge.net>

Rotor Design for the Performance Optimization of Canard Rotor/Wing Aircraft

Jae-Woo Lee^{1*}, Kwon-Su Jeon², Min-Ji Kim², Yung-Hwan Byun³,
Chang J. Kim⁴, and Yung H. Yu³

¹ Professor, Department of Aerospace Engineering
jwlee@konkuk.ac.kr

² Graduate Research Assistant, Department of Aerospace Engineering

³ Professor, Department of Aerospace Engineering

⁴ Assistant Professor, Department of Aerospace Engineering,

Next generation Innovative Technology Research Institute,
Konkuk University, Seoul 143-701, Republic of Korea

Abstract. A program for the sizing and performance analysis is developed for Canard Rotor/Wing (CRW) aircraft which operates in both fixed wing and rotary wing modes. The system characteristics, such as reaction driven rotor system, are analyzed first and then the system design process is defined. The developed program is verified for both fixed wing and rotary wing modes with existing aircraft data and the design optimization process is performed for a reconnaissance mission. For the CRW aircraft optimization for both fixed wing and rotary wing modes, a multi-objective function is constructed using weighting factors. For several design cases with different weighting factors and several design constraints, the optimization analysis is performed and improved results are derived.

1 Introduction

Compared with a conventional aircraft, a rotorcraft can take-off and land vertically, and has unique hovering capability. These capabilities make various missions possible, including reconnaissance, rescue, close battlefield combat, and transportation. Meanwhile, the flight speed is severely limited, due to shock waves at the advancing side and dynamic stall at the retreating side. To resolve this issue, various design concepts, including Canard Rotor/Wing (CRW) aircraft, have been studied [1-5].

CRW aircraft is a combined concept of rotorcraft and fixed wing aircraft. For take-off and landing, the wing rotates as a reaction-driven rotor as a tip-jet rotor concept, and during a cruise mode, the rotor is stopped and acts as a fixed-wing of aircraft, and the jet is used for the required propulsive force [4].

Conventional design analysis programs for either fixed wing aircraft or rotorcraft are not adequate and difficult to apply for the design of CRW aircraft which has multi flight modes. Therefore, in this study, a dedicated CRW sizing and performance code is developed by investigating the existing design methods and the performance

* Corresponding author.

programs for both fixed wing aircraft and rotorcraft. Then the optimal CRW configuration will be studied for the minimum gross weight, while satisfying the specified missions and design requirements of the both fixed wing and rotary wing modes.

2 CRW Design Program Development

2.1 CRW Sizing and Performance Analysis Process

Figure 1 shows the CRW sizing and performance analysis program process. Basic design variables for the configuration and the mission profile are specified first. By initially guessing the gross weight, the payload, and the disk loading, the sizing of the CRW is performed to obtain the required power (which can derive the required engine size) and basic configuration parameters. From the mission profile and the required fuel weight, the empty weight and the gross weight are estimated. This process is repeated until the available fuel weight and the required fuel weight converge within given error tolerance. From the sizing process, the engine size and the rotor configuration are derived, which satisfy both rotorcraft and fixed wing modes.

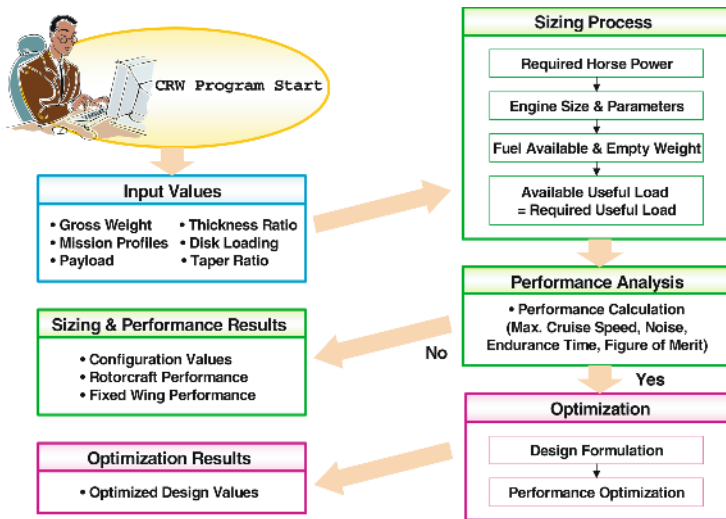


Fig. 1. The CRW sizing and performance analysis program process

Using the sizing results, the performance of both the fixed wing and rotary wing modes are estimated. At the rotary wing mode, the available power is obtained through the reaction driven rotor analysis, and the Figure of Merit, the acceleration, and the rotor noise are estimated. At the fixed wing mode, the required power, the available power, and the power curve are obtained first, and then the range, the endurance, the rate of climb, the maximum/minimum level flight speed, and the absolute/service ceiling are calculated sequentially.

The estimated performance results are either utilized as the aircraft performance at the certain design point, or connected to the optimization module to derive the objective function and the design constraints according to the values of the design variables.

2.2 CRW Design Program Structure

The entire structure of the CRW design program has three modules: a sizing module, a performance analysis module, and an optimization module.

In the sizing module, the aircraft configuration analysis, the mission analysis, the propulsion system, the engine/rotor library routines are included. From the specified configuration inputs and mission requirements, appropriate vehicle sizing results are obtained.

The performance analysis module has two sub-modules; a fixed wing mode and a rotary wing module. The rotary wing module can estimate the aerodynamic characteristics and the performance of rotorcraft. In the fixed wing mode, the aerodynamic analysis routine and the performance routine of fixed wing aircraft are provided. The lifting line theory and semi-empirical drag estimation methods are used for the aerodynamic analysis. The range, the endurance, the rate of climb, the maximum/minimum level flight speed, and the absolute/service ceiling are obtained in the performance analysis routine.

In the optimization module, the optimization formulation selects the design variables, the design space, the objective function and the design constraints first, and then the values of the objective function and the design constraints, and their sensitivities are calculated through the design optimization process, according to the variation of the design variables. In this study, the gradient-based optimization – tool is the DOT (Design Optimization Tools) version 4.0 [7] – methods are utilized, which can get the optimal solution relatively fast and effectively.

2.3 Verification of the CRW Design Program

2.3.1 Verification in the Rotary Wing Mode

To validate the accuracy of the rotary wing mode of the program, MD 500E (Fig. 2) configuration and mission data are specified and the performance analysis has been performed. It has the simple mission; Take off and climb for 3 min. → Cruise for 140 min. at 5000 ft → Descent and landing for 3 min. → Taxi for 2 min. The total endurance time is 2.5 hrs and the total range is 337 nm. Table 1 shows the MD 500E specifications, and Table 1 shows the verification results and the errors of MD 500E.

The calculated results are compared with the actual MD 500E performance data, which show a maximum error of 8.5 % of the service ceiling estimation and a 2.9 % error of the empty weight. The major source of these errors is the uncertainty of the mission profile of MD 500E, and the current mission and performance evaluation conditions are simplified, because of the lack of the exact mission data. By considering the accuracy of the weight and performance results, the current program for the rotary wing mode is acceptable for the design and analysis of CRW aircraft.



Fig. 2. MD 500E light commercial helicopter

Table 1. Specifications of MD 500E [8]

Engine	One Allison 250-C20B
Dimensions	
Main Rotor Diameter	26.4 ft
Height	9.5 ft
Length	30.8 ft
Width	6.2 ft

Table 2. Weight and performance results and errors of MD 500E

		Specification	Results	Error (%)
Weight	Gross Weight (lbs)	3000	3000	-
	Empty Weight (lbs)	1481.5	1438.5	2.9
	Fuel Weight (lbs)	403.4	398.5	1.2
Performance	Max. Cruise Speed (knots)	134.4	134.8	0.2
	Max. Range (nm)	239	242.5	1.4
	Max. Endurance (hr)	2.8	2.79	0.3
	Service Ceiling (ft)	16000	17500	8.5

2.3.2 Verification in the Fixed Wing Mode

For the verification in the fixed wing mode, Cessna 182 Skylane (Fig. 3) is selected and the performance analysis results are compared. Table 3 shows the specification of Skylane.



Fig. 3. Cessna 182 Skylane

Table 3. Specification of Skylane 182 [9]

Engine	One Continental O-470-R	
Dimensions	Wing Span	36 ft
	Height	9.1 ft
	Length	25.1 ft
	Wing Area	174 ft ²
Weight	Gross Weight	2550 lbs
	Empty Weight	1621 lbs

Table 4. Weight and performance results and errors of the Cessna 182 Skylane

Performance	Specification	Results	Error (%)
Max. Cruise Speed (knots)	140	138.7	0.9
Rate of Climb (SL) (ft/min)	1200	1224	1.9
Service Ceiling (ft)	20000	19159	4.3

Table 4 shows the percent errors of the fixed wing mode performance: less than a 1 % error for the maximum cruise speed, 1.9 % for the rate of climb at sea level, and 4.3 % for the service ceiling. With these, the current CRW design program seems to be adequate for the fixed wing mode performance estimation.

3 CRW Rotor Design and Optimization

3.1 Mission Profile Definition

The CRW aircraft is assumed to operate in Korea, the total mission distance to be 220 nm, and the loitering time to be 2 hrs. The cruise altitude and cruise speed are assumed to be 30000 ft and 110kt, respectively. Figure 4 shows the mission profile of the CRW aircraft.

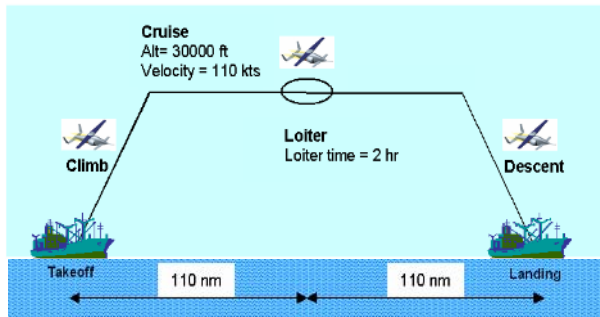


Fig. 4. CRW mission profile

3.2 Sensitivity Analysis for the Design Optimization Formulation

Because the CRW operates both in rotary wing and fixed wing modes, the design factors for the dual modes must be considered. In this study, four design variables are selected for formulating an optimization problem and the sensitivity analysis has been performed for five performance parameters: a gross weight, Figure of Merit, noise level at hover condition, a maximum cruise speed, and total endurance time. The baseline configuration for the sensitivity analysis is Boeing’s X-50 Dragonfly [5]. The range of the design variables are given at Table 5.

Table 5. Candidate design variables for the sensitivity analysis

Variables	Definition	Unit	Lower Bound	Baseline	Upper Bound
X_1	Taper Ratio	Non-Dim.	0.70	0.88	1.00
X_2	Thickness Ratio	Non-Dim.	0.15	0.22	0.30
X_3	Disk Loading	lbs/ ft ²	10.00	13.30	15.00
X_4	Rotor Tip Speed	ft/sec	600.00	725.00	800.00

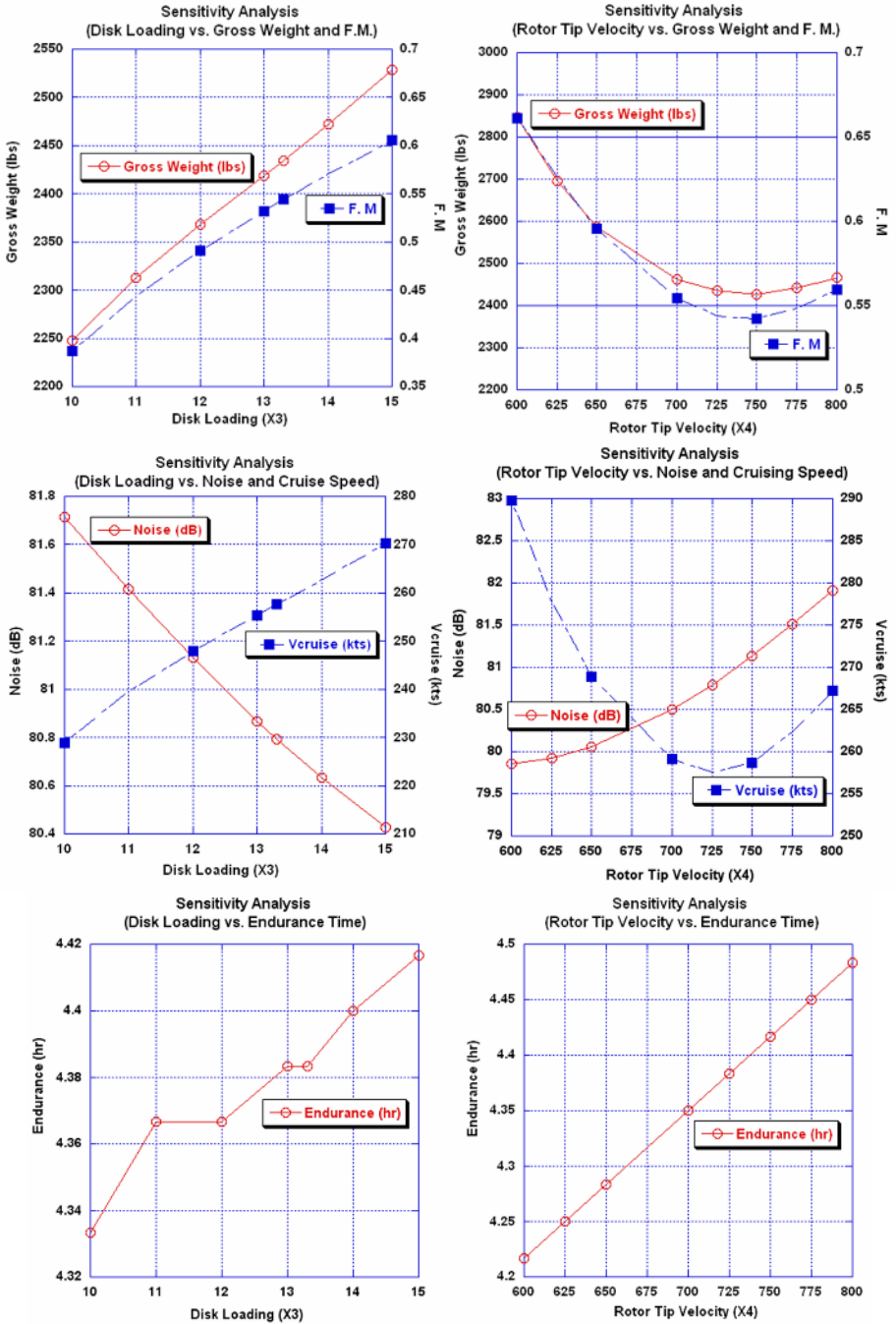


Fig. 5. Sensitivity analysis results for X_3 and X_4

Figure 5 shows the results of the sensitivity analysis for the design variables X_3 and X_4 . From the sensitivity analysis, it is verified that all four design variables considerably affect the five performance parameters. In fixed wing mode, the taper ratio does not have strong influence on the endurance. Meanwhile, the rotor tip speed, which is a key factor in rotary wing mode, has strong effects on the performance of the fixed wing mode. To attain the target rotor tip speed, the rotor blade (or wing span) geometry and the engine size are the important design parameters.

3.3 Design Formulation and the Optimization Results

From the sensitivity analysis the CRW optimization problem is formulated as follows:

Multi-objective optimization with 3 design constraints. Four design variables are selected and the range of the design variables (design space) is the same as that of the sensitivity analysis. Three design constraints are selected: By considering the stealth capability during the reconnaissance mission, the hover noise constraint of 81 dB (approx. average automobile noise level) at rotary wing mode is imposed. Second constraint is imposed to achieve the high cruise speed requirement at fixed wing mode. The maximum cruising velocity requirement of 250 knots came from the Korean smart UAV project [10]. From the sensitivity analysis, the total endurance time of 4.3 hrs from takeoff to landing is feasible, hence it is imposed as last design constraint.

$$\begin{aligned}
 &\text{Minimize } f = \omega \cdot F.M._{baseline} / F.M. + (1 - \omega) \cdot GW / GW_{baseline} & (1) \\
 &\text{Subject to } g(1) = \text{Noise}(@ \text{Hover}) \leq 81dB \\
 &\quad g(2) = V_{\max_cruise} \geq 250knots \\
 &\quad g(3) = \text{Time}(@ \text{Endurance}) \geq 4.3hrs & (2) \\
 &\text{Design Variables } X_i : i=1, \dots, 4 \\
 &\quad 0.7 \leq X_1 \leq 1.0 : \text{Rotor Taper Ratio (Non-dim.)} \\
 &\quad 0.15 \leq X_2 \leq 0.30 : \text{Thickness Ratio (Non-dim.)} \\
 &\quad 10.0 \leq X_3 \leq 15.0 : \text{Disk Loading (lbs/ft}^2\text{)} \\
 &\quad 650 \leq X_4 \leq 800 : \text{Rotor Tip Speed (ft/sec)} & (3) \\
 &\text{Where } \omega : \text{Weighting Factor} \quad F.M. : \text{Figure of Merit} \\
 &\quad GW : \text{Gross Weight (lbs)} \quad V_{\max_cruise} : \text{Maximum Cruise Speed (knots)}
 \end{aligned}$$

As the objective function, the key performance parameters of the both rotary wing and fixed wing modes are combined like the multi-objective function with a weighting factor: maximization of the Figure of Merit in the rotary wing mode and minimization of the gross weight in the fixed wing mode. These parameters are normalized using the performance values of the baseline configuration. Six different design problems with different weighting factor values from 0.0 to 0.5 are formulated and optimized. Weighting factors are the direct representation of the objective function, hence the design results can be very different. When ω is zero, the design becomes a single objective function optimization problem, which considers only the gross weight. When ω equals to 0.5, the Figure of Merit and the gross weight are considered with

the same importance. With three design constraints, the design results are summarized at Table 6. As can be seen at this Table, the influence of the weighting factor is not strong when the additional constraints for the objective function are specified.

Multi-objective optimization with 5 design constraints. Basically the design formulation is same as above. Two additional design constraints are included to guarantee the improvement of both the Figure of Merit and the gross weight compared with the baseline after the design optimization

$$g(4) = F.M. \geq F.M._{baseline} \quad g(5) = GW \leq GW_{baseline} \quad (4)$$

Table 6. CRW optimization results (with 3 constraints)

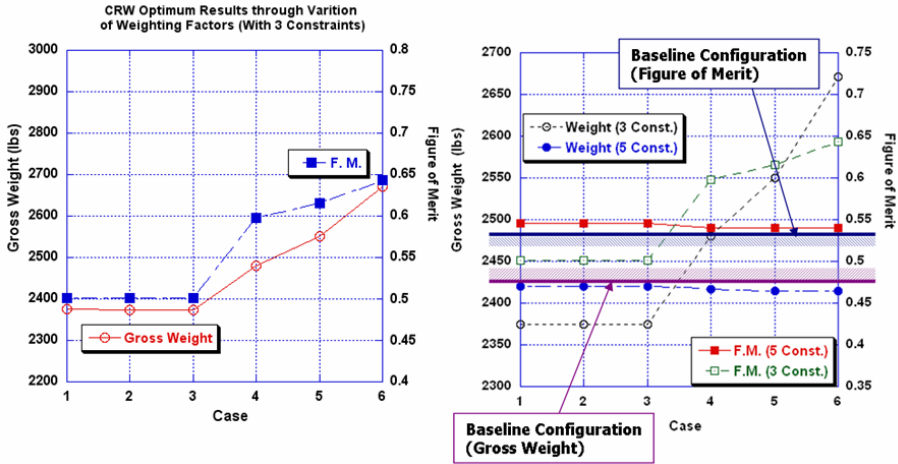
ω	Baseline	(0.0,1.0)	(0.1,0.9)	(0.2, 0.8)	(0.3, 0.7)	(0.4, 0.6)	(0.5, 0.5)
X_1	0.8800	0.7031	0.7028	0.7023	0.7000	0.7000	0.7076
X_2	0.2200	0.2541	0.2538	0.2533	0.2074	0.2527	0.2605
X_3	13.3000	12.1137	12.1214	12.1264	15.0000	15.0000	14.7698
X_4	725.00	692.33	692.70	692.80	741.59	687.32	644.18
Object Func.	-	0.9811	0.9902	0.9994	0.9865	0.9839	0.9736
GW (lbs)	2434.00	2374.70	2374.40	2374.10	2479.90	2550.40	2671.50
F.M.	0.5441	0.5008	0.5009	0.5010	0.5974	0.6154	0.6436
Noise (dB)	80.7948	80.7864	80.7879	80.7867	80.7000	80.0864	79.7947
V_{max} (knots)	257.60	249.02	249.03	249.03	268.89	271.69	280.11
Endure. (hr)	4.3833	4.3167	4.3167	4.3167	4.4333	4.3500	4.2833

Table 7. CRW optimization results (with 5 constraints)

ω	Baseline	(0.0,1.0)	(0.1,0.9)	(0.2, 0.8)	(0.3, 0.7)	(0.4, 0.6)	(0.5, 0.5)
X_1	0.8800	0.7000	0.7000	0.7000	0.7000	0.7000	0.7001
X_2	0.2200	0.2287	0.2287	0.2285	0.2407	0.2406	0.2410
X_3	13.3000	13.2950	13.2958	13.2861	13.0884	13.0872	13.1851
X_4	725.00	697.09	697.09	696.95	694.80	694.68	700.92
Object Func.	-	0.9999	0.9986	0.9973	0.9986	0.9986	0.9974
GW (lbs)	2434.00	2420.10	2420.20	2419.70	2416.80	2416.90	2414.90
F.M.	0.5441	0.5460	0.5460	0.5457	0.5395	0.5395	0.5406
Noise (dB)	80.7948	80.5165	80.5164	80.5169	80.5505	80.5494	80.5974
V_{max} (knots)	257.60	256.82	256.82	256.76	255.78	255.78	256.09
Endure. (hr)	4.3833	4.3500	4.3500	4.3500	4.3500	4.3500	4.3500

With five design constraints, the design results are summarized at Table 7. As can be seen at this Table, the influence of the weighting factor is also not strong when the additional constraints for the objective function are specified.

Figure 6(a) shows the optimized results with three design constraints for several different weight factors, and Figure 6(b) is the case with five design constraints. The upper boundary of Figure 6(b) denotes the value of baseline Figure of Merit and the lower boundary shows the value of the baseline gross weight. With these design constraints, both the gross weight and the Figure of Merit have values near the baseline for different values of the weighting factors.



(a) F.M and GW with 3 constraints (b) Comparison of 3 and 5 constraints

Fig. 6. Optimization results with different design constraints

4 Conclusions

In this study, the sizing and performance analysis program is developed for CRW aircraft that operates in both fixed wing and rotary wing modes. The system operating characteristics are analyzed first and then the system design process is defined. The CRW optimization module is also included for the CRW system optimization. The developed program is verified for both fixed wing and rotary wing modes with the existing aircraft data and the design optimization formulation is made to perform the reconnaissance mission. For the CRW aircraft optimization, both the fixed wing and rotary wing modes must be considered at the same time, therefore a multi-objective function is constructed using weighting factors. For several design cases with different weighting factors and several design constraints, the optimization is performed and improved design results are derived. The program developed for the CRW type aircraft will have more accurate design results with the development of refined analysis modules.

Acknowledgement

This work was supported by “the International R&D Center Recruit Project ”of Ministry of Science and Technology in 2005.

References

1. Smith, C.R., "Hot Cycle Rotor/Wing Composite Research Aircraft," Hughes Tool Company, Aircraft Division, Culver City, CA, (1968)
2. Sutton, J.G., and Sawicki, A.C., "X-wing Application", Presentation submitted to the Sixth Annual Northeast Regional Conference of the Society of Allied Weight Engineers, Smithtown, New York, (1985)
3. Schwartz, A.W., and Rogers, E.O., "Tipjet VLAR UAV: Technology Development Status," Paper presented at the 20th Annual Symposium and Exhibit of the Association for Unmanned Vehicle Systems, Washington, D.C. (1993)
4. Clark A. M., and Barvara. J. V., "The Canard Rotor Wing (CRW) Aircraft – A New Way To Fly," AIAA Symposium, (2003)
5. Ramon. L., "X-50 Dragonfly Poised For Takeoff," *Aerospace America*, (2002)
6. "Helicopter-Plane Hybrid Ready For Take-Off," www.newscientist.com, (2002)
7. *DOT Users Manual*, Vanderplaats Research & Development, Inc., (1995)
8. *Jane's All the Worlds Aircraft 1995-96*, Jane's Information Group, (1995) 594-595
9. *Jane's All the Worlds Aircraft 1991-92*, Jane's Information Group, (1995) 385,
10. Chul-Ho Lim(KARI), "Overview of the SMART UAV PROGRAM," Euro-UVS 2003 Conference. (2003)

Process Decomposition and Choreography for Distributed Scientific Workflow Enactment

Jae-Yoon Jung¹, Wookey Lee^{2,*}, and Suk-Ho Kang³

¹ Dept. of Technology Management, Eindhoven University of Technology,
PO Box 513, 5600 MB Eindhoven, The Netherlands

J.Y.Jung@tue.nl

² Dept. of Computer Science, Sungkyul University,
147-2, Anyang-dong, Manan-gu, Anyang-city, Kyonggi-do, Republic of Korea

Tel: +82-31-467-8174

wook@sungkyul.edu

³ Dept. of Industrial Engineering, Seoul National University,
San 56-1, Shillim-dong, Kwanak-gu, Seoul, Republic of Korea

shkang@snu.ac.kr

Abstract. Workflow is introduced to automate and control processes in scientific problem-solving environments. Scientific workflow requires detailed design of data sets and systematic description of interaction between activities and data sets, for it is more data-initiative than business workflow. Furthermore, scientific workflow needs high-performance computing facilities that are often scattered in distributed environments. As a result, distributed workflow enactment can enhance the performance and efficiency of scientific problem-solving. This research proposed a methodology of distributed process enactment for data-initiative scientific workflow. This methodology extracts an activity-based process model for general workflow systems, and then decomposes the model to distributed workflow processes and choreographs them with process interoperability messages. This research will facilitate to design complicated data-initiative workflow models and realize distributed workflow enactment for scientific problem-solving.

1 Introduction

Modern scientific problems often require quite complex experiments with large data sets. Scientific workflow is a useful tool that enables to design, manage, and execute the procedural problem-solving process. Workflow was originally a technology to automate and control business processes. However, it has been adapted for effective and efficient scientific problem-solving in various fields, such as GIS [2], bioinformatics [9] or physics computing [5]. It is called scientific workflow. Scientific workflow requires detailed modeling of data sets and systematic description of interaction between activities and data sets, for scientific experiments are usually more data-oriented than business activities. Early researches focused on data and resource management by database management

* Corresponding author.

systems [1] [7] or decision support systems [10]. Furthermore, scientific workflow usually needs high-performance computing facilities that are often scattered in distributed environments such as laboratories or gene banks [11]. As a result, distributed workflow enactment can enhance the performance and efficiency of scientific problem-solving. So, recent researches are also investigating the issue on distributed execution of scientific workflow and shared data storages [12] [13]. In addition, advanced information technology, such as web service and grid computing, urged the issue [3] [4]. This paper also treats a methodology of distributed scientific workflow. However, we do not focus on the technology, but the deployment to workflow enactment.

Workflow technology has evolved and various products are provided by many vendors. They support design tools and enactment engines for general workflow models. However, they have not been sufficient to investigate how to design data-initiative models for scientific experiments and transform them to process models for general workflow systems in distributed environments.

In this research, we proposed data-initiative modeling for scientific workflow by using object-process modeling. The model enables apparent experiment design as it provides object-oriented data modeling and data-initiative process modeling. The OPM model is used to extract activity-based process models, which is acceptable to workflow process design in general workflow systems. Next, the models are transformed to distributed workflow designs with process interoperability messages. The distributed workflow models can interact with each other in run-time through workflow servers that may administrate the facilities participating in scientific problem-solving environments. Our paper supplies a guideline of how to design and apply workflow models in distributed scientific problem-solving environments. This research on data-initiative design and distributed execution help to implement effectively distributed workflow for scientific problem-solving, especially in high-performance computing environments.

2 Scientific Workflow Modeling in OPM

Object Process Modeling (OPM) is an integrated modeling approach that designs objects and processes in a single model to describe the structure and behavior of a system. Object and process are considered as equal significance in the modeling [8]. This paper presents a kind of OPM for scientific workflow modeling. The OPM consists of entities or links. An entity can be an object or an activity. Objects are used to design data sets in a scientific problem, while activities are used to design experiments in the problem. An activity can create or consume several objects, or transform the state of objects. On the other hand, a link can be structural or procedural. Structural links are used to represent object-oriented concepts, such as aggregation, generalization, characterization, and instantiation, while procedural links are used to describe interactions between an activity and an object, such as creation, consumption, and transformation.

Scientific workflow modeling in OPM is composed of three stages: data set, experiment, and agent modeling. In data set modeling, scientific problem

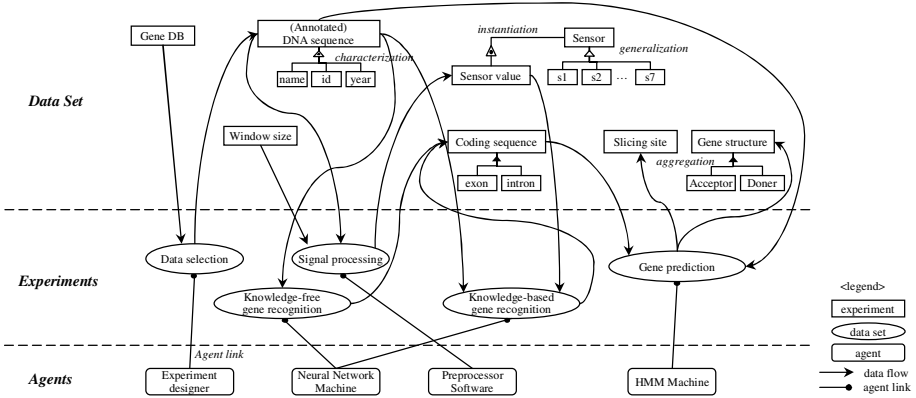


Fig. 1. Gene Identification in DNA sequences

statements are analyzed and data sets are extracted. Data sets may be expressed by the object-oriented relations, such as aggregation, generalization, characterization, and instantiation. Next, in experiment modeling, the experiments to create or consume existing data sets are described with intermediate data sets. An experiment has several input or output data sets. Finally, the agent modeling assigns each agent to each experiment. The agent can be an application or a computer program performing the experiment in distributed environments; however it must be able to be controlled by any workflow system for distributed execution and interoperability.

Figure 1 shows an example of scientific workflow modeling in OPM. The model illustrates the experiment of Gene Identification in DNA Sequences with three parts: data sets, experiments, and agents. Data sets were symbolized by rectangular boxes, and the relations of aggregation, generalization, characterization, and instantiation are discriminated by lines with solid, empty, doubled, and dotted triangles, respectively. The experiments were symbolized by ovals and connected with the input and output data sets by arrows. Finally, the agents were symbolized by rectangles and connected with their experiments by arrows with dots.

3 Scientific Workflow Process Extraction

Workflow is automated and enacted on the basis of dependencies among process activities. Workflow management systems and process modeling tools usually use an activity-based process design in directed graph because activity-based graph design is easy and apprehensive to process designers and analyzers. This section describes how process models in a graph design are extracted from the scientific OPM model. In addition, a data dependency graph guiding correlation of data sets in the experiments is also presented.

On an OPM graph, G is a set of objects O and relations R . An object is a union of data sets D , experiments E , and agents A . And, a relation R is a union of structural relation and procedural relation. To extract a workflow process, we analyze the procedural relations of a data set and an experiment. The data set and the experiment have a membership of predecessor list $\text{pred}(o)$ and successor list $\text{succ}(o)$. First, we determine the depth of the objects that will be included in the process. The procedure *Depth-counting* below is an algorithm that counts the depth of the objects on the OPM graph. We can search data sets and experiments and count their depth by traversing the procedural relation ($\text{pred}(o)$ and $\text{succ}(o)$) on the graph. As a result, the depth of data sets is odd and that of experiments is even. The procedure may call the sub-procedure *isUpper*(v, v') to avoid cycling in depth counting. The sub-procedure returns true if v' is the upper node of v , otherwise false.

```

PROCEDURE Depth-counting (in  $G$ , out ( $O$ ,  $\text{depth}(O)$ ))
  for all object  $o \in O$  do
    if ( $\text{pred}(o) = \phi$ ) then
      if ( $o \in D$ ) then  $\text{depth}(o) := 1$ ; add  $o$  in QUEUE;
      else if ( $o \in E$ ) then  $\text{depth}(o) := 2$ ; add  $o$  in QUEUE;
      end if
    next
  while ( $\text{QUEUE} \neq \phi$ ) do
    let  $v$  be the first element of QUEUE; remove  $v$  from QUEUE;
    for all  $v' \in \text{succ}(v)$  do
      if ( $\text{depth}(v')$  is null) then  $\text{depth}(v') := \text{depth}(v) + 1$ ;
      else if ( $\text{depth}(v') < \text{depth}(v) + 1$  && isUpper( $v, v'$ ) = false) then
         $\text{depth}(\text{succ}(v)) := \text{depth}(v) + 1$ ;
      if (all  $v'' \in \text{pred}(v')$  have  $\text{depth}(v'')$ ); then append  $v'$  to QUEUE;
    next
  end while
end Depth-counting

```

By using the algorithm *Depth-counting*, we can extract the objects for the workflow process and count the depth of the objects from the example of Gene Identification, as shown in Table 1.

Table 1. Depth of objects in gene identification $\text{depth}(O)$

$\text{depth}(O)$	object O
1	Gene DB, Window size
2	Data selection
3	(Annotated)DNA sequence
4	Knowledge-free gene recognition, Signal processing
5	Sensor value
6	Knowledge-based gene recognition
7	Coding sequence
8	Gene prediction
9	Slicing site, Gene structure

The extracted objects are matched to workflow activities (experiments) and their input and output data sets in the workflow process. The procedure *Workflow-generation* generates a workflow process from objects and their depths.

```

PROCEDURE Workflow-generation (in ( $O$ ,  $\text{depth}(O)$ ), out  $WF$ )
  for all object  $o \in O$  do
    if ( $\text{depth}(o)$  is odd) then
      for all  $e \in \text{succ}(o)$  do
        add  $o$  to  $\text{in}(e)$ ;
        if ( $\text{depth}(o)=1$ ) then  $\text{pred}(e) := \phi$ ;
        else append  $\text{pred}(o)$  to  $\text{pred}(e)$ ;
        append  $e$  to  $\text{succ}(e')$  and  $o$  to  $\text{out}(e')$  for all  $e' \in \text{pred}(o)$ ;
      next
      remove  $o$  from  $O$ ;
    end if
  next
end Workflow-generation
  
```

By another algorithm similar to the procedure *Workflow-generation*, a data dependency graph is also generated in order to guide the correlation of data sets in the experiments. The algorithm was left out for want of space. The extracted workflow process and the data dependency graph of the example Gene Identification is shown in Figure 2 and 3, respectively.

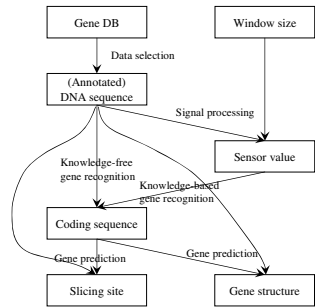
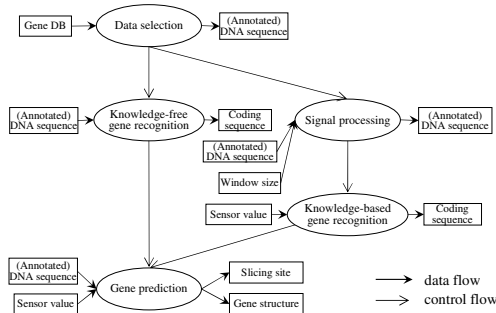


Fig. 2. Workflow process model with in/out data **Fig. 3.** Data dependency graph

4 Process Decomposition and Choreography

Scientific workflow is crucial to success in high-performance computing. And scientific problem-solving usually involves the invocation of a number and variety of analysis tools [11]. In this section, we propose a methodology of dividing and deploying a global process into distributed workflow servers. By this methodology, we can use general workflow systems for distributed execution of scientific workflows. Heterogeneous workflow systems in distributed environments can be implemented to communicate with each other by the workflow interoperability standard message Wf-XML of WfMC [6].

The procedure of distributed workflow modeling is as follows: 1) workflow server assignment to each experiment, 2) process decomposition in the same server, and 3) process choreography for distributed workflow execution. First, we should decide a workflow server for each scientific experiment. Workflow servers may be implemented for distributed laboratories or institutes with experiment equipments. The servers play a leading role in assigning and controlling the experiments in scientific problem-solving. We assumed that an experiment should be performed and controlled by only one server.

Next, the experiments that are assigned to the same workflow server are merged into several processes. This step is called process decomposition. A process will be enacted and administrated in a workflow server as a part of the scientific problem-solving. The procedure *Process-decomposition* shows an algorithm, in which activities are merged into the same process if they have dependencies with each other in a workflow server.

```

1: PROCEDURE Process-decomposition (in  $WF$ , out  $(P, M)$ )
2:   append all starting nodes to QUEUE;
3:   while (QUEUE $\neq\phi$ ) do
4:     let  $v$  be the first element of QUEUE;
5:     remove  $v$  from QUEUE;
6:     for all  $v'\in\text{pred}(v)$  do
7:       if ( $\text{svr}(v)=\text{svr}(v')$  &&  $\text{proc}(v)$  is null) then  $\text{proc}(v):=\text{proc}(v')$ ; remove
       $v'$  from STACK;
8:       else if ( $\text{svr}(v)=\text{svr}(v')$  &&  $\text{proc}(v)\neq\text{proc}(v')$ ) then append  $\text{init}(\text{proc}(v'))$ 
      to QUEUE;  $\text{proc}(i):=\text{proc}(v)$  for all  $i\in\text{init}(\text{proc}(v'))$ ; remove  $v'$  from STACK;
9:       else if ( $\text{svr}(v)\neq\text{svr}(v')$ ) then add message pairs  $(v',v)$  to  $M$ ;
10:      next
11:      for all  $l\in\text{STACK}$  do
12:        if ( $\text{svr}(v)=\text{svr}(l)$  &&  $\text{isUpper}(l,v)=\text{true}$ ) then
13:          remove  $l$  from STACK;
14:           $\text{proc}(v):=\text{proc}(l)$ ; break;
15:        next
16:        if ( $\text{proc}(v)$  is null) then
17:          create a new process  $p$ ; add  $p$  to  $P$ ;
18:           $\text{proc}(v):=p$ ; append  $v$  to  $\text{init}(p)$ ;
19:        end if
20:        append all  $v''\in\text{succ}(v)$  to QUEUE;
21:        append  $v$  to STACK;
22:      end while
23: end Process-decomposition

```

The procedure begins by appending nodes to QUEUE that is storage for breadth-first searching. The **while** statement (lines 3-22), the main part of the procedure, has three conditional statements to search nodes in QUEUE. First, in the **for** statement of lines 6-9, a node is attached to the process of its adjacent predecessor node if they have the same server (line 7). However, if the node has two or more adjacent predecessors and their processes are different with each other, then the processes are merged into one (line 8). Otherwise, i.e. if the node and its predecessor are in different servers, they are connected by message flow (line 9). Second, the **for** statement of lines 11-15 resumes the process when the server of a suspended process gets a control flow again after

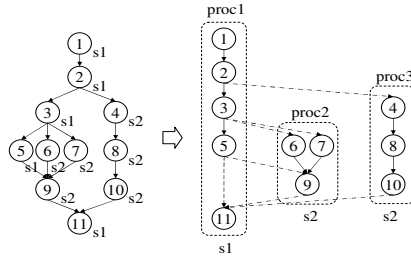


Fig. 4. Example of process decomposition

a pause during another server’s workflow execution. Third, the *if* statement of lines 16-19 creates a new process if there is no process in the node’s server or, if the process is independent of the node. Finally, in lines 20-21, the successors of the node are appended to QUEUE for recursion and the node is appended to STACK storage of the leaf nodes. The leaf node will be removed later from the list if any successor is attached to the same process.

An example of process decomposition is illustrated in Figure 4. The procedure *Process-decomposition* appends the nodes in the graph to QUEUE by breadth-first searching. The processing sequence of the nodes is 1,2,3,4,5,6,7,8,9,10,(7,9),11. Nodes 1, 4, 6, and 7 create a new process because they have different servers from their predecessors. And nodes 2, 3, 5, 8, 9, and 10 are attached to the processes of their predecessors. Note that node 9 merges the process of node 7 with that of node 6 because the two processes rendezvous at node 9. The parenthesis (7, 9) in the sequence shows backtracking to merge the two processes. Finally, node 11 is attached to the suspended process *proc1*. The process was found when any node of leaf nodes in STACK was the predecessor of the node and had the same server. As a result, the three processes on the right of Figure 4 are generated by the procedure *Process-decomposition*.

In the last step of distributed workflow modeling, the distributed processes get interconnected with each other by standard messages. This step is called process choreography. Control flow between two processes of different servers was transformed to message flow in the procedure *Process-decomposition*. Process interoperability operations are introduced to choreograph the distributed workflow processes. The operations were devised to choreograph processes in distributed environments by analyzing process interoperability patterns [6].

There are five process interoperability operations, which can accompany with five types of states. Table 2 shows the list of the operations. Two operations *Instantiate* and *Initiate* make a new invocation between two processes. And the other operations *Resume*, *Transit*, and *Synchronize* continue the invoking process in different ways. All the operations except for *Synchronize* can have five types of states: *waited*, *suspended*, *terminated*, *disconnected*, and *continued*. They represent the states of the invoking process after its invocation.

The process interoperability operations are used for decomposed workflow processes to interoperate with each other via workflow engines. The interaction

Table 2. Process interoperability operations

Operation	Description
<i>Instantiate</i>	create an instance of a process and return that instance's key
<i>Initiate</i>	find a process instance waiting after its previous activities are done
<i>Resume</i>	resume a suspended or waiting process after invocation
<i>Transit</i>	continue an on-going process after its previous activities are completed
<i>Synchronize</i>	make two process instances continue their next activities only after their appointed activities are done

types of the two processes can be summarized in the six primitive interoperability patterns in Figure 5. They are classified into three groups. Chained substitutive (CS) and chained additive (CA) patterns trigger another process's creation or enactment before the invoking processes continue or terminate, respectively. The nested synchronized (NS), nested deferred (ND), and nested parallel (NP) patterns trigger another process's execution while the invoking processes waiting, resuming, or continuing. In particular, pattern NS can be used to express an in-zooming process in OPM modeling. Finally, parallel synchronized (PS) patterns let two processes continue their enactment only after both have reached interoperability activity.

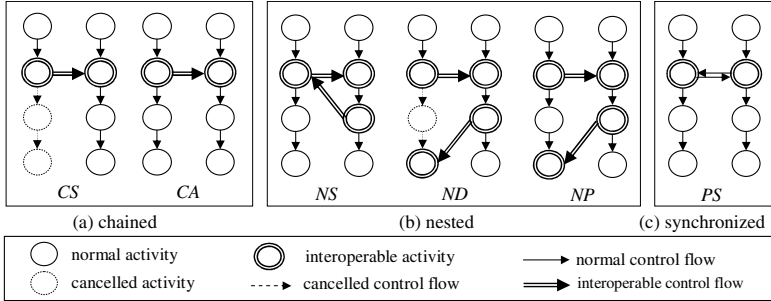


Fig. 5. Process interoperability patterns

The interoperability operation can include not only five six primitive patterns, but hybrid patterns can mix with the primitive patterns. In Figure 4, the interaction of proc1 and proc3 is pattern NP, and they are transformed into the interoperability operations *Instantiate*(state= 'continued') and *Transit*(state= 'terminated') of node pairs (2,4) and (10,11), respectively. On the other hand, the interaction of proc1 and proc3 is the hybrid pattern of two CS and a ND. The pattern can be transformed into operations two *Instantiate*(state='continued'), *Initiate*(state= 'suspended') and *Resume*(state='terminated') of node pairs (3,6), (3,7), (5,9), and (9,11). These operations will be implemented by workflow standard message Wf-XML in workflow systems.

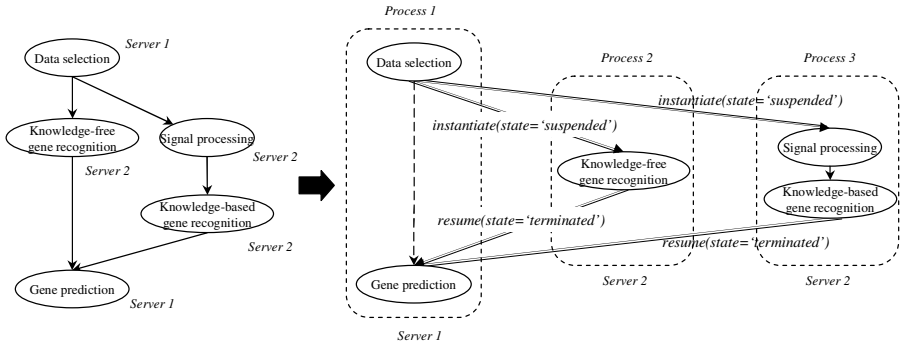


Fig. 6. Process decomposition and choreography of Gene Identification workflow

5 Distributed Scientific Workflow Enactment

Distributed workflow models with interoperability operations are implemented by using the workflow standard message Wf-XML of WfMC. Most workflow engines support the standard for workflow interoperability with other heterogeneous systems. In scientific problem-solving environments, distributed workflow systems coordinate the scattered experiment equipment in laboratories and they can interoperate with other workflow systems by the standard messages.

In the example of Gene Identification in Figure 1, experiment designer and HMM machine are controlled in Workflow server 1 and Neural network machine and Preprocessor software are done in Workflow server 2, as shown on the left of Figure 6. The result of process decomposition and choreography is shown to the right of the figure. Process1 in Server1 sends two request messages *Instantiate*(state=*'suspended'*) to Process2 and Process3 in Server2 after the experiment *'Data selection'* is done. Then, two processes return the response message *Resume*(state=*'terminated'*) after they are terminated.

Our prototype workflow system uses the XML-based process definitions, XPDL of WfMC. The definitions are designed by activity-based process modeling from the process decomposition. The system adapted Web service technology to implement the workflow interoperability standard message. The messages are transformed to SOAP-binding messages conformant to Wf-XML standard. Two interoperability operations of Figure 6 are converted to *CreateProcessInstance* and *ChangeProcessInstanceState* request messages of Wf-XML standard. They will wait for the corresponding response messages via Web service by the interchange mechanism.

6 Conclusions

Workflow facilitates scientific problem-solving that requires high performance by scattered computing equipment. Scientific workflow also needs a systematic

description of interaction between activities and data sets because it is more data-initiative than business workflow.

This paper presents a data-initiative scientific workflow modeling method and its transformation mechanism to activity-based process models for general workflow systems. Furthermore, we proposed a methodology of deploying the process model to distributed workflow environments with process interoperability messages. This work enables collaborative scientific problem-solving in distributed environments with scattered experiment equipment. This research will be helpful to implement effectively data-initiative and distributed workflow in scientific problem-solving environments.

References

1. Ailamaki, A., Ioannidis, Y.E., Livny, M.: Scientific workflow management by database management. In: Proc. Conf. on Scientific and Statistical Database Management (1998) 190–199.
2. Alonso, G. Hagen, C.: Geo-Opera: workflow concepts for spatial processes. In: Proc. Symp. Spatial Databases (1997) 82–92.
3. Altintas, I., Berkley, C., Jaeger, E., Jones, M., Ludascher, B., Kepler, S.: An extensible system for design and execution of scientific workflows. In: Proc. 16th Int'l Conf. on Scientific and Statistical Database Management (2004) 423–424.
4. Deelman, E., Blythe, J., Gil, Y., Kesselman, C., Mehta, G., Patil, S., Su, M.-H., Vahi, K.: Pegasus: Mapping Scientific Workflows onto the Grid. In: Proc. European Across Grids Conf.. LNCS. 3165 (2004) 11–20.
5. Graham, G., Evans, D., Bertram, I: McRunjob: A High Energy Physics Workflow Planner for Grid Production Processing. In: Proc. Computing in High Energy Physics (2003) 1–7
6. Jung, J., Hur, W., Kang, S., Kim, H.: Business Process Choreography for B2B Collaboration. IEEE Internet Computing 8(1) (2004) 37–45.
7. Leung, C., Lee, W.: Exploitation of Referential Integrity Constraints for Efficient Update of Data Warehouse Views, In: British Nat'l Conf. on Databases (2005) 98–110.
8. Liu, H., Gluch, D.: Conceptual modeling with the object-process methodology in software architecture. J. of Comp. in Small Colleges. 19(3), (2004) 10–21.
9. Meidanis, J., Vossen, G., Weske, M.: Using workflow management in DNA sequencing. In: Proc. IFCIS Conf. on Cooperative Information Systems. (1996)
10. Seffino, L.A., Medeiros, C.B., Rocha, J.V., Yi, B.: WOODSS - a spatial decision support system based on workflows. Decision Support Systems 27(1/2) (1999) 105–123.
11. Singh, M.P. Vouk, M.A.: Scientific Workflows, NSF Workshop on Workflow and Process Automation in Information Systems, State-of-the-art and Future Directions. (1996)
12. Vouk, M.A.: Integration of heterogeneous scientific data using workflows - a case study in bioinformatics. In: Proc. Conf. on Information Technology Interfaces. (2003) 25–28.
13. Zhang, J., Pennington, D., Michener, W.: Using Web Services and Scientific Workflow for Species Distribution Prediction Modeling. In Proc. WAIM, LNCS 3739, Springer (2005) 610–617

Adaptive Multi-carrier Direct-Sequence CDMA System Using Fast-Frequency-Hopping

Kyesan Lee and Gigan Lee

Kyunghee Univ.,
Seochunri, Kihung-eup,
Yongin-si, Gyunggi-do, 449-701, Korea
Kyesan@khu.ac.kr

Abstract. A novel adaptive Fast Frequency Hopping based MC-DS/CDMA is proposed to improve the performance in the frequency selective fading channel. The FH/MC DS-CDMA scheme achieves the diversity gain the frequency diversity gain as well as the time diversity gain. The proposed system can achieve the frequency diversity gain provided by Fast Multi-carrier hopping, and the proposed system creates the time diversity gain with maximum ratio combining (MRC) at the Rake receiver. Therefore, the performance of this Fast FH MC-DS/CDMA is improved compared to the conventional MC-CDMA in the frequency selective fading channel.

1 Introduction

From this section, input the body of your manuscript according to the constitution that you had. For detailed information for authors, please refer to [1].

Mobile communication systems are required to be sufficiently flexible to support a variety of multimedia services such as video, image, picture, and data services with high quality. A multi-carrier modulation scheme providing high data rate transmission with high frequency utilizing efficiency has been proposed for the DS/CDMA system based on Orthogonal Frequency Division Multiplexing (OFDM), which is a parallel data transmission technique. It is crucial for multi-carrier transmission to have a non frequency selective fading channel over each sub-carrier.

The OFDM DS/CDMA system is effective in providing high data rate avoiding ISI(Inter Symbol Interference) in frequency selective fading channel.

Fast frequency hopping can achieve the diversity gain using the symbol having the independent fading pattern enable to robust against Jamming compared to Slow hopping.

A novel adaptive Fast Frequency Hopping MC-DS/CDMA is proposed to improve the performance in the frequency selective fading channel. The adaptive FH/MC DS-CDMA scheme achieves the frequency diversity gain as well as the time diversity gain provided by Fast Multi-carrier hopping, and the proposed system creates the time diversity gain with maximum ratio combining (MRC) at the Rake receiver. Therefore, the performance of this Fast FH MC-DS/CDMA is improved compared to the conventional MC-CDMA in the frequency selective fading channel.

This paper is organized as follow. In section 2, we present the conventional MC-DS/CDMA system. In section 3, the detailed contents of the proposed system model are explained, and section 4 shows these simulation results, Finally, in section 5, conclusion is described.

2 Adaptive Fast FH/MC-DS-CDMA

The transmitter of the proposed adaptive fast FH/MC-DS-CDMA system is shown in Fig.1.

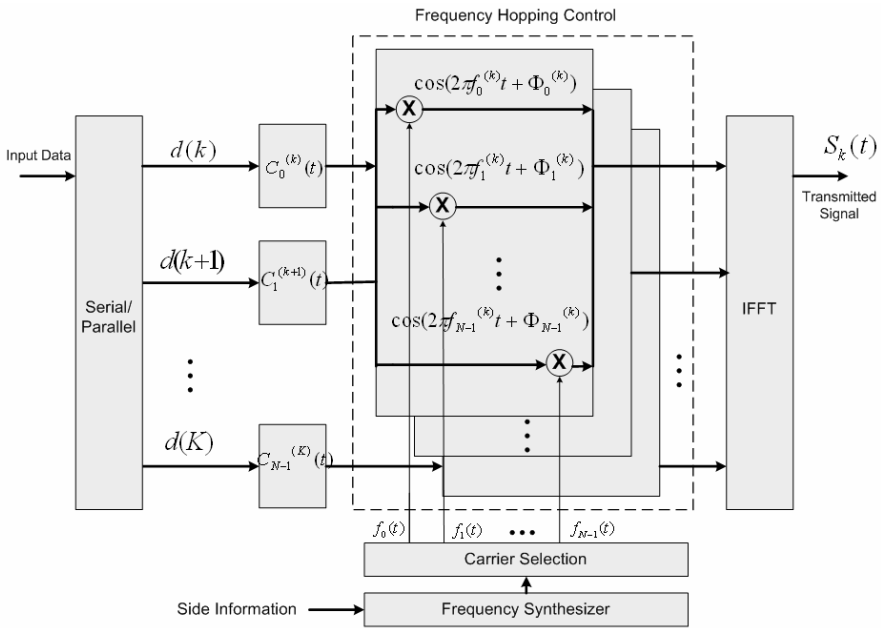


Fig. 1. The proposed fast FH/MC-DS-CDMA transmitter diagram for multiple access

The proposed system is an effective MC-DS-CDMA system involving in the fast frequency hopping. Input data is converted serial to parallel, The output of the serial-/parallel block is mapped and grouped by subcarriers. The frequency hopped signal is spreaded by PN codes. The spreading signal is hopped using a Fast hopping pattern and transmitted by each subcarriers. Each subcarrier of a user is assigned by a pseudo random spreading sequence code. The equivalent frequency hopping pattern should be used in the transmitter as well as in the receiver. IFFT(Inverse Fast Fourier Transform) is utilized for multi-carrier modulation. The output signal of the adaptive fast FH/MC-DS-CDMA transmitter is

$$S_k(t) = \sum_{U_k=0}^{U_k-1} \sqrt{2P} d_{U_k}^{(k)}(t) \cdot C_{U_k}^{9k0}(t) \cdot \cos(2\pi f_{U_k}^{(k)} t + \phi_{U_k}^{(k)}) \tag{1}$$

where the transmitted data is d and the users are U_k . The spread spectrum code is C and the transmitted power is P .

The Fig.2 shows the receiver of the proposed FH/MC-DS-CDMA system.

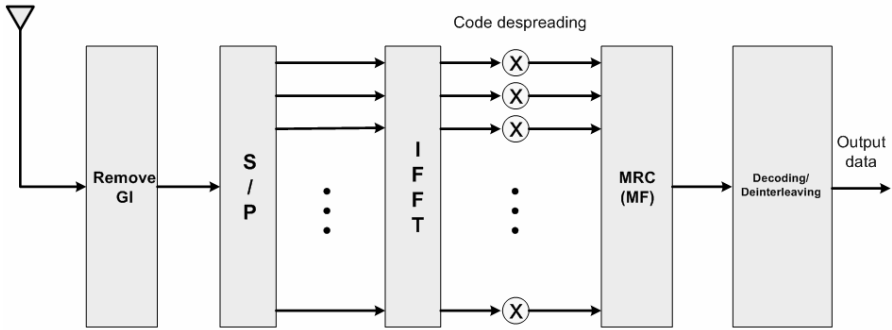


Fig. 2. Receiver System of fast FH/MC-DS-CDMA system

The receiver received the transmitted signals, which are converted from serial to parallel, and FFT is used to demodulate all the carrier. The frequency hopping pattern in the receiver is identical as one in the transmitter. The signals of the proposed FH/MC-DS-CDMA system is Maximal Ratio Combined (MRC) at a Matched Filter, it is a Rake combiner. Since the receiver has a grouping for multi-carrier with the frequency hopping pattern, The proposed FH/MC-DS-CDMA system can achieve the frequency diversity gain due to the fast frequency hopping. The hopping rate is greater than the symbol rate. In this case, the carrier frequency changes a number of times during the transmission of one symbol, so that one bit is transmitted at different frequencies. Finally, the received data is outputted after decoding and de-interleaving.

The received signal is

$$R(t) = n(t) + \sqrt{2P} \sum_{k=1}^K \sum_{U_k=0}^{U_{k-1}} \alpha_{U_k}^{(k)} d_{U_k}^{(k)} (t - \tau_k - IT) \cdot C_{U_k}^{9k0} (t - \tau_k - IT) \cdot \cos(2\pi f_{U_k}^{(k)} t + \phi_{U_k}^{(k)}). \tag{2}$$

where $n(t)$ is additive white Gaussian noise(AWGN) with two sided power spectral density of $N_0/2$, α_n^k is the path gain due to Rayleigh fading of n th subcarrier for k th user, τ_k is the propagation delay of the k th user.

The adaptive FH/MC DS-CDMA scheme achieves the frequency diversity gain as well as the time diversity gain provided by Fast Multi-carrier hopping, and the proposed system creates the time diversity gain with maximum ratio combining (MRC) at the Rake receiver. Therefore, the performance of this Fast FH MC-DS/CDMA is improved compared to the conventional MC-CDMA in the frequency selective fading channel.

3 Simulation Results and Analysis

3.1 Simulation Condition

We proposed an adaptive a fast FH/MC-DS-CDMA system and show simulation results. The performance of the proposed system was demonstrated by computer simulation in a frequency selective Raleigh fading channel. In particular, The channel model is used by 18 Rayleigh fading path model. It is the exponential decay model, 1dB decay between the 0th path and the 1st path. Also, we assume that sub-carriers, codes and bits are exactly synchronized in this simulation. The simulation Parameters shows in

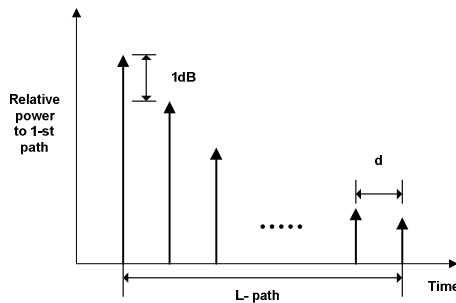


Fig. 3. Multi-path Channel model

Table 1. Simulation parameters

Number of sub-carriers	64
Short spreading code	Walsh-Hadamard code
Data modulation	BPSK
Number of (hop vs. bit)	64
Number of user	4
Spreading Factor	4
Guard interval	1/4
Noise	AWGN
Channel model	Raleigh Fading l(18 path)
Maximum Doppler frequency	5Hz

3.2 Result of the Proposed Fast FH/MC-DS/CDMA Systems

The bit error rate(BER) performance of the proposed Fast. Frequency Hopping/MC-CDMA is evaluated as a function of E_b/N_0 .

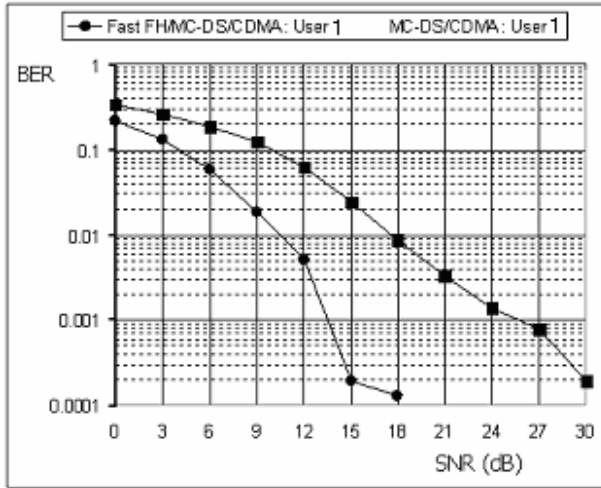


Fig. 4. BER performance of the proposed system

Fig.4 shows BER results in terms of SNR(dB) to compare between a MC-DS-CDMA system and the proposed fast FH/MC-DS-CDMA system under same channel circumstance. It is shown in Fig. 4 that the BER performance vs. E_b/N_0 in case of single user. The performance of the proposed system is about 5dB better than a MC-DS-CDMA system.

The proposed system achieves the frequency diversity gain by combining the fast hopping multi-carrier signals. The fast FH/MC-DS-CDMA, which is proposed in this paper, shows better performance due to same symbol is allocated using different frequencies, so that it achieves the frequency-time diversity.

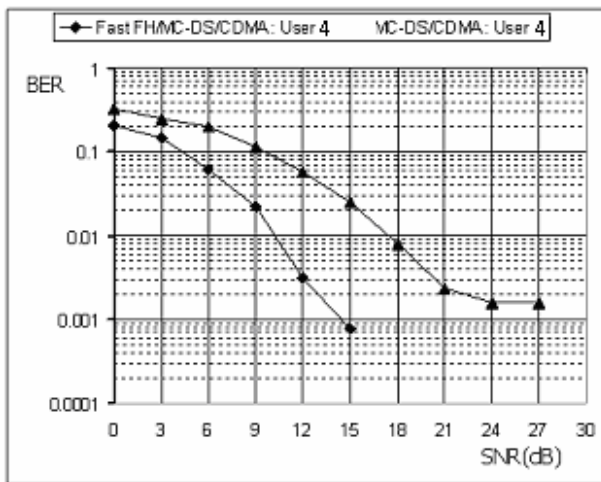


Fig. 5. BER performance of the proposed system

Fig.5 shows the results of multi-user in the frequency selective fading channel. The BER performance of the proposed system is also improved the frequency diversity gain of the fast frequency hopping with multi-carriers. In multi-user, the proposed system can achieve the frequency diversity gain with multi-carrier, because the carrier changes a number of times during the transmission of one one symbol. So that, one bit is transmitted at different frequency, results in the frequency diversity gain.

As a result, signal frequencies that are amplified at one carrier frequency are attenuated at another carrier. At the receiver, the responses at the different hopping frequencies are averaged, thus reducing the multi-path interference.

4 Conclusion

In this paper, we proposed an new adaptive FH/MC-DS-CDMA system to achieve the frequency diversity gain with multi-carrier. The simulation results showed substantially improved performance can be obtained by the proposed system compared to the conventional MC-DS/CDMA systems due to frequency diversity gain. It was verified by simulation that the proposed system with fast frequency hopping is effective and practical in the frequency selective fading channel. Therefore, the proposed system is appropriate for supporting a variety of multimedia services with high quality in the broadband wireless channel.

Acknowledgments

Insert acknowledgment, if any.

References

1. Shinsuke Hara, Ramjee Prasad.: Overview of Multicarrier CDMA, IEEE Communications Magazine December 1997
2. L.-L. Yang and L. Hanzo.: Slow Frequency- hopping Multicarrier DS-CDMA over Nakagami Multipath Fading Channels, IEEE JSAC, July 2001
3. L.-L. Yang and L. Hanzo.: Blind Joint Soft-detection Assisted Slow Frequency-Hopping Multicarrier DS-CDMA, IEEE Trans. Commun., Sept. 2000,
4. Q. Chen, E. S. Sousa, and S. Pasupathy.: Multicarrier CDMA with adaptive frequency hopping for mobile radio systems, IEEE J. Select. Areas Commun., Dec. 1996.
5. S. Kondo and L. B. Milstein.: Performance of multicarrier DS CDMA systems, IEEE Trans. Commun., Feb. 1996.
6. Lajos Hanzo, L-L. Yang, E-L. Kuan, K. Yen.: Single and Multi-Carrier DS-CDMA: Multi-User Detection, Space-Time Spreading, Synchronisation and Standards, Book, Sep. 2003, chapter1.
7. Lie-Liang Yang and Lajos Hanzo.: Multirate Transmission in Frequency-Hopping Multicarrier Direct-Sequence Code-Division Multiple Access Systems, IEEE Trans. Commun. 2001,

Object Modeling for Mapping XML Document Represented in XML-GDM to UML Class Diagram^{*}

Dae-Hyeon Park¹, Chun-Sik Yoo², Yong-Sung Kim², and Soon-Ja Yeom³

^{1,2} Division of Electronics and Information Engineering,
Chonbuk National University, 664-14 1ga Duckjin-Dong, Duckjin-Gu,
Jeonju, Jeonbuk, 561-756, Republic of Korea
³ School of Computing, University of Tasmania, Australia
empire@ms.krf.or.kr, {csyoo, yskim}@chonbuk.ac.kr,
S.Yeom@utas.edu.au

Abstract. XML has been popular as a means of sharing and distributing data due to its flexible and open architecture. XML-GL, a visual and intuitive query language for XML document, is easily used to search structures of XML documents and share information, since it represents the semantics of query and the structure of found documents visually. UML is used as a tool to analyze and design an object oriented system via defined notation and various diagrams. In this paper, we will propose a new object modeling method to map XML documents based on XML-GDM (a data model of XML-GL) to UML class diagrams. Thus, XML documents can be converted and stored and managed into object oriented data by an intuitive method. Applying the object oriented search method will improve the effectiveness in search of XML documents.

1 Introduction

As documents in XML (extensible Markup Language) [1] are widely utilized, the need of a new language to search and extract information from XML documents is emerging [2]. Stylesheet syntax is required to visualize the query and its results in order to extract the required information from XML documents: the language that satisfies all of these is XML-GL [2, 3, 4]. XML-GL has defined syntax and semantics based on visual structure and visual arithmetic. XML documents need to be presented visually first in order to execute queries to XML documents by using XML-GL, and XML-GDM is for such a use.

There are many researches and systems to modeling and storing XML documents in object-oriented approach due to its rapid growth in use of the Internet [8]. A representative tool of object-oriented modeling of XML documents is Unified Modeling Language (UML) [9]. UML supports various diagrams including class diagrams for analysis and architecture of object oriented and uses them widely to generate database schemas and object oriented code. In this paper, we will propose an object oriented modeling methodology to improve user's readability, and support effective visual queries for XML documents. This can be achieved by mapping XML documents, XML DTD, queries into class diagrams so that XML documents with

^{*} This work was supported by Korea Research Foundation Grant (KRF-2004-042-D00168).

various attributes of object oriented model are produced. XML documents visualized, stored and managed in UML based object oriented graphical data model will provide the use with intuitive and visually representative queries. UML representation is a commonly used object oriented modeling tool so that it doesn't require learning of new query expressions to use visual and intuitive queries to web based XML documents. The content of XML document, the grammar and syntax of queries in XML-GDM– by applying a same modeling tool- accomplish a series of functions such as string to a database, searching from a database consistently by applying the same modeling tool called UML class diagram.

The paper is structured in 5 chapters. In chapter 2, we examine XML Query languages as related topics. The elements and characteristics of XML-GDM are covered in chapter 3. Chapter 4 describes the mapping method of XML documents in XML-GDM into UML class diagram and verifies it. Finally in chapter 5, we talk about conclusions and future research.

2 Related Works

The most common query languages that support queries based on the structure of XML data are XML-QL [5], Xquery [6], XSL [7], and LOREL [10].

There are single document query languages such as XSL [7] and XQL [13]. XSL (Extensible Stylesheet Language) consists of patterns and templates and becomes a basis of the others. XQL is a notation to select and filter the elements and texts of XML documents and it is an extension of XSL pattern syntax. Its purpose is to design simple and concise syntax with its limited representation.

XML-GL and Blended Browsing and Querying (BBQ) have queries on multiple documents. Graphical user interface such as XML-GL which visualizes and enhances its accessibility to a complex structure of documents is highly recommended. XML-GL, graphic query language, represents XML documents and DTD in XML graph but it relies on a separate XML graphic data model (XML-GDM) [2]. XML Matching And Structuring (XMAS) [11] defined BBQ. BBQ is a separate graphical user interface to generate queries. It is based on a tree structure and uses a window of visualizing XML data. XMAS used an idea from XML-QL which has a CONSTRUCT-WHERE structure as a declarative rule-based query language and uses strong grouping and ordering in order to generate newly combined XML objects from existing ones.



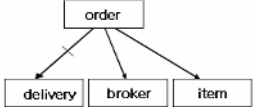
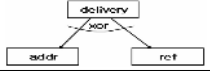
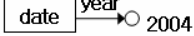
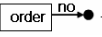
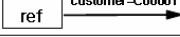

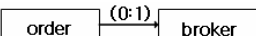
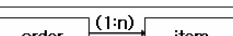
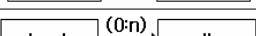
LOREL [10], XML-QL [5], and XQuery are expressional multiple document query languages. LOREL was originally designed for semi-structured data and has been developed as an extension of XML data. It is designed for users' convenience with a SQL/OQL style. XML-QL has a SELECT-WHERE structure as SQL and consists of WHERE: describing XML pattern, IN: describing data sources, and CONSTRUCT: describing the format of XML results. XML-QL is an extended language from SQL and includes transformation/metamorphosis to combine XML data from other resources. XQuery [6] is derived from Quilt [12] – one of XML query languages, set to a standard of XML query language by W3C and has a FLWR (For-Let-Where-Return) structure.

In this paper, we define rules to convert XML-GDM (a data model of XML-GL) to UML class diagrams in order to store it effectively into an object oriented database. By doing this, a search on XML documents will be done effectively.

3 XML-GDM

XML-GL has a data model to store XML documents in a database. It is called XML-GDM. XML-GDM is used to represent XML documents (document instance) and XML DTD that shows the structure of XML documents. Also the syntax of XML-GDM is used in expressing XML-GL queries. Major notations of XML-GDM are in table 1.

Table 1. XML-GDM notation

Feature	XML DOCUMENT	Graphic Representation
Element	<code><order>...</order></code>	
Containment of Elements	<code><order><delivery>...</delivery></order></code>	
Order of Sub-elements	<code><order> <delivery>...</delivery> <broker>...</broker> <item>...</item> </order></code>	
Mutual Exclusion	<code><delivery><addr>...</addr></delivery> or <delivery><ref>...</ref></delivery></code>	
Element with PCDATA Content	<code><date><year>2004</year></date></code>	
ID Attribute	<code><order no="1">...</order></code>	
IDREF Attribute	<code><ref custom="C0001">...</ref></code>	
Mixed Content	<code><order> An year of order is <date><year>2004</year></date> </order></code>	
Multiplicity	0:1 <code><order>...</order> or <order><broker>...</broker></order></code>	
	1:N <code><order><item>...</item></order> or <order><item>...</item> ...</order></code>	
	0:N <code><book>...</book> or <book><author>...</author>...</book></code>	

XML documents are presented in directed graphs with labels called XML graphs in XML-GDM. XML graphs consist of element nodes, attribute nodes, and contents nodes. Each node is connected with containment arcs and reference arcs. A containment arc is used to represent the parent and children relation between element nodes and a reference arc is used in connecting element nodes and/or contents nodes and attribute nodes. Element nodes are displayed in labeled rectangles and element names are labels. Attribute nodes and contents nodes are in labeled circles. White circles represent content nodes and black represent attribute nodes. Arcs connect nodes with labeled arrows and containing arc could use either a label, "CONT," or

nothing. Reference arcs use attributes or #PCDATA style element names as labels. First child node of containment arcs will be stroked with slant lines and the other child nodes will be displayed in an anti-clock wise fashion.

4 Object Oriented XML Document Modeling to Mapping in UML Class Diagram

This chapter proposes a conversion method of XML documents represented in XML-GDM into UML class diagram in order to store them into object oriented database and search them. Object oriented XML modeling for mapping XML-GL into UML class diagram can be divided into three parts: a data model part that transforms XML-GDM to UML class diagram, a query extension part for conversion into UML diagrams according to XML-GL enquiry patterns, and a multiple queries expression part that converts XML-GL multiple queries. We will look at only the data model part, XML-GDM in this paper.

4.1 Mapping Rules

Although UML provides lots of modeling elements, we need to define generation rules precisely to map XML documents to UML class diagrams. We apply the following definitions and rules to generate UML class diagrams from DTDs described in XML-GDM and instances of XML documents.

[Definition 1] The elements of XML-GDM will be mapped into UML class diagram congregation.

A summary of mapping method from XML documents in XML-GDM to UML class diagram is displayed in Table 2.

Table 2. The mapping of XML-GDM and UML

XML-GDM		Our Data Model
Elements	Default	Class
	Containment of Elements	Aggregation
	Order of Sub-element	{ordered} Constraint
	Mutual Exclusion	{XOR} Constraint
Property	Element with PCDATA Content	Derived from "String" Class
	Mixed Content	{XOR} Constraint
	ID Attributes	Private Attribute
	IDREF Attributes	Public Attribute
Multiplicity	0:1	'0..1'
	1:N	'1..*'
	0:N	'0..*'

We will explain mapping methods of each element of XML-GDM to UML class diagram in the next section in detail.

(1) Element

The first rule of mapping elements of XML-GDM to UML is as [rule 1].

[Rule 1] an element of XML-GDM is mapped to a class of UML.

An element that has child elements applies [Rule 2], [Rule 3], and [Rule 4] according to their attributes. [Rule 2] is a mapping rule for elements that have child elements and elements that have child elements map in terms of aggregation of UML.

[Rule 2] If an element contains a child element, each child element applies [Rule 1] to map classes in UML and super and sub classes have aggregation.

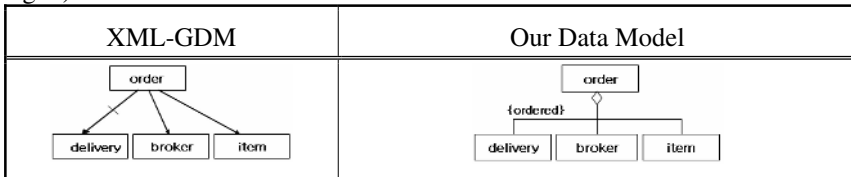
[Rule 3] is a mapping rule when the order of child elements is decided. It uses a limited condition extension mechanism.

[Rule 3] When an element of XML-GDM contains order-defined child elements, an {ordered} condition of aggregation will be defined in UML.

E.g. 1) an element contains child element



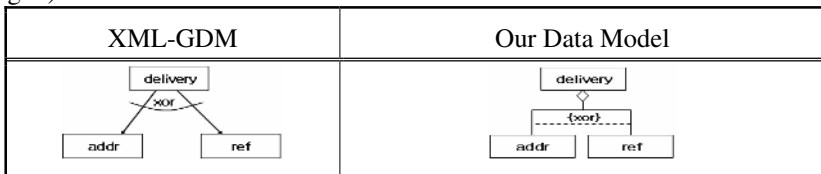
E.g. 2) ordered lower element



[Rule 4] is a mapping rule when a selection relation is defined among child elements, and uses a condition extension mechanism.

[Rule 4] If an element of XML-GDM contains a defined child element with selection, UML designates {xor} constraints in aggregation.

E.g. 3) a defined child element with selection



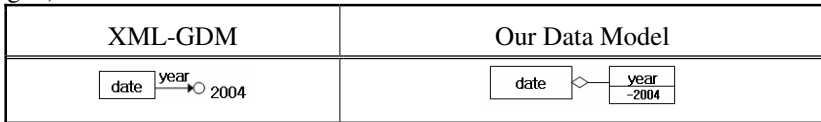
(2) Property

The property of XML-GDM shows displayable values either CDATA (Character data) or PCDATA (parsed CDATA) and is distinguished into contents of element and attributes. The attributes are divided into ID, CDATA, IDREF, and IDREFS. ID and CDATA have their own attributes and IDREF and IDREFS are referencing other values of attributes. Mapping of XML-GDM’s properties applies [Rule 5], [Rule 6], [Rule 7], and [Rule 8].

[Rule 5] is a mapping rule for an element in XML-GDM properties. The content of the element is the #PCDATA type so that it is represented with the inheritance of basic referencing class of UML, “string.”

[Rule 5] The element of XML-GDM’s content inherits from “string” that is a basic data class of UML.

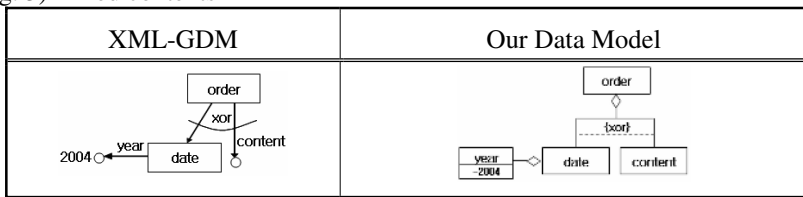
E.g. 4) element content



[Rule 6] is a mapping rule for the mixed content of XML-GDM properties. It uses [Rule 4] and [Rule 5].

[Rule 6] In case of the mixed content of XML-GDM, element applies [Rule2] and [Rule 5]. The text string part generates a temporary class called “content” and applies [Rule 5], then it defines the selection relation

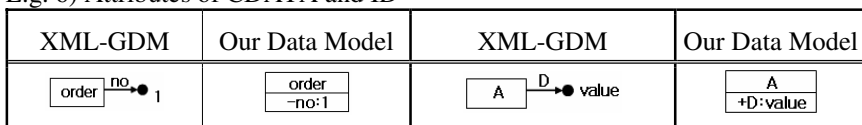
E.g. 5) mixed contents



[Rule 7] is a mapping rule about ID and CDATA type attributes from the properties of XML-GDM. Since the attributes of ID are referred by the attributes of IDREF, it needs to be mapped as public attributes for external classes’ references.

[Rule 7] CDATA’s attributes are private attributes of UML and ID’s attributes are public ones in XML-GDM.

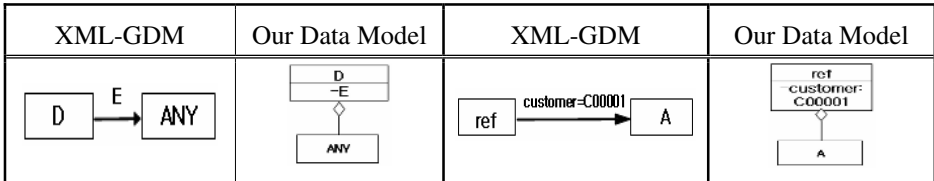
E.g. 6) Attributes of CDATA and ID



Below is a mapping rule of IDREF(S) from XML-GDM’s properties. IDREF(S) of DTD. It refer(s) to an ID attribute of other elements so that a temp-class is generated to indicate a referring class.

[Rule 8] IDREF(S) type attribute of XML-GDM maps the element class as private attributes. Then it generates a temp-class called “ANY”, then it applies [Rule 2] to the “ANY” class and the element class with IDREF(S) attribute.

E.g. 7) IDREF and IDREFS’s attributes



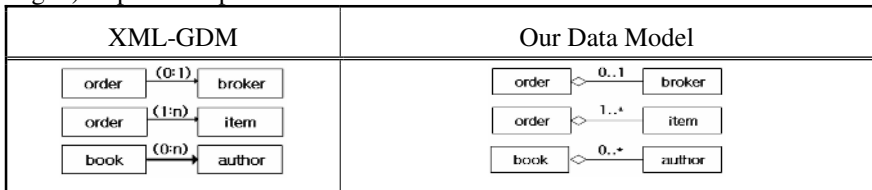
The “ANY” class is replaced by the actual ID attribute of an element class in an instance of XML document then [Rule 2] is applied and mapped into an element class with IDREF(S) attributes and an element class with the ID attribute.

(3) Repetition Operator (Multiplicity)

Multiplicities are ‘0:1’, ‘1:N’, ‘0:N’ in XML-GDM this means that 0 or 1 are more than one time, more than zero time respectively. They are mapped to the next rule. When the multiplicity is not defined, the default value is 1.

[Rule 9] ‘0:1’, ‘1:N’, ‘0:N’, repetition operator of XML-GDM, maps ‘0..1’, ‘1..*’, ‘0..*’ of UML.

E.g. 8) Repetition operator



4.2 Applications

We will prove the efficiency of mapping rules by applying these rules into XML documents related book order.

Figure 1 is a DTD (order.dtd) representing the document structure related book order. Figure 2 is a result of modeling XML DTD into XML-GDM, and Figure 3 is a mapping result of mapping Figure 2 into a UML class diagram.

Figure 4 is an example of XML document (“order.xml”) produced by XMLDTD of Figure 1. When modeling XML documents of Figure 6 into XML-GDM is done it will be like Figure 5. The modeled XML document in XML-GDM from Figure 5 becomes Figure 6. That is the result of the mapping it into a UML class diagram.

```

<!ELEMENT order (delivery, broker?, item+, date)>
<!ATTLIST order no CDATA #REQUIRED>
<!ELEMENT delivery (addrref)>
  <!ELEMENT addr (company?, city, detail_addr+)>
  ...
  <!ELEMENT ref EMPTY>
    <!ATTLIST ref custom IDREF>
  <!ELEMENT broker (#PCDATA)ref>
  <!ELEMENT item (book, count, discount)>
    <!ELEMENT book (ISBN, title?, price, author*)>
      <!ELEMENT ISBN (#PCDATA)>
      ...
      <!ELEMENT author (last_name, first_name)>
      ...
    <!ELEMENT count (#PCDATA)>
    <!ELEMENT discount (#PCDATA)>
  <!ELEMENT date (year, month, day)>
    <!ELEMENT year (#PCDATA)>
    ...
  <!ELEMENT person (last_name, first_name?, addr)>
    <!ATTLIST person personalID ID>
    <!ELEMENT last_name (#PCDATA)>
    <!ELEMENT first_name (#PCDATA)>
  
```

Fig. 1. DTD of XML Document related book order (order.dtd)

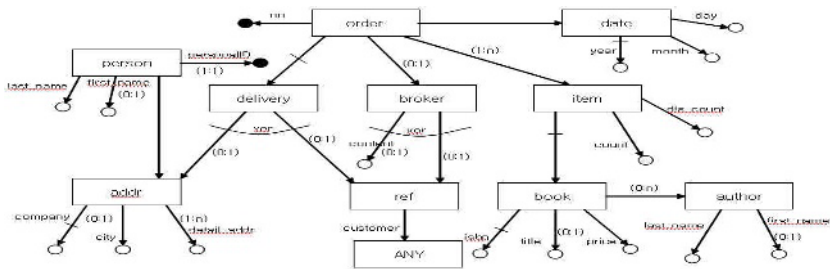


Fig. 2. “order.dtd” represented by XML-GDM

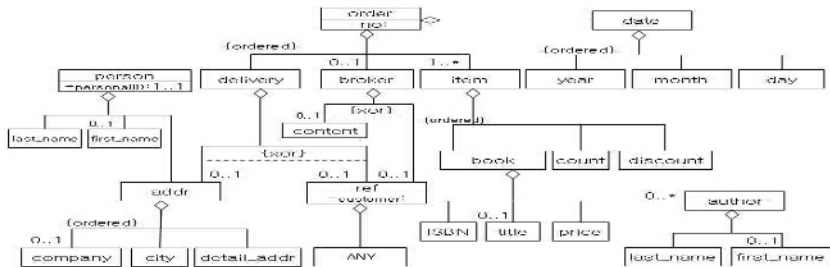


Fig. 3. “order.dtd” represented by UML Class Diagram

```

<DOCTYPE order SYSTEM " order.dtd">
< order no=1>
<delivery><ref customer="C00001"></ref></delivery>
<broker>GDHong</broker>
<item>
<book>
<ISBN>15536455</ISBN><title>XML Introduction</title><price>25000</price>
<author><last_name>Kim</last_name><first_name>CS</first_name></author>
</book>
<count>6</count><discount>.20</discount>
</item>
<item>...</item>
<date><year>2004</year><month>2</month><day>1</day></date></order>
< order no=2>
<delivery>
<addr><company> AAA Bookshop </company><city>Jeonju</city>
<detail_addr>aa st. 840-2</detail_addr></addr>
</delivery>
...
<person personalID="C00001">
<last_name>Yeom</last_name><first_name>SJ</first_name>
<addr><company>BBB Bookshop</company><city>Seoul</city>
<detail_addr>bb st. 1318</detail_addr></addr>
</person>
...
    
```

Fig. 4. XML Document related book order(order.xml)

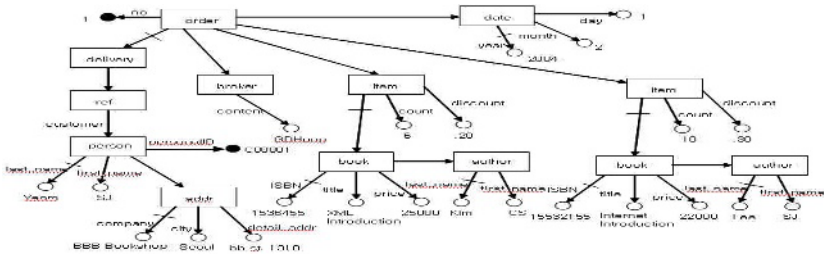


Fig. 5. "order.xml" represented by XML-GDM

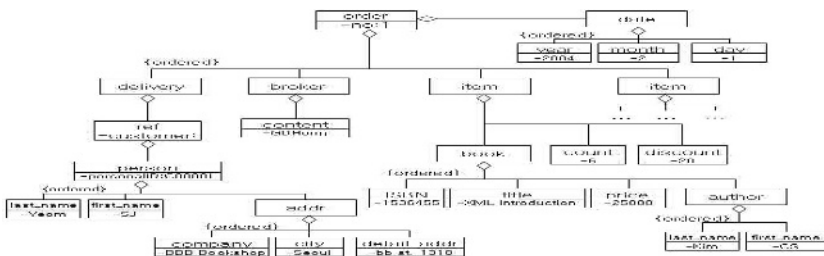


Fig. 6. "order.xml" represented by UML Class Diagram

5 Conclusion and Future Works

We have proposed a modeling technique of XML documents via a visualizing method. It is done based on XML-GDM that is a graphical data model of XML-GL. It has a visual modeling function of XML document and DTD and a visual query function about it. We used UML in order to propose new object oriented modeling rules for XML document. By doing this, we could visualize XML documents, as a result, we improved readability of XML documents and established a basis to provide an intuitive structural query function. Our model provides a ground of efficient storage, management and search of XML documents due to good use of content-based characteristics of XML and object oriented attributes. This also removes the existing database storage techniques that didn't utilize structural characteristics of XML documents and a limitation of query techniques.

For better applications of the proposed method, research about intuitive visualized query in XML document database should be done. Also visual XML database systems with the proposed object oriented modeling techniques and query modeling techniques needs to be developed.

References

1. Tim Bray, et al., XML 1.0 (Third Edition). W3C Recommendation. <http://www.w3.org/TR/2004/REC-xml-20040204> (2004)
2. Stefano Ceri, et al., XML-GL: a graphical language for querying and restructuring XML Documents. *Computer Networks*. Vol. 31. (1999) 1171-1187
3. Stefano Ceri, et al., Complex queries in XML-GL. Proc. of 2000 ACM symposium on Applied Computing (SAC2000). Como, Italy (2000) 888-893
4. S. Comai, E. Damiani, and P. Fraternali, Computing Graphical Queries over XML Data. *ACM Transaction on Information System (TOIS)*, Vol. 19. No. 4. (2001) 371-430
5. Alin Deutsch, et al., XML-QL: A Query Language for XML. <http://www.w3.org/TR/NOTE-xml-ql> (1998)
6. Scott Boag, et al., XQuery 1.0: An XML Query Language. <http://www.w3.org/TR/xquery> (2004)
7. Sharon Adler, et al., Extensible Stylesheet Language (XSL) Version 1.0. <http://www.w3.org/TR/xsl/> (2001)
8. V. Christophides, S. Abiteboul, S. Cluet, and M. Scholl, From Structured Documents to Novel Query Facilities. *ACM SIGMOD Record*. Vol. 23. No. 2. (1994) 313-324
9. OMG, OMG Unified Modeliing Language Specification Version 1.5. <http://www.Zomg.org/docs/formal/03-03-01.pdf> (2003)
10. Serge Abiteboul, et al., The Lorel Query Language for Semistructured Data. *Int'l Journal on Digital Libraries*. Vol. 1. No. 1. (1997) 1-21
11. Bertram Ludäscher, Yannis Papakonstantinou, and Pavel Velikhov, A Brief Introduction to XMAS. <http://www.npaci.edu/DICE/Pubs/XMAS-intro.pdf> (1999)
12. Don Chamberlin, Jonathan Robie, and Daniela Florescu. Quilt: An XML Query Language for Heterogeneous Data Source. Proc. of the 3rd Int'l Workshop on the Web and Databases(WebDB 2000). Dallas, USA (2000) 53-62
13. Jonathan Robie, Joe Lapp, and David Schach, XML Query Language (XQL). <http://www.w3.org/TandS/QL/QL98/pp/xql.html>. (1998)

A Two-Phase Local Server Security Model Based on XML Certificate*

Yong-Hwa Kim¹, Jin-Sung Kim¹, Yong-Sung Kim¹, and Jang-Sup Shim²

¹ Division of Electronic and Information Engineering, Chonbuk National University,
664-14 1ga Duckjin-Dong, Duckjin-Gu, Jeonju, 561-756, Republic of Korea
{kyh, kpjjju, yskim}@chonbuk.ac.kr

² Institute of Information Technology Assessment 52, Eoeun-dong, Yuseong-gu,
Daejeon-si, 305-333, Republic of Korea
sjs@iita.re.kr

Abstract. This paper proposes server security certificate management system applying the mechanism of public key infrastructure and XML Security technology specification to secure the information and resources open in network. This model is the system that permits the access only to the authorized users at a request of the status of the certificate through certifying server after issuing and requesting wire, wireless certificate on-line and registering on the XML certificate managing server. Also, this paper investigates the methods to support independent and various styles of information exchanges at platform using SOAP Message to provide remote server with the service of certificate request and inquiry.

1 Introduction

In this paper, XCMS(XML Certificate Management Server) and XCAS(XML Certificate based Authority Server) are proposed to permits the access only to the authorized users on the local server at a request of the status of the certificate through certifying server based on XML Certificate[1]. The essence of this system is to decide whether to permit the access or not to the local server according to the status of the users by using the message in XCAS inquiring the users' certificate and the status of the certificate after issuing public key infrastructure based X509 v.3 wire, wireless certificate through on-line and constructing XCMS providing inquiring and registering service to the issued certificate. To do this process, the request and reply message to register the certificate issued by the organization and the request and reply message to inquire the certificate from XCAS to XCMS are presented by SOAP (Simple Object Access Protocol). To solve the problem of OCSP (Online Certificate Status Protocol), the existing certificate controlling program, it permits the independent server access to the platform using SOAP Message. This paper proposes server security system model assuring far better security than the existing security mechanism enabling harmonious communication between the systems using XML characteristics and by separating the certificate issuing organization from the organization providing certificate registration and reference after constructing server security system based on XML security technology specification [2, 3, 4].

* This work was supported by Korea Research Foundation Grant (KRF-2004-042-D00168).

2 Related Work

In this chapter, researches connected with XML-Signature and local server security is compared and analyzed. First, researches about XML digital signature base Systems Design and implementation are presented in [2] and [3]. The [2] and [3] proposed XML Signature base electronic commerce server security system. Also, research about XML digital signature techniques is in [4] and [5]. [4] creates XML digital signature, presented mechanism that quote service bundle without certification process, [5] presented techniques that can offer Time Stamping Protocol in XML server techniques. While [6] introduces about basic idea about XML Encryption and XML Signature and schema and [7] presents algorithm to analyze electronic payment protocol using symmetric encryption digital signature techniques. [6] is describing details about schema example and sub element about XML Signature and XML Encryption. [7] is about research that analyze responsibility whereabouts proof for message that is transmitted between transaction person concerned in Information-Communication protocol of symmetric encryption digital signature techniques for electronic commerce.

3 XML-Signature and SOAP

This chapter describes about SOAP, the basic technology XML-Signature for “the certificate management system modeling using XML certificate”.

3.1 XML-Signature

XML-Signature [2] is used to verify the transactions or identify of the users on cyberspace as a verifying method. XML-Signature based on XML was standardized in February 12, 2002, through the efforts of W3C and IETF. Standardized contents describe clear statement of the regulations on XML-Signature to maximize the security and the extents of the standardized contents, integrity, message and user authentication and non-repudiation. The primary elements of XML-Signature are digital signature information and digest information and the presentation of XML Schema (Fig. 1) on X509.

Signature elements consist of SignedInfo with digital signature information, Signature Value with actual digital signature value and KeyInfo [9] with digital signature key information and X.509 certificate. In particular, SignedInfo describes how signature information is standardized and the algorithm for the signature and the subordinate algorithm, Reference, consists of DigestMethod, the algorithm summarizing signature data, and the element, DigestValue showing the result.

```

<Signature>
  <SignedInfo>
    <CanonicalizationMethod>
    <SignatureMethod>
    <Reference> <DigestMethod/> <DigestValue/> </Reference> </SignedInfo>
    <SignatureValue>
    <KeyInfo>
  </Signature>

```

Fig. 1. XML Digital Signature Elements

KeyInfo described in XML Security is used to encode XML Digital Signature and XML. In particular, X509Data [3], one of the subordinate elements of KeyInfo includes X509 v.3 certificate key identifier, X509 v.3 certificate and certificate repeal list.

3.1.1 SignedInfo Element

Schema presentation of SignedInfo element is as follows.

```

<Signature>
  <SignedInfo>
    <CanonicalizationMethodAlgorithm=http://www.w3c.org/TR/REC-xml-200135#"/>
    <SignatureMethod Algorithm="http://www.w3c.org/2000/09xmldsig#dsa-sha1"/>
    <Reference URI=http://www.w3c.org/TR/2000/signature-example.xml>
      <DigestMethod Algorithm=http://www.w3c.org/2000/09xmldsig#sha1/>
      <DigestValue> Zu0kjegV355VZWWdbZ79sjk </DigestValue>
    </Reference> </SignedInfo>
    <SignatureValue> w5smjh45/89VVd3DBaq </SignatureValue>
  </Signature>

```

Fig. 2. SignedInfo Element

Signedinfo element is consisted of Canonicalizationmethod element , Signature-method element and Reference element. Canonicalizationmethod element includes algorithm that signature information is formalized. Signaturemethod element contains algorithm for signature. Reference element compresses signature data and includes compression result. Also, signaturevalue element includes calculated signing in signedinfo element.

3.1.2 KeyInfo Element

KeyName element, including the string used to identify the appropriate key from the person performing digital signature and encoding to the receiver, is the element which includes the actual value of a public key useful in identifying the key, deciphering the data, and certifying KeyValue element digital signature. In addition, X509Data element consists of X509 key identifier, at least one, X 509 certificates, and certificate revocation lists (CRL).

```

<element name="KeyInfo" type="ds:KeyInfoType"/>
  <complexType name="KeyInfoType" mixed=true">
    <choice maxOccurs="unbounded">
      <element ref="ds:KeyName"/> <element ref="ds:KeyValue"/>
      <element ref="ds:X509Data"/>
      :
    </choice>
    <X509Certificate name="id" type="ID" use="optional"/>
  </complexType>

```

Fig. 3. KeyInfo Element

3.2 SOAP (Simple Access Object Protocol)

SOAP is the protocol supporting various types of information exchanges to the platform or operation system based simple XML for information exchanges in disperse environments. The function of SOAP is transmitting the message requested by customers. The service supporter calls the requested function and sends the replying message. The following is the form of a SOAP message.

4 Two-Phase Local Server Security Model

It is the system to protect local server against the trespass based wire/wireless XML. After requesting and issuing wire/wireless certificate, the certificate is registered on the certificate management system.

XCMS plays the role not only registering the certificate but also sending the reply message on the certificate and the status inquiring messages requested on the certificate server. Through this inquiring process, this system can permit the access only to the certified users to the server.

4.1 Two-Phase Local Server Security Model's Configuration Diagram

Server security certificate system consists of certificate system and XCMS and XCAS. Figure 4 shows the process of server security certificate system.

The elements and functions of Server Security Certificate System can be briefly described as follows:

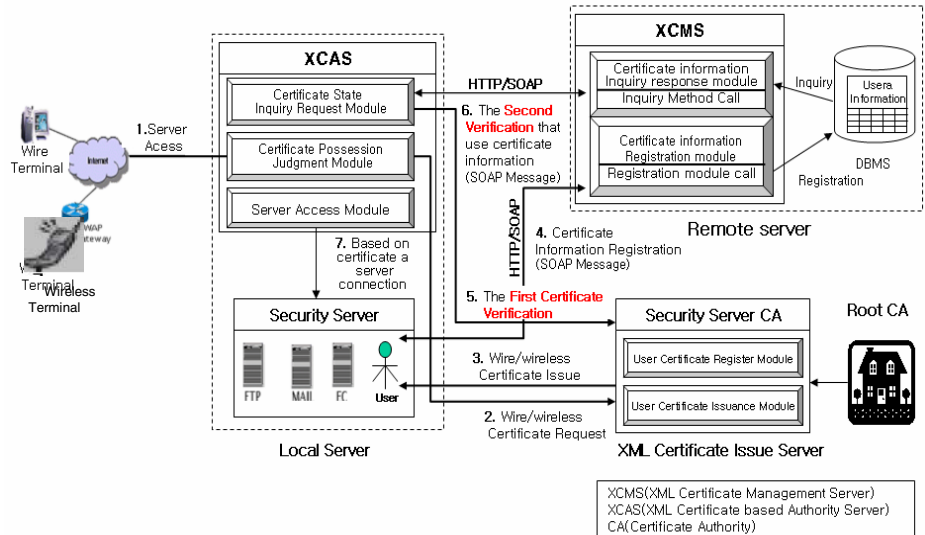


Fig. 4. Architecture of Authority System for Server Security

(1) Security Server Certification Authority

When users request the certificate on-line, the registration authorities identify the status of users, and then the certificate authorities issue the certificate. This system is applied to this process to transmit the request message for certificate registration and to register certificate issued to certificate management server.

(2) XCMS (XML Certificate Management Server)

It is the server that receives the certificate from certificate authorities and registers it on the server certificate depot. Also, it offers certificate inquiring service if the access control server requests the certificate or the status of the certificate.

(3) XCAS (XML Certificate based Authority Server)

It is the server that inquires the certificate and the status of the certificate to certificate management server after writing out certificate inquiry request message obtaining the users' certificate password when wire/wireless terminal users log on local server.

4.2 Two-Phase Local Server Security Model's Achievement Algorithm

Achievement algorithm of two-phase local server security model of xml certificate base is as follows.

```

input : Certificate password and addition list
output : Decision whether or not local server connection
begin
{
  // Information abstraction that is log of server connector
  log_Info = get_User_Info( )
  // By judgment module whether or not certificate possession certificate information
  abstraction
  certificate_Info=certificate_possession_Judg(log_Info)
  // When there is certificate
  if (certificate_Info) {
    // Verification request in the certification authority
    verification_request_CA(certificate_Info)
    result1 = verification_response_CA(Certificate, Validity)
    // The first verification : User certificate information and CA's certificate information
    comparison
    if(certificate_Info == result1) {
      // The second verification : Certificate information verification that use SOAP message
      between XCAS and XCMS
      verification_request_mess(Certificate Password, Addition information)
      result2 = verification_response_mess(Certificate, Validity, Addition information)
      if(certificate_Info == result2)
        sever_Access_Success() // Server connection success
    }
    else
      sever_Access_Fail() // Server connection failure
  }
  // When there is no certificate information
  else {
    // To issue certificate user information abstraction
    user_Info = get_user_info()
    request_CA(user_Info) // Certificate issuance request
    if(When something wrong does not exist in identity) {
      issue_CA(Certificate) // Certificate issuance success
      // By XCMS in security server certificate information registration request message
      transmission
      reg_request_mess(Certificate Information, addition list)
      // By security server in XCMS certificate information registration request response
      message transmission
      reg_response_mess(Serial number, Registration result)
      sever_Access_Success() // Server connection success
    }
    else {
      not_issue_CA() // Certificate issue failure
      sever_Access_Fail( ) // Server connection failure
    }
  }
}
end

```

Fig. 5. Two-Phase Local Server security model's achievement algorithm

5 Two-Phase Local Server Security Model Implementation

In this section we describe the implementation screen that request online and issue XML-Signature extension part and X509 v.3 wire/wireless certificate for two-phase verification. And also we describe about SOAP message to enroll certificate to XCMS.

5.1 Security Server Certificate Authority

5.1.1 XML-Signature Extension Part

The Extended XML-Signature's example that creates certificate information for certificate and two-phase verification that issue security server Certificate Authority is as follows.

```

<Signature>
  <SignedInfo      // Actuality information about signature
  <CanonicalizationMethod Algorithm="http://www.w3c.org/TR/2001/REC-xml-c14n-20010315#"/>
  <SignatureMethod Algorithm="http://www.w3c.org/2000/09xmldsig#dsa-sha1"/>
  <Reference URI="http://www.w3.org/TR/2000/signature-example.xml">
    <DigestMethod Algorithm="http://www.w3c.org/2000/09/xmldsig#sha1"/>
    <DigestValue> Zu0kjegV355VZWWdbZ79sjk </DigestValue>
  </Reference>
</SignedInfo>
<SignatureValue>w5smjh45//89VVd3dBAQ</SignatureValue> //Actuality value of digital signature
<KeyInfo          // Information about key
  <KeyName> kimjs </KeyName>
  <KeyValue> Xa7u+eOyH5..</KeyValue>
<X509Data        // Information about x509 certificate
  <X509IssuerName>CN=kimjs, C=KR.. </X509IssuerName>
  <X509SerialNumber>1234567 </X509SerialNumber>
  <X509SubjectName>Certificate A </X509SubjectName>
  <X509Certificate>MIICSTCCA... </X509Certificate>
  <X509Items> // Extended Part
    <CertificationCenter> CN_Sign </CertificationCenter>
    <CertificateSerialNumber> CS_0001 </CertificateSerialNumber>
    <CertificateDate> 2005-06-10 </CertificateDate>
    <CertificatePermissionCode> CN_Sing_Kimjs </CertificatePermissionCode>
    <SignatureAlgorithm/> dsa-sha1 </SignatureAlgorithm>
    <CertificateSubscriber/> Kim-js </CertificateSubscriber>
    <PersonalNumber>601011-234567 </PersonalNumber>
  </X509Items>
</X509Data>
</KeyInfo>
</Signature>

```

Fig. 6. Extended XML-Signature's example

5.1.2 User Certificate Issuance Module

(1) Wire/wireless Certificate Request Process

The following picture is the interface of the certificate request form between local server and Security Server Certification Authority.

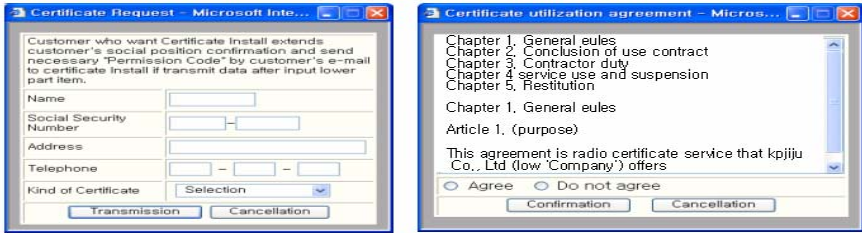


Fig. 7. Wireless and wire certificate request interface

The process of certificate request is finished with the user's agreement with the provision after writing out the requested form. The registration authorities send the admission code by e-mail after identifying the user's status with the form the user sent.

(2) Wire/wireless Certificate Issuing Process

If the certificate request from registration authorities to certificate authorities goes on successfully, the interface to issue the certificate have two steps as shown below.



Fig. 8. Digital Signature Generation Interface

After the user puts the admission code he receives by email, he chooses save directory and receives the password to create the digital signature contained in the certificate.

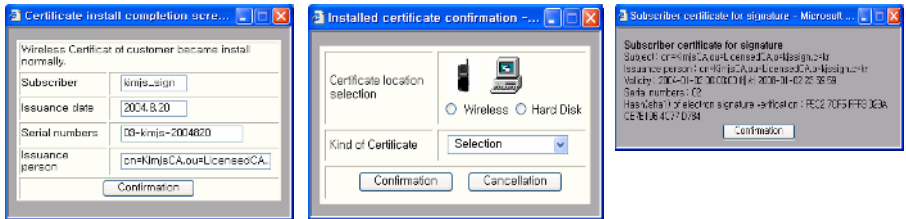


Fig. 9. Certificate Install and Generation Interface

After creating the digital signature and the certificate is installed successfully, the user can confirm the certificate by clicking the button “certificate view”.

5.1.3 User Certificate Register Module

Local server transmits certificate issuance information and x509 v.3 certificate information making out request message to register certificate information to xcms by parameter.

```

<SOAP-ENV:Body>
  <SOAPXCMS:Register>
    <X509IssuerName> CN=KIM JS </X509IssuerName>
    <X509SerialNumber> 03 </X509SerialNumber>
    <X509SubjectName> Certificate A </X509SubjectName>
    <X509Password>***** </X509Password>
    <X509Certificate> MIIC34PzCCA0+....KTV </X509Certificate>
    <X509CRL> 2010-12-30 </X509CRL>
    <X509Items>
      <CertificateSerialNumber> 03 </CertificateSerialNumber/>
    </X509Items>
  </SOAPXCMS:Register>
</SOAP-ENV:Body>
    
```

Fig. 10. Certificate registration request message

5.2 XCAS (XML Certificate Based Access Server)

XCAS makes and transmits the request message to verify the validity of the certificate to XML certificate management sever (XCMS) when the user input one's own certificate password to log on.

5.2.1 User Login Screen

XCAS provides login image requesting certificate password as shown below when the user tries to log onto the server.

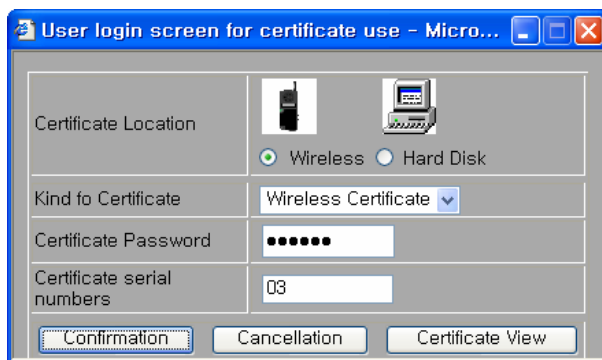


Fig. 11. User Login Screen

To select one to do random in <X509Item> Element's contents connected with certificate information for security reinforcement of screen that is user log to supplement side that problem can be caused through unlawful certificate pecculation and hacking of certificate password.

5.2.2 Message Requesting Certificate Verification

The certificate password input by the user creates the message requesting certificate verification by the certificate in XCAS and status verification module. The message requesting certificate verification is as follows:

```
<?xml version="1.0">
<SOAP-ENV:Envelope
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <SOAPXCMS:Request>
      <X509Password> ***** </X509Password>
      <X509Item> Certificate SerialNumber </X509Item>
    </SOAPXCMS:Request>
  </SOAP-ENV:Body> </SOAP-ENV:Envelope>
```

Fig. 12. Certificate Checkup Request Message

5.3 XCMS (XML Certificate Management Server)

XCMS provides XML certificate registration service and certificate information service.

5.3.1 XML Certificate Registration Service

In XCMS, the reply message for the certificate registration service to the request message for the certificate registration is as follows.

```
<SOAP-ENV:Envelope
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <SOAPXCMS:RegisterResponse>
      <RegisterSerialNumber>231-645-7754</RegisterSerialNumber>
      <ResultMessage>Certificate Registered success!!</Result_Message>
    </SOAPXCMS:RegisterResponse>
  </SOAP-ENV:Body> </SOAP-ENV:Envelope>
```

Fig. 13. XML Certificate Registration Request Message

The certificate information sent from certificate authorities calls the related method at XML certificate management server, register related information, and send the message noticing certificate registration serial number and whether registered or not.

5.3.2 XML Certificate Information Service

In XCMS, the reply message to verify the certificate and the status of it about the request message for the service of certificate verification and validity from XCAS is as follows.

```
<SOAP-ENV:Envelope
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Body>
  <SOAPXCMS:Request>
    <X509Certificate>MIIC34PzCCA0+....KTV</X509Certificate>
    <X509CRL>2010-12-30</X509CRL>
    <CertificateSerialNumber> 03 </CertificateSerialNumber>
  </SOAPXCMS:Request>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Fig. 14. Certificate and State Response Message

The result of the inquiry consists of X509Certificate element containing the user's certificate information and X509CRL element including the information on the status of the certificate.

6 Conclusion and Further Study

The interest in security has been dealt with seriously among individuals, companies and the countries. In particular, as a respect of the security of information, indiscriminate lifting from other people's privacy and trespass and destruction of information resources give huge side effects on our daily life and even national security. Therefore, this study proposes the server security model permitting the access to the server only to the certified users as a securing method to preserve the server of personal users and the companies applying the mechanism of remote call of the certificate based on the existing public key infrastructure and XML security technology.

Further study should be focused on the mechanism of fast progress in dealing with the certifying process and message transmitting process because the speed of the system can be slow during the certificate based login process to the server. Also, the preceding study on XML security technology spec about the wireless certificate should be done.

References

1. Ki-Young Moon, "XML XML information protection abstract," KIPS journal, Volume 10, Number 2, pp. 108-116, 2003. 3.
2. Hyoung-seok Lee, "Design and Implementation of EC Server Security based on XML Digital Signature," Proceedings of the 29th KISS Spring Conference, pp.760-792, April 2002.
3. Se-Young Kim "Design and Implementation of e-commerce system Supporting XML Digital Signature," Proceedings of KISS Conference, Volume 28, Number 2, pp.766-768, 2001. 10.

4. Hee-Young Lim. "Bundle Authentication using XML Signature in the OSGi Service Platform," Proceedings of the KISS Conference, Volume 31, Number 01, pp.196-198, 2004. 04.
5. Won-Jin Lee, "XML Signature Scheme with Time Stamping Protocol," Proceedings of the KISS Conference,, Volume 31, Number 01, pp.214-216, 2004. 04.
6. Elisa Bertino, Barbara Carminati and Elena Ferrari, "XML security," Information Security Technical Report, Volume 6, Issue 2, Pages 44-58, 1 June 2001.
7. Young-Dal Kim, "Extention of Kailar Accountability Logic for Symmetric Key Digital Signature and Accountability Analysis of an Electronic Payment Protocol," The Transactions of the KISS Processing Society Volume 09 Issue 3, pp.3046-3059, 1999. 11.
8. <http://www.w3c.org/TR/2002/REC-xmlsig-core-20020212/>
9. <http://www.w3c.org/TR/xmlsig-core>.
10. Dr. Andrew Blyth, Dr. Daniel Cunliffe and Dr. Iain Sutherland, "Security analysis of XML usage and XML parsing," Computers & Security, Volume 22, Issue 6, Pages 494-505, September 2003.
11. Elisa Bertino, Barbara Carminati and Elena Ferrari, "XML security," Information Security Technical Report, Volume 6, Issue 2,Pages 44-58, 1 June 2001.
12. K. Komathy, V. Ramachandran and P. Vivekanandan, "Security for XML messaging services—a component-based approach," Journal of Network and Computer Applications, Volume 26, Issue 2,Pages 197-211, 1 April 2003.
13. Antonio F. Gómez, Gregorio Martínez and Óscar Cánovas, "New security services based on PKI," Future Generation Computer Systems, Volume 19, Issue 2, Pages 251-262, February 2003.
14. Stephen Farrell and Michael Zolotarev, "XML and PKI — What's the story?," Network Security, Volume 2001, Issue 9, Pages 7-10, 1 September 2001.

Integrated Object Modeling for Web-Based XML Application Documents*

Chun-Sik Yoo¹, Jin-Sung Kim¹, Yong-Sung Kim¹, and Jang-Sup Shim²

¹ Division of Electronic and Information Engineering, Chonbuk National University, 664-14 1ga Duckjin-Dong, Duckjin-Gu, Jeonju, 561-756, Republic of Korea.

² Institute of Information Technology Assessment 52, Eoeun-dong, Yuseong-gu, Daejeon-si, 305-333, Republic of Korea
{csyoo, kpjiju, yskim}@chonbuk.ac.kr, sjs@iita.re.kr

Abstract. For having various applications, XML is widely used in various fields. But, there has not been a system to integrate and manage XML and its applications together. In this paper, we propose methods to integrate web-based XML applications(SMIL, RDF, WIDL) and for object-oriented modeling of each DTD and document instance. We propose a system to merge object modeling of XML applications. With the proposed integrating algorithm, we can not only easily analysis various web-based XML applications which are represented by complex tags, but also generate object-oriented schema for each document and store it to OODBMS.

1 Introduction

XML(eXtensible Markup Language) has flexibility that can define element, attribute, and Entity according to the specific application domain such as SMIL(Synchronized Multimedia Integration Language), RDF(Resource Description Framework), WIDL(Web Interface Definition Language), etc.[1]. These XML applications are based on WWW, so they will be used widely. SMIL is a standard grammar[2] to transmit multimedia contents on web such as graphics and audio. RDF is a framework that offers an interoperability between applications to exchange information or on Web to process meta data[3]. WIDL is meta data grammar to define application program interfaces(APIs) for web data and service.

An issue has Had been ignored that access directly to web data in business application field so far but lately, an interface is described and used that can access web resources by standard web protocol in remote system by using WIDL.

WIDL's purpose is to supply a general method to represent request/response interaction for standard web protocol, and to automate an interaction that uses resources raving a form of HTML/XML to various integration platforms. [4, 5, 6].

WIDL having these features is an XML application that is object-oriented, but it does not propose object modeling methodologies schema for it up to date. Therefore, this paper proposes an algorithm to integrate SMIL, RDF, WIDL that is representative web-based XML application and to do object modeling. And, we propose rules applied commonly to DTD without distinction of XML application.

* This work was supported by Korea Research Foundation Grant (KRF-2004-042-D00168).

2 Related Work

Approach on web document offering API normalized for XML document and there is DOM(Document Object Model) [1] by method to manufacture, this does not represent attribute or aggregation relation etc. that is object base structure that define logical structure of document but detailed information of class because is form of Tree class structure properly. Additionally, object modeling research about DTD is XOMT(eXtended Object Modeling Technique) and the UML class diagram.

XOMT extended many OMT's function, but there is part that do not fit well to object-oriented concept such as class that define attribute.

Than this UML class diagram DTD according to object intention-oriented object modeling do [7]. Therefore, this study that proposes algorithm that map rightly to XML DTD based on rule that map XML DTD of [7] in UML class diagram, and generation UML class diagram through this. In addition to, by modeling[8] for XML document was proposed, and Extending this UML Use Case diagram about SMIL document, object modeling is proposed[10] in the UML class diagram by Semantic analysis by synchronization modeling[9] and RDF resource using Sequence and Collaboration Diagram. But, yet SMIL, there is not specific modeling method about XML application is presented except RDF, There was no research about these Web-Based application's integration. Therefore, in this study that integrates Web-Based XML application, and XML DTD that doing object modeling, did so that can generation object modeling and object-oriented code about each XML application document.

3 Web-Based XML Document Modeling

In this chapter modeling rule to create UML class diagram about representative Web-Based XML documents, member function of each class, and propose modeling algorithm.

3.1 Modeling Rule

The followings are rules necessary to do to map Web-Based XML application document instance to set of UML class diagram.

(1) Element

The following defines rules about element of beginning tag.

This time, same type of class iteration when is created attach order number in each class name and distinguish this.

[Rule 1] Element that become SMIL's media tag, hyper link tag, selection tag, RDF's <RDF:Description> tag, WIDL's beginning tag gets into class.

(2) Attribute and Value

Rule about attribute and the value is same as following.

[Rule 2] Attribute of RDF schema, attribute and value get into Private attribute and value of relevant class in WIDL's Element tag.

(3) Relation between attributes

Relation between included Elements defines as following inside with Element.

[Rule 3] RDF's <rdfs:Container>, Element that come inside WIDL's Element tag gets into composition relation between class and sub class.
[Rule 4] RDF's <rdfs:subClassOf> gets into generalization relation between Element class and sub class [9].

3.2 Modeling Function

SMIL, RDF, WIDL document when did to map in UML class diagram, member functions inserted on operation list part of each class as each following same. These member functions do structure grasping and transformation of relevant class diagram to be easy.

3.2.1 SMIL's Member Function

In the case of SMIL document, because modeling function extract class from object of sequence diagram, it need synchronization function about occurrence sequence of class, and function about reference class. Contents are same with table 5 in reply [9].

Table 1. Modeling function of SMIL class

Functions	Explanation
par_o()	Classes that happen same time
seq_o()	Next, class that happen
href_o()	Class referred while class executes
anchor_n()	Class referred while class executes

3.2.2 RDF's Member Function

The following is member function that come hereupon, when changed by class of RDF resources [10]. Basically, need function that represent supermarket class and subclass and function that represent included attribute in relevant class. And, need function connected with relation between sub classes that compose super class.

Table 2. RDF Member Function of Resources Class

Functions	Explanation
p()	Super Class
c()	Sub Class
cons()	Connector's kind
r()	Sub Class order
m()	Attribute

3.2.3 WIDL's Member Function

In the case of WIDL, basically, need bow that define service number and input/output parameter of binding except function connected with class and attribute. Member function of class created by WIDL is same with table 8.

Table 3. WIDL Member Function of Class

Functions	Explanation
p()	Super Class
c()	Sub Class
s()	Service number
i()	input parameter value of binding
o()	output parameter value of binding
m()	Attribute

3.3 Modeling Algorithm

In this section proposes algorithm that input XML document instance such as RDF or WIDL and create UML class diagram. Only, spoke in [9] already by changing to class and create class diagram drawing object from order diagram in SMIL's case. create_DI_ClassDiagram()

```

Input: XML application Document
Output: UML Class Diagram
begin {
make_class() //Generate rootclass (WIDL, one generations among Resource)
for (No of Attribute List)
insert_attlist_function() // Insert Attribute and Value
insert_member_function() //InsertionMember Function
for (Beginning tag or No of <rdf:Description>) {
make_class() // Class generation
for (Attribute list)
insert_attlist_function() // Insertion Attribute and value
insert_member_function() // Insertion Member function
if (root class == WIDL)
make_composition() // Form Composition relation
else
make_generation() // Form Generalization relation
while not (</rdf:Description>) {
if (<rdf:type>)
Define_classtype()
else if (<rdf:subClassOf>)
make_generation() // Form Generalization relation
else if (<rdf:Container>)
make_composition() // Form Composition relation
else {
if (not end tag(/))
for (No of Beginning tag) {
make_class () // Create class
for (No of attribute list)
insert_attlist_function() // Insert Attribute and value
insert member_function() // Insert member function
make_composition // Form composition relation
} } } } }
end;

```

Table 4. Mapping table of class diagram from DTD

XML DTD		UML Class Diagram	
Element Declaration	Declaration Part	Class	
	Contents Part	Connector	Composition Relation
		Occurrence Pointer	Multiple
Attribute List Declaration	Attribute	Private Attribute	

4 Integration System

In this chapter, We propose system and application result that integrate modeling about each XML application that proposes in chapter 4. Before this, we propose modeling rule and algorithm applied commonly to create class diagram from each application XML DTD.

4.1 System Configuration

When DTD about XML application and document instance were inputted, system configuration diagram about diagram and object -oriented code generation is same with figure 1.

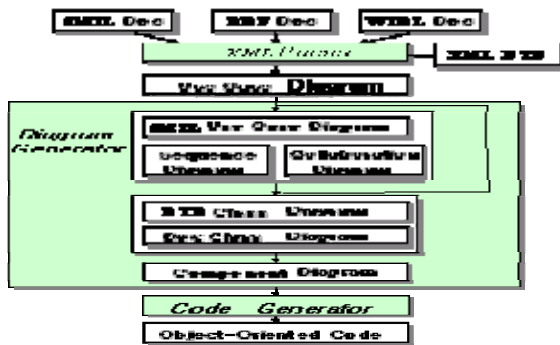


Fig. 1. XML Application Integration System Configuration

(1) XML Parser

XML DTD and document instance being inputted error of grammar examine and create Parsing table.

(2) Use Case Diagram

Various application of XML distinguishes to each use case of UML and handles. It is same with figure 2.

(3) Diagram Generator

Tag used to XML instance creates use case and sequence diagram first in case of tag that define in SMIL DTD and generation collaboration diagram and class diagram automatic generation.

DTD and RDF, create class diagram justly without special diagram generation about WIDL document.

(4) Code Generator

Create component diagram from each class diagram that is created from XML DTD and document instance and C++ code that is object-oriented code about each component.

4.2 Application Result

Do document instance by input with DTD by this algorithm and examine the application result.

4.2.1 Use Case Diagram

Various application of XML distinguishes to each use case of UML and handles.

It is same with figure 2.



Fig. 2. Use Case Diagram

4.2.2 DTD Class Diagram

In this study does generation class diagram to input XML DTD.

(1) XML DTD

Used WIDL by a example of DTD, and WIDL DTD is same as following.

```

-----
<!ELEMENT WIDL (SERVICE | BINDING )*>
<!ATTLIST WIDL NAME CDATA #IMPLIED VERSION (1.0|2.0|... ) "2.0"
  TEMPLATE CDATA #IMPLIED BASEURL CDATA #IMPLIED
OBJMODEL(wmdom|... )"wmdom*6" >
<!ELEMENT SERVICE EMPTY>
<!ATTLIST SERVICE NAME CDATA #REQUIRED URL CDATA #REQUIRED
METHOD(Get|Post)
  "Get" INPUT CDATA #IMPLIED OUTPUT CDATA #IMPLIED AUTHUSER CDATA #IMPLIED
  AUTHPASS CDATA #IMPLIED TIMEOUT CDATA #IMPLIED RETRIES CDATA #IMPLIED >
<!ELEMENT BINDING (VARIABLE | CONDITION | REGION)* >
<!ATTLIST BINDING NAME CDATA #REQUIRED TYPE (INPUT|OUTPUT) "OUPUT" >
<!ELEMENT VARIABLE EMPTY>
  NAME CDATA #REQUIRED FORNAME CDATA #REQUIRED
  TYPE (String | String[] | String[][] ) "String" USAGE
(Default | Header | Internal) "Function" REFERENCE CDATA #IMPLIED
  VALUE CDATA #IMPLIED MASK CDATA #IMPLIED NULLOK #BOOLEAN >
<!ELEMENT CONDITION EMPTY>
<!ATTLIST CONDITION TYPE (Success|Failure|Retry) "Success"
  REF CDATA #REQUIRED MATCH CDATA #REQUIRED
  REBIND CDATA #IMPLIED SERVICE CDATA #IMPLIED
  REASONREF CDATA #IMPLIED REASONTEXT CDATA #IMPLIED
  WAIT CDATA #IMPLIED RETRIES CDATA #IMPLIED >
<!ELEMENT REGION EMPTY>
<!ATTLIST REGION NAME CDATA #REQUIRED START CDATA #REQUIRED
END CDATA #REQUIRED >
-----

```

(2) DTD parsing Table

Table 5 and table 6 are represented element and attribute table from parsing result

Table 5. Parsing element table

element name	connector		element contents	occurrence indicator			exception contents
	,			*	+	?	
WIDL	0	1	SERVICE	1	0	0	0
			BINDING				
SERVICE	0	1	EMPTY	0	0	0	0
BINDING	0	0	VARIABLE	1	0	0	0
			CONDITION				
			REGION				
VARIABLE	0	0	EMPTY	0	0	0	0
CONDITION	0	0	EMPTY	0	0	0	0
REGION	0	0	EMPTY	0	0	0	0

• Element table

Element table compose of element name, connector, element contents, occurrence indicator, above WIDL document DTD, parsing element table is the following

• Attribute table

Attribute table compose of element type, attribute name, attribute value and default value. Above WIDL document DTD, attribute table is the following.

Table 6. Parsing attribute table

element type(Name)	attribute Name	attribute Value or List	default value or reserved word
WIDL	NAME	CDATA	Implied
	VERSION	(1,0 2,0 ...)	2,0
	TEMPLATE	CDATA	Implied
	BASEURL	CDATA	Implied
	OBJMODEL	(wmdoml...)	Wmdom
SERVICE	NAME	CDATA	=# REQUIRE
	URL	CDATA	=# REQUIRE
	METHOD	(Get Post)	Get
	INPUT	CDATA	Implied
	OUTPUT	CDATA	Implied
	AUTHUSER	CDATA	Implied
	AUTHPASS	CDATA	Implied
	TIMEOUT	CDATA	Implied
RETRIES	CDATA	Implied	
BINDING	NAME	CDATA	=# REQUIRE
	TYPE	INPUT OUTPUT	OUTPUT
VARIABLE	NAME	CDATA	=# REQUIRE
	FORNAME	CDATA	=# REQUIRE
	TYPE	(S S J S J)	String

Table 6. (Continued)

element type(Name)	attribute Name	attribute Value or List	default value or reserved word
	REFERENCE	CDATA	Implied
	USAGE	DefaultHeaderInternal	Function
	REFERENCE	CDATA	Implied
	VALUE	CDATA	Implied
	MASK	CDATA	Implied
	NULLOK	CDATA	Implied
CONDITION	TYPE	SuccessFailureRetry	Success
	REF	CDATA	=# REQUIRE
	MATCH	CDATA	
	REBIND	CDATA	Implied
	SERVICE	CDATA	Implied
	REASONREF	CDATA	Implied
	REASONTEXT	CDATA	Implied
	TIMEOUT	CDATA	Implied
RETRIES	CDATA	Implied	
REGION	NAME	CDATA	=# REQUIRE
	START	CDATA	=# REQUIRE
	END	C	R

(3) DTD Class Diagram

Result that change DTD of (1) in UML class diagram is same with figure 3.

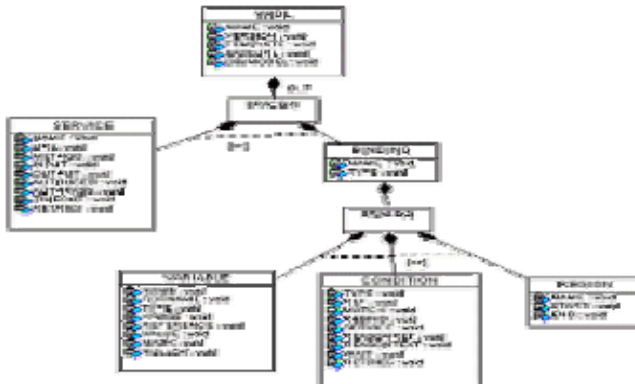


Fig. 3. DTD Class Diagram

4.2.3 Document Class Diagram

Generation class diagram and object-oriented code when did document instance that correspond to Web-Based XML application by input.

- (1) The parsing table of WIDL document

The following WIDL parsing table contain of tab name, attribute and it value.

Table 7. Parsing table of WIDL document

Tag name		Attribute	Value
WIDL		NAME	FedExShipping
		TEMPLATE	Shipping
		BASEURL	http://FedEx.com
		VERSION	2.0
SERVICE		NAME	TrackPackage
		METHOD	GET
		URL	/cgi-bin/tract_jt
		INPUT	TrackInput
		OUTPUT	TackOutput
BNDING(1)		NAME	TrackInput
		TYPE	INPUT
	VARLABLE(1)	NAME	TrackingNum
		TYPE	String
		FORMNAME	Trk_num
	VARLABLE(2)	NAME	DestCountry
		TYPE	String
		FORMNAME	dest_cntry
	VARLABLE(3)	NAME	ShipDate
		TYPE	String
FORMNAME		ship_data	
BNDING(1)		NAME	TrackOutput
		TYPE	OUTPUT
	CONDITION(1)	TYPE	FAILURE
		REFERENCE	doc.p[0].text
		MATCH	FedEx Warning Form
		REASONREF	doc.p[0].text['&*']
	CONDITION(2)	TYPE	SUCCESS
		REFERENCE	doc.title[0].text
		MATCH	FedEx Airbill
		REASONREF	doc.p[1].value
	CONDITION(4)	NAME	disposition
		TYPE	String
		REFERENCE	doc.h[3].value
		MASK	\$*
	CONDITION(5)	NAME	deliveredOn
		TYPE	String
		REFERENCE	Doc.h[5].value
		MASK	%%*\$
	CONDITION(6)	NAME	deliveredTo
		TYPE	String
		REFERENCE	doc.h[7].value
		MASK	*;

(2) Document Instance Class Diagram

Is same with figure 4 if create UML class diagram because do by input (1).



Fig. 4. Document Instance Class Diagram

Specific picture about class "BINDING(1)" and "BINDING(2)" is same with each figure 5, figure 6 in figure 4.

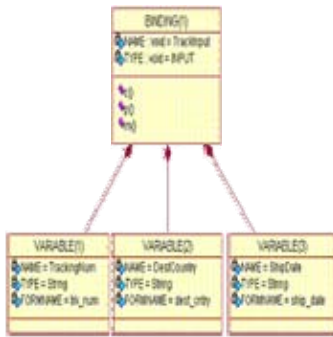


Fig. 5. "Binding(1)" of Class Diagram

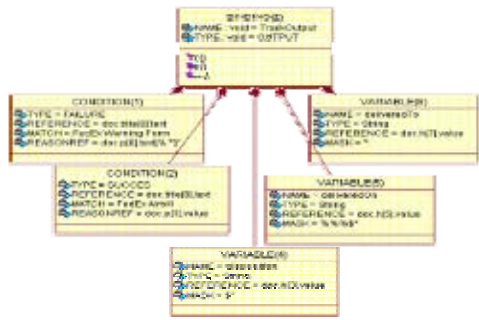


Fig. 6. "BINDING(2)" of Class Diagram

(4) Document Instance Object-Oriented Code Component diagram about class WIDL of figure 4 is same with figure 7, and this paper used C++ cord. File WIDL.cpp has compile relativity about file WIDL.h, and WIDL.h has relativity about SERVICE.h. Present code WIDL.cpp and WIDL.h about WIDL class in postscript.

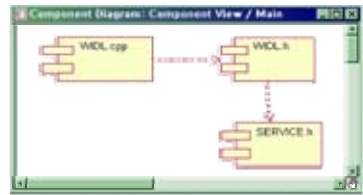


Fig. 7. "WIDL" Component Diagram of Class

5 Conclusion and Further Research Task

This paper proposed algorithm and system to integrate SMIL that is XML's Web-Based application, RDF, WIDL and do object modeling.

Defined rule and member function of each class that map in UML class diagram from XML each application for this.

Therefore, because structure analysis of XML document is easy by in this study, that document developer is various easily for XML document instance create can .

Also, inputting Web-Based XML DTD or document instance object modeling and code because is gotten database designer without necessity to analyze kind of tag or grammar by XML application schema create can .

Most sense of this study is that become base in document management that is Web-Based XML's object-oriented because sense can generation easily object-oriented schema.

Further Research task knows first Web-Based XML application only just generation XML DTD diagram and document instance diagram that integrate all other applications. Second, generation schema by each OODBMS kind automatic movement based on this.

References

1. Natanya Pitts-Moultis, Cheryl Kirk, "XML Black Book", The Coriolis Group Inc., 1999.
2. W3C, "Resource Description Framework(RDF) Model and Syntax Specification", August 1998, <http://www.w3.org/TR/1998/WD-rdf-syntax-19980819/>.
3. W3C, "Synchronized Multimedia Integration Language(SMIL) 1.0 Specification," W3C, June 1998, <http://www.w3.org/TR/1998/REC-smil-19980615/>.
4. "Automating the with WIDL", <http://xml.webmethods.com.technology/Automating.html>.
5. W3C, "Web Interface Definition Language (WIDL)", September 1997, <http://www.w3.org/TR/NOTE-widl-970922>.
7. "WIDL", <http://turtle.ee.ncku.edu.tw/~fencer/WIDL/>
8. WIDL.HTM.
9. Y-Ha, YJ-Hwang, YS-Kim, "Mapping algorithm of UML class diagram that use SGML DTD", Journal of KISS(B), Volume 26, number 4, pp. 508-520, 1999. 4.
10. WS-Chae, Y-Ha, YS-Kim, "XML document structure Diagramming that use UML class diagram", The Transactions of KIPS, Volume6, number 10, pp. 2670-2679, 1999. 10.
11. GM-Lee, Y-Ha, YS-Kim, "By RDF schema UML Class Diagram conversion", The Transactions of KIPS, Volume 7, number 1, pp. 29-40, 2000. 1.
12. WS-Chae, Y-Ha, YS-Kim, "SMIL document synchronization that use UML use case and sequence Diagram", Journal of KISS(C), Volume 27, number 4, pp. 357-369, 2000. 4.

Model of Generating SMIL Document Using Temporal Scripts of Animation Component*

Chun-Sik Yoo¹, He-Jue Eun¹, Yong-Sung Kim¹, and Jang-Sup Shim²

¹Division of Electronics and Information Engineering, Chonbuk National University,
664-14 Iga Duckjin-Dong Duckjin-Gu Jeonju, 561-756, Republic of Korea
{csyoo, hjeun, yskim}@chonbuk.ac.kr

²Institute of Information Technology Assessment 52, Eoeun-dong,
Yuseong-gu, Daejeon-si, 305-333, Republic of Korea
sjs@iita.re.kr

Abstract. The SMIL specification that is recently approved by the W3C and is meant to help deliver multimedia contents to the Web, is widely used these days and they have continuously emerged tools or software related with that. In this paper, we propose a system to convert temporal scripts of RASP that is an experimental toolkit for computer animation that promotes interaction-based programming over time into a SMIL document. For making better use of SMIL documents, we can improve reusability of animation components. the main contribution of this paper is that it verifies the sequence diagram generated for synchronization of SMIL documents by reconvertng SMIL from UML sequence diagram.

1 Introduction

XML (eXtensible Markup Language) has the flexibility to define elements, attributes, and entities according to a specific application purpose. Depending on the user's objective, these applications can distinguish by Web and Internet application, meta-data and storing application, multimedia application etc. In particular, XML based multimedia application uses XML language and syntax to present information such as graphics, video and digitalized language in the Web[1]. SMIL (Synchronized Multimedia Integration Language), PGML (Precision Graphics Markup Language), JSML (Java Speech Markup Language) are representative examples. SMIL, the W3C recommendation, is an XML application that integrates individual multimedia objects by synchronizing multimedia presentations. It makes multimedia presentations such as Web TV[2]. The functions of SMIL are as follows. First, it describes the temporal action of the presentation. Second, it describes the arrangement of the presentation in a display. Third, it combines hyperlinks with the media object[3]. Currently SMIL documents are increasing, and SMIL related software or tools are being developed vigorously. Therefore, the possibility of SMIL documents may rise. On the other hand, the RASP (Robotics Animation Simulation Platform) tool kit is a representative example that is developed and used on the software reuse side. When we develop visual simulation, this defined common structure or set is used to make investigations

* This work was supported by Korea Research Foundation Grant (KRF-2004-042-D00168).

convenient. It is based on the object-oriented principle and various simulation techniques and it was made in C++. [4]. So, when we visualize the script, it presents the temporal relation of the animation components in the RASP tool kit, as a UML sequence diagram. And we create SMIL documents using this diagram, regenerate animation components to SMIL documents and maximize the reusability of these animation components.

The purpose of this study is to generate SMIL documents from sequence diagrams as a verification of algorithms[5] for the synchronization of SMIL documents with existing study.

2 Related Works

There is a concentrated interest in software reuse in the computer graphics field. When an animation scene is visualized, code and design are reused, to reduce time, effort, and expense. But because it is not easy to animate interaction between components which are changing most tools support limited relation.

It was recently suggested that a new method named RASP tool kit had solved this. The RASP tool kit is a tool which composes and controls interaction hierarchically, helps to compose time-varying interaction and to properly reuse that interaction at each step. Here, time-varying interaction increases interaction that can be reused by temporal attributes. That is, the attribute prescribes in what condition - such as 'when', 'how often' – the interaction occurs and the interaction establishes the relation between the components which use this attribute[6].

On the other hand, use case diagrams and sequence diagrams are presentation methods for the temporal synchronization of documents[5]. They extract objects from a SMIL document Using use case diagrams, sequence diagrams, cooperation diagrams and logical view class diagrams of UML use case view. Then they present a synchronization and cooperation relation between them. It is object modeling for logical relations through class diagrams. Therefore, this study proposes an algorithm to create a SMIL document from a sequence diagram as a verification for the UML sequence diagram from the SMIL document.

3 RASP, UML, SMIL Document

We explain the RASP, UML diagrams, and the basic tag of SMIL documents.

3.1 RASP Tool Kit

RASP, an experimental tool kit for computer animation, is based on interaction programming, It consists of tools for geometrical model building, rendering, and animating. Because it supports interaction according to time that can be reused, it promotes reuse. It uses hierarchic structure in order to systematically connect components according to time and it makes it easy to decide what component, when, and how often to do an interaction.

3.1.1 Primitive

The primitive hierarchical structure is the as the one shown in Figure 1. Events, management for one interaction, forms time binding to communicate between components. Activities, management for interaction that form behaviors, limit temporal intervals to control interaction by how often they occur and in which sequence. TimingActs and Processions gather activity that form temporal script. The temporal script decides how the action connects and when the action happens.

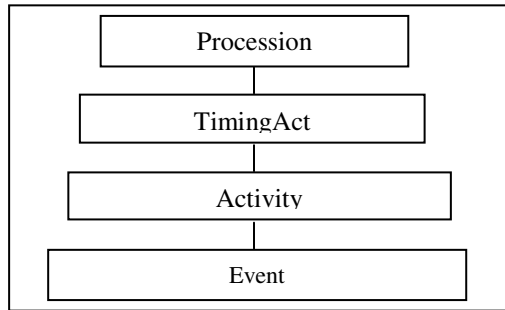


Fig. 1. Primitive Hierarchical Structure

3.1.2 Reuse

The reuse of software is accessed differently according to the primitive hierarchy. There are fine-grain, medium-grain, and coarse-grain. Fine-grain is a reuse which is related in events. Medium-grain is a reuse which is related in activities and coarse-grain is a reuse which is related in temporal scripts. The purpose of coarse-grain reuse, which is used in this study, is not a reuse of interactions or behavior but a reuse of sequence.

3.2 UML

Use case diagrams, sequence diagrams, and UML diagrams that apply to this study, can be explained as follows.

3.2.1 Use Case Diagram

The use case diagram presents relevance between external behavior and Use case that is a system offered function. A use case presents one of the system offered functions, it can insert sequence diagrams, cooperation diagrams, class diagrams etc.

The notation of a use case diagram is a graph that consists of a set of external users and use cases, and the relations between them. This has the advantage that it naturally derives the object from user requirement and communicates with the user in standardized diagram form[7].

The following table presents components of use case diagrams and gives an explanation of them.

3.2.2 Sequence Diagram

Sequence diagram focuses on the sequence of the message flowing between other objects. The notation makes 2 axes, the vertical axis represents the current of time

Table 1. Components of Use Case Diagram

Components	Explanation
Actor	System and subsystem, or external user, process etc. that interacts with class
Use Case	A unit of relative behaviour that does not present the internal structure of the system

and the horizontal axis presents the relevant object. The Object appears in a rectangular form, and the name of the object draws underline, and the lifeline of the object appears in a dotted perpendicular line. Interaction between objects is attained through the flowing of messages. The message becomes a horizontal line between the lifeline of the object and the focus of control presents the time zone, the object acts in a long rectangle.

The following presents components of a sequence diagram and an explanation of them[8].

Table 2. Components of sequence diagram

Components	Explanation	
Event identifier	Identifier of which event the message refers to	
Time constraint	Time display of relevant time between events	
Message	Peer-to-Peer	One object sends a special message to only one object
	Broadcast	Message that is sent by one object to more than one object at the same time

3.3 SMIL Document

SMIL, a XML based language, can represent temporal synchro relation between multimedia data that is untreated in HTML[9].

A SMIL document consists of a <head> part and a <body> tag part inside <smil>, </ Smil> tag. The following is to explain about detailed tags.

3.3.1 <head> Tag

This is a tag about information that is not presented according to sequence. It includes meta element and <switch> or <layout> tags[3].

1) <layout> tag

This decides what form element is put in the <body> of document.

2) <region> tag

This controls position, size etc.. of the media object element

3) <switch> tag

This prescribes a set of preferential elements and selects one of several elements. This tag is available in the <body>.

3.3.2 <body> Tag

This is an element which includes information connected with the temporal connection behavior of the document[9].

1) media tag

This is an element that presents the media object. <ref>, <animation>, <audio>, , <video>, <text>, <textstream> etc. belonging to the media tag. This study creates an <animation> tag among them.

2) synchronization tag

This is used for temporal synchronization. <par> tag makes the child of element overlapping happen at the same time and <seq> tag makes the element' child have temporal sequence.

3) hyperlink tag

<anchor> tag and <a> tag are connected with hyperlink. <a> tag is similar to the <a> tag of HTML and fixes the whole media resource from start time to ending time so that the link may be possible. <anchor> tag, hyperlink element such as <a> tag, can be designated anywhere on the screen during the defined period[10].

4 SMIL Document Generating System

This chapter presents a SMIL document generating system, an algorithm for that system and the result of its application when temporal script related in animation component is entered, First, a sequence diagram of UML is created from the temporal script about animation script. Second, a SMIL document is generated from the sequence diagram of UML.

4.1 System Configuration Diagram

First, the whole system configuration in this paper is the same as Figure 2, and the function for each component is as follows.

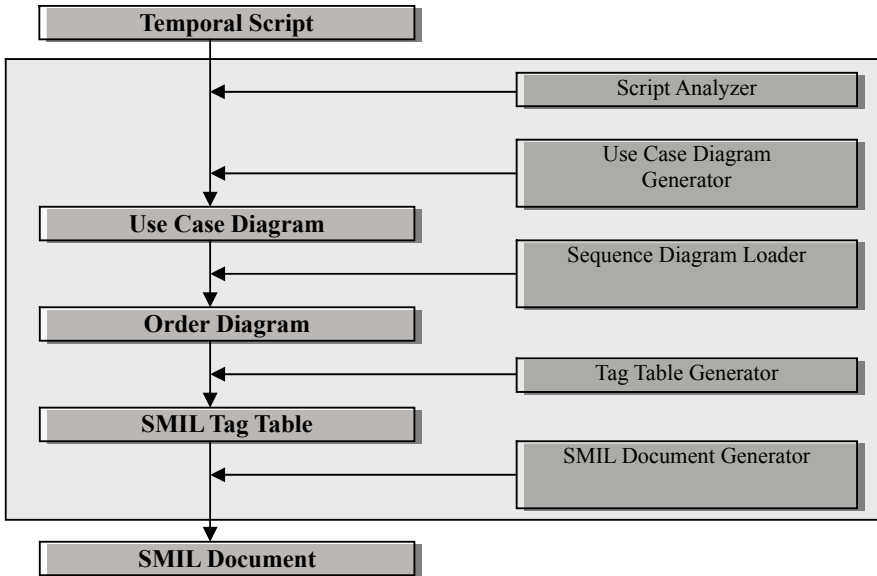


Fig. 2. SMIL Document Generating System Diagram

1) Script Analyzer

The script analyzer translates the temporal relation by following the message mapping table.

Table 3. Sequence Diagram Message Mapping Table about Relation of Temporal Script

Relation	Message
MEETS	seq()
DELIMITS	par()
STARTS	par()
STOPS	$\{e_{iend}-e_{jend}=0\}$ only, e_i, e_j are event identifier
TimingAct(Object,begin,end)	$\{e_{iend}-e_{ibegin}\}$
TimingAct(Object i ,begin,end) TimingAct(Object j ,begin,end)	$\{e_{jbegin}-e_{iend}\}$

The results of temporal script analysis of the next 5 examples by the above table are as follows.

Example 1) and example 2) are examples connected with the message. The following is an example of seq().

Example 1) ObjectB→setRel(MEETS, ObjectC);

Table 4. Script analysis Table of Example 1

object		Message
begin	End	
ObjectB	ObjectC	seq()

The following is an example of par ().

Example 2) ObjectC→setRel(DELIMITS, ObjectE);

Table 5. Script Analysis Table of Example 2

object		Message
begin	End	
ObjectC	ObjectE	par()

The following is an example of constraints. The constraints to set the ending time between 2 objects are as follows.

Example 3) ObjectF→setRel(STOPS, ObjectD);

Table 6. Script Analysis Table of Example3

object	event identifier		constraints
	begin	end	
ObjectF	e_{1begin}	e_{1end}	$\{e_{1end}-e_{2end}=0\}$
ObjectD	e_{2begin}	e_{2end}	

The following is marking live time of a object by constraints.

Example 4) proc→addTimingAct(ObjectA,1,10);

Table 7. Script Analysis Table of Example 4

object	event identifier		constraints
	begin	end	
ObjectA	e_{begin}	e_{end}	$\{e_{end}-e_{begin}=9\}$

The last following example presents time lags between two objects.

Example 5) proc→addTimingAct(ObjectA,1,10);
 proc→addTimingAct(ObjectB,30,40);

Table 8. Script Analysis Table of Example 5

object	event identifier		constraints
	begin	end	
ObjectA	e_{1begin}	e_{1end}	$\{e_{2begin}-e_{1end}=20\}$
ObjectB	e_{2begin}	e_{2end}	

2) Use Case Diagram Generator

This creates a use case diagram with a diagram generation algorithm and use case to create a user and SMIL document.

3) Sequence Diagram Loader

The inserts a sequence diagram about use case of a use case diagram using parsed messages which are made by a script analyzer.

4) Tag Table Generator

This creates a SMIL tag table extracting tags from the sequence diagram. A tag table distinguishes synchronization, media, and hyperlink tags.

5) SMIL Document Generator

This creates SMIL document instance from the SMIL tag table input.

Basically, the declaration statement, comment statement, begin tag and end tag of <smil> and <body> are created from the document instance.

4.2 Algorithm

The following is an main algorithm that finally creates a SMIL document through a sequence diagram, and tag table which is made from temporal script input.

```

input: temporal script
output : SMIL document
begin
// script analysis algorithm
while not(script)

parsing object and relation
if(relation)
    allocate to message
// use case diagram generation algorithm
generate actor
generate use case
establish actor and user case relation
// generate SMIL document from SMIL tag table and sequence diagram
create sequence diagram
create SMIL tag table
generate SMIL document from SMIL tag table
End

```

4.3 Application Result

The following is a sequence diagram, tag table, and SMIL document from temporal script input.

4.3.1 Temporal Script

The temporal script decides how the action connects and when the action happens.

```

(1) ObjectB→setRel(MEETS,ObjectC);
(2) ObjectC→setRel(MEETS,ObjectF);
(3) ObjectC→setRel(DELIMITS,ObjectE);
(4) ObjectC→setRel(MEETS,ObjectD);
(5) ObjectF→setRel(STOPS,ObjectD);
    add timingActs to procession
(6) Procession *proc = new procession();
(7) proc→addTimingAct(ObjectA,1,10);
(8) proc→addTimingAct(ObjectB,30,40);

```

4.3.2 Diagram

A diagram form is needed to change the above temporal script to SMIL document form. This paper uses UML use case diagrams and sequence diagrams.

1) Use Case Diagram

Figure 3 presents an actor interacting with a SMIL document generation use case.



Fig. 3. SMIL document generation use case diagram

2) Sequence diagram

Figure 4 presents a sequence diagram inserted into a SMIL document generation use case. Sequence diagram presents objects, messages between objects, and constraints etc.

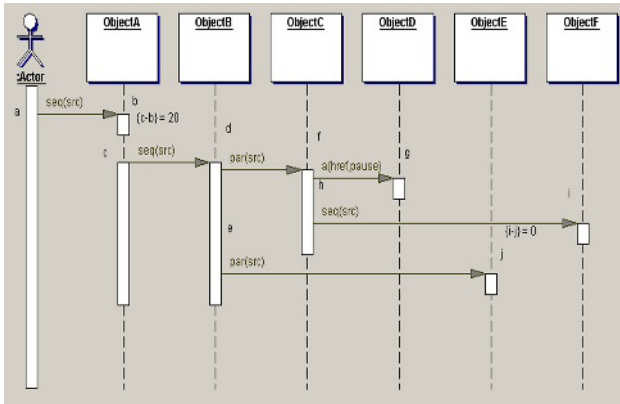


Fig. 4. SMIL Document Generation Sequence Diagram

4.3.3 Tag Table

A tag table is created for the SMIL tag dividing synchronization tag, hyperlink tag, and media object from sequence diagram.

Table 9. SMIL tag table

Synchroniza tion Tag	Mediaobject			
	Synchroniza tion Tag	Media Object	Hyperlink Tag	Media Object
Seq	ObjectA			
	ObjectB			
	Par	ObjectC	a	ObjectF
	ObjectE			
ObjectF				

4.3.4 SMIL Document

A SMIL document generated from Tag Table and Sequence diagram.

```

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE smil PUBLIC "-//W3C//DTD
SMIL1.0//EN" "http://www.w3.org/TR/REC-
smil/SMIL10.dtd">
<smil>
  <body>
    <seq>
      <animation src="ObjectA", begin=1, end=10>
    <seq>
      <animation src="ObjectB" begin=30, end=40>
      <par>
        <seq>
          <par>
            <a href="D", show="pause">
              <animation src="ObjectC"> </a>
            <animation src="ObjectE">
          </par>
          <animation src="ObjectF">
        </seq>
      </par>
    </seq>
  </body>
</smil>

```

5 Conclusion and Further Study

SMIL, an XML application to create a multimedia presentation using the Web, was proposed and is now used widely. Related software such as parser, editor, player etc. are being developed vigorously. So, components that are used in computer animation are necessary to manage a SMIL document.

Therefore, this study proposed a system that changes the temporal script of RASP, a computer animation tool kit, into a SMIL document form in order to do interaction programming by the flowing of time. This system creates SMIL documents from UML sequence diagrams. So it has a big significance in verifying sequence diagrams which are generated for synchronization of a SMIL document.

The next research task is to make a management system that generates SMIL documents from components including temporal concept and various tools for computer animation, and to integrate them.

References

1. Natanya Pitts-Moultis, Cheryl Kirk, "XML Black Book", The Coriolis Group Inc., 1999.
2. written by Elliotte Rusty Harold, translated by Kim young kwon, "XML Bible", information culture company, 1999
3. <http://my.dreamwiz.com/gojirael/html/smil10spec/smil10spec.html>
4. RASP-Robotics and Animation Simulation Platform,<http://www.cs.ubc.ca/spider/gslee/RASP/rasp.html>
5. Chai won-seok, Ha yan, Kim yong-sung, "SMIL document synchronization using UML use case and sequence diagram", KISS journal(software and application), Volume 27, Number 4, 2000. 4.
6. Gene S. Lee, "Reusable Interactions for Animation", The 5th International Conference on Software Reuse, June 1998.
7. Bruce Power Douglass, "Real-Time UML Developing Efficient Objects for Embedded Systems", Addison-Wesley Longman Inc., 1998.
8. James Rumbaugh, Ivar Jacobson, Grady Booch, "The unified modeling language reference manual", Addison Wesley Longman Inc., 1999.
9. W3C, "Synchronized Multimedia Integration Language(SMIL) 1.0 Specification," W3C, June 1998, <http://www.w3.org/TR/1998/REC-smil-1998-0615/>.
10. M. J. Perez-Iuque, T. D. C Little, "A Temporal Preference Framework for Multimedia Synchronization, "IEEE Journal on Select Areas in Communications, Vol. 14, No. 1m pp. 36-51, 1996.

Marginal Bone Destructions in Dental Radiography Using Multi-template Based on Internet Services

Yonghak Ahn¹ and Oksam Chae²

¹ Dept. of Information System Eng., Hansung Univ., Korea
yohan1110@paran.com

² Dept. of Computer Eng., Kyunghee Univ., Korea

Abstract. This paper proposes a method to automate image alignment and detect marginal bone destructions, based on subtraction radiography for dental radiographic images necessary for Internet-based dental PACS. The proposed method enables a quick and precise detection of marginal bone destructions around teeth including implant through multi-template matching in reference to Region of Interest (ROI) obtained from applicable teeth using information about their geometric forms to solve problems single-template matching is exposed to. Actually, the performance test showed that it was possible not only to quickly and precisely detect marginal bone destructions around teeth, but also to get more objective and quantitative results through the proposed method.

1 Introduction

As one of triggering subsequent methodologies to analyze and translate various dental X-ray images, subtraction radiography that refers to a technique in which two pieces of dental X-ray images taken at different times are overlapped to secure a standard of judgment for treatments and diagnoses by using the difference between them, is used for examining and researching most of dental diseases [1-2].

Subtraction radiography for dental radiographic images covered in this study aims to promptly identify and treat marginal bone losses seen around natural teeth or implant. However, with a recent increase in users using digitalized X-ray images, there comes to be a need for researching a way to apply the existing film-based subtraction radiography to digitalized images [3]. It can be largely said that the detection of marginal bone destructions based on subtraction radiography goes through two steps including image alignment and the detection of marginal bone destructions. So-far researches to automate image alignment for subtraction radiography includes two methods: one of them is a method where a dental implant is fixed into one's teeth, followed by the detection of its edge for the image alignment of ROI [4], and the other is a method where the size of an image is adjusted a fourth time as large as its original to overcome the shortcomings of image alignment [5].

However, they have problems as concern the speed of calculation or its accuracy since it engages the alignment of entire images. And it's difficult to maintain image information when distortion parameter for image alignment is set, related to accuracy because the image alignment involves entire image.

In general, there are two types of approaches for the detection of peri-implant marginal bone destructions: The one is to carry out subtraction after a user selects a reference point and then detects a straight segment to align images [6]. The other is to measure bone resorption by detecting the precise contour of implant after a user has set an optimal threshold value [7]. In the case of them, there are so many of calculations for accurate matching according to a change in position or orientation, along with a difficulty in matching owing to global template matching. If all large-patterned images with their own distortion are matched, it's difficult to find out an accurate matching point. Even if it's been found out, the farther from the central point, the larger an error resulting from such distortion.

To minimize those problems above, this paper adopting domain knowledge that such marginal destructions around teeth as parodontitis are limited to a specific region, proposes a method for accurate matching through multi-template matching.

2 Detection of Marginal Destructions

The existing methods from the central point matched in entire distorted images, the larger the resulting error because those researches have them entire aligned. On top of that, a change in position and orientation causes an increase in the calculation amount. Figure 1, an example of matching using global template, shows the difficulty in finding out a generally precise matching point. Since, even if a matching point has been found out, the farther from it, the larger the resulting error, it's very difficult to detect marginal destructions after image alignment. The calculation amount according to a change in orientation and position to find out such matching point gets larger in proportion to the image size.

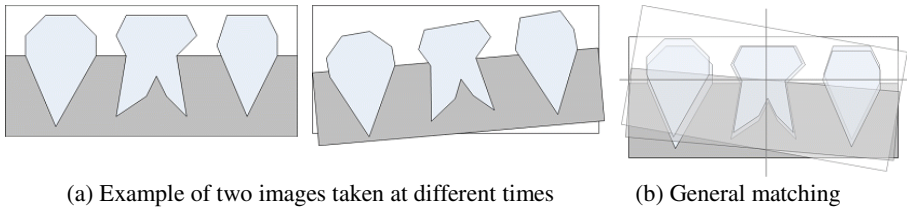


Fig. 1. Problems of matching in general

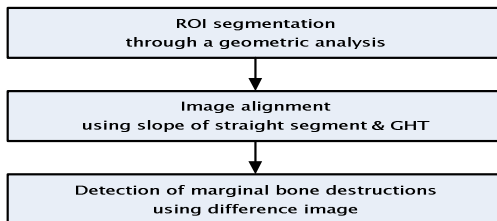


Fig. 2. The proposed method

Another problem is that, since there is a slight change in the gray level of points around a region, starting from which it can be said to be bone tissues (i.e., gum) in an X-ray image to detect such marginal destructions around teeth as parodontitis after image alignment, it's difficult to obtain information about an applicable position using the existing image analysis algorithms that identify the region in reference to the difference of a relatively larger gray level, compared with that of surrounding points.

2.1 ROI Segmentation

The detection of teeth that serves as a judgment reference is prioritized to any others, starting from detecting a straight segment characterizing teeth which contain information about the left and right range of the gum surrounding teeth including the location of teeth in themselves.

Most of straight segments of implant are perpendicular. Therefore, the values of X-profile are first obtained with use of horizontal scan lines of images to be scanned. The position at which the largest of measured X-profile point variations is located is defined as a boundary point of implant. Those straight segments of implant can be found out by connecting multiple boundary points derived out from multiple X-profiles, multiple boundary points can be obtained.

However, when the difference among point variations from the gum to implant is almost invisible, a total of summated value of 5 points including upper 2 points and lower 2 points, respectively, is considered as a single X-profile value, so that such difference are large enough. So, a use of upper and lower 15 points, respectively, would enable you to get 6 sets of X-profile values. Of point variations measured among them, the maximal value and the minimal one are used to obtain a straight segment of implant. If you use the average of the slopes of lines connecting those points and one of the points, you can obtain a straight line for implant as shown in Figure 3.

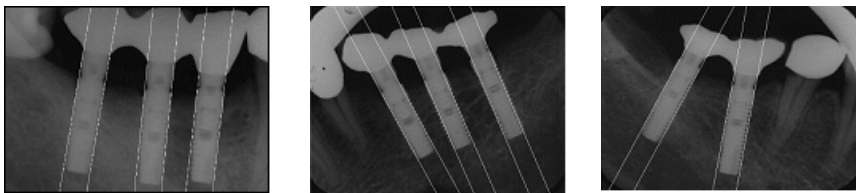


Fig. 3. Detection of straight segment in implant

Different from implant, it's very difficult to detect a straight segment using X-profile values of natural teeth because the difference among point variations around their gum is almost invisible. To solve such problem, this study detects the contour characterizing natural teeth and then the resulting straight segment.

This paper uses Canny edge detection algorithm [3] to detect an accurate contour of teeth. The proposed method uses hysteresis threshold to detect the contour of teeth. First, a part of the contour is detected with use of lower threshold values. And then

edges from edges made by those lower values are detected with a basis of higher threshold values. An excessive connection of detected edges is prevented by limiting them in their number with use of edge segments detected through lower threshold values. It means that teeth tend to be perpendicular with gradient magnitude in a regular direction. Based on such a geometric analysis of teeth, edges within a specific range are selected, and the contour of teeth as in Figure 4 is detected.

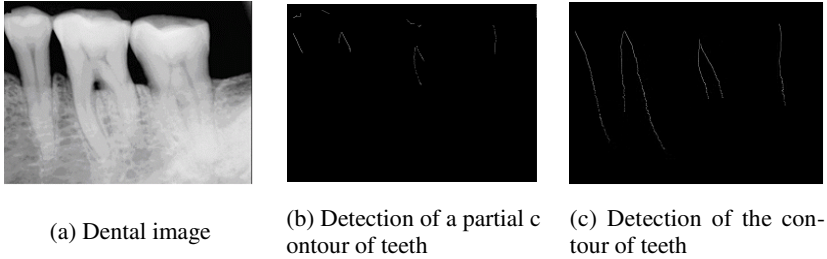


Fig. 4. Results of detecting the contour of teeth

If you use a calculated slope and a point as shown in Equation (1) together with the detected contour, a straight segment of teeth as shown in Figure 5 can be detected:

There is a case where it's difficult to detect the contour because its value of points is very similar to that of the gum surrounding them. In that case, line fitting carried out in accordance with information about the contour of teeth may be inaccurate. Considering that, of such information, the important thing for setting ROI is the region, starting from which it can be said to be the gum, namely “the lower part of teeth”, we made it possible to accurately detect that region by placing a high weight on the edge point for the lower part when line-fitting

$$\Delta = \frac{1}{n} \sum \left(\frac{y_i - y_{i+1}}{x_i - x_{i+1}} \times f_{weight}(w_i) \right) \tag{1}$$

Where Δ refers to the slope of a line with (x_i, y_i) meaning obtained coordinates, and $f_{weight}(w_i)$ is a weight for the slope. The weight is a value for line fitting of the contour of teeth.



Fig. 5. Detection of the straight segment of teeth

Since there is just a minute change in the value of points around the region in an X-ray image, starting from which it can be said to be the gum, it's very difficult to obtain information to detect a destructed region through the existing methods.

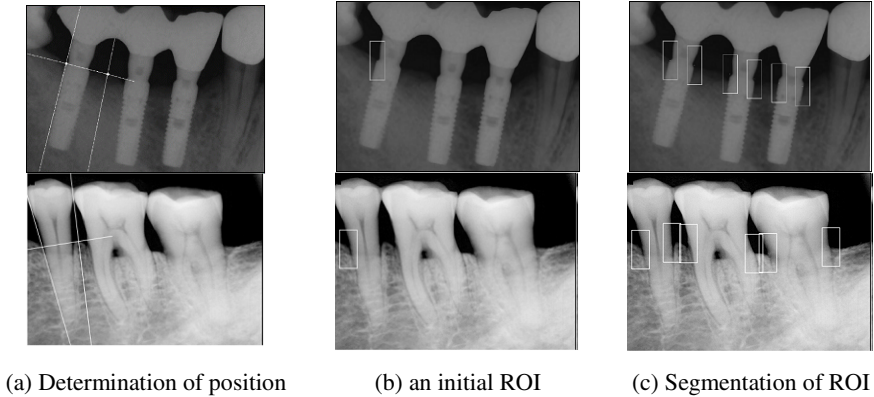


Fig. 6. Segmentation of ROI in implant & natural teeth

To get more reliable results, the summation method whose main purpose is to obtain ROI by identifying the starting region of the gum has to be carried out in accordance with the slope of a revolving image when it has revolved. For the purpose, the slope of a straight line vertically crossing a middle dental straight line obtained with use of already-obtained straight segments is calculated to summate the points corresponding to the vertical line along each point of the middle line.

A region below a summated average corresponds to the starting region of the gum. One-dimensional smoothing of the region results in an increase in the summated value around the starting region of the gum. Therefore, that region is considered the starting region of the gum. Then, ROI as shown in Figure 6 can be identified. The forgoing process goes on until partial images of all teeth have been secured.

2.2 Image Alignment

Image alignment that refers to a process to obtain reliable difference information about two images taken at different times aims for their precise matching by adjusting slight differences in the position and orientation of implant as shown in each of them.

Information about the contour of teeth already calculated is used to speed up alignment by reducing a possibility of image alignment. The calculation amount can be significantly reduced with help of such information because it offers a relatively high level of accuracy related to the orientation and position of teeth. The study adopts GHT[3]-based image matching method to detect an arbitrary object with use of the range of error and the orientation of teeth calculated from the two images.

In the proposed image alignment, edges are derived out from ROI of a model image to identify reference pattern. And then matching is carried out with use of GHT in a comparative image. To reduce the time taken for operation and heighten accuracy,

the range of accumulator is limited in reference to a calculated position and orientation including the range of their error.

When there is a revolution process to accommodate a revolving variation in the process of image alignment, a large-patterned single template as shown in Figure 7 is difficult to accurately match. The farther from the center, the larger the range of error becomes, even if it's possible.

On the other hand, if the pattern is small, an accurate matching and alignment is possible because the multi-template matching is applied only to an infected region, showing a significant difference in calculation amount.

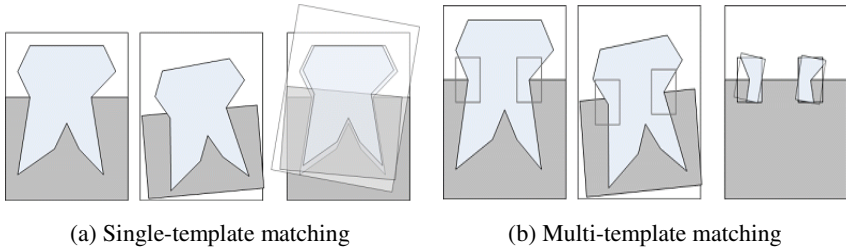


Fig. 7. Difference in matching according to the size of pattern

The proposed method uses an already obtained straight segment to cut down a comparative range of revolution for reducing the number as many times as which GHT is repeated, and to consider a mutual adjustment of the left and right in thickness due to such revolution. That is, since the revolution is limited to a range specified for the slope difference of the obtained straight segment, variations resulting from that revolution by each ROI can be independently applied, which implies that a more accurate matching is possible.

2.3 Detection of Marginal Destructions

After the alignment of ROI has been completed, difference image referring to a variation between two images has to be sought. It means an absolute value of the difference between aligned images as calculated in Equation (2):

$$sub(x, y)_{ROI} = |ROI(x, y)_{input1} - ROI(x, y)_{input2}| \tag{2}$$

where (x, y) refers to each coordinate, and $ROI_{input1}(x, y)$ and $ROI_{input2}(x, y)$ means ROI segmented in the input images.

The region with destructions shows a high level of difference image. However, their variations in difference image are so tiny because a region with marginal destructions around the gum is darkened on an X-ray image. So, it's almost impossible to identify marginal destructions around the gum with use of a general thresholding method. An application of a single global threshold value for thresholding may make the surrounding erroneous pieces of information detected more definitely rather than actual marginal destructions. To solve such problem, this study proposes a local

thresholding method based on multi-template matching which can reflect each ROI status for difference images obtained by each of identified ROI.

In the proposed method, local threshold values are sought to identify the gum, based on information about its contour approximately calculated in the process of analyzing the dental structure. To detect such marginal destructions as peri-implantitis, threshold values containing information about intensity of the gum or its background are used. Those threshold values is applied for their thresholding after they're applied to difference image as calculated in Equation (3):

$$g(x, y) = \begin{cases} 1 & \text{if } sub_{ROI}(x, y) > T_i \\ 0 & \text{if } sub_{ROI}(x, y) \leq T_i \end{cases} \quad (3)$$

where $sub_{ROI}(x, y)$ refers to difference image obtained from ROI, T_i means a calculated i -th local threshold value with $g(x, y)$ meaning thresholding image.

Different from a method using global threshold values, since a limitation of probing area and a determination of threshold values based on geometric data are applied to such region as is exposed to, for example, peri-implantitis, an unnecessary calculation or improper report can be omitted or prevented. Of regions segmented like this, similar regions are mutually merged and their point values are labeled to quantify each area and girth.

3 Experiments and Results

It was implemented with use of general PC and widely-used OS "Windows 2000." A development tool to implement an algorithm is a image processing algorithm development tool "MTES" [3]. For the method, the one group of 15 patients with implant and the other group of 8 patients suffering from parodontitis had X-ray images of their implants and natural teeth, respectively, taken.

To compare the accuracy of image alignment, RMS [4] was used. RMS refers to a method to measure the accuracy of image alignment with use of intensity difference between two images. If image alignment has been completely carried out, the resulting value points to "0". As a result of measuring the accuracy of image alignment in reference to 10 pairs dental images taken from the patients, the method proposed in Figure 8 was more accurate than the existing methods.

The existing methods involve all images for their alignment. So, it's very difficult to detect an accurate matching point due to the differences attributed to variability in such input environments as a patient's physical position or the solid-geometric angle of central beam of X-ray applied to a subject. On the other hand, in the proposed method, since ROI for image alignment is identified by finding out a relative position of marginal alveolar bone based on cemento-enamel junction or restoral crown margin, the accuracy for relatively small areas can be improved.

To obtain a test image showing marginal destructions found in an actually-digitalized dental radiographic image, we created in the set of two images taken from 10 patients suffering from parodontitis marginal destructions with a profile similar to that of an actual image within the infected region, which refers to the right and left bone resorption region.

Figure 9 shows a comparison of the proposed method with the existing methods in the detection of marginal destructions: The former is by far more accurate than the latter. The reason is that the latter shows a relatively larger noisy region than what

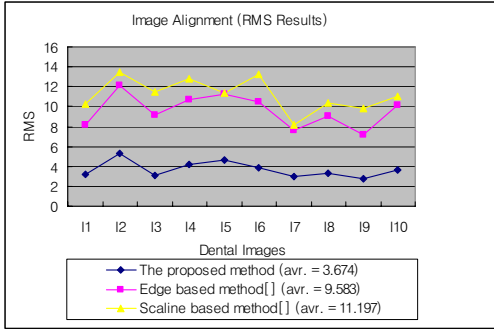


Fig. 8. RMS results

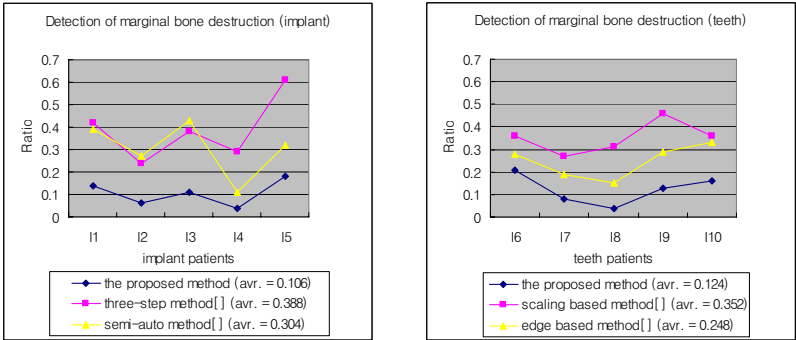


Fig. 9. Comparison of detection of marginal destructions

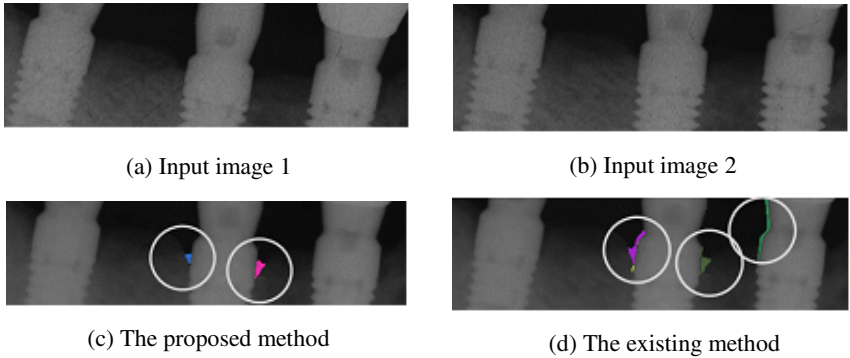


Fig. 10. Result of detecting marginal destructions (implant)

an actually-infected region would have since the surrounding noisy destructions are detected more larger than those of actual bone tissues because general matching and global threshold values are used in those methods, while the former can accurately-identify only marginal destructions around teeth because it uses local threshold values, targeting its own ROI. Figure 10 shows the results of detecting marginal destructions:

It is an example of the detection of marginal destruction around implant, showing 20 and 40 in the left and right variation of actual points, respectively. The point values detected in the proposed method are 21 and 42, while the existing methods showing 49 and 51.

4 Conclusion

This paper proposed a method to detect marginal bone destructions around teeth including implant and natural teeth, based on subtraction radiography for dental radiographic images necessary for Internet-based dental PACS.

The proposed method offered the accuracy and objectivity of results through solving such problems as the existing methods had because they involved all images. In particular, the method engaged itself in its own ROI while the existing methods used to show erroneous difference information because of a change in input environments, a misdirected X-ray scanner or any other conditions. Also, the proposed method addressed those problems by calculating local threshold values with use of multi-template matching during the identification of a region with marginal destructions to reflect locality by each ROI, which process the existing method using global threshold values couldn't handle.

References

1. Compend Contin Educ Dent, "Computerized Image Analysis in Density: Present Status and Future Application", Vol.XIII, No.11.
2. TM Lehmann, H-G Grondahl and DK Benn, "Computer-based registration for digital subtraction in dental radiography", *Dentomaxillofacial Radiology* (2000) 29, p.323-346, 2000.
3. Yonghak Ahn, Oksam Chae, "Automatic Subtraction Radiography Algorithm for Detection of Periodontal Disease in Internet Environment", ICCSA2005, Springer, LNCS3481, pp.732-740, 2005.
4. DC Yoon, "A new method for the automated alignment of dental radiography" *Dentomaxillofacial Radiology* 29, pp.11-19, 2000.
5. Paul F. van der Stelt, Wil G.M.Geraets, "Computer-Aided Interpretation and Quantification of Angular Periodontal Bone Defects on Dental Radiographs", *IEEE Transactions on Biomedical, Engineering*, Vol.38, No.4, pp.334-338, April 1991.
6. C.C. Leung, P.C.K. Kwok, K.Y.Zee, F.H.Y. Chan, "Estimation of the gray level variations in soft and hard peri-implant tissue from X-ray images", 19th International Conference IEEE/EMBS, pp.802-804, 1997.
7. Bernard Imbert, Jean Meunier, Aldo Camarda and Roni Berbari, "A system for osseointegration quantification in oral implantology", *IEEE/EBMBS and CMBEC Theme 2 : Imaging*, pp.425-426, 1995.

The Band Selection Algorithm in Supervised Classification Using Mixed-Pixels and Canonical Correlation Analysis

Hoon Chang¹, Hwan-Hee Yoo², and Hong Sok Kim¹

¹ Dept. of Urban Planning and Engineering, Yonsei University,
Seodaemun-gu, Seoul, Korea
hchang@yonsei.ac.kr, Hskim66@yonsei.ac.kr

² Urban Engineering Department,
Gyeongsang National University,
Gazwa-dong, Jinju, Gyeongnam, Korea
hhyoo@nongae.gsnu.ac.kr

Abstract. The commonly used methods for the optimum band selection in supervised classification of multi-spectral data are Divergence, Transformed divergence (TD) and Jeffreys-Matusita distance (JM distance). But those methods might be ineffective when there is a need to change in the number of bands used and some spectral information in multi-spectral data can be redundant in classification process. This study introduces new algorithm with “bands variables set” and “classes variables set”, the canonical correlation analysis is made use of feature classification. Using the canonical cross-loadings we can orderly identify the bands correlation that largely affects the remotely sensed data. To verify the suitability of the new algorithm, the classifications using the each best band combination through TD, JM distance and new method were performed and the accuracy was assessed. As a result of classification accuracy assessment, overall accuracy and k^{\wedge} for the new method were superior to TD's and had competitive results to JM distance method.

1 Introduction

Most commercial software vendors in remote sensing provide two classification methods from satellite image, the unsupervised and the supervised classification. The supervised classification requires training areas for each class based on the spectral information of each class. It is always important to extract which bands should be used for determining training areas, so the extraction of characteristics between classes has been frequently done by statistics information.

Most classifying processes require sufficient spectral information to highlight band characteristics of satellite image, but that does not always mean that more the bands are used, the better the classification results are. It is often inefficient way to use all or many bands to extract the spectral information, then pixels could be classified into inappropriate classes due to overlapped spectral information (Swain and Davis, 1978). The prevailing band selection methodologies are Divergence, Transformed

Divergence (TD), Jeffreys-Matusita Distance (JM distance), and etc. Those methodologies were essentially based on the statistical separability measurement between two classes using the mean vector and the covariance matrix of the selected bands (Swain and King, 1973; Swain and Davis, 1978)., Those methodologies, however, assume that the pixel distribution of selected bands follows a normal distribution, and the boundary between classes is rigid. The possible combinations from two classes independently measured the statistical separability, so these methodologies did not take into account all classes simultaneously. Moreover, they should recalculate the mean vector and the covariance matrix of bands if the user wants to change the number of bands used. Dean and Hoffer (1983) addressed that in case of multi-bands image the classification results from four bands could be economical by considering the accuracy of classification results and the process time.

Therefore it is important to select appropriate bands among multi- or hyper-spectral data, not to overlap the spectral information, but to separate spectral characteristics between classes reasonably. This study introduced new algorithm which incorporated the mixed pixels and the canonical correlation analysis to improve the use of spectral information from all bands once. New algorithm was then applied to actual satellite image. Mausel et al. (1990) concluded that TD and JM distance methods showed the highest classification results, so the classification results of new algorithm were compared with conventionally provided methods, TD, and JM distance in commercial software.

2 Methodology

This study intended to extract the appropriate band combination from in-depth spectral information, so the canonical correlation analysis was used to analyze the structural relationships with respect to two sets of variables. Two sets of variables were (i) band variables and (ii) class variables. The band variables represent pixel values, and the class variables represent the mixed pixel ratios.

2.1 Mixed Pixel Analysis

The mixed pixel analysis used in this study was the Possibilistic C Mean (PCM) and the membership, u_{ik} , to i class of k pixel can be defined as equation (1) below,

$$u_{ik} = \frac{1}{1 + \left(\frac{d_{ik}^2}{\eta_i} \right)^{\frac{1}{m-1}}} \quad (1)$$

where, d_{ik} means the distance between the center of i class, and k pixel, η_i represents the distance between each pixel on a feature space of multiple dimensions (the number of bands) and the center of i class. In a exponent, m is defined as a weighting index called a fuzzier, and is always equal to or over 1. If $m=1$, then there is no fuzziness in memberships to each class, therefore the classification process could be processed in "hard state." That is the boundary between classes may be distinct, but it would be un realistic in reality. The larger m means that the mixed state of memberships is between classes, so their boundaries can be represented in proportional form.

In PCM, m value should be set to 1.5 for the membership of each class (Krishnapuram and Keller, 1996).

2.2 Canonical Correlation Analysis

The Canonical Correlation Analysis is an additional procedure for assessing the relationship between variables. Specifically, this analysis allows us to investigate the relationship between two sets of variables and would be the appropriate method of analysis in case of dealing with two sets of variables. The structural relationship between two sets, W and V , would be simply a linear form expressed as below,

$$\begin{aligned} W &= b' B = b_1 B_1 + b_2 B_2 + \dots + b_n B_n \\ V &= c' C = c_1 C_1 + c_2 C_2 + \dots + c_n C_n \end{aligned} \tag{2}$$

where, W and V are canonical variables of two sets of variables, and b and c are canonical coefficients of each set. The canonical coefficients vector maximizing correlation coefficients between linear-combined canonical variables can be equal to calculate the largest eigenvalue, λ from the specific equations below,

$$\begin{aligned} |\rho_{BB}^{-1} \rho_{BC} \rho_{CC}^{-1} \rho_{CB} - \lambda I| &= 0 \\ |\rho_{CC}^{-1} \rho_{CB} \rho_{BB}^{-1} \rho_{BC} - \lambda I| &= 0 \end{aligned} \tag{3}$$

where, ρ_{BB} , ρ_{CC} , and $\rho_{BC}(=\rho_{CB})$ are defined as the variance-covariance matrix of band variables, the variance-covariance matrix of class variables, and the covariance matrix between two sets of variables, respectively.

The canonical coefficients produced the canonical cross loadings of band variables, and these loadings can be measurements to examine not only the relationship between each variable in one set and variables in other set, but also the degree of effects. In short, the largest canonical loadings means the largest correlations, so the optimum bands can be drawn from these loadings.

2.3 Statistical Significance Test

In case of non correlation between two sets of variables, the covariance matrix should be 0, so it is required to test for the null hypothesis, $H_0: \sum_{BC}=0$. The test statistics, Wilk's Λ (Mardia et al., 1979; Lindeman et al., 1980; Johnson and Wichern, 1998), used in this study can be represented in

$$\Lambda = \prod_{j=k}^p (1 - \rho_j^{*2}) \tag{4}$$

where ρ_j^* means the j th canonical coefficient. Bartlett (1951) suggested that the revised test statistics for large samples, and the equation is

$$V = - \left[n - \frac{1}{2} (p + q + 3) \right] \ln \Lambda \tag{5}$$

and this statistics approximately forms χ^2 distribution with pq degree of freedom. In equation (5), n should be larger than 1,000 or 20 times the number of variables.

3 Area and Data Sets

This paper select the northeastern part of Seoul Metropolitan Area, and it is located at (187234.0, 455977.0)~(196054.0, 449922.0) in TM coordinate system, figure 1. This area showed mixed features with urban built-up and forest areas, and the agricultural areas were located at the northwestern part of the study area.

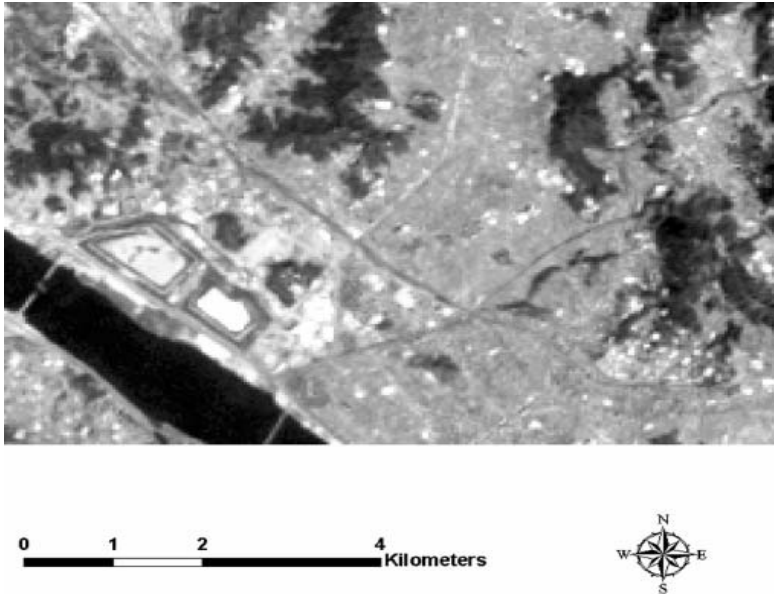


Fig. 1. Area: northeaster part of Seoul Metropolitan

The satellite image used in this study was from Landsat ETM+ taken in April 29, 2000. Yet Landsat image has total of 8 bands; 7 multispectral and 1 panchromatic image, this study employed 6 bands (band 1, 2, 3, 4, 5, 7) without panchromatic and thermal bands. The classification results were evaluated by reference data, which was available in Department of Environment in Korea.

4 Results and Analysis

The program written in C language processed the canonical correlation analysis for two sets of variables, and the conventional classification methods were provided in ERDAS 8.6.

4.1 Mixed Pixel Analysis and Canonical Correlation Analysis

As a pre-step to calculate PCM, the center vectors for each class were obtained, and then the center vectors played an important role to investigate the spectral information in supervised classification. The total of 6 classes was selected and table 1 shows the results of center vectors between 6 classes and bands.

Table 1. The center vectors of each class

	Agricultural	Bare land	Forest	Urban	Water	Grass
band1	95.663	124.620	86.431	104.263	86.984	96.976
band2	78.288	116.829	66.732	85.034	59.779	80.810
band3	84.100	142.556	63.190	91.079	51.190	80.119
band4	45.613	75.422	58.758	50.872	20.835	75.190
band5	68.525	146.594	81.824	84.329	19.939	103.524
band7	53.575	124.727	55.732	75.339	16.443	70.714

The eigenvalues from canonical correlation analysis for satellite image are 0.8230, 0.6166, 0.1435, 0.0479, 0.0195, and 0.0033. The test statistics for this image was 122735.24 from equation (4) and (5). This value is substantially larger than 67.9850, which is the significance level 0.001 in chi-square with degree of freedom (36)., so the null hypothesis was rejected, in other words, there exists a correlation between classes and bands. Table 2 lists canonical loadings for bands.

Table 2. Calculated canonical cross loadings

Variable vector	Band 1	Band 2	Band 3	Band 4	Band 5	Band 7
Cross loadings	-0.252746	0.497961	-0.104641	-0.034020	-0.831551	0.282643

4.2 Comparison with Conventional Methods

At first, the optimum bands for each methods showed small differences, that is, band 1, 2, 4, 7, band 1, 3, 5, 7, and band 1, 2, 5, 7, for TD, JM distance, and new method, respectively. For accurate classification assessment, the minimum 70 pixels were determined in each class, but urban class has 100 pixels, therefore total of 460 pixels were used for accuracy assessment. Test pixels were located at the same place for all methods.

Kappa statistics is a conventional method to evaluate classification results and the equation is below (Fitzpatrick-Lins, 1981; Marsh et al., 1994). N is the number of sample, p=the expected accuracy, q=100-p, E=the permitted error (%), and Z=the 95% standard normal distribution value. Given the expected accuracy was 87.5% and the permitted error was 5%, the minimum sample number was 168 pixels. The classification results from each method were listed in table 3, 4, and 5.

$$N = \frac{Z^2 pq}{E^2} \tag{6}$$

Table 3. Classification results by TD (band 1 2 4 7)

	Reference	Classified	Correct No.	Producer Accuracy	User Accuracy
Agricultural	70	39	30	42.86%	76.92%
Bare land	70	48	38	54.29%	79.17%
Forest	80	68	63	78.75%	92.65%
Urban	100	174	86	86.00%	49.43%
Water	70	63	63	90.00%	100.00%
Grass	70	68	43	61.43%	63.24%
Overall Classification Accuracy: 70.22%					
Overall Kappa Statistics: 0.6368					

Table 4. Classification results by JM distance (band 1 3 5 7)

	Reference	Classified	Correct No.	Producer Accuracy	User Accuracy
Agricultural	70	54	39	55.71%	72.22%
Bare land	70	58	45	64.29%	77.59%
Forest	80	72	65	81.25%	90.28%
Urban	100	149	82	82.00%	55.03%
Water	70	59	59	84.29%	100.00%
Grass	70	68	46	65.71%	67.65%
Overall Classification Accuracy: 73.04%					
Overall Kappa Statistics: 0.6726					

Table 5. Classification results by new algorithm (band 1 2 5 7)

	Reference	Classified	Correct No.	Producer Accuracy	User Accuracy
Agricultural	70	54	33	47.14%	61.11%
Bare land	70	55	43	61.43%	78.18%
Forest	80	73	66	82.50%	90.41%
Urban	100	152	82	82.00%	53.95%
Water	70	61	61	87.14%	100.00%
Grass	70	65	43	61.43%	66.15%
Overall Classification Accuracy: 71.30%					
Overall Kappa Statistics: 0.6513					

From above results, the overall accuracy was the highest in JM distance, new algorithm, and TD in order. But, accuracies were not substantially different, 73.04%, 71.30%, and 70.22%. The kappa statistics was the same order, 0.6726, 0.6513, and 0.6368, respectively. The classification accuracies by new algorithm were higher in water and forest areas compared to JM distance, but agricultural area was poorly

classified in new algorithm than JM distance methods. The classification accuracy was slightly different due to this agricultural area in overall.

5 Conclusions

For efficient classification process, the spectral information of classes should not be duplicated, and moreover selected bands should be statistically separable in feature space. This study introduced new algorithm, which class set was set by mixed pixel ratio or PCM, then the canonical correlation analysis calculated all pixels in class set to obtain canonical loadings for each class. From loadings, the optimum band can be selected. New algorithm was compared with two prevailing methods, TD and JM distance by commercial software.

In conclusion, new algorithm was no need to assume the normal distribution of pixel in each band, and all spectral information was simultaneously incorporated unlike conventional methods. Although there is a change in number of bands selected, new algorithm is not required to recalculate, but conventional methods should recalculate for optimum bands.

The classification results showed that new algorithm was competitive to JM distance method and prevailed to TD in overall accuracy and kappa index. The classification order in overall accuracy and kappa index was JM distance, new algorithm, and TD, but differences were minimal. This study applied new algorithm Landsat scene, which has only 9 bands, for better performance comparison, hyperspectral image would be more appropriate for future studies. The results, however, proved that new algorithm is still competitive for multispectral image classification.

References

1. Bartlett, M. S. The Goodness of Fit of a Single Hypothetical Discriminant Function in the Case of Several Groups. *Annals of Eugenics* (1951) 199-216
2. Dean, M. E. and R. M. Hoffer.: Feature Selection Methodologies using Simulated Thematic Mapper Data. Symposium on Machine Processing of Remote Sensed Data, LARS, Purdue University, West Lafayette, Indiana (1983) 347-356
3. Fitzpatrick-Lins, K., Comparison of Sampling Procedures and Data Analysis for a Land-use and Land-cover Map. *Photogrammetric Engineering and Remote Sensing.*, vol.47 (1981) 343-351
4. Johnson, R. A. and D. W. Wichern. *Applied Multivariate Statistical Analysis*, Prentice Hall, London (1998)
5. Krishnapuram, R. and J. Keller. The Possibilistic C-Means Algorithm: Insights and Recognitions. *IEEE Trans. Fuzzy System.*, Vol. 4. (1996) 385-393
6. Lindeman, R. H., P. F. Merenda, and R. Z. Gold. *Introduction to Bivariate and Multivariate Analysis*, Scott, Foreman and Company, London (1980)
7. Mardia, K. V., J. T. Kent, and J. M. Bibby. *Multivariate Analysis*, London Academic Press (1979)
8. Marsh, S.E., J.L. Walsh, and C. Sobrevila, Evaluation of Airborne Video Data for Land-cover Classification Accuracy Assessment in an Isolated Brazilian Forest, *Remote Sensing of Environment.*, 48 (1994) 61-69

9. Mausel, P. W., W. J. Kamber, and J. K. Lee. Optimum Band Selection for Supervised Classification of Multispectral Data. *Photogrammetric Engineering and Remote Sensing*, vol. 56(1) (1990) 55-60
10. Swain, P. H. and R. C. King Two Effective Feature Selection Criteria for Multispectral Remote Sensing. *Proc. First Int. Joint Conference on Pattern Recognition. IEEE* (1973) 536-540
11. Swain, P. H. and M. Davis.: *Remote Sensing: The Quantitative Approach*. McGraw-Hill, New York (1978) 166-174

Domain Analysis for Components Based Developments

Ha-Jin Hwang

Department of Management information Systems, Catholic University of Daegu,
Kyung San, Daegu, 712-708, Korea
hjhwang@cu.ac.kr

Abstract. Domain engineering is the foundation for emerging “product line” software development approaches and affects the maintainability, understandability, usability, and reusability characteristics of similar systems. However, the existing domain engineering methods do not elicit information necessary for the component-based software development process in selecting and configuring appropriate components. In this paper, we suggest a method that systematically defines, analyzes and designs a domain to enhance reusability effectively in component-based software development (CBSD). We extract information objectively that can be reused in a domain from the requirement analysis phase. We sustain and refine the information, and match them to artifacts of each phase in domain engineering. Through this method, reusable domain components and malleable domain architecture can be produced. In addition, we demonstrate the practical applicability and features of our approach for a news information storage domain.

Keywords: Domain engineering, Domain analysis, reuse, Component-based Software Development, Domain architecture.

1 Introduction

The notation of a domain is still somewhat ambiguous in the literature. In this paper we will take the application-oriented definition of domain given in which domain is defined as “a family or set of systems including common functionality in a specified area.”

The application-oriented domain analysis includes “objects” and “operation” that reflect components of the software systems themselves [2]. We can incorporate it as useful information when developing another system that belongs to that domain, if we can observe commonality and variability within a certain domain and develop it under a repeat operation status. This ability allows increases productivity and reduces development time and cost. However, software has many variables, which differ from the reusability of hardware, and software variations are much more difficult to standardize, identify, and control. The possibility for development was envisioned by realizing new paradigms as CBSD.

Domain engineering supports application engineering by producing artifacts necessary for efficiency of application development. Therefore, domain engineering has to be tailored to CBSD process. The existing domain engineering methods don't elicit

information necessary for CBSD process, in selecting and configuring appropriate components. Also, the existing domain analysis and design method do not represent objective analysis processes that extract and determine the properties of the domain, such as commonality and variability. In addition, the method that these domain information are explicitly reflected to the domain component and the domain architecture is not complete and valid.

In this study, the Component-Based Domain Engineering (CBDE) method, which systematically defines, analyzes, and designs the domain as an effective reuse method to develop component-based software, is presented. The reusable components within the domain, namely the common factors, are extracted objectively through the requirement analysis step and should be continuously maintained, refined throughout the processes and reflected to the output of each step. Through this process, the domain components with common factors can be identified and domain architecture can then be designed. Domain architecture with the property of commonality and variability can be used for various systems that belong to the domain; thus, domain architecture has the flexibility that can reflect a variety of features of each system. Software reusability is enhanced through CBDE, which is presented in this study, and supports relationships of systematic replication by allowing implementation of reusable software.

The structure of the paper is as follows; A search for existing research related to this study in Section 2. A description of the domain design method of the component base that is suggested in this study in Section 3. Section 4 describes a case study and discusses the issues that have been identified. Conclusion and some words on further works are followed.

2 Domain Analysis and Design

The general Domain-driven Component-based Software development process is presented in this study is as in Figure.1. Our process model for component-based software development explicitly considers reuse-specific activities, such as componential design, component identification, and component adaptation.

It is comprised of seven major activities, starting with context comprehension and requirement analysis, continuing with the combination of componential design and component identification, component creation, component adaptation, and finally ending with component assembly. Throughout the process, explicitly stated domain artifacts- domain specifications, domain model, and domain architecture - are produced.

Component-based Domain Engineering depends on the component-based software development process. In the first step of domain engineering, domain definition, the purpose of the domain is decided, and its scope is confirmed. In the domain modeling step, a domain model is obtained by analyzing the domain. Domain analysis has to identify the stable and the variable parts of the domain. Based on this domain model, the domain components are identified, and the domain architecture is created.

Our process model for domain engineering has an objective analysis activity in each step, i.e. *generalization process*. The generalization process is tasks that classify the properties of domain requirement, domain usecase, and domain component and

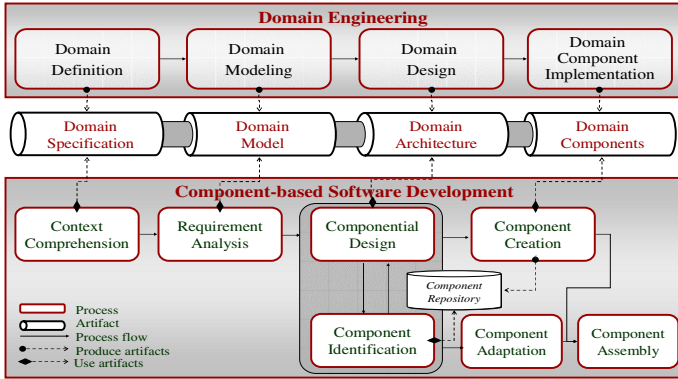


Fig. 1. Domain-driven CBSD Process

transform these into reusable form according to the properties. The artifacts of each step are maintained and saved with interrelationships. They are reused as useful information during component-based software development.

In this paper, we suggest some domain engineering processes- domain definition, domain modeling, and domain design- for launching a study among the Domain-driven CBSD process that is represented in Figure.1.

2.1 Domain Definition

The purpose of the Domain Definition step is to create domain specifications by bounding the domain scope and defining the domain purpose. In addition, requirements of domain are extracted from legacy and new systems in the domain and converted to generalized type reflecting properties- common, optional, variable.

2.1.1 Decide Domain Scope

As defined earlier, the domain is a collection of related systems, which can lead to vague interpretations, so it is imperative that ambiguities are made clear. If the scope of the domain is large, more systems can be contained in that domain, and it will be easy to contain new systems in the future. However, this leads to a reduction in commonality in the domain. Consequently, more commonality can be extracted in a domain of smaller scope.

1) *Distinguish Domain External Stakeholder.* Domain external stakeholder means people with interest in the functions provided by a domain. People who are interested in input or output of a domain or people who handle an external system related to the domain can be extracted as external stakeholders.

2) *Define Domain Assumption.* The domain assumption means pre-conditions that are to be satisfied by using components that are provided by the domain. Domain assumption performs a basic role to decide whether or not a system can be included in the domain in the initial step. Subsequently, it has influence on the decision of the domain’s component properties that will be extracted later.

3) *Describe Domain Environment.* Domain environment is divided into domain external environment and domain internal environment. Domain external environment presents clearly the boundary of the domain by analyzing interaction between the domain and its external factors. Domain internal environment presents factors that should be distributed within the domain and its functions accordingly.

2.1.2 Define Domain Purpose

After the scope of the domain is set, a rough outline centering on the functionality of the domain is explained. Additionally, a domain concept schematic diagram is drawn outlining the domain's business processes related to its purpose.

1) *Describe Domain Purpose.* The important function of the domain is described. It is an essential factor that all the systems belonging to the domain should have. Furthermore, it functions as a basis to decide whether the system should be included in the domain.

2) *Model Domain Concept.* Major tasks, which need to be clearly defined within the domain, and related terminology are extracted. Furthermore, relationships among these are identified in general drawings. Through these activities concepts within a domain are expressed.

2.2 Domain Modeling

The purpose of the Domain Modeling step is to analyze the domain and to develop the domain model composed of a domain requirement model and a domain type model with commonality and variability.

A domain model captures the most important "things" – business objects or process and prepares variable things within the context of the domain. We use usecase analysis technique as an appropriate way to create such a model. The usecase leads to a natural mapping between the business processes and the requirements [9].

2.2.1 Develop Domain Requirement Model

The domain requirement model expresses the requirements extracted from the domain by the usecase diagram of UML. This induces the analyzed primitive requirements to be bundle into a suitable unit.

1) *Construct Domain Usecase Diagram.* The actor is extracted from the domain stakeholder and the domain external environment. The requirements of such an actor and domain operations are extracted as a domain usecase.

Then a domain usecase diagram is drawn. The domain usecase is written with different levels of detail.

2) *Describe Domain Usecase Description.* The primitive requirements identified during the prior step should all be allocated to usecases. This provides an important link in terms of traceability between the artifacts. The domain usecase diagram should be modified to reflect the properties of domain usecase after the domain usecase generalization process.

2.2.2 Develop Domain Type Model

Based on the domain concept model produced during the domain definition step and the domain usecase description, the domain type model is developed by extracting detailed information and status that should be controlled by the system.

In this model, not only physical but also non- physical, such as a processor, can be a domain type. This allows common comprehension on the domain and enables the possibility of applying a consistent glossary to overall processes.

The domain type model is presented as a type of class diagram of UML. It defines the attributes of each domain type, and limitations of the model such as multiplicity of relationships.

2.2.3 Domain Usecase Generalization Process

A task to classify the properties of domain usecase and reconstruct the domain usecase according to these properties is defined as ‘domain usecase generalization process’. Properties of domain usecase are influenced by PR’s properties.

1) *Construct PR-Usecase Matrix.* Create a PR-Usecase matrix to recognize the property of each usecase by referring to the domain usecase diagram and description and the PR-Context matrix. The usecase name, primitive requirement, and the property of primitive requirement are displayed in the matrix. Moreover, the primitive requirements that are contained in each usecase are analyzed. Fig.5. presents the PR-Usecase matrix.

2) *Generalize Domain Usecase.* When analyzing usecase, we can consider usecase conditions as the following; at this time, we can divide and rearrange usecases on their necessity. This is presented in Fig.2. First in considering the usecase condition, a usecase contains primitive requirements, which does not overlapped with that of other usecases. (① of Fig.4 and 5). In this case, no re-arrangement is necessary. Second, the primitive requirement is spread over to many usecases (② of Fig.2). In this case, separate commonly overlapped primitive requirements, make it an independent usecase, and connect it to include-relationships. Third, a usecase includes variable primitive requirements. (③ of Fig.2). In this case, a confirmation on the possibility of

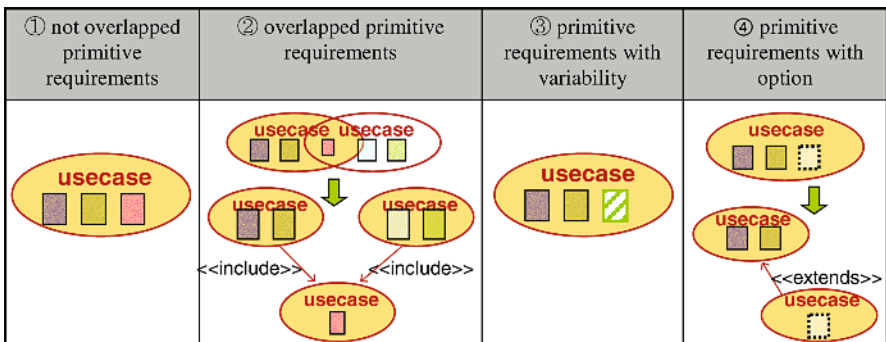


Fig. 2. Property Identification Process from PR-Usecase Matrix

whether variable primitive requirements can be separated and created as independent usecase is addressed. If possible, they are separated. If not, they are maintained as involved in a usecase and a variable point is stored. Finally, a usecase includes optional primitive requirements (④ of Fig.4 and 5). In this case, the optional primitive requirements are separated and connected to the extend-relationship.

The usecases that were reorganized by this process are classified by the properties as follows:

- 1) **Common Usecase** – When the usecase has primitive requirements, which must exist within the domain, it is classified as a common usecase and represents an important process in the system.
- 2) **Variable Usecase** – When the usecase is composed of variable primitive requirements, this is classified as a variable usecase. It means a usecase with requirements that exist in each specific application of a domain but can be variable. Mainly, it tends to appear overlapping in many usecases. In case it was divided into an independent usecase through the PR-Usecase matrix analysis, it belongs to this class.
- 3) **Optional Usecase** – It represents the usecase that doesn't always need to exist when handling a process in the system; this corresponds to a usecase composed of optional primitive requirements.
- 4) **Usecase with Variables** – When primitive requirements with variation are difficult to be separated independently, this is involved in the usecase. Even though this cannot be divided separately, it can be used when identifying a domain component of the next step and draw the component interaction diagram at the domain design step by classifying this status.

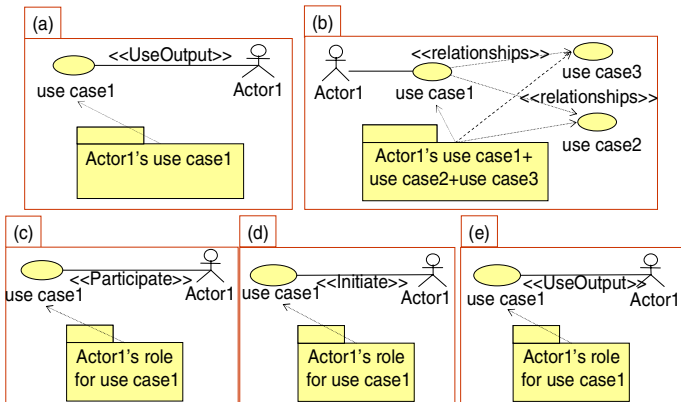


Fig. 3. Domain Component Extraction Standard

3 Domain Design

The purpose of the Domain Design step is to identify the domain components and to develop the domain architecture. The domain component, which is different from the

physical component that can be deployed immediately during software development, is defined as a service central unit package of platform independent logical level. Domain architecture is represented out of the identified domain components in a concrete and analyzable format. Domain architecture is different from software architecture in that domain architecture must allow for variability.

3.1 Identify Domain Component

The most important process of component-based software development is that of extracting the component. Therefore, this process is also important for component-based domain design.

When creating applications, it is possible to allocate different granularity, which can be extracted from the requirement of the system. Variable granularity of these components can be supplied through the component that was extracted based on the service.

So the domain component is extracted based on domain usecase because usecase is a description of set of sequences of actions that a system performs that yield an observable result of value to an actor [10], i.e. one service. The process of extracting the component is as follows:

3.2 Domain Component Generalization Process

Each extracted domain component executes a relationship based on usecase, and is divided by its properties of commonality, optional, and variability in review of the PR-Usecase matrix.

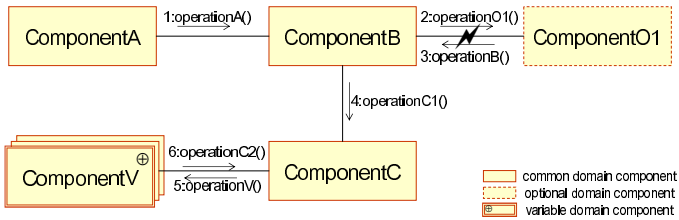


Fig. 4. Domain Component Interaction View

In this process, the components are reorganized upon their necessity, and an abstraction is performed. We call this process “*domain component generalization process.*”

Domain component interaction view is displayed in figure 4.

3.3 Develop Domain Architecture

Domain architecture presents the structure of domain components, interaction between domain components in multiple views, and specifications of the domain component. Domain architecture should be independent of any specific technology or set

of developmental tools. Domain architecture should reflect properties such as commonality, variability and optional that were initialized from the requirement analysis step, refined, and maintained. Such features allow part of the architecture to be divided and replaced according to the component's property when creating the component-based software development. So, malleable architecture can be created.

1) *Domain Component Interaction View*. Domain Component Interaction View represents interactions between domain components that perform specific requirements. In addition, a domain component interface is extracted by analyzing operations between components. Domain Component Interaction View is presented by using an Interaction diagram, and component interface is described by using class notation. Fig.4 presents Domain Component Interaction View.

2) *Domain Development View*. All computer applications have three general areas of functionality; User services, Business services and Data services. Domain structure can be divided into common, variable and optional parts by the features of the domain.

In the domain development view, the domain structure is divided and presented in namely 2nd dimension layers through logical partitioning of functionality as horizontal and property division of the domain as vertical. Not only does the systemized view allow for independent performance and quick change at each step, but also is becomes the foundation for various physical partitioning (deployment alternatives) such as 2 tier or 3 tier, n tier, and Web-enabled applications.

The vertically divided view determines the optional component easily by the application's specific factor, and easily supports modifying the variable component, so it covers various systems that belong to the domain. Fig.5 represents the Domain Development View of a 2nd dimension division.

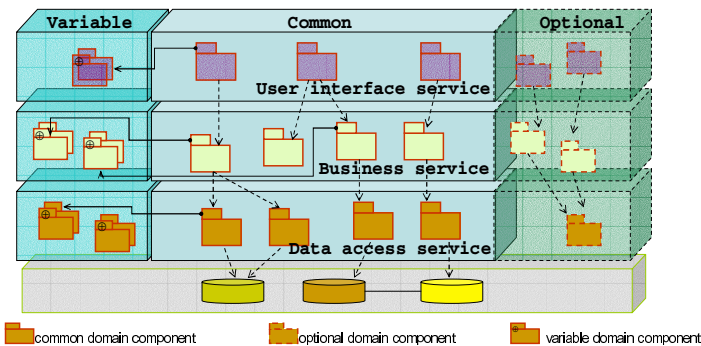


Fig. 5. Domain Development View

3) *Domain Component Specifications*. Domain Component Specifications describes the purpose and interfaces of a component and furnishes information about what the component does and how it can be used. A deployable component, which is developed using a Domain Component Specifications, can differ in granularity according to applications. Hence, we will describe the related functions as interface and

supplement required interfaces to effectively support variable granularity of the component. In this way when interfaces are developed independently, required interfaces can be recognized easily. Also the Domain Component property is explicitly represented using a 'type' tag in the interface. The 'type' tag can have common, variable, or optional values. If the 'type' tag has a variable or optional value, it can be described as a predictable case by a 'rule' tag in the interface.

4 Conclusion and Future Work

In this study, different processes for domain analysis and design method that have suited to component-based software development were suggested. Namely, in the existing study, it could not obtain information on procedures to assemble components in consideration of their relationship using architecture and recognition of domain components. This study recognized and selected components that were required during the development of component base software. Furthermore, a connected relationship between the components and the interface information through domain engineering processes were identified which supported the component base software development process.

Also, this study described a method to find commonality and variability, which is necessary to extract information with objectivity through the generalization processes while existing studies depended solely on experience and intuition by a domain specialist. In addition, this information was relocated into matrix form to be maintained, refined, and used in each step to find common usecase and common domain component. This study reflected such features into the shape of the domain architecture, created a malleable architecture that can be partially separated architecture, and replaced them by the property of the components during component based software development.

Future studies will progress in two directions. We will review the possibility to implement a domain component by using domain architecture and study ideas and technologies how they can be applied. Also we will study a process that can be implemented for the development of component based software by using a proposed domain analysis and design method.

References

1. SEI in Carnegie Mellon University, Domain Engineering and Domain Analysis, URL:<http://www.sei.cmu.edu/str/descriptions/dade.html>
2. Creps D., Klingler, C., Levine, L., and Allemang, D.: Organization Domain Modeling (ODM) Guidebook Version 2.0, Software Technology for Adaptable, Reliable Systems (STARS) (1996).
3. Kang, K.C.: Feature-Oriented Domain Analysis for Software Reuse, Joint Conference on Software Engineering (1993) 389-395.
4. Kang, K.C., Kim, S., Lee J., and Kim, K.: FORM: A Feature-Oriented Reuse Method with Domain Specific Reference Architectures, Pohang University of Science and Technology(POSTECH) (1998).

5. Klingler, C.D.: DAGAR: A Process for Domain Architecture Definition and Asset Implementation, In: Proceedings of ACM TriAda (1996).
6. Coplien, J.; Hoffman, D.; Weiss, D.: Commonality and variability in software engineering, IEEE software , Volume: 15 Issue: 6 (1998) 37-45.
7. Gupta, N.L., Jagadeesan, L.J., Koutsofios, E.E., Weiss, D.M.: Auditdraw: Generating Audits the FAST Way, Requirements Engineering, 1997., Proceedings of the Third IEEE International Symposium (1997) 188-197.
8. Digre T.: Business Object Component Architecture, IEEE software Vol.15, No.5, September/October (1998) 60-69.
9. Jacobson, I., Booch, G., and Rumbaugh, J.: The Unified Software Development Process, Addison-Wesley, January (1999).
10. Larman, C.: Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design, Prentice Hall. (1998).

Author Index

- Abbas, Cláudia Jacy Barenco V-819
Abraham, Ajith IV-40
Adamidis, Panagiotis V-108
Adolf, David I-711
Ahn, Byung Jun II-77
Ahn, Dong-In III-251
Ahn, Heejune IV-603
Ahn, Jaehoon V-522
Ahn, Jung-Chul IV-370
Ahn, ManKi III-48
Ahn, Sang-Ho III-279
Ahn, Seongjin II-400, II-410, II-487,
V-829, II-1169
Ahn, Sung-Jin II-982
Ahn, Sungsoo V-269
Ahn, Sungwoo II-175
Ahn, Taewook IV-388
Ahn, Yonghak V-1001
Ahn, Youngjin II-661
Akbar, Ali Hammad II-186, II-847
Alam, Muhammad Mahbub II-651
Albertí, Margarita I-721
Alfredo-Badillo, Ignacio III-456
Ali, Hassan IV-217
Ali, Saqib IV-217
Allayear, Shaikh Muhammad II-641
Almendra, Daniel V-819
Al-Mutawah, Khalid I-586
Alvarez, Susana III-1073
Amarnadh, Narayanasetty I-1
Ambler, Anthony P. V-531
An, Kyoungwan II-155
An, Sunshin II-730
Anagun, A. Sermet III-11, III-678
Anan, Yoshiyuki II-40
Andersen, Anders Magnus IV-98
Angelides, Marios C. IV-118
Arce-Santana, Edgar R. V-412
Armer, Andrey I-974
Arteconi, Leonardo I-694

Badea, Bogdan I-1166
Bae, Hae-Young I-914, IV-1126
Bae, Hyo-Jung I-151
Bae, Joonsoo II-379
Bae, Suk-Tae II-309
Bae, Yong-Geun IV-828
Bae, Youngchul III-244
Baek, Jun-Geol V-839
Baek, Myung-Sun V-752
Bagherpour, Morteza III-546
Bahn, Hyokyung I-1072
Bai, Zhang I-885
Baik, Heung Ki V-236
Baixauli, J. Samuel III-1073
Bala, Piotr V-394
Balas, Lale I-547
Balci, Birim I-373
Ban, Chaehoon II-175
Bang, Hyungbin II-319
Bang, Young-Cheol III-1090, III-1129
Bardhan, Debabrata I-10
Bartolotta, Antonino I-821
Bashir, Ali Kashif II-186
Basu, Kalyan I-566
Bawa, Rajesh Kumar I-1177
Bellaachia, Abdelghani V-346
Bentz, Cédric III-738
Berbegall, Vicente V-192
Berkov, Dmitri V-129
Bertoni, Guido III-1004
Biscarri, Félix V-725
Biscarri, Jesús V-725
Blibech, Kaouthar III-395
Boada, Imma I-364
Bohli, Jens-Matthias III-355
Bolze, Raphael V-202
Bories, Benoît I-744
Bravo, Maricela IV-169
Brennan, John K. V-743
Breveglieri, Luca III-1004
Brzeziński, Jerzy IV-1166, V-98
Buiati, Fabio V-819
Burns, John I-612
Byun, Doyoung V-537
Byun, Sang-Seon II-1189
Byun, Sang-Yong III-84
Byun, Sung-Wook I-232

- Byun, Tae-Young III-134
 Byun, Young Hwan V-457
 Byun, Yung-Cheol V-185
 Byun, Yung-Hwan V-512, V-932

 Caballero-Gil, Pino I-577, III-1035
 Caballero, Ismael III-984
 Cáceres, Santos II-18
 Cai, Guoyin IV-1090
 Calderon, Alejandro IV-1136
 Calero, Coral III-984
 Camahort, Emilio I-510
 Camara, José Sierra V-798
 Campos-Delgado, Daniel U. V-412
 Cao, Wenming V-375
 Capacho, Liliana III-554
 Cappelletti, David I-721
 Carballeira, Félix García V-108
 Carlone, Pierpaolo I-794
 Caro, Angelica III-984
 Caron, Eddy V-202
 Carretero, Jesus IV-1136
 Castro, Mildrey Carbonell V-798
 Cattani, Carlo I-785, I-828, I-857
 Cha, Byung-Rae II-1090
 Cha, Eui-Young I-1110
 Cha, Guang-Ho I-344
 Cha, Jae-Sang V-312
 Cha, JeongHee V-432
 Chae, Kijoon I-1072, IV-440
 Chae, Oksam V-1001
 Chae, Young Seok II-760
 Challiol, Cecilia IV-148
 Chan, Yung-Kuan V-384
 Chan, Yuen-Yan I-383, III-309, III-365,
 III-507, IV-406
 Chang, Chung-Hsien I-171
 Chang, Hangbae IV-255, IV-707
 Chang, Hoon IV-577
 Chang, Hoon V-1010
 Chang, Hsi-Cheng V-158
 Chang, Kuo-Hwa III-944
 Chang, Ok-Bae III-188, III-222, IV-893,
 IV-955, V-644
 Chang, Soo Ho II-451
 Chang, Sujeong II-77
 Chang, Yu-Hern III-649
 Chaudhry, Shafique Ahmad II-847
 Chaudhuri, Chitrita II-1
 Chen, Chiou-Nan IV-1107
 Chen, Chun V-39
 Chen, Gencai V-39
 Chen, Huifen III-944
 Chen, Kai-Hung V-384
 Chen, Kaiyun IV-756
 Chen, Ken I-307
 Chen, Lei II-1149
 Chen, Ling V-39
 Chen, Tzu-Yi III-1081
 Chen, Yen Hung III-631
 Cheng, Jingde III-1
 Cheng, Yu-Ming I-171, I-181
 Cheon, Saeng Hoon III-718
 Cheon, SeongKwon III-73
 Cheun, Du Wan II-451
 Cheung, Yen I-586
 Chi, Sang Hoon IV-58
 Chih, Wen-Hai III-668
 Chlebiej, Michał V-394
 Cho, Cheol-Hyung I-101
 Cho, Daerae IV-787
 Cho, Dongyoung IV-491
 Cho, Eun Sook II-1003, IV-985
 Cho, Haengrae V-214
 Cho, Ik-hwan I-326
 Cho, Jae-Hyun I-1110
 Cho, Jong-Rae III-832, III-994
 Cho, Juphil V-236
 Cho, KumWon V-522
 Cho, Kwang Moon IV-1003
 Cho, Mi-Gyung I-904
 Cho, Minju II-760
 Cho, Nam-deok V-546
 Cho, Sang-Hun II-288
 Cho, Sok-Pal II-1082
 Cho, Sung-eon V-600
 Cho, Tae Ho IV-58
 Cho, Yongyun IV-30
 Cho, Yookun II-701, IV-499, IV-549
 Cho, Youngsong I-111
 Cho, You-Ze II-631
 Choi, Bong-Joon V-912
 Choi, Byung-Cheon III-785
 Choi, Byungdo IV-808
 Choi, Byung-Sun II-945
 Choi, Chang IV-567
 Choi, Changyeol II-562, IV-1156
 Choi, Deokjai IV-128
 Choi, Eun Young IV-316
 Choi, Ho-Jin II-796

- Choi, Hwangkyu II-562, IV-1156
 Choi, Hyung-Il V-441
 Choi, Hyun-Seon III-728
 Choi, Jaeyoung IV-11, IV-30
 Choi, Jonghyoun II-525, II-895
 Choi, Jongmyung II-1033
 Choi, Jong-Ryeol IV-893
 Choi, Junho IV-567
 Choi, Junkyun V-829
 Choi, Kuiwon I-335
 Choi, Kyung Cheol IV-659
 Choi, Misook II-49, IV-966
 Choi, Sang-soo V-618
 Choi, Sang-Yule V-312, V-322, V-355
 Choi, Seongman III-222, IV-955, V-644,
 V-675
 Choi, Su-il II-77
 Choi, Sung-Hee IV-937
 Choi, Tae-Young I-307, I-317
 Choi, Wan-Kyoo IV-828
 Choi, Wonjoon IV-279
 Choi, Yeon Sung I-993
 Choi, Yong-Rak IV-432
 Choi, Yun Jeong II-298
 Chon, Jaechoon I-261, III-1172
 Chon, Sungmi II-28
 Choo, Hyunseung II-165, II-288, II-534,
 II-661, II-710, II-856, II-923, II-934,
 II-1121, III-1090, III-1129
 Choo, MoonWon IV-787
 Chun, Junchul I-410
 Chung, Chin Hyun I-929, I-964
 Chung, Chun-Jen III-862
 Chung, Ha Joong IV-549
 Chung, Hyoung-Seog V-491
 Chung, Il-Yong IV-828
 Chung, Jinwook II-487, II-982
 Chung, Kyoil III-375, IV-584, V-251
 Chung, Min Young II-77, II-288, II-534,
 II-856, II-934, II-1121
 Chung, Mokdong IV-1042
 Chung, Shu-Hsing III-610
 Chung, TaeChoong II-390
 Chung, Tae-sun I-1019
 Chung, Tai-Myoung II-135, II-239,
 III-486, V-626, V-655
 Chung, YoonJung III-54, IV-777
 Chung, Younky III-198, III-234
 Ciancio, Armando I-828
 Ciancio, Vincenzo I-821
 Clifford, Raphaël III-1137
 Cocho, Pedro III-964
 Cokuslu, Deniz II-681
 Coll, Narcis I-81
 Cong, Jin I-921
 Cools, Ronald V-780
 Cordero, Rogelio Limón IV-726
 Costantini, Alessandro I-738
 Crane, Martin I-612
 Cruz, Laura II-18
 Culley, Steve J. II-279
 Cumplido, René III-456
 Czekster, Ricardo M. I-202
 Daefler, Simon I-566
 Dagdeviren, Orhan II-681
 D'Anjou, Alicia III-1143
 Darlington, Mansur J. II-279
 Das, Gautam K. II-750
 Das, Sajal I-566
 Das, Sandip I-10, II-750
 David, Gabriel IV-78
 De Cristófolo, Valeria IV-148
 de Deus, Flavio E. V-808
 de Doncker, Elise V-789
 de Oliveira, Robson V-819
 de Frutos-Escrig, David IV-158
 de Ipiña, Diego López IV-108
 de Sousa, Rafael V-819
 Deineko, Vladimir III-793
 Demirkol, Askin V-365
 den Hertog, Dick III-812
 Deo, Puspita I-622
 Derevyankin, Valery I-974
 Desprez, Frederic V-202
 Dévai, Frank I-131
 Diaz, Olivia Graciela Fragoso IV-50
 Doallo, Ramón I-701
 Dogdu, Erdogan IV-88
 Drummond, L.A. V-192
 Duan, Guolin V-450
 Duan, Yucong IV-746
 Durán, Alfonso III-964
 Ekinci, Murat III-1216
 Eksioğlu, Burak III-748
 Eksioğlu, Sandra Duni III-708
 Eom, Jung-Ho II-239
 Eom, Young Ik I-1028
 Erciyes, Kayhan II-681

- Esquivel, Manuel L. III-841
 Eun, He-Jue V-990
 Evangelisti, Stefano I-744

 Fang, Zhijun II-964
 Färber, Gerrit III-638
 Farsaci, Francesco I-821
 Farzanyar, Zahra I-1100
 Fathy, Mahmood V-118
 Fei, Chai IV-179
 Feixas, Miquel I-449
 Feng, Dan I-1045
 Feregrino-Uribe, Claudia III-456
 Ferey, Nicolas I-222
 Fernandez, Javier IV-1136
 Fernández, Marcel III-527
 Fernández, Marcos I-490
 Fernandez, Reinaldo Togores I-30
 Fernández-Medina, Eduardo III-1013,
 III-1024, III-1044
 Fey, Dietmar V-129
 Filomia, Federico I-731
 Fiore, Ugo III-537
 Fleissner, Sebastian I-383, IV-406
 Forné, Jordi IV-1098
 Fort, Marta I-81
 Frausto, Juan IV-169
 Frick, Alexander I-847
 Fu, Xiaolan IV-746
 Fúster-Sabater, Amparo I-577, III-1035

 Gabillon, Alban III-395
 Galindo, David III-318
 Gallego, Guillermo III-822
 Gao, Yunjun V-39
 Garcia, Felix IV-1136
 Garcia, Jose Daniel IV-1136
 García, L.M. Sánchez V-108
 García-Sebastian, M. Teresa III-1143
 Gattiker, James R. III-1153
 Gattton, Thomas M. III-244, IV-947,
 V-665, V-675
 Gaudiot, Jean-Luc IV-622
 Gavrilova, Marina L. I-61, I-431
 Ge, He III-327
 Gerardo, Bobby D. III-144, IV-899,
 V-867
 Gervasi, Osvaldo I-212, I-665
 Gherbi, Rachid I-222
 Ghosh, Preetam I-566
 Ghosh, Samik I-566
 Gil, Joon-Min II-1169
 Go, Sung-Hyun V-867
 Goh, John I-1090
 Goh, Sunbok II-204
 Goi, Bok-Min IV-424
 González, Ana I. III-1143
 Gonzalez, César Otero I-30
 González, J.J. V-772
 González, Juan G. II-18
 González, Luis I-633
 González, Patricia I-701
 Gordillo, Silvia IV-148
 Górriz, J.M. V-772
 Graña, Manuel III-1143
 Gros, Pierre Emmanuel I-222
 Gu, Boncheol IV-499, IV-549
 Gu, Huaxi V-149
 Gu, Yuqing IV-746
 Guillen, Mario II-18
 Guo, Jiang III-974
 Guo, Jianping IV-1090
 Guo, Weiliang I-938
 Gutiérrez, Miguel III-964

 Ha, Jong-Eun III-1163
 Ha, Jongsung II-49
 Ha, Sung Ho III-1110
 Hahn, GeneBeck II-769
 Hamid, Md.Abdul II-866
 Han, Chang-Hyo III-832
 Han, DoHyung IV-594
 Han, Dong-Guk III-375
 Han, Gun Heui V-331
 Han, Hyuksoo IV-1081
 Han, Jizhong I-1010
 Han, Jong-Wook IV-360
 Han, Joohyun IV-30
 Han, JungHyun I-1028
 Han, Jungkyu IV-549
 Han, Ki-Joon II-259
 Han, Kijun II-1159
 Han, Kunhee V-584
 Han, Long-zhe I-1019
 Han, Sang Yong IV-40
 Han, Seakjae V-682
 Han, SeungJae II-359
 Han, Sunyoung II-601
 Han, Youngshin V-260
 Harbusch, Klaus I-857

- Hashemi, Sattar I-1100
 Hawes, Cathy I-644
 He, S. III-934
 Helal, Wissam I-744
 Heng, Swee-Huay III-416
 Heo, Joon II-989, II-1066
 Heo, Junyoung II-701, IV-499, IV-549
 Hérissou, Joan I-222
 Herrero, José R. V-762
 Higdon, David III-1153
 Hinarejos, M. Francisca IV-1098
 Hoesch, Georg V-202
 Hoffmann, Aswin L. III-812
 Hong, Bonghee II-155, II-175
 Hong, Choong Seon II-651, II-866
 Hong, Dong-Suk II-259
 Hong, Dowon IV-584
 Hong, Gye Hang III-1110
 Hong, Jiman II-701, IV-499, IV-558,
 IV-603
 Hong, John-Hee III-832
 Hong, Kwang-Seok I-354
 Hong, Maria II-400
 Hong, In-Hwa IV-245
 Hong, Seokhie III-446
 Hong, Soonjwa III-385
 Hong, Suk-Kyo II-847
 Hong, Sukwon I-1019
 Hong, Sung-Je I-151
 Hong, Sung-Pil III-785
 Hong, WonGi IV-577
 Hong, Youn-Sik II-249
 Horie, Daisuke III-1
 Hosaka, Ryosuke I-596
 Hsieh, Shu-Ming V-422
 Hsu, Chiun-Chieh V-158, V-422
 Hsu, Li-Fu V-422
 Hu, Qingwu IV-746
 Hu, Yincui IV-1090
 Huang, Changqin V-243
 Huang, Chun-Ying III-610
 Huang, Wei I-518
 Huh, Euinam II 390, II-515, II-827,
 II-905, V-717
 Huh, Woong II-224
 Huh, Woonghee Tim III-822
 Hur, Tai-Sung II-224
 Hwang, An Kyu II-788
 Hwang, Chong-Sun II-369, II-816
 Hwang, Ha-Jin V-1018
 Hwang, Hyun-Suk III-115, III-125,
 V-895
 Hwang, InYong II-1140
 Hwang, Jin-Bum IV-360
 Hwang, Jun II-760
 Hwang, Ken III-668
 Hwang, Soyeon IV-344
 Hwang, Suk-Hyung IV-767, IV-937
 Hwang, Sungho III-134
 Hwang, Sun-Myung IV-909
 Hwang, Tae Jin V-236
 Ikeguchi, Tohru I-596
 Im, Chaeseok I-1000
 Im, Eul Gyu III-54, IV-777
 Im, SeokJin II-369
 Im, Sungbin II-806
 Inan, Asu I-547
 Inceoglu, Mustafa Murat I-373
 Iordache, Dan I-804
 Isaac, Jesús Téllez V-798
 Isaila, Florin D. V-108
 Ishii, Naohiro II-40
 Iwata, Kazunori II-40
 Jang, Byung-Jun V-752
 Jang, Hyo-Jong II-106
 Jang, Injoo III-206
 Jang, Jun Yeong I-964
 Jang, Kil-Woong II-671
 Jang, Moonsuk II-204
 Jang, Sangdong IV-1116
 Jang, Taeuk II-760
 Jang, Yong-Il IV-1126
 Je, Sung-Kwan I-1110
 Jeon, Hoseong II-934
 Jeon, Hyung Joon II-974, II-1009
 Jeon, Hyung-Su III-188
 Jeon, Jongwoo III-718
 Jeon, Kwon-Su V-932
 Jeon, Segil V-522
 Jeon, Sung-Eok III-134
 Jeong, Byeong-Soo II-505, II-796
 Jeong, Chang-Sung I-232, II-462
 Jeong, Chang-Won IV-853
 Jeong, Chulho II-430
 Jeong, Dong-Hoon II-996
 Jeong, Dongseok I-326
 Jeong, Gu-Beom IV-1032
 Jeong, Hye-Jin V-675

- Jeong, Hyo Sook V-609
 Jeong, In-Jae III-698
 Jeong, Jong-Geun II-1090
 Jeong, Karpjoo V-522
 Jeong, Kugsang IV-128
 Jeong, KwangChul II-923
 Jeong, Sa-Kyun IV-893
 Jeong, Su-Hwan V-895
 Jeong, Taikyeong T. I-993, V-531
 Jhang, Seong Tae IV-631
 Jhon, Chu Shik IV-631
 Ji, JunFeng I-420
 Ji, Yong Gu IV-697
 Ji, Young Mu V-457
 Jiang, Chaojun I-938
 Jiang, Di I-50
 Jiang, Gangyi I-307, I-317
 Jiang, Yan I-921
 Jianping, Li I-885
 Jin, DongXue III-73
 Jin, Hai IV-529
 Jin, Honggee IV-687
 Jin, Mingzhou III-708, III-748
 Jo, Geun-Sik II-779
 Jo, Jeong Woo II-480
 Jodlbauer, Herbert V-88
 Johnstone, John K. I-500
 Joo, Su-Chong III-251, IV-798, IV-853,
 IV-899
 Joye, Marc III-338
 Juang, Wen-Shenq IV-396
 Ju, Hyunho V-522
 Ju, Minseong IV-271
 Jun, Jin V-839
 Jung, Cheol IV-687
 Jung, Eun-Sun IV-416
 Jung, Hyedong II-691
 Jung, Hye-Jung IV-1052
 Jung, Inbum II-562, IV-1156
 Jung, Jae-Yoon II-379, V-942
 Jung, JaeYoun III-64
 Jung, Jiwon II-155
 Jung, Won-Do II-186
 Jung, Kwang Hoon I-929
 Jung, Kyeong-Hoon IV-448
 Jung, Kyung-Hoon III-115
 Jung, Myoung Hee II-77
 Jung, SangJoon III-93, III-234, IV-1022
 Jung, Seung-Hwan II-462
 Jung, Se-Won II-837
 Jung, Won-Do II-186
 Jung, Won-Tae IV-1052
 Jung, Youngsuk IV-1022
 Jwa, JeongWoo IV-594
 Kabara, Joseph V-808
 Kangavari, Mohammadreza I-1100
 Kang, Dazhou II-1179
 Kang, Dong-Joong II-309, III-1163
 Kang, Dong-Wook IV-448
 Kang, Euisun II-400
 Kang, Euiyoung IV-558
 Kang, Eun-Kwan IV-947
 Kang, Heau-jo V-690
 Kang, Hong-Koo II-259
 Kang, Hyungwoo III-385
 Kang, Jeonil IV-380
 Kang, Jinsuk I-993
 Kang, Maing-Kyu III-898
 Kang, Mikyung IV-558
 Kang, Mingyun V-575
 Kang, Namhi III-497
 Kang, Oh-Hyung III-287, IV-1060
 Kang, Sanggil I-1127
 Kang, Sang-Won II-369
 Kang, Sangwook II-730
 Kang, Seo-Il IV-326
 Kang, Seoungpil II-1066
 Kang, Sin Kuk III-1200
 Kang, Suk-Ho IV-787, V-942
 Kang, Sukhoon II-1060, IV-271, IV-432
 Kang, Wanmo III-777, III-822
 Kang, Yunjeong V-665
 Karsak, E. Ertugrul III-918
 Kasprzak, Andrzej III-1100, III-1119
 Katsionis, George I-251
 Kaugars, Karlis V-789
 Keil, J. Mark I-121
 Képès, François I-222
 Kettner, Lutz I-60
 Key, Jaehong I-335
 Khader, Dalia III-298
 Khonsari, Ahmad V-118
 Khoo, Khoongming III-416
 Kim, Backhyun IV-68, IV-1146
 Kim, Bonghan V-851
 Kim, Bong-Je V-895
 Kim, Byeongchang III-21
 Kim, Byung Chul II-788

- Kim, Byunggi II-319, II-330, II-740,
 II-1033
 Kim, Byung-Guk II-996
 Kim, Byung-Ryong III-476
 Kim, Byung-Soon II-671
 Kim, Chang J. V-932
 Kim, Changmin III-261, IV-787
 Kim, Chang Ouk V-839
 Kim, Chang-Soo III-115, III-125, V-895
 Kim, Cheol Min I-278, I-288, IV-558
 Kim, Chonggun III-64, III-73, III-93,
 III-234, IV-808, IV-818, IV-1022
 Kim, Chulgoon V-522
 Kim, Chul Jin II-1003, IV-985
 Kim, Chul Soo V-185
 Kim, Dai-Youn III-38
 Kim, Deok-Soo I-101, I-111, I-440
 Kim, DongKook II-340, II-349
 Kim, Dong-Oh II-259
 Kim, Dong-Seok IV-853
 Kim, Dongsoo IV-687
 Kim, Donguk I-101, I-111, I-440
 Kim, Duckki II-195
 Kim, Duk Hun II-856
 Kim, Eung Soo III-31
 Kim, Eunhoe IV-11, IV-30
 Kim, Eun Mi III-1190, IV-893
 Kim, Eun Yi III-1200
 Kim, Gil-Han V-284
 Kim, Gui-Jung IV-835
 Kim, Guk-Boh IV-1032
 Kim, Gukboh II-214
 Kim, Gu Su I-1028
 Kim, Gwanghoon IV-344
 Kim, GyeYoung II-106, V-432, V-441
 Kim, Gyoung Bae I-914
 Kim, Hae Geun III-104
 Kim, Haeng-Kon III-84, III-163,
 III-198, IV-844, IV-927, IV-976
 Kim, Haeng Kon IV-873
 Kim, Hak-Jin III-928
 Kim, HanIl IV-558, IV-567, IV-594
 Kim, Hee Taek I-914
 Kim, Hong-Gee IV-937
 Kim, Hong-Jin II-1082
 Kim, Hong Sok V-1010
 Kim, Hong-Yeon I-1053
 Kim, Ho-Seok I-914, IV-1126
 Kim, Ho Won III-375
 Kim, Howon IV-584, V-251
 Kim, Hye-Jin I-955
 Kim, Hye Sun I-288
 Kim, HyoJin II-359
 Kim, Hyongsuk III-1172
 Kim, Hyun IV-466
 Kim, Hyuncheol V-829
 Kim, Hyung-Jun IV-483
 Kim, Hyunsoo III-852
 Kim, Iksoo IV-68, IV-1146
 Kim, IL V-912
 Kim, Ildo II-87
 Kim, InJung III-54, IV-777
 Kim, In Kee V-1
 Kim, Intae IV-21
 Kim, Jaehyoun II-934
 Kim, Jae-Soo II-572
 Kim, Jae-Yearn III-590
 Kim, Jaihie II-96
 Kim, Jee-In I-983
 Kim, Je-Min II-1219
 Kim, Jeong Hyun II-996, II-1066
 Kim, Jin-Geol IV-288
 Kim, Jin Ok I-929, I-964
 Kim, Jin Suk II-480
 Kim, Jin-Sung V-968, V-979
 Kim, Jin Won IV-499, IV-509
 Kim, John II-114
 Kim, Jong-Hwa V-503
 Kim, Jongik II-552
 Kim, Jongsung III-446
 Kim, Jongwan II-369
 Kim, June I-1028, I-1053
 Kim, Jungduk IV-255, IV-707
 Kim, Jung-Sun V-922
 Kim, Junguk II-760
 Kim, Kap Hwan III-564
 Kim, Kibom III-385
 Kim, Ki-Chang III-476
 Kim, Ki-Doo IV-448
 Kim, Ki-Hyung II-186, II-847
 Kim, Ki-Uk V-895
 Kim, Ki-Young IV-612
 Kim, Kuinam J. II-1025
 Kim, Kwang-Baek I-1110, III-172,
 III-279, V-887
 Kim, Kwangsoo IV-466
 Kim, Kwanjoong II-319, II-1033
 Kim, Kyujung II-28
 Kim, Kyung-Kyu IV-255
 Kim, Kyung Tae IV-519

- Kim, LaeYoung II-1131
 Kim, Min Chan IV-669
 Kim, Min-Ji V-932
 Kim, Minsoo III-154, IV-697, V-269,
 V-922
 Kim, Minsu III-134
 Kim, Min Sung III-31
 Kim, Misun II-420, III-154
 Kim, Miyoung II-885
 Kim, MoonHae V-522
 Kim, MoonJoon IV-577
 Kim, Moonseong II-710, III-1054,
 III-1090, III-1129, V-626
 Kim, Myeng-Ki IV-937
 Kim, Myoung-Joon I-1053
 Kim, Myoung-sub V-700
 Kim, Myung Keun I-914
 Kim, Nam-Gyun I-241
 Kim, Pankoo IV-567
 Kim, Sangbok II-515
 Kim, Sangho V-491
 Kim, Sang-II III-728
 Kim, Sangjin IV-388
 Kim, Sangki II-87
 Kim, Sangkuk II-11
 Kim, Sangkyun IV-639, IV-716
 Kim, Seki III-1054
 Kim, Seoksoo II-1060, IV-271, V-565,
 V-575, V-584, V-591, V-700
 Kim, Seok-Yoon IV-612
 Kim, Seong Baeg I-278, I-288, IV-558
 Kim, Seungjoo II-954, V-858
 Kim, Seung Man I-480
 Kim, Seung-Yong IV-612
 Kim, Sijung V-851
 Kim, SinKyu II-769
 Kim, Soo Dong II-451, IV-736
 Kim, Soo Hyung IV-128
 Kim, Soon-gohn V-690
 Kim, Soon-Ho III-172
 Kim, So-yeon V-618
 Kim, Su-Nam IV-448
 Kim, Sungchan I-459
 Kim, Sung Jin V-609
 Kim, Sung Jo IV-669
 Kim, Sung Ki II-876
 Kim, Sung-Ryul III-1137
 Kim, Sung-Shick III-928
 Kim, SungSoo I-904
 Kim, Sungsuk IV-567
 Kim, Tae-Kyung II-135
 Kim, Taeseok I-1062
 Kim, Tai-hoon V-700
 Kim, Ung Mo II-165, IV-456
 Kim, Ungmo I-1028, V-139
 Kim, Won II-106
 Kim, Woo-Jae II-720
 Kim, Wu Woan IV-1116
 Kim, Yang-Woo II-905
 Kim, Yeong-Deok IV-271
 Kim, Yong-Hwa V-968
 Kim, Yong-Min II-340, II-349
 Kim, Yongsik IV-687
 Kim, Yong-Sung V-958, V-968, V-979,
 V-990
 Kim, Yong-Yook I-241
 Kim, Yoon II-562, IV-1156
 Kim, Young Beom II-515, II-827
 Kim, Youngbong IV-226
 Kim, Youngchul II-319, II-1033
 Kim, Younghan III-497
 Kim, Younhyun II-611
 Kim, Young-Kyun I-1053
 Kim, Youngrag III-64
 Kim, Young Shin V-457
 Kim, Youngsoo II-545
 Kim, Yunkuk II-730
 Knauer, Christian I-20
 Ko, Eung Nam IV-475
 Ko, Hyuk Jin II-165
 Ko, Il Seok V-331, V-338
 Ko, Kwangsun I-1028
 Ko, Kyong-Cheol IV-1060
 Kobusińska, Anna IV-1166
 Koh, Byoung-Soo IV-236, IV-245
 Koh, Kern I-1062
 Koh, Yunji I-1062
 Kohout, Josef I-71
 Kolingerová, Ivana I-71
 Kong, Jung-Shik IV-288
 Koo, Jahwan II-487
 Kosowski, Adrian I-141, I-161
 Koszalka, Leszek V-58
 Koutsonikola, Vassiliki A. II-1229
 Kozhevnikov, Victor I-974
 Krasheninnikova, Natalia I-974
 Krasheninnikov, Victor I-974
 Kreveld, Marc van I-20
 Krusche, Peter V-165
 Ku, Chih-Wei II-1210

- Ku, Hyunchul II-827
 Kurzynski, Marek III-1210
 Kwak, Jae-min V-600
 Kwak, Jin II-954
 Kwak, Jong Min V-338
 Kwak, Jong Wook IV-631
 Kwak, Keun-Chang I-955
 Kwon, Dong-Hee II-720
 Kwon, Dong-Hyuck III-38
 Kwon, Gihwon IV-1081, V-905
 Kwon, Jang-Woo II-309, V-887
 Kwon, Jungkyu IV-1042
 Kwon, Oh-Cheon II-552
 Kwon, Oh-Heum IV-306
 Kwon, Seungwoo III-928
 Kwon, Soo-Tae III-767
 Kwon, Taekyoung II-769, II-915
 Kwon, Tae-Kyu I-241
 Kwon, Yoon-Jung V-503
- Laganà, Antonio I-212, I-665, I-675,
 I-694, I-721, I-738, I-757
 Lago, Noelia Faginas I-731
 Lai, Jun IV-179
 Lai, Kin Keung I-518
 Lan, Joung-Liang IV-1107
 Laskari, E.C. V-635
 Lawrence, Earl III-1153
 Lazar, Bogdan I-779
 Lazzareschi, Michael III-1081
 Le, D. Xuan IV-207
 Lee, Amy Hsin-I III-610
 Lee, Bo-Hee IV-288
 Lee, Bongkyu IV-549, V-185
 Lee, Byung-kwan III-38, III-172,
 III-261
 Lee, Byung-Wook I-946, II-495
 Lee, Chae-Woo II-837
 Lee, Changhee I-440
 Lee, Changhoon III-446
 Lee, Changjin V-537
 Lee, Chang-Mog IV-1012
 Lee, Chang-Woo IV-1060
 Lee, Chien-I II-1210
 Lee, Chilgee V-260
 Lee, Chulsoo IV-777
 Lee, Chulung III-928
 Lee, Chung-Sub IV-798
 Lee, Dan IV-994
 Lee, Deok-Gyu IV-326, IV-370
- Lee, Deokgyu IV-344
 Lee, Dong Chun II-1017, II-1051,
 II-1082
 Lee, Dong-Ho III-728
 Lee, Dong Hoon III-385, IV-316
 Lee, DongWoo IV-197, IV-491
 Lee, Dong-Young II-135, III-486, V-626,
 V-655
 Lee, SungYoung II-390
 Lee, Eun Ser IV-1070, V-546, V-555
 Lee, Eung Ju IV-187
 Lee, Eunseok II-430, II-621, V-49
 Lee, Gang-soo V-618
 Lee, Gary Geunbae III-21
 Lee, Geon-Yeob IV-853
 Lee, Geuk II-1060
 Lee, Gigan V-952
 Lee, Gueesang IV-128
 Lee, Gun Ho IV-659
 Lee, Hanku V-522
 Lee, Ha-Yong IV-767
 Lee, Hong Joo IV-639, IV-716
 Lee, HoonJae III-48, III-269
 Lee, Hosin IV-255
 Lee, Ho Woo III-718
 Lee, Hyewon K. II-214
 Lee, Hyobin II-96
 Lee, Hyun Chan I-111
 Lee, Hyung Su II-691, IV-519
 Lee, Hyung-Woo V-284, V-294
 Lee, Ig-hoon I-1036
 Lee, Im-Yeong IV-326, IV-370
 Lee, Inbok III-1137
 Lee, Jaedeuk V-675
 Lee, Jae Don I-1000
 Lee, Jae-Dong IV-1126
 Lee, Jae-Kwang II-945
 Lee, Jae-Seung II-945
 Lee, Jaewan III-144, III-178,
 IV-899, V-867
 Lee, Jae Woo V-457, V-512, V-932
 Lee, Jaewook II-487
 Lee, Jae Yeol IV-466
 Lee, Jaeyeon I-955
 Lee, Jae Yong II-788
 Lee, Jangho I-983
 Lee, Jang Hyun II-1199
 Lee, Jeong Hun III-600
 Lee, Jeonghyun IV-21
 Lee, JeongMin IV-577

- Lee, Ji-Hyun III-287, IV-994
 Lee, Jin Ho III-875
 Lee, Joahyoung II-562, IV-1156
 Lee, Jongchan II-1033
 Lee, Jong Gu III-1190
 Lee, Jong Sik V-1
 Lee, Jong-Sool III-564
 Lee, Jong-Sub III-898
 Lee, Jongsuk II-49
 Lee, Jungho I-326
 Lee, Junghoon IV-558, V-185
 Lee, Jungsuk V-269
 Lee, Junsoo V-175
 Lee, Kang-Hyuk II-309
 Lee, Kang-Woo IV-466
 Lee, Kang-Yoon II-827
 Lee, Keun-Ho II-816
 Lee, Keun Wang II-1074
 Lee, Kihyung II-175
 Lee, Kil-Hung II-572
 Lee, Kilsup IV-917, V-877
 Lee, Ki-Young II-249
 Lee, Kunwoo I-459
 Lee, Kwang Hyoung II-1074
 Lee, Kwangyong IV-499
 Lee, Kwan H. I-480
 Lee, Kwan-Hee I-151
 Lee, Kyesan II-905, V-708, V-717,
 V-952
 Lee, Kyujin V-708
 Lee, Kyu Min IV-483
 Lee, KyungHee IV-380
 Lee, Kyung Ho II-1199
 Lee, Kyunghye II-410
 Lee, Kyungsik III-777
 Lee, Kyung Whan IV-873
 Lee, Malrey III-244, IV-947, V-644,
 V-665, V-675
 Lee, Mun-Kyu IV-584
 Lee, Myungho I-1019
 Lee, Myungjin I-1072
 Lee, Na-Young V-441
 Lee, Samuel Sangkon II-231
 Lee, Sangjin IV-245
 Lee, Sang-goo I-1036
 Lee, Sang Ho IV-1070, V-555, V-609
 Lee, Sang-Hun II-239
 Lee, Sang Hun I-459
 Lee, Sangjin III-446, IV-236
 Lee, Sang Joon V-185
 Lee, Sang-Jun V-503
 Lee, Sangjun IV-549
 Lee, Sang-Min I-1053
 Lee, Sangyoung II-87, II-96
 Lee, Seojeong IV-966
 Lee, Seok-Cheol III-115
 Lee, Seon-Don II-720
 Lee, SeongHoon IV-491
 Lee, Seonghoon IV-197
 Lee, Seong-Won IV-622
 Lee, Seoung-Hyeon II-945
 Lee, Seoung-Soo V-503
 Lee, SeoungYoung II-1140
 Lee, Seungbae V-467
 Lee, Seung-Heon II-495
 Lee, Seunghwa II-621, V-49
 Lee, Seunghwan III-64, III-93
 Lee, Seung-Jin V-512
 Lee, Seungkeun IV-21
 Lee, Seungmin V-476
 Lee, Seung-Yeon II-905
 Lee, SeungYong V-922
 Lee, Se Won III-718
 Lee, SooCheol II-552
 Lee, SuKyoung II-1131
 Lee, Su Mi IV-316
 Lee, Sungchang II-923
 Lee, Sung-Hyup II-631
 Lee, Sung Jong IV-917
 Lee, Sung-Joo IV-828
 Lee, SungYoung II-390
 Lee, Sungkeun II-204
 Lee, Tae-Dong II-462
 Lee, Taehoon IV-1081
 Lee, Tae-Jin II-288, II-534, II-661,
 II-710, II-856, II-923, II-1121
 Lee, Vincent I-586
 Lee, Wankwon IV-491
 Lee, Wansuk II-954
 Lee, Wongoo II-11, V-851
 Lee, Won-Hyuk II-982
 Lee, Wookey IV-787, V-942
 Lee, Woongho I-326
 Lee, Yang-sun V-600
 Lee, Yongjin IV-197
 Lee, Yongseok V-665
 Lee, YoungGyo III-54
 Lee, Young Hoon III-875
 Lee, Young-Koo II-505
 Lee, Youngkwon II-915

- Lee, Young-Seok III-144
 Lee, Youngsook III-517, V-858
 Lee, YoungSoon V-675
 Lee, Yun Ho III-875
 Lee, Yun-Kyoung I-232
 Leininger, Thierry I-744
 León, Carlos V-725
 Leong, Chee-Seng IV-424
 Lho, Tae-Jung II-309, III-1163, V-887
 Liang, Yanchun I-938
 Liang, Zhong III-928
 Liao, Yuehong III-974
 Li, Fucui I-317
 Li, Haisen S. V-789
 Li, Jie II-59
 Li, Jin III-309, III-365, IV-406
 Li, Kuan-Ching IV-1107
 Li, Li I-895
 Li, Lv V-32
 Li, Qu I-393
 Li, Sheng I-420
 Li, Shiping I-317
 Li, Shujun V-789
 Li, Xun I-895
 Li, Yanhui II-1179
 Li, Yunsong V-149
 Li, Zhanwei V-450
 Li, Zhong I-1118, I-1134
 Lim, Andrew III-688
 Lim, Chan-Hyoung III-832
 Lim, Hyotaek IV-380
 Lim, Hyung-Jin II-135, II-239, III-486,
 V-626, V-655
 Lim, Jeong-Mi IV-679
 Lim, JiHyung IV-380
 Lim, Jiyoung IV-440
 Lim, Sungjun IV-707
 Lim, Taesoo IV-687
 Lim, Younghwan II-28, II-400,
 II-410, II-487
 Lin, Ching-Fen III-944
 Lin, Chuen-Horng V-384
 Lin, Hon-Ren V-158
 Lin, Hung-Mei III-338
 Lin, Kung-Kuei V-158
 Lin, Woei II-1111
 Ling, Yun IV-649
 Lísal, Martin V-743
 Lisowski, Dominik V-58
 Liu, Chia-Lung II-1111
 Liu, Fuyu IV-88
 Liu, Guoli III-659
 Liu, Heng I-528
 Liu, Joseph K. IV-406
 Liu, Jun IV-649
 Liu, Kai III-748
 Liu, Qun I-1045
 Liu, Shaofeng II-279
 Liu, Xianxing II-59
 Liu, XueHui I-420
 Loke, Seng Wai IV-138
 Lopes, Carla Teixeira IV-78
 López, Máximo IV-169
 Lu, Jiahui I-938
 Lu, Jianjiang II-1179
 Lu, Jiqiang III-466
 Lu, Xiaolin I-192, I-875
 Luna-Rivera, Jose M. V-412
 Luo, Ying IV-1090
 Luo, Yuan I-431
 Lv, Xinran V-450

 Ma, Hong III-688
 Ma, Lizhuang I-1118, I-1134
 Ma, Shichao I-1010
 Madern, Narcis I-81
 Magneau, Olivier I-222
 Mah, Pyeong Soo IV-509
 Makarov, Nikolay I-974
 Małafiejski, Michał I-141, I-161
 Mamun-or-Rashid, Md. II-651
 Manos, Konstantinos I-251
 Manzanares, Antonio Izquierdo V-798
 Mao, Zhihong I-1118, I-1134
 Markiewicz, Marta I-684
 Markowski, Marcin III-1119
 Marroquín-Alonso, Olga IV-158
 Martín, María J. I-701
 Mateo, Romeo Mark A. III-178, V-867
 Matte-Tailliez, Oriane I-222
 Maynau, Daniel I-744
 McLeish, Tom I-711
 McMahan, Chris A. II-279
 Mecke, Rüdiger I-268
 Meek, Dereck I-1118
 Mehlhorn, Kurt I-60
 Meletiou, G.C. V-635
 Mellado, Daniel III-1044
 Meng, Qingfan I-938
 Merabti, Madjid IV-352

- Mercorelli, Paolo I-847, I-857
 Miao, Zhaowei III-688
 Mijangos, Eugenio III-757
 Mikołajczak, Paweł V-394
 Millán, Rocío V-725
 Min, Byoung Joon II-270, II-876
 Min, Hong IV-499, IV-549
 Min, Hong-Ki II-224
 Min, Hyun Gi IV-736
 Min, Jun-Ki II-67
 Min, Kyongpil I-410
 Min, So Yeon II-1003, II-1074, IV-985
 Mitra, Pinaki I-1, II-1
 Moet, Esther I-20
 Moh, Chiou II-1111
 Mohades, Ali V-735
 Moin, M. Shahram III-1180
 Mok, Hak-Soo III-832, III-994
 Molinaro, Luis V-808
 Monedero, Íñigo V-725
 Moon, Aekyung V-214
 Moon, Il Kyeong III-600
 Moon, Ki-Young II-945
 Moon, Kwang-Sup III-994
 Moon, Mikyeong II-441, IV-226
 Moon, Young Shik V-404
 Morarescu, Cristian I-771, I-779,
 I-804, I-814, I-839
 Moreno, Anna M. Coves III-638
 Moreno, Ismael Solís IV-50
 Morillo, Pedro I-490
 Morimoto, Shoichi III-1
 Morphet, Steve I-1127
 Mouloudi, Abdelaaziz V-346
 Mouriño, Carlos J. I-701
 Mu, Yi III-345
 Mukhopadhyay, Sourav III-436
 Mukhtar, Shoab II-847
 Mun, Gil-Jong II-340
 Mun, YoungSong II-195, II-214, II-319,
 II-400, II-410, II-420, II-471, II-487,
 II-525, II-611, II-740, II-885, II-895
 Murzin, Mikhail Y. I-605
- Na, Yang V-467, V-476
 Na, Yun Ji V-331, V-338
 Nah, Jungchan IV-440
 Nakashima, Toyoshiro II-40
 Nam, Do-Hyun II-224
 Nam, Junghyun III-517, V-858
 Nam, Taekyong II-545
 Nandy, Subhas C. II-750
 Naumann, Uwe I-865
 Navarro, Juan J. V-762
 Neelov, Igor I-711
 Neumann, Laszlo I-449
 Ng, Victor I-383
 Niewiadomska-Szynkiewicz, Ewa I-537
 Nilforoushan, Zahra V-735
 Noh, Bong-Nam II-340, II-349, V-922
 Noh, Hye-Min III-188, IV-893
 Noh, Min-Ki II-1169
 Noh, Sang-Kyun II-349
 Noh, Seo-Young II-145
 Noh, SiChoon II-1051
 Noh, Sun-Kuk II-582
 Noori, Siamak III-546
 Noruzi, Mohammadreza III-1180
 Nowiński, Krzysztof V-394
 Nyang, DaeHun IV-380
- Ogryczak, Włodzimierz III-802
 Oh, Am-Suk II-309, V-887
 Oh, Hayoung IV-440
 Oh, Heekuck IV-388
 Oh, Hyukjun IV-603
 Oh, Inn Yeal II-974, II-1009
 Oh, Jaeduck II-471
 Oh, Jehwan V-49
 Oh, Juhyun II-760
 Oh, June II-1199
 Omary, Fouzia V-346
 Onosato, Masahiko I-469
 Orduña, Juan Manuel I-490
- Ortiz, Guillermo Rodríguez IV-50
 Ould-Khaoua, Mohamed V-118
- Paar, Christof III-1004
 Pacifici, Leonardo I-694
 Pahk, Cheryl Soo III-1190
 Paik, Juryon IV-456
 Pak, Jinsuk II-1159
 Palazzo, Gaetano Salvatore I-794
 Palmieri, Francesco III-537
 Pamula, Raj III-974
 Papadimitriou, Georgios I. II-1229
 Pardede, Eric I-1146, IV-207
 Park, Chang Mok IV-296

- Park, Chang-Seop IV-679
 Park, Chang Won IV-549
 Park, Chiwoo IV-697
 Park, Choung-Hwan II-1043
 Park, Dae-Hyeon V-958
 Park, DaeHyuck II-400
 Park, Dea-Woo IV-883
 Park, DongSik V-260
 Park, Eun-Ju IV-927
 Park, Geunyoung IV-549
 Park, Gilcheol V-565, V-591
 Park, Gi-Won II-631
 Park, Gyungleen II-760, IV-558, V-185
 Park, Hee-Un V-700
 Park, HongShik II-1140
 Park, Hyeong-Uk V-512
 Park, Ilgon IV-509
 Park, Jaehyung II-77
 Park, Jaekwan II-155
 Park, Jaemin IV-549
 Park, Jang-Su IV-370
 Park, Jea-Youn IV-835
 Park, Jeongmin II-430
 Park, Jeong Su IV-316
 Park, Jeung Chul I-480
 Park, Jong Hyuk IV-236, IV-245
 Park, Jongjin II-525
 Park, Joon Young I-111
 Park, Jungkeun I-1000
 Park, Jun Sang V-457
 Park, Ki-Hong IV-1060
 Park, Kisoeb III-1054
 Park, Ki Tae V-404
 Park, Kyoo-Seok III-125, V-912
 Park, Kyungdo III-928
 Park, Mee-Young V-512
 Park, Mi-Og IV-883
 Park, Namje V-251
 Park, Neungsoo IV-622
 Park, Sachoun V-905
 Park, Sangjoon II-319, II-1033
 Park, Sang Soon V-236
 Park, Sang Yong IV-1
 Park, SeongHoon V-68
 Park, Seungmin IV-499
 Park, Seung Soo II-298
 Park, Soo-Jin IV-432
 Park, Soon-Young IV-1126
 Park, Sung Soon II-641
 Park, Taehyung II-806
 Park, Wongil II-330
 Park, Woojin II-730
 Park, Yong-Seok IV-370
 Park, Young-Bae II-224
 Park, Young-Jae II-515
 Park, Young-Shin IV-432
 Park, Youngsup I-402
 Park, Young-Tack II-1219
 Parpas, Panos III-908
 Pastor, Rafael III-554
 Paun, Viorel I-779, I-804
 Pazo-Robles, Maria Eugenia I-577
 Pazos, Rodolfo II-18, IV-169
 Pegueroles, Josep III-527
 Pérez, Jesús Carretero V-108
 Pérez, Joaquín IV-169
 Pérez-Rosés, Hebert I-510
 Perrin, Dimitri I-612
 Petridou, Sophia G. II-1229
 Phillips, Robert III-822
 Piao, Xuefeng IV-549
 Piattini, Mario III-984, III-1013,
 III-1024, III-1044
 Pillards, Tim V-780
 Pineda-Rico, Ulises V-412
 Pion, Sylvain I-60
 Pirani, Fernando I-721, I-738
 Poch, Jordi I-364
 Pont, Michael J. V-22
 Pontvieux, Cyril V-202
 Porrini, Massimiliano I-721
 Porschen, Stefan I-40
 Pozniak-Koszalka, Iwona V-58
 Prados, Ferran I-364
 Puchala, Edward III-1210
 Pulcineli, L. V-819
 Puntonet, C.G. V-772
 Pusca, Stefan I-763, I-771, I-779,
 I-804, I-839
 Puttini, Ricardo Staciariini V-808
 Qin, Xujia I-393
 Qu, Xiangli V-224
 Qu, Zhiguo I-921
 Quintana, Arturo I-510
 Quirós, Ricardo I-510
 Rabenseifner, Rolf V-108
 Rahayu, J. Wenny I-1146, IV-207
 Rahman, Md. Mustafizur II-866

- Ramírez, J. V-772
 Rao, Imran II-390
 Reed, Chris I-644
 Rehfeld, Martina I-268
 Reitner, Sonja V-88
 Reyes, Gerardo IV-169
 Rhee, Choonsung II-601
 Rhee, Gue Won IV-466
 Rhee, Yang-Won III-287, IV-1060
 Rico-Novella, Francisco III-527
 Riganelli, Antonio I-665
 Rigau, Jaume I-449
 Rim, Kiwook IV-21
 Rodionov, Alexey S. I-605
 Roh, Byeong-hee IV-279
 Rosa-Velardo, Fernando IV-158
 Rossi, Gustavo IV-148
 Roy, Sasanka I-10
 Rubio, Monica I-510
 Ruskin, Heather J. I-612, I-622
 Rustem, Berç III-908
 Ryba, Przemyslaw III-1100
 Ryu, Jong Ho II-270
 Ryu, Yeonseung I-1000, I-1019
- Sadjadi, Seyed Jafar III-546, III-574
 Safaei, Farshad V-118
 Sakai, Yutaka I-596
 Salavert, Isidro Ramos IV-726
 Salgado, René Santaolaya IV-50
 Samavati, Faramarz I-91
 Sarac, T. III-678
 Sarkar, Palash III-436
 Saunders, J.R. I-556, III-934
 Sbert, Mateu I-449
 Schirra, Stefan I-60
 Schizas, Christos N. IV-118
 Schoor, Wolfram I-268
 Schurz, Frank V-129
 Ścisło, Piotr V-394
 Sedano, Iñigo IV-108
 Segura, J.C. V-772
 Sellarès, J. Antoni I-81
 Semé, David V-10
 Seo, Dae-Hee IV-326
 Seo, Dong Il II-270
 Seo, Dongmahn II-562, IV-1156
 Seo, JaeHyun III-154, V-922
 Seo, Jeongyeon I-101
- Seo, Kyu-Tae IV-288
 Seo, Manseung I-469
 Seo, Won Ju III-718
 Seo, Young-Jun IV-864
 Seo, Yuhwa III-954
 Severiano, José Andrés Díaz I-30
 Severn, Aaron I-91
 Shao, Feng I-307
 Shi, Qi IV-352
 Shi, Wenbo III-213
 Shibasaki, Ryosuke I-261
 Shim, Choon-Bo II-114
 Shim, Donghee IV-491
 Shim, Jang-Sup V-968, V-979, V-990
 Shim, Junho I-1036
 Shim, Young-Chul II-125, II-591
 Shimizu, Eihan I-261
 Shin, Chang-Sun III-251, IV-798
 Shin, Chungsoo II-740
 Shin, Dae-won III-261
 Shin, Dong-Ryeol IV-483
 Shin, Dong Ryul II-165
 Shin, Dongshin V-467
 Shin, Hayong I-440
 Shin, Ho-Jin IV-483
 Shin, Jeong-Hoon I-354
 Shin, Kee-Young IV-509
 Shin, Kwangcheol IV-40
 Shin, Myong-Chul V-312
 Shin, Seung-Jung II-487
 Shin, Woochul I-895
 Shin, Yongtae III-954
 Shuqing, Zhang I-885
 Siem, Alex Y.D. III-812
 Singh, David E. IV-1136
 Skouteris, Dimitris I-757
 Śliwiński, Tomasz III-802
 Smith, William R. V-743
 Sobaniec, Cezary V-98
 Sofokleous, Anastasis A. IV-118
 Soh, Ben IV-179
 Soh, Wooyoung V-682
 Sohn, Hong-Gyoo II-989, II-1043
 Sohn, Sungwon V-251
 Sohn, Surgwon II-779
 Soler, Emilio III-1024
 Soler, Josep I-364
 Son, Jeongho II-1159
 Son, Kyungho II-954
 Son, Seung-Hyun III-590

- Song, Eungkyu I-1062
 Song, Eun Jee II-1051
 Song, Ha-Joo IV-306
 Song, Hyoung-Kyu V-752
 Song, Jaekoo V-575
 Song, Jaesung I-469
 Song, JooSeok II-359, II-769, II-1131
 Song, Jungsuk IV-245
 Song, Ki Won IV-873
 Song, Sung Keun V-139
 Song, Wang-Cheol V-185
 Song, Yeong-Sun II-1043
 Song, Young-Jae IV-835, IV-864
 Soriano, Miguel III-527
 Sosa, Víctor J. II-18, IV-169
 Souza, Osmar Norberto de I-202
 Stanek, Martin III-426
 Stankova, Elena N. I-752
 Sterian, Andreea I-779, I-804
 Stewart, Neil F. I-50
 Storch, Lorian I-675
 Suh, Young-Ho IV-466
 Suh, Young-Joo II-720
 Sun, Jizhou V-450
 Sun, Lijuan V-450
 Sun, Youxian IV-539
 Sung, Jaechul III-446
 Sung, Sulyun III-954
 Susilo, Willy III-345
 Syukur, Evi IV-138
- Tae, Kang Soo II-231
 Takagi, Tsuyoshi III-375
 Talia, Domenico I-1080
 Tan, Pengliu IV-529
 Tan, Wuzheng I-1118, I-1134
 Tang, Chuan Yi III-631
 Tang, Lixin III-659
 Tang, W.J. I-556
 Taniar, David I-1090, I-1146
 Tarantelli, Francesco I-675
 Tasan, Seren Özmehmet V-78
 Tasoulis, D.K. V-635
 Tasso, Sergio I-212
 Tate, Stephen R. III-327
 Teng, Lirong I-938
 tie, Li V-32
 Tiskin, Alexander III-793, V-165
 Toma, Alexandru I-839
 Toma, Cristian I-779
- Toma, Ghiocel I-804
 Toma, Theodora I-771
 Torabi, Torab IV-98, IV-217
 Torres-Jiménez, José IV-726
 Tragha, Abderrahim V-346
 Trujillo, Juan III-1024
 Trunfio, Paolo I-1080
 Tsai, Cheng-Jung II-1210
 Tsai, Chwei-Shyong III-406
 Tsai, Yuan-Yu I-171, I-181
 Tunali, Semra V-78
- Uhm, Chul-Yong IV-448
- Vafadoost, Mansour III-1180
 Vakali, Athena I. II-1229
 Val, Cristina Manchado del I-30
 Vanhoucke, Mario III-621
 Varnuška, Michal I-71
 Vazquez, Juan Ignacio IV-108
 Vehreschild, Andre I-865
 Verdú, Gumersindo V-192
 Verta, Oreste I-1080
 Vidal, Vicente V-192
 Vidler, Peter J. V-22
 Villalba, Luis Javier García V-808,
 V-819
 Villarroel, Rodolfo III-1024
 Villarrubia, Carlos III-1013
 Villecco, Francesco I-857
 Virvou, Maria I-251
 Vlad, Adriana I-1166
 Voss, Heinrich I-684
 Vrahatis, M.N. V-635
- Walkowiak, Krzysztof II-1101
 Wan, Wei IV-1090
 Wan, Zheng II-964
 Wang, Bo-Hyun I-946
 Wang, Chung-Ming I-171, I-181
 Wang, Gi-Nam IV-296
 Wang, GuoPing I-420
 Wang, K.J. III-885
 Wang, Kun V-149
 Wang, Kung-Jeng III-668
 Wang, Shoujue V-375
 Wang, Shouyang I-518
 Wang, Weihong I-393
 Wang, Yanming III-309
 Wang, Zhengyou II-964

- Wang, Zhensong I-1010
 Watson, Mark D. I-121
 Wawrzyniak, Dariusz V-98
 Wee, Hui-Ming III-862, III-885
 Weidenhiller, Andreas V-88
 Wei, Guiyi IV-649
 Wei, Tao IV-262
 Wen, Chia-Hsien IV-1107
 Wheeler, Thomas J. I-654
 Wild, Peter J. II-279
 Wollinger, Thomas III-1004
 Won, Dong Ho II-165
 Won, Dongho II-545, II-954, III-54,
 III-517, IV-777, V-251, V-858
 Won, Youjip I-1062
 Woo, Sinam II-730
 Woo, Yo-Seop II-224
 Woo, Young-Ho II-224
 Wu, Chaolin IV-1090
 Wu, Chin-Chi II-1111
 Wu, EnHua I-420
 Wu, Hsien-Chu III-406
 Wu, Mary III-93, IV-818, IV-1022
 Wu, Q.H. I-556, III-934
 Wu, Qianhong III-345
 Wu, Shiqian II-964
 Wu, Xiaqing I-500
 Wu, Zhaohui II-1149
- Xia, Feng IV-539
 Xia, Yu III-1064
 Xiao, Zhenghong V-243
 Xiaohong, Li V-32
 Xie, Mei-fen V-375
 Xie, Qiming V-149
 Xie, Xiaoqin IV-756
 Xu, Baowen II-1179
 Xu, Fuyin V-243
 Xue, Yong IV-1090
- Yan, Jingqi I-528
 Yang, Byounggak III-581
 Yang, Ching-Wen IV-1107
 Yang, Hae-Sool IV-767, IV-937, IV-976,
 IV-1052
 Yang, Hwang-Kyu III-279
 Yang, Hyunho III-178
 Yang, Jong S. III-1129
 Yang, Kyoung Mi I-278
 Yang, Seung-hae III-38, III-261
- Yang, Xuejun V-224
 Yang, Young-Kyu II-495
 Yang, Young Soon II-1199
 Yap, Chee I-60
 Yeh, Chuan-Po III-406
 Yeh, Chung-Hsing III-649
 Yeo, So-Young V-752
 Yeom, Hee-Gyun IV-909
 Yeom, Keunhyuk II-441, IV-226
 Yeom, Soon-Ja V-958
 Yeun, Yun Seog II-1199
 Yi, Sangho II-701, IV-499, IV-549
 Yi, Subong III-144
 Yildiz, İpek I-547
 Yim, Keun Soo I-1000
 Yim, Soon-Bin II-1121
 Yoe, Hyun III-251
 Yoh, Jack Jai-ick V-484
 Yoo, Cheol-Jung III-188, III-222,
 IV-893, IV-955, V-644
 Yoo, Chuck II-1189
 Yoo, Chun-Sik V-958, V-979, V-990
 Yoo, Giljong II-430
 Yoo, Hwan-Hee V-1010
 Yoo, Hyeong Seon III-206, III-213
 Yoo, Jeong-Joon I-1000
 Yoo, Kee-Young I-1156, V-276, V-303
 Yoo, Ki-Sung II-1169
 Yoo, Kook-Yeol I-298
 Yoo, Sang Bong I-895
 Yoo, Seung Hwan II-270
 Yoo, Seung-Jae II-1025
 Yoo, Seung-Wha II-186
 Yoo, Sun K. I-335
 Yoon, Eun-Jun I-1156, V-276, V-303
 Yoon, Heejun II-11
 Yoon, Hwamook II-11
 Yoon, Kyunghyun I-402
 Yoon, Won Jin II-856
 Yoon, Won-Sik II-847
 Yoon, Yeo-Ran II-534
 Yoshizawa, Shuji I-596
 You, Ilsun IV-336, IV-416
 You, Young-Hwan V-752
 Youn, Hee Yong II-691, III-852,
 IV-1, IV-187, IV-456, IV-519,
 V-139, V-185
 Young, Chung Min II-534
 Yu, Jonas C.P. III-885
 Yu, Jun IV-649

Yu, Ki-Sung II-525, II-982
Yu, Lean I-518
Yu, Mei I-307, I-317
Yu, Sunjin II-87, II-96
Yu, Tae Kwon II-451
Yu, Young Jung I-904
Yu, Yung H. V-932
Yuen, Tsz Hon I-383
Yun, Jae-Kwan II-259
Yun, Kong-Hyun II-989

Zeng, Weiming II-964
Zhai, Jia IV-296
Zhang, David I-528
Zhang, Fan II-59
Zhang, Fanguo III-345
Zhang, Jianhong IV-262

Zhang, JianYu IV-262
Zhang, Jie V-149
Zhang, Minghu IV-529
Zhang, Xinhong II-59
Zhang, Zhongmei I-921
Zhao, Mingxi I-1118
Zheng, He II-954
Zheng, Lei IV-1090
Zheng, Nenggan II-1149
Zhiyong, Feng V-32
Zhong, Jingwei V-224
Zhou, Bo IV-352
Zhou, Yanmiao II-1149
Ziaee, M. III-574
Zongming, Wang I-885
Zou, Wei IV-262
Żyliński, Paweł I-141, I-161