INFOCOMP 2014

The Fourth International Conference on Advanced Communications and Computation

ISBN: 978-1-61208-365-0

July 20 - 24, 2014

Paris, France

INFOCOMP 2014 Editors

Claus-Peter Rückemann, Westfälische Wilhelms-Universität Münster /
Leibniz Universität Hannover / North-German Supercomputing Alliance, Germany
Malgorzata Pankowska, University of Economics, Katowice, Poland

INFOCOMP 2014

Foreword

The Fourth International Conference on Advanced Communications and Computation (INFOCOMP 2014), held between July 20-24, 2014, in Paris, France, continued a series of events dedicated to advanced communications and computing aspects, covering academic and industrial achievements and visions.

The diversity of semantics of data, context gathering and processing led to complex mechanisms for applications requiring special communication and computation support in terms of volume of data, processing speed, context variety, etc. The new computation paradigms and communications technologies are now driven by the needs for fast processing and requirements from data-intensive applications and domain-oriented applications (medicine, geo-informatics, climatology, remote learning, education, large scale digital libraries, social networks, etc.). Mobility, ubiquity, multicast, multi-access networks, data centers, cloud computing are now forming the spectrum of de factor approaches in response to the diversity of user demands and applications. In parallel, measurements control and management (self-management) of such environments evolved to deal with new complex situations.

We take here the opportunity to warmly thank all the members of the INFOCOMP 2014 Technical Program Committee, as well as the numerous reviewers. The creation of such a broad and high quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and efforts to contribute to INFOCOMP 2014. We truly believe that, thanks to all these efforts, the final conference program consisted of top quality contributions.

Also, this event could not have been a reality without the support of many individuals, organizations, and sponsors. We are grateful to the members of the INFOCOMP 2014 organizing committee for their help in handling the logistics and for their work to make this professional meeting a success.

We hope that INFOCOMP 2014 was a successful international forum for the exchange of ideas and results between academia and industry and for the promotion of progress in the areas of communications and computations.

We are convinced that the participants found the event useful and communications very open. We hope that Paris, France, provided a pleasant environment during the conference and everyone saved some time to enjoy the charm of the city.

INFOCOMP 2014 Chairs:

INFOCOMP General Chair
Claus-Peter Rückemann, Westfälische Wilhelms-Universität Münster / Leibniz Universität Hannover / North-German Supercomputing Alliance, Germany

INFOCOMP Advisory Chairs
Hans-Joachim Bungartz, Technische Universität München (TUM) - Garching, Germany
Petre Dini, Concordia University - Montreal, Canada / China Space Agency Center - Beijing, China
Sik Lee, Supercomputing Center / Korea Institute of Science and Technology Information (KISTI), Korea
Subhash Saini, NASA, USA

INFOCOMP 2014

COMMITTEE

INFOCOMP General Chair

Claus-Peter Rückemann, Westfälische Wilhelms-Universität Münster / Leibniz Universität Hannover / North-German Supercomputing Alliance, Germany

INFOCOMP Advisory Chairs

Hans-Joachim Bungartz, Technische Universität München (TUM) - Garching, Germany
Petre Dini, Concordia University - Montreal, Canada / China Space Agency Center - Beijing, China
Sik Lee, Supercomputing Center / Korea Institute of Science and Technology Information (KISTI), Korea
Subhash Saini, NASA, USA
Manfred Krafczyk, Institute for Computational Modeling in Civil Engineering (iRMB) - Braunschweig, Germany

INFOCOMP Academia Chairs

Alexander Knapp, Universität Augsburg, Germany
Malgorzata Pankowska, University of Economics, Katowice, Poland

INFOCOMP Research Institute Liaison Chairs

Kei Davis, Los Alamos National Laboratory, USA
Edgar A. Leon, Lawrence Livermore National Laboratory, USA
Ivor Spence, School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Northern Ireland, Research for High
Performance and Distributed Computing / Queen's University Belfast, UK

INFOCOMP Industry Chairs

Alfred Geiger, T-Systems Solutions for Research GmbH, Germany
Hans-Günther Müller, Cray, Germany

INFOCOMP Special Area Chairs on Large Scale and Fast Computation

José Gracia, High Performance Computing Center Stuttgart (HLRS), University of Stuttgart, Germany
Björn Hagemeier, Juelich Supercomputing Centre, Forschungszentrum Juelich GmbH, Germany
Walter Lioen, SURFsara, Netherlands
Lutz Schubert, Institute of Information Resource Management, University of Ulm, Germany

INFOCOMP Special Area Chairs on Networks and Communications

Noelia Correia, University of the Algarve, Portugal
Wolfgang Hommel, Leibniz Supercomputing Centre - Munich, Germany

INFOCOMP Special Area Chairs on Advanced Applications

Bernhard Bandow, Max Planck Institute for Solar System Research (MPS), Göttingen, Germany
Diglio A. Simoni, RTI International - Research Triangle Park, USA

INFOCOMP Special Area Chairs on Evaluation Context

Dominic Eschweiler, Frankfurt Institute for Advanced Studies (FIAS), Germany
Huong Ha, University of Newcastle, Australia (Singapore campus)
Philipp Kremer, German Aerospace Center (DLR), Institute of Robotics and Mechatronics, Oberpfaffenhofen, Germany

INFOCOMP Special Area Chairs on Biometry

Ulrich Norbisrath, Nazarbayev University, Kazakhstan / BIOMETRY.com, Switzerland

INFOCOMP 2014 Technical Program Committee

Wassim Abu Abed, Institute for Computational Modelling in Civil Engineering - Technische Universität Braunschweig, Germany
Ajith Abraham, Machine Intelligence Research Labs (MIR Labs), USA
Mehmet Aksit, University of Twente, Netherlands
Ali I. Al Mussa, King Abdulaziz City for Science and Technology (KACST), Saudi Arabia
Angelos-Christos Anadiotis, School of Electrical and Computer Engineering (SECE), National Technical University of Athens (NTUA), Greece
Daniel Andresen, Kansas State University, USA
Bernadetta Kwintiana Ane, Institute of Computer-aided Product Development Systems, Universitaet Stuttgart, Germany
Douglas Archibald, University of Ottawa, Canada
John Ashley, NVIDIA Corporation, USA
Hazeline U. Asuncion, University of Washington, Bothell, USA
Simon Reay Atkinson, The University of Sydney, Australia
Bernhard Bandow, Max Planck Institute for Solar System Research (MPS), Göttingen, Germany
Khalid Belhajjame, Université Paris Dauphine, France
Belgacem Ben Youssef, King Saud University Riyadh, KSA / Simon Fraser University Vancouver, British Columbia, Canada
Martin Berzins, University of Utah, USA
Rupak Biswas, NASA Ames Research Center, USA
Rim Bouhouch, National Engineering School of Tunis, Tunisia
Steffen Brinkmann, High Performance Computing Centre Stuttgart (HLRS), Germany
Elzbieta Bukowska, Poznan University of Economics, Poland
Hans-Joachim Bungartz, Technische Universität München (TUM) - Garching, Germany
Diletta Romana Cacciagrano, Computer Science Division, School of Science and Technology, University of Camerino, Italy
Xiao-Chuan Cai, University of Colorado Boulder, USA
Elena Camossi, European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen (IPSC) - Ispra, Italy

Jinyuan Jia, Tongji University, China
Kai Jiang, Shanghai Supercomputer Center, China
Seifedine Kadry, American University of the Middle East, Kuwait
David Kaeli, Northeastern University, USA
Izabela Karsznia, University of Warsaw, Department of Cartography, Warsaw, Poland
Christos Kartsaklis, Oak Ridge National Laboratory (ORNL), USA
Stavros Kassinos, University of Cyprus, Cyprus
Takahiro Kawamura, Toshiba Corporation, Japan
Abdelmajid Khelil, Huawei Research, Germany
Jinoh Kim, Texas A&M University-Commerce, USA
Marie Kim, Electronics and Telecommunications Research Institute (ETRI), Republic of Korea
Alexander Kipp, Robert Bosch GmbH., Germany
Christos Kloukinas, City University London, UK
Alexander Knapp, University of Augsburg, Germany
Manfred Krafczyk, Institute for Computational Modeling in Civil Engineering (iRMB), Braunschweig, Germany
Philipp Kremer, German Aerospace Center (DLR) / Institute of Robotics and Mechatronics - Oberpfaffenhofen, Germany
Herbert Kuchen, Westfälische Wilhelms-Universität Münster, Institut für Wirtschaftsinformatik, Praktische Informatik in der Wirtschaft, Münster, Germany
Michael Lang, Los Alamos National Lab, USA
Robert S. Laramee, Swansea University, UK
Sik Lee, Supercomputing Center / Korea Institute of Science and Technology Information (KISTI), Korea
Paulo Leitão, Polytechnic Institute of Braganca, Portugal
Edgar A. Leon, Lawrence Livermore National Laboratory, USA
Walter Lioen, SURFsara, Netherlands
Yanting Li, Kyushu Institute of Technology, Iizuka, Japan
Fotis Liarokapis, Coventry University, UK
Georgios Lioudakis, National Technical University of Athens (NTUA), Greece
Frank Löffler, Louisiana State University, USA
Darrell Long, University of California, USA
Joan Lu, Informatics, University of Huddersfield, UK
Richard Lucas, University of Canberra and Charles Sturt University, Australia
Teng Ma, NetApp Inc., USA
Tony Maciejewski, Colorado State University, USA
Janna L. Maltseva, Lavrentyev Institute of Hydrodynamics, Novosibirsk, Russia
Dirk Malzahn, OrgaTech, Lunen, Germany
Suresh Marru, Indiana University, USA
Nikolaos Matsatsinis, Technical University of Crete, Greece
Lois Curfman McInnes, Mathematics and Computer Science Division - Argonne National Laboratory, USA
Igor Melatti, Sapienza Università di Roma, Rome, Italy
Despina Meridou, School of Electrical and Computer Engineering (SECE), National Technical University of Athens (NTUA), Greece
Jelena Mirkovic, Center for Shared Decision Making and Collaborative Care Research, Oslo University Hospital, Norway
Hans-Günther Müller, Cray, Germany
Marian Mureșan, Faculty of Mathematics and Computer Science, Babes-Bolyai University, Cluj-Napoca, Romania

Copyright Information

Table of Contents

Internationalisation and Localisation of a Wireless Response System for the Arabic Language

Abduladim Ali and Joan Lu
School of Computing and Engineering
University of Huddersfield
Huddersfield, United Kingdom
{Abduladim.Ali@hud.co.uk, j.lu@hud.ac.uk}

***Abstract*-This paper presents the internationalization and localization of a Wireless Response System for the Arabic language. It outlines the reasons why Arabic was selected as the first language for localization. It states the methods selected for localization and why they were selected. The Arabic interface was tested using native Arabic speakers and the results and analyses of these tests are presented. The paper concludes with an examination of the future work required to improve the Wireless Response System, for people who use Arabic. This work will facilitate future localization of Wireless Response System into other languages.**

Keywords- Arabic Language Translation; Internationalization; localization; M-Learning; Wireless Response System (WRS)

I. INTRODUCTION

The Internet and computer technologies are changing the way teaching and learning are taking place [1]. Software and hardware technology are facilitating new ways of delivering education and testing students. This brings with it significant changes to the process of education, by making learning faster, cheaper and more interactive [2].

These changes are becoming more and more evident in the Arabic speaking countries. The adoption of new technologies requires new software tools to support them and the Wireless Response System (henceforth WRS) is one example of a software that can facilitate this change [3]. The WRS is a Mobile Learning (M-learning) technology which does not currently support the Arabic language. This paper presents the work done to solve this limitation and discusses the localization of the WRS for the Arabic language.

The WRS was developed using Adobe® AIR® runtime and Action Script® with Adobe Flash Builder 4.6. This enables it to run on a range of desktops, smart phones and tablets while using a client server configuration, as shown in Figure 1 below. The Web Server is Apache with (state PHP in full) PHP and a MySQL Database.

In the rest of this paper we introduce the WRS and place internationalization in context. We then discuss M-learning in the Arabic speaking world and present the methods used to create the Arabic interface for the WRS. Finally, we present the results of our tests of the WRS by Arabic speaking users.

II. WIRELES RESPONSE SYSTEM (WRS)

The Wireless Response System (WRS) is an M-learning application. It enables the use, of mobile devices to respond and give feedback and in so doing, enhances the student and teacher interaction. M-learning is defined as Learning across multiple contexts, through social and content interaction, using personal electronic devices [4]. The XML Database and Information Retrieval (XDIR) research group at the University of Huddersfield [5] developed the WRS.

The WRS, like many M-learning applications, is a technology that is used in a wide range of platforms [6] including: PC's, Laptops, Tablets, and Smart Phones; this makes it convenient because it is accessible from virtually anywhere in the world. This technology only requires the user to have access to the internet and a suitable device and therefore offers a very interactive learning experience [7]. As it is portable and highly responsive for instructors and their students, M-learning accommodates the needs of an increasingly mobile student population [5].

The WRS empowers instructors, both in the classroom setting and in the field [8], for example, it enables the instructors to create learning material, while they are on a field trip to a museum, gallery or visiting a site. This then enables them to send the learning material to students and to get response instantly. In so doing, they are fully engaged in the learning activity. Teachers can monitor student responses and adapt the material, to cater for their needs. The ability to create learning material, on the spot and in the field, allows teachers to provide a more learner tailored Education [9]. This enables teachers to meet the specific needs of their students.

One of the limitations of the WRS is its English Language interface. Due to this, the need for internationalization and localization of WRS was identified. Internationalization was necessary because it enabled us to adapt the WRS to many different languages. It was a pre-requisite that enabled us to complete the localization for the Arabic language. The aim of this was to make WRS more accessible to a wider international community of teachers and students.

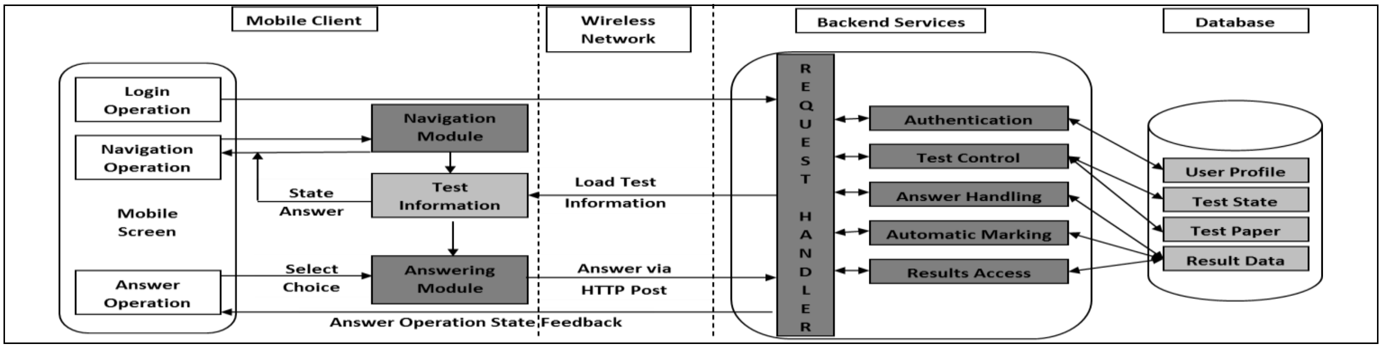


Figure 1. The Architecture of WRS [10].

III. INTERNATIONALISATION I18N

A. Theory

The term Internationalization can be defined as "the process of generalizing a product, so that it can handle multiple languages and cultural conventions, without the need for redesign. Internationalization takes place at the level of program design and document development." [10].

Internationalization is interrelated with translation, localization and globalization. Figure 2 below shows this relationship. It shows that translation is a core part of the localization process, whereas localization is central to internationalization [11]. It is important to understand that globalization manages the process of making software more widely accessible and usable, but internationalization is a process that makes the application available in worldwide markets. Moreover, localization is an essential step that adapts the application to specific linguistic and cultural differences of a given region [12] while translation is the process of recreating the source language text to a target language [13].

B. Technology

The i18n of software is a process of designing and coding software to support localization and translation, to various languages and locales [14].

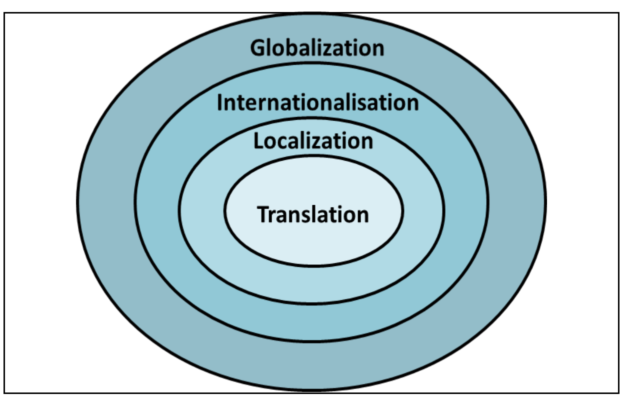


Figure 2. Interrelationship of Translation, Localization, Internationalization and Globalization.

The WRS was modified to support i18n and is now able to support multiple languages. This was achieved through changes to the software code which made it easier to insert additional languages, as need arises. Users are able to select the language of their choice from the interface after starting the application. This was implemented in the form of a drop down selection box on the home page.

IV. LOCALIZATION L10N

The term localization has been defined as adapting a product to a particular locale [13]. A locale refers to a collection of people, who share a common language, writing system and any other properties, which may require a separate version of a particular product. This could be a region, a country, or just a language community [15].

The l10n is a process for tailoring software to a specific language or a specific region. This is done by adding locale specific features into the software such as currency, and date formats. A large part of this process is the translation of the text used throughout the applications interface [3]. The process of translation, in the context of interfaces, is defined as "Communicating the meaning of some data and information from the original language into another intended language" [16]. Kompf states that "translation affects the usability of the interface" [16]. Thus, if the translation is done successfully, it can increase the number of users of the software worldwide [3, 17].

The WRS has been translated into Arabic, Italian, Romanian and Indonesian. In the rest of this paper, we focus on the Arabic localization, with a close look at the interface and some of the challenges it presented.

V. ARABIC LANGUAGE

The Arabic language is one of the world's oldest languages. Currently, it is the fifth most used language worldwide. It is spoken by a significant percentage of the world's population. More than 290 million people speak Arabic as their first language[17, 18]. As a result, Arabic is an important language on the Internet. This is partly due to the growing number of Arabic speakers online, many of whom are searching for Arabic content and applications online. Recent figures from the Internet World Statistics

 ISBN: 978-1-61208-365-0

show that there are 90 million Internet users from the Arab speaking world [3].

A. M-learning in the Arabic Speaking World

M-learning has become an essential tool used to enhance the learning process in the Arabic speaking world. This is reflected at the highest levels; in governments and policy making circles. In many cases, budgets have been allocated and policies implemented in order to enhance M-learning [19]. We give some examples from the Arab world below:

In September 2012, the Qatari government announced, that all the instructional content in the public schools would be stored in digital format by 2013; this work started in 2011. The Kuwaiti government also began rolling out the mobile learning products in middle schools, elementary schools and kindergartens. By October 2012, all the textbooks in Kuwait were digitized [20].

In June 2013, the UAE government indicated that they would equip all state run schools with learning platforms by 2015. The UAE Education minister announced that they were establishing a state of the art Information and Communications Technology (ICT) infrastructure in all the state schools. They would be publishing 7,000 e-lessons and e-contents. They stated that every student in the public schools would be using a personal device for learning by 2017 [20]. The UAE government launched a project to provide every student with an electronic tablet and access to high-speed 4G networks by 2017. It envisioned that over 20,0000 personal learning devices would by then be distributed to the public schools and students [20].

Further to this, the government of the UAE launched the federal higher education mobile learning initiative. In this initiative, about 14,000 iPads were distributed to all first term students in the three federal universities. These tablets were preloaded with educational apps [20].

Another Arabic speaking country: Egypt has also announced a large-scale project, in which over 20 million tablets will be distributed to different schools in stages by 2018. This government had distributed over 10,000 tablets by August 2013 [20].

The Saudi Electronic University (SEU) was launched in August 2011 by the Saudi government. In 2013, the SEU launched their mobile-friendly site in HTML, which can be viewed on a smart phone [20].

In the last example, the Arab Open University makes extensive use of mobile learning, in their educational programs. They are a pioneer of mobile learning in the region, having launched a content library for java-enabled phones as early as 2007 [20].

These developments in the Arabic speaking world make a compelling case for why the WRS should be localized to the Arabic language.

VI. METHOD USED TO CREATE ARABIC INTERFACE FOR WRS

Two approaches were considered for translating the WRS interface: The first was to use online translation tools. Several of these tools were tested. Some of these tools were discovered to be more widely used than others, for example Google Translate [3]. All the tools we tested presented problems in a number of areas. These included: grammatical structure, spelling, sentence clarity and logic [2] as a result, it was difficult to produce clear and understandable Arabic translations using this method. While some of these tools proved to be more useful than others it was clear that they would not be sufficient in themselves.

The second approach was to use a specialist in the Arabic language who was also a native speaker. This approach was preferred because it gave a more precise translation, with a more consistent style in the Arabic language and vocabulary.

Adobe Flex Builder 4.6 and Adobe Action Script® were used to code the application. This was used for the development work on the teacher interface. For the student interface, the PHP programming language was used.

To make the task of localization simpler and more manageable for developers, it was divided into two phases: the first phase was the translation of both the trigger side and response side of the WRS's interface, and the second phase consisted of the testing and the evaluation of these two sides to understand how teachers and students experienced them.

A. Translation of WRS Interface

The translation Interface was broken down into three steps. The first step was to undertake analyses of the system; this was achieved by using the WRS in a practical session, with teachers and some students. It was done jointly with the developers and coders from whom we gained a deeper understanding of how the WRS works, for both teachers and students. Insight was also gained by using the WRS in the role of a teacher and a student on different devices. A valuable exercise at this point, was the production of the flow charts shown in Figure 3. It shows the different elements of the teachers interface. These helped in visualizing and understanding the system as a whole.

The second step required the extraction of all the English language text used in the interface. This was very useful as it served to highlight all the words and phrases used in the interface. A document was at this point produced to manage all the WRS's interface text. An extract from this document is shown in Table I WRS Interface Text Translation. Language translators and developers maintain this document and it is used by developers to code the language into the WRS.

Developers add any new text used in the application to this document. The translators maintain the translations for each language. This makes it simpler to code each language into the localization files. A unique identifier (UID) is used to identify each pair of words or phrases.

TABLE I. WRS INTERFACE TEXT TRANSLATION

UID	English	العربية
1	Wireless Response System	نظام الاجابة اللاسلكية
1_1	Sign in	تسجيل الدخول
1_2	Support	دعم

The translation involves analyses of each word and its use in context. This helped us to produce a more accurate translation for the Arabic version.

The third step of this process required the table, to be coded into the application. Because the WRS will support several languages, each language will have its own folder and a file.

This file will localize the application to one locale. With this structure the WRS will be able to support any additional languages that are added in the future.

The final step of the translation process involved testing the Arabic interface. First a walk through test was done to ensure that all the English text was showing in the Arabic language.

Then, a side by side comparison was made to see how the two interfaces looked. Figure 4 shows the student interface side by side in the two languages. The same review process was done for the teacher interface and an example is shown in Figure 5.

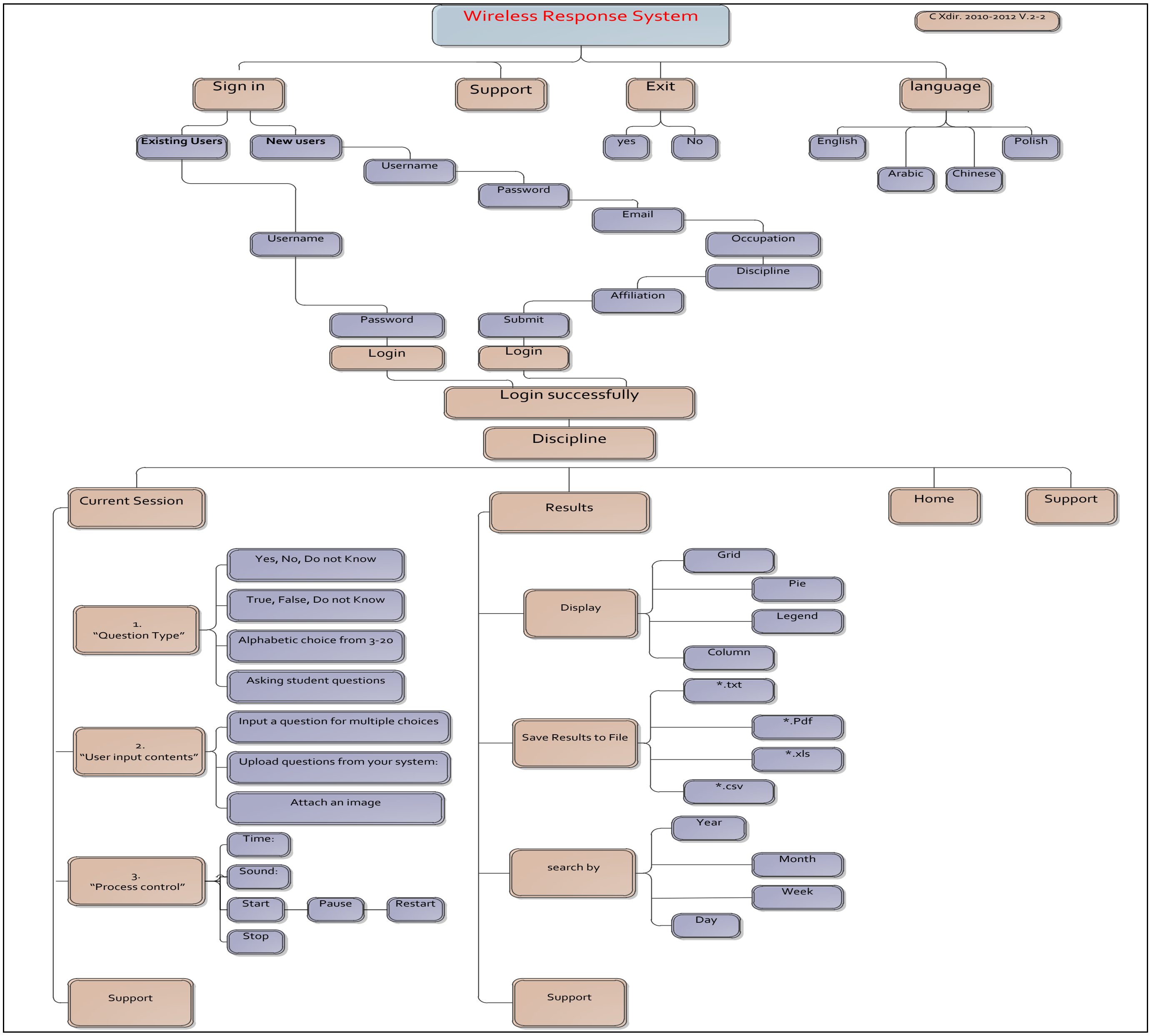


Figure 3. WRS Teacher Interface Elements .

Figure 4. WRS Student Interface English and Arabic.

B. Testing and Evaluation of the WRS

Both the student and the teacher Arabic language interfaces were tested. A sample of thirty Arabic speakers was used to test the WRS. These users were selected from the international student community at the University of Huddersfield. While all of them were students, some of them were also teachers in their home countries. This enabled them to understand and test the WRS from both the student and teacher perspective. All the testers were new to the WRS and had not used it before.

A test script was produced outlining several test cases, to test both the student and teacher interfaces. Each tester was asked to complete the test cases and provide feedback. Testers were asked for any comments or feedback they wished to make about the test they had just performed. The testers were also asked to evaluate the interfaces, in terms of their functionality and usability.

The testing environment consisted of a Laptop (PC or Apple), iPhone Smart phones, and iPod or iPad tablet computers.

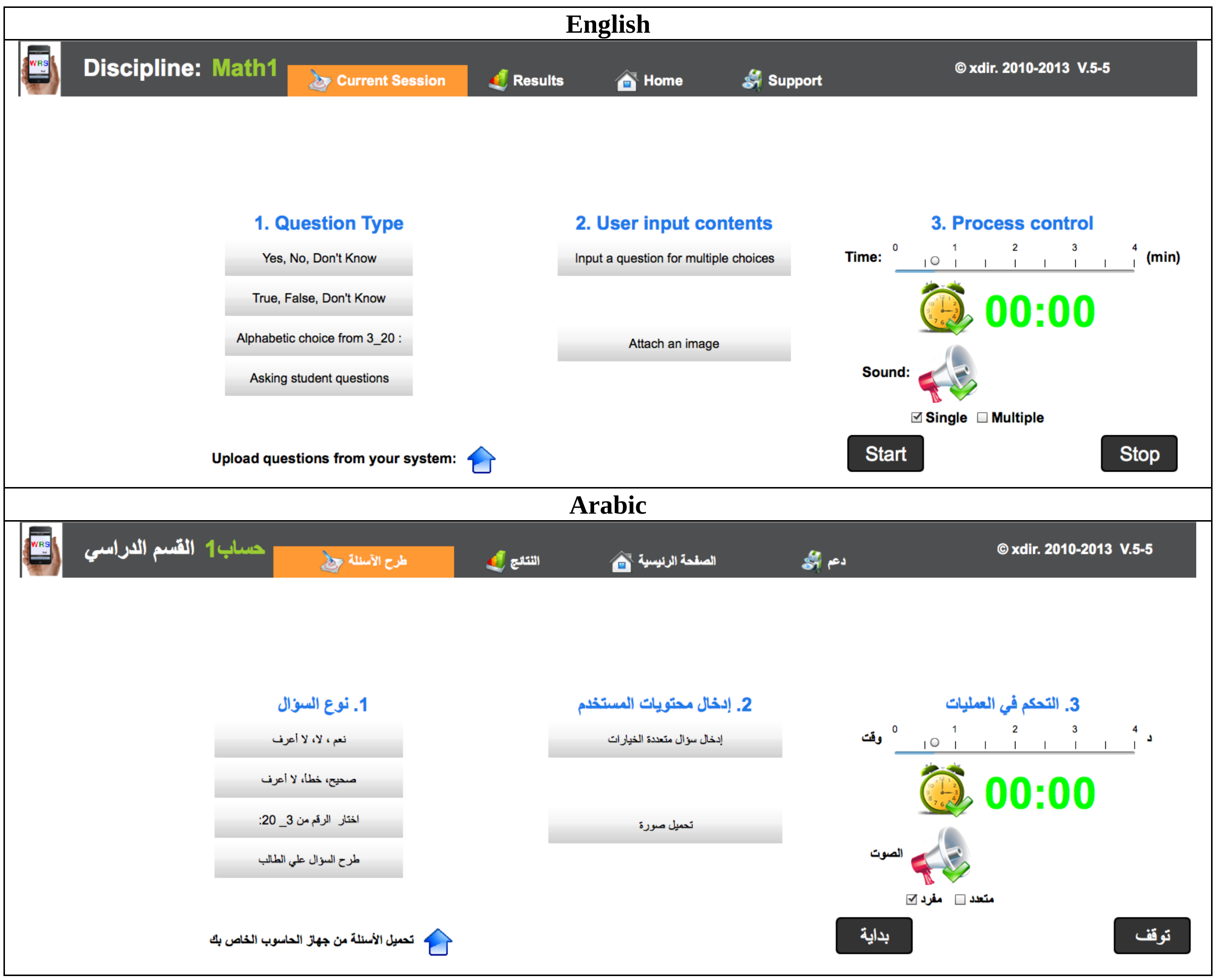


Figure 5. User Testing of WRS's Teacher Interface, Functionality and Usability.

 ISBN: 978-1-61208-365-0

C. Test Cases

We used test cases to test specific elements of the teacher and student applications. Table II shows the test cases we used to test the teacher interface. Some of the insights gained from this testing are shown in the test results column. Table III, on the other hand, shows the test cases used to test the student interface of WRS.

D. Testing the Teachers Application

In the teacher application interface, functionality and usability was tested. The results are presented in Figure 6 below. A few interesting points emerged from this testing. For example, on the results screen, testers found that the charts were very useful for viewing the responses from the students. However, they found that the date alone was not an efficient or effective way to search past tests and results. They rated this as below average and suggested that improvement could be made to facilitate better searching. They also felt that teachers would benefit better if more data was collected for each test giving them greater insight into the progress attained by students and the effectiveness of the teaching material used.

All the users tested the functionality of the teachers' application. This included the installation and the launching of the WRS-Teachers Application, which was done successfully by all the testers. They gave this an average and an above average rating.

Signing in was also completed by all the testers. Some of the testers suggested the interface could be made simpler, by combining the two "Existing Users" and "New User" dialogue boxes into one box. Testers suggested that, as the "New User" interface would only ever be used once by a new user, it should not be shown separately or take up so much space on the screen. They pointed out that combining them would make the interface less cluttered.

TABLE II. TEST CASES USED TO TEST WRS ARABIC TEACHERS APPLICATION AND RESULTS

No	Test Case	Test Result
1	Application Launch	All the testers managed to successfully launch the application and select the Arabic interface.
2	Sign In	All the testers signed in successfully. Some testers noted that they could not recover usernames or passwords to their email addresses. Some of them also pointed out that the interface could be improved by combining the existing user and new user's login boxes into one box.
3	Current Session	Some of the users noted that the start and stop buttons on the current session screen, was Left-to-Right (LTR) and not Right-to-Left (RTL). It was also felt by many testers that this interface was a little confusing. Partly because of the mouse over action that brings elements into view. These are not shown by default. Some users had to use trial and error to discover how to navigate this screen. Also, they pointed out that the work flow in this screen was not intuitive, especially for the multiple choice questions.
4	Result	Many of the testers commented on the graphs. They noted how it could rapidly inform the teacher of the student's comprehension. They felt this rapid feedback empowered the teacher allowing them to adapt the teaching material and testing to focus on specific areas.
5	Home	All the testers managed to complete this test case successfully.
6	Support	Testers commented that the font size was too small. The text was not aligned properly to the right hand side making it difficult to read.
7	Exit	This test case was completed successfully by all the testers. Some commented that the confirmation dialogue box was not necessary.

TABLE III. TEST CASES USED TO TEST WRS ARABIC STUDENTS APPLICATION AND RESULTS

No	Test Case	Test Result
1	Application Launch	The student application was launched successfully by all the testers and the Arabic interface was selected from the language drop down box.
2	Sign In	All the testers signed in successfully. Testers suggested Discipline and Student ID was not secure enough for student logins and opined that a password would be more appropriate. They also rooted for an option for email recovery of lost passwords.
3	Respond to Questions	Testers found this simple and easy to use.

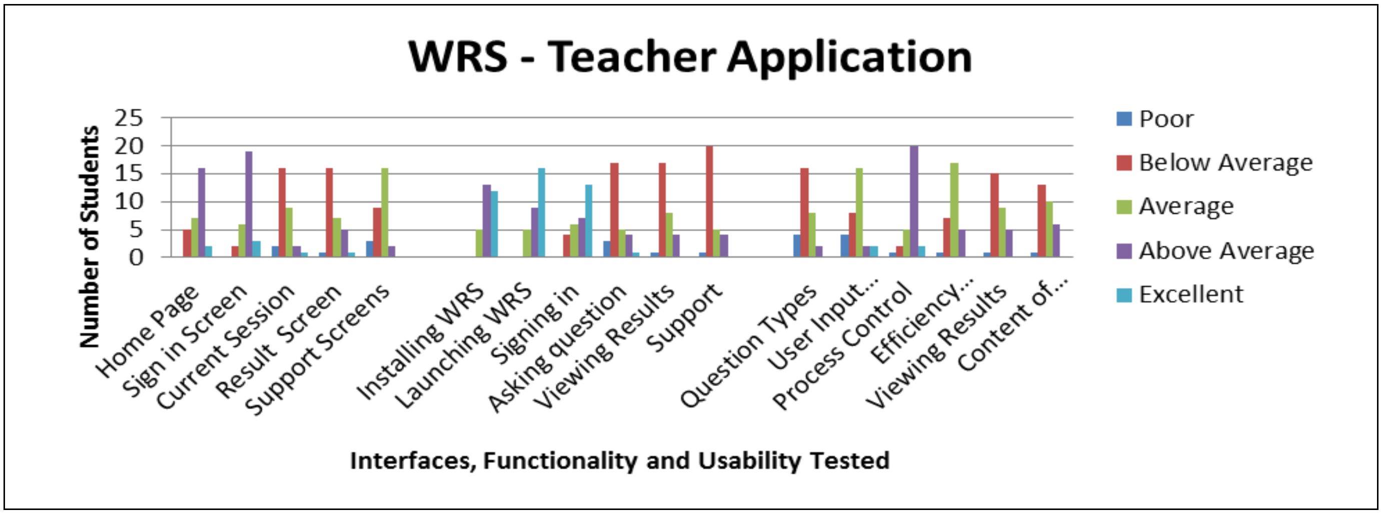


Figure 6. User Testing of WRS Teacher Interface, Functionality and Usability.

Testers found the functionality for asking questions was limited. They would have liked more question types and due to this, they rated it as below average. The testers also rated the functionality for "Viewing Results" as below average. They suggested it could be improved, to show results for a time period for example, one term or one academic year. This would enable them to see students' progress over a period of time. Currently the "Viewing Results" only shows the result test by test.

Testers found Support in the application was minimal for the users. This was reflected in the below average rating they gave to this. Some testers found the font difficult to read. They also suggested more support text could be offered in the help text. Our Arabic testers also rated the usability of the "Question Types" as below average saying this part of the interface could be improved to make it more usable. A further suggestion was that the Arabic interface would work more effectively if the question was presented in the interface alongside the responses

The User Input Content was rated as average. Feedback from testers suggested that this could be made more efficient. Users found the process control simple to use, enabling them to control the time allocated for a response to the question. The usability of this was rated as above average. Users found this very usable and easy to understand.

Users rated the efficiency of this interface as average. The ability to paste multiple questions into the system it was noted would increase the interface efficiency, while the ability to save and reuse old questions or adapt them into new questions would also improve the efficiency.

Testers commented on Viewing Results, which they said could be improved. Many testers found the charts very useful. However, they commented that access to the historical results could be made easier and simpler, by giving users the option to search using additional criteria. Finally, the testing of the Content of Support in WRS identified problems with the Arabic font. Many users found this font difficult to read.

E. Testing WRS Student Application

The student applications interfaces, functionality and usability, was tested on smart phones, tablets and PCs and the results are shown in Figure 7. Our testers rated the interface as above average on the smart phones and tablets. Some of our testers suggested the interface while interactive, could be improved and made more responsive. They suggested that the time remaining to answer the question could be shown on the interface.

Smartphone functionality was tested and the majority of testers found it was above average and excellent. All in all, testing showed that our users found the student interface could be used efficiently, effectively and interactively.

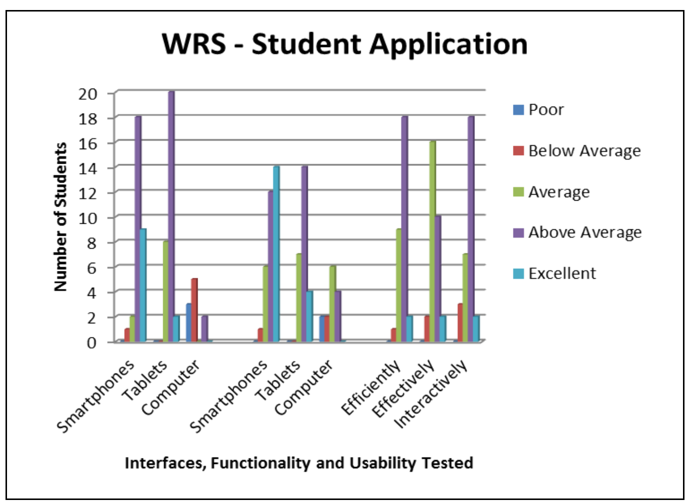


Figure 7. User Testing of WRS Student Interface, Functionality and Usability.

VII. CONCLUSION AND FUTURE WORK

A. Conclusion

Internationalization and localization of WRS to the Arabic language has made it accessible to new users. It has also provided a new insight into how the application itself could be improved.

Attention has been drawn to the following:

1. Testing showed that WRS Arabic interface was usable by both students and teachers.
2. Native Arabic users found the interfaces easy to use in the Arabic language.
3. Improvements need to be made to some parts of the interface to help improve the layout, login and searching for students' past test results
4. Testers found they needed more questions types to test students more effectively.
5. Users expressed a need for more application help to explain how each interface should be used.
6. Testers suggested that the students' interface should show a countdown of the time remaining to answer the question.
7. Student access to WRS could be made more secure by using a password in place of the current Student ID number.

This process, of localizing the WRS to Arabic, has helped to pave the way for localization to other languages. It has also highlighted ways in which future versions of WRS and interfaces could be improved.

B. Future Work

Testing has been very valuable in providing feedback and insight into the WRS. The XDIR group will incorporate these into future versions of WRS. These will include:

1. More question types.
2. Improved interface layout and design in order to support RTL and LTR languages more effectively.
3. The WRS interface workflow will be improved to help and aid future localization.
4. The Current Session interfaces will be changed to only show what is needed when it is needed. This will improve WRS usability and aid future localization of the application and at the same time make the interface simpler to use.
5. Future versions of the WRS will also support more languages in addition to English and Arabic, these will include: Italian, Romanian, Turkish, Indonesian, Polish and Mandarin Chinese with other languages being added as required.

ACKNOWLEDGMENTS

The author would like to sincere appreciation for the support and constructive discussions from Wei Guo, the Libyan embassy; for financial support and (XDIR) Research Group at the University of Huddersfield.

REFERENCES

[1] A. Kurti, M. Milrad, F. Alserin, and J. Gustafsson, "Designing and implementing ubiquitous learning activities supported by mobile and positioning technologies," in *the Ninth IASTED International Conference computers and Advanced Technology in Education, Lima, Peru*, 2006.

[2] A. Al-Amoudi, H. AlMazrua, H. Al-Moaiqel, N. AlOmar, and S. Al-Koblan, "An Exploratory Study of Arabic Language Support in Software Project Management Tools," *International Journal of Computer Science Issues (IJCSI),* vol. 10, 201.3

[3] N. Albalooshi, N. Mohamed, and J. Al-Jaroodi, "The challenges of Arabic language use on the Internet," in *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for*, 2011, pp. 378-382.

[4] H. Crompton, "A historical overview of mobile learning: Toward learnercentered education," *Handbook of mobile learning. Florence, KY: Routledge*, p. 4, 2013.

[5] F. Manga and J. Lu, "An Investigation in the Impact of Mobile Learning on today's Educational Environment," *International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government.EEE (2013). WorldComp 2013,* 2013.

[6] J. Lu, R. P. Pein, G. Hansen, K. L. Nielsen, and J. B. Stav, "User Centred Mobile Aided Learning System: Student Response System (SRS)," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 2010, pp. 2970-2975.

[7] Z. Lu and I. Global, *Learning with mobile technologies, handheld devices, and smart phones: Innovative methods*: Information Science Reference, 2012.

[8] J. Lua, Z. Meng, G. Lu, and J. B. Stav, "A new approach in improving operational efficiency of wireless response system," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 2010, pp. 2676-2683.

[9] J. Lu, "Student Response System (SRS)/Wireless Response System (WRS)–a Next-Generation Student Response System for Academia and Industry," 2011.

[10] B. Esselink, *A practical guide to localization* vol. 4: John Benjamins Publishing, 2000.

[11] N. De Liso and R. Leoncini. (2010). *Internationalization, Technological Change and the Theory of the Firm (1 ed.)*. Available: http://hud.eblib.com/patron/FullRecord.aspx?p=557254

[12] E. M. Del Galdo and J. Nielsen, *International users interface*: John Wiley & Sons ,Inc., 1996.

[13] P. Sandrini, "Website localization and translation," in *EU-High-Level Scientific Conference Series MuTra*, 2005.

[14] S. Casteleyn, F. Daniel, P. Dolog, and M. Matera, *Engineering Web Applications*: Springer, 2009.

[15] M. A. Jimenez-Crespo ,*Translation and Web Localization*: Routledge, 2013.

[16] M. Kompf, "Usability and internationalization of information technology," *Education and Information Technologies*, vol. 11, pp. 187-189, 2006.

[17] N. Aykin, *Usability and internationalization of information technology*: CRC Press, 2004.

[18] G. P. International. (2013). *The Arabic Language*. Available: http://www.globalizationpartners.com/resources/arabic-translation-quick-facts/the-arabic-writing-system.aspx

[19] A. Sawsaa, J. Lu, and Z. Meng, "Using an Application of Mobile and Wireless Technology in Arabic Learning System," *Learning with Mobile Technologies, Handheld Devices and Smart Phones: Innovative Methods,* p. 171, 2012.

[20] S. S. Adkins, "The 2012-2017 Middle East Mobile Learning Market," *Ambient Insight Regional Report*, 2013.

Semi-Analytic Modelling of Stratified Flows

Theory and Applications

Nikolay Makarenko, Janna Maltseva, Alexander Cherevko
Lavrentyev Institute of Hydrodynamics,
Novosibirsk State University,
Novosibirsk, Russia
{makarenko,maltseva,cherevko}@hydro.nsc.ru

Abstract— **The problem on non-homogeneous shear flows over the rough terrain is considered semi-analytically. Mathematical modelling of these flows is interesting due to important applications in meteorology and oceanography. Known results presumably refer to the wave phenomena appearing in the flows over single bell-shaped obstacle. Presently, most intrinsic problem is to describe a complicated interference patterns which can be forced by multiple-ridged topography. In this paper, a non-linear model of a stratified flow over combined obstacle is constructed under the small amplitude assumption for the topography. Attention is focused on the stationary wave patterns formed directly above the hill range. Wave solutions corresponding to the topography with a finite number of peaks are calculated. These solutions predict rigorously the splitting of a near-field flow to the separate wave zones having different spatial scales.**

Keywords-semi-analytical mode; perturbation method; stratified flows.

I. INTRODUCTION

Modeling of stratified flows plays a significant role in several environmental disciplines, especially in meteorology and oceanography [1][2]. Internal waves in the non-homogeneous atmosphere and ocean are generated frequently from the interaction of the mean flow with orographic obstacles, such as mountains and submarine ridges. Lee waves arise downstream of the obstacle under appropriate upwind conditions. These waves possess horizontal lengths amounting to tens of kilometers and typical magnitudes of vertical displacement are on the order of hundreds of meters. Therefore, they can present a hazard to air traffic and sub-sea operations.

The theory of lee waves deals with the mathematical model of inviscid incompressible non-homogeneous fluid. Long's model is based on the linear Helmholtz equation for a steady stream function which should satisfy appropriate boundary conditions and radiation condition at infinity (we refer to the paper [3] for a mathematical details of the Long's theory).

This linear partial differential equation arises as a leading-order approximation to more general non-linear Dubreil-Jacotin – Long equation of stratified fluid [4]. Despite the linearity, explicit analytic solutions are known only for the simplest topographies, such as a single semi-circular obstacle [5][6]. Numerical solutions to Long's theory also encounter substantial difficulties due to the specific form of a boundary condition for arbitrary topography [7][8].

We develop a semi-analytical approach [9] involving the von Mises transformation of both dependent and independent variables in the non-linear version of the Dubreil-Jacotin – Long equation. The main idea of this method is to satisfy the exact topography condition by solving approximate equations in an auxiliary rectangular domain. The impact of the non-linearity is analyzed by the perturbation procedure with a small parameter which characterizes typical height of an obstacle. Our attention is focused on the fragmentation effects for the near-field wave patterns forced by the rough topography of finite extension.

This paper is organized as follows: Section II describes the mathematical setup, including the formulation of a basic model; Section III characterizes the perturbation procedure combined with the Fourier method to construct an analytical solution; Section IV illustrates preliminary results of numerical modelling of stratified flows. Discussion and conclusions are presented in Section V.

II. MATHEMATICAL FORMULATION

The mathematical model of a steady stratified 2-D flow over an uneven bottom is formulated as the boundary value problem for a second-order elliptic partial differential equation, i.e., DJL (Dubreil-Jacotin – Long) equation, which has the form

$$\psi_{xx} + \psi_{yy} + \lambda(\psi - y) = \frac{1}{2}\sigma\left(\psi_x^2 + \psi_y^2 - 1\right), (-\infty < x < \infty),$$

$$\psi(x, \alpha y_0(x)) = 0, \quad \psi(x,1) = 1, \tag{1}$$

$$\psi(x, y) \to y \quad (x \to -\infty).$$

Here, the unknown function $\psi(x, y)$ is the stream function and the constants $\sigma > 0$ and $\lambda > 0$ are the Boussinesq parameter and the inverse densimetric Froude number, respectively. These dimensionless parameters are defined by the formulae

 ISBN: 978-1-61208-365-0

$$\sigma = \frac{N^2 h}{g}, \quad \lambda = \frac{\sigma g h}{c^2},$$

where g is the gravity acceleration, h is the total depth of the stratified fluid layer, N is the constant Brunt–Väisälä frequency (i.e., the buoyancy frequency of air or ocean water), and c is the speed of the far-upstream flow. Quantity σ determines the slope of the density profile for a uniformly stratified fluid being at rest and λ indicates the value of the sub- or super-criticality of the upstream flow with respect to the phase speed of infinitesimal internal waves. Finally, the small parameter α characterizes a typical height of the bottom topography $y = \alpha y_0(x)$ towered above the ground level *y=0*.

From the mathematical point of view, problem (1) is a non-linear eigenvalue problem with spectral parameter λ as the bifurcation parameter. A non-trivial wave solution can bifurcate from the wave-less regimes if the magnitude of topography α is sufficiently small. Bifurcation occurs by λ belonging to a continuous spectrum of linear waves (see Fig. 1).

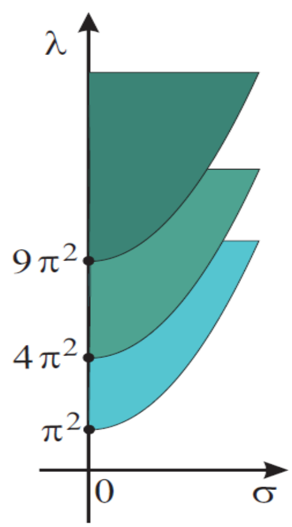


Figure 1. The spectrum of normal modes.

A parametric range of *m*-modal lee waves is formed by the sub-critical spectral domain determined by the inequalities

$$\pi^2 m^2 + \frac{1}{4}\sigma^2 < \lambda < \pi^2 (m+1)^2 + \frac{1}{4}\sigma^2.$$

Based on that, a non-trivial solution should have periodic asymptotics with respect to spatial variable x far-downstream the obstacle. In that sense, problem (1) can be also considered as the non-linear diffraction problem. The main difficulty is that the amplitude of stationary wave forced behind the obstacle is unknown ***a priory***.

III. ANALYTIC SOLUTION

We apply a semi-analytical approach involving von Mises transformation of the DJL equation. Namely, we seek the streamlines in the form $y = Y(x,\psi)$ with a new independent (x,ψ) -variables so that the flow domain transforms to the unit strip $0 < \psi < 1$. This transformation does not permit overhanging streamlines which are typical for developed structures of lee waves of large amplitude. However, such a geometric assumption allows to satisfy the exact topographic boundary condition at leading order approximate solution.

By given σ and λ, we construct solution $Y(x,\psi)$ with small α as the power series

$$Y(x,\psi) = \psi + \alpha w_0(x,\psi) + \alpha^2 w_1(x,\psi) + \ldots$$

The leading-order coefficient w_0 should satisfy both the homogeneous linear partial differential equation and the non-homogeneous topographic boundary condition at the bottom line $\psi = 0$; such that we have a linear elliptic boundary value problem

$$w_{0xx} + w_{0\psi\psi} - \sigma w_{0\psi} + \lambda w_0 = 0, \quad 0 < \psi < 1,$$
$$w_0(x,0) = y_0(x), \quad w_0(x,1) = 0.$$

Certainly, this approximation corresponds to the familiar equations of the Long's model. The difference is that here this model involves a more convenient topographic boundary condition than usual.

For Froude number λ belonging to the sub-critical spectral range of *m*-modal lee waves, we obtain the leading-order solution as follows:

$$w_0(x,\psi) = e^{\frac{\sigma\psi}{2}} \left\{ W(\psi) y_0(\psi) + \sum_{n=1}^{\infty} w_0^{(n)}(x) \sin \pi n \psi \right\}. \quad (2)$$

Here, function $W(\psi)$ corresponds to the hydrostatic mode of the flow over uneven bottom. This function is given by the formula

$$W(\psi) = \frac{\sin k_0 (1-\psi)}{\sin k_0}, \quad k_0 = \sqrt{\lambda - \frac{\sigma^2}{4}}.$$

The wave number k_0 here is real while parameter λ is sub-critical and Fourier-coefficients $w_0^{(n)}(x)$ are determined by the shape of the obstacle only.

Similarly, we can construct the second-order solution, which takes into account a non-linear correction of the flow by solving the boundary value problem

$$w_{1xx} + w_{1\psi\psi} - \sigma w_{1\psi} + \lambda w_1 = f(w_0), \quad 0 < \psi < 1,$$
$$w_1(x,0) = w_1(x,1) = 0.$$

Here, the right-hand side involves the non-linearity, which has the form

$$f = \left(w_x w_\psi\right)_x + \frac{1}{2}\left(w_x^2 + 3w_\psi^2\right)_\psi - \frac{1}{2}\sigma\left(w_x^2 + 3w_\psi^2\right).$$

For known w_0, solution w_1 can also be presented as an infinite modal Fourier-series (2) with separated variables x and ψ.

IV. Examples of Calculated Wave Patterns

Wolfram Mathematica® [10] was used at all stages of semi-analytic calculations. Symbolic computer algebra was applied to present truncated solution (2), which provides fast convergence. Most of the numerical simulations used the series for coefficients w_0 and w_1 with ten basic harmonics. Computational flow domain involved the discretization with 50 points in horizontal direction x and 10 points in ψ. The calculation of a non-linear second-order solution used a numerical result for a leading-order linear solution presented by 6-order interpolation splines. Multiple series of calculations were carried out on the two node computer cluster at Novosibirsk State University.

Figure 2 and Figure 3 demonstrate some examples of the calculated 1-mode lee wave patterns, which appear in the flow region over the finite number of obstacles. Parameters α and λ are taken as α =0.04 and λ=15 in all cases. The Boussinesq parameter σ is chosen as σ =0.2.

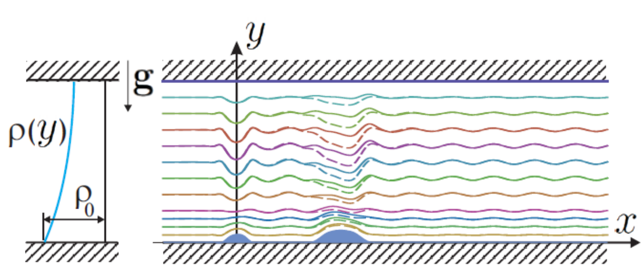


Figure 2. Lee waves over two bell-shaped obstacles.

Figure 2 illustrates the influence of the non-linearity on the stratified flow formed over the double bell-shaped topography. The non-linearity essentially corrects only the wave column immediately above the second obstacle but the downstream wave-tail still remains non-perturbed behind the obstacles.

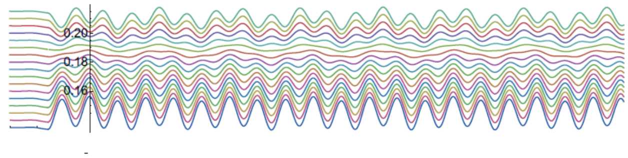


Figure 3. Separation of stratified flow.

Figure 3 illustrates an interesting effect of the wave interference, which can be observed in the near-bottom region of the boundary-trapped waves over a multi-hill topography. The near-bottom flow is clearly separated from the upper region of slowly modulated waves having the maximum amplitude at the mid-height of the fluid layer. The separation between lower and upper wave zones occurs at the height predicted by the zero points of the hydrostatic mode.

V. Conclusion and Future Work

In this paper, we outline semi-analytic approach assigned to simulate atmospheric stratified flows over combined 2D topography. The method exploits calculation the Fourier series which present modal decomposition of the waves forced by localized multi-bumped obstacle. Such an analytic solution of fluid mechanics is constructed by the perturbation procedure taking into account the non-linearity of mathematical problem. As noted, the limitations can arise by modelling the flows with overturning streamlines above the sharp-crested terrain with high peaks. However, the method seems to be well-conditioned while it predicts realistically the fragmentation of wave patterns due to interference of lee waves from adjacent ridges. Preliminary results demonstrate the ability to provide fast computations of the flows even for irregular-shaped topography. From a geophysical viewpoint, an efficient method is also needed to provide accurate computation of the fronts of separated wave zones. This work is in progress now. Next technical steps will operate with obtained Fourier solutions in order to evaluate analytically the impact of modal decomposition on the fragmentation effect observed by numerical experiments. Furthermore, we also plan to extend this method to modelling of stratified air flows over topography in local regions being of interest from meteorological viewpoint. By that, important issue is to estimate the computation requirements which are asserted to the algorithm by such a real topography.

Acknowledgment

The work was supported by the Russian Foundation of Basic Research (grant No 12-01-00671) and the Program RAS No 23 (Project No 2).

REFERENCES

[1] R. S. Scorer, Environmental Aerodynamics, Halsted Press, N.-Y., 1978.

[2] P. G. Baines, Topographic Effects in Stratified Flows, Cambridge Univ. Press, New-York, 1995.

[3] R. R. Long, "Finite amplitude disturbances in the flow of inviscid rotating and stratified fluids over an obstacle," Annu. Rev. Fluid Mech., no 4, Jan. 1972, pp. 69–92.

[4] M. L. Dubreil-Jacotin, "A complement an earlier note on permanent type waves in heterogeneous liquids", Atti Acad. Lincei Rend. Cl. Sci. Fis. Mat. Nat., vol. 21, no 6, 1935, pp. 344–346.

[5] V. N. Kozhevnikov, "Orographic perturbations in the two-dimensional stationary problem", Atmos. Ocean. Phys. (Izv. Akad. nauk SSSR, Fiz. atmos. okeana), vol. 4, July–Aug. 1968, pp. 16–27.

[6] J. W. Miles, "Lee waves in a stratified flow. Part 2," Semi-circular obstacle. J. Fluid Mech., vol. 33, no 4, Sept. 1968, pp. 803–814.

[7] M. Humi , "Long's equation in terrain following coordinates," Nonlin. Processes Geophys., no 16, Aug. 2009, pp. 533–541, doi:10.5194/npg-16-533-2009.

[8] D.J. Muraki, "Large-amplitude topographic waves in 2D stratified flow," J. Fluid Mech., vol. 681, June 2011, pp. 173-192.

[9] N. I. Makarenko and J. L. Maltseva, "Interference of lee waves over mountain ranges," Nat. Hazards Earth Syst. Sci., vol. 11, Jan. 2011, pp. 27–32.

[10] Wolfram Research, Inc., Mathematica, Version 9.0, Champaign, IL (2012).

Minimizing Total Tardiness in a Hybrid Flexible Flowshop with Sequence Dependent Setup Times

Aymen Sioud, Caroline Gagné, and Marc Gravel
Département d'informatique et de mathématique
Université du Québec à Chicoutimi
Email: asioud@uqac.ca, c3gagne@uqac.ca, mgravel@uqac.ca

***Abstract*—In this paper, we propose different local search algorithms to solve a realistic variant of the flowshop problem. The variant considered here is a hybrid flexible flowshop problem with sequence-dependent setup times, and with the objective of minimizing the total tardiness. In this variant of flowshop, stage skipping might occur, i.e., not all stages must be visited by all jobs. This scheduling problem is frequently used in batch production, helping to reduce the gap between research and operational use. While there is some research on minimizing the makespan, to our knowledge no work has been reported on minimizing the total tardiness for this problem. The proposed approaches present different neighborhood searches. Numerical experiments compare the performance of the different algorithms on new benchmarks generated for this problem.**

Keywords*—*hybrid flexible flowshop; sequence dependent setup times; total tardiness; local search; scheduling.

I. INTRODUCTION

Scheduling problems are decision-making processes with the goal of optimizing one or more objectives. Indeed, they deal with the allocation of resources to perform a set of activities over a period of time [1]. The Flowshop scheduling problem is one of the most well-studied scheduling environments in the last decades. In this configuration, all jobs follow the same operational order, where a set of n jobs need to be processed in a set of m machines disposed in series. All jobs follow the same processing route through the machines, i.e., they are first processed on machine 1, then on machine 2 and so on until machine m. This associated problem can be considered as the basic model for several variants of real problems. Moreover, real production systems rarely employ a single machine at each stage. Therefore, in many situations, the regular flowshop problem is extended to a set of usually identical parallel machines at each stage. That is, instead of having a series of machines, we have a series of stages of parallel machines. The goal here is to increase the capacity and reduce the impact of bottleneck stages. Furthermore, it is frequent in practice that optional treatments are applied on products, like polishing or additional decorations in ceramic manufacturing as examples [2][3]. In this latter case, some jobs will skip some stages. We obtain thereby the hybrid flexible flowshop.

Moreover, in many industries such as pharmaceutics, metallurgy, ceramics and automotive manufacturing, there are setup times on equipment between two different jobs. Many papers assume that setup time is negligible, or part of the job processing time. But explicit setup times must be included in scheduling decisions in order to model a more realistic variant of hybrid flowshop scheduling problems. These setup times may or may not be sequence dependent. Dudek et al. [4] reported that 70% of industrial activities include dependent setup times. More recently, Conner [5] pointed out in 250 industrial projects that 50% of these projects contain setup-dependent times and when these setup times are applied, 92% of the order deadline could be met. Production of good schedules often relies on good management of these setup times [6][7].

The present paper considers the hybrid flexible flowshop problem with sequence dependent setup times (SDST/HFFS) minimizing the total tardiness. In accordance with the notation for hybrid flowshops introduced by Vignier et al. [8] who extended the well-known three fields notation $\alpha/\beta/\gamma$ of Graham et al. [9], this problem is noted as $((PM)^{(i)})_{i=1}^{m}/F_j, s_{ijk}/\Sigma T_j$. According to Du and Leung [10], the total tardiness minimization problem is NP-hard for the specific case of one machine and therefore the SDST/HFFS total tardiness problem studied in this article is also NP-hard.

The $((PM)^{(i)})_{i=1}^{m}/F_j, s_{ijk}/\Sigma T_j$ problem may be defined as a set of N jobs, $N=\{1,..., n\}$ available for processing at time zero on a set of M stages, $M=\{1,..., m\}$. At every stage i, $i \in M$, we have a set of M_i, $M_i=\{1,..., m_i\}$ of identical parallel machines. Every machine at each stage can process all the jobs. Each job has to be processed in exactly one out of the M_i identical parallel machines at stage i. However, some jobs will skip some stages. F_j denotes the set of stages that the job j, $j \in N$ has to visit. Furthermore, only stage skipping is allowed, so it is not possible for a given job to visit stages $\{1, 2, 3\}$ and another one to visit stages $\{3, 2, 1\}$. p_{ij} denotes the processing time of job j at stage i. Each job have a due date noted as d_j. Finally, s_{ijk} denotes the setup time between jobs j and k, $k \in N$ at stage i. The completion time of a given job j at stage i, noted as C_{ij}, is calculated as $C_{ij} = max\{C_{i,j-1}; C_{i-1,j}\} + s_{i,j-1,j} + p_{ij}$, where $C_{i,j-1}$ is the completion time of the previous job in the sequence that was assigned to the same machine and $C_{i-1,j}$ is the completion time of job j at the previous stage that this job visited. The tardiness of a job j noted as T_j is calculated as $T_j = max\{0, C_{mj} - d_j\}$ where C_{mj} is the completion time of the job j on the last stage. The optimization criterion is the minimization of the total tardiness of all the jobs, which will be expressed as $\sum_{j=1}^{n} T_j$.

This problem is a significant one in real production cases commonly found in various types of manufacturing systems, such as ceramics [11] and the production of printed circuit boards [12]. In addition, the total tardiness minimization is an optimization criterion of strategic importance. Indeed,

 ISBN: 978-1-61208-365-0

Allahverdi et al. [6] highlight the consequences that order tardiness may present, such as the cost of lost sales and even penalties in a sales contract. To the best of our knowledge, there has been no study on the SDST/HFFS problem minimizing the total tardiness, but we can find in the literature some papers proposing heuristics and/or metaheuristics for the SDST/HFFS problem minimizing the makespan (C_{max}), such as [13]–[17], and studies about related problems, such as [2][11][18]–[20], also minimizing the makespan.

Concerning the total tardiness minimization, there are papers about variations of the SDST/HFFS problem. Indeed, Ruiz et al. [21] introduce two iterated greedy heuristics (IGH) for a hybrid flowshop problem with the objectives of minimizing the makespan and the weighted tardiness. In this paper, we consider release dates for machines, machine eligibility, possibility of the setup times to be both anticipatory and non-anticipatory, precedence constraints and time lags. Mainieri et al. [22] propose five heuristics to solve a hybrid flowshop without setup times. The heuristics are based on list scheduling algorithms. Naderi et al. [18] present a simulated annealing to solve a hybrid flowshop with setup-dependent and transportation times. They used the well known NEH heuristic [23] and three different neighborhood structures based on the swap, shift and inversion operators. Jungwattanakit et al. [24] consider the flexible flowshop problem with both sequence- and machine-dependent setup times. They propose constructive heuristics, shift neighborhood search and a genetic algorithm. Finally, we refer the reader to a detailed literature revue about the hybrid flowshop in [25], where the authors highlight the lack of studies dealing with the setup times and the total tardiness in general.

In this work, to solve the SDST/HFFS problem, we introduce different local search algorithms tested on a new benchmark. The body of this paper is organized into five sections. Section II describes the proposed resolution approaches. The computational testing, benchmark and discussion are presented in Section III. Finally, we conclude with some remarks and future research directions.

II. Heuristics for the SDST/HFFS total tardiness problem

Heuristic algorithms can be classified into dispatching rules, constructive and improvement heuristics. Dispatching rules, also called greedy algorithms, are algorithms for which the decision about which job to scheduled next is made based on the jobs or/and the time in greedy way. Constructive heuristics build a schedule from empty or partial solution by making a series of passes through the list of unscheduled jobs, where at each pass one or more jobs are selected and scheduled. In this case, the selection of the job to be scheduled can be done using the history of jobs running, or by computing tentative schedules. Contrary to constructive heuristics, improvement heuristics start from an existing solution and apply some improvement procedure. We present in the following subsections the retained dispatching, constructive and improvement heuristics.

A. Dispatching rules and Constructive heuristics

According to Pinedo [1], dispatching rules are used very often in practice and as an initial sequence in some improvement heuristic and metaheuristic methods. They are useful when one attempts to find a reasonably good schedule. Let $C_j(S)$ be the completion time of job $j \notin S$ if it is scheduled at the end of a sequence S. We consider in this paper :

- Early Due Date (EDD) : At time *t*, the job with minimum d_j value is selected.
- SLACK : At time *t*, the job with the minimum value of $d_j - C_j(S)$ is selected.
- Modified due date (MDD): At time *t*, the job with the minimum value of $max\{d_j - C_j(S)\}$ is selected.

Pinedo [1] mentions other dispatching rules, but states that the three aforementioned rules are common for total tardiness minimization.

Concerning constructive heuristics, the NEH heuristic [23] is regarded as the best heuristic for the permutation flowshop scheduling problem with the makespan minimization criterion [2]. In the original version of NEH, the jobs are sorted in non-increasing order of the sum of processing times on all machines. In the presence of due dates, several methods can be used to sort the jobs, such as the EDD or SLACK rules.

B. Improvement heuristics

An improvement heuristic algorithm starts with a solution and iteratively tries to obtain a better solution. Neighborhood search algorithms (alternatively called local search algorithms) are a wide class of improvement heuristics where at each iteration an improved solution is found by searching the neighborhood of the current solution. A comprehensive survey on neighborhood search algorithms (NSAs) is given by Prandtstetter and Raidl [26]. An outline of the local search minimization algorithm is given in Figure 1 where the evaluation function f is the total tardiness in our case. As we can see from a $Current$ solution we generate a neighborhood $\mathcal{N}(Current)$ of feasible solutions achievable from $Current$. Then, from this generated neighborhood, we select a solution which will become the $Current$ solution. The choice of the neighborhood structure and the selection scheme will be very important in finding a good solution [26]. We describe in the next subsections a variety of proposed strategies to solve the SDST/HFFS total tardiness problem.

Require: $Current$, an initial solution
Require: $Next$, a solution
  repeat
    Generate $\mathcal{N}(Current)$ a neighborhood of $Current$
    $Next \leftarrow$ Select a solution $\in \mathcal{N}(Current)$
    if $f(Next) \leq f(Current)$ **then**
      $Current \leftarrow next$
    end if
  until Achieving a stopping criterion

Fig. 1. Local Search minimization algorithm

1) Neighborhood search structure: Several neighborhood search structures have been applied to scheduling problems [26]. In this section, we introduce some of them that have been extracted from published works and used in this paper.

Swap move: The positions of two randomly chosen jobs are swapped. An example of the swap operator is presented below where the jobs at position 3 and 8 are swapped:

Before swap: 4 5 7 3 2 9 6 1 8

After swap: 4 5 1 3 2 9 6 7 8

Inversion move: The inversion move is a unary operator where the elements between two random crosspoints are reversed. An example of the inversion operator is presented below where the job block (2, 3, 9, 6) is inverted:

Before inversion: 4 5 7 | 3 2 9 6 | 1 8

After inversion: 4 5 7 | 6 9 2 3 | 1 8

Insertion move: In this scheme, a randomly chosen job is inserted in another random position, different from its initial position. It is also possible to move a job block. Finally, Or [27] introduces the *OrOpt* move where *k* consecutive jobs with $k \in \{1,2,3\}$ are moved from one position to another.

Shift move: Two shift moves can be defined depending on the displacement of the affected job: backward shift (noted as SHIFT_B) and forward shift (noted as SHIFT_F) moves. In a backward shift move the current sequence configuration at position *j* is moved to position *i* with $i < j$, whereas all jobs at locations k, with $k = i, ..., j-1$, are shifted one position backward. An example of the backward shift move is presented below with $i = 3$ and $k = 8$:

Before backward shift: 4 5 7 3 2 9 6 1 8

After backward shift: 4 5 3 2 9 6 1 7 8

Also, an example of the forward shift move is presented below with $i = 8$ and $k = 7$:

Before forward shift: 4 5 7 3 2 9 6 1 8

After forward shift: 4 5 1 7 3 2 9 6 8

2) Neighborhood size and selection scheme: If we consider a sequence *S* of *n* jobs and we generate a neighborhood using the swap move where we interchange only job *i* and job *i + 1* in the sequence without disturbing the remaining jobs, we can generate *(n-1)* different solutions. Hence, using a swap move and considering all the possible moves, the neighborhood of *S* have a size of $n*(n-1)$. For this purpose, we generally generate only a subset of the neighborhood noted as the *k-move* neighborhood where *k* represents the neighborhood size [26]. In this latter case, the neighborhood can be visited randomly (i.e., one among all randomly generated) or in an oriented way (i.e., the best one). Indeed, the selection scheme will choose the next solution to be selected and different schemes can be used [26], such as *Best-Improve* (the best in the neighborhood), *First-Improve* (the first solution improving current in the neighborhood), *k-Improve* (a set of *k* solutions), etc.

If we consider a maximum number of evaluations as the stopping criterion, we present below two generalizations of the selection scheme that have been extracted from published works and used in this paper.

- *Descent Algorithm*: This algorithm is also known as the Hill Climbing Algorithm. In this algorithm, as shown in Figure 2, using a move operator, we generate only one solution in the neighborhood and the $Current$ solution will be updated only if the total tardiness will be improved.

$k \leftarrow 0$
while $k \leq MAX\_EVALUATIONS$ **do**
  $Next \leftarrow move(Current)$
  if $TT(Next) < TT(Current)$ **then**
    $Current \leftarrow Next$
  end if
  $k \leftarrow k + 1$
end while

Fig. 2. Descent Algorithm

- *Neighborhood Move Algorithm*: In this algorithm, using a move operator, we generate *NEIGHBORHOOD_SIZE* solutions representing the neighborhood $\mathcal{N}(Current)$, as shown in Figure 3. Then, we choose the *Next* solution which represents the $best(\mathcal{N}(Current))$, i.e., the best solution in the neighborhood, or the first one, or a random one. We can also add some perturbation policies, such as randomly assigning the best solution to the $Current$ solution.

$k \leftarrow 0$
while $k < MAX\_EVALUATIONS$ **do**
  $Generate\ \mathcal{N}(Current)$
  $Next \leftarrow best(\mathcal{N}(Current))$
  if $TT(Next) < TT(Current)$ **then**
    $Current \leftarrow Next$
  end if
  $k \leftarrow k + NEIGHBORHOOD\_SIZE$
end while

Fig. 3. Neighborhood Move Algorithm

III. EXPERIMENTAL EVALUATION

A. Data generation

The benchmark problem set consists of 160 problem tests. The instances are combinations of *N* and *M*, where *N* = {20, 50, 80, 120} and *M* = {2, 4, 8}. The processing times are generated from a uniform [1, 99] distribution. The setup times are generated according to two distributions [1, 25] and [1, 50]. This corresponds to a ratio between setup and processing times of 25% and 50% respectively. The number of parallel machines at each stage is sampled from a uniform distribution in the range [1, 4]. The probability of skipping a stage for each job is set at 0.10 and 0.40. Finally, due dates are uniformly distributed between *P(1-T - R/2)* and *P(1-T + R/2)* [28], where *T* and *R* are the tardiness factor of jobs and the dispersion range of due dates, respectively, while *P* is a lower bound of the makespan proposed by Santos et al. [29]. The pair (*T*, *R*) has values (0.3, 0.3) and (0.6, 0.3).

B. Computational results and discussion

All the experiments were run on an Intel Core i7 2.8 GHz processor with 8 GB of main memory. Each instance was executed 10 times. Since the evaluation of the SDST/HFFS total tardiness problem is very time consuming, all the experiments were done with a stopping criterion set to 1000 evaluations. To evaluate the different algorithms we use the relative percentage deviation (*RPD*) as shown in Equation 1.

$$RPD = \frac{Heu_{sol} - Best_{sol}}{Best_{sol}} \times 100 \tag{1}$$

where Heu_{sol} is the best total tardiness obtained by a given algorithm and $Best_{sol}$ is the best total tardiness obtained by the whole experiment. The response variable is the minimum of the 10 executions for the considered heuristic.

The first experiments are done to compare the different heuristics and neighborhood search structures. In Table I, we compare different neighborhood search structures with the EDD, SLACK, MDD and NEH heuristics. The different neighborhood search algorithms use algorithm in Figure 3 with the neighborhood size equal to 20. Note that the choice of this size was made following other numerical experiments not reported in this paper. The considered neighborhood search structures are *swap*, *OrOpt*, *shift backward*, *shift forward*, *inversion* and *insertion* moves noted as SWAP, ORPT, SH_B, SH_F, INV and INS, respectively in Table I. The results are grouped by *n* and *m* and the best results are shaded

TABLE I. COMPARISON OF THE BEST RESULT AVERAGES OF DISPATCHING RULES, CONSTRUCTIVE HEURISTICS AND NSA

Instances	EDD	SLACK	MDD	NEHT	SWAP	ORPT	SH_B	SH_F	INV	INS
20×2	52.75	142.17	97.81	105.25	**2.59**	2.71	6.71	4.58	10.36	3.14
20×8	36.62	107.33	66.69	89.10	2.03	1.82	4.04	**1.55**	7.91	1.97
50×2	56.01	108.27	80.21	88.55	**3.50**	6.12	8.23	10.13	15.02	6.34
50×4	48.00	108.24	78.29	88.27	**4.03**	4.52	9.07	5.59	15.85	4.63
50×8	40.44	83.31	65.11	73.49	4.04	3.70	8.92	**3.42**	15.91	3.47
80×2	41.41	66.93	62.48	66.35	**4.35**	6.51	10.52	8.49	16.49	8.11
80×4	44.94	69.89	56.85	61.97	**5.34**	6.27	11.13	8.29	17.76	6.65
80×8	29.62	51.59	36.31	41.93	**3.12**	4.36	7.48	4.48	11.46	4.37
120×2	47.77	66.79	58.47	61.45	**7.16**	9.07	13.84	12.60	22.39	11.38
120×4	27.77	47.82	40.35	44.63	**3.90**	5.75	9.16	6.49	11.84	7.57
120×8	47.03	63.38	59.51	58.53	7.69	**7.51**	13.93	9.51	24.04	9.54
Average	**42.94**	**83.25**	**63.83**	**70.87**	**4.34**	**5.30**	**9.37**	**6.83**	**15.37**	**6.11**

Table I show us that the *swap* neighborhood provides the best results among the tested algorithms, with an average *RPD* value of 4.34%, and the best *RPD* average for all the group instances except for the 20×8, 50×8 and the 120×8. The worst performing algorithms are the dispatching rule (EDD, SLACK, MDD) and the NEH algorithm with *RDP* averages of 42.94%, 83.25% 63.83% 70.87%, respectively. As the problem is very complex, it was expected that these latter algorithms give similar results.

After comparing the neighborhood structure, we evaluate different neighborhood search algorithm strategies. We present here three different strategies:

- The first strategy, noted *S1*, is that defined by algorithm in Figure 3 and its results are presented above in Table I.
- The second strategy, noted *S2*, is defined by a modification at the selection scheme in Figure 3. Indeed, the neighborhood can be generate from the best solution in the last neighborhood or from the best solution found by the algorithm. The choice of the solution is made randomly, i.e., by a fair coin toss.
- The third strategy, noted *S3*, evaluates the algorithm in Figure 2 which, as a reminder, represents a *hill climbing* algorithm.

Furthermore, we can improve the neighborhood search using simultaneous different *moves* [30]. Indeed such approaches can diversify the solution search space. For this purpose we retain the *swap* and the *OrOpt moves*. Thereby, we obtain 9 different algorithms whose results are presented in Table II. Under each strategy column there are three subcolumns : SWAP, ORPT and S/O representing the *swap moves*, the *OrOpt moves* and the algorithm which chooses the move randomly at each time by a fair coin toss. The results are also grouped by *n* and *m* and the best results are also shaded.

TABLE II. COMPARISON OF THE BEST RESULT AVERAGES OF DIFFERENT NEIGHBORHOOD SEARCH ALGORITHM STRATEGIES.

	S1 Strategy			*S2* Strategy			*S3* Strategy		
Instances	SWAP	ORPT	S/O	SWAP	ORPT	S/O	SWAP	ORPT	S/O
20×2	2.59	2.71	2.45	4.09	3.66	5.20	2.85	4.36	**1.39**
20×8	2.03	1.82	6.31	2.73	5.97	1.97	2.02	1.86	**1.29**
50×2	3.50	6.12	4.83	2.73	4.35	4.58	**0.96**	3.36	1.96
50×4	4.03	4.52	4.10	**0.92**	3.80	1.52	1.90	2.07	2.42
50×8	4.04	3.70	6.73	4.13	11.10	5.33	1.36	2.33	**1.12**
80×2	4.35	6.51	6.00	6.93	5.44	6.57	**0.85**	2.60	1.25
80×4	5.34	6.27	4.82	4.00	2.78	3.24	**1.03**	1.76	1.05
80×8	3.12	4.36	3.64	2.86	3.17	3.60	**1.01**	1.43	1.29
120×2	7.16	9.07	5.14	7.72	7.06	4.56	1.72	2.19	**0.46**
120×4	3.90	5.75	5.93	4.54	5.63	6.35	**0.79**	1.87	1.19
120×8	7.69	7.51	5.95	7.18	7.06	6.68	1.50	1.05	**0.97**
Average	**4.34**	**5.30**	**5.08**	**4.35**	**5.46**	**4.51**	**1.45**	**2.26**	**1.31**

The first observation is that the *S3* strategy obtains the best average with 1.45%, 2.26%, 1.31% for the SWAP, ORPT and S/O, respectively. Moreover, the *S3* strategy SWAP and S/O algorithms provide 10 of the 11 best group instance averages. Indeed, the S/O algorithm averages are better than the ORPT ones, but not as good as the SWAP ones. In fact, the results are very similar. Thus, neither changing the replacement scheme or using two different neighborhoods have made effective improvements, in general. With the *S1* strategy, S/O improves on SWAP and ORPT in only 4 and 8 instances, respectively, and with the S2 strategy, S/O improves on the other two algorithms in only 5 instances. Furthermore, the SWAP, ORPT and S/O results are better with S2 than with S1 in 5, 8 and 7 instances respectively

We now analyze the *S3* strategy results. The first interesting conclusion is that the *hill climbing* algorithm significantly improves most of the results, outperforming the other two strategies in 9, 9 and 10 instances, for SWAP, ORPT and S/O, respectively. We believe that the *S1* and *S2* strategies cannot perform better because the 1000-evaluation stopping criterion is not sufficient to reach good sequences. Moreover, with S3, the S/O algorithm improves on SWAP and ORPT in 5 and 10 instances, respectively. We can conclude that using these two neighborhoods together enhances the search results with

 ISBN: 978-1-61208-365-0

the *S3* strategy. Also, as we can see in Figure 4, both *S3-S/O* and *S3-SWAP* perform better than the other S/O algorithms strategies, in general and especially for larger instances.

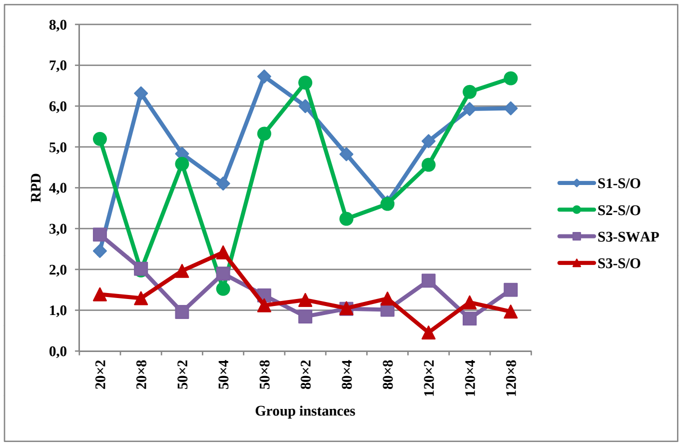


Fig. 4. Comparison of different neighborhood search algorithm strategies RPD.

It is also necessary to analyze the efficiency of the different algorithms. We measured the time in seconds that a given method needs in order to provide a solution. We remarked that all the neighborhood search algorithms have very similar CPU times, i.e., less than 1 second of deviation. Therefore, we report in Table III only the S/O algorithm with *S3* strategy, noted NSA. We also summarize there the CPU times of EDD, SLACK, MDD and NEHT grouped by n and m.

TABLE III. AVERAGE CPU TIMES OF THE DISPATCHING RULES, CONSTRUCTIVE HEURISTICS AND NSA.

Instances	EDD	SLACK	MDD	NEHT	NSA
20*2	0.00	0.00	0.07	0.07	0.36
20*8	0.01	0.01	0.12	0.81	4.19
50*2	0.00	0.01	0.18	3.90	3.31
50*4	0.01	0.02	0.20	13.75	9.54
50*8	0.04	0.04	0.35	44.58	34.68
80*2	0.02	0.03	0.25	32.34	9.94
80*4	0.05	0.04	0.28	113.09	36.41
80*8	0.17	0.17	0.45	470.76	130.81
120*2	0.03	0.04	0.26	190.43	29.62
120*4	0.12	0.11	0.41	681.66	97.34
120*8	0.49	0.45	1.24	1490.41	362.27
Average	**0.09**	**0.08**	**0.35**	**276.53**	**65.32**

The first observation is that the NEHT, executing $n * (n-1)/2$ evaluations, is very time consuming. Furthermore, concerning the NSA algorithms, we remark that dealing with the 8 stage instances notably increase the CPU time due to the evaluation of the SDST/HFFS total tardiness problem.

IV. CONCLUSION

In this work, we have introduced several algorithms to solve the hybrid flexible flowshop problem with sequence dependent setup times, which minimizes the total tardiness. We remind readers that this problem has never been addressed. We compare the behavior of different approaches as dispatching rules, constructive heuristics and a neighborhood search on the new introduced benchmarks. The results support our claim that stage skipping and setup times need to be specifically considered in the solution methods if high performance is desired, considering that this problem is very time consuming.

A perspective of this work is to enhance proposed approaches, such as parallelizing them, and to introduce a more robust algorithm such as metaheuristics.

REFERENCES

[1] M. Pinedo, Scheduling Theory: Algorithm and Systems. Prentice-Hall, 2002.

[2] R. Ruiz and C. Maroto, “A genetic algorithm for hybrid flowshops with sequence dependent setup times and machine eligibility,” European Journal of Operational Research, vol. 169, no. 3, March 2006, pp. 781–800.

[3] A. Allahverdi and H. Soroush, “The significance of reducing setup times/setup costs,” European Journal of Operational Research, vol. 187, no. 3, 2008, pp. 978 – 984.

[4] R. Dudek, M. Smith, and S. Panwalkar, “Use of a case study in sequencing/scheduling research,” Omega, vol. 2, no. 2, 1974, pp. 253–261.

[5] G. Conner, “10 questions,” Manufacturing Engineering Magazine, 2009, pp. 93–99.

[6] A. Allahverdi, C. Ng, T. Cheng, and M. Y. Kovalyov, “A survey of scheduling problems with setup times or costs,” European Journal of Operational Research, vol. 187, no. 3, 2008, pp. 985 – 1032.

[7] X. Zhu and W. E. Wilhelm, “Scheduling and lot sizing with sequence-dependent setup: A literature review,” IIE Transactions, vol. 38, no. 11, 2006, pp. 987–1007.

[8] A. Vignier, J. C. Billaut, and C. Proust, “Scheduling problems of hybrid flowshop type : state of the art,” RAIRO - Operations Research, vol. 33, no. 2, 1999, pp. 117–183.

[9] R. L. Graham, E. L. Lawler, J. K. Lenstra, and A. G. H. R. Kan, “Optimization and approximation in deterministic sequencing and scheduling: a survey,” Annals of Discrete Mathematics, vol. 5, 1979, pp. 287–326.

[10] J. Du and J. Y. T. Leung, “Minimizing total tardiness on one machine is np-hard,” Mathematics and Operations Researchs, vol. 15, 1990, pp. 438–495.

[11] R. Ruiz, F. S. Serifoglu, and T. Urlings, “Modeling realistic hybrid flexible flowshop scheduling problems,” Computers and Operations Research, vol. 35, no. 4, 2008, pp. 1151 – 1175.

[12] Z. H. Jin, K. Ohno, T. Ito, and S. E. Elmaghraby, “Scheduling hybrid flowshops in printed circuit board assembly lines,” Production and Operations Management, vol. 11, no. 2, 2002, pp. 216–230.

[13] M. Zandieh, S. Fatemi Ghomi, and S. Moattar Husseini, “An immune algorithm approach to hybrid flow shops scheduling with sequence-dependent setup times,” Applied Mathematics and Computation, vol. 180, no. 1, 2006, pp. 111 – 127.

[14] H. Mirsanei, M. Zandieh, M. Moayed, and M. Khabbazi, “A simulated annealing algorithm approach to hybrid flow shop scheduling with sequence-dependent setup times,” Journal of Intelligent Manufacturing, vol. 22, 2011, pp. 965–978.

[15] B. Naderi, R. Ruiz, and M. Zandieh, “Algorithms for a realistic variant of flowshop scheduling,” Computers and Operations Research, vol. 37, no. 2, Feb. 2010, pp. 236–246.

[16] P. Gomez-Gasquet, C. Andres, and F. Lario, “An agent-based genetic algorithm for hybrid flowshops with sequence dependent setup times to minimise makespan,” Expert Systems with Applications, vol. 39, no. 9, 2012, pp. 8095 – 8107.

[17] A. Sioud, M. Gravel, and C. Gagne, “A genetic algorithm for solving a hybrid flexible flowshop with sequence dependent setup times,” in Evolutionary Computation (CEC), 2013 IEEE Congress on, June 2013, pp. 2512–2516.

[18] B. Naderi, M. Zandieh, and V. Roshanaei, “Scheduling hybrid flowshops with sequence dependent setup times to minimize makespan and maximum tardiness,” The International Journal of Advanced Manufacturing Technology, vol. 41, 2009, pp. 1186–1198.

[19] F. Jabbarizadeh, M. Zandieh, and D. Talebi, “Hybrid flexible flowshops with sequence-dependent setup times and machine availability constraints,” Computers and Industrial Engineering, vol. 57, no. 3, Oct. 2009, pp. 949–957.

[20] N. Javadian, P. Fattahi, M. Farahmand-Mehr, M. Amiri-Aref, and M. Kazemi, “An immune algorithm for hybrid flow shop scheduling problem with time lags and sequence-dependent setup times,” The International Journal of Advanced Manufacturing Technology, vol. 63, 2012, pp. 337–348.

[21] R. Ruiz and T. Stutzle, “An iterated greedy heuristic for the sequence dependent setup times flowshop problem with makespan and weighted tardiness objectives,” European Journal of Operational Research, vol. 187, no. 3, 2008, pp. 1143 – 1159.

[22] G. Mainieri and D. Ronconi, “New heuristics for total tardiness minimization in a flexible flowshop,” Optimization Letters, vol. 7, no. 4, 2013, pp. 665–684.

[23] M. Nawaz, E. E. Enscore, and I. Ham, “A heuristic algorithm for the m-machine, n-job flow-shop sequencing problem,” Omega, vol. 11, no. 1, 1983, pp. 91 – 95.

[24] J. Jungwattanakit, M. Reodecha, P. Chaovalitwongse, and F. Werner, “Algorithms for flexible flow shop problems with unrelated parallel machines, setup times, and dual criteria,” The International Journal of Advanced Manufacturing Technology, vol. 37, no. 3-4, 2008, pp. 354–370. [Online]. Available: http://dx.doi.org/10.1007/s00170-007-0977-0

[25] R. Ruiz and J. A. Vzquez-Rodrguez, “The hybrid flow shop scheduling problem,” European Journal of Operational Research, vol. 205, no. 1, August 2010, pp. 1–18.

[26] M. Prandtstetter and G. R. Raidl, “An integer linear programming approach and a hybrid variable neighborhood search for the car sequencing problem.” European Journal of Operational Research, vol. 191, no. 3, 2008, pp. 1004–1022.

[27] I. Or, “Traveling salesman-type combinatorial problems and their relation to the logistics of regional blood banking,” Ph.D. dissertation, Northwestern University, Illinois, 1976.

[28] C. Potts and L. V. Wassenhove, “A decomposition algorithm for the single machine total tardiness problem,” Operations Research Letters, vol. 1, no. 5, 1982, pp. 177 – 181.

[29] D. Santos, J. Hunsucker, and D. Deal, “Global lower bounds for flow shops with multiple processors,” European Journal of Operational Research, vol. 80, no. 1, 1995, pp. 112 – 120.

[30] N. Mladenovic and P. Hansen, “Variable neighborhood search,” Computers and Operations Research, vol. 24, no. 11, 1997, pp. 1097 – 1100.

An Evaluation of Smoothing Filters for Gas Sensor Signal Cleaning

Enobong Bassey, Jacqueline Whalley and Philip Sallis
Geoinformatics Research Centre, School of Computer and Mathematical Sciences
Auckland University of Technology
Auckland, New Zealand
e-mails: {ebassey@aut.ac.nz, jwhalley@aut.ac.nz, psallis@aut.ac.nz}

***Abstract*— This paper explores signal response and methods for extracting the desired digital signal, from gas sensor arrays, while maintaining the shape and resolution of that signal. A comparative evaluation of Savitzky–Golay smoothing, moving average, local regression and robust local regression filters for cleaning signals obtained from gas sensor devices during the pre-processing phase is provided. It was found that the Savitzky–Golay smoothing filtering method provided the best approximation of the sensor response.**

Keywords-denoising; gas sensor arrays; signal processing.

I. Introduction

Typically, raw signals acquired from gas sensors are contaminated by noise and outliers and as a result the signal is occluded to a significant degree making accurate measurement of a sensor's response impossible. Noise in sensor systems has several possible sources and is introduced at various stages in the measurement process. Several forms of noise, including thermal and shot noise, are irreducible because they are inherent to the underlying physics of the sensors or electronic components. Other forms of noise which could be avoided originate from processes, and include 1/f noise, transmission, and quantization noise [1]. Noise introduced in the early measurement stages is considered to be the most harmful as it propagates and can be amplified through subsequent stages in the signal pathway [2].

While physical filters have been found to be successful in producing a cleaner signal they do not cover the full resolution and shape of the curve. In order to improve the interpretability, sensitivity and selectively of gas sensor array signals it is preferable to use the full resolution and coverage of the signal.

Several signal processing approaches have been investigated as an approach to reducing noise levels [3]. However, these approaches are typically static or steady state approaches and therefore do not encompass the full temporal signal [4].

In this paper we report on an evaluation of methods for feature extraction and denoising the digital signal from thin film zinc oxide and tin dioxide composite gas sensor devices. The aim was to find a method that not only cleaned the signal but that also maintained the shape, precision and resolution of the signal regardless of sensor composition. In Section II the stages of gas sensor array signal processing is outlined. Details of various approaches to signal pre-processing are then discussed in Section III. In Section IV the signal pre-processing methods evaluated are detailed. Section V gives the results of applying each of these signal denoising methods. Finally, Section VI provides a summary of our results and suggests possible avenues for future work.

II. Gas Sensor Array Signal Processing

The signal processing of gas sensor data can be divided into four steps [5]: (1) *pre-processing*, for further processing of the sensor signal (e.g., denoising, drift compensation, concentration normalization); (2) *dimensionality reduction* (of the input signal to avoid problems associated with high dimensionality data); (3) *prediction* (of the interesting properties of the sample, e.g., class membership, related odour samples); and (4) *validation*, where model and parameter settings are selected in order to optimize a criterion function (e.g., classification rate, mean-squared error). A useful summary of statistical and optimization methods that have been used to process gas sensor array signals is provided by Gutierrez-Galvez [6]. The work reported here focuses on improving existing pre-processing techniques used to eliminate noise, smooth and filter data, enhance sensor signals and ultimately improve measurement.

III. Signal Pre-processing

Signal pre-processing facilitates noise elimination, data smoothing/filtering and signal enhancement, with the sole aim of increasing the signal-to-noise ratio without greatly distorting the signal. The choice of signal pre-processing method is known to have a significant impact on the results and performance of the pattern analysis system [1][7].When developing a pre-processing method three criteria should be considered [8]. The algorithm must: preserve the chemical selectivity differences between different profiles and limit run-to-run retention/migration time shift, be fast and less memory-demanding to deal with large numbers of data sets in a short period of time, and the resulting precision of retention/migration time estimation should be significantly improved in comparison with that initially provided by the instrumentation [1][7]. We propose that wavelet transform smoothing filters, for this purpose, should meet all three criteria.

Wavelets are a family of wavelet transforms that are considered to be a time-frequency representation for continuous-time (analog) signals [9]. They have a compact support (i.e., they differ from zero only in a limited time domain) and easily represent the different features of a signal, especially sharp signals and discontinuities. When applied to analytical signal processing wavelet transforms provide a simple procedure with short operation time, low

 ISBN: 978-1-61208-365-0

memory requirements, high precision, and good reproducibility [10]. Examples of wavelet transforms for denoising signals include the Savitzky–Golay Smoothing Filter (SGF) [11], Fast Fourier transform (FFT), Multivariate Wavelet Denoising (MWD), Discrete Wavelet Transform (DWT) [12], and Continuous Wavelet Transform (CWT) [2].

For this work, we have elected to evaluate the use of an SGF by comparing its performance with moving average filter and local regression methods. SGF is known to be superior to other adjacent averaging FIR filters because it tends to preserve the features of the data in the signal, such as peak height and width. Moreover, when using SGF it is possible to increase the smoothness of the result by changing the window size, or increasing the number of data points used, in each local regression. Although SGFs are considered to be less successful than standard averaging FIR filters at eliminating noise, they are more effective at preserving the pertinent high frequency components of the signal [4], and are optimal in minimising the least-squares error in fitting a polynomial to frames of noisy data. Moreover, SG filters can preserve more of the high-frequency content of a signal, but this is at the expense of reduced noise elimination.

Therefore, an SGF might prove to be a good choice for gas senor signal cleaning where it is important to preserve the height, width, amplitude and overall profile of the signal.

IV. METHODOLOGY

In order to evaluate the usefulness of wavelet transforms for preprocessing gas sensor arrays we elected to investigate the performance of an SGF, using tin dioxide (SnO_2) and zinc oxide (ZnO) sensor devices.

For a given experiment $\boldsymbol{E}$, a response matrix R is usually obtained in which each column represents a response matrix associated with the concentration of the target gas produced C at operating temperature T and the rows give the response matrices of each individual sensor (1).

$$E = \begin{pmatrix} R_{11} & R_{12} & \cdots & R_{1T} \\ R_{21} & R_{22} & \cdots & R_{2T} \\ \vdots & \vdots & R_{pq} & \vdots \\ R_{C1} & R_{C2} & \cdots & R_{CT} \end{pmatrix} \qquad (1)$$

For this work we opted, as a preliminary investigation, to evaluate the signal cleaning methods using two sensor devices rather than an array of sensors. Thus the experimental matrix $\boldsymbol{E}$ can be represented as vector $Rq = (R1q, R2q, Rpq... RCq)^T$. Each of these sensor devices were individually primed with 150ppm methanol at 250°C and operated at three different temperatures [150, 250 and 350 ºC] for the target gas, methanol, at three different concentrations [100, 150 and 200 ppm].

The data were visualised and smoothed using multiple fitting algorithms. The parameters of the curve after residual analysis were then analysed and fits generated. Then the curve was reconstructed to determine the accuracy of the models. Subsequently, an optimal model was selected for generating the best polynomial model.

The performance of the SGF was then compared with a moving average filter, lowess, loess, rlowess, and rloess methods. Details of these six methods and the results of the experiments are provided in the following sections.

A. Moving Average Filtering

A moving average filter, equivalent to low pass filtering, can be used to smooth data by replacing each data point with the average of the neighbouring data points within a specified span of data points. This process is described by the difference equation (2) [13], where $y_s(i)$ is the smoothed value for the i^{th} data point, N is the number of neighbouring data points on either side of $y_s(i)$, and 2N+1 is the span.

$$y_s(i) = \frac{1}{2N+1}\left(y(i+N-1) + \cdots + y(i-N)\right) \qquad (2)$$

B. Local Regression Smoothing: rLowess & rLosess

The names lowess and loess are derived from the term "locally weighted scatter plot smooth," as both methods use locally weighted linear regression to smooth data.

The smoothing process is considered local because each smoothed value is determined by neighbouring data points defined within the span. The process is weighted because a regression weight function is defined for the data points contained within the span. The local regression first and second degree polynomial models are lowess and loess, respectively. The robust local regression method (rlowess and rloess) assigns a lower weight to outliers in the regression and assigns a zero weight to data outside six mean absolute deviations.

Like the moving average method, the lowess and loess smoothed value is determined by neighbouring data points defined within a span [14]. However, in this case the process is weighted by a regression weight function that is defined for all the data points contained within the specified span. In addition to the regression weight function, a robust weight function can be used; this makes the process resistant to outliers.

Lowess and loess are differentiated by the model used in the regression: lowess uses a linear polynomial, while loess uses a quadratic polynomial.

C. Savitzky–Golay Smoothing Filter (SGF)

The SGF is based on local least-squares polynomial approximation [11]. It is a generalization of the finite-impulse response (FIR) or moving average filter with filter coefficients determined by an unweighted linear least-squares regression and a polynomial model of specified degree. The process, equivalent to discrete convolution with a fixed impulse response, involves fitting a polynomial to a set of input data and evaluating the resulting polynomial at a single point within the approximation interval. The SG smoothing procedure consists of replacing the central point of a window (containing an odd number of points, 2p + 1) with the value obtained from the polynomial fit. The window is moved one data point at a time until the whole signal is scanned; thus, creating a new, smoothed value for each data point. The smoothed signal g(t) is then calculated by convolving the signal f(t) with a smoothing (or convolution) function h(t) [9] for all observed data points p where f(m) is the curve function at point m and h(m - t) $\neq$ 0 (3). The convolution function h(t) is defined for each combination of degree of the polynomial and window size.

$$g(t) = f(t) * h(t) = \frac{\Sigma f(m)h(m-t)}{\Sigma h(m)} \qquad (3)$$

A typical digital filter can be applied to a series of equally spaced data values $f_i \equiv f(t_i)$, where $t_i \equiv t_0 + i\Delta$ for some constant sample spacing Δ and i = …-2, -1, 0, 1, 2, …. Therefore, the SG smoothing operations consist of the replacement of each data point f_i with a linear combination of g_i and a number of nearby neighbours *n* [10] where *nL* is the number of neighbouring points prior to the data point i and *nR* is the number of neighbours after data point *i* (4)

$$g_i = \sum_{n=-nL}^{nR} c_n f_{i+n} \qquad (4)$$

and where the coefficients c_n are the weights of the linear combination and a causal filter would have an *nR* of zero [2][15][16]. For the simplest possible averaging smoothing filter (similar to the moving average window), the smoothed point is the average of an odd number of neighbouring data points. This moving window average (5) is computed as g_i, i.e., as the average of the data points from f_{i-nL} to f_{i+nR}, for some fixed nL = nR = M; and the weights c_n = 1/(nL + nR + 1) [12]:

$$g_i = \sum_{n=-M}^{M} \frac{f_{i+n}}{2M+1} \qquad (5)$$

The weights c_n are chosen in such a way that the smoothed data point gi is the value of a polynomial fitted by least-squares to all (nL + nR + 1) points in the moving window. That is, for the group of 2M+1 data centered at n = 0, and the coefficient of the polynomial is obtained as (6) [15][16].

$$c_n = p(n) = \sum_{k=0}^{N} a_k n^k \qquad (6)$$

This minimises the mean-squared approximation error (7) for the group of input samples centred on n = 0:

$$\varepsilon_n = \sum_{n=-M}^{M} \left(p(n) - x[n]\right)^2 = \sum_{n=-M}^{M} \left(\sum_{k=0}^{k} a_k n^k - x[n]\right)^2 \qquad (7)$$

Therefore, the smoothed data point g_i by the Savitzky–Golay algorithm [10] is given by (8):

$$g_i = \frac{\sum_{n=-nL}^{nR} c_n f_{i+n}}{\sum_{n=-nL}^{nR} c_n} \qquad (8)$$

V. RESULTS

A. Smoothing

Local regression smoothing (lowess and loess) and robust local regression (rlowess and rloess) were carried out using a span of 10% of the data points. Moving average and SGFs were used to smooth the data using a span of 5 and 55. These values were chosen because they gave comparable results.

The results from smoothing the raw data using local regression smoothing and robust local regression were found to give essentially the same shape resolution (Fig. 1). With the moving average and SGFs, using a span of 55 gave better smoothing/shape resolution than using a span of 5, as shown in Fig. 2. For the ZnO device rloess, rlowess, and losses gave improved smoothing over lowess (Fig. 3). Moving average and SGF with a span of 55 gave better smoothing than with a span of 5 as shown in Fig. 4.

However in all cases, although smoothing was improved, the approximation of the curve was poorer because less raw data points were fitted.

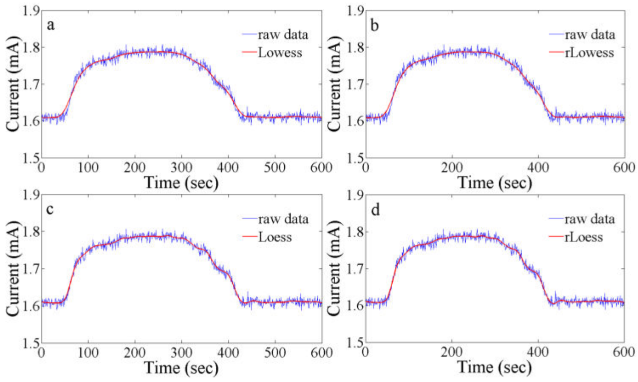


Figure 1. SnO_2 Sensor Local Regression Smoothing (a) Lowess, (b) rLowess and Robust Local Regression Smoothing; (c) Loess (d) rLoess.

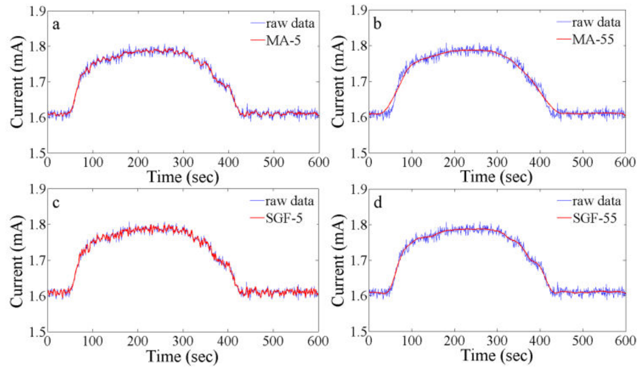


Figure 2. SnO_2 Sensor (a) MA, span = 5, (b) MA span = 55, (c) SGF, span = 5, and (d) SGF, span = 55.

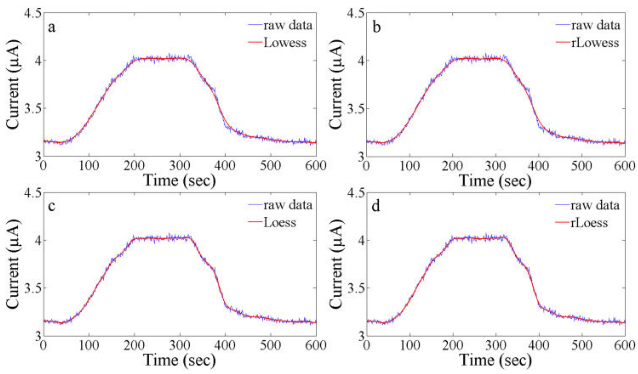


Figure 3. ZnO Sensor Local Regression Smoothing (a) Lowess, (b) rLowess and Robust Local Regression Smoothing; (c) Loess (d) rLoess.

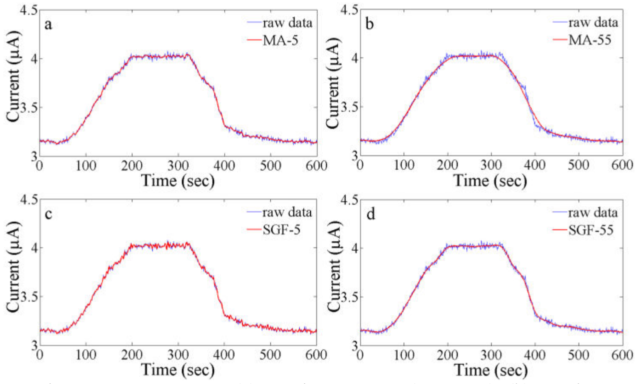


Figure 4. ZnO Sensor (a) Moving Average (Span = 5), (b) Moving Average (Span = 55), (c) SGF, span = 5, and (d) SGF, span = 55.

It was also found that using SGF, the height and width of narrow peaks is accurately captured by higher degree polynomials, but wider peaks are poorly smoothed. For optimality, a polynomial degree of three was applied for the implementation of the SG filtering.

B. *Curve Fitting Accuracy*

Curve fitting was undertaken for each of the smoothing processes and the coefficient of determination (R-squared (R^2)) was calculated using a polynomial of three (9).

R-squared indicates how well data points fit a statistical model and provides a measure of how well observed outcomes are replicated by the model, as the proportion of total variation of outcomes explained by the model [17]. In other words, R^2 is proportional to the variability of the response signal in the polynomial model.

In our case, R^2 indicates the proportionate amount of variation in the response signal explained by the independent variables *t* in the polynomial model where SSE is the sum of squared error, SSR is the sum of squared regression, and SST is the sum of squared total.

$$R^2 = \frac{SSR}{SST} = 1 - \frac{SSE}{SST} \tag{9}$$

In all cases, the R^2 value for the SnO_2 device was greater than that observed for the ZnO device indicating that a better fit of the model is obtained for the SnO_2 device (Fig. 5)

The best value of R^2 was obtained using the moving average smoothing method with a span of 55, followed closely by the lowess local regression for both the SnO_2 and ZnO devices.

However, visual observation of the smoothing results indicates that the SGF and the loess methods gave better shape resolution. The norms of residuals were found to be the same regardless of the smoothing method for each device (5.25E-04 and 3.62E-06 for SnO_2 and ZnO, respectively).

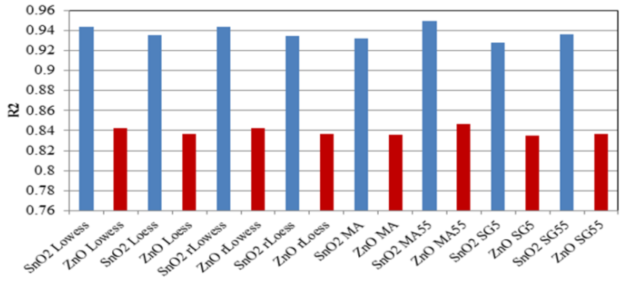


Figure 5. Coefficient of Determination vs. the Curve Fitting Process.

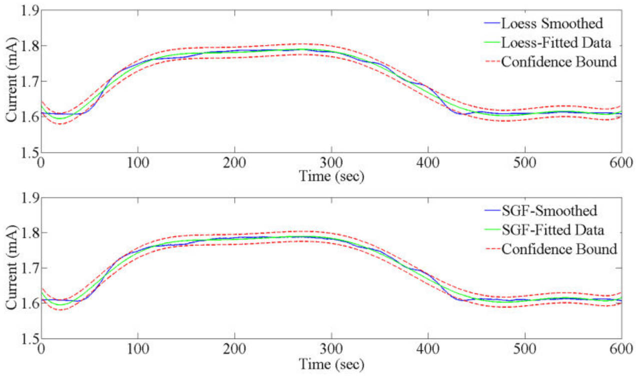


Figure 6. Polynomial Fit with Confidence Bounds and Smoothed SnO_2 Device Data: (top) Loess, (bottom) SGF-55.

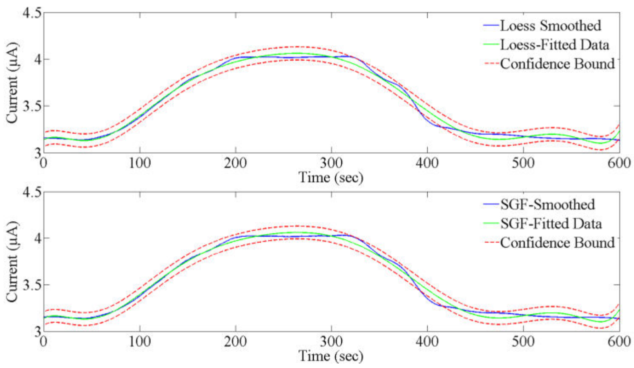


Figure 7. Polynomial Fit with Confidence Bounds and Smoothed ZnO Device Data: (top) Loess, (bottom) SGF-55.

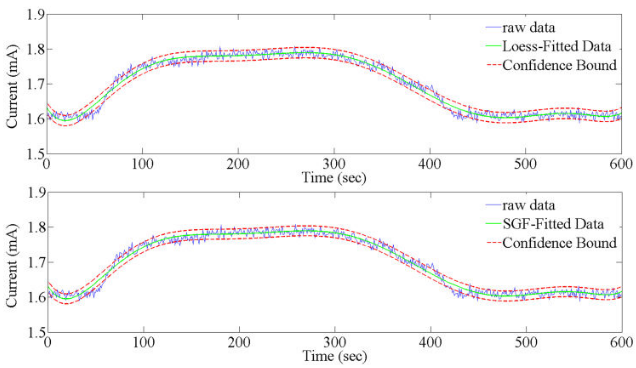


Figure 8. Fitting the Confidence Bounds over the SnO_2 Device Raw Data: (top) Loess, (bottom) SGF.

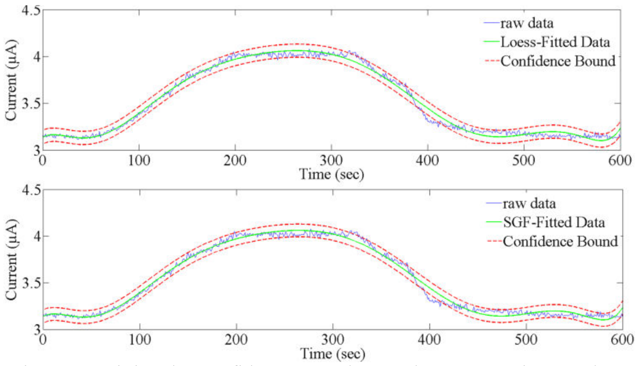


Figure 9. Fitting the Confidence Bounds over the ZnO Device raw data: (top) Loess , (bottom) SGF.

C. *Model Calibration*

To calibrate the model, different polynomial models were tested on the raw data to determine the best fit within the confidence bounds. An attempt to fit the data using a higher degree polynomial is presented using the SGF (span = 55) and the loess (span = 10%) methods. The best fit was found to occur using a polynomial degree of nine for both the loess and the SGF methods. For the SnO_2 device, the norms of residuals were 1.8034E-04 for loess and 1.714E-04 for the SGF respectively (Fig. 6). For the ZnO device, the norms of residuals were 8.47E-07 and 8.27E-07 for the loess and SGF methods, respectively (Fig. 7). Further analysis of the raw data and the fitted data showed that the two smoothing methods (loess and SGF) present very good confidence bounds when fitted over the raw data for both devices (see Fig. 8 and Fig. 9).

VI. CONCLUSION AND FUTURE WORK

This study has explored signal response, and methods for extracting the desired digital signal while maintaining the shape and resolution of that signal. A simple procedure to test different polynomial models, with confidence bounds, on the raw data was developed for easy application to quantised gas sensor response data. Curve fitting approaches were used to validate the results of three possible methods.

Of the six methods investigated, and as expected, it was found that the SGFs give the best resolution and best maintain the shape of the signal and therefore provided the best approximation of the sensor response. After testing SGF with various polynomial models, the ninth degree of the polynomial model was observed to provide the best fit to the raw data for both the SnO2 and ZnO sensor devices. For both sensor devices, the raw data were observed to fall within the confidence bounds simulated from the polynomial models. This is a promising result and future work will involve testing the SGF signal pre-processing method on signals produced from an array of sensors.

REFERENCES

[1] I. García-Pérez, M. Vallejo, A. García, C. Legido-Quigley, and C. Barbas, "Metabolic fingerprinting with capillary electrophoresis," J. Chromatogr. A, vol. 1204, issue 2, 2008, pp. 130-139.

[2] R. Gutierrez-Osuna, H. T. Nagle, B. Kermani, and S. S. Schiffman, "Signal Conditioning and Preprocessing," Handbook of Machine Olfaction: Electronic Nose Technology. Wiley-VCH Verlag GmbH & Co. KGaA, pp. 105-132, 2004.

[3] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, "Numerical Recipes: The Art of Scientific Computing," Cambridge, New York Cambridge University Press, 2007.

[4] S. J. Orfanidis, "Introduction to Signal Processing," New Jersey, USA: Prentice Hall, Inc, 1996.

[5] R. Gutierrez-Osuna, "Pattern analysis for machine olfaction: a review," Sensors Journal, IEEE, vol. 2, issue 3, 2002, pp. 189-202.

[6] A. Gutierrez-Galvez, "Coding and learning of chemosensor array patterns in a neurodynamic model of the olfactory system," Ph.D., Texas A&M University, United States – Texas, 2006.

[7] E. Szymańska et al., "Increasing conclusiveness of metabonomic studies by cheminformatic preprocessing of capillary electrophoretic data on urinary nucleoside profiles," Journal of Pharmaceutical and Biomedical Analysis, vol. 43, issue 2, 2007, pp. 413-420.

[8] K. J. Johnson, B. W. Wright, K. H. Jarman, and R E.. Synovec, "High-speed peak matching algorithm for retention time alignment of gas chromatographic data for chemometric analysis," Journal of Chromatography A, vol. 996, issues (1–2), 2003, pp. 141-155.

[9] C. Perrin, B. Walczak, and D. L. Massart, "The Use of Wavelets for Signal Denoising in Capillary Electrophoresis," Analytical Chemistry, vol. 73, issue 20, 2001, pp. 4903-4917.

[10] L. Bao, J. Mo, and Z. Tang, "The Application in Processing Analytical Chemistry Signals of a Cardinal Spline Approach to Wavelets," Analytical Chemistry, vol. 69, issue 15, 1997, pp. 3053-3057.

[11] A. Savitzky and M. J. E. Golay, "Smoothing and Differentiation of Data by Simplified Least Squares Procedures," Analytical Chemistry, vol. 36, issue 8, 1964, pp. 1627-1639.

[12] M. Zuppa, C. Distante, P. Siciliano, and K. C. Persaud, "Drift counteraction with multiple self-organising maps for an electronic nose," Sensors and Actuators B: Chemical, vol. 98, issues 2–3, 2004, pp. 305-317.

[13] MathWorks(R) MATLAB: Curve Fitting Toolbox, Filtering and Smoothing Data. Available from: http://www.mathworks.com/help/curvefit/smoothing-data.html [retrieved: April 2014].

[14] MathWorks(R) MATLAB: Wavelet Toolbox, Multivariate Wavelet Denoising. Available from: http://www.mathworks.com/help/wavelet/examples/multivariate-wavelet-denoising.html [retrieved: April 2014].

[15] R. Schafer, "What Is a Savitzky-Golay Filter?," Signal Processing Magazine, IEEE, vol. 28, issue 4, 2011, pp. 111-117.

[16] D. J. Thornley, "Novel Anisotropic Multidimensional Convolutional Filters for Derivative Estimation and Reconstruction," IEEE International Conference on Signal Processing and Communications ICSPC 2007, 2007, pp. 253 - 256.

[17] R. G .D. Steel and J. H. Torrie, "Principles and Procedures of Statistics with Special Reference to the Biological Sciences," McGraw Hill, pp. 187-287, 1960.

Using Mobile Serious Games for Learning Programming

Jiayi Zhang, Joan Lu
School of Computing and Engineering
University of Huddersfield,
Huddersfield, West Yorkshire, UK
e-mail: {zjybyron@gmail.com, J.lu@hud.ac.uk}

***Abstract*— Serious games, which are entertaining games for learning, have attracted obvious attention in the field of education, and the mobile educational game is an important issue in recent years. The purpose of this article is to propose and evaluate iPlayCode which is a mobile serious game for learning programming. The Felder-Silverman Learning Style Model (FSLSM) and Kolb's experiential learning theory have been used in this game to improve learning efficiency. In addition, simple interface design improves user experience, and the use of game elements eliminates the tension in learning programming. To sum up, iPlayCode incorporates rigorous teaching methods, scientific interface design and practical game elements.**

Keywords-serious game; mobile; learning programming

I. INTRODUCTION

In recent years, serious games, which are entertaining games aimed at learning academic knowledge, have received obvious attention; Mitamura et al. explained that serious games have found great success in improving the learning environment and learning efficiency [1]. In addition, mobile devices are similar to earlier computers, and even now, ordinary computers in their hardware performance. They provide favourable conditions, meaning that people can develop serious games for mobile devices based on mobile operating systems, such as iOS, Android and Windows. Xin emphasised that numerous entertaining games have been developed for mobile learning, such as SimCity, E-Friction, Civilization, and so on [2].

Kapralos argued that because of the rapid development of mobile serious games, it should be determined that they are reasonably designed to achieve the expected objectives [3]. Prensky found that serious games must combine two powerful factors for success in the field of education: one is the key purpose of the game, in which a learner can be pushed into a learning environment unconsciously in the game; the other is the integration of learning methods which enhance the teaching efficiency and reduce boredom from learning at school [4].

iPlayCode, which we developed, aims at simplifying the learning of programming by including entertainment. Mitamura et al. highlighted that learning programming languages is abstract and complex at university-level because students do not feel that the learning environment is motivating and are not interested in computer programming [1]. Therefore, teaching methods play an important role in the educational process, and mobile serious games provide an opportunity to resolve this issue. The purpose of this article is to propose and evaluate mobile serious games for programming learning based on the learning model.

The rest of the paper is organized as follows. Section II provides the background and problems of serious game. The positive combination of game with learning theories is discussed in detail in Section III. The interface design and implementations are demonstrated in Section IV and Section V. The assessment results are then shown in Section VI, followed by the conclusion in Section VII.

II. RELATED WORKS

Programming languages are used in every corner in the field of computing. But Khenissi et al. argued that teaching and learning programming languages are definitely not a simple task for teachers and students [5]. Learning a programming language requires meticulous logical thinking and students should understand abstract concepts from real problems. Moreover, computer science students come from various academic backgrounds, and, especially, there are ones without basic computer knowledge. Therefore, the development of serious games to improve learning efficiency and motivation is a common topic for many researchers and developers.

A. Serious Game

According to Lu et al. [6], serious games have received significant concern in the field of education, and a mobile educational gaming community has been formed in recent years. Apple announced that the value of the application for iPad and iPhone is more than $10 billion in the App Store in 2013. Furthermore, App Store has more than 65,000 educational applications, primarily intended for iPad, which cover a wide range of fields suitable for different levels and learning styles [7]. Serious games help students gain experience in practice, which resulted in their rising popularity. Furthermore, a serious game is a combination of education and entertainment. Students can discover knowledge in entertainment and refresh their learning attitudes.

B. Fun and Learning

Franzwa et al. state that the biggest challenge for serious games development is the combination of game ideas and teaching concepts [8]. Many educational games focused on educational methods but ignore entertainment sense; on the other hand, numerous entertaining games emphasize means

 ISBN: 978-1-61208-365-0

of entertainment yet reduce educational elements. The authors believe that the evaluation of a serious game should depend on the efficiency of learning. Serious games would be more easily accepted than traditional teaching methods and students could learn better through serious games than by themselves.

C. *Application Platform*

According to devices used, serious games are divided into three categories, which include computer games, phone games and tablet games. While most serious games with high system requirements are used on the computer, mobile devices run various serious games with low system requirements. In addition, websites are also a very popular serious game media for cross-platform development [6]. Their advantages and disadvantages are summarised in TABLE I.

TABLE I. A COMPARISON OF SERIOUS GAMES PLATFORM

	Computer	**Phone**	**Tablet**
Storage	Enough	Medium	Medium
Processing Capacity	Strong	Medium	Medium
Operation	Complexity	Simplicity	Simplicity
Interface Size	Large	Small	Medium
Game Effect	Good	Low quality	Medium
Mobility	Bad	Very strong	Strong

This table shows that computer-based games are designed to provide perfect game conditions, but they are limited with certain situations. Moreover, mobile devices, phones and tablets are comprehensive and their characteristics are well-suit to the requirements of mobile serious games.

D. *iPlayCode*

This application was built for learning programming and the target audience are learners with no programming skills. Through the syntactic judgments and help system, learners can raise their learn how to write correct syntax based on C++ programming language. At the same time, iPlayCode aims to become a serious game that incorporates elements of the game into the learning environment, such as incentives and time constraints.

III. GAMES BASED ON LEARNING

The study by Zapusek et al. [9] found that educational games can increase motivation for learning. However, the quality of learning not only needs motivated learners but also requires attractive learning materials and methods. This section will introduce several learning theories which have been used in iPlayCode as a mobile serious game.

A. *Student's Learning Style*

Each individual's learning style will affect his / her learning process and their learning outcomes. When students learn to use the method that matches their styles of accessing and processing information, their learning will be more efficient [10]. The Felder-Silverman Learning Style Model (FSLSM) describes four dimensions to distinguish students: Active/Reflective, Sensory/Intuitive, Visual/Verbal, and Sequential/Global [11]:

- Active/Reflective: iPlayCode facilitates both reflective and active learning. While reflective students can learn the correct syntax through their experiments in the game, active ones can also look for the underlying reasons using the help button which provides tips and explanations for the correct answers.
- Sensory/Intuitive: While intuitive learners are capable of understanding programming languages without having many difficulties, sensory ones may find it hard to understand rules and abstract concepts. iPlayCode can help them solve this problem by providing direct examples of each concept and rule.
- Visual/Verbal: Visual learners focus on the images and diagrams, and the verbal learner is more likely to learn through textual representation. A graphical interface avoids the monotony of boring programming languages.
- Sequential/Global: Sequential learners follow a gradual linear learning progress, which is supported by the flow of levels in iPlayCode. However, users are not required to follow such sequence, which is helpful for global learners as they learn from diverse knowledge acquisition.

B. *Student's Learning Cycles*

Kolb's experiential learning theory describes four major steps of learning processing and knowledge learning process needed to understand and apply a theory (see Figure 1).

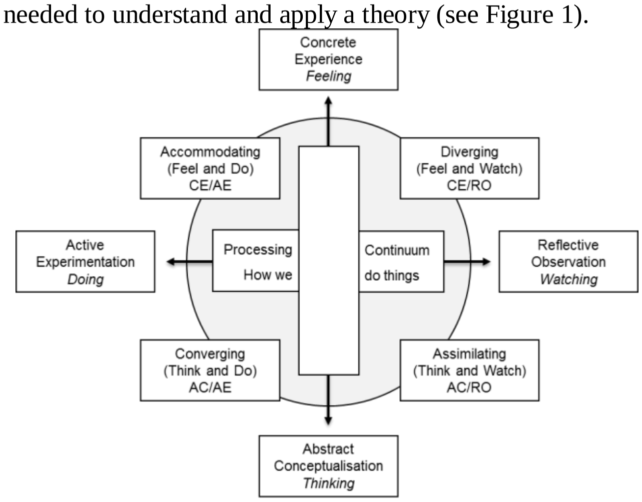


Figure 1. Four Stage Cycle of Kolb's Experiential Theory [12]

It is noteworthy that this theory supports the idea that learning is a cyclical process based on experience, and effective learning depends on positive repetition, as stated by Park et al. [12].

Through continuous repetition, learners will discover new points from different syntax. In addition, Clow analysed the notion that multiple practices will help learners to understand abstract concepts, and that learners can discover underlying theory through observation [13]. If the practice is inconsistent in its outcomes and expectations, learners will think about this problem and generate curiosity.

IV. SERIOUS GAME DESIGN

A. *User Interface*

Aesthetics & graphics is one of six important elements in supporting serious games systems, according to Mitgutsch and Alvarado [14]. User interface, as a core component, affects the coherence and cohesion of the entire game system. Audiences determine the direction of visual effects design.

1) *Look and Feel Styles*

According to the questionnaires, university students look forward to more lively and brilliant colours in the game interface. Therefore, designers use vivid colours such as blue, pink, purple and green to attract students on login screen (see Figure 2).

Figure 2. User Interface Design of Home screen

Bright colours are often used to attract attention but they may not be beneficial if the purpose of the designer is to draw students' focus on screen for long period. Instead, such complementary colours as red-green, and white-black will be effective in highlighting learning contents.

2) *Structure*

The storage capacity of a mobile device is limited, so developers should exploit all possible ways to reduce the file size of the program and installation package. Tabs usually require complex programming and several background images. Therefore, we found that superimposed pictures will facilitate interface design and reduce the file size (see Figure 3).

Figure 3. Tab switches design

Developers only need to change the underlying background to achieve interface effects. At the same time, the hot zone is also designed to solve the limitations of the text menus' focus. The menu event will be triggered as soon as the user touches the hot zone.

3) *Usability*

Serious games should minimize the user's operation and provide specific necessary tips. The main game interface design is coherent with the style of Select screen (see Figure 4). A timer, which directly connects with time incentives, is placed on the left side of the screen. The more time remains, the higher bonus will be added to the total score.

Figure 4. Main Screen

In addition, the entire screen only uses three buttons and developers use multiple gestures as a trigger condition to avoid complex interfaces. In order to reduce duplication of pictures loaded, different buttons use the same set of background images with different words on the pictures.

B. *Game Mechanics*

Game mechanics influence the game's entertainment and education. iPlayCode has two mechanisms to improve learning efficiency, including incentive mechanisms and competition mechanisms, which will be discuss in detail in this section.

1) Incentive Mechanisms

Any game must reward excellence players and punish failed players. As a result, this serious game has a punishment mechanism. In details, players will be deducted 5 points when they choose the wrong answer. Furthermore, according to the speed of answering, each correct answer gains up 10 points as an award. However, if the student does not answer the questions within the prescribed time, bonus points will be cancelled.

The reward mode is divided into two sub-modes including medal mode and coins mode. Firstly, visual incentives will trigger visual learners' motivation, which is why medal images as well as texts are used to represent the result (see TABLE II).

TABLE II. MEDAL MODE

		
0%-39%	40%-69%	70%-100%

Secondly, coin mode is set up to highlight the distinction within one medal as the users with the same medal can have different scores. Moreover, it is also useful to reward users' continuous effort in the way that coins are accumulated throughout the game until it gets to a certain quantity. At this point, users are awarded a certificate to mark their milestones.

2) Competition Mechanisms

Competition also plays an important role in motivating students. In this game, students will need to compete with themselves rather than other people as they can repeat the level until they get a satisfactory result. By such repeated practice, students may find it easier to remember the knowledge and find more details within the problem.

V. IMPLEMENTATION

The main purposes of iPlayCode are to create good user experience and improve the expandability of the game as well as to enhance learning environment. To achieve these goals, we will introduce the construction of the following parts of the game.

A. Interface Implementation

1) Tab Navigation

According to previous design, tab navigation will be divided into two parts, namely, foreground and background. Text menu as foreground controls page contents using CCMenuItemFont class and it can also change the background image layer to show the selected tab. setTag() method defines the tag of label and getTag() method can obtain the tag of label to determine the selected tab.

The effective selection area of text menu is usually limited to the text size or length. setContentSize() method can set a specific area as a text hotspot. Users only need to click on a fixed area to trigger the selected menu.

```
void MenuSelect::menuCallback(CCObject* pSender){
    CCMenuItemImage* item = pSender;
    if (item->getTag() == 1) {// show level 1
        pTabBackground1->setVisible(true);
    } else if (item->getTag() == 2) { // show level 2
        pTabBackground2->setVisible(true);
    }
}
```

2) Simplified Buttons

Buttons are an indispensable part of serious games. However, a large number of button increases the complexity of the interface and the use of them can be confusing to users. Consequently, we reduce the number of buttons using CCMenuItemImage and CCLabelTTF class. In details, CCMenuItemImage class as background can be triggered as an image menu item and its upper layer is a text layer, CCLabelTTF, which can be changed by setString() method. In addition, this serious game is a multi-language application, and changing a text in different languages will be easier than changing an image button. So, text is used in the simplified button. Implementation of this function is as follows:

```
void GamePlay::menuCallback(CCObject* pSender){
  if (menu is answering){
     button0->setString(“%d”,Right_string);//change text
     button1->setString(“%d”,Wrong_string);//change text
  } else if (menu is answered) {
     button0->setString(“%d”,Help_string);//change text
     button1->setString(“%d”,Next_string);//change text
  } ... // change actions of buttons
}
```

B. Game Elements Implementation

1) Timing

Animation, combined with sound effects, will enhance the game's entertaining effect and a timer will accelerate the speed of the game. On the other hand, the speed of users to make correct decisions is also a crucial criterion to measure the efficiency of their learning. Therefore, CCSpriteFrame and SimpleAudioEngine class will be used to practice the timer in order to improve teaching effectiveness. Schedule Class as system timer will trigger the animation and play sound effects using the following method:

```
void GamePlay:: schedule_step(){
    CCArray* animFrames = CCArray::
     createWithCapacity (30);
    for(int i = 1; i <31; i++){
      CCSpriteFrame* frame = cache->
     spriteFrameByName("clock-%d.png", i);
      animFrames->addObject(frame);
    }
    CCAnimation* animation = CCAnimation::
    createWithSpriteFrames(animFrames, 0.5f);
    clockSprite->runAction(animation);
```

sharedEngine()->playBackgroundMusic("timer.caf");

}

2) *Self-competition*

According to Kolb's experiential learning theory, learning requires repeated practice and thinking. To motivate students to learn and master the basic knowledge, self-competition mechanism plays an important role. The results of users are stored in the database and are shown in the results interface. Results for each subject are also presented in the menu page.

Moreover, all students' results will be stored in myResult[], which is an array of integers, and uploaded to the server so that teacher can check students' learning progress and outcome.

VI. TECHNICAL ASSESSMENT

Alpha testing has been carried out, in this project and this section will provide detailed test results, including functional testing, performance testing and usability testing.

A. *Functional Testing*

TABLE III describes the performance of different functions in a network environment and a non-network environment. Information reading and writing are running properly in the corresponding module.

TABLE III. FUNCTIONAL TESTING RESULTS

Functions	Stand-alone	Online
Obtain Information	-	√
Upload Information	-	√
Save Local File	√	-
Virtual Keyboard	√	√
Level Switching	√	√
Screen Transition	√	√
Answer Judgment	√	√
Incentive Mechanism	√	√
System Prompts	√	√
Display Results	√	√
User Logout	-	√

Moreover, main functions of the system obtained positive feedback in both modules.

B. *Performance Testing*

System performance determines the user experience as well as the fluency of the game. Performance test chose the equipment with different operating systems. Test environments are iOS 7.0.2 (11A501), iOS7.0.3 (11B511) and iOS 7.0.4 (11B554a). The test results are preisstent and positive.

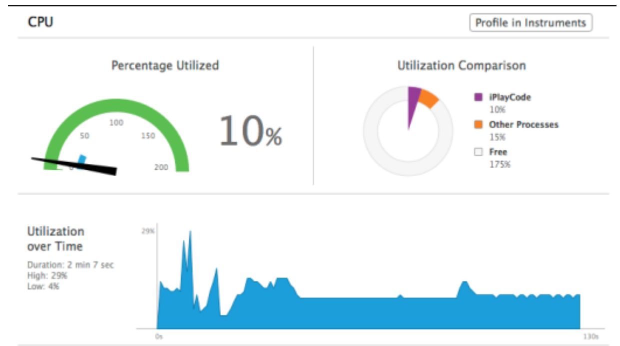


Figure 5. Performance testing of CPU

Figure 5 summarizes the performance of iPlayCode on these systems.

A. *Usability Testing*

This test includes five components: learnability, efficiency, memorability, errors and satisfaction. 36 students were invited to participate in the usability testing. The test results are as follow:

Learnability: Every user can manage this application when they first encounter this design.

Efficiency: Experienced users can quickly complete a concept within three minutes.

Memorability: When users are asked to play it again, most users can pay direct attention to the questions without thinking about operations steps.

Errors: Users' errors can be corrected by the system prompts. In addition, the back button can easily recover the system from a user's misuse.

Satisfaction: 61% of users prefer to use this game, because the interface is easy to use and manage. Furthermore, they enjoy iPlayCode with incentives and competition mechanisms.

VII. CONCLUSION AND FUTURE WORK

In this paper, based on the learning theory and model, the approach of using the mobile serious game for programming learning has been proposed and evaluated. Learning from this paper are the following:

1. Serious games should be developed as a learning cycle mode to improve the efficiency of learning and differentiated learning should also be designed in the early stage of software development.
2. Serious games should try to use vibrant colours (blue, pink, purple, green) to attract attention and complementary colours to get effective learning. System testing found that simple operation and appropriate prompt improve the user's experience.
3. A property list file implements multi-resolution adaptation and multilingual environment. Automatic data acquisition enhances the data analysis capabilities.

In the future, the development team will expand to include (1) more formative feedback to students, such as grade based on the score, ranking in game centre and the prompt of learning tasks, and (2) statistical analysis functions for teacher to gain more accurate information about students' engagement, progress, and performance.

REFERENCES

[1] T. Mitamura, Y. Suzuki, and T. Oohori, "Serious games for learning programming languages," Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on. IEEE, 2012, pp. 1812-1817.

[2] C. Xin, "Multiplayer Game in Mobile Phone Serious Game," Artificial Intelligence, 2009. JCAI'09. International Joint Conference on. IEEE, 2009, pp. 56-58.

[3] B. Kapralos, "A course on the design and development of serious games and virtual simulations," Games Innovation Conference (IGIC), 2012 IEEE International. IEEE, 2012, pp. 1-4.

[4] M. Prensky, "Digital game-based learning," Paragon House Publishers, 2007.

[5] M. A. Khenissi, F. Essalmi, and M. Jemni, "Presentation of a Learning Game for Programming Languages Education," Advanced Learning Technologies (ICALT), 2013 IEEE 13th International Conference on. IEEE, 2013, pp. 324-326.

[6] J. Lu, Z. Meng, and J. B. Stav, "A new approach in improving operational efficiency of wireless response system," Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on. IEEE, 2010, pp. 2676-2683.

[7] Apple. Eduction: ipad apps books and more. [Online]. Available from: http://www.apple.com/education/ipad/apps-books-and-more/ [accessed: 2014-01-29]

[8] C. Franzwa, Y. Tang, and A. Johnson, "Serious Game Design: Motivating Students through a Balance of Fun and Learning," Games and Virtual Worlds for Serious Applications (VS-GAMES), 2013 5th International Conference on. IEEE, 2013, pp. 1-7.

[9] M. Zapusek, S. Cerar, and J. Rugelj, "Serious computer games as instructional technology," MIPRO, 2011 Proceedings of the 34th International Convention. IEEE, 2011, pp. 1056-1058.

[10] S. A. Gamalel-Din, "An intelligent etutor-student adaptive interaction framework," Proceedings of the 13th International Conference on Interacción Persona-Ordenador. Elche, Spain, New York, NY, USA: ACM, 2012, pp. 12:1-12:8.

[11] A. K. Hazra, P. Patnaik, and D. Suar, "Influence of learning styles and academic achievement on performance and preference in different learning modes: An adaptive hypermedia approach," Intelligent Human Computer Interaction (IHCI), 2012 4th International Conference on. IEEE, 2012, pp. 1-7.

[12] J. H. Park, B. Abirached, and Y. Zhang, "A framework for designing assistive technologies for teaching children with ASDs emotions," CHI '12 Extended Abstracts on Human Factors in Computing Systems. Austin, Texas, USA, New York, NY, USA: ACM, 2012, pp. 2423-2428.

[13] D. Clow, "The learning analytics cycle: closing the loop effectively," Proceedings of the 2nd International Conference on Learning Analytics and Knowledge. Vancouver, British Columbia, Canada, New York, NY, USA: ACM, 2012, pp. 134-138.

[14] K. Mitgutsch and N. Alvarado, "Purposeful by design?: a serious game design assessment framework," Proceedings of the International Conference on the Foundations of Digital Games. ACM, 2012, pp. 121-128.

[15] F. Manga and J. Lu, "An Investigation in the Impact of Mobile Learning on today's Educational Environment," Proceedings of the 2013 International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government. EEE: WorldComp, 2013, ISBN: 1-60132-235-6.

.

CUDA Accelerated Entropy Constrained Vector Quantization and Multiple K-Means

John Ashley
NVIDIA UK Ltd.
London, UK
jashley@nvidia.com

Amy J. Braverman
Jet Propulsion Laboratory
Pasadena, CA, USA
amy.j.braverman@jpl.nasa.gov

***Abstract*—Multi-trial sampled K-means performance and scalability is studied as a stepping stone towards a Graphical Processing Unit implementation of Entropy Constrained Vector Quantization for interactive data compression. Basic parallelization strategies and data layout impacts are explored with K-means. The K-means implementation is extended to Entropy Constrained Vector Quantization, and additional tuning specific to the anticipated use case is performed. The results obtained are sufficiently promising that this will in the next phase be applied to the interactive exploration and visualization of very large satellite datasets.**

Keywords- K-Mean; Entropy Constrained Vector Quantization; Graphical Processing Unit; CUDA.

I. INTRODUCTION

This is a work in progress, and is currently in an early stage. The ultimate goal is to apply k-means or Entropy Constrained Vector Quantization (ECVQ) to interactive data compression as a component in a data exploration and visualization solution. Initially, this would support exploration of the Multi-angle Imaging SpectroRadiometer (MISR) Level 3 aerosol data sets. This phase of the work is intended to create an understanding of the scalability and performance of simple Graphical Processing Unit (GPU) accelerated versions of ECVQ and its algorithmically similar but simpler cousin, k-means clustering. K-means and ECVQ offer the potential to provide information preserving data compression on large datasets. Further research will then apply data visualization and exploration techniques on the reduced datasets.

In this paper, we first discuss k-means and ECVQ, and then proceed to an overview of GPUs and CUDA programming. The structure of the research codes, including the primary parallelization and tuning options explored, are presented. A review of some of the prior art is followed by relative performance results. Conclusions are drawn and the next steps in the work are briefly discussed.

II. K-MEANS AND ECVQ

The k-means algorithm is familiar in a wide variety of contexts. In this paper, a relatively simple version of the algorithm is adopted using sampling and multiple trials to extend the scalability to large datasets. Interested readers can consult a variety of texts and surveys of the field [1].

ECVQ can be viewed as a compression or clustering technique similar to k-means but with information-theoretic penalties applied to the distance function used to assign vectors to cluster centroids [7]. Specifically, it adds a multiple of the absolute value of the log of the fraction of measurements in a cluster to the L2 distance measure, which adds computational complexity but minimal additional data movement to the k-means algorithm. It is useful in a variety of contexts; this work was motivated by the use of ECVQ in the production of certain compressed NASA datasets [3].

Ignoring initialization and iteration limits, the basic algorithm to implement k-means with a number of training sets, each of a certain sample size, and a testing set is shown in Fig. 1.

```
For each training-set
    Repeat until labels are stable
        For each sample assign to nearest k
        For each k, calculate new centroid
For each testing set's final centroids
    For each test case assign to nearest k
    For each k calculate a quality measure
    Aggregate quality measures for the test set
Select best set of k
```

Figure 1: Algorithm Outline.

In Fig. 1, “nearest” is the L2 norm in the case of k-means or the L2 norm augmented by the information theoretic penalty function in the case of ECVQ.

There are several levels of parallelism available in the algorithm, as evidenced at the highest level by the “for each” lines of the algorithm. There are also serial data dependencies between the steps in the repeat loop and before the selection of the best k at the end.

III. GPUS AND CUDA

The General Purpose Graphics Processing Unit (GPGPU or usually just GPU) is the evolution of massively parallel hardware graphics accelerators whose base data types are the pixel, triangle, and image and whose basic functions were rasterization and shading. The programming model for these accelerators and their performance has evolved significantly, to the point where NVIDIA’s CUDA extensions to C++ and Fortran have been used in supercomputers and industrial

 ISBN: 978-1-61208-365-0

.

systems since 2006. There are numerous resources for learning more about GPU programming and software that is already GPU accelerated [4].

A. Logical Programming Model-- CUDA

A function to be executed on the GPU is called a *kernel*. These kernels are logically composed of many lightweight *threads* (frequently thousands to millions) which are launched as a *grid*. These threads are grouped together into *blocks*. The same kernel code is executed by every thread, but threads have unique thread and block indices which means each thread can operate on different data and follow different paths through the code. Threads within a block can synchronize with each other and can use a block-wide very fast pool of *shared memory* for coordination.

All threads in all blocks have access to fast global device memory on the accelerator. There are also ways to access the normal (relatively slow) memory of the host CPU system that are not important in the context of this problem.

As a programmer, the CUDA logical model guarantees that all the threads within a block will be assigned to an active hardware Streaming Multiprocessor with multiple cores at the same time. It does not guarantee which blocks will execute in what order.

B. Physical Execution Model

Physically, the GPU uses a hardware block and thread scheduler to assign blocks to hardware units called *Streaming Multiprocessors* (SMs). Depending on the hardware generation and model of the chip, the GPU may have one or more (14-16 for high end compute cards on the Fermi and recent Kepler generation chips) SMs each. In the latest Kepler generation GPUs, each of these SMs has 192 *cores* that perform the actual computing.

Because of the very large number of cores, and the way they are designed, GPUs are also sometimes characterized as being “throughput oriented” as opposed to traditional serial CPU cores which are “latency oriented”. A throughput oriented GPU’s thousands of cores are designed to enable very large numbers of concurrent threads to execute (or be ready to execute) simultaneously, thus hiding any latency a single set of threads might experience with productive work for other threads. A CPU’s dozen or so cores, in contrast, use much larger caches, branch prediction, out of order execution, and other optimizations to prevent latency from causing a very costly context switch of a very small number of threads.

GPU cores within an SM are grouped into sets of 32 cores. Threads from a block are assigned to cores in groups of 32 called *warps*. Threads within a warp effectively share a program counter and can follow different branches of code using hardware managed masking. Note that when a warp has threads which need to follow multiple paths of a branch construct, the warp will effectively serialize execution of each portion of the branch – this is commonly referred to as branch divergence; the GPU manages all this in hardware whereas on the CPU, the vector units face the same issue but have to manage it in software using explicit mask registers.

Blocks which have more than 32 threads require more than one warp of resources in the SM to execute. SMs have varying capacities in regards to resources available but generally are most efficient when running many blocks and warps on a SM simultaneously; this lets the SM hide the latency caused by various memory accesses and other activities by always having one or more warps ready and waiting to execute.

The memory hierarchy on the GPU, in order of increasing size and decreasing bandwidth, consists of thread private *registers*, block private *shared memory*, shared *L2 cache*, and *global device memory*. Peak bandwidth for global device memory on recent high end compute GPUs is 288 GB/second, significantly higher than traditional CPU memory.

The performance numbers in this research were developed on an NVIDIA K40 GPU with factory (base) settings, using the CUDA 5.5 toolkit on Linux. The conclusions should be broadly applicable to other hardware when scaled appropriately for compute and bandwidth.

IV. Code Structure

In the particular implementation strategy we use, which is modeled after the processing used to create ECVQ compressed datasets for the MISR and AIRS satellite data, some number of trials are performed, each using a set of training vectors sampled from the overall population. These are clustered to produce candidate cluster centroids. Candidate cluster centroids are evaluated against a larger testing set and the final set of cluster centroids are selected.

The focus of this investigation is on the performance of the three most important and time consuming components of the solution – steps that will be referred to as *Label*, *Calculate*, and *Score*.

A. Parallelization Strategy

Label assigns training vectors to cluster centroids, and determines if the solution has converged. Each trial is performed by a single thread block, and each thread within that block will work on one training vector, evaluating the distance from each centroid, and performing the assignment. In cases where there are more training vectors than there are threads per block, the threads will stride over the set of vectors until each vector has been updated.

Calculate updates the cluster centroids based on the training vectors assigned to that cluster centroid. Each trial is performed by a single thread block, and each thread within that block will work on one centroid, which it will update. In cases where there are more centroids than there are threads per block, the threads will stride over the set of centroids until each centroid has been updated.

Score will evaluate every testing vector against the set of centroids from each trial, and produced the per cluster dispersion. Each thread block will evaluate the set of testing vectors against the centroids from a single trial. The threads within the block will each stride over the testing vectors until all vectors have been evaluated.

B. K-Means Codes

A basic, "naïve" version of k-means along the lines of the code described above was created. This version is referred to as *K1*. This code attempts to be as simple as possible, and as straightforward, to reflect code that could be delivered to, maintained by, and possibly extended by a typical scientific programmer, if such a person actually exists.

One common performance issue for GPU codes is related to memory access patterns – memory requests from within a warp can be combined if they are for adjacent memory locations. This can drastically increase the efficiency of the memory subsystem and have substantial performance impacts on the code. *K1* uses the first layout in Fig. 2, below. A second version of the code, using the second layout below, called *K2*, was also tested. This code differs only in the data layout used, and while perhaps less "natural" to a scientific programmer, would not be difficult to maintain or extend.

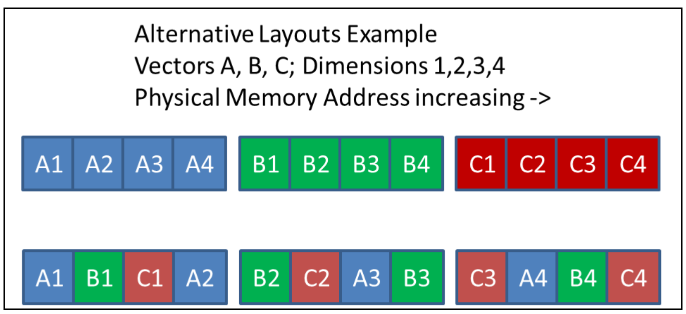


Figure 2: Memory Layouts.

C. ECVQ Code

One of the versions of the k-means code (*K2*) was converted into an ECVQ code via the addition of the information theoretic penalty functions and associated bookkeeping. This version is called *E2*.

A second version of the ECVQ code was also developed that begins to explore the performance impacts of tuning for a specific final problem size. This version is called *E3*, and the very minor tuning specializations it incorporates are discussed along with the performance results.

V. Prior Art

The motivation for the current work is based firmly in a selection of the prior art. A technique for displaying large numbers of weighted clusters of high dimensional data vectors applied to the AIRS cluster compressed data appears promising for application to the MISR dataset as well [6]. Current processing of the MISR dataset using ECVQ faces the same operational limits as the AIRS data, and can take no more than 2 hours per 5-days of input data per 5^o x 5^o earth grid cell but provides excellent compression and information retention [2,7]. While this performance is acceptable for offline data processing, allowing interactive use in visualization will require higher performance.

K-means is closely related to ECVQ [2] and is well studied on the GPU [5,9,10]. Most prior work has focused on the relative acceleration with respect to various CPU only codes. In this work, we explore only the actual performance of the GPU version of the code, although absolute performance numbers for earlier generations of GPUs are available for some problems [10].

The use of ECVQ in data compression is well established [2]. There is a small body of work on the use of ECVQ in satellite data applications [3,7,8]. To date there appears to be little if any published work on using GPUs to accelerate computation of ECVQ.

VI. Performance Results

This research is currently using parameterized random data generation for test purposes. This allows exploration of the parameter space for performance characterization and allows the code to be self-contained. The first actual deployment target of this research will be a MISR aerosol dataset with 8 data dimensions plus spatial and time metadata. Current NASA processing on this dataset uses 200 trials each with 200 training vectors, with a maximum K value of 100. Our basic test case is deliberately chosen to be similar to these values. Other envisioned uses would be to apply the technique to NASA AIRS datasets with 32 data dimensions plus meta-data; this defines the size of one of the larger test cases.

A. Test Cases

We define a set of parameters which will be varied to examine the performance of the code over a small range of values as defined in Table 1.

TABLE 1. Test Scale Parameters.

Variable	Description
N	Data dimensions
K	Maximum number of clusters
T	Trials
S	Training Vectors (Sample Size)
V	Testing Vectors

We use these parameters to both define test cases and set expectations on the performance of each problem phase (Label, Calculate, Score) for each test. The phases are sensitive to the Test Scale Parameters as shown in Table 2.

TABLE 2. Performance Sensitivity Expectations.

Phase/Value	N	K	T	S	V
Label	X	X	X	X	
Calculate	X	X	X	X	
Score	X	X	X		X

.

Given that there is going to be some overhead in each phase, we expect good code to have better than linear response to an increase in the appropriate parameters, unless we exceed the capacity of some resource (such as cache) that was not exhausted at the lower scale. More specifically, if we increase N by a factor of 4, we would expect all phases to show execution time increases of something somewhat less than four.

Test cases were defined with Test Case 1 as a "base" case, with each of cases 2-6 testing the scaling of a different parameter. Test Case 7 shows the scaling on a larger problem. Details of each test case are in Table 3.

TABLE 3. TEST CASES.

Test Case	N	K	T	S	V
1	8	128	256	256	100,000
2	8	256	256	256	100,000
3	8	128	512	256	100,000
4	8	128	256	512	100,000
5	8	128	256	256	200,000
6	32	128	256	256	100,000
7	8	128	1024	1024	1,000,000

B. *Scaling with K1 Across Cases*

The first round of testing verified the expected scaling behavior of the K1 "naïve" version of the code across the various test cases. The actual timing results for 100 iterations of Label and Calculate, and one final round of Scoring, on Test Case 1, are in Table 4.

TABLE 4. MEAN EXECUTION TIMES.

Execution	100xLabel	100xCalculate	Score
Time	104.1ms	129.3ms	2.58s

The Score phase is far longer than the other phases, as would be expected, as V >> S. All performance charts following this express performance relative to the values in Table 4. For the K1 code, performance is broadly in line with expectations, as can be seen from Fig. 3.

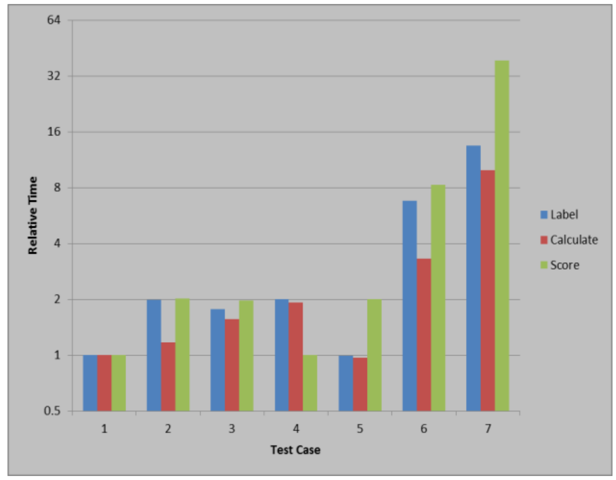


Figure 3. Relative performance of K1 across test cases.

We see roughly expected scaling except that Calculate doesn't see as much impact in Test Case 2 as might be expected, since it should have runtime proportional to the Label step. The actual code in K1 is quite naïve, and launches more threads per trial than are needed for K=128; specifically, it launches 256 threads. In cases with less than 256 clusters, some threads start and exit, doing no effective work. In Test Case 2, these threads work and then exit, and so have minimal impact on the runtime. The Label and Score steps, in Test Case 6, seem to be running longer than expected. This appears to be because more registers spill to cache with D=32 than with D=8, causing some additional impact.

C. *Relative Performance of Codes in Test 7*

In Test Case 7, we would expect to see any impact from improvements in code or increases in the complexity of calculations to be magnified by the scale of the problem. To that end, codes K2 and E2 were tested against Test Case 7, with the results shown in Fig. 4.

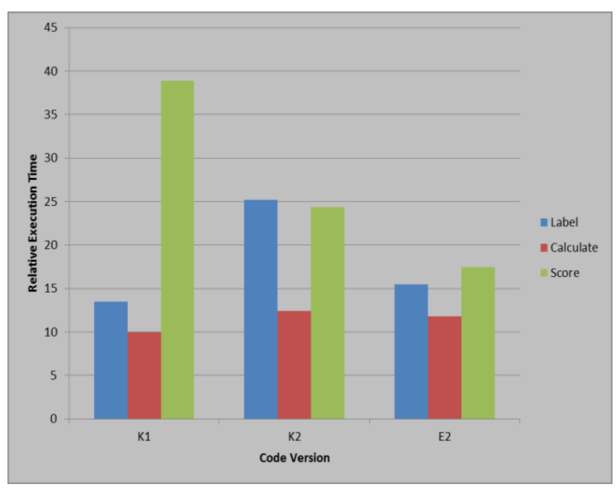


Figure 4. Relative Performance of Code Versions.

 ISBN: 978-1-61208-365-0

.

As we discussed earlier in sections IV.B and IV.C, the *K2* version of the K-means code uses a more GPU performance friendly data layout than *K1*. This code is actually slower than the naïve code for Label and Calculate, which appears to be due to cache and compiler generated code optimization interactions, but the additional efficiency of the memory layout pays significant dividends on the much longer Score phase. Because the overall runtime is significantly reduced, the code for the first ECVQ version (*E2*) was based on the *K2* code and data layout.

D. Initial Exploration of Problem Specialization

The code in E2 is already almost fast enough for interactive use on real problems, but it would be better if it were even faster. Earlier we admitted that unlike typical "finished" work, this code was relatively general and made relatively few concessions to what is sometimes called "ninja tuning". We did, however, explore a very simple specialization to the problem using a very simple performance enhancer, namely, a "#pragma unroll" directive. This directive, embedded in a comment before a loop, instructs the compiler to rewrite the loop to have more copies of the code inside it and make correspondingly less trips through the loop. Our code *E3* is optimized for values of D that are a multiple of 8, with one inner loop in each phase unrolled by a factor of 8. The performance impact on Test Case 1, the test case closest to our envisaged real world workload, is significant, as can be seen in Fig. 5.

The Score phase, in particular, benefited greatly from this very minor optimization.

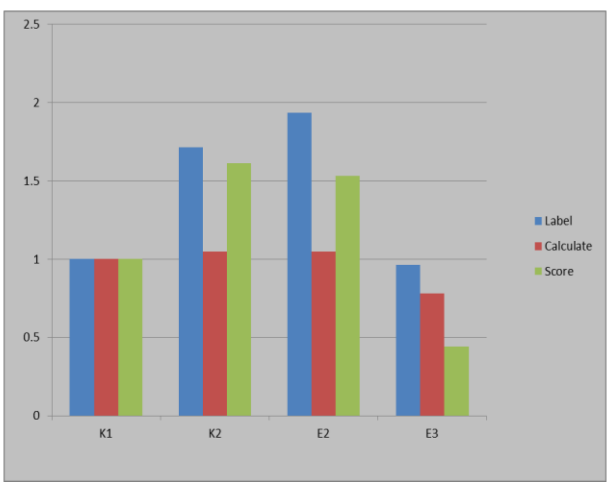


Figure 5. Relative performance including tuned code.

Additional, possibly more code invasive tuning should allow for further improvements.

VII. Conclusions and Future Work

We set out to explore the suitability of K-means or ECVQ for interactive data compression in support of data exploration of a specific NASA dataset. Scalability testing on synthetic data showed that the code has relatively predictable and linearly bounded performance. Conversion of the compression from K-means to ECVQ was shown to have minimal impact to overall performance.

Finally, with even very simple performance tuning that specializes the solution to the anticipated problem, significant performance gains were observed, with overall execution times approach one second, which would be sufficient for many interactive uses.

Next steps for this research include exploring some additional tuning to reflect the anticipated problem sizes and then to do performance and quality testing with real data. These next steps will then be incorporated into a data exploration environment for the MISR data.

Acknowledgment

John Ashley would like to thank Dr. Daniel Carr at George Mason University, for his support and insights during this work. John Ashley would also like to thank my employer, NVIDIA, for their support.

References

[1] R. Xu and D. Wunsch, "Clustering," IEEE Press Series on Computational Intelligence, 2009.

[2] P. A. Chou, T. Lookabaugh, and R. M. Gray, "Entropy-constrained vector quantization," IEEE Trans. on Acoustics, Speech, and Signal Processing, Jan 1989, Vol 37, Issue 1, 1989, pp.31- 42.

[3] A. J. Braverman, E. J. Fetzer, B. H. Kahn, E. M. Manning, R. B. Oliphant, and J. P. Teixeira, "Massive dataset analysis for NASA's Atmospheric Infrared Sounder," Technometrics, 2012 [b], 54:1, pp. 1-15.

[4] NVIDIA Corporation, "http://docs.nvidia.com/cuda," 2014.03.12, unpublished.

[5] B. Catanzaro, "https://github.com/BryanCatanzaro/kmeans," 2014.03.12, unpublished.

[6] J. Ashley, "Techniques for exploring cluster compressed geospatial-temporal satellite datasets," Ph.D. Dissertation, George Mason University, 2013.

[7] A. Braverman, ''Compressing massive geophysical datasets using vector quantization," Journal of Computational and Graphical Statistics, 2002, 11, pp. 44–62.

[8] A. Braverman, E. Fetzer, A. Eldering, S. Nittel, and K. Leung, ''Semi-streaming quantization for remote sensing data," Journal of Computational and Graphical Statistics, 2003, 12 (4), pp. 759–780.

[9] S. A. Arul Shalom, M. Dash, and M. Tue, "Efficient k-means clustering using accelerated graphics processors," Data Warehousing and Knowledge Discovery Lecture Notes in Computer Science Volume 5182, 2008, pp. 166-175.

[10] K. J. Kohlhoff, V. S. Pande, and R. B. Altman, "K-means for parallel architectures using all-prefix-sum sorting and updating steps," IEEE Transactions on Parallel and Distributed Systems, Aug 2013, Vol 24, No. 8, pp. 1602-1612.

 ISBN: 978-1-61208-365-0

Scheduling periodic Tasks on Multiple Periodic Resources

Xiayu Hua, Zheng Li, Hao Wu, Shangping Ren
Department of Computer Science
Illinois Institute of Technology
Chicago, IL 60616, USA
{xhua, zli80, hwu28}@hawk.iit.edu, ren@iit.edu

***Abstract*—In this paper, we study the problem of scheduling periodic tasks on multiple periodic resources. We take two step approach by first integrating multiple periodic resources to an equivalent single periodic resource so that existing real-time scheduling theorems on single periodic resource can be applied. Second, we extend the schedulability tests of periodic tasks on a single periodic resource in continuous time domain given in[1] to discrete and finite time domain so that the schedulability tests can be applied in practice. We further empirically study the performance of periodic resource integration. Experiment results reveal the following interesting behaviors: 1) increasing the number of periodic resources does not necessarily increase the integrated resource's capacity; 2) integrating smaller capacity periodic resources has higher capacity increase than integrating larger capacity periodic resources; and 3) integrating periodic resources that have the same capacity results in the most capacity increase in the integrated resource.**

***Keywords*—Periodic Resource; Real-time scheduling; Resource integration; Task assignment.**

I. Introduction

In real-time community, for a long time, the focus of scheduling problems has been on *dedicated* resources, the resources that are constantly available to tasks. However, as virtualization technology develops, resources, especially virtual resources, are not dedicated resource any more. The virtual resources are often modeled as *periodic resources* which are only available for certain amount of time within a given period [2][3][4][5][6].

The study of periodic resources can be traced back to the time when the concept of time-division sharing is proposed. Time-division sharing is one of the most important technologies and also one of the most efficient way to accommodate multiple applications on a single resource [2][7]. One realistic example is the virtualization system like XEN [6] where multiple virtual machines may share one CPU, so each virtual machine obtains a portion of the CPU's execution time. With time-division sharing scheduling algorithms, such as round-robin and server-based scheduling algorithms, resources manifested to applications are periodic resources. The purpose of these algorithms is to partition a dedicated resource to serve multiple applications, rather than how to schedule a task on a periodic resource. Research on the schedulability issue of multiple tasks on a single periodic resource started in late 90s [2] and has recently draw more attention in the community [1][3][4][8][9][10]. However, until now, there has not been much, if any, work in the literature dealing with the issue of scheduling a periodic task set on multiple periodic resources when none of the individual periodic resource has large enough capacity to support the given task set.

In this paper, we study the problem of scheduling periodic task set on multiple periodic resources. To address the issue, we take two steps, first study how multiple periodic resources can be integrated into an equivalent single periodic resource so that the existing real-time scheduling theorems on a single periodic resource can be applied. Second, we extend one of the existing schedulability test for a single periodic resource proposed by Lee [1] from continuous time domain to discrete and finite time domain so that the test can be of practice use. We further use extensive simulation to observe the resource capacity increase patterns when periodic resources of different capacities are integrated.

The rest of paper is organized as follows: Section II discusses the related work. Section III defines terms and models that the paper is based on and also formulates the problem to be addressed in the paper. The equivalent transformation of multiple periodic resources into a single periodic resource is discussed in Section IV. In Section V, we extend Lee's schedulability test [1] of multiple tasks on a single resource from continuous time domain to discrete and finite time domain. Section VI empirically studies the performance of integrating periodic resources with different capacities. Finally, we conclude in Section VII.

II. Related Work

Real-time scheduling problem has been studied extensively for half century. Most of the researches on the problem are focusing on dedicated resources over past decades. As the computer technology develops, single resource nowadays can provide thousands of more computational capabilities compared to decades ago. Hence, the real-time scheduling problem is extended from how to schedule a group of tasks onto a dedicated resource to how to schedule multiple groups of tasks onto a dedicated resource. One of the most intuitive way to schedule multiple groups of tasks onto a single dedicated resource is to split the dedicated resource into several partitions; then, schedule each group of tasks to its corresponding partition. This is the essential concept of periodic resource [2].

Although the periodic resource model has not been formally defined until later 90s [2], the insight of periodic resource can be traced back as early as the concept of time-division sharing was proposed. Time-division is one of the most efficient way to distribute resources to tasks [2][7]. Server-based scheduling

 ISBN: 978-1-61208-365-0

mechanism is one of the most popular time-division mechanisms to accommodate multiple groups of tasks and provide some level of schedulability guarantees [11], and extensive research work [12][13][14] developed different mechanisms to improve tasks' response time.

Server-based mechanisms can be treated as strategies to adjust the resource partition to meet tasks' specific demands. Considering the resource partition is given and cannot be adjusted, Shirero *et al.* [2] first defined periodic resources and proposed a real-time round robin scheduling algorithm in 1999. They also introduced the concept of *resource regularity*. Based on resource regularity, they proposed schedulability bounds for periodic tasks. Mok *et al.* [3][15], then, extended Shirero's work and proposed a more comprehensive schedulability analysis for periodic resources under Earliest Deadline First (EDF) and Rate Monotonic (RM) scheduling algorithms. However, both Shirero and Mok's periodic resource model had constraints that either the resource pattern or the resource regularity should be given. By removing the constraints, Shin *et al.* then extended the periodic resource model to a more general case and provided a complete schedulability analysis under such model and gave the schedulability bounds for both EDF and RM accordingly [1][10].

Also, both Shirero's original periodic resource model and Shin's extended model were only trying to solve the real-time scheduling problems on single periodic resource. Instead, in this paper we investigate the problem of how to integrate multiple periodic resources into an equivalent single periodic resource so that the existing theorems for single periodic resource can be applied.

III. System Models and Problem Formulation

A. Terms and Definitions

In this section, we first give the definitions and notations that are used in the following parts. Then, we define the system models and formulates the problem we are to address.

Task Set Model Γ

A task set contains a set of periodic tasks, i.e., $\Gamma = \{\tau_1, ..., \tau_n\}$ with $\tau_i = (p_i, e_i)$, where p_i and e_i are the task's period and worst case execution time, respectively.

Resource Model R

The resource we consider is a periodic resource, represented as $R = (\pi, \theta)$, where π is a period and θ is the total amount of available time durations $(0 < \theta < \pi)$ within each period.

Capacity of Resource $C(R)$

The capability of a periodic resource $R(\pi, \theta)$ is defined as $C(R) = \frac{\theta}{\pi}$.

Periodic Resource Pattern(P_R)

Given a periodic resource $R(\pi, \theta)$, its pattern P_R defines its time availability within its period, i.e., $P_R(t) = 1$ indicates that the resource is available at time t, or it is not available at time t if $P_R(t) = 0$.

Fixed Pattern Periodic Resource

If a periodic resource is of fixed pattern, then $P_R(t) = P_R(t + k \times \pi)$, where $k \in \mathbb{N}^+$.

Continuous Periodic Resource

Given fixed pattern periodic resource $R = (\pi, \theta)$, it is a continuous periodic resources if and only if $\forall i \in [0, \theta - 1], k \in \mathbb{N}^+, P_R(i + k \times \pi) = 1$.

Synchronized Periodic Resource

Two periodic resources are synchronized if the start points of the two periods are the same.

Equivalent Single Resource Transformation of Periodic Resource Set ($I(\Psi)$)

For a set of periodic resource $\Psi = \{R_1, R_2, ..., R_n\}$, its equivalent single periodic resource transformation is defined as $I(\Psi)$ with $\forall t \in [0, LCM_{1 \le i \le n}(\pi_i)], P_{I(\Psi)}(t) = P_{R_1}(t) \vee P_{R_2}(t) \vee ... \vee P_{R_n}(t)$.

B. Problem Formulation

Given a set of periodic resources $\Psi = \{R_1, R_2, ..., R_n\}$ with $R_i = (\pi_i, \theta_i)$ and a periodic task set $\Gamma = \{\tau_1, \tau_2, ..., \tau_m\}$, decide schedulability test if the task set is schedulable on the resource set with EDF and RM, respectively.

We take two steps to address the problem, first, transform the periodic resource set into an equivalent single periodic resource (Section IV), and second apply extended single periodic resource schedulability test (Section V) to decide whether the given task set is schedulable on the given resources.

It is worth pointing out that the discrete time system is assumed, i.e., $\forall i \ p_i, e_i, \pi_i, \theta_i \in \mathbb{N}$. We also assume that tasks can not be executed parallelly, i.e., at each time instance t, tasks can only execute on one resource. Further more, we assume there is no overhead for task migration between different resources.

IV. Integration of Periodic Resources

Based on the definition of equivalent single periodic resource of a periodic resource set $\Psi = \{R_1, R_2, ..., R_n\}$, i.e., $P_{I(\Psi)} = P_{R_1}(t) \vee P_{R_2}(t) \vee ... \vee P_{R_n}(t)$, we can develop an algorithm to calculate $I(\Psi)$ as illustrated in Algorithm 1.

ALGORITHM 1: RES_INT($\Psi = \{R_1, R_2, ..., R_n\}$)

Calculate the hyperperiod of Ψ as $\lambda = \prod_{i=1}^{n} \pi_i$
$P_{I(\Psi)}(t) = 0, \forall t \in \{0, 1, ..., \lambda - 1\}$
$t = 0$
while $t < \lambda$ **do**
    for $i = 1$ ***to*** n **do**
        $P_{I(\Psi)}(t) = P_{I(\Psi)}(t) \vee P_{R_i}(t)$
    end
    $t = t + 1$
end
return $P_{I(\Psi)}$

Fig. 1. Algorithm 1

With Algorithm 1, we can obtain the equivalent single resource of a periodic resource set. However, Algorithm **??** needs to check whether each time unit is available or not within the hyperperiod λ, which is time consuming. In the following, we first give the upper and lower bound analysis of the equivalent single periodic resource's capacity, and then propose closed-form formula to directly calculate the

 ISBN: 978-1-61208-365-0

equivalent single periodic resource if the periodic resources satisfy certain conditions.

Lemma 1: Given a set of periodic resources $\Psi = \{R_1, R_2, ..., R_n\}$, then the capacity of its equivalent single periodic resource, i.e., $C(I(\Psi))$, satisfies the following condition

$$\max\{C(R_i), 1 \leq i \leq n\} \leq C(I(\Psi)) \leq \min\{1, \sum_{i=1}^{n} C(R_i)\} \tag{1}$$

Proof: By definition, $P_{I(\Psi)}(t) = P_{R_1}(t) \vee P_{R_2}(t) \vee ... \vee P_{R_n}(t)$, hence, we have $P_{I(\Psi)}(t) \geq \max\{P_{R_i}(t), 1 \leq i \leq n\}$, therefore, $\max\{C(R_i), 1 \leq i \leq n\} \leq C(I(\Psi))$.

If the available time slots of each periodic resource are not overlapped with each other, then the capacity $C(I(\Psi))$ is the sum of each individual periodic resource, i.e., $C(I(\Psi)) = \sum_{i=1}^{n} C(R_i)$. However, if the available time slots of any two periodic resources are overlapped, then $C(I(\Psi)) < \sum_{i=1}^{n} C(R_i)$. In addition, the resource capacity cannot exceed 1, so we have $C(I(\Psi)) \leq \min(1, \sum_{i=1}^{n} C(R_i))$. ■

It is worth pointing out that both the upper and lower bounds are tight bounds. For instance, with $R_1(3, 2)$ and $R_2(3, 1)$ with $P_{R_1}(0) = P_{R_1}(1) = 1$, $P_{R_1}(2) = 0$ and $P_{R_2}(0) = 0$, $P_{R_2}(1) = P_{R_2}(2) = 1$. Then for the equivalent single resource $I(R_1, R_2)$, $C(I(R_1, R_2)) = C(R_1)$. Similarly, with $R_1(3, 2)$ and $R_2(3, 1)$ and $P_{R_1}(0) = P_{R_1}(1) = 1$, $P_{R_1}(2) = 0$ and $P_{R_2}(0) = P_{R_2}(1) = 0$, $P_{R_2}(2) = 1$. Then for the equivalent single resource $I(R_1, R_2)$, we have $C(I(R_2, R_2)) = C(R_1) + C(R_2)$.

When the periods of periodic resources are mutually prime, we can derive the following Lemmas to simplify the calculation of periodic resource integration.

We first consider a simple case where one of the periodic resource has only 1 time slot available in each period.

Lemma 2: Given two fixed pattern periodic resource $R_1 = (\pi_1, \theta_1)$ and $R_2 = (\pi_2, 1)$. If π_1 and π_2 are mutually prime, then $I(R_1, R_2) = (\pi', \theta')$, where $\pi' = \pi_1 \cdot \pi_2$ and $\theta' = \pi_2 \cdot \theta_1 + \pi_1 - \theta_1$.

Proof: Suppose the pattern of R_2 is $P_{R_2}(k + i \cdot \pi_2) = 1$ where i is the number of period. That is, the kth slot of every period π_2 is available. We first assume the following condition hold and will prove it later:

- if $i_1 \neq i_2 \wedge i_1, i_2 \in \{0, 1, ..., \pi_1 - 1\}$, then

$$((k + i_1 \cdot \pi_2) \bmod \pi_1) \neq ((k + i_2 \cdot \pi_2) \bmod \pi_1) \tag{2}$$

The condition indicates that $\forall k \in \{0, 1, ..., \pi_1 - 1\}$, the kth time slot of resource R_1's period π_1 is overlapped with the available time slot of R_2 once within their hyperperiod $\pi_1 \cdot \pi_2$.

As within the hyperperiod $\pi_1 \cdot \pi_2$, $\pi_2 \cdot \theta_1$ available time slots are provided by R_1, $\pi_1 \cdot 1$ available time slots are provided by R_2, while θ_1 time units are overlapped, hence, we have $\theta' = \theta_1 \cdot \pi_2 + \pi_1 \cdot 1 - \theta_1 \cdot 1$.

Now, we prove that the above assumption holds.

Suppose that:

$$\exists i_1, i_2 : (k + i_1 \cdot \pi_2) \bmod \pi_1) = ((k + i_2 \cdot \pi_2) \bmod \pi_1)$$

then we have: $(k + i_1 \cdot \pi_2) \bmod \pi_1 - (k + i_2 \cdot \pi_2) \bmod \pi_1 = 0$, which implies

$$(k + i_1 \cdot \pi_2 - (k + i_2 \cdot \pi_2)) \bmod \pi_1 = 0 \tag{3}$$

hence, we have $(i_1 - i_2)\pi_2 \bmod \pi_1 = 0$.

Since $i_1 \neq i_2$ and $i_1, i_2 \in \{0, 1, ..., \pi_1 - 1\}$, then π_1 and π_2 are not mutually prime, which contradicts our assumption that π_1 and π_2 are mutually prime. Therefore, our assumption holds. ■

Lemma 2 gives the formulation to calculate the integration of two periodic resources when one of them only has one time slot available within each period, next, we remove this assumption and generalize the analysis to the integration of two fixed pattern periodic resources with arbitrary capacities.

Lemma 3: Given two fixed pattern periodic resources $R_1(\pi_1, \theta_1)$ and $R_2(\pi_2, \theta_2)$, if π_1 and π_2 are mutually prime, then $I(R_1, R_2) = (\pi', \theta')$ where $\pi' = \pi_1 \cdot \pi_2$ and $\theta' = \theta_1 \cdot \pi_2 + \theta_2 \cdot \pi_1 - \theta_1 \cdot \theta_2$.

Proof: According to Lemma 2, if R_2 has only one time slot available with each period, then R_1 and R_2 have θ_1 available time slots are overlapped within each hyperperiod $\pi_1 \cdot \pi_2$. Then if R_2 has θ_2 available time slots within each period, applying the similar proof of Lemma 2, we have $\theta_1 \cdot \theta_2$ available time slots are overlapped within each hyperperiod $\pi_1 \cdot \pi_2$. Since the total available time slots of R_1 and R_2 are $\theta_1 \cdot \pi_2 + \theta_2 \cdot \pi_1$, hence, we have $\theta' = \theta_1 \cdot \pi_2 + \theta_2 \cdot \pi_1 - \theta_1 \cdot \theta_2$. ■

Lemma 3 integrates two periodic resource, the following lemma generalize the calculation to multiple resources.

Lemma 4: Given a periodic resource set $\{R_1, R_2, ..., R_n\}$ with $R_i = (\pi_i, \theta_i)$, if all the periods of the periodic resources in this set are mutually prime with each other, then $I(R_1, R_2, ..., R_n) = (\pi'_n, \theta'_n)$, where

$$\theta'_n = \begin{cases} \theta_1 \cdot \pi_2 + \theta_2 \cdot \pi_1 - \theta_1 \cdot \theta_2 & \texttt{if } n = 2 \\ \theta'_{n-1} \cdot \pi_n + \theta_n \cdot \pi'_{n-1} - \theta_n \cdot \theta'_{n-1} & \texttt{if } n > 2 \end{cases} \tag{4}$$

where $\pi'_n = \prod_{i=1}^{n} \pi_i$.

Proof: With Lemma 3, we can obtain the equivalent single periodic resource of R_1 and R_2, i.e., $I(R_1, R_2) = (\pi_1 \cdot \pi_2, \theta_1 \cdot \pi_2 + \theta_2 \cdot \pi_1 - \theta_1 \cdot \theta_2)$. By treating $I(R_1, R_2)$ as a single resource, applying Lemma 3 to integrate resource R_3, we have $I(R_1, R_2, R_3) = (\prod_{i=1}^{3}, \theta'_2 \cdot \pi_3 + \theta_n \cdot \pi'_2 - \theta_3 \cdot \theta'_2)$. Follow the procedures, repeating the above steps until the resource R_n finishes the proof. ■

The previous lemmas have a constraint that resource periods are mutually prime. We now remove the constraint and discuss a general case for integrating two synchronized and continuous periodic resources.

Lemma 5: Given two synchronized and continuous periodic resource $R_1(\pi_1, \theta_1)$ and $R_2(\pi_2, \theta_2)$. Without loss of generality, we assume $\pi_1 \geq \pi_2$ and their hyperperiod be π'. Let $tail_i = (i + 1)\pi_1 \text{mod} \pi_2, i \in [0, \pi'/\pi_1 - 1]$ and $k_i = \lfloor \frac{\pi_1 - \theta_1 - tail_i}{\pi_2} \rfloor$, then integrated resource capacity within a hyperperiod is:

$$\theta' = \sum_{i=1}^{\pi'/\pi_1} \theta_1 + \max\{\min\{\theta_2, tail_i\} - \max\{\theta_1 - (\pi_1 - tail_i), 0\}, 0\} + \max\{k_i\theta_2 + \max\{0, \pi_1 - tail_i - (k_i + 1) + \theta_2 - \theta_1\}, 0\} \tag{5}$$

The proof of the lemma is illustrated in our technical report [16] .

V. SCHEDULABILITY ANALYSIS ON SINGLE PERIODIC RESOURCE

For self-containment, we first introduce the existing work about schedulability test on single periodic resource given in [1].

A. Existing Schedulability Tests on Single Periodic Resource

Given a periodic resource R, the resource *supply bound function* $sbf_R(t)$ represents the minimum available time that resource R can guarantee to supply within any time interval of length t. It can be calculated as below [17]:

$$sbf_R(t) = \begin{cases} t - (k+1)(\pi - \theta) \ \texttt{if} t \in [(k+1)\pi - 2\theta, (k+1)\pi - \theta] \\ (k-1)\pi \ \texttt{otherwise} \end{cases} \tag{6}$$

where $k = \max(\lceil (t - (\pi - \theta))/\pi \rceil, 1)$.

In order to meet timing constraints of task set Γ, a *demand bound functions* $dbf_{\text{EDF}}(\Gamma, t, \tau_i)$ and $dbf_{\text{RM}}(\Gamma, t)$ under EDF and RM scheduling policies, respectively, represent the maximum possible resource demand that $\tau_i (\tau_i \in \Gamma)$ may required within time interval of length t in order to meet the timing constraint. They can be calculated as below [17]:

$$dbf_{EDF}(\Gamma, t) = \sum_{\tau_i \in \Gamma} \left\lfloor \frac{t}{p_i} \right\rfloor e_i \tag{7}$$

$$dbf_{RM}(\Gamma, t, \tau_i) = e_i + \sum_{\tau_k \in HP(\tau_i)} \left\lceil \frac{t}{p_k} \right\rceil e_k \tag{8}$$

where $HP(\tau_i)$ is the set of higher-priority tasks than $\tau_i \in \Gamma$.

With the resource demand bound functions and resource supply bound functions, the schedulability test under EDF and RM scheduling policies can be represented as follows:

Lemma 6: (Theorem 4.1 in [1]) Given $\Gamma = \{\tau_1, ..., \tau_n\}$ and a periodic resource is R, the task set Γ is schedulable under EDF if and only if

$$\forall t : 0 < t \leq LCM_\Gamma : \ dbf_{EDF}(\Gamma, t) \leq sbf_R(t) \tag{9}$$

where LCM_Γ is the least common multiple of p_i of all $\tau_i \in \Gamma$.

Lemma 7: (Theorem 4.2 in [1]) Given $\Gamma = \{\tau_1, ..., \tau_n\}$ and a periodic resource R, the task set is schedulable under RM if and only if

$$\forall \tau_i \in \Gamma, \ \exists t_i \in [0, p_i] : \ dbf_{RM}(\Gamma, t_i, \tau_i) \leq sbf_R(t_i) \tag{10}$$

It is not difficult to see that both the schedulability tests are in continuous time domain, hence, they are only of theoretic value and can not be directly applied as schedulability tests in practice.

B. Discrete Time Domain Schedulability Tests

In this subsection, we give corresponding discrete time domain schedulability tests.

1) Schedulability Test under EDF:

Lemma 8: Given $\Gamma = \{\tau_1, ..., \tau_n\}$ and a periodic resource R, the task set Γ is schedulable under EDF if and only if :

$$\forall t \in \Omega : dbf_{EDF}(\Gamma, t) \leq sbf_R(t) \tag{11}$$

where Ω is a time point set defined in (12) and sorted in ascending order:

$$\Omega = \bigcup_{j=1}^{n} \Phi_j, \Phi_j = \{1, 2, ..., \text{LCM}_\Gamma / p_j\} \tag{12}$$

where LCM_Γ is the least common multiplier of all p_i with $\tau_i \in \Gamma$.

Proof: We prove this Lemma by proving (11) $\leftrightarrow$ (6).

We first prove formula (11) $\rightarrow$ (6) and we prove by contradiction.

Suppose that formula (11) $\rightarrow$ (6) does not hold, i.e.,

$$\forall t \in \Omega, dbf_{EDF}(\Gamma, t) \leq sbf_R(t)$$

but,

$$\exists t', 0 < t' < LCM_\Gamma, dbf_{EDF}(\Gamma, t') > sbf_R(t')$$

Without loss of generality, we further assume $t_i < t' < t_{i+1}$, where t_i and t_{i+1} are consecutive points in Ω.

As both demand and supply bound functions are non-decreasing functions [17], hence, we have

$$sbf_{EDF}(t') \geq sbf_{EDF}(t_i) \tag{13}$$

and,

$$dbf_{EDF}(\Gamma, t') \geq dbf_{EDF}(\Gamma, t_i) \tag{14}$$

Based on the assumptions, we have:

$$dbf_{EDF}(\Gamma, t_i) \leq sbf_{EDF}(t_i) \tag{15}$$

and,

$$dbf_{EDF}(\Gamma, t') > sbf_{EDF}(t') \tag{16}$$

From formula (13) and formula (15), we have

$$sbf_{EDF}(t') \geq sbf_{EDF}(t_i) \geq dbf_{EDF}(\Gamma, t_i) \tag{17}$$

Since demand bound function $dbf_{EDF}(\Gamma, t)$ is a step function and the value is only changed at $t \in \Omega$, we have

$$dbf_{EDF}(\Gamma, t') = dbf_{EDF}(\Gamma, t_i) \tag{18}$$

 ISBN: 978-1-61208-365-0

From (17) and (18), we have

$$sbf_{EDF}(t') \geq dbf_{EDF}(\Gamma, t') \tag{19}$$

which contradicts the assumption of (15).

Now, we prove (6) $\to$ (11). This proof is straightforward. Since $\Omega \subseteq [0, LCM_\Gamma]$, (6) $\to$ (11) holds. ■

2) Schedulability Test under RM:

Lemma 9: Given a task set $\Gamma = \{\tau_1, ..., \tau_n\}$ and a periodic resource R, the task set is schedulable under RM if and only if

$$\forall \tau_i \in \Gamma, \exists t_0 \in \Omega_i : dbf_{RM}(\Gamma, t_0, \tau_i) \leq sbf_R(t_0) \tag{20}$$

Ω_i is a time point set defined in (21):

$$\Omega_i = \bigcup_{\forall \tau_k \in \text{HP}(\tau_i)} \Phi_{\tau_k}, \Phi_{\tau_k} = \{1, 2, ..., \lfloor (p_i/p_k) \rfloor\} \tag{21}$$

where $\texttt{HP}(\tau_i)$ is a task set which contains the tasks has higher priority than τ_i under RM scheduling policy.

Proof: We prove this Lemma by proving (7) $\leftrightarrow$ (20).

We first prove (7) $\to$ (20).

According to the definition of demand bound function $dbf_{RM}(\Gamma, t, \tau_i)$, i.e. formula (8), it is a staircase function and only rises at the time instants $t^* + \epsilon$, where $t^* \in \Omega_i$ and ϵ is very small and could be closed to 0. In addition, the supply bound function $sbf_R(t)$ is non-decreasing, hence, we have:

$$\begin{aligned}\exists t_0 \in \Omega_i : & dbf_{RM}(\Gamma, t_0, \tau_i) - sbf_R(t_0) \\ & = \min\{dbf_{RM}(\Gamma, t, \tau_i) - sbf_R(t) | 0 \leq t \leq p_i\}\end{aligned}$$

Hence, if

$$\exists t_i \in [0, p_i] : \quad dbf_{RM}(\Gamma, t_i, \tau_i) \leq sbf_R(t_i)$$

then

$$dbf_{RM}(\Gamma, t_0, \tau_i) - sbf_R(t_0) \leq dbf_{RM}(\Gamma, t_i, \tau_i) - sbf_R(t_i) \leq 0$$

therefore, we have:

$$\exists t_0 \in \Omega_i : dbf_{RM}(\Gamma, t_0, \tau_i) \leq sbf_R(t_0)$$

We now prove (20) $\to$ (7).

This proof is straightforward, since $\Omega_i \subseteq [0, p_i]$, formula (20) $\to$ (7) holds.

■

VI. EXPERIMENTS

In this section, we empirically study the behaviors of periodic resources integration.

The first experiment illustrates how the capacity of integrated periodic resource varies under different periodic resource set. In order to observe the variation of integrated periodic resource, we integrate two periodic resources (R_1, R_2) under different scenarios. For each periodic resource, we set nine different capacities ranging from 0.1 to 0.9. Hence, we have total 81 combinations for two periodic resources under different capacities. For each combination, we randomly generate 100 pair of periodic resources which do not have fixed patterns. Fig. 2 shows the variations of average integrated periodic resource capacity. X-axis represents the capacity of periodic resource R_2 and Y-axis represents the capacity of the integrated periodic resource. Each curve represents the variation of the capacity of integrated periodic resource that integrated by a fixed capacity periodic resource R_1 and R_2 which has changing capacity.

As indicated by Fig. 2, in general, the integrated resource has larger the capacity than each of composing periodic resource. However, integration of periodic resources with different capacities have different impact on the capacity of integrated periodic resource. For instance, two periodic resources with both capacities equal to 0.1 produce a integrated periodic resource with capacity 0.19, which is almost equal to the summation of the two individual resources. However, two periodic resources with both capacities equal to 0.9 produce a integrated periodic resource with capacity 0.99. About 90% of the periodic resource's capacity is wasted. This observation brings an interesting question: what type of period resources shall be integrated together to result in the most benefit?

To get an insight about the question, we first need to understand what is the benefit. We first define "benefit" as capacity increase ratio ρ as:

$$\rho(I(R_1, R_2)) = \frac{C(I(R_1, R_2)) - \max(C(R_1), C(R_2))}{\max(C(R_1), C(R_2))} \tag{22}$$

Fig. 3 depicts the integrated periodic resources' capacity increase ratio. There is a interesting observation that if one periodic resource integrates with another one that has the same capacity, the integrated periodic resource always has the highest capacity increase ratio. Furthermore, the closer the two periodic resources' capacities are, the higher the increase ratio.

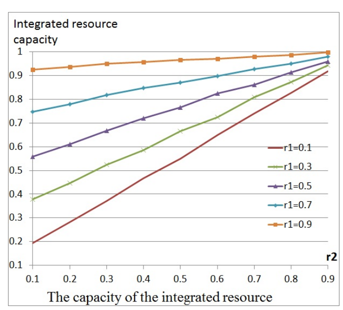


Fig. 2. Integrated Resource Capacity

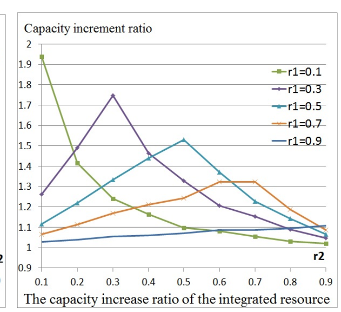


Fig. 3. Capacity Increase Ratio

From the previous observations, it is not difficult to see that the integration causes waste of periodic resources' capacities. Hence, we are also interested in knowing how integration causes waste. We measure waste as the overhead of an integration, which is defined as:

$$O(I(R_1, R_2)) = \frac{(C(R_1) + C(R_2)) - C(I(R_1, R_2))}{C(R_1) + C(R_2)} \tag{23}$$

Fig. 4 depicts the overhead. It clearly indicates that integrating small capacity periodic resource has lower waste ratio compared with resources with large capacities. Hence, we should avoid integrating large capacity periodic resources.

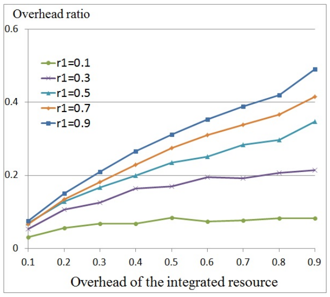


Fig. 4. Integration Overhead

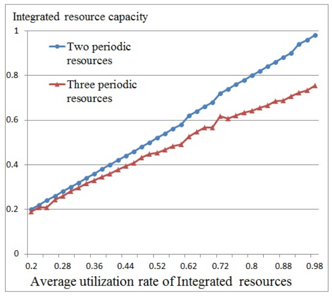


Fig. 5. Resource Number Influence

Till now, our experiments are mainly focusing on integrating two periodic resources. Next, we investigate the properties of periodic resource integration by integrating more than two resources. In this set of experiments, we fix the periodic resource set's total capacity, and then change the number of periodic resources. For each number, we randomly distribute the resource set's total capacity to each periodic resource. For each periodic resource set's total utilization and each number of periodic resources in the resource set, we repeat the experiment 50 times. Fig. 5 shows the average value of the results. The X-axis represents the total capacity for each periodic resource set and Y-axis represents the capacity of integrated periodic resource.

As shown in Fig. 5, the resource integrated by two periodic resources has higher capacity compared with the resource integrated by three periodic resources. This is because the overlap situation between periodic resources happens more frequent when the number of periodic resources increases and hence makes the overhead larger.

VII. Conclusion and Future Work

In this paper, we addressed the issue of scheduling a periodic task set on multiple periodic resources. We first transformed a set of periodic resources into an equivalent single periodic resources and then applied extended schedulability test of multiple tasks on this single resource. We also investigated the properties of periodic resource integration and provide theoretic analysis for the integrated periodic resource capacity. In addition, we extended the existing schedulability test for periodic tasks on single periodic resource from continuous time domain to discrete time domain. We further experimentally studied the behavior and performance of periodic resource integration and pointed out some interesting observations: 1) increasing of the number of periodic resources does not necessarily increase the integrated resource's capability; 2) integrating small capacity periodic resources gains more benefit compared to the integrating large capacity ones; and 3) integration of two periodic resources that have same capacities can maximize benefit.

Our future work is to take the task migration overhead into consideration and implement the proposed algorithm on the real virtualization platform, such as XEN, to utilize the resources of different virtual machines.

Acknowledgement

The research is supported in part by NSF under grant number CAREER 0746643 and CNS 1018731.

References

[1] I. Shin and I. Lee, “Compositional real-time scheduling framework with periodic model,” vol. 7, no. 3. ACM, 2008, pp. 30–62.
[2] S. Shirero, M. Takashi, and H. Kei, “On the schedulability conditions on partial time slots,” in Real-Time Computing Systems and Applications, 1999. RTCSA'99. Sixth International Conference on. IEEE, 1999, pp. 166–173.
[3] A.K. Mok and X. Alex, “Towards compositionality in real-time resource partitioning based on regularity bounds,” in Real-Time Systems Symposium, 2001.(RTSS 2001). Proceedings. 22nd IEEE. IEEE, 2001, pp. 129–138.
[4] A.K. Mok , X. Feng, and D. Chen, “Resource partition for real-time systems,” in Real-Time Technology and Applications Symposium, 2001. Proceedings. Seventh IEEE. IEEE, 2001, pp. 75–84.
[5] Y. Li, A. Cheng, and A.K. Mok, “Regularity-based partitioning of uniform resources in real-time systems,” in Embedded and Real-Time Computing Systems and Applications (RTCSA), 2012 IEEE 18th International Conference on. IEEE, 2012, pp. 368–377.
[6] J. Lee et al., “Realizing compositional scheduling through virtualization,” in Real-Time and Embedded Technology and Applications Symposium (RTAS), 2012 IEEE 18th. IEEE, 2012, pp. 13–22.
[7] W. Chu, “A study of asynchronous time division multiplexing for time-sharing computer systems,” in Proceedings of the November 18-20, 1969, fall joint computer conference. ACM, 1969, pp. 669–678.
[8] N. Fisher and F. Dewan, “Approximate bandwidth allocation for compositional real-time systems,” in Real-Time Systems, 2009. ECRTS'09. 21st Euromicro Conference on. IEEE, 2009, pp. 87–96.
[9] F. Dewan and N. Fisher, “Approximate bandwidth allocation for fixed-priority-scheduled periodic resources,” in Real-Time and Embedded Technology and Applications Symposium (RTAS), 2010 16th IEEE. IEEE, 2010, pp. 247–256.
[10] I. Shin and I. Lee, “Periodic resource model for compositional real-time guarantees,” in Real-Time Systems Symposium, 2003. RTSS 2003. 24th IEEE. IEEE, 2003, pp. 2–13.
[11] S. Baruah, J. Goossens, and G. Lipari, “Implementing constant-bandwidth servers upon multiprocessor platforms,” in Real-Time and Embedded Technology and Applications Symposium, 2002. Proceedings. Eighth IEEE, 2002, pp. 154–163.
[12] B. Sprunt, L. Sha, and J. Lehoczky, “Aperiodic task scheduling for hard-real-time systems,” Real-Time Systems, vol. 1, no. 1, 1989, pp. 27–60.
[13] J.K. Strosnider, J.P. Lehoczky, and L. Sha, “The deferrable server algorithm for enhanced aperiodic responsiveness in hard real-time environments,” Computers, IEEE Transactions on, vol. 44, no. 1, Jan 1995, pp. 73–91.
[14] L. Sha, J. P. Lehoczky, and R. Rajkumar, “Solutions for some practical problems in prioritized preemptive scheduling.” in RTSS, 1986, pp. 181–191.
[15] X. Feng and A.K. Mok, “A model of hierarchical real-time virtual resources,” in Real-Time Systems Symposium, 2002. RTSS 2002. 23rd IEEE. IEEE, 2002, pp. 26–35.
[16] X. Hua, Z. Li, H. Wu and S. Ren, “Tech report: Scheduling periodic tasks on multiple periodic resources,” in http://gauss.cs.iit.edu/~code/techreports/PeriodicIntegration.pdf. IIT, 2014.
[17] I. Shin and I. Lee, “Compositional real-time scheduling framework,” in Real-Time Systems Symposium, 2004. Proceedings. 25th IEEE International, 2004, pp. 57–67.

P2P4GS: A Specification for Services Management in Peer-to-Peer Grids

Bassirou Gueye and Ibrahima Niang
Département de Mathématiques et d'Informatique
Université Cheikh Anta Diop
Dakar, Senegal
Email: {bassirou.gueye, ibrahima1.niang}@ucad.edu.sn

Olivier Flauzac and Cyril Rabat
CReSTIC, UFR Sciences Exactes et Naturelles
Université de Reims Champagne Ardenne
Reims, France
Email: {olivier.flauzac, cyril.rabat}@univ-reims.fr

***Abstract*—The grid-based peer-to-peer architectures were used either for storage, data sharing and computing. So far, the proposed solutions of grid services are generally based on hierarchical topologies, which present a high degree of centralization. The main issue of this centralization is the unified management of resources. Therefore, it is difficult to react rapidly against failures that can affect end-users. In this paper, we propose an original specification, called P2P4GS, that enables self-managed services in peer-to-peer grids. The objective is to design a self-adaptive solution allowing services deployment and invocation based on the paradigm of peer-to-peer services. These tasks are completely delegated to the platform and are achieved through a transparent manner to the end-user. The proposed specification is not linked to a fixed peer-to-peer architecture or to a services management protocol. Furthermore, we propose a detailed illustration of our P2P4GS specification.**

Keywords-Peer-to-peer network; Grid computing; Web Services; Information Systems.

I. INTRODUCTION

Grid Computing is a technology which aims to offer to virtual organizations and scientific community virtually unlimited computing resources [1][2]. The goal of such a paradigm is to enable to virtual organizations (VO) the federated resource sharing in dynamic and distributed environments. Indeed, end-users can access large computing and storage resources that they could not operate otherwise.

The emergence of Web Services [3] provided a framework that initiated its alignment with the grid computing technologies as well as cloud computing [4]. These convergences allowed the appearance, on one hand, of grid services [5][6] and on the other hand, of cloud services [7][8].

Indeed, grid services are the result of research established by the OGF (*Open Grid Forum*) and leading to the OGSA (*Open Grid Service Architecture*) [5] and the OGSI (*Open Grid Service Infrastructure*) [6]. These grid services enable to use resources more rationally. This is due to leveraging load-balancing mechanism between nodes. A particular effort was made in order to normalise the grids services. Like Web Services, the goal is to gather resources in order to promote the development of applications that use grid based services.

Notwithstanding, grids that use the concept of services are generally based on highly centralized hierarchical architectures [2][9]. This centralization involves an unified management of resources as well as a difficulty to react promptly against failures and faults that affect the community (the community designates the set of nodes of the grid).

To overcome these drawbacks, convergence solutions of grid computing and peer-to-peer systems have been proposed [10][11][12][13]. However, a semantics of the services execution chain does not exist in the literature. Most of proposed solutions around peer-to-peer grids are limited on resource discovery and are generally distinguished by the type of search algorithm used.

The main goal of this paper is to present a new specification of services management in a grid computing based on peer-to-peer architecture. This specification, called P2P4GS (*Peer-To-Peer For Grid Services*), presents the originality to not dissociate the peer-to-peer infrastructure to the service management platform. Indeed, we propose to separate the peer-to-peer grid management layer to the location and runtime services layer. Since the proposed specification is generic, any combination of peer-to-peer protocol in accordance with the constraints of our model could be composed with any services execution platform. Deployment as well as invocation is absolutely delegated to the platform. Consequently, both tasks become transparent to the end-user. In fact, the end-user can be a simple user who has no knowledge of the system (a student or a researcher for instance) or an administrator of grid services.

The remainder of the paper is organized as follows. Firstly, Section II is devoted to present an overview on the related work. Next, in Section III, we describe the model that we use, as well as different aspects of the P2P4GS specification. Subsequently, we propose a detailed illustration of our specification in Section IV. Finally, Section V concludes the paper and outlines our future works.

II. RELATED WORK

The remote code execution has been defined in various manners. The possibility to remotely call a procedure led to the concept of RPC (*Remote Procedure Call*). RPC specification specifies how information is exchanged between a

 ISBN: 978-1-61208-365-0

consumer (client) and a resource (server). Different implementations that consider different languages, protocols and systems have been proposed. For instance, we can cite the following implementations based on Web Services: XML-RPC, SOAP [3]. RPC concept has been transferred in the grid either from libraries that enable technical solutions, like Globus [14], or directly from the solutions that are designed to ensure grid RPC. However, the proposed solutions are hierarchical and need centralization points that gather the related information to a given service. For example, tools such as DIET [9] should register their requirements (e.g., computational or memory resource, data resource, applications, etc.) on a fixed centralization point.

In addition, in the case of Web Service execution on the Internet, solutions of deployment [6] and resource discovery [15][16] in such environments have been proposed. In fact, the authors of [15] proposed a hierarchical topology of web services for resource discovery in Grids based on Globus Toolkit. In this proposed solution, the Grid system is divided into virtual organizations (VO). On the other hand, Fouad et al. [16] presented scalable Grid resource discovery through a distributed search. The proposed model includes the application layer which provides a web interface for the user and the collective layer which is a web service to discover resources. The resource discovery model contains the metadata and resource finder web services to provide a scalable solution for information administrative requirements when the grid system expands over the Internet.

Nevertheless, these works are based on solutions with hierarchical architectures that have a very low degree of dynamicity and whose infrastructural services are themselves centralized. Indeed, these centralized or hierarchical approaches suffer from a single point of failure, of bottlenecks in highly dynamic systems, and lack of scalability in highly distributed environments [17].

Fortunately, grid and P2P systems share several features and can profitably be integrated. Convergence of the grid system with the philosophy and techniques of the P2P architecture is a promising approach to alleviate the disadvantages of traditional grid systems. Torkestani [18] asserted that P2P Grids exploit the synergy between the Grid system and peer-to-peer network to efficiently manage the Grid resources and services in large-scale distributed environments. The decentralized approach can enhance scalability and fault-tolerance but it induces a very large network traffic and may limit search effectiveness. In addition, Marin Perez et al. [19] argue that the ultimate goal of building P2P Grid is to integrate the P2P, Grid, and Web Services.

However, most of proposed solutions with respect to peer-to-peer grids are limited to the resource discovery [10][11][12][13][18] and are generally distinguished by the type of search algorithm used. The authors of the survey [20] argue that the resource discovery (which aims to discover appropriate resources based on a requested task) is one of the essential challenges in Grid. There are certain factors that make the resource discovery problem difficult to solve. For instance, Torkestani [13] proposed a multi-attribute distributed learning automata-based resource discovery algorithm for large-scale peer-to-peer grids. Based on the learning automata theory, the author proposed a method that enables to route the resource query through the path having the minimum expected hop count toward the grid peers including the requested resources.

III. Overview of the P2P4GS specification

Initially, we defined the concepts related to the various components of our systems. Then, in order to present our specification, we describe the application model.

A. Preliminaries

1) Node concept: a node is a machine (with acceptable computational power) or a site (cluster). We assume that each node has a unique identifier in the communication network. Nodes are in charge of the local management of the network. Therefore, they collectively provide the tasks described in Section III-B. Moreover, they manage the execution platform, which ensures the following tasks: the deployment, the life cycle of services, the management of requests and their executions. In addition, each node maintains a table called "*Service Registry*", which lists the services owned by this node, as well as the other services located inside the grid and learn during a discovery process.

2) Service concept: the services can be viewed as different objects that are integrated to the runtime platforms located in each node. A service is characterized by:

- the implementation platform;
- the required resources for its execution (computational power, data resource and connection resource, etc.);
- the format and constraints according to the requested invocation and obtained results.

B. Modelization

We define an architecture model composed of four layers. This enables us to define each layer independently. Indeed, with this model, each layer solves a number of problems (handles a number of tasks required by the overall system), in order to provide well-defined services to the higher layers. Figure 1 illustrates the architecture of our specification. In the following, we describe the different layers of the architecture.

1) Physical layer: this layer provides addressing, routing and communication functions. We are modeling this layer as a directed and connected graph $G_1 = (V, E_1)$ where V is the set of nodes that host the services and E_1 the set of directed communications links between the nodes.

These definitions allow taking into account the different characteristics of the network:

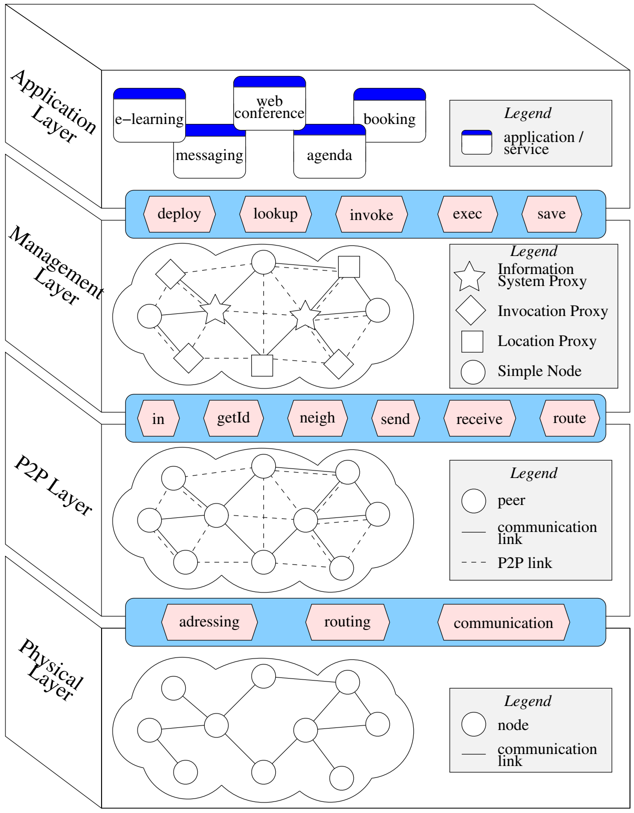


Figure 1: Architecture of P2P4GS specification

- security elements such as firewalls that restrict the possibility of communication of the nodes;
- configuration and implementation elements of the network such as the NAT.

2) P2P layer: it corresponds to the peer-to-peer middleware and provides communication functionalities and maintenance of the topology. P2P layer is modeled as an undirected and connected graph $G_2 = (V, E_2)$ where V corresponds to the set of nodes that hosting the services and E_1 the set of undirected communications links between the nodes established by the P2P protocol.

We assume that this layer offers at the minimum the following primitives :

- **in()** : this primitive is executed by a new node that is connected to the P2P community;
- **getId()** : returns the P2P node's identifier;
- **neigh()** : retrieves the list of all its P2P neighbors;
- **send(id, message)** : sends a message to a node identified by "id" in the system;
- **receive()** : receives a message from a node of the system;
- **route(id, message)** : routes a message to a destination.

Therefore, any peer-to-peer system presenting these basic features can be exploited by our specification.

3) Management layer: this layer constitutes the core of our specification. All tasks of management, administration and maintenance of a service are defined in this layer. These tasks ensure the management of life cycle of a given service. Indeed, P2P4GS specification provides a set of primitives that are "*deploy*", "*lookup*", "*invoke*", "*exec*" and "*save*" for respectively deployment, location, invocation, execution and recording of a service. These primitives are described in Section III-C.

Given that the size of distributed systems grows in terms of number of nodes, services and users, in order to ensure scalability, we propose to limit the knowledge on some nodes that we call *proxies*. In fact, we define three types of proxies: the ISP *(Information System Proxy)*, the IP *(Invocation Proxy)* and the LP *(Location Proxy)* for effectively ensure function of the primitives above mentioned. According to the P2P paradigm, the status of the nodes is not fixed and can evolve during execution. Note that, the default node status is *Simple Node*. The different proxy nodes are described in Section III-D.

4) Application layer: this layer is the upper layer that interfaces with the end-users. Primitives of the underlying layer are exploited by different platforms with whom they interact in order to provide services to Application layer.
Note that, the access to P2P grid resources will be done in a transparent manner with respect to the end-user.

C. Services specification in P2P environment

In this section, we define the set of primitives and specific operations to the services runtime on our P2P grid system.

1) Service deployment ("deploy"): the service deployment requires the detection of nodes that are able to host and execute a given service. A subset of nodes of the community will be candidates for hosting the service. The following strategies can be used in order to select the node that hosts the service among the candidate nodes:

1) a *random strategy* based on a random selection of a node where the service will be deployed on;
2) a *balanced strategy* based on statistic data gathering about nodes, and selection of the less loaded nodes where the service can be deployed on;
3) a *first node strategy* based on exploration: the first node able to support the service is selected.

Remark 1. *The first strategy needs to know all candidate nodes for deployment; the second one to know all candidate nodes and information on each; the third limits the required knowledge and also reduces the communications costs but can cause problems of load-balancing.*

2) Service location ("lookup"): the service location is the first step of a service execution process. Each node of the peer-to-peer grid has a table called *Service Registry* that stores node's identifier of the grid according to their signatures. "*lookup*" can be considered as a local service.

 ISBN: 978-1-61208-365-0

Indeed, it is available on each node of the community, but cannot be invoked from a remote machine.

Any node of the P2P4GS community that receives a service location request, invokes the "*lookup*" function which performs the following operations:

- if the service is located on the node, this latter returns its identifier and information about the service (e.g., binding, invocation constraints, ...);
- if the service is not located on the node, then :
  - if the node knows the location of service, it routes the request to the node that hosts it;
  - if the node does not know the location of service, it forwards the request to its neighbors.

Remark 2. *The required service may be missing within the grid, whether due to a failure, otherwise because it has not been yet deployed. In this case, we can use an algorithm like PIF (Propagation of Information and Feedback), which returns to the entry point (III-C3) an error code that will be sent to the sender of the request.*

3) Service invocation ("invoke"): the invocation of a given service can be achieved from any node of the community. In the case where an outside node of community wishes to invoke a given service, it passes through a node of the community which becomes "entry point" and thus its "*invocation point*". This entry point is in charge of making the invocation of the service, retrieves the result and returns it to the request source.

Remark 3. *A node "entry point" is a node from which an end-user logs in to access the community. In fact, the system provides to the end-user a kind of black box in which all tasks will be done in a transparent manner. Note that any node of the community can serve as an "entry point".*

4) Service execution ("exec"): once the request has reached the node that keeps the service, it is executed. The first step is to identify the required invocation parameters for the execution. The execution can either produce the result, or trigger an error. Once the result has been produced, it is routed to the "invocation point".

5) Service recording ("save"): it is possible to exploit the platform through research without memory of services on each invocation. As we stated previously, we can increase the performance of our platform with distributed service registries. We plan the construction of these registries according to two main strategies:

- *Flooding deployment*: in this first strategy, the diffusion of the information on the service location will be achieved according to a flooding approach.
- *Broadcast-based on response invocation*: in this second strategy, the location information will be broadcast after the response of the invocation. Each node that relays the response towards the invocation point will store the information on the service location.

Remark 4. *In order to avoid a node overloading-memory by the service register, it is possible to aggregate information on several consecutive nodes.*

D. Specification of the node proxy concept

As our specification is not related to a particular peer-to-peer architecture, we propose an organizational model of nodes in the system which tends to limit the knowledge on some nodes called proxies in order to avoid an overloading-memory of the community nodes. In fact, we propose to limit knowledge about the location on some nodes in the system (as well as their list of services) on nodes we call ISP *(Information System Proxy)*.

An ISP acts as an information system for a set of nodes. Consequently, it knows the location of a certain number of services in the community.

In order to limit the ISP overload, we delegate invocation and execution services tasks for nodes called IP *(Invocation Proxy)*. Moreover, services have not the same execution constraints in terms of CPU, RAM, execution platform, etc., Thus, a node is defined as IP for a given service, if it knows its location and respects its implementation constraints. Therefore, IP node owns the client part of this service (stub).

A node having only a knowledge about the location of a given service but not having its stub will be called LP *(Location Proxy)* for this service.

It should be noted that a node is both invocation proxy and location proxy for its own services.

Remark 5. *In order to avoid the overload of the memory of the ISP, IP and LP nodes, we propose to remove the knowledge about a given service at the end of a TTL (Time-To-Live). Accordingly, a service that is rarely requested will not be stored indefinitely. In contrast, a node will be always an invocation proxy for a service frequently requested of the fact that its TTL will be reset after each new invocation. In the case of the ISP nodes, this TTL is only applicable on services known through other ISP nodes.*

IV. Management of the P2P4GS community nodes

In this section, we describe a detailed illustration of our specification. We firstly present the creation process of the P2P4GS community. Afterwards, we describe the location and deployment processes of a given service in this community.

A. Organization of the P2P4GS community

Given that nodes of a grid present minimum capacities in terms of CPU, memory and bandwidth, any node can potentially become ISP. Thus, no election of ISP node is necessary. Moreover, in a large-scale environment where nodes are geographically dispersed, the network does not formed spontaneously. Therefore, using the concept of direct neighborhood, we propose a progressive ISP election

 ISBN: 978-1-61208-365-0

according to node's connection. We assume that direct neighborhood of a node is established upon first connection and can evolve during execution.

We define the concept of direct neighborhood as follows: for any pair of nodes (u, v) of the P2P4SG community, u and v are direct neighbors if and only if:

- u can communicate with v and *vice-versa*. This means that there exists a bidirectional communication link between u and v;
- u knows v in its list of neighbors and vice-versa.

The following steps describe the process creation of P2P4GS community:

- The first node connected to the system (then it does not have any neighbors), elects itself as ISP ;
- Any new node that connects to the system checks its neighborhood table:
  - If it has at least one ISP as neighbor then it keeps its status (simple node). Moreover, if it has hosted services, it sends information on services to its ISP that will update their *Service Registry* ;
  - Otherwise, it elects itself as ISP and informs its neighbors.

B. Elasticity management in the P2P4GS community

As large scale systems can be highly dynamic, disconnection of a node can occur at any time. In order to ensure scalability, it is necessary to take into account the disconnection of the nodes. Thus, according to the disconnected node's status, we propose these following approaches.

- Disconnection of a simple node: in this case, its services become unavailable. As noted in Remark 5, if a service remains unavailable until end of the TTL, its knowledge will be deleted at the different service registries having recorded it.
- Disconnection of a LP node: in this case, source node will start a new process of discovery if it does not know another LP for desired service.
- Disconnection of an IP node: same treatment as the case of a disconnected LP.
- Disconnection of an ISP node: in this case, one of the following events occurs:
  - In the case of the service location, processing remains the same as those IP or LP node;
  - In the case of the service deployment, if candidate node has other ISP neighbors, it sends services information to its ISP neighbors that will update their *Service Registry*. Otherwise, it elects itself as ISP and informs its neighbors.

C. Location and deployment process in the P2P4GS community

In this section, we first describe the service location process by using the example shown in Figure 2. Subsequently, we explain the deployment process.

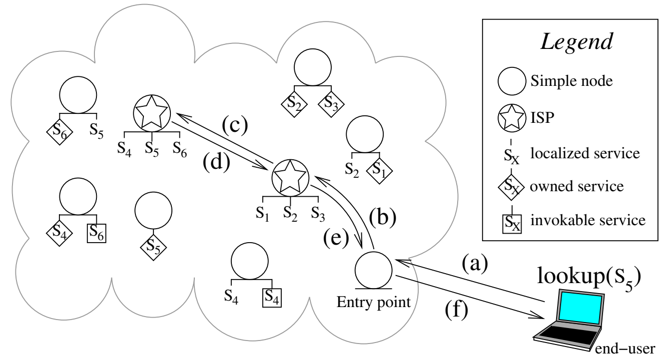


Figure 2: Example of location process in P2P4GS community

In this example, the *end-user* is connected to its *entry point* and the requested service is named S_5 (a). If the *entry point* knows the location of the requested service, it directly responds to the *end-user* by sending the corresponding service address. Else, if the node does not know the location of the service, it forwards the request to its ISP neighbors (b).

Any ISP that receives the location request consults its registry and performs a following tasks:

- if the service is registered, it responds to the source node by sending the corresponding service address;
- otherwise, we propose two strategies in order to explore others node's community:
  - construction of a structured overlay formed by ISP;
  - utilization of a wave algorithm such as the PIF for example.

The first strategy allows ISP nodes to communicate to each other in order to facilitate the processing of location request. However, this method induces costs for maintaining the overlay. The second limits the necessary knowledge therefore it is simpler to implement. However, it presents a non-negligible communication cost.

In this example, we have used the structured overlay formed by ISP nodes (c). According to the used approach, if the service is found, the response takes the opposite path of the location request. By using the "*save*" primitive, all intermediate ISP and the *entry point* node will update their service registry (d, e, f). Note that, as we have showed in Remark 5, a TTL is applied on this knowledge.

In the case of the deployment of a new service within the community, one of the strategies (random, balanced or first node) proposed in Section IV.C.1 can be applied. Note that for these strategies, the election process of node candidate keeps typically the same approach as for the location of service. The request will be based on the execution constraints (CPU, memory resource, execution platform, etc.) of the service to be deployed. Once the deployment is successfully completed, the candidate node sends to its ISP neighbors the information on the new hosted service.

 ISBN: 978-1-61208-365-0

V. Conclusion and future work

In this paper, we proposed an original specification of a "self-managed service in peer-to-peer grid" named P2P4GS. This specification is generic, not linked to a fixed peer-to-peer architecture or a given services management protocol. Given that the size of distributed systems grows in terms of number of nodes, services and users, we have proposed to limit the knowledge on some nodes that we have called *proxies*, in order to ensure scalability. After having described our model, as well as different aspects of the P2P4GS specification, we have presented a detailed illustration of this specification.

Currently, we are working on the validation of our specification under *Oversim framework* based on *OMNeT++* simulator in order to evaluate: service's deployment and location in each strategy, communication cost in terms of messages and fault tolerance mechanisms.

As future work, we plan to implement and compare our specification with other existing solutions.

References

[1] I. Foster and A. Iamnitchi, "On death, taxes, and the convergence of peer-to-peer and grid computing," in *Peer-to-Peer Systems II*. Springer, 2003, pp. 118–128.

[2] I. Foster, C. Kesselman, and S. Tuecke, "The anatomy of the grid: Enabling scalable virtual organizations," *International journal of high performance computing applications*, vol. 15, no. 3, pp. 200–222, 2001.

[3] G. Alonso, F. Casati, H. Kuno, and V. Machiraju, *Web services - Concepts, Architectures and Applications*. Springer Verlag, ISBN 3-540-44008-9, chapter 5, 2004.

[4] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica *et al.*, "A view of cloud computing," *Communications of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[5] I. Foster, H. Kishimoto, A. Savva, D. Berry, A. Djaoui, A. Grimshaw, B. Horn, F. Maciel, F. Siebenlist, R. Subramaniam *et al.*, "The open grid services architecture (ogsa), version 1.5." OGF Specification GFD-I. 080, July 2006.

[6] S. Tuecke, K. Czajkowski, I. Foster, J. Frey, S. Graham, C. Kesselman, T. Maquire, T. Sandholm, D. Snelling, and P. Vanderbilt, "Open grid services infrastructure (ogsi), version 1.0," June 2003.

[7] S. Bhardwaj, L. Jain, and S. Jain, "Cloud computing: A study of infrastructure as a service (iaas)," *International Journal of engineering and information Technology*, vol. 2, no. 1, pp. 60–63, 2010.

[8] K. R. Jackson, L. Ramakrishnan, K. Muriki, S. Canon, S. Cholia, J. Shalf, H. J. Wasserman, and N. J. Wright, "Performance analysis of high performance computing applications on the amazon web services cloud," in *IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom)*, 2010, pp. 159–168.

[9] E. Caron and F. Desprez, "Diet: A scalable toolbox to build network enabled servers on the grid," *International Journal of High Performance Computing Applications*, vol. 20, no. 3, pp. 335–352, 2006.

[10] P. Trunfio, D. Talia, H. Papadakis, P. Fragopoulou, M. Mordacchini, M. Pennanen, K. Popov, V. Vlassov, and S. Haridi, "Peer-to-peer resource discovery in grids: Models and systems," *Future Generation Computer Systems*, vol. 23, no. 7, pp. 864–878, 2007.

[11] T. Kocak and D. Lacks, "Design and analysis of a distributed grid resource discovery protocol," *Cluster Computing*, vol. 15, no. 1, pp. 37–52, 2012.

[12] D. Chen, G. Chang, X. Zheng, D. Sun, J. Li, and X. Wang, "A novel p2p based grid resource discovery model," *Journal of Networks*, vol. 6, no. 10, pp. 1390–1397, 2011.

[13] J. A. Torkestani, "A multi-attribute resource discovery algorithm for peer-to-peer grids," *Applied Artificial Intelligence*, vol. 27, no. 7, pp. 575–598, 2013.

[14] I. Foster, "Globus toolkit version 4: Software for service-oriented systems," *Journal of computer science and technology*, vol. 21, no. 4, pp. 513–520, 2006.

[15] T. Gomes Ramos and A. C. M. A. de Melo, "An extensible resource discovery mechanism for grid computing environments," in *Cluster Computing and the Grid, 2006. CCGRID 06. Sixth IEEE International Symposium on*, vol. 1. IEEE, 2006, pp. 115–122.

[16] F. Butt, S. S. Bokhari, A. Abhari, and A. Ferworn, "Scalable grid resource discovery through distributed search," *International Journal of Distributed and Parallel Systems (IJDPS)*, vol. 2, no. 5, pp. 1–19, 2011.

[17] Y. Deng, F. Wang, and A. Ciura, "Ant colony optimization inspired resource discovery in p2p grid systems," *The Journal of Supercomputing*, vol. 49, no. 1, pp. 4–21, 2009.

[18] J. A. Torkestani, "A distributed resource discovery algorithm for p2p grids," *Journal of Network and Computer Applications*, vol. 35, no. 6, pp. 2028–2036, 2012.

[19] J. M. Marin Perez, J. B. Bernabe, J. M. Alcaraz Calero, F. J. Garcia Clemente, G. M. Perez, and A. F. Gomez Skarmeta, "Semantic-based authorization architecture for grid," *Future Generation Computer Systems*, vol. 27, pp. 40–55, 2011.

[20] N. Jafari Navimipour, A. Masoud Rahmani, A. Habibizad Navin, and M. Hosseinzadeh, "Resource discovery mechanisms in grid systems: A survey," *Journal of Network and Computer Applications*, pp. 389–410, 2013.

Benchmarking the Problem of Optimal Autonomous Systems Aggregation on Different Computer Architectures

Leszek Borzemski, Michał Danielak, and Grzegorz Kotowski
Institute of Informatics
Wroclaw University of Technology
Wrocław, Poland
e-mail: {leszek.borzemski, michal.danielak, grzegorz.kotowski}@pwr.edu.pl

***Abstract*—This paper presents and formalizes the problem of optimal Autonomous Systems aggregation in computer network, and shows how this problem can be calculated in a real-life case on two computer architectures: RISC and CISC. On the one hand, the optimal autonomous systems aggregation problem was formulated as an instance of the minimum set cover NP-hard computational problem. On the other hand, the multiplicity of such calculations to be made using massive, distributed and collected in real-time datasets results in challenges of Big Data analysis. Nowadays, RISC based processors have cornered the market of mobile computing solutions, whereas CICSs are dominating in desktop and server computing. But, a new trend in server design, based on RISC system-on-chip processors is deliberated. Therefore we need to consider both processors especially in current computational problems to choice which computer architecture should be used to run the computations. This paper defines the problem of Autonomous Systems aggregation as a set cover problem, gives a brief overview on CISC and RISC architectures, and presents our performance and topology measurements of the Internet as well as our comparison of computational efficiency of both processor architectures with respect to the size of a computation task. We find that the optimal solution of the AS aggregation problem is extremely demanding and time-consuming, especially for the huge number of ASs. Based on the obtained results, we can state that CISC architecture should be chosen to solve the AS aggregation problem.**

Keywords-Autonomous Systems; autonomous systems aggregation; CISC; RISC, performance evaluation; computer network monitoring; Big Data; high performance computing.

I. INTRODUCTION AND MOTIVATION

Nowadays, the Internet has become the main source of any information. One of the key advantages of such information is its almost instantaneous accessibility. Considering the growth of web page complexity level and new technology development, one can observe the constant growth of file sizes that are hosted by web servers (e.g., CD/DVD ISO images, FullHD movies, etc.). As a derivative of size, the obtaining time may of course vary depending on the file. However, it may also vary, considering the same file, depending on the source (this hypothesis is discussed in more detail in Section 5), and the differences in downloading time between sources may extend from minutes to hours. Thus, if the selected web object is mirrored (copied to another location or multiple locations), selection of the suitable source may result in substantial obtaining time reduction. In most cases, web-hosting companies provide a user with a list of their servers located around the world for the manual selection. Such a list usually contains some additional information about the servers such as geographical position or server owner (some companies or organizations mirror their servers mutually), which may help the end-user to manually select the most suitable source. Unfortunately, the choice based on geographical distance or user individual preference is not always the optimal one.

The optimal selection ought to rely on a network structure and its analysis. However, the structure of the Internet is extremely large and immensely complex. Therefore, to simplify the management of such a vast network, it should be divided into smaller parts. One smaller part is called Autonomous System (AS) and it can be described as a set of IP addresses under common administration that has a strictly defined routing schema applied. Each of the Autonomous Systems has its registered and globally unique number (ASN).

A few Interior Gateway Protocols (IGP) are used to transfer data within an autonomous system, while Exterior Gateway Protocols (EGP) such as Border Gateway Protocol (BGP) are generally used to exchange routing information between autonomous systems [1]. What is more, BGP is currently the widely used inter-domain BGP on the Internet.

Exchanging information about network reachability with other systems is the primary function of ASs that use BGP. This information is exchanged between ASs and is kept in BGP tables. Finally, data from BGP tables are sufficient to create a graph that represents connections between autonomous systems [2].

Almost 85 percent of ASs registered around the world (approximately 60 000) are active and providing about 200 000 network subnets. Moreover, the global interconnection number equals almost 120 000 [3].

To make the image clearer, one can make real life analogy and compare the above structure to the example of political geography (see Table I).

At the first glance, the simplest method for analysis of the Internet would be to acquire real-time full characteristics of every single host in every AS. Unfortunately, taking into account only the aforementioned numbers, one can notice that the real time analysis or even the simple monitoring of

 ISBN: 978-1-61208-365-0

so complex a structure, even from one point of view, tends to be virtually impossible. What is more, the computational power and network limits (which have been recently both continuously raising) are usually insufficient, too expensive and/or limited. Therefore, to deal with the whole AS network, its structure has to be somehow simplified so that its complexity would significantly decrease. This can be achieved by conducting two simple steps: the selection of ASs representatives and the AS aggregation. The first step is to choose a group of hosts belonging to a single AS as its representatives, while the other consists in reducing the set of monitored ASs by aggregating (grouping) them into entities called MetaASs. What is more, both steps have to be conducted, because choosing even a few representatives for an AS makes a number of few hundred thousands of hosts to observe in total, so the aggregation process is indispensable.

TABLE I. INTERNET AND WORLD TERMINOLOGY COMPARISON

Network	Real life
Internet	World
Autonomous System	Country
Autonomous System Number	Country name
AS routing map	Country road map
AS interconnections	Border checkpoints between countries
AS subnets	Country administrative division

Moreover, not only does applying such a reduction slightly decrease the global number of monitored ASs and consequently the number of representative hosts, but it also gives a compromising Internet structure; simultaneously, so simplified approach is not deprived of drawbacks – the structure constructed by this process strongly depends on the location of an observation source and corresponds only to a certain point of view, so it cannot be simply applied to another part of the structure.

One might wonder whether the aggregation of so vast number of ASs is justified, especially for parallel aggregation. Research indicate that the average number of ASs that constitute an AS-path, i.e., a sequence of intermediate ASs between the sender and the receiver, is generally lower than twenty. In case of BGP prepending, however, this path is deliberately lengthened and the maximum AS path can reach even 160 ASs. What is more, in case of parallel aggregation which is solved in this paper, use of ASs aggregations seems to be even more justifiable, because all upstream (or downstream) ASs of a given AS must be aggregated. And generally, this number of ASs is quite large: for AS7029, for instance, the number of its downstream servers is 150 [3]. This considerable number of ASs to aggregate results in extremely demanding computational problem. This is why this particular problem solved here an instance of a Big Data analysis, which needs a specific approach to run computations in hybrid computer systems consisting of various Instruction Systems Architectures (ISAs) processing components, to provide required computations effectively; these ISAs can be either Reduced Instruction Set Computing [3] or Complex Instruction Set Computing [3].

The rest of the paper is organized as follows. Section II formulates the problem of optimal autonomous systems aggregation; Section III gives an overview on Reduced Instruction Set Computing and Complex Instruction Set Computing processing computer architectures; Section IV presents the experiments performed in the Internet and discusses the results of computations made to find optimal Autonomous Systems aggregations for four hardware and software configurations and different numbers of ASs on Internet paths. The paper concludes with a brief review of related work in Section V, and a conclusion summarizing our work and presenting future research plans in Section VI.

II. AUTONOMOUS SYSTEMS STRUCTURE REDUCTION

The reduction of the whole AS structure needs to be performed in a few steps.

A. Removal of Transitive Autonomous Systems

The static information about the Autonomous Systems (provided, for instance, by Bates et al. [4]) contains the types that AS can be applied to, i.e., *ORIGIN* (having content), *TRANSIT* (inter-AS communication only) and *ORG+TRN* (hybrid). As we are interested only in web content, the transit part of the network is unnecessary to monitor and may be treated as transparent.

Unfortunately the “transit-only part” does not exceed a few percent of the whole network, so the reduction process has to be more radical.

B. AS Characteristics

The vast number of parameters may be used to characterize a single network node. The most common are response times of the remote host, such as Round Trip Time (RTT), Transfer Control Protocol (TCP) connect time, or HyperText Transfer Protocol (HTTP) response time. These parameters may vary inside AS; so, AS characteristics is usually based on their average values.

Round trip time is based either on Internet Control Message Protocol (ICMP) or User Datagram Protocol (UDP) and it is usually the simplest way of determining the response time of a remote host. Unfortunately, not every host replies to *Echo request* (mostly due to administrative policies) which is essential to obtain the RTT. In problems of Web systems, slightly more useful are *TCP connect time* and *HTTP response time*, because in contrary to RTT they are always available; namely, every web server accepts connections incoming to adequate TCP port. TCP connect time describes the time that is needed for establishing the connection (by using the three-way handshake), whereas the HTTP response time is the time between sending the first bytes of the request, e.g., *GET* (see Section 9.3 in [5]) and receiving the first bytes of the response, e.g., *200 OK* (see Section 10.2.1 in [5]). Yet, the three aforementioned examples of characteristics are rather basic, and one may use more complex (comprising of the basic ones) characteristics.

ISBN: 978-1-61208-365-0

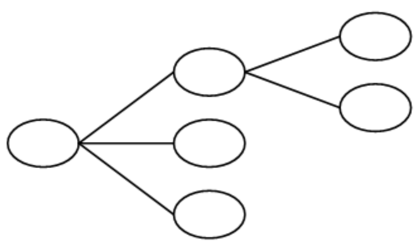
C. Aggregation

The subsequent step consists in achieving a simplified structure of ASs that would allow to monitor and/or analyze ASs in (almost) real-time; this process is called the aggregation. The similarity of two AS paths can be described as the longest path segments these paths share. For example, if the destinations are located 9 AS hops away from the source and the paths towards them are the same through 8 AS hops, it can be said that the paths are very similar. In the terms of the real-life example: if we travel from Warsaw to London or Paris, we have to use mostly the same way through Germany and Belgium. As time and distance are roughly the same we may say that our journey is “the same”.

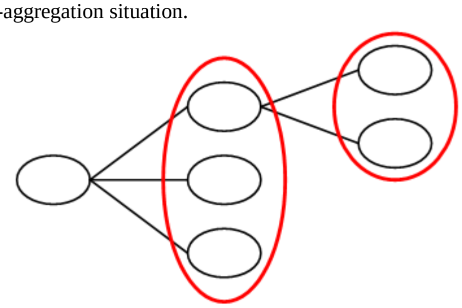
Considering the aforementioned example, two cases of aggregation can be distinguished:

1. Siblings (parallel) grouping – grouping ASs directly upstream adjoined to the same AS (see Figs 1a÷c).
2. Parent-child (serial) grouping – path shortening, grouping ASs that are mutually adjoined (up- and downstream); see Figs. 1 a-c.

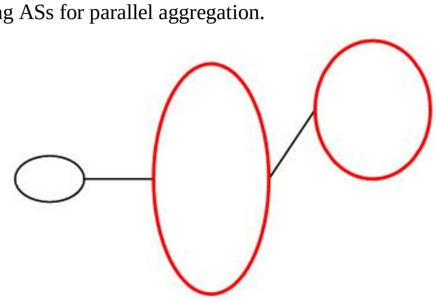
This paper deals only with the first case.



a/ Pre-aggregation situation.



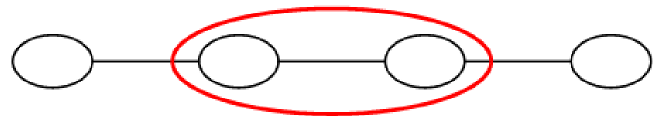
b/ Choosing ASs for parallel aggregation.



c/ Post-aggregation situation.

Figure 1. Siblings grouping.

a/ Pre-aggregation situation.



b/ Choosing ASs for serial aggregation.

c/ Post-aggregation situation.

Figure 2. Serial grouping.

In this work we focus only on the first case – parallel grouping. Let

$$A = \{1,2,\ldots,N\} \tag{1}$$

Be the set of sibling ASNs and

$$A_i \in 2^A \tag{2}$$

be Meta-AS, i.e., a subset of sibling ASNs fulfilling

$$\underset{i \in A_k}{\forall} \left| t(i) - \frac{\sum_{j \in A_k} t(j)}{|A_k|} \right| \le \Delta t \tag{3}$$

where:

$$t : A \to R_+ \tag{4}$$

is the considered performance index (RTT); $t(i)$ is the value of the performance index for i -th AS, whereas Δt is a limiting parameter. In other words, we assume that performance indices for ASs forming a MetaAS cannot deviate from the average by more than Δt. This assures that the aggregated ASs have similar values of performance indices – in the worst case, the difference between the extreme values of these parameters in MetaAS equals to $2\Delta t$.

One can formulate the optimal aggregation problem as follows:

Given (1), (4), find the optimal set of MetaASs C^*:

$$C^* = \arg\min |C| \tag{5}$$

where

$$C \subseteq 2^A \tag{6}$$

such that

$$\bigcup_{A_k \in C} A_k = A \tag{7}$$

$$\underset{A_i \in C, A_j \in C, A_i \neq A_j}{\forall} A_i \cap A_j = \varnothing \tag{8}$$

$$\underset{A_k \in C}{\forall} \underset{i \in A_k}{\forall} \left| t(i) - \tau(k) \right| \leq \Delta t \tag{9}$$

where:

$$\tau(k) = \frac{\sum_{j \in A_k} t(j)}{|A_k|} \tag{10}$$

is the performance index of a Meta-AS. Constraint (7) states that the sum of all MetaASs should give the set of all ASs, while constraint (8) assures that each AS can only belong to one MetaAS. Finally, constraint (8) states that all MetaASs should fulfill (3).

One can notice that the AS aggregation problem (5) – (10) is an instance of the minimum set cover problem, which is NP–hard. The suboptimal solution algorithms of the generic minimum set cover problem are studied in literature, e.g., in [6][7], but they are not applicable as we search the best solution. Therefore, we solve problem (5) – (10) by means of a brute-force (exhaustive search) algorithm that finds the best solution and offers an easy design but is a long-running time approach, unfortunately.

III. PROCESSING COMPUTER STRUCTURES

Reduced Instruction Set Computing (RISC) and Complex Instruction Set Computing (CISC) are two major computer architectures that can be successfully used to solve the optimal aggregation problem. Despite numerous initial differences between them, these two architectures have become somewhat dependent on each other and the proven solutions from first have gradually started to be adapted in the other and vice versa.

In comparisons of RISC and CISC architectures we can compare them either in qualitative or quantitative way [3]; the former examines the issues of high language support and uses the very large scale of integration (by combining thousands of transistors into single chips) in order to create an integrated circuit, while the later compares applications' size and their execution speeds. This work is a quantitative comparison whose main task is to suggest architecture for the most efficient data processing in the problem of optimal aggregation.

Every quantitative comparison of RISC and CISC architectures should take into account two problems: there is no pair of RISC and CISC machines that would be directly comparable in terms of levels of technology, complexity of compilers or cost and it is impossible to define a set of test programs that would unambiguously evaluate the performance of examined machines [8]. Nevertheless, because the aim of this research is to discover the most efficient architecture for the optimal aggregation problem, the latter problem in this paper seems to be inessential.

The subsequent part of this paper compares the initial assumptions made in CISC and RISC architectures and provides a brief outline of two operating systems that have been used on both architectures to find the optimal hardware and software combination for the optimal aggregation problem.

A. Main Differencies

CISCs are defined as the computers with a full set of computer instructions designed to provide needed capabilities in the most efficient way. It was later discovered, however, that by reducing the aforementioned full sets of instructions to those most frequently used, computers would be able to get more tasks done in a shorter amount of time. This reduced approach was defined as RISC. Table II presents the short comparison of those two architectures.

TABLE II. A BRIEF COMPARISON OF RISC AND CISC ARCHITECTURES IN TERMS OF THEIR INITIAL ASSUMPTIONS; SOURCE [9].

CISC	RISC
Primary goal is to complete a task in as few lines of assembly as possible	Primary goal is to speedup individual instruction
Emphasis on hardware	Emphasis on software
Includes multi-clock complex instructions	Single-clock, reduced instruction only
Memory-to-memory: "LOAD" and "STORE" Incorporated in instructions	Register to register: "LOAD" and "STORE" are Independent instructions
Small code size	Large code sizes
Variable length Instructions	Equal length instructions which make pipelining possible

B. IBM AIX and Red Hat Enterprise Linux on RISC and CISC Architectures

Both studied processing structures support Linux operating system which should also be considered in the choice of computing platform. What is more, one should compare all the features and characteristics of evaluated operating systems in order to choose 'the best' operating system. Naturally, this task is virtually impossible to tackle. Nevertheless, this section tries to briefly characterize a few differences between two systems that have been used in this research: Red Hat Enterprise Linux (RHEL), a commercial Linux distribution developed by Red Hat, Inc., and IBM Advanced Interactive eXecutive (AIX).

The first major difference between evaluated operating systems is their availability; namely, RHEL have been ubiquitous and widely used by various business entities in the recent years, while AIX have been used only by these who have chosen IBM's POWER-based IT solutions. Not only can RHEL run on computers with IA-32, IA-64, POWER processors, but it can also be used as an operating system for many embedded devices, mobile computers and servers. On the other hand, IBM has done their bests so that AIX could be more available; currently, one can find AIX-based computers on a large suite of systems, ranging from blades, through small rack units and up to full-rack systems.

Scalability is another significant factor. According to Galvin, RHEL is capable to simultaneously use only 64 cores and 256 GB if Random Access Memory (RAM) (128 cores and 256 GB) on CISC (RISC) architecture. In comparison, AIX can use four times more cores and over thirty times more memory (256 cores and 8192 GB memory). What is more, comparing the actual performance of operating systems is an extremely challenging task, because benchmarks are generally designed to measure either hardware or application performance.

Operating systems that have been used for solving the AS aggregation task could be characterized in more detail in terms of features, such as computer virtualization, code debugging, as well as system installation and administration. Nonetheless, given the characteristics of the AS aggregation task, there is no need to discussed all of them; detailed comparison of the functionality of AIX and RHEL can be found in [9][10].

C. *Hardware Platforms*

All experiments were conducted in the Department of Distributed Computer Systems at Wroclaw University of Technology. The tests were conducted on three servers equipped with RISC processors, successively referred to as: RISC-AIX, RISC-RHEL, RISC-RHEL-ND and one CISC-based processor IBM Blade CISC server referred to as CISC-RHEL.

TABLE III. HARDWARE AND SOFTWARE CONFIGURATIONS

Component	RISC-AIX	RISC-RHEL	RISC-RHEL-ND	CISC-RHEL
Processor	4.0 GHz POWER6	4.0 GHz POWER6	4.0 GHz POWER6	3.0 GHz Xeon 4C
# of CPUs	2	2	2	2
CPU cores	2	2	2	4
CPU type	x64	x64	x64	x64
Memory	4GB	4GB	4GB	8GB
HDD storage	73.4 GB SAS 10 000 rpm	73.4 GB SAS 10 000 rpm	n/a	73.4 GB SAS 10 000 rpm

ND suffix stands for no disc; this means that every piece of equipment that is marked with ND does not contain internal storage. Moreover, in case of RISC, 4 cores CPUs are in fact 2 double-cored CPUs. The detailed hardware description of the above-mentioned servers is shown in Table III.

All RISC-based computers (those with RISC prefix) contain two dual-core POWER6 processors (see Fig. 3). Each POWER6 processor consists of two 4.0 GHz cores that are capable of two-way Simultaneous MultiThreading (SMT), which allow multiple independent threads to be executed, and one AltiVec (previously called IBM VMX) which is a floating point and integer Single Instruction Multiple Data (SIMD) instruction set accelerator. Therefore, in this paper, we are trying to evaluate to what extent the use of AltiVec acceleration may improve the general performance of POWER-based computers in the optimal AS aggregation problem.

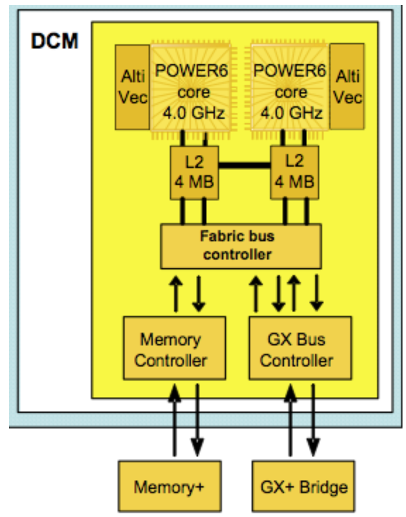


Figure 3. POWER6 [IBM].

The configuration of server RISC-RHEL-ND differs from the one of RISC-RHEL only in terms of lack of internal disk storage and its operating system is run using local network from the external disk array. This configuration enabled us to examine whether the lack of internal disk storage and thus the need to install an operating system on the external disk array, affects (and if it does, to what extent) the efficiency of numerical calculations in the optimal aggregation problem.

IV. BENCHMARKING EXPERIMENTS

This section is divided into two parts: the first part presents a sample method that may be used to monitor a group of ASs; the other describes all the experiments that were conducted in order to select the best combination of software and hardware architecture for solving the optimal AS aggregation problem.

But, before we explain the procedures carried out, let us go back to the very beginning of this paper. In the first section, we have formulated the hypothesis concerning the relationship between resource download time and the server location in the Internet. We have carried out a simple experiment to prove it. To achieve this, we have randomly selected 30 web servers with identical lists of available resources (in this case, we used official mirror servers with Linux Ubuntu 13.04 installation image file; its file size

 ISBN: 978-1-61208-365-0

equals to 735MB). In the subsequent step, we have measured download times of the aforementioned resource from the all considered web servers. Fig. 4 presents average download times of the resource. To make the figure more readable, we have used the logarithmic scale.

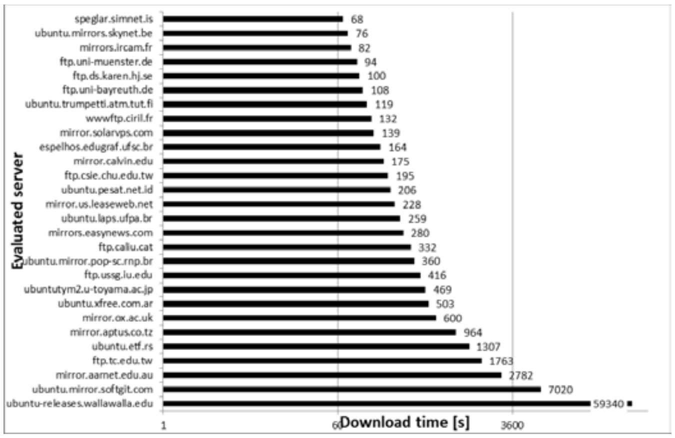


Figure 4. Download times.

The conducted experiment may be also considered as a method for the evaluation of AS' representative's characteristics (and consequently the characteristics of a whole AS). However, one ought to remember that even the simple selection of the download file is extremely crucial and may have a significant influence on the accuracy of the results and thus their usability for further processing. Therefore, the resource should be selected carefully; namely, the size of the resource should be neither too small (because the measurements should be greater than a statistical error) nor too large (the measurements cannot excessively burden the evaluated representative hosts of a considered AS).

The experiments described in Sections IV.A and IV.B were performed using the same input data (i.e., RTT) for evaluated ASs. In the first experiment, the values are converted to milliseconds and stored as integers. In the second experiment, however, the values are converted to seconds (with fractional part) and stored as single precision floating-point numbers.

Unfortunately, due to a substantial time-consuming nature of the experiment for both, integer and floating point numbers, the double precession numbers were not considered in this work. Nevertheless, they are another worth pondering example to be examined in the future work.

A. AS Aggregation: Integer Case

Fig. 5 shows the relationship between the aggregation time and the number of ASs for the integer case. One may notice that the aggregation time grows exponentially. What is more, it turned out that CISC computer is able to solve the aggregation task much more efficiently. Take the last measurement (wherein the number of ASs is 25) for instance. It took 169 days (almost half a year) for RISC-AIX server to generate the desired MetaASs, whereas its CISC counterpart solved this problem in barely 128 days (less than four and the half months). One should realize that the difference is immense in terms of execution time and this quick evaluation survey speaks for CISC solutions even for so small a size of the aggregation problem.

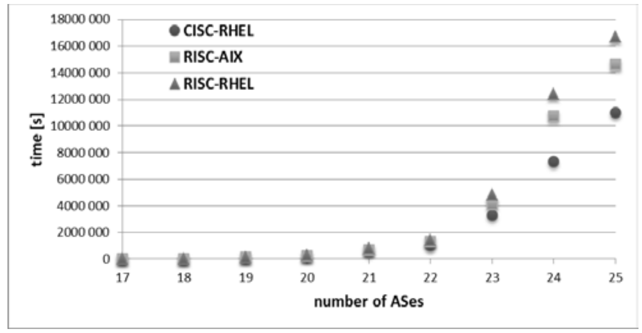


Figure 5. Aggregation time vs. the number of ASs. Integer case, computed on a single core .

The choice of an operating system for calculation is also essential. Namely, calculations conducted on the same model of server are performed slightly faster on AIX than on RHEL.

It turned out that the results obtained for the RISC-RHEL-ND and RISC-RHEL were strikingly similar for all considered cases, so they were neglected and they are not presented in any figure. This also showed that the speed of calculations depends only on the central processing unit.

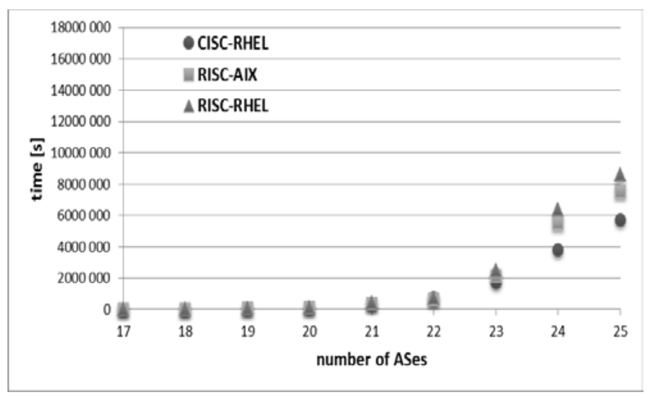


Figure 6. Aggregation time vs. the number of ASs. Integer case, computed on two cores.

Fig. 6 presents the relationship between the aggregation time and the number of ASs subjected to that process, calculated on two cores for the integer case. One may notice a dramatic decrease of execution time that is needed to find the optimal solution. Time needed to obtain the result for 25 ASs by RISC machine is almost two times smaller than that for the aggregation running on a single core. In this case, CISC is also much more efficient than RISC-equipped computers. The execution time for CISC-RHEL and RISC-RHEL for 23 ASs equals 20 and 29, respectively. The selection of the operating system has also the impact on the calculation time; this impact is similar to that of presented in the Fig. 5.

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-365-0

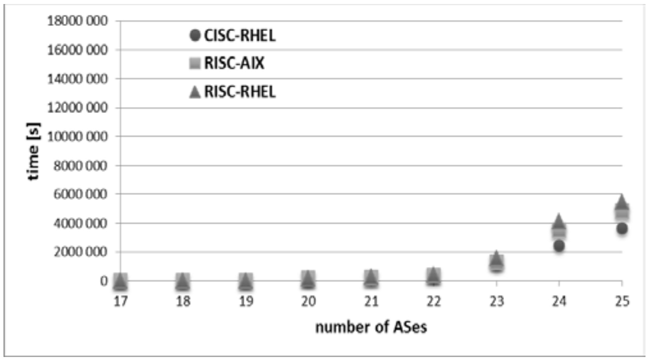


Figure 7. Aggregation time vs. the number of ASs. Integer case, computed on four cores.

Fig. 7 presents the relationship between the aggregation time and the number of ASs subjected to that process, calculated on four cores for the integer scenario. One may notice a decrease (comparable with that of the previous figure) of execution time that is needed to find the optimal solution. To illustrate the chasm in the computational speed between RISC and CISC, one may compare the results obtained for 24 ASs and 25 ASs by RISC-AIX and CISC-RHEL, respectively – they are almost the same.

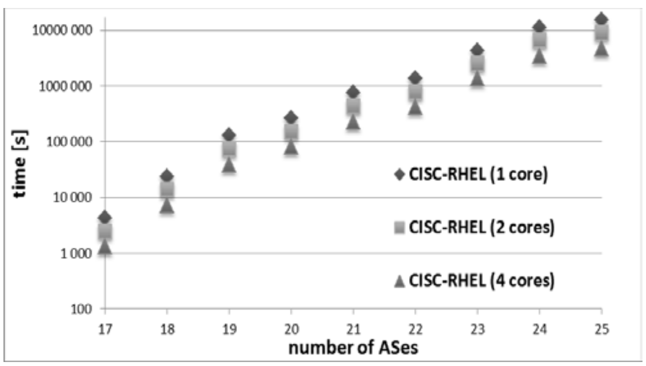


Figure 8. Aggregation time vs. the number of ASs. CISC architecture multicore comparison for the integer case, presented on logarithmic scale.

Fig. 8 shows calculations on a logarithmic scale, conducted for the CISC machine for all considered integer cases. This illustrates two things: the exponential computational complexity of the aggregation problem, and constancy of the increase of power achieved by involving additional CPU cores.

B. AS Aggregation: Floating Point Case

Figs. 9, 10, and 11 present the results obtained for characteristics represented as floating points for a single core, two cores and four cores scenarios, respectively. The situation turned out to be completely different from the research conducted for ASs' characteristics represented as integers. The POWER-based computers turned out to be the more efficient than the evaluated CISC machine.

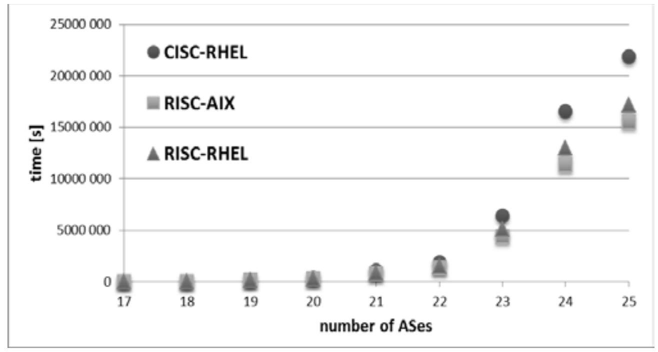


Figure 9. Aggregation time vs. the number of ASs. Floating point case, computed on a single core.

The choice of an operating system for calculation is as essential as in the case of integer scenarios; therefore, all conclusions that can be drawn from the conducted experiments are similar to those from the previous subsection.

The most surprising hypothesis that can be proposed, however, is that with the simultaneous increase in both the number of cores and the number of ASs to be aggregated, the differences between two considered architectures gradually commence to narrow.

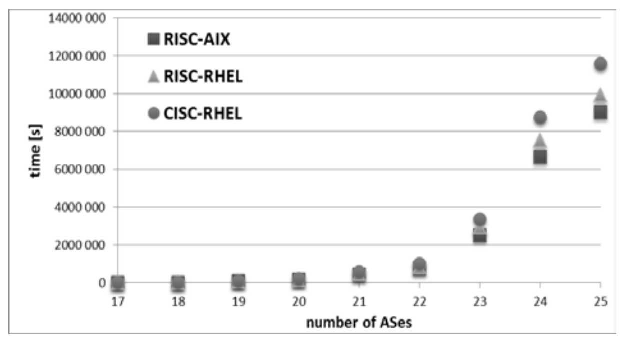


Figure 10. Aggregation time vs. the number of ASs. Floating point case, computed on two cores.

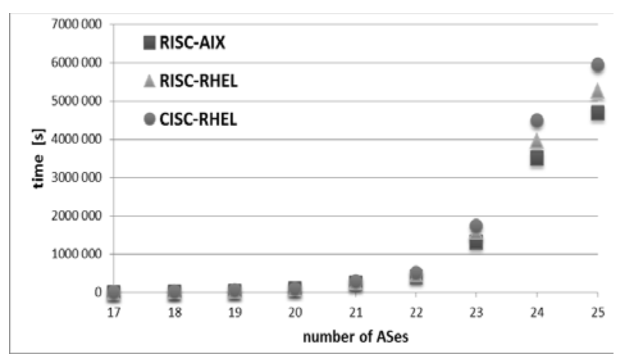


Figure 11. Aggregation time vs. the number of ASs. Floating point case, computed on 4 cores.

C. Matrix Multiplication

Performing numerous arithmetic calculations is a prerequisite to perform the AS aggregation. We benchmark the speed of arithmetic calculation, by performing simple matrices multiplications. The aim of this subsection is to examine, whether the floating-point accelerator that can be found in RISC architecture has (and if it does, to what extent) an impact on the calculation speed.

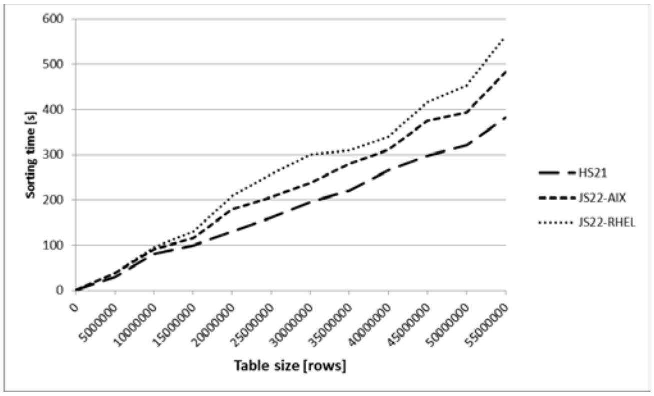


Figure 12. Multiplication time vs. matrix size.

Fig. 12 presents the relationship between the time needed to perform multiplication of two square matrixes and their size (*N*). Both matrixes consisted of *N*×*N* floating point numbers. One should note that choice of the operating was essential. Strictly speaking, calculations conducted on the same server are performed slightly faster on AIX than on RHEL. Furthermore, due to the use of floating point numbers, RISC computers were able to use their accelerators and thus needed less time to obtain the correct results. This proved that the built-in floating-point accelerator might significantly increase the speed of calculations.

V. RELATED WORK

Diversity of techniques and approaches that deal with the problem of AS topology decomposition may be found in the literature. Dimitropoulos et al., for instance, use information retrieval techniques (in this case, this is an expert system along with simple text classification techniques) to analyze data from Internet Routing Registers [11]. Mostly, however, scientists tackle the problem of AS aggregation by analyzing BGP-derived AS graphs that represent connections between ASs. Ge et al. use Consumer-to-Provider (C2P) relationships to classify ASs into seven groups (tiers); basically, their concept is based on the idea that all providers should be in higher ASs than their clients [12]. Subramanian et al. extend this approach by taking into account peer-peer relationships [13].

Nevertheless, these approaches usually suffer from a slight drawback; namely, they rely exclusively on BGP-derived AS graphs. Unfortunately degree-based classification may result in an incomplete AS topology and bring about imprecise decomposition. The approach presented in this paper tries to solve this problem in a slightly different manner; namely, by using BGP-derived AS interconnection structure we try to identify and measure the characteristics of ASs' representatives in order to use them in the aggregation process.

The literature focusing on AS-level Internet topology research is extensive and has been quickly growing in the past few years [14][15][16][17][18]. Roughan et al. [14] and Jyothi et al. [15] discuss the most important problems found in the previous work on AS topology phenomenon and propose some advancements towards improving measuring and modeling in this research. Chen et al. [16] touch problems of revealing AS-topology in the context of Peer-to-Peer (P2P) networks development. Borzemski and Nowak [17] introduce the novel algorithm to predict performance of web servers using revealed information about AS topology between a web server and a web client. Durairajan et al. [18] propose to build a comprehensive and geographically accurate map of the physical Internet, including ASs, for future research and operational applications. This proposal, as well as, several other efforts in Internet measuring, analysis, and modelling are instances of Big Data analysis conducted in Fan et al. [19]. Big Data paradigm promises new scientific levels of Internet research. According to the reference [3] in [19], two main goals of analyzing Big Data are to develop effective methods that can accurately predict the future observations, and at the same time to gain insight into the relationships between the features and response for scientific purposes. Taking into account these goals, Borzemski [20] proposes Web Performance Mining (WPM) - a new dimension in web mining analysis - to predict web server performance as experienced by the web user. Another approach, which is based on geostatistical Turning Bands Methods, has a similar aim and is described in [21]. Borzemski [20], and Borzemski and Kamińska-Chuchmała [21] explore large databases containing continuously collected records of performance measurements of Internet connections. References [22][23] present our distributed measurement infrastructure MWING that allows to measure the Internet from multiple vantage points, like in [13].

VI. CONCLUSION AND FUTURE WORK

Based on the obtained results, it can be stated that CISC architecture should be chosen to solve the AS aggregation problem discussed in this paper. Not only are they capable of producing correct results more rapidly than RISC-based computers, but also they are less expensive. One may, however, argue that ASs' characteristics are usually fraction values; so RISC-based computers could be the solution. Nonetheless, it turns out that in such cases it is somehow possible to convert such data into integer values without losing any information.

The operating system may also influence the general performance for it turns out that IBM AIX can slightly more efficient than Red Hat Enterprise Linux.

The optimal solution of the AS aggregation problem is extremely demanding and time-consuming, especially for the huge number of ASs. Nevertheless, in a real-life case scenario, we do not always have to find the optimal result because the suboptimal is often satisfactory. Therefore, we can simplify the whole aggregation by performing it gradually. This could result in the significant reduction in the time needed to perform the aggregation (the processing time increases exponentially to the size of the problem).

Nonetheless, due to the complexity of the examined phenomena, the research presented in this paper were conducted only for the single precision floating-point number representation. In the future work, we would like to focus on conducting another experiment that compares differences in performance (if there are any) between single and double precision numbers.

Considering the results of the conducted experiments in case of the floating-point scenarios, it can be assumed that the more cores of multicore processor are used in the optimal AS aggregation, the smaller the differences between the obtained performance indices become. Therefore, in the future research, one should consider the comparison of the architecture performance in more complex computing structures such as High Performance Clusters. In this scenario, three cases should be considered:

1. Homogeneous CISC-based Clusters.
2. Homogeneous RISC-based Clusters.
3. Heterogeneous Clusters (consisting of both CISC and RISC based computational nodes).

ACKNOWLEDGMENT

The authors gratefully acknowledge partial support of project EU COST Action IC0805: Open Network for High-Performance Computing on Complex Environments.

REFERENCES

[1] J. Hawkinson and T. Bates, “Guidelines for creation, selection, and registration of an autonomous system”, Request for Comments 1930, Internet Engineering Task Force, 1996.

[2] Y. Rekhter, T. Li, and S. Hares, “A border gateway protocol 4”, Request for Comments 4271, Internet Engineering Task Force, 2006.

[3] W. Stallings, Computer Organization and Architecture: Designing for Performance. Prentice Hall Inc., a Simon Schuster Company, 2009.

[4] T. Bates, P. Smith, and G. Huston, “CIDR Report for 27 May 14, 2014, vol. 2014, http://www.cidr-report.org/as2.0/ [accessed: 2014-05-27].

[5] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, “Hypertext Transfer Protocol” – HTTP/1.1, June 1999, Request for Comments: 2616.

[6] V. Cgvatal, “A greedy heuristic for the set-covering problem”, Mathematics of Operations Research, vol. 4 no. 3, 1979, pp. 233–235.

[7] V. Vazirani, Approximation Algorithms. Springer-Verlag, 2001.

[8] C. Chen, G. Novick, and K. Shimano, “The intellectual excitement of computer science: RISC architecture”, http://www-cs-faculty.stanford.edu/~eroberts/courses/soco/projects/2000-01/risc/ [accessed: 2014-05-24].

[9] P. Galvin, “Pete’s all things Sun: comparing Solaris to Red Hat Enterprise and AIX, 2010.

[10] P. Galvin, “Pete’s all things Sun: comparing Solaris to Red Hat Enterprise and AIX — Virtualization Features”, 2011.

[11] X. Dimitropoulos, G. Riley, and K. Claffy, “Revealing the autonomous systems taxonomy: The Machine Learning Approach”. Proc. of Passive and Active Measurement Conference (PAM), pp. 91-100, 2006.

[12] Z. Ge, D. Figueiredo, S. Jaiwal, and L. Gao, “On the hierarchical structure of the logical Internet graph. Proc. SPIE vol. 4526, pp. 208-222, 2001.

[13] L. Subramanian, S. Agarawal, S. Rexfors, and R. H. Katz, “Characterizing the Internet hierarchy from multiple vantage points”. IEEE INFOCOM, 2002.

[14] M. Roughan, W. Willinger, O. Maennel, D. Perouli, and R. Bush, “10 lessons from 10 years of measuring and modeling the Internet's autonomous systems”. IEEE Journal on Selected Areas in Communications 29(9): 1810-1821, 2011.

[15] S. A. Jyothi, A. Singla, B. Godfrey, and A. Kolla, “Measuring and understanding throughput of network topologies”. CoRR abs/1402.2531, 2014 [accessed: 2014-05-24].

[16] K. Chen, D.R. Choffnes, R. Potharaju, Y. Chen, F.E. Bustamante, D. Pei, and Y. Zhao, “Where the sidewalk ends: extending the Internet AS graph using traceroutes from P2P users”. IEEE Trans. Computers 63(4): 1021-1036, 2014.

[17] L. Borzemski and Z. Nowak, Using autonomous system topological information in a web server performance prediction”. Cybernetics and Systems 39(7): 753-769, 2008.

[18] R. Durairajan, S. Ghosh, X. Tang, P. Barford, and B. Eriksson, “Internet atlas: a geographic database of the internet”. HotPlanet '13 Proceedings of the 5th ACM workshop on HotPlanet, pp. 15-20, 2013.

[19] J. Fan, F. Han, and H. Liu, “Challenges of Big Data analysis”. National Science Review Advance Access publication Feb 6, 00:1-22, 2014.

[20] L. Borzemski, “The use of data mining to predict web performance”. Cybernetics and Systems 37(6): 587-608, 2006.

[21] L. Borzemski and A. Kaminska-Chuchmala, “Distributed web systems performance forecasting using Turning Bands method”. IEEE Trans. Industrial Informatics 9(1): 254-261, 2013.

[22] L. Borzemski, L. Cichocki, and M. Kliber, “Architecture of multiagent Internet measurement system MWING Release 2”. Lecture Notes in Artificial Intelligence, vol. 5559, pp. 410-419, 2009.

[23] L. Borzemski, “The experimental design for data mining to discover web performance issues in a Wide Area Network”. Cybernetics and Systems 41(1): 31-45, 2010.

The Designing and Implementation of a Smart Home System with Wireless Sensor/Actuator and Smartphone

Omar Ghabar
School of Computing and Engineering
University of Huddersfield
Huddersfield- UK
Email: omar.ghabar@hud.ac.uk

Joan Lu
School of Computing and Engineering
University of Huddersfield
Huddersfield- UK
Email: j.lu@hud.ac.uk

***Abstract*—This paper presents the design and implementation of a prototype system that employs standing techniques for smart home sensing and control for a future home environment. Smartphones currently show great potential in sensing, processing and communication capabilities. The prototype provides solutions for communications between home users, electronic equipment and a Smartphone. The home equipment is linked wirelessly via Wi-Fi technology to a household server, which can be controlled through the smart phone using an iOS application. In particular, the main objective of this work is to design a system named Wireless Sensor Actuator Mobile Computing in a Smart Home (WiSAMCinSM) that makes multifunctional contributions to assisting elderly people in their daily lives. Part of this system has been tested within the laboratory; firstly, through a WI-Fly Serial Adapter using Tera Term technology, and secondly, through WI-Fly and iPhone using the Ad hoc network. The prototype system consists of a Smartphone, Microcontroller Unite (STC89C52RC), WiFly-RN370 and seven sensors, as well as an iMac and a Personal Digital Assistant (PDA). The prototype system has been implemented based on the Smartphone and commercially available low cost sensors, actuators and logic converters. Results show great potential in employing the information and evaluation of high quality prototypes for the functions of data acquisition.**

Keywords*–*smartphone; sensors/actuators; smart home; WI-Fly.

I. INTRODUCTION

It is widely known that embedded sensors and actuators within mobile computing in the smart home can be useful in improving elderly people’s daily lives [1]. Today, elderly people are the fastest growing segment of the population in developed countries, and they want to live as independently as possible; but, these lifestyles come with risks and challenges. The ageing population has continued to grow since 1950; the world percentage of elderly people has increased steadily from 8% in 1950 to 11% in 2009 and is expected to reach 22 % by 2050 [2]. It has been noted that the continuing decrease in the mortality rates for the elderly, means that the proportion of older people in the population will continue to increase [2].

The smart home is equipped with wireless sensors and actuators to recognise environment-sensing data and to control electric devices. The technology will be converted to a digital system mapping the movement of the body within the environment surrounding it. This will then be transmitted to the Microcontroller Unit (MCU) to perform certain applications, for example: monitoring, appliance control, and processing, most of which require and utilise software information. This is in addition to the automatic transmission by means of an algorithm located in a different address [3].

All phones also come with the ability to communicate over the cellular networks, and most have built-in short range communication capabilities such as Bluetooth and Wi-Fi, that can allow them to communicate with and control appliances in their surrounding environment [4]. Khan et al. [5] found that over the last decade, the mobile computing service has been commonly accepted and has become an integrated digital method of assistance, not only for key computing and communication mobile devices, but also for other purposes, such as predicting the global environment, controlling greenhouses and for social networking.

Smart phones are now the preferred mode of interaction with many appliances because the phone is always available and can provide a better user interface with its improved hardware. Precedents exist for people using their phones to control their environment remotely [4].

The model in this study is the wireless Sensor Actuator Mobile Computing in Smart Home (WiSAMCinSH), which consists of various appliances to monitor occupant activity and can also be used in other circumstances to control the devices that are used indoors. The system is equipped with a number of wireless sensors and actuators that can make decisions and acquire data according to the behaviour of the house occupant. The Smartphone technology is used to receive information from wireless sensors in real time. It is believed that information collected from sensors can engage with a large proportion of data to indicate possible human behaviour. That kind of information can be gathered and transferred to the Smartphone or a personal computer for

 ISBN: 978-1-61208-365-0

storage and analysis using advance computation and data processing methods.

The rest of the paper is structured as follows: Section 2 describes the background, with respect to wireless sensor/ actuator and mobile computing in a smart home. Section 3 introduces the prototype system used in formulation of the method of smart home design. Section 4 presents the system design by describing the prototype for human mobile computer interaction in a smart home and how it can integrate with other equipment such as wireless sensors, actuators and the MCU, using a wireless network. Section 5 outlines the appliances and technology used with sensor implementation. Section 6 defines two techniques to set up configurations of the test plan using Tear Term and smartphone. Section 7 considers an evaluation of the results while Section 8 provides the conclusion and future work.

II. RELATED WORK

Alam et al. [6] reviewed collective information on various technologies used in the smart home, and defined the smart home as "an application of ubiquitous computing that is able to provide user context-aware automated or assistive service in the form of ambient intelligence, remote home control, or home automation". Ding et al. [7] used a survey to assess the effect that various sensor technologies have on sensing environments and infrastructures mediated in the smart home, where appliances are located on elderly people and placed in the home infrastructure.

Recent studies by Makonin et al. [8] and Kononen et al. [9], which involved integration between mobile computing and computational intelligence, provide an opportunity to assist inhabitants dynamically with interaction in smart home technologies. These devices and patterns of usage are the main concentration of new projects. There is therefore a need to understand more about integrating, locating and implementing these technologies to help occupants in constructing additional resources to enable decision making.

Tag4M and Wi-Fi were used to measure temperature, humidity, light and pressure in a room environment in the smart home. The use of hardware and software techniques presented a condition for the monitoring of the ambiance in the room. The results illustrate that gathering data using Wi-Fi Tag might be a preferable method in wireless application [10].

Data are gathered from the sensors and actuator network to monitor the environment and activity of regular living; and these are then communicated through a base station, finally being saved in a central database [11].

Suryadevara et al. [12] and Majeed [13] have recently developed a well-being function for the elderly in the intelligent home, with the support of devices using ZigBee [12] and wireless sensor. The well-being function is used to compute the run time of the system design as a related procedure throughout. It takes the sensing action period from the specific records of the workstation system. This index was instantaneously detailed in the database for upcoming information processing and estimation of the uncommon behaviour of the occupants.

Rather than use a massive amount of monitoring devices, Gaddam et al. [14] have experimented with a limited number of expensive wireless sensors of high quality, to deal with the challenges of the prototype system and reliability. They suggested a microcontroller with wireless radio frequency communication, for example ZigBee; which allows for the data collected from sensors and transmitted to a base station to be installed on a PC. Some experiments have been done by linking wireless sensors to electronic equipment such as: a kettle; microwave; bed; and TV; to determine the reliability and performance of the system design. The results showed that for longer distances reliability decreases and also, the effect of Wi-Fi noise caused communication to become unreliable.

In 2012, Jiang et al. [15] carried out a number of investigations into the methods used to monitor the home environment, including: pressure, temperature, humidity, and electric power. The method it was hoped could solve any problems that arose and give warning alarms instantly to the mobile agent. The authors found that the prototype system includes three aspects, namely, (i) the mobile agent is not causing any delay in the network, (ii) there is a decreased latency in the data stream, and finally, (iii) the technology of WSN support is used to resolve the difficulty of knowing whether a location is inhabited.

Makonin et al. [8] presented a method called a Smart Intervention (SI); this function involved: residents requirements, home, context, and measurements. The devices used in this module included: sensors, actuator and wireless network. Formula (1) below has been used in experiment to control the light in the middle of the night when the occupants get out of bed. It was found that this system design has the benefit of permitting the functionality to be extensible and flexible in the smart home, and it can be developed for many other numbers of reasons.

$$H's = SI\ (Hs, H, O, Ctx, Aut, E) \tag{1}$$

where Hs is the state before measurements, H is the home, O is the occupant, Ctx is the context-aware, Aut is the automations and E is the evaluation for accuracy and ability.

III. METHOD EMPLOYED IN SMART HOME

Through the benefits of the application of sensors such as actuators, wireless adapters, and processor units, many previous developments in the smart house have been replaced. As mobile computing becomes more universal, there will be an increasing number of computerized devices in our environment that are capable of being controlled [16].

Framework theories for human and mobile computing interaction in the smart home, particularly for elderly people, are nonexistent, especially in the area of smart phone and wireless sensors and actuators. On the other hand, smart intervention is lacking in its description of human-home interaction. Because of this, there is a motivation to develop a method that can be used to support work with the system design used by residents in the smart home. Therefore, the main function of Smart Intervention (SI) can takes the following formula (2) [8] :

$$H's = SI\ (R, WS/A, Ctx, Aut, Hs, E), \qquad (2)$$

where H's is the home state, R is the resident, WS/A refers to wireless sensor and actuator, Ctx is the context-aware, Aut is the home automation, Hs is the smart home and E is the evaluation for reliability, efficiency, and usability.

The electrical equipment in the smart home needs to be controlled by actuators in order to maintain it within a certain range of data collection, such as: temperature and light to execute the action of on or off immediately, or as scheduled by the resident's command. The smart home intelligence network is to detect serious conditions that can be picked up by the smart home sensors, when there is a likelihood of an event taking place. In addition, smart intervention can be used to elicit an interaction between the environment and the home equipment. For example, a better automatic action can be made regarding the data received from the environment in the smart home, such as regulating the light and fan. This can be done with the scheduled intelligent intervention which are in built, when the devices are correctly switched on or off by the occupants.

IV. SYSTEM DESIGN

Regarding the formula of the smart intervention in the previous section, we add one parameter to this equation namely; wireless sensors and actuators, to be engaged in this prototype system. The comprehensive system architecture from the communication, electronic devices and data management viewpoint is given in Fig 1. Different challenges based on the design and, related to sensing and control in detecting the wireless network, have been addressed in the related work.

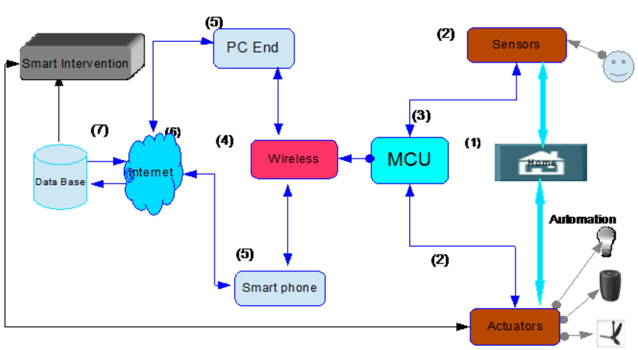


Figure 1: Block Diagram of General Architecture.

- The system design is based on a wireless adapter: WI-Fly-RN370, rather than other wireless technology, because this has the ability to cover up to 300m in an open area, as well as being able to connect with the smartphone and PC through Ad hoc or infrastructure networks.
- The service remains an open topic; new methods of methodical design, conceptual models, and common architecture are required. Complete technical solutions and technology need to be included in the scheming sensors so as to improve the computer system, and to work with the physical user intervention. This will enable us to explore a universal extendible smart home architecture that assists these models in working together and to show it alongside our prototype WiSAMCinSH.

Consequently, this study will attempt to provide sensitive architecture and technology solutions to common context, effectively collecting discrete sensor technologies under an ambient background. This will result in automated proactive and personalized service and optimization of context-aware decision making.

Through the benefits of the applications of sensors such as actuators, wireless adapters, and processor units, many previous developments in the smart house have been replaced. Working on developments to the prototype will ensure that newly created interfaces allow for features with which the user has interacted previously.

A. *Framework Layers for WiSAMCinSM*

This section shows the WiSAMCinSH architecture system consisting of four layers; as shown in Figure 2.

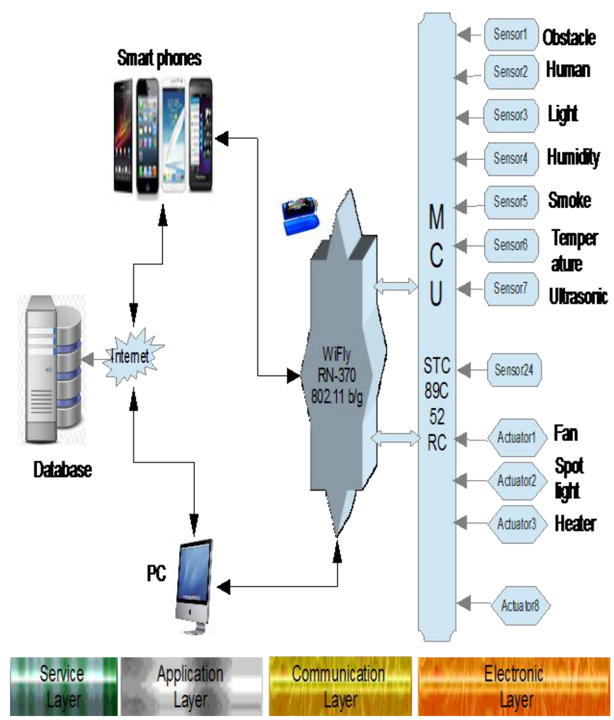


Figure 2 .Framework Layers in the Prototype System.

1) *Electronic Layer:* In the electronic layer, which is located in the lowest level, the sensors and actuators are organised in rooms in different places to gather raw data such as obstacle avoidance, human body activity, light levels, smoke, humidity, temperature, and ultrasonic distance measuring, as well as to control the appliances that the householder decides to use, for example a fan, light, or heater. This information is collected by MCU (STC89C52RC), which is connected to a WI-Fly adapter and can also be used to store an application program embedded with flash memory.

2) *Communication Layer*: In the communication layer, sensing information from different sensors is used according to their applications. This layer communicates with the application layer and then transmits the users' decision to the electronics section, and transfers information written or read to the successive interface consisting of an iPhone and computer control. This data is transmitted through a TCP/IP socket where an Ad hoc or infrastructure network has the ability to use wireless connections to several WI-Fly adapters.

3) *Application Layer*: The application layer is able to build platform interfaces with elderly people, for example a user can get data or make decisions using the smartphone, personal computers, or tablets. Moreover, the householder can send commands to a wireless sensor over the microcontroller unit, if any abnormal information is received. Reliability, satisfaction, effectiveness, efficiency, and usability are requirements for everyday use and this device is able to provide all these. In addition, there is a control program in the application layer that can be operated through the smartphone or PC to acquire the data from the sensors.

4) *Service Layer*: The database server and Internet in the service layer is where information is gathered from the sensors and actuators. This layer provides a computing service based on the database. Important and useful information from historical data can predict abnormal conditions, such as: very high humidity; natural gas or smoke using the smoker sensor; and so on. At the same time, the database system offers an opportunity for another user to share the information, for example, a healthcare professional can monitor the situation of their patient.

V. SYSTEM IMPLEMENTATION

The main model system is broken down into two main parts; hardware and software that are currently available in the laboratory.

B. *Hardware Parts*

- Wireless adapter (WiFly-RN370).
- MCU (STC89C52RC).
- Seven kinds of sensors.
- IPhone (Version iOS 6.1.3) and iMac version 10.7.5.

C. *Software Parts*

- C language for MCU.
- Objective-C for iPhone application.

1) *WI-Fly (RN-370):* The Wireless adapter is powered by: an external AC to 5V DC and two AAA batteries which run up to eight hours on full charge. The device is connected with only a RS-232 serial port interface of the DB9. It receives information from sensors over the MCU, and then sends it to end devices such as iPhone and PC. The data is also transferred over a reliable TCP/IP socket using an Ad hoc or infrastructure network. This has the benefit of low wireless construction and can be connected to any type of WI-Fly serial adapter. An overview of this set up can be shown in Figure 3.

There are different types of connections available to create Wi-Fi applications, for example: remote environment sensors, control and monitoring appliances, diagnostics, and mobile phone connections; such as GPS and sensors. Therefore, WI- Fly configurations can be set as peer-to-peer (Ad hoc) networking to an iPhone, by using an IP address which is (169.254.1.1) and Subnet mask (255.255.0.0), with the need to set the Service Set Identifier (SSID) and WI-Fly-GSX-a5 in a wireless mobile computing network [17].

2) *Microcontroller Unit (Logic Converter):* The Microcontroller Unit is connected to the computer in order to collect data from sensors, pre-process raw data, and direct data to the phone. It is also connected to a wireless module Wi-Fi to accept the wireless connection through the smart home server. The STC89Cxx series MCU is an important part of the system design as it is an 8-bit single-chip microcontroller. This chip is compatible with outlying device communication that monitors resident activity, and motion by gathering data from sensors, interfaced with the WI-Fly wireless transceiver, and embedded with 64K bytes flash memory to store data, which is shared with In-system Programming (ISP). It also has an, In-system Application (ISA) to assist the operators. These communication requirements are based on a microcontroller need to be adapted with a Universal Asynchronous Receiver Transmitter (UART) [18]. This is an appliance that transmits and receives raw information from the choice of MCU to support a low level programming language. C provides many different ranges of development tools and pins diagrams, as illustrated in Figure 4.

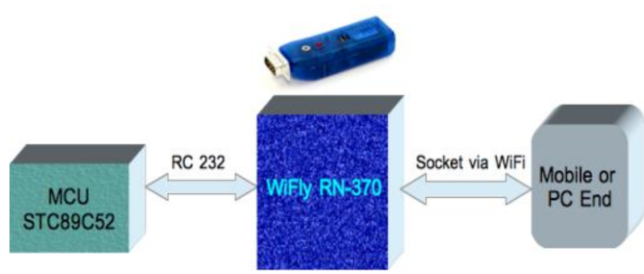


Figure 3 Overview of the WI-Fly Adapter Connection

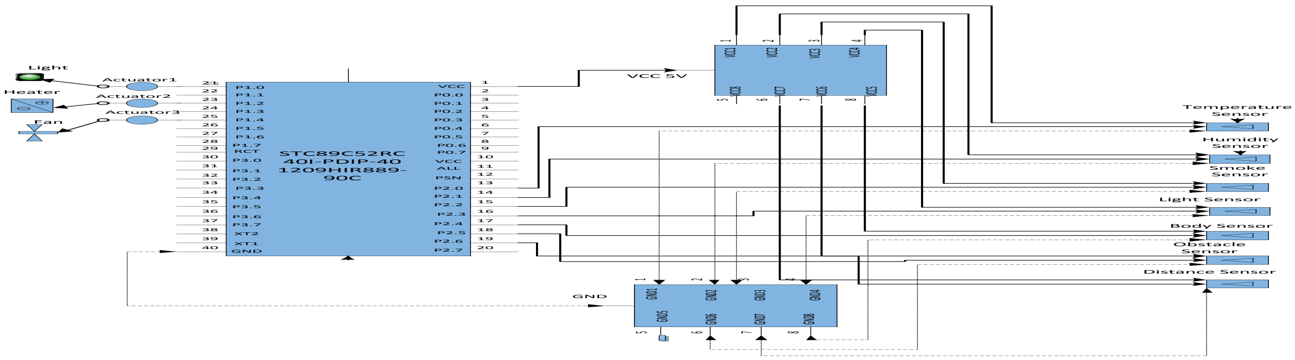


Figure 4 Microcontroller Units STC89C52RC-schematic pin diagrams of the system.

3) *Sensors Involved:* There is great demand for the use of sensors for several applications in the prototype. The most commonly used being: obstacle avoidance sensor, smoke sensor, human detection sensor, light level sensor, humidity sensor, temperature sensor, and ultrasonic distance measuring. These are the different types of sensors that have been used in the system design. The main idea of this function is to transfigure physical variables in reality to digital variables and real numbers, which are processed in the computing system.

The function of the temperature sensor DS18B20 [19] is to gather data from the room environment, when the software program runs in the MCU. The brightness sensor BH1750, is dependent upon the level of light in the home; the smoke sensor ZYMQ-2 is used to monitor whether there is any smoke or gas close to the sensor area; the humidity sensor HR202LM393 is used to sense the level of nearby humidity when environmental humidity is high; the obstacle avoidance sensor E18-D50NK has a detection distance between 3cm and 80cm with an adjustable resistor; the human body sensor DYP-ME393 reliably detects the human body when it comes to within seven meters of the sensing area; the last sensor is the ultrasonic distance measuring HC-SR04 [20], used to measure distance from 2cm to 4m when the function is working well.

4) *Smart Phones and PCs (End Use):* In this system, the implementation of an end-use like iPhone, Android, BlackBerry and Windows Phone as the platform for the prototype system means they can receive the gathered information from sensors and control the actuator. The smart phone platform can be programmed using Object-C to communicate over CFNetwork sockets. Zdziarski offers a code using a CFNetwork socket to connect between the web server and smart phone or among peer-to-peer networks such as Ad hoc connections [21].

5) *Software Structure:* The information gathered from the seven sensors are stored in the memory of embedded system STC89C52RC provisionally, then when it is running, the software program and compiler passes through the Test Program in Debugger (Keil uVision3) for the debugger instruction. At the same time the program language C also will run in the STC-ISP.exe, after selecting the hex file and the port from the PC to be ready for sending the collected data over wireless technology.

The iPhone SDK (Version IOS 6.1.3) and Apple iMac version 10.7.5 run with Xcode version 4.6.2 were used in this experiment. Objective-C and Cocoa Touch were the programs that were most used in the implementation of this part of the project, where Cocoa Touch is used by Object-C which offers the structure for iPhone application.

VI. TESTING PLAN

A. *Experiment Condition:*

Testing the prototype system firstly required connection of the seven types of sensors to the MCU as follows: obstacle avoidance sensor; human body; brightness; smoke; humidity; temperature and ultrasonic distance measuring; to the ports from P2^0 to P2^7 of STC89C52RC. This unit has the ability to gather data from 32 sensors; because it contains four sets of ports P1, P2, P3 and P4 - each with eight pin. The WI-Fly Serial Adapter is interfaced with the MCU by using connector Pin DB9; it is also connected through serial port communication RS232. This appliance is designed to work with an input power supply from 4.5 to 5 VDC. There are three cable interfaces (RXD, TXD and GND) between the WI-Fly and Microcontroller and five cable interfaces between the WI-Fly and computer.

B. *Steps:*

There are two techniques to setup configurations of the software as follows:

1) *Setup Configuration through WI-Fly Serial Adapter Using Tera Term:* This configuration is used through the Ad hoc Mode (point to point), with switch 1–ON. The Ad hoc Mode powers up the Wi-Fly device, which is only connected between two appliances that are Smartphone (iPhone) or PC, to gather the data or control a device through the serial interface as shown in Figure 5. This WI-Fly device needs to set the constructor default value as follows: Service Set Identifier SSID, which is WiFly-GSX-a5 to the IP address (169.254.1.1), IP net mask of (255.255.0.0), and TCP port (2000) [22].

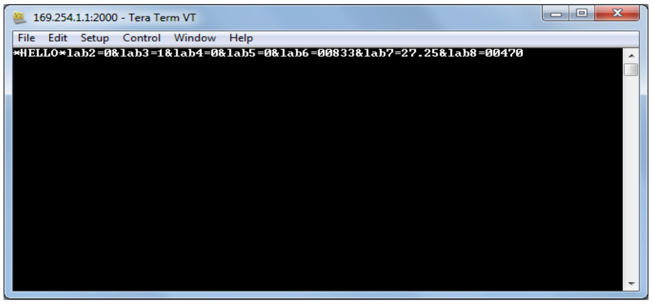


Figure 5. The value of the seven sensors using Tera Term screen.

Once the connection is linked with the Ad hoc mode, it might take up to one to two minutes to share an IP address with the computer. Next, click "OK" if the connection is successful. The program of Tera Term will show the message "HELLO". After that, the user can receive information from various sensors that were connected with the MCU and WI-Fly using program Tera Term. This also, displays the data regarding the environment and locations of the operator to the sensors.

2) *Setup Configuration through WI-Fly RN370 using iPhone:* To set [15] WI-Fly and iPhone using the Ad hoc Mode interface, it is not required to have the Access Point to set up the Wi-Fly network data together. The wireless appliance can accept information directly, and it is point to point communication.

Firstly, move Switch 1 Ad hoc to position "ON" in the WI-Fly and switch on the power supply. Secondly, the wireless network is connected with an iPhone via the WI-Fly. It is possible to build a wireless system with a Smartphone using Dynamic Host Configuration Protocol (DHCP).

The Smartphone will create an Ad hoc Mode using Service Set Identifier (SSID) and the associated WI-Fly holders of a number of IP addresses. In this case the client iPhone will be their IP address: 169.254.1.1. The sensing data is first collected by the MCU, and then sent to the Smartphone within the WI-Fly transceiver, as shown in Figure 6.

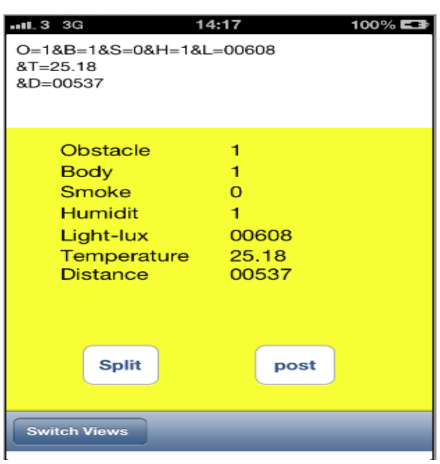


Figure 6. The value of seven sensors collected by iPhone.

VII. EVALUATION

The accuracy of the sensors' measurement is distinguished according to the performance of each sensor. The results will show how the accuracy can be faithful to the actual value. The most improved sensor has high quality of performance. To succeed, we must make a comparison with other evaluations and use real word results such as distance measuring meters to contrast with the ultrasonic distance sensor.

The results have been taken from some sensors, such as; obstacle, human body, brightness, temperature, and ultrasonic distance sensor; in order to further understand whether or not these sensors can work accurately according to their functions. The first experiment began with the temperature sensor to measure the room temperature. The results were measured at each hour from 9am to 8pm for three days. The results in Figure 7 show evaluation of the temperature sensor which took place for three days in the sensor system. The average measured temperature in the room during the three days in the morning and afternoon was recorded using temperature sensor (DSI-2B20). There was a rise in temperature between 20.5°C and 24.5 °C from 9am to 4pm. After that, the afternoon temperature shows a fluctuation between 4pm and 8pm with average temperature between 24°C and 24.5 °C. Generally, the graph illustrates that the average temperature is mostly high in the afternoon and low in the early morning.

A comparison can be made between the results of room temperature monitoring using the TC1046VNB sensor when the temperature rises up with a heater [10], and the result of this experiment for the same situation using the DS18B20 sensor. It can be understood that temperature increased when the heater began to warm up and started to drop when the heater was switched off.

For the ultrasonic distance sensor measurement Figure 8 shows the accuracy of measurement results between 5cm and 80cm by using an obstacle object to measure the distance between the sensor and the object. The sensor has the exact results between 5cm and 40cm. After that the sensor results vary from 45cm to 60cm, showing some errors with 0.9cm for each 5cm, then the measurement drops to 1.1cm, and starts to increase by 5cm up to 80cm. This sensor still needs more work to improve its accuracy and measuring of distance.

The third step was to identify whether the obstacle, human body and smoke sensors can be implemented for long distances using an ultrasonic distance sensor to measure the distance between the sensors and the object detection. The graph in Figure 9 shows how in this experiment the performance results of three sensors were initiated, from a distance of 5cm and then increased up to 80cm. The obstacle sensor can be interacted with the object from 5cm to 40cm with high voltage (1), than drops to (0) volt from 45cm to 80cm. However, the human body sensor can be attracted with the object between 5cm and 80cm with

TABLE I TEST AND EXPECTED RESULTS

Sensor Type	Function	Methods		Expected	Results
		Tear Term	iPhone		
Obstacle	Avoidance obstacle of object in line	✓	✓	0 or 1	1
Human body	Human body sensing	✓	✓	0 or 1	1
Smoke	Detection gas and smoke	✓	✓	0 or 1	0
Humidity	Humidity detection and raindrop	✓	✓	0 or 1	0
Light	Measure intensity of light	✓	✓	(0 - 1000) Lux	(0 - 753) lux
Temperature	Measure room temperature	✓	✓	(3 - 40) °C	(19.18 - 24.87)°C
Distance	Measure current distance	✓	✓	(0.2cm - 4m)	(0.2- 60) cm

(Note: √ represents acceptable)

high voltage (1). The smoke sensor was however not tested because there was no event related to this function in the room.

Another comparison was made [23], using light brightness sensors LDR to measure the light intensity during daytime. To evaluate the brightness sensor BH170 in this prototype system, the results were taken between 9am and 8pm with and without light in the room as illustrated in Figure 10 and 11, to show the performance of the light sensor to be used with LED light in the smart home and controlled by smart phone. In addition, the accuracy designates just how faithfully the sensor can measure the real world factor value.

Test results are shown in Table I. According to the information collected from the data, there are two methods of sensory perception. Firstly, the four sensors: obstacle, human body, smoke, and humidity express their results in a digital format, comprising factors of zero and one. Secondly, the temperature, brightness, and ultrasonic distance sensors produce results in an integer format.

VIII. CONCLUSION AND FUTURE WORK

A. Conclusion

This paper defined the different types of technologies and equipment related to the design system to control and to sense smart home appliance operated by Smartphone and personal computer. It was also used to sense unusual patterns during daily activities. This project offered a comprehensive wireless system from the Smartphone host user to the end appliance used by an elderly or a disabled person at home. Additionally, different aspects, such as methods elaborated in the smart home and methodology have been explored. Furthermore, four framework layers of architecture design have been explained according to their implementation in smart space. The module system has been integrated with some technology to build software and hardware systems, as well as requiring a user interface consisting of Smartphone and PC to be simple to use for elderly people. This investigation contributes to the following points:

- The system intends to implement smart home control at both a basic level, with active sensing, and at a higher level, which also includes user home automation.
- The system aims to create a convenient and inexpensive development within the area of home sensing system.

B. Future Work

The next stages will be setting the network connection wireless adapter with wireless router and server. After that, a MySQL database table will be created to receive the script language code, which will be run by PHP. And then, with the network the sensor data from the mobile can be sent to the server and saved in the database for computing tasks.

Moreover, extra works have been decided on for experiment and investigation in the next steps, such as using an ultrasonic distance sensor to make it more accurate to measure up to 4m, as well as assisting with the human body and obstacle avoidance sensors for monitoring issues. Home automation is a part of the research; therefore some appliances will be involved in the prototype, such as actuator to control the fan, LED light and heater using Smartphone to assist the occupant. Another future piece of work, will be computing algorithms to investigate reliability and usability which has been necessitated by information from various sensors and the control of electrical devices. Finally, other Smart phones such as, Android and BlackBerry will be involved in the system design.

ACKNOWLEDGMENT

I would like to express my deep gratitude and respect to Zhaozong Meng whose advice and insight was invaluable to me, because of all I learned from him. I would also like to thank his assistant for the expert guidance.

REFERENCES

[1] H. Medjahed, D. Istrate, J. Boudy, J.-L. Baldinger, and B. Dorizzi, "A pervasive multi-sensor data fusion for smart home healthcare monitoring," in *Fuzzy Systems (FUZZ), 2011 IEEE International Conference on*, 2011, pp. 1466-1473.

[2] U. Nations, "World Population Ageing 2009 " *Economic and Social Affairs,* 2010

[3] M. A.-Q. a. J. S. Jeedella, "Integrated wireless technologies for smart home applications," *inTech*, p. 42, 2010.

[4] J. Nichols and B. A. Myers, "Controlling home and office appliances with smart phones," *Pervasive Computing, IEEE*, vol. 5, pp. 60-67, 2006.

[5] W. Z. Khan, Y. Xiang, M. Y. Aalsalem, and Q. Arshad, "Mobile phone sensing systems: a survey," *Communications Surveys & Tutorials, IEEE*, vol. 15, pp. 402-427, 2013.

[6] M. B. I. R. a. M. A. M. A. Muhammad Raisul Alam, "A Review of Smart Homes—Past, Present, and Future," *IEEE Transactions on System Man and Cypernetics-Part C:*, vol. 42, pp. 1190-1203, 2012.

[7] D. Ding, R. A. Cooper, P. F. Pasquina, and L. Fici-Pasquina, "Sensor technology for smart homes," *Maturitas*, vol. 69, pp. 131-136, 2011.

[8] L. B. a. F. P. Stephen Makonin, "A Smarter Smart Home:Case Studies of Ambient Intelligence," *IEEE CS*, p. 9, 2013.

[9] V. Könönen, J. Mäntyjärvi, H. Similä, J. Pärkkä, and M. Ermes, "Automatic feature selection for context recognition in mobile devices," *Pervasive and Mobile Computing*, vol. 6, pp. 181-197, 2010.

[10] S. Folea, D. Bordencea, C. Hotea, and H. Valean, "Smart home automation system using Wi-Fi low power devices," in *Automation Quality and Testing Robotics (AQTR), 2012 IEEE International Conference on*, 2012, pp. 569-574.

[11] A. L. Sawsan Mahmoud, Caroline Langensiepen, "Behavioural pattern identification and prediction in intelligent environments," *Elsevier Applied Soft Computing*, p. 10, 2013.

[12] N. Suryadevara, S. Mukhopadhyay, R. Rayudu, and Y. Huang, "Sensor data fusion to determine wellness of an elderly in intelligent home monitoring environment," in *Instrumentation and Measurement Technology Conference (I2MTC), 2012 IEEE International*, 2012, pp. 947-952.

[13] B. A. M. a. S. J. Brown, "Developing a well-being monitoring system—Modeling and data analysis techniques," *Elsevier*, p. 10, 2006.

[14] A. Gaddam, S. C. Mukhopadhyay, and G. Sen Gupta, "Trial & experimentation of a smart home monitoring system for elderly," in *Instrumentation and Measurement Technology Conference (I2MTC), 2011 IEEE*, 2011, pp. 1-6.

[15] Z. Jiang, X. Gu, J. Chen, and D. Wang, "Development of an Equipment Room Environment Monitoring System based on Wireless Sensor Network and Mobile Agent," *Procedia Engineering*, vol. 29, pp. 262-267, 2012.

[16] A. Rosendahl, J. F. Hampe, and G. Botterweck, "Mobile Home Automation-Merging Mobile Value Added Services and Home Automation Technologies," in *ICMB*, 2007, p. 31.

[17] R. Networks, "Wifly Serial Adapter RN-370 & RN-374," *Install Guide and User Manual*, vol. 1.00, p. 21, 2009.

[18] L. STC MCU, "STC89Cxx. STC89LExx Series MCU Data Sheet,," *Data Sheet*, 2011.

[19] M. Integrated. (2008). *DS18B20: programmable resolution 1-wire digital thermometer*. Available: http://datasheets.maximintegrated.com/en/ds/DS18B20.pdf

[20] C. Technologies, "Ultrasonic Ranging Module HC-SR04," *User's Manual*, vol. v1.0, p. 7, 2012.

[21] J. Zdziarski, *iPhone SDK Application Development: Building Applications for the AppStore*: O'Reilly Media, Inc., 2009.

[22] T. Teranishi. (2007, February). *Tear Term Version 2.3*. Available: http://logmett.com/index.php?/products/teraterm.html

[23] A. Goswami, T. Bezboruah, and K. Sarma, "Design of an embedded system for monitoring and controlling temperature and light," *Int. J. Electron. Eng. Res*, vol. 1, pp. 27-36, 2009.

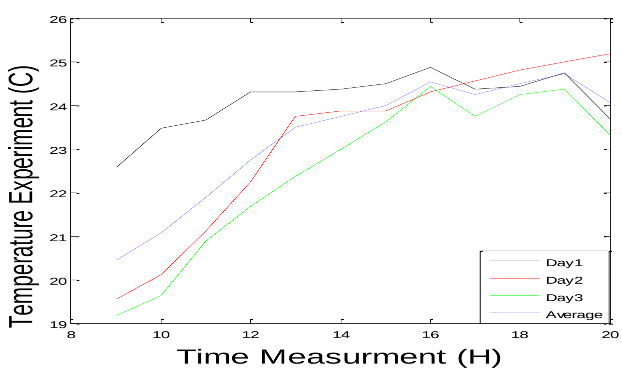


Figure 7. The evaluation of temperature sensor (DS18B20): (a) the temperature when the heater is on (b) the dashed line for average value

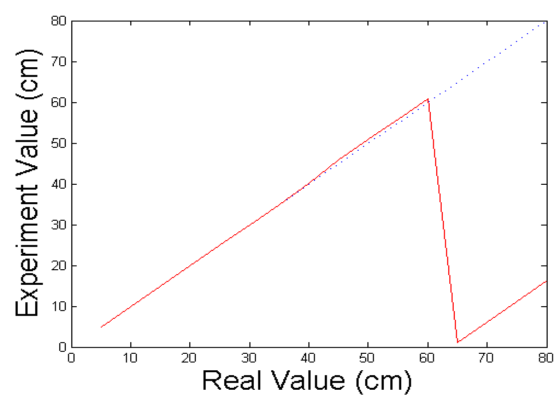


Figure 8. The ultrasonic measuring sensor and the dashed line is the real

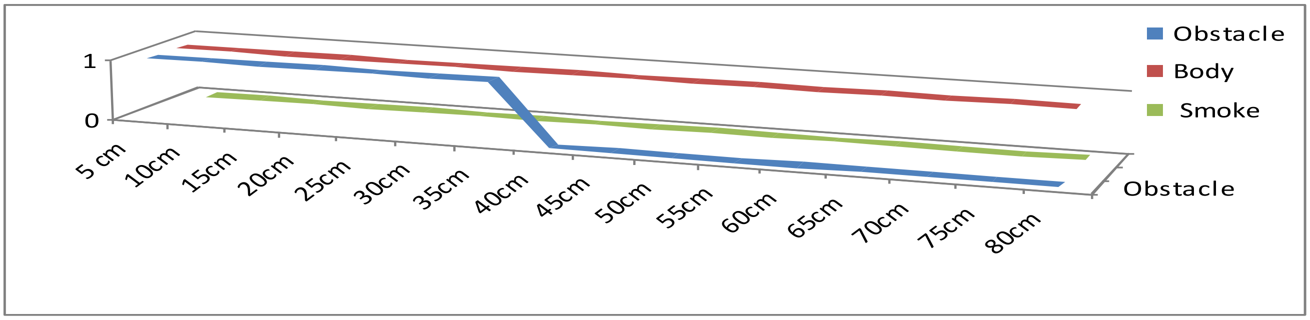


Figure 9. Illustrate the results of three digital sensors

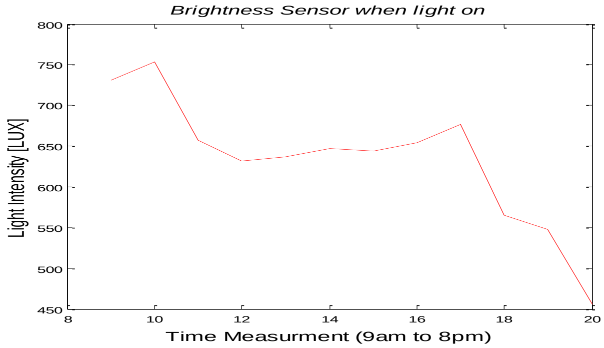


Figure 10. Graphical illustration of the brightness intensity during daytime with light

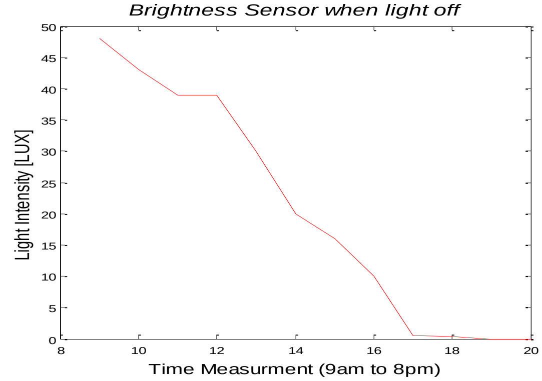


Figure 11. Light intensity during daytime without light.

 ISBN: 978-1-61208-365-0

Outage Probability of Full-duplex Systems in Multi-spectrum Environments

Jaeyeong Choi, Dongkyu Kim, and Daesik Hong
Dept. of Electrical and Electronic Eng., Yonsei Univ.
Seoul, Korea
E-mail: {jychoi1989, dongkyu, daesikh}@yonsei.ac.kr

Seunglae Kam
LG Electronics Co.
Seoul, Korea
E-mail: seunglae.kam@lge.com

***Abstract*—The goal of this paper is to investigate outage performance in a multi-spectral bi-directional full-duplex system (M-BFD). The system considered is two-way communication between two nodes equipped with a single shared antenna. Because full-duplex transmission is being employed, the required SNR associated with the target rate at each node for BFD is smaller than that for a bi-directional half-duplex system (BHD). In a single spectrum environment, therefore, BFD outperforms BHD in terms of outage probability. From a practical perspective, we investigate whether BFD remains advantageous over BHD in a multi-spectrum environment. We investigate the optimal spectrum selection strategy in terms of outage probability for M-BFD. The outage probability is derived as a closed-form expression under this selection strategy.**

The results show that the diversity orders for M-BFD and multi-spectral BHD (M-BHD) are identical. In the high signal-to-noise ratio (SNR) range, furthermore, the SNR difference between the outage curves for M-BFD and for M-BHD is shown to be inversely proportional to the number of available spectra, but in proportional to the target data rate.

***Index Terms*—bi-directional full duplex; multi-spectrum environment; spectrum selection.**

I. Introduction

Bi-directional full-duplex systems (BFD) have the potential to increase the system capacity of two-way networks with multiple antennas. In BFD, two source nodes simultaneously exchange signals by utilizing the same frequency resource [1]. If we assume that self-interference cancellation is perfect, BFD can achieve up to double the system capacity of bi-directional half-duplex systems (BHD). Numerous papers have shown the superiority of BFD over BHD in terms of system capacity [1]-[4], but system reliability is also a key metric in measuring system performance.

In BFD, it is inevitable that both nodes divide the spatial resources relatively into two subsets for simultaneous transmission and reception [1][2]. As a result, the achievable diversity order decreases, since the division reduces the number of transmit and receive antennas at each node.[1] In order to improve the achievable diversity order in BFD, a transmit antenna-switched receive diversity for the bi-directional beamforming scheme was proposed [6]. It was assumed that the antennas at each node are divided into two subsets which specifically perform only transmission or reception in [6]. Shared antennas can be exploited to avoid any division of spatial resources which causes diversity order reduction [7]. Throughout this paper, we will consider a two-way communication system equipped with a single shared antenna.

Recently, there has been growing interest in exploiting the multi-spectrum environment [8]-[10]. In [8], a closed-form expression of the capacity gain achieved from spectrum selection diversity was calculated in cognitive radio environments. In [9], a fair scheduling scheme was proposed in multi-spectrum environments. Those works argue that spectrum selection diversity can improve system reliability. In particular, the outage probability in a multi-spectrum system is investigated [10]. One way to enhance system performance, therefore, would be to bring BFD into the multi-spectrum network. Based on the above, BFD should also be considered in multi-spectrum environments. To the best of the authors' knowledge, however, there has been no investigation of the outage probability for M-BFD to date.

Multi-spectral BFD (M-BFD) requires an efficient spectrum selection strategy. The outage probability is defined as the probability that one of the SNRs at both nodes will be unable to support the required SNR [4]. For two-way communication in M-BFD, both nodes simultaneously utilize the same spectrum so that just one selection is needed. In a multi-spectral bi-directional half-duplex system (M-BHD), in contrast, each node independently selects the spectrum during its own transmission period so that twice as many spectrum selections are needed. In order to avoid outage events in M-BFD, both links should be considered simultaneously.

The remainder of this paper is organized as follows: Section II describes the system model. Section III investigates a spectrum selection strategy for M-BFD which minimizes the outage probability. Under this spectrum selection strategy, in Section IV, we will then derive the outage probabilities for M-BFD and M-BHD as a closed-form expression. We will also investigate the diversity orders and the asymptotic SNR difference between the outage curves for M-BFD and M-BHD. Finally, our conclusions are presented in Section V.

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MEST) (No. 2012R1A2A1A05026315).

D. Hong is the corresponding author with School of Electrical and Electronic Engineering, Yonsei University, Korea.

[1]Multiple input multiple output (MIMO) system with M transmit and N receive antennas; the maximum achievable diversity order is MN in a slow Rayleigh fading environment [5]. In BFD, at least one antenna at each node is used for opposite directional communication so that the maximum diversity order is $(M-1)(N-1)$ [6].

 ISBN: 978-1-61208-365-0

II. System Model

Let us first consider our two-way communication system. It consists of two transceivers, node a and node b, equipped with a single antenna [7]. Let $link_{ab}$ and $link_{ba}$ denote the data transmission links from a to b and b to a, respectively. We assume that each transmission link uses time T sec and one spectrum B Hz. We also assume the number of available spectra to be K.

Fig. 1 describes the M-BFD system [11]. Node a and node b simultaneously transmit and receive signals during time period T with the same selected spectrum from among K available spectra. We presume that the antennas at each node are able to transmit and receive signals simultaneously using a circulator in the BFD system with self-interference cancellation [7]. We also assume that the self-interference is perfectly eliminated as described in [1][2] and [6].[2]

Fig. 2 shows the M-BHD system. In order to perform two-way communication, M-BHD requires time $2T$ [1]. Each single time period of T sec is utilized for a single transmission link using the independently selected spectrum. In other words, during time $[0, T]$, node a transmits signals to node b through $link_{ab}$ using the selected k^H_{ab}-th spectrum. Then, during time $[T, 2T]$, node b transmits signals to node a through $link_{ba}$ using the selected k^H_{ba}-th spectrum.

$(\cdot)^F$ and $(\cdot)^H$ stand for $(\cdot)$ for M-BFD and M-BHD, respectively. The received signal at node i which is transmitted by node j, y_i $(i, j \in \{a, b\})$, can then be expressed respectively as

$$y^m_{k,i} = h^m_k x^m_j + n_i, \tag{1}$$

where $m \in \{F, H\}$. x_j is the transmitted signal from node j.[3] n_i is the additive noise at receiver node i and distributed as $\mathcal{CN}(0, \sigma^2)$. The channel coefficient for the k-th selected spectrum, h_k ($k \in \{1, ..., K\}$), is distributed as $\mathcal{CN}(0, 1^2)$. The channel state is constant in a single period, since it is assumed that the coherence time and the coherence bandwidth of each channel are T and B, respectively. Therefore, the h_k's are independent and identically distributed (i.i.d) Rayleigh fading. In M-BFD, the channel coefficients for both links are identical, since we assume channel reciprocity between both links [15]. Note that each node in M-BFD simultaneously receives signals during time $[0, T]$ while each node in M-BHD receives signals during different periods, $[0, T]$ and $[T, 2T]$, respectively.

[2]Up to 70dB of self-interference can be eliminated by isolating the antennas[7]. Since each node knows its own transmitted data, self-interference can be subtracted from the desired signal [12]. A number of papers have been published on practical full-duplex transmission [13][14].

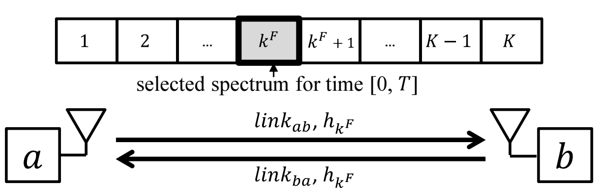


Fig. 1. M-BFD system model.

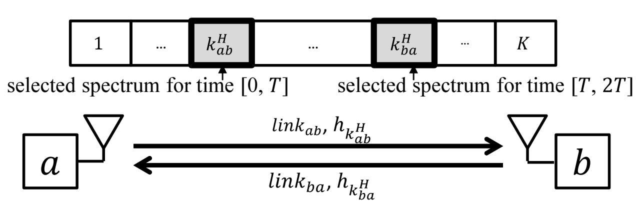


Fig. 2. M-BHD system model.

III. Spectrum Selection Criterion and Outage Probability

In this section, we investigate the spectrum selection criteria for M-BFD and M-BHD in order to minimize the outage probability. The outage probabilities are derived as closed-form expressions under the spectrum selection criteria, after which the diversity orders are then also derived.

A. Optimal Spectrum Selection Criterion in Terms of Outage Probability

In two-way communication, an outage occurs when one of the two links cannot support the required SNR, which is denoted by γ_{th} [4]. We assume that perfect CSI is available [16]. In this case, the outage probability, P_O, is expressed as

$$P_O = 1 - \Pr\left[\gamma_{k,a} > \gamma_{th}, \, \gamma_{k,b} > \gamma_{th}\right], \tag{2}$$

where $\gamma_{k,i} = \frac{|h_k x_j|^2}{\sigma^2}$ is the SNR at receiver node i utilizing the k-th selected channel.

Let us first consider the spectrum selection criterion for M-BFD. In M-BFD, the received SNRs at nodes a and b utilizing the selected spectrum both need to simultaneously support the required SNR, since each node utilizes the same time and spectrum resources. The outage probability can then be expressed as [10]

$$P^F_O = 1 - \Pr\left[\min_{i=a,b} \gamma^F_{k,i} > \gamma^F_{th}\right]. \tag{3}$$

In order to minimize the outage probability for M-BFD, we need to select the spectrum that maximizes the SNR for the weaker link. Therefore, the spectrum selection criterion for M-BFD can be expressed as

$$k^F = \arg \max_{k=1,\dots,K} \min_{i=a,b} \gamma^F_{k,i}. \tag{4}$$

In M-BFD, the SNRs at both nodes are identical, since we assume channel reciprocity between both links [15]. Therefore, without loss of generality, (4) can be expressed as

$$k^F = \arg \max_{k=1,\dots,K} \gamma^F_{k,a}. \tag{5}$$

[3]For the sake of fair comparison, the M-BFD has half the transmission power of the M-BHD, i.e., $\mathcal{E}\left[\left|x^F\right|^2\right] = \frac{P}{2}$ and $\mathcal{E}\left[\left|x^H\right|^2\right] = P$, where $\mathcal{E}[\cdot]$ stands for the expectation operator.

On the other hand, in M-BHD, note that the received SNRs at node a and b are independent, since the spectra can be independently selected at each node during different time periods. Therefore, the outage probability for M-BHD can be expressed as

$$P_O^H = 1 - \Pr[\gamma_{k,a}^H > \gamma_{th}^H] \Pr[\gamma_{k,b}^H > \gamma_{th}^H]. \tag{6}$$

In order to minimize the outage probability for M-BHD, each node should independently select the spectrum that maximizes the received SNR at the corresponding transmission time. The spectrum selection criterion for each link in M-BHD can then be expressed as

$$\begin{aligned} k_{ab}^H &= \arg \max_{k=1,\ldots,K} \gamma_{k,b}^H, \\ k_{ba}^H &= \arg \max_{k=1,\ldots,K} \gamma_{k,a}^H. \end{aligned} \tag{7}$$

From (5) and (7), we can observe the effects on the outage probability by the number of the available spectra. Both (5) and (7) can achieve full spectrum selection gain since the spectra which maximize the received SNRs are independently selected at each node during the corresponding transmission time periods.

B. Outage Probability

In this subsection, we derive the outage probabilities for M-BFD and M-BHD as closed-form expressions. We first consider the outage probability for M-BFD. As mentioned above, an outage occurs when one of the two nodes cannot support the required SNR. We define the target rate as R bps/Hz, so that the required SNR for M-BFD, γ_{th}^F, is $2^R - 1$. The received SNRs at node i in M-BFD are

$$\gamma_{k,i}^F = \frac{|h_k|^2 \frac{P}{2}}{\sigma^2} = \frac{|h_k|^2 \eta}{2}, \tag{8}$$

where η is the common SNR, which is expressed as P/σ^2. The $|h_k|^2$'s are modeled as i.i.d exponential random variables whose mean value is 1 because it is assumed that the h_k's are i.i.d Rayleigh fading. We define $f_{|h_k|^2}(x)$ as the PDF of $|h_k|^2$, which are expressed as e^{-x} and independent with respect to k. Then, using (3), (5), and (8), the outage probability for M-BFD can be expressed as

$$\begin{aligned} P_O^F &= 1 - \Pr\left[\gamma_{k^F,a}^F > \gamma_{th}^F\right] \\ &= 1 - \Pr\left[\max_{k=1,\ldots,K} |h_k|^2 > \frac{(2^R-1)}{\eta/2}\right]. \end{aligned} \tag{9}$$

Using (9) and order statistics [17], the outage probability for M-BFD can be expressed as

$$\begin{aligned} P_O^F &= 1 - \left(1 - \left(\int_0^{\frac{(2^R-1)}{\eta/2}} f_{|h_k|^2}(x)dx\right)^K\right) \\ &= \left(1 - e^{-\frac{(2^R-1)}{\eta/2}}\right)^K. \end{aligned} \tag{10}$$

In M-BHD, an outage occurs when one of the SNRs received at the two nodes cannot satisfy the required SNR at the corresponding transmission time. Since M-BHD utilizes double the time for two way communication compared to M-BFD, M-BHD transmission for each link needs to be performed twice as fast as that for M-BFD in order to achieve the same target rate. Therefore, the required SNR for M-BHD, γ_{th}^H, can be expressed by $2^{2R} - 1$. The received SNRs at node i for M-BHD can then be expressed as

$$\gamma_{k,i}^H = \frac{|h_k|^2 P}{\sigma^2} = |h_k|^2 \eta, \tag{11}$$

Using (6), (7), and (11), the outage probability for M-BHD can be expressed as

$$\begin{aligned} P_O^H &= 1 - \Pr\left[\gamma_{k_{ba}^H,a}^H > \gamma_{th}^H\right] \Pr\left[\gamma_{k_{ba}^H,b}^H > \gamma_{th}^H\right] \\ &= 1 - \left(\Pr\left[\max_{k=1,\ldots,K} |h_k|^2 > \frac{2^{2R}-1}{\eta}\right]\right)^2. \end{aligned} \tag{12}$$

Using (12) and order statistics [17], the outage probability for M-BHD can be expressed as

$$\begin{aligned} P_O^H(\eta, R, K) &= 1 - \left(1 - \left(\int_0^{\frac{2^{2R}-1}{\eta}} f_{|h_k|^2}(x)dx\right)^K\right)^2 \\ &= 1 - \left(1 - \left(1 - e^{-\frac{2^{2R}-1}{\eta}}\right)^K\right)^2. \end{aligned} \tag{13}$$

In the following subsections we will move on to investigating the outage probabilities with respect to diversity order and SNR difference the in high SNR regime.

C. Diversity Order

In this subsection, we derive the diversity orders for M-BFD and M-BHD in order to investigate the effect of the multi-spectrum diversity gain on the outage probability. We define the diversity order as the magnitude of the slope in the high SNR regime where the outage probability versus SNR is represented on a log scale [18]. We can define the diversity order, d, as

$$d = \lim_{\eta \to \infty} \left(-\eta \frac{\partial \log P_O}{\partial \eta}\right). \tag{14}$$

Substituting (10) and (13) into (14), the diversity orders for M-BFD and M-BHD can be derived respectively as

$$d^F = \lim_{\eta \to \infty} \left(-\eta \frac{\partial \log P_O^F}{\partial \eta}\right) = K \tag{15}$$

and

$$d^H = \lim_{\eta \to \infty} \left(-\eta \frac{\partial \log P_O^H}{\partial \eta}\right) = K. \tag{16}$$

Note that each system achieves the same diversity, K. This is because both M-BFD and M-BHD select one spectrum from among K available spectra in a single time period. It can be inferred that M-BFD and M-BHD are identically affected by

 ISBN: 978-1-61208-365-0

the number of available spectra in terms of reliability. On the other hand, M-BFD has half the transmission time compared to M-BHD with the given common SNR. Considering both reliability and transmission time, it can be inferred that M-BFD offers an advantage in two-way communications.

D. Asymptotic Difference Between Outage Probability

In this subsection, we investigate the asymptotic difference between the outage probability for M-BFD and for M-BHD. From (15) and (16), it can be inferred that the log-scaled outage probability versus the dB-scaled SNR curves for M-BFD is a shifted version of that for the corresponding M-BHD in the high SNR regime. We define the SNR difference between the outage probability curve for M-BFD and M-BHD as the *SNR gap*, $\Delta(R,K)$. We assume ζ as a desired outage probability for a given target rate R. Then,

$$P_O^F\left(\eta^F,R,K\right)=P_O^H\left(\eta^H,R,K\right)=\zeta, \tag{17}$$

where η^F and η^H denote the SNR values which achieve the desired outage probability for M-BFD and M-BHD, respectively. From Appendix A, the overall SNR gap can be obtained as

$$\Delta(R,K)=\underbrace{\frac{10\log_{10}2}{K}}_{\substack{spectrum\,selection\\ diversity\,gain\\ difference}}+\underbrace{10\log_{10}\left(2^R+1\right)}_{required\,SNR\,gain}-\underbrace{10\log_{10}2}_{power\,gain}. \tag{18}$$

Note that the SNR gap is determined by the number of available spectra and the target data rate. The SNR gap is in inverse proportion to K, but increases almost linearly along with R.

The first term of the SNR gap originates from the difference in the spectrum selection diversity gain between M-BFD and M-BHD. For two-way communication, both nodes in M-BFD simultaneously utilize the same spectrum so that just one selection is needed. In M-BHD, in contrast, each node independently selects the spectrum in its transmission time so that twice as many spectrum selections are needed. From this perspective, M-BFD is more advantageous with respect to avoiding outages than M-BHD. As K increases, the probability difference between the existence of a satisfactory spectrum in one time period and that in two consecutive time periods decreases. Therefore, as shown in (18), the gain decreases along with K.

The second term and the third term originate from the difference in the required SNR and power usage between M-BFD and M-BHD, respectively. The required SNR gain of M-BFD increases logarithmically with the ratio of the required SNR for M-BHD to that for M-BFD which can be expressed as 2^R+1. The negative constant power gain of M-BFD originates from the fact that both nodes in M-BFD transmit with half the power of those in M-BHD, as mentioned in (8) and (11).

We also find that the SNR gap has a non-negative value. This is because $\frac{10\log_{10}2}{K}\geq 0$ and $10\log_{10}\left(2^R+1\right)\geq\log_{10}2$, since K and R are non-negative. Hence, it can be inferred that M-BFD outperforms M-BHD in terms of outage probability.

IV. Numerical Results

In this section, we present the outage probabilities for M-BFD and M-BHD to verify our analysis. In the figures, the lines and symbols represent the theoretical results and simulation results, respectively.

Fig. 3 compares the outage probabilities for M-BFD and M-BHD according to the SNR with various numbers of available spectra ($K=1,5,10$). We set the target data rate, R, to be 1 bps/Hz. Each system has the same diversity order under fixed R and K. In addition, we can see that the outage probabilities for both systems decrease with the power of K. This means that the effect of the number of available spectra on the diversity orders in each system is equivalent, as shown

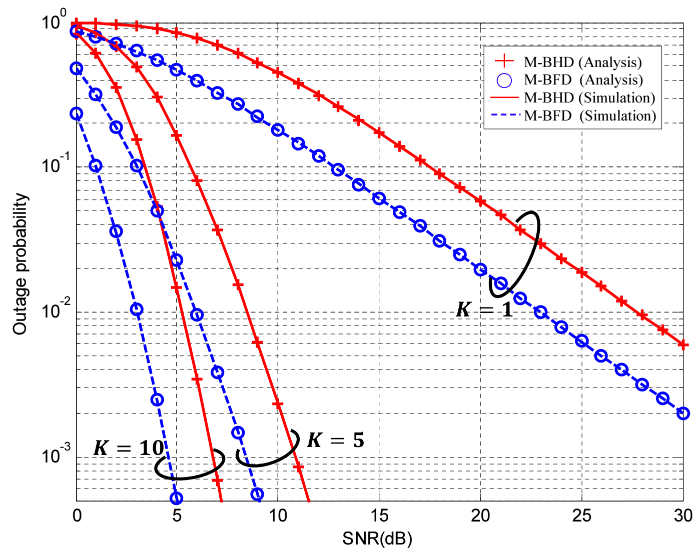


Fig. 3. Outage probabilities for M-BFD and M-BHD. (R = 1bps/Hz, K = 1,5,10)

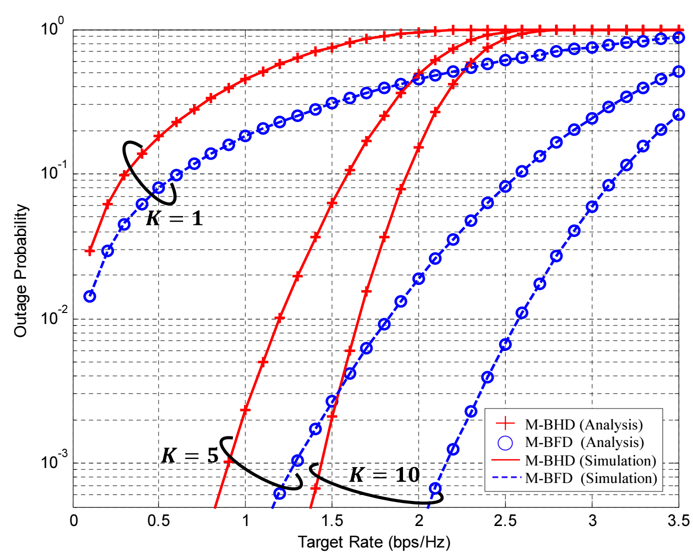


Fig. 4. Outage probabilities for M-BFD and M-BHD. (SNR = 10dB, K = 1,5,10)

in (15) and (16). The SNR gap decreases as K increases under fixed R and with the desired outage probability, but becomes saturated at $\log_{10}\left(\frac{2^R+1}{2}\right)$ dB as shown in (18). From these results, we can confirm that M-BFD outperforms M-BHD.

Fig. 4 compares the outage probabilities according to the target rate with various numbers of available spectra ($K = 1, 5, 10$). We set the SNR to be 10 dB. The difference in the achievable data rate between M-BFD and M-BHD increases along with K under fixed SNR and with the desired outage probability. This originates from the fact that the ratio of the required SNR for M-BHD on M-BFD for the desired outage probability increases along with K as shown in (10) and (13). From this result, it can be inferred that M-BFD can achieve a higher data rate compared to M-BHD, and that the difference increases along with K.

V. Conclusions

We investigated spectrum selection strategies for M-BFD and M-BHD in order to minimize outage. After applying the spectrum selection strategies, M-BFD was shown to be superior to M-BHD in terms of outage probability. Due to the smaller spectrum selection, M-BFD achieves a greater spectrum selection diversity gain than M-BHD despite the fact that the difference decreases along with the number of available spectra. A reduction in time usage due to simultaneous transmission at both source nodes leads M-BFD to achieve the required SNR gain at a better rate than M-BHD. The advantage of M-BFD expands at high target data rates with a large number of available spectra.

Appendix

A. Proof of the SNR Gap

Let ω be the ratio of η^H to η^F in high SNR regime which can be expressed as

$$\omega = \lim_{\eta^H \to \infty} \frac{\eta^H}{\eta^F}. \tag{19}$$

Substituting (10), (13) and (19) to (18), we can obtain

$$\begin{aligned}
&\lim_{\eta^H \to \infty} \frac{1-\left(1-\left(1-e^{-\frac{2^{2R}-1}{\eta^H}}\right)^K\right)^2}{\left(1-e^{-\frac{(2^R-1)\omega}{\eta^H/2}}\right)^K} \\
&= \lim_{\eta^H \to \infty} \frac{\left(2-\left(1-e^{-\frac{2^{2R}-1}{\eta^H}}\right)^K\right)\left(1-e^{-\frac{2^{2R}-1}{\eta^H}}\right)^K}{\left(1-e^{-\frac{(2^R-1)\omega}{\eta^H/2}}\right)^K} \\
&= 1.
\end{aligned} \tag{20}$$

Applying L'Hopital's rule, we have

$$2\left(\frac{2^R+1}{2\omega}\right)^K = 1. \tag{21}$$

From (21), ω can be obtained as

$$\omega = \left(\frac{2^R+1}{2}\right) 2^{\frac{1}{K}}. \tag{22}$$

The SNR gap in dB-scale, Δ, can then be expressed as

$$\Delta = 10\log_{10}\omega. \tag{23}$$

Substituting (22) to (23), the SNR gap is obtained as

$$\Delta(R, K) = \frac{10\log_{10}2}{K} + 10\log_{10}\left(2^R+1\right) - 10\log_{10}2. \tag{24}$$

From (24), we can investigate the SNR with respect to the spectrum selection diversity gain difference, required SNR gain, and power gain.

References

[1] H. Ju, X. Shang, H.V. Poor, and D. Hong, "Bi-Directional Use of Spatial Resources and Effects of Spatial Correlation," *IEEE Trans. Wireless Commun.*, vol.10, no.10, pp.3368-3379, Oct. 2011.

[2] H. Ju, D. Kim, H.V. Poor, and D. Hong, "Bi-Directional Beamforming and its Capacity Scaling in Pairwise Two-Way Communications," *IEEE Trans. Wireless Commun.*, vol.11, no.1, pp.346-357, Jan. 2012.

[3] A. Host-Madsen and J. Zhang, "Capacity bounds and power allocation for wireless relay channels," *IEEE Trans. Inform. Theory*, vol.51, no.6, pp.2020-2040, Jun. 2005.

[4] R. Vaze, K.T. Truong, S. Weber, and R.W. Heath, "Two-Way Transmission Capacity of Wireless Ad-hoc Networks," *IEEE Trans. Wireless Commun.*, vol.10, no.6, pp.1966-1975, Jun. 2011.

[5] L. Zheng and D. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Trans. Inform. Theory*, vol.49, no.5, pp.1073-1096, May. 2003.

[6] D. Kim, H. Ju, S. Kim, and D. Hong, "Transmit Antenna-Switched Receive Diversity for Bi-directional Beamforming in Two-way Communications," in *Proc. of the 47th Asilomar Conference on Signals, Systems, and Computers*, pp.19-23, Nov. 2013.

[7] D. Bharadia, E. McMilin, and S. Katti, "Full Duplex Radios," in *Proc. of the ACM SIGCOMM.*,pp.375-386, Aug. 2013.

[8] H. Wang, J. Lee, S. Kim, and D. Hong, "Capacity of Secondary Users Exploiting Multispectrum and Multiuser Diversity in Spectrum-Sharing Environments," *IEEE Veh. Technol.*, vol.59, no.2, pp.1030-1036, Feb. 2010.

[9] Y. Liu and E. Knightly, "Opportunistic Fair Scheduling over Multiple Wireless Channels," in *Proc. of IEEE INFOCOM*, pp.1106-1115, Mar. 2003.

[10] S. Lee, M. Han, and D. Hong, "Average SNR and Ergodic Capacity Analysis for Opportunistic DF Relaying with Outage over Rayleigh Fading Channels," *IEEE Trans. Wireless Commun.*, vol.8, no.6, pp.2807-2812, Jun. 2009.

[11] S. Kam, D. Kim, and D. Hong, "Bi-directional Full-duplex Systems in a Multi-spectrum Environment," submitted to *IEEE Trans. Veh. Technol.*.

[12] D. Kim, H. Ju, S. Part, and D. Hong, "Effects of channel estimation error on full-duplex two-way networks," *IEEE Trans. Veh. Technol.*, vol.62, no.9, pp.4666-4672, Nov. 2013.

[13] M. Jain, et al., "Practical, Real-time, Full Duplex Wireless," in *Proc. of the 17th annual international conference on Mobile computing and networking*, pp.301-312, Sep. 2011.

[14] M. Duarte, A. Sabharwal, V. Aggarwal, R. Jana, K.K. Ramakrishnan, C.W. Rice, and N.K. Shankaranarayanan, "Design and Characterization of a Full-duplex Multi-antenna System for WiFi networks," *IEEE Trans. Veh. Technol.*, vol.63, no.3, pp.1160-1177, Mar. 2014.

[15] M. Guillaud, D. Slock, and R. Knopp, "A practical Method for Wireless Channel Reciprocity Exploitation through Relative Calibration," in *Proc. of ISSPA*, pp.403-406, Aug. 2005.

[16] J. Peha, "Approaches to spectrum sharing," *IEEE Commun. Mag.*, vol.43, no.2, pp.10-12, Feb. 2005.

[17] A. Papoulis and S. Pillai, "Probability, Random Variables, and Stochastic Processes," , Tata McGraw-Hill Education, 2002.

[18] H. Lee, J.G. Andrews, E.J. Powers, "Information Outage Probability and Diversity Order of Symmetric Coordinate Interleaved Orthogonal Designs," *IEEE Trans. Wireless Commun.*, vol.7, no.5, pp.1501-1506, May. 2008.

Testing of feasibility of QKD system deployment in commercial metropolitan fiber networks

Monika Jacak

National Laboratory of Quantum Technology
Wrocław, Poland
jacak.monika@gmail.com

Damian Melniczuk
and Lucjan Jacak

Institute of Physics
Wrocław University of Technology
Wrocław, Poland
lucjan.jacak@pwr.edu.pl

Ireneusz Jóźwiak
and Piotr Jóźwiak

Institute of Informatics
Wrocław University of Technology
Wrocław Poland
ireneusz.jozwiak@pwr.edu.pl

***Abstract*—A description of test-assessment of TELECOM 1550 nm optical fiber used for a quantum channel in entangled Quantum Key Distribution (QKD) setup, EPR S405 Quelle (Austrian Institute of Technology) is presented. The system at work was observed and parameters related to dark quantum channel were collected by an appropriately designed test card. Series of measurements were carried out for various configurations of 1550 nm (optimal transmission wave-length) optical fiber patch-cord the same as used in standard metropolitan TELECOM networks including distances up to 6.5 km long. The particular attention has been paid to model the real lines with welding points and connectors in view of rigorous requirements regarded conservation of photon polarization in EPR S405 system. Tests allowed for assessment of Qantum Bit Error (QBER) level in standard telecommunication fiber infrastructure when trying to implement entangled QKD system vulnerable in particular to polarization perturbations. Another drawback, incommensurability of the central transmission wave-length in fiber with the wave-length of photons in EPR S405 system, was also assessed and the possibility of implementation of QKD EPR S405 system with 1550 nm optical fibers has been verified.**

Keywords–Quantum Key Distribution; TELECOM network; optical fibers; quantum cryptography; quantum entanglement; photon polarization

I. INTRODUCTION

Quantum cryptography is a newly developed field in the security information area [1]. It is closely related to progress in Quantum Information Processing (QIP) and utilizes advances in practical implementation of quantum technology [1][2]. Recently reported achievements in construction of large quantum computer additionally enhance significance of cryptography methods which would be resistant against attack of quantum computer. Such a technique is linked to quantum cryptography, which is regarded as absolutely safe, at least in theory. Growing importance of security of information in classical communication systems create also challenging problems for sufficient level of safety for communication at least for some special applications. In this regard, quantum cryptography also offers in principle unconditional safe protocols for secret key distribution which can be used for encryption/decryption of classical communication in OTP (One-Time-Pad) scheme. The quantum cryptography offers with this respect a method of quantum key distribution (QKD) over quantum channel of communication [1]. This channel is, however, extremely fragile and vulnerable to various perturbations. Requirement to ensure the sufficient level of so-called quantum coherency needed for error-less and safe communication is the major drawback of QKD technology severely limiting distance of quantum protected information exchange to ca. 100 km over uniform well selected laboratory optical fibers. Because TELECOM optical fiber networks used commercially in metropolitan communication systems do not meet prohibitive requirements for quantum communication as were provided in laboratory installations, there arose the question of assessment of possible usage of commercial already installed optical fiber networks to deploy QKD protected communication. This is the aim of the reported here investigation carried out in National Laboratory of Quantum Technology (Wrocław) in collaboration with a TELECOM company. In this report we summarize tests of commercial communication patch-cords of optical fibers supplied by the TELECOM company, which are the same as typically installed in metropolitan network. In particular, the tested lines where attributed with numerous weldings of fibers and standard connectors also typical in telecommunication practice. The length of tested quantum lines varied between several meters up to 6.5 km. The commonly used fibers works at transmission window close to 1550 nm (infra-red) and the usefulness of such fibers to apply as quantum channel was an especially important question to answer.

The object for testing was the QKD system on entangled photons, EPR S405 Quelle designed and manufactured by Austrian Institute of Technology (AIT) [3]. Verification of the possibility of application of commercial network fibers to establish dark quantum channel for EPR S405 Quelle system was performed with emphasizing the role played by polarization characteristics of optical fibers because the tested system employs polarization of photons as flying qubits for quantum Alice-Bob communication. The photon polarization has a fragile character and high level of coherence (conservation of particular quantum state) is required by QKD protocol utilizing quantum entanglement phenomenon in terms of photon polarization.

Moreover, the photons for the dark channel of communication in the original EPR S405 system have wave-length 810 nm near infra-red photons while the standard 1550 nm wave-length fibers poorly fit with their transmittance maximum to the carrying qubit photon wave-length. Therefore, to answer the question whether is it possible to use EPR S405 system in commercial networks 1550 nm, commonly utilized at present

 ISBN: 978-1-61208-365-0

in city networks in already installed optic fiber connections, seems to be of high significance for QKD practical implementation without additional cost for new connection lines better adjusted to photon wave-length.

II. Short characterization of QKD EPR S405 Quelle system

Generally, there are two types of QKD systems: one type create systems using nonentangled photons for dark quantum communication, and the second type–systems employing entangled pairs of photons. The former are more popular and encode quantum information in the phase of the light, additionally using quantum generator of random numbers for tossing the phase. In this sense, they are not strictly quantum and as a matter of fact it is not proved their equivalence to real quantum systems with discrete variables, though such a installations allow for successful implementation of the fundamental QKD protocol, BB84 [4] and its modifications like SARG04 [5]. The system on entangled photons is more fundamentally quantum, as utilizes completely nonclassical phenomenon of quantum entanglement. At present there is only one such system produced by Austrian Institute of Technology spin-off Vienna University conducted by Zeilinger's group [3]. This system called EPR S405 Quelle (the acronym EPR indicates linkage to commonly known Einstein-Rosen-Podolsky paradox positively resolved by experiment of Aspect in eighties of the last century [6]). Entanglement takes advantage of linear property of tensor product of Hilbert spaces, and corresponds to the decomposition of the wave function of larger system onto components related to subsystems A and B,

$$\Psi_{AB} = \sum_{i,j} c_{ij} \psi_A \otimes \psi_B. \quad (1)$$

Due to this simple property, none of two subsets A or B is its own pure quantum state as due to summation many various pure states of both systems $\psi_{A(B)}$ contribute to the total wave function Ψ_{AB}. The latter state is called as entangled if the formula (1) cannot be factorized [1]. In such a case, both subsystems are linked in quantum sense and have mutually exchanged information symmetrically imprinted in both (according to so-called Schmidt representation) [1][2]. The mutual dependence of entangled photons utilized in EPR S405 system provides higher level of security for QKD precluding possibility of some class of hacker attacks in the case of imperfect optoelectronics of cryptography devices. This costs, however, the lower tolerance for various, even small perturbations, because entanglement is extremely vulnerable and fragile. Therefore, a verification of stability of this system in conditions of real imperfect optical fiber networks is of particular importance. Two EPR S405 systems are installed and available in Wroclaw at NLQT WUT and in laboratory of CompSecur.

EPR S405 QKD system was designed to implement E91 protocol [7] accommodated to entangled carriers of information, i.e., flying qubits. In EPR S405 system, flying qubits are associated with polarization of photons because entangled pairs are created here in the process called *Parametric Down Conversion* [8] in a birefringent nonlinear crystal beta Barium Borate (BBO). In BBO crystal, a photon with energy $\hbar\omega$ decays upon nonlinear process into two photons, each with half the original energy $\hbar\omega/2$. Birefringence allows then for

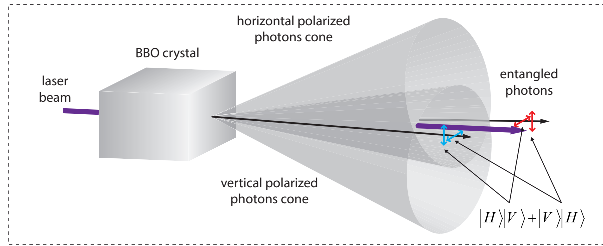


Figure 1. Generation of entangled photon pair in birefringent, nonlinear crystal BBO as a result of photon decay into two photons with half energy each; in the birefringent crystal there are created two conical photon beams with opposite polarization (upper beam with vertical polarization and lower beam with horizontal polarization); at the intersection of the cones, the states have not determined polarization—they are mixed states of entangled photons

creation of two conical beams, the upper one with vertical polarization and the lower one with horizontal polarization; see Fig. 5. At the intersection of the two beams the photons do not have a defined polarization and there are created entangled states of photons. In EPR S405 Quelle system there is used BBO crystal illuminated by laser diode (power 500 mW and wave-length 405 nm [violet]). The wave-length of entangled photons is thus 810 nm [near infra-red]. Photons are then separated by prism mirrors and guided along appropriately selected paths to realize E91 protocol. Generation of entangled photon pairs takes place in a component located in Alice station and still entangled photons travel then separately, one of them to the distant Bob station. Due to quantum link between both entangled photons any perturbation over the Alice-Bob channel could be detected by the counterpart photon at Alice which protect the system against eavesdropping by third party (Eve), but also rises sensitivity to any noise caused decoherence. EPR S405 Quelle system allows to organize communication between Alice and Bob blocks over quantum fiber channel or, alternatively, with telescope open-air connection. According to the producer (AIT), fiber connection has the range of about 50 km, while telescopic connection has the range of approximately 1 km (provided little optical perturbations along the open-air connection) [3]. In EPR S405 Quelle system, Alice block is more complicated than Bob one—it contains a component generating pairs of entangled photons. Although Bob block is less complicated, both blocks contain complete sets of avalanche detectors (four in Alice station and four in Bob station). Each of the stations is connected to separate computers, which control the system and quantum key distribution process.

A. Why 1550 nm wave-length optical fiber networks?

EPR S405 set allows for two ways of transmitting photons between parties in quantum communication, depending on the user decision. If telescopes are chosen, there should be some modifications done compared to fiber connection (other configuration elements and classical channel do not need to be modified). However, for metropolitan communication network the optical fiber connections would be of more interest because of highly developed already infrastructure of a city communication systems.

For generating photon pairs in EPR S405 system it is used 405 nm laser beam which generates pairs of photons of 810 nm wave-length (in principle it could be shifted as the properties of BBO crystal are maintained in larger range and an application of another laser would result in distinct wave-length, accommodated to optimal Alice-Bob transmission requirements). 810 nm fits to the so-called first telecommunication window, which was suitable to transmit light within $800 - 900$ nm band. The problem with such a window is that fibers have relatively high losses at these wave-lengths. Further development of fiber networks led to proposing of the so-called second telecommunication window. This window is defined around 1300 nm wavelength. Current optical networks are, on the other hand, built based on 1550 nm window (called as third telecommunication window) because of better transmission properties of optical signal with this wave-length even over relatively long distances.

Even though the large incommensurability between photon wave-length and optimal transmission window in the present standard TELECOM networks it is interesting to verify efficiency of quantum communication over such lines. In the case of insufficient effectiveness of system work in such incommensurability condition one would take into account that the better matching of wave-length can be achieved by changing either the laser in the system or the network fiber. The latter solution is, however, especially inconvenient as connected with high cost of new large scale metropolitan network installation.

In the present report, we summarize the series of tests which have been carried out on the prototype system EPR S405 Quelle (AIT) using various configurations of standard 1550 nm wave-length optical fibers for quantum dark channel between Alice and Bob stations of the system. The parameters of the system functioning were collected using the specially designed data card and referred to the optimal functioning of the system at laboratory conditions. The main parameter is the Quantum Bit Error (QBER) which is observed in time when the secret key is created and distributed between Alice and Bob over the quantum channel. The collected series of measurements by use of this card allows for assessment of quality of the quantum communication over the fiber connection especially in view of coherence losses and polarization perturbations. This is a central problem, even more important than the signal attenuation caused by discrepancy of the optimal transmission window of the fiber with photon wave-length, because polarization is the information carrier in the considered system. Unpredictable perturbations of the polarization are induced due to birefringence of glass material of fibers connected with random strain in fibers and also by weldings and connectors typically used in conventional optical already installed networks. The measurement procedure and the results are presented in the following sections.

B. *Polarization of photons as flying qubit in quantum channel*

Using pairs of entangled photons to transfer information over quantum channel is based on E91 key distribution protocol [7]. The source of pairs of entangled photons sends one of the photons to Alice and the other one to Bob. The quantum state of photons is regarded as entangled one with respect to their polarizations. In the mixed state of single photon of the entangled pair none polarization is determined, i.e., this is a mixture of both mutually orthogonal polarizations according to rules of entanglement. Measurement of the polarization in this mixed state restores its value and violates entanglement. The same causes any perturbation and noise along the transmission line similarly damaging quantum coherence required for QKD protocol realization. In EPR S405 system the source is located in Alice block, but it may be installed as a separate element of the system somewhere in between Alice and Bob. The entangled photons are delivered to Alice and Bob detectors, in which their polarizations are measured in randomly selected ON bases (of two possible bases–vertical-horizontal and diagonal $\pi/4,\ 3\pi/4$). In the next step Alice and Bob use the public channel to determine only those of the measurements in which the same bases were selected by both parties, but not revealing the particular measurement results. That way a shared secret key is generated in a raw form, which then undergoes classical treatment (error correction and privacy amplification), identical to all cryptographic key generation procedures, including QKD. The first part of E91 protocol, although different in photon entanglement from standard BB84 procedure [4], is in fact equivalent to the latter. It is, however, believed that using entangled states positively influences security level, but it has not yet been proved with all details. Nevertheless, analysis of attack detections in case of entangled carriers indicates better performance of such systems. Ekert [7] suggested that his protocol security level could be increased by using Bell inequality [9], which is connected to quantum entanglement and direct application of this criterion for detecting a possible eavesdropper (unfortunately, it requires using a third basis and developing the system with more detectors) [10][11]. This approach also allows to directly verify entanglement of the states of photons emitted by the source.

The measure of quantum transmission quality is the total number of errors called Quantum Bit Error, shortly QBER, as in case of other QKD systems. To reduce its value there are used error correction procedures and privacy amplification procedures performed over public connection. The reasons of errors are technical imperfections of the system and possible eavesdropper. In case the number of errors exceed a preset error limit, the connection is considered to be eavesdropped and the whole key is discarded. In case the number of errors does not exceed the limit, correction procedures allow to eliminate errors efficiently (to any desired level), but at the cost of reducing the length of original raw key. The QBER achieving a fraction of percent up to single percent is considered as a result good enough to use the cryptographically generated quantum shared key in communication between Alice and Bob.

III. DESRCIPTION OF THE TEST PROCEDURE

A. *Control of polarization*

In the case of photon pair produced and utilized to communication in EPR S405 system, the mutual correlation of polarization of both counterparts of the entangled pair is fixed after measurement by Alice, which encoded a bit of cypher into it. This correlation can be, however, perturb in due of transmission of the photon to Bob in a fiber. This is caused by a polarization drift in the fiber due to its bending, strain induced birefringence, defects in connectors and in welding regions. Photons are still correlated, but we do not know at which angle. To restore perpendicularity we are using manual polarization controller.

 ISBN: 978-1-61208-365-0

After putting two perpendicularly aligned linear polarizers on both paths, we can restore original polarization correlation. To achieve it, we are changing polarization controller manipulators toward to minimize the number of counts on each path (on detectors which are counting photons with polarization perpendicular to applied by polarizers). After one obtains the values of counts as low as possible, one can, basing on the properly correlated photon number and the improperly correlated photons number, get the so-called visibility ratio (the ratio of these two amounts of photons). This ratio, when is higher than 0.9, is assumed as good enough to start communication over the quantum channel.

B. Methodology of the test—measured parameter

For quality assessment of quantum channel the observation of QBER (Quantum Bit Error Rate) value over some time is convenient. QBER is the most practical parameter displaying by the system software and describing the quality of quantum channel because it allows to estimate how much information could a potential eavesdropper get. This is because that any action of eavesdropper unavoidably causes errors which is registered and rises actual QBER. In situation when there is no eavesdropper, QBER indicates the influence of all perturbations caused by imperfections of optics and electronics in the system and in the quantum channel. Therefore, the QBER is a suitable characteristics for assessment of quality of transmission in the optical fiber used as the quantum channel. The varying in time QBER can be registered and displayed graphically by the use of special card gathering observed data and displaying them in the form of an appropriate chart.

C. Standard-mode working system

As the reference ideal quantum channel we used two 1 m long 810 nm patch-cords and we connected both parties (Alice and Bob subsystems) by them. Stable room temperature was maintained (around 20^{o}C). When short patch-cord connection is used, photon count numbers at both communication sides are at similar level (130 k to 150 k counts). In this case, we assume that the system works in an optimal manner without information losses in the quantum channel. Errors are cased only by other imperfections of the system out of the channel. After restoring-polarization-correlation as was described above, the system was restarted and the appropriate log-file from the observed process was written out in duration of around 15 minutes. Then, the system was stopped, the log-file was copied and used as an input file for GNU R script which was responsible for the extracting, formatting and plotting data.

As we see from Fig. 2, the corresponding process of generation of secret key using the quantum channel with wavelength 810 nm referencing short fibers in 15 minutes time window is stable, which we assume as the standard-mode of system operation.

D. Testing of 1550 nm wave-length fiber for quantum connection in EPR S405 system

For testing the ability to coherently transmit photons in commercially used telecommunication window (1550 nm), we have used SMF-28 fiber with the following parameters:

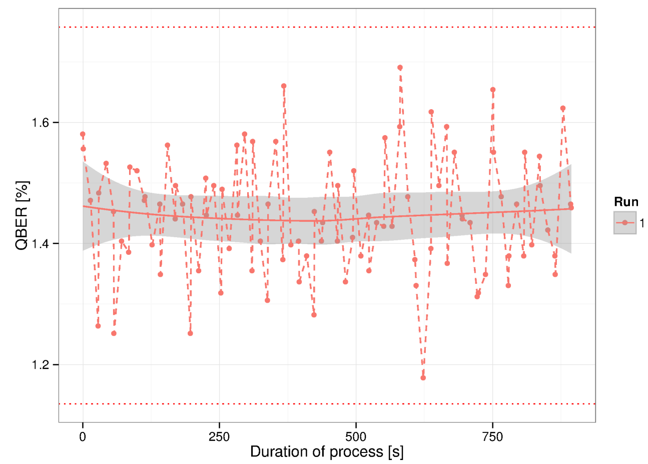


Figure 2. Plot of Quantum Bit Error Rate (QBER) in percents during functioning of EPR S405 system versus time measured in seconds. After termination of process, there were additional values calculated—local regression smoothing function (LOESS) with confidence interval and mean value with two lines: upper control limit (UCL) and lover control limit (LCL). Smoothing function is marked with solid line with gray area around which represents 95% confidence interval. UCL and LCL lines which are placed in distance 3 times standard error from mean value, are horizontal dotted lines. Since all data points are placed between UCL and LCL one can assume that plotted results were obtained in fairly stable process.

- core diameter [μm]: 8.2;
- cladding diameter [μm]: 125 $\pm$ 0.7;
- coating diameter [μm]: 242 $\pm$ 5;
- maximum attenuation for 1310 nm [dB/km]: 0.33 to 0.35;
- maximum attenuation for 1550 nm [dB/km]: 0.19 to 0.20;
- maximum attenuation for 1625 nm [dB/km]: 0.20 to 0.23;
- dispersion for 1310 nm [ps/nm km]: less than 1.0;
- dispersion for 1550 nm [ps/nm km]: less than 18.0;
- dispersion for 1625 nm [ps/nm km]: less than 22.0;
- temperature dependence [C]: -60 to +85;
- single fiber length [m] in patch-cord: 802 $\pm$ 10;
- number of weldings/connectors in patch-cord of 6.5 km for length: $5-7$.

Such fibers were fixed to the system output/input establishing in this way quantum connection between Alice and Bob. After restoring the proper polarization correlation before each measurement (in the same manner as described previously) and achieving an acceptable QBER level, we started recording the measurement of QBER value over iterating series of repeating process. The collected results are summarized and plotted in Fig 3, where three distinct runs of the system with 600 m length dark channel are illustrated. In Figs. 4 and 5, the QBER observation for dark channel 1550 nm fiber with length 200 m, 400 m and 800 m, for comparison are plotted.

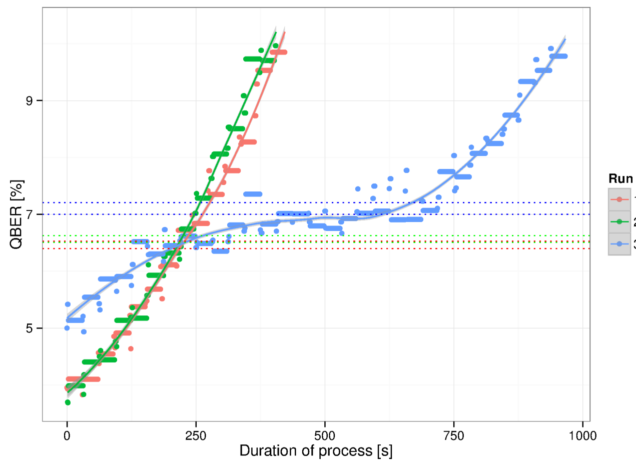


Figure 3. Improperly functioning system: plot of Quantum Bit Error Rate (QBER) in percents during three runs of EPR S405 system versus time measured in seconds. After termination of process, there were additional values calculated—local regression smoothing function (LOESS) with confidence interval and mean value with two lines: upper control limit (UCL) and lover control limit (LCL). Smoothing function is marked with the solid line (which color corresponding to color of data points) with gray area marked represents 95% One can notice the tendency to rapidly achieve critical level of QBER, precluding stable quantum communication.

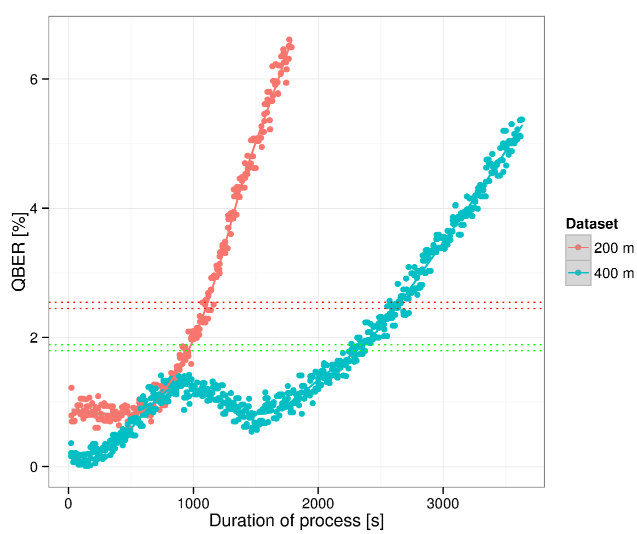


Figure 4. Multiple plots represents QBER measured for connection with 200 and 400 m (+- 10 m) optical fiber 1550 nm. Time window for measurement was one hour. Despite repeated measurements, connection based on shorter fiber was less stable. The shorter fiber brought higher ratio of polarization drift probably because of quality loss near FC/PC connectors.

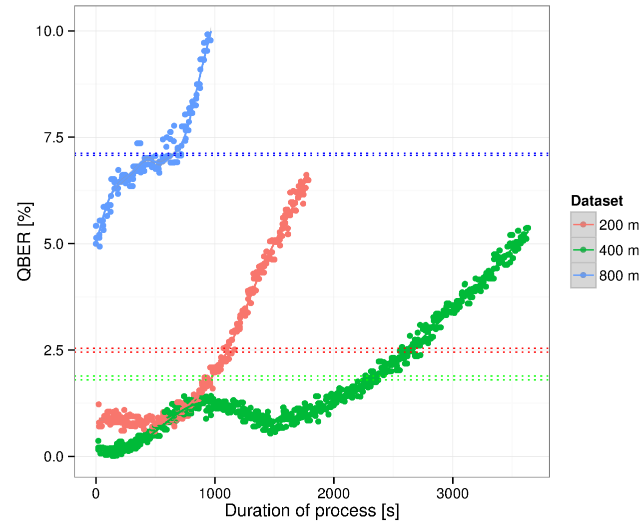


Figure 5. Multiple plots represents QBER observed for connection with 200, 400 and 800 m (+- 10 m) fiber 1550 nm. Time window for measurement was one hour. Despite repeated measurements, connection based on shorter fiber (200 m) was less stable than on two times longer fiber (400 m). The longest fiber produced accordingly to expectations the highest instability.

Control charts generated for above measurements show clearly that there are strong external or internal decoherent/destructive factors that are affecting the whole process. The initial QBER is quickly and continuously rising during the process. Moreover, after obtaining QBER value higher than 10 percent, the system stops because of too high value of error ratio. During the measurements 1 and 2 this too high value was obtained very quickly (after 454 and 438 seconds, correspondingly).

IV. Conclusion

Current implementation of entanglement photon pairs based key distribution system in EPR S405 suffers from the lack of efficient automatic polarization stability control allowing to instantly verify and improve quantum signal exchanges when connection between Alice and Bob uses standard 1550 nm fiber. By polarization stability, we mean ability to properly recognize pairs with perpendicular polarizations in both communicated parties, i.e., with required polarization correlation in the entangled pair after measurement. Without this ability, the data transmitted through the quantum channel are randomly identifying with constantly rising number of errors, which interrupts quickly the connection. To restore communication, the thorough and time-consuming manual regulation of polarization is necessary, which makes all the communication practically impossible.

To overcome this highly inconvenient tendency we propose to replace the manual polarization control with an highly-efficient automatic one. Automatic polarization controller would instantly compensate polarization drift and recover the system functionality. Such an improvement of the EPR S405 system would result in maintaining a sufficiently low and stable value of QBER ratio allowing entangled QKD over commercial network, though still for not longer distance than ca. 1 km and without weldings and connectors. The performed tests indicated also that in order to improve quality of 1550 nm quantum channel, the shift of wave-length of photons is necessary by application of lower energy laser activating BBO crystal. This would allow for better matching of optimal window for transmission of the standard 1550 nm fiber. As it follows from our tests, the welding decreases quality of quantum channel in a critical manner, which is probably connected with additional polarization mishmash due to a strain and imperfections in the region of welding or standard connections. Thus, for establishing of efficient quantum channel avoiding of weldings and connectors is necessary.

The polarization of optical signal turned out to be very unstable for the tested connections, which resulted in very rapid QBER rise precluding practical usefulness of this connection for secure quantum exchange of cryptographic key over practically significant distances. The main obstacle was the polarization decoherence as well as generally poor transmitting properties of 1550 nm fiber for much shorter wave-length photons used by EPR S405 system. As mentioned above, in order to maintain the quantum channel active very frequent manual corrections of polarization control were required so we expect that by designing and applying of an automatic polarization control module one would stabilize visibility ratio and lower QBER to an acceptable level conditioning. Such a solution together with the change of laser activation energy toward longer wave-length, might admit future implementation of entangled QKD systems in commercial networks.

References

[1] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. Cambridge: Cambridge UP, 2000.

[2] D. Bouwmeester, A. Ekert, and A. Zeilinger, The Physics of Quantum Information. Berlin: Springer, 2000.

[3] Austrian Institute of Technology, “AIT QKD Software project documentation,” 2010.

[4] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, 1984, p. 175.

[5] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, “Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations,” Phys. Rev. Lett., vol. 92, 2004, p. 057901.

[6] A. Aspect, P. Grangier, and G. Roger, “Experimental realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A new violation of Bells inequalities,” Phys. Rev. Lett., vol. 49, 1982, p. 91.

[7] A. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett., vol. 67, 1991, p. 661.

[8] D. C. Burnham and D. L. Weinberg, “Observation of simultaneity in parametric production of optical photon pairs,” Phy. Rev. Lett., vol. 25, 1970, p. 84.

[9] J. S. Bell, “On the Einstein-Podolsky-Rosen paradox,” Physics, vol. 1, 1964, p. 195.

[10] M. Curty, M. Lewenstein, and N. Lutkenhaus, “Entanglement as precondition for secure quantum key distribution,” Phys. Rev. Lett., vol. 92, 2004, p. 217903.

[11] A. Garg and N. D. Mermin, “Detector inefficiencies in the Einstein-Podolsky-Rosen experiment,” Phys. Rev. D, vol. 35, 1987, p. 3831.

Decision Making and Taking in Changing Ecologies Considering Network Law

Simon Reay Atkinson
Complex Civil Systems Research & Project Management Program, FEIT, University of Sydney,
Sydney, Australia
e-mail: simon.reayatkinson@sydney.edu.au

Gregory Tolhurst
Faculty of Law
University of Sydney
Sydney, Australia
e-mail: greg.tolhurst@sydney.edu.au

Liaquat Hossain
Information Management Division of Information and Technology Studies, The University of Hong Kong
Hong Kong
e-mail: lhossain@hku.hk

***Abstract*—This conceptual paper considers Law as different types of network and how an understanding of these networks, at the systems level, might assist in decision making and taking processes necessary for: information assurance; privacy; and, security applications in Law – as may be applied in Cyber through emerging legal networks. We first identify the systems we might be working with before considering Law as a networked ecology. We then look at law beyond existing stable, more certain and ruled jurisdictions and how it might be applied to decision making and taking in Cyber. We consider an example of how law may apply in areas of uncertainty and where existing jurisdictional remits may no longer apply e.g., in stateless jurisdictions. We conclude by considering how Legal Networks may assist in the decision making, taking and social problem solving processes in Cyber and so contribute to system resilience.**

Keywords-Collaboration; Network Law; Jurisdictional and Jurisprudential Networks; Fuzzy Logic; Ecologies; Resilience.

I. INTRODUCTION

This conceptual paper considers Law as comprising different networks and how an understanding of these networks at the *systems* level might assist in the decision making and taking processes with particular application in addressing complex problem solving such as recovery from recession and in Cyber. We first identify the systems we might be working with before considering Law as a networked ecology. We note that Europe has two different types of jurisdictional systems identified as *Common Law* and *Statutory / Codified* Law. We suggest that in recovering from recession, both these 'conceptual and normative tools [will be necessary] to [re]connect…Europe to its institutional design' [1]. Furthermore having both *Common* and *Statutory* Law may provide a unique European *co-adaptive* [2] advantage by providing the essential *variety* [3] for complex problem solving. Regeneration of Europe without enabling interaction between the two codes would potentially 'exclude large groups of citizens from the political process, but also, in the long run, destabilize and delegitimize the European…project' [1]. As John Dunne [4] comments, 'if a clod be washed away by the sea, Europe is the less'. This paper looks at law as networks and the lacunae that exist between and beyond largely state-based jurisdictions, e.g., in Cyber. We consider how such an approach might be applied to better managing instabilities, such as containing or preventing an epidemic or recovery from recession. We identify examples of how law and civil infrastructures and their associated networks may interact. We conclude by considering *Jurisprudential Networks* and *Network Law* and how their ecology may exist with similarly entangled legal networks.

Combined, the authors are thematic leads in the areas of complex systems, contract law, digital and cyber ecologies, the management of knowledge including commercial law, restitution and dynamic social networks. The authors' bring this knowledge to bear in the emerging area they posit to be 'Network Law' and 'Jurisprudential Networks'. Section II identifies the legal statutory and network systems and structures we may be working within before in the next Section examining law as a network. We then consider Law where it presently stands and as it may be applied in areas beyond the state and thereby more certain jurisdictional controls and enforcement. Finally, we consider what may be termed 'Cyber-in-Law' and scope how such legal ecologies may emerge and may assist the decision making and taking process.

II. SYSTEMS IDENTIFICATION

Communications literature maintains that hierarchical structures provide a superficial representation of how work actually gets done [5]. Similarly, Stacey [6] posits that dynamic organizations should be viewed as a collection of informal social networks (i.e., shadow structures beneath the formal structures); so allowing their elasticity to sustain continuous innovation and learning [7]. Using this as a basis for system identification, we consider decision making and taking as to 'how work gets done in networks'; 'how work may be organizationally gradated within Law', and finally, in terms of the two predominant 'codes' of law.

A. Abbreviations and Acronyms

Within organizations and networks, we consider one of the underlying principles to be that of *trust* and the trusts established between networks to allow *systems* to work without being ordered to do so. These systems we contend extend to include Law and its application. As identified by Shaw [8]:

> Perhaps the most important general principle, underpinning many international legal rules is that of *good faith*. This principle is enshrined in the UN Charter, which provides in Article 2(2) that "all Members…shall fulfill in *good faith* the obligations assumed by them in accordance with the Charter".

Similarly, the International Court declared in the *Nuclear Tests* case [9], *inter alia*:

> One of the basic principles governing the creation and performance of legal obligations, whatever their source, is the principle of *good faith*. *Trust* and *confidence* are inherent in international co-operation [we call collaboration], in particular in an age when this co-operation in many fields is becoming increasingly essential. Just as the rule of *pacta sunt servanda* [agreements must be kept] in the law of treaties is based on good faith, so also is the binding character of an international obligation assumed by unilateral obligation [10].

These understanding of trust are very similar to those developed by Augustin José Menéndez where he states, *inter alia*:

> The first [*instrument*] is the instrumental inclusion of *trust*. From the political perspective, *trust* needs to be developed in the EU, to *legitimize* majoritarian and redistributive politics and strengthen center-periphery relations. *Trust* both enhances societal compliance with transnational norms of cooperation and conformity, and at the same time provides the *common* framework in which transnational cooperation enables the construction of social institutions. This is…the implicit trust and understanding that comes from a continent full of citizens that interact, on a continuous and *intuitive* basis. And that sense of *mutual trust* that comes from communication, and communication alone, can further stabilize both the European space and legitimize the Union's position in it [1].

Mumford [11] considered an important *risk* factor to be *trust*: 'because innovation is frequently a journey into the unknown, *trust* is a major factor in its successful assimilation'. Contrastingly, Giddens [12] defines trust as 'confidence in the reliability of a person, or system, regarding a set of outcomes or events' and Mumford further observes 'risk and trust are inextricably intertwined'. Considering *good faith* as combining *trust* and *confidence* and taking forward Mumford, Giddens and Mintzberg's [11]-[13] understanding, it is suggested that:

> '*Trust* may be a function of the Likelihood of a person or system being able to comprehend, explain, understand [risk] by logic and deal with a set of outcomes or events' [14].

Therefore, *Risk* may be considered as obverse to *Trust*:

> '*Risk* may be a function of both the Likelihood of an adverse event occurring and a system or person's ability to comprehend, explain and understand [risk] by logic' [14].

We posit (after Hossain & Wigand [10]) that organizations need to be seen as dynamic (elastic and plastic) *social-influence* networks (*SINners*!) In these collaborative [14] networks, complex operations (requiring tacit knowledge exchange [15]), are achieved through social (and in this respect, also cyber-) interactions beneath the formal hierarchical control structures. *Co-adaptive* [2] viability in maintaining operational effectiveness and efficiency [16] may therefore depend more on how we socialize and capitalize 'our' formal (hierarchical) and informal (social) networks to achieve shared common goals. In this paper, we consider *law* as a network applying both formal coordination by control and rule (CRC) and informal collaborative social influence (CSI) networks [17]. We further identify, building on work by Harmaakorpi et al. [18] a 'techno-socio-economic paradigm', aligning significantly to CRC networks, in which:

> '*Info/Techno-Socio* (ITS) systems seek to *program* (as opposed to *programme*) the relationship between technical processes and humans by digitizing performance *fidelity* and coding for repeatable *risk free* procedures in computer-control-spaces so that data and communication do not [temporally] contradict each other' [14].

Info/Techno-Systems [19] are seen to be ideal for achieving "in time" coordination by control and rule (CRC). By contrast Socio-Info/Techno systems are seen to be capable of enabling collaboration (CSI), "over time", in which:

> 'Socio-Info/Techno (SIT) systems stress the reciprocal interrelationship between humans and computers to foster improved *shared awareness* for *agilely* shaping the social programmes of work, in such a way that humanity and ICT [control] programs do not contradict each other' [16].

Based on this understanding of the Cyber combining both CRC / ITS and CSI / SIT networks, it is considered Cyber-may comprise:

> 'A technologically bounded, largely immeasurable, strongly scientific, stochastic control space; comprising virtual-media and the display of data dealing with the *real* communication of *facts* and the *conceptualization* of other plausible possibilities, themselves capable of generating *strong* physical and *weaker* more social effects and *influencing* them' [20].

III. Jurisdiction and Jurisprudence

We consider *Jurisdiction* (from the Latin *ius*, *iuris* meaning 'law' and *dicere* meaning 'to speak') as the *practical authority* granted to a formally constituted legal body to make pronouncements on legal matters and to administer justice within a defined *legal environment*. It also refers to the inherent authority of a court to hear a case and to declare a judgment and the [sovereign] power to govern or legislate; make or enforce laws and the power / right to exercise authority in that *environment*.

We take a more specific understanding of *Jurisprudence* (*juris prudentia*) as being about the *ecology* of law, including its *cultural* and *social* underpinnings. In this understanding, we consider jurisprudence as acting in two interconnected ways:

1. *Interstitial* issues of law as a social organization and legal instrument relating to the local political, sûréte (considered in the French as including assurance, sureness, trusts, reassurance, safety and security) and economic (PŜE) [21] global social ecology in which it functions.

2. *Existential* issues of law as a *social institution* and *legal system* relating to the *global* political, sûréte and economic social *ecologies* in which it *functions*.

A. Statutory / Codified (Roman) Law and Common Law

We identify two predominant systems of law:

1. Common (Customary) Law is a *system* of laws originating from the English *Commonwealth* (or 'common weal / good') and based on court decisions, on the doctrines *implicit* in those decisions, and on *customs* and *usages* rather than on *codified* written laws. It is underpinned by a *jurisprudential* body of law responsible for *socializing* judicial *decisions* and *customs*, as distinct from those of *statute* law. Common-law courts base their decisions on prior judicial pronouncements rather than on legislative enactments. Under the doctrine of *stare decisis*, common-law judges are obliged to adhere to previously decided cases, or precedents, where the facts are substantially the same. Customary *practice* allows common law to *adapt* to the local *ecology*; at the same time, stare decisis provides certainty, uniformity, and predictability and makes for a stable jurisdictional *environment*;

2. Civil / Codified (Statutory) or Roman (Latin) Law is a legal system originating in Western Europe, intellectualized within the framework of 'late Roman law' (the Code of Justin overlaid by Germanic law and local *environmental* practices). The most prevalent feature is that its core principles are *codified* into a *referential* jurisdictional *system* which serves as the primary source of law. This contrasts with 'common law systems' whose intellectual framework comes from judge-made *decisional* law giving *precedential* authority to prior court decisions. *Codified* or *Statutory* law is written (as opposed to oral or customary); set down by a legislature / legislator and approved by its law creating *jurisprudential* body. Conceptually, codified law proceeds from social *abstractions*; to formulate general *environmental* principles that distinguish *substantive* (formal / *statutory*) from *procedural* (informal / *customary*) rules. It holds case law to be secondary and subordinate to statutory law. Consequently the judicial *ecology* is socially *inquisitorial* and *unbound* by precedent.

IV. LAW AS NETWORKS

From the above *systems* analysis it is possible to consider three different network *ecologies* operating across the law:

1. *Network Law* we consider to be: programmable / downloadable and to exist within current jurisdictions; connecting between existing jurisprudences and jurisdictions. It is codified / programmed entirely or largely by CRC / ITS systems, in which the main interaction is between IT, and IT and human users – with minimal involvement from the legal system, lawyers and solicitors.

2. *Jurisdictional Networks* we consider to 'have the authority and responsibility for making pronouncements on legal matters; administering justice within a defined *jurisdiction*; declaring judgments; legislating and enforcing laws *in time* within that *environment*. They are a distinct *entity* or *being* contained within existing jurisdictions and *connecting* between them and different jurisprudences – and which may create and have value by combining / *synthesizing* the existing historical legal codes, for example Common and Customary Law'.

3. *Jurisprudential Networks* we consider to be: '*entities* and *beings* with a responsibility for understanding the social and cultural underpinnings of the law. Over time these networks influence law and allow it to adapt to change, they promote *collaboration*. The concern of such networks is with law as a *social* organization and law as a *social* institution'.

A. Jurisdictional Networks

We consider legal networks as they may be applied through Common and Statutory legal systems through the associated executive, legislative, judicial and enforcement bodies. In this respect, we identify four *hard* coordination, rule and control *jurisdictional* networks: the *executive*; the *legislative*; the *judicial* and *enforcement*. In democracies, the executive is provided by the elected ruling party and the legislative by parliaments elected to hold the ruling party to account and to legislate. This forms the *legislative* jurisprudence. Responsible for implementing (the statutory legal system) and interpreting (the customary legal system) laws and connecting between the executive, the legislative and enforcement bodies is the judiciary. This forms the *judicial* jurisprudence. The third jurisprudence is provided by those responsible for enforcing civil legislation – which in most states includes policing, taxation, border, health, defense and social services administration. This is suggested to be the *enforcement* jurisprudence. Figure 1 situates the different legal 'beings' as vertically integrated, with the *public* jurisprudence – the conversation of public opinion and consent – lowermost. Also shown are the two different codes of law: one, Codified / Statutory Law which is more top down; the other, Common / Customary Law, which is more rhyzomic. Significantly, the *judicial* jurisprudence in both codes interprets and makes *social sense* of the law either through *inquisition* (Codified) or *precedence* (Common).

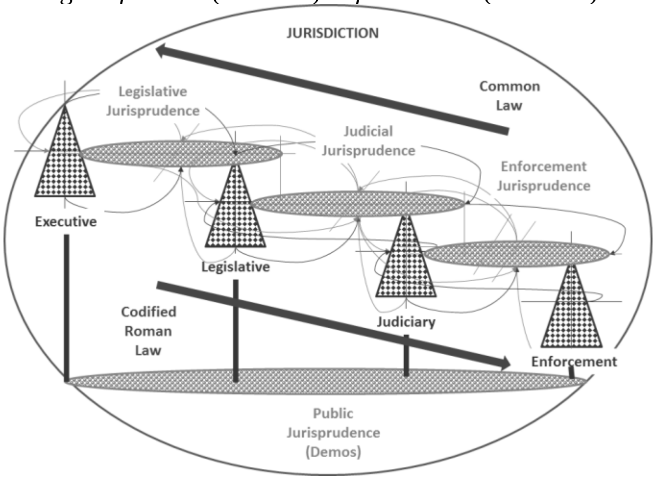


Figure 1. Jurisdictional and Jurisprudential Bodies

B. Jurisprudential Networks

We can identify three principal jurisprudential networks, the legislative, the judicial and enforcement, see Figure 2. At first glance this appears similar to the jurisdictional networks we identified. We do recognize that their responsibilities overlap. However, the jurisdictional networks are concerned with coordination and control (rank), while the jurisprudential networks are concerned with collaboration and influence (position). Examined from a horizontal perspective, *jurisprudential* responsibilities may be considered more in terms of position (than rank) and overlapping areas of responsibility. Significantly, this view also situates the Law within its *civil*, public and *social* settings. The *inquisitorial* and *precedential* interpretative roles of judicial jurisprudence also become clearer. Judicial jurisprudence connects between both *legislative* and *enforcement* jurisprudences. Specialist *soft* jurisprudence networks are identified to exist between the legislative and the judicial and the judicial and enforcement networks. We call these *Statutory* and *Customary* Jurisprudences. From a *Customary* and *Statutory* Law position, this analysis also identifies the priority given to the different judicial environments. Under *Statutory* Law, precedent is given to formal / codified rules and then to informal / customary ones. The position is reversed under *Common* Law, which gives precedent to informal *customs* and then to formally *codified* laws (the principle of *stare decisis*).

This research reinforced the position that 'for understanding and implementing cross-jurisdictional decision *making* and *taking* one needs to understand the different jurisprudences'. More precisely, one needs to interact at the jurisprudential level between both codes and specifically with the *statutory* and *customary* jurisprudences. This is not always well understood – for example the continuing struggle between the English Courts and British Parliament in implementing European Court of Human Rights statutes. Most significantly, it is the social and collaborative *jurisprudential* networks that enable the Law to be *seen as*, *shared* and practiced *justly*.

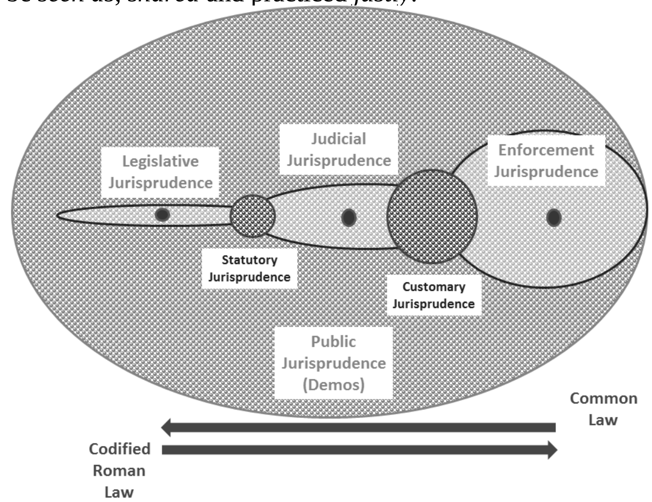


Figure 2. Jurisprudential Networks

V. Decision Making and Taking

There is a morality / ethicality to the decision making and taking process that is not always understood and rarely articulated [22]. Considering Boyd's simple OODA Loop (Observe, Orient, Decide, Act) [23] there are essentially two loops contained within the one. One loop (Loop 1) is the observe-orient-decision-make loop; the other the decision-take-act loop (Loop 2). Together, arguably, they preserve a moral and ethical basis with decisions being made and taken based upon the available facts and the three relatives (3Rs: time, timing and tempo):

Loop 1 may be the home of the diplomat, the public servant, the researcher, designer and planner [24]. Loop 1 can be described in terms of its focus upon the methodology, on managing the loop from observation (experimentation, for example) through to orienting the structure appropriately for a decision to be made. The danger in Loop 1 is its focus on the levers and structures of power not necessarily the agency / and agents necessary to implement and carry out its decisions or inform its designs [22].

Loop 2, by contrast, concentrates on decision-taking and action with no previous research or observation, scant regard for theory and philosophy and believes largely in the delivery of action through agency / agents in order to exploit the results. This is the home of the Neo-Cons, who focus on action as a means of changing the status quo in their favor and breaking existing structures, methods and processes they see as constraints to their behavior. Their emphasis is on controlling the perception and the narrative as a means of coordinating and dictating the process and methodology [22].

In an adaptive ecology, one would expect the decision making and taking process to be continuous. After Bunge [25] (who considers knowledge as social), the collaborative social, *decision making* phase may be described more by CSI / SIT networks, while the *decision taking* phase may be described more by coordination, rule and control (CRC / ITS) networks. In a legal setting, it may be suggested that the *jurisprudential* networks provide for reflection and adaptation and the *jurisdictional* networks the necessary order for coordination and control. This recognizes work by Gray [26] and Luttwak [27] 'that places emphasis on the importance of *strategic culture* in *networked social processes* and which underpin planning, *decision-making* and so *decision-taking*: good decisions are not capability driven' [28]. It is often these reflective, social networks that are *sacrificed* to *optimization* regimes that concentrate on *objective* metrication [16].

VI. CYBER-IN-LAW

Zadeh [29] noted *decision making* and *taking* has been dominated by Probability Theory, while Clark et al. [30] suggested that 'a new mathematical model, based upon vagueness, fuzzy sets and partial possibilities [dealing with uncertainty], may be required to advance the science'. Pólya, additionally recognized the relative ease of statistical programming for verification 'has tended to favor the heuristic [evidence based] reasoning of the mathematician rather than the inductive reasoning of the physicist' [31].

Cyber may be seen to consist of both the internet and the social networks that the internet supports; connecting between two poles. One sub-system may be identified and classified as being by **"**Coordination Rule and Control (CRC)" (akin to Network Law) (*explicit*); the other described as being through "Collaboration and Social Influence (CSI)" (akin to Jurisprudential Networks) (*implicit*) [32][33]. These system attributes provide the necessary and "requisite variety" [3] to enable both control, "in time", e.g., Just In Time (JIT), and influence [34]-[38], "over time".

Our research indicates that understanding the connections between these poles involves *Fuzzy Logic* (FL). Emerging from Probability Theory (PrTh) with its binary logic-sets Zadeh [39] put forward Fuzzy Logic where 'linguistic variables with a truth value ranging in degree between 0 and 1 may be 'managed by specific functions'. Its main conceptual difference with PrTh, is that *Fuzzy Logic* considers degrees of truth; *vagueness* (in terms of lack of specificity and not knowing precisely); *partial truth*; *partial possibility* [40] and *uncertainty*. Whereas, standard Probability Theory deals with the stochastic – thereby global – partitioning of certainties; not the understanding of partial possibilities or partial truths:

> 'Viewed through the prism of partiality, probability theory is, in essence, a theory of partial *certainty* and random behavior. What it does not address – at least not explicitly – is partial truth, partial precision and partial possibility – facets which are distinct from partial certainty and fall within the province of fuzzy logic. This observation explains why PrTh and FL are, for the most part, complementary rather than in competition' [29].

Noting the linkage between PrTh and FL since the 1990s Zadeh [29], recognized: 'the concerted drive toward automation [and control] of decision-making in a wide variety of fields [e.g., Cyber]…A side effect…is the widening realization that most real-world probabilities are far from being *precisely* known or *measurable* numbers'. Tong [41], had previously concluded that: 'Fuzzy models can be made to work…and, even in more complex situations (more variables or less data for example) they could capture basic behavior'. He considered them relatively simple to construct, being themselves quite simple structures whose greatest value lay in communicating process to others, where the linguistic value of a highly complex [Bayesian] model is doubtful. Tong went onto to suggest that fuzzy models are perhaps 'most valuable as tools for understanding basic characteristics rather than as detailed descriptions of process [and control] behavior'.

In law we may consider a road speed limit as an example of compliance / control by reason of certain sanction. People, generally, obey for fear of a fine if caught going over the limit [42], and the speed limit may result in a reduced number of accidents caused by speeding. We do not question the need for formal hard rules; every network needs such rules to operate *efficiently* [43]. A concern may be the extent to which it is possible to promote good behavior, including in Cyber and beyond state-based jurisdictions, based simply on Law. The set speed limit may not promote responsible driving; it may simply ensure people do not go over the speed limit; indeed, it may simply promote driving at the speed limit in all situations, regardless. Traffic conditions vary for many different reasons requiring drivers to *make* and *take* decisions about speed. In this case we are dealing with a complex system, for which a hard rule cannot regulate behavior. Hence, as noted, the resort to more fuzzy concepts [44] for dealing with *uncertainty* in more complex ecologies, such as exists in Cyber. We posit that it is the *trust* and confidence of CSI principles that are central to *influencing* people to act in a good and collaborative way – particularly in areas of uncertainty where reflective *learning* plays a key role. In saying this, we do not doubt that well-formed principles of CRC / ITS may help, particularly as regards to enforcement and providing guidance as to *fail-safe* protocols and procedures. We also note, though, that even enforcement agencies are influenced by CSI / ITS principles as they, too, are parts of the jurisprudential networks.

VII. NEW ECOLOGIES

We consider that in an *adaptive* system, the decision making and taking processes are continuous and part of an ecology continuously *testing* for both success and failure – so as to avoid catastrophic degradation. The law can be seen as a fixed immovable, post-hoc, *metricable* object like a castle. Examined from a *jurisdictional* point of view, the *objective* of law can be seen as 'controlling in order to rule' based upon the *representation* of evidence (data). The means have become the ends and the jurisdiction drives the strategy. What constitutes jurisdictional or process *knowledge* in law and control-engineering is not the same as what constitutes *knowledge* in strategy and so decision making and taking.

 ISBN: 978-1-61208-365-0

Strategic knowledge in Law, is vested within its *jurisprudential* social networks as it is within the social *techné* (expert 'know how'; subjective knowledge of how to 'changes things') and *phronesis* (reflective wisdom, which provides plausible explanation and guidance in times of uncertainty') contained within any successful organization. It is this co-*adaptive* knowledge that is so important in understanding decision making and taking.

We contend that there is a need in the 21st Century, to 'put humanity back in the loop', and that people will be employed more often in those *complex* lacunae where no amount of control, rule or coordination will *make* sense. We also see these as being the vital decision making and taking *commons* fundamental to delivering timely laws; design; strategies; and, policies that will prevail / pervade 'over time'. We also recognize that *resilience* does not come from the info-techno-socio control type networks but from investment in *socializing* and capitalizing our socio-info-techno influence networks. One cannot understand these *complex* systems without understanding their underpinning networks and how they are managed and *controlled*; *influenced* and *led*. Understanding how Law interacts at the project, unit, *jurisdictional* and systems *influence* and *jurisprudential* levels is therefore important. Not simply to aid understanding in times of crises, but to provide sustainable future programmes and to enable timely, collaborative, social responses to shocks and uncertainties, be they human-made or natural.

We consider Network Law as a *hard* entity contained within existing *Jurisdictional Networks* and *connecting* through IT between them and different jurisprudences. We suggest that they may have specific value in combining and synthesizing historical legal codes, such as Common and Codified Law. We do not advocate new laws, for example for Cyber, but for improved understanding and the establishment of connecting *soft* networks – hence, *Jurisprudential Networks* – to better socialize connections between existing jurisdictions, *Network Laws* and the cyber-internet. It is in the area of Cyber and Law that this paper makes a contribution and which, based upon the principles derived and outlined in this paper including for Fuzzy Logic and Fuzzy Law, that the authors are taking forward for application and future development.

ACKNOWLEDGMENT

We acknowledge in particular the Faculties of Law, Engineering and Information Management & Technology at the Universities of Sydney and Hong Kong.

REFERENCES

[1] Menéndez, A.J., "Review of Developments in German, European and International Jurisprudence", in Special Issue – Regeneration Europe M. Hartmann, and F. de Witte, Eds., German Law Journal: Berlin. 2013, pp. 441-712.

[2] Grisogono, A.-M., "Co-Adaptation". Proceeedings of SPIE - the International Society for Optics and Photonics, 16 January, 2006, vol. 6039, article no. 603903.

[3] Ashby, R., An Introduction to Cybernetics,1957, London: Chapman and Hall.

[4] Dunne, J., "Meditation XVII: Nunc Lento Sonitu Dicunt, Morieris". John Dunne (1572-1631), English, Roman Catholic convert to Protestantism, Lawyer, Diplomat, Poet, Vicar and Prolocutor to King Charles the First (of England), 1632, England.

[5] Stacey, E., "Collaborative learning in an online environment". Journal of Distance Education. 14(2). 1999, pp. 14-33.

[6] Stacey, R.D., Complexity and creativity in organizations, 1996, San Francisco, CA: Berrett-Koehler Publishers.

[7] Hossain, L., and R.T. Wigand., "Understanding virtual collaboration through structuration", in Proceedings of the 4th European Conference on Knowledge Management, 2003, pp. 475-484

[8] Shaw, M.N., International Law. 4th Edition, 1997, Cambridge, England: CUP.

[9] ICJ, "International Court of Justice (ICJ) Reports". ICJ Reports quoting International Law Research (ILR), 1974, pp. 253, 257-267; ILR p. 398, 412.

[10] Hossain, L., and R.T. Wigand., "ICT Enabled Virtual Collaboration through Trust". Journal of Computer Mediated Communication, JCMC 10 (1) November\. 2004, pp.22-31.

[11] Mumford, E., "Risky ideas in the risk society". Journal of Information Technology, 1996. vol. 11, pp. 321-31.

[12] Giddens, A., The Consequences of Modernity, 1990, Cambridge: Polity Press.

[13] Mintzberg, H., D. Dougherty, J. Jorgensen, & F. Westley, Some surprising things about collaboration - knowing how people connect makes it work better. Organizational Dynamics. Spring. 1996, pp. 60-71.

[14] Reay Atkinson, S., A.M., Maier, N.H.M., Caldwell, & P.J., Clarkson., "Collaborative trust networks in engineering design adaptation", in International Conference of Engineering Design, ICED11, 2011: Technical University of Denmark, Lyngby.

[15] Reay Atkinson, S., S. Lesher & D. Shoupe., "Information Capture and Knowledge Exchange: The Gathering Testing and assessment of Information and Knowledge through Exploration and Exploitation", in 14th ICCRTS: C2 and Agility, 2009, CCRP: Washington.

[16] Reay Atkinson, S., A. Goodger, N.H.M Caldwell, & L. Hossain., "How lean the machine: how agile the mind". The Learning Organization. vol. 19 issue: 3, 2012, pp. 183 - 206.

[17] Walker, D., S. Reay Atkinson, & L. Hossian., "Counterinsurgency through Civil Infrastructure Networks", in the Second International Conference on Social Eco-Informatics (SOTICS) October 21 - 26, 2012, SOTICS: Venice.

[18] Harmaakorpi, V., I., Kauranen, & A., Haikonen., "The Shift in the Techno-socio-economic Paradigm and Regional Competitiveness", in The 43rd Conference of European Regional Sciences Association (ERSA), 27-31 Aug, 2003, Helsinki University of Technology: Lahti Center, Jyväskylä, Finland.

[19] Ropohl, G., Philosophy of socio-technical systems, in Society for Philosophy and Technology. vol. 4, 1999, Virginia Tech: Blacksburg, VA.

[20] Reay Atkinson, S., Cyber-: "Envisaging New Frontiers of Possibility". UKDA Advanced Research & Assessmnent Group, 2009. Unpublished, Occasional Series, 03/09.

[21] Reay Atkinson, S., I. Hassall, N.H.M. Caldwell, M. Romilly, & R. Golding., "Versatile Modular System (VMS™) designs for a Versatile Modular Fleet (VMF™)" in paper presented at EAWWIV Conference, 2011, Old RN College, Greenwich, London.

[22] Reay Atkinson, S., Vakarau Levula, A., Caldwell, N.H.M., Wigand, R.T., & L. Hossain. "Signalling Decision Making and Taking in a Complex World", in International Conference on Information Technology and Management Science (ICITMS 2014), May 1-2. 2014. Hong Kong: WIT Transactions on Engineering Sciences (submitted).

[23] Fadok, D.S., John Boyd and John Warden: Air Power's Quest for Strategic Paralysis, ed. Air-University. 1995. Maxwell Air Force Base, Alabama: Air University Press.

[24] Reay Atkinson, S., "Returning Science to the Social". The Shrivenham Papers, UK Defence Academy, 2010. Number 10, July (July).

[25] Bunge, M.A., "Ten Modes of Individualism - None of Which Works - And Their Alternatives". Philosophy of the Social Sciences. 30(3). 2000, pp. 384-406.

[26] Gray, C.S., Weapons Don't Make War, in Policy, Strategy and Military Technology, Editor: Lawrence, 1993, University Press: Kansas.

[27] Luttwak, E.N., The Logic of War and Peace, Revised Edition, 2001, Cambridge, MA: Harvard University Press.

[28] Reay Atkinson, S., and A. Goodman., "Network Strategy and Decision Taking". ARAG Occasional, UK Defence Academy, 2008. 11 / 08.

[29] Zadeh, L.A., "Toward a perception-based theory of probabilistic reasoning with imprecise probabilities". Journal of Statistical Planning and Inference, vol. 105. 2002, pp. 233-26.

[30] Clark, T.D., J.M. Larson, J.N. Mordeson, J.D. Potter and M.J. Wierman., Applying Fuzzy Mathematics to Formal Modelling in Comparative Politics. Studies in Fuzziness & Soft Computing, 2008. vol 225: Springer.

[31] Pólya, G., Heuristic Reasoning in the Theory of Numbers, in Reprinted in: The random walks of George Pólya, G.W. Alexanderson, Ed., 1959 (2000), Mathematical Association of America: Washington, DC.

[32] Walker, D., S., Reay Atkinson, & L., Hossain, "Collaboration Without Rules - A New Perspective on Stability Operations", presented at IEEE Cyber Conference, 14-16 Dec, 2012, IEEE: Washington.

[33] Reay Atkinson, S., S., Feczak, A., Goodger, N.H.M., Caldwell & L. Hossain, "Cyber-internet: a potential eco-system for innovation and adaptation", in European Alliance for Innovation: Internet as Innovation Eco-System Summit and Exhibition, 4-6 Oct. 2012, EAI: Riva del Garda: Italy.

[34] Cartwright, D., Influence, leadership, control, in Handbook of Organizations, J.G. March, Editor, 1965, Rand McNally: Chicago. pp 1-47.

[35] David, P.A., "Path Dependence - A Foundational Concept for historical Social Science". Cliometrica -The Journal of Historical Economics and Econometric History, 2007. 1(2), Summer 07.

[36] Dahl, R.A., "The Concept of Power". Behavioral Science, 2:3, July. 1957, p. 201.

[37] Hossain, L., M., D'Eredita, and R.T., Wigand, "Towards a Product Process Dichotomy for Understanding Knowledge Management, Sharing and Transfer Systems in Organizations". Submitted to Information Technology and People, 2002.

[38] Wrong, D.H., "Some Problems in Defining Social Power". The American Journal of Sociology. vol. 73, No. 6 May. 1968, pp. 673-681.

[39] Zadeh, L.A., "Fuzzy sets". Information and Control, vol. 8(3). 1965, pp. 338-353.

[40] Ross, T.J., J.N., Booker, & W.J. Parkinson., Fuzzy Logic and Probability Applications: Bridging the Gap. Fuzzy Logic and Probability Applications. 2002. Philadelphia, PA: Society for Industrial & Applied Mathematics (SIAM). p. 209.

[41] Tong, R.M., "Analysis of Fuzzy Control Algorithms using the Relating Matrix", in CUED, 1976, Cambridge University: Cambridge.

[42] Schauer, F., "Do People Obey the Law", in Julius Stone Address, Sydney University Faculty of Law (unpublished): Sydney University, 13 March, 2014.

[43] Reay Atkinson, S., and J, Moffat, The Agile Organization, 2005, Washington: CCRP Publications.

[44] Waldron, W., "Vagueness and the Guidance of Action, in Philosophical Foundations of Language and the Law", A. Marmor, and S., Soames Eds., 2011, Oxford Scholarship Online, www.oxfordscholarship.com: Oxford, retrieved March 2014.

Flow Adjustment – a Flexible Routing Strategy for Demand Protection Against Multiple Partial Link Failures

Yoannn Fouquet* Dritan Nace* Michal Pióro†‡ Michael Poss*
* Laboratoire Heudiasyc UMR CNRS 7253, Université de Technologie de Compiègne, France
† Institute of Telecommunications, Warsaw University of Technology Poland
‡ Departement of Electrical and Information Technology, Lund University, Sweden
Emails :{yoann.fouquet, dritan.nace, michael.poss}@hds.utc.fr, mpp@tele.pw.edu.pl

***Abstract*—In this paper, we study a flexible routing strategy for demand protection and a corresponding optimization problem for networks that permanently experience fluctuations of the capacity available on their links. This is an important and novel topic as limited link availability is a fundamental feature of wireless networks; yet majority of work in survivable network design is restricted to total failures of single links. Hence, protection against partial failures of multiple links is considered as congestion avoidance. We assume a given finite set of network states. Each state is characterized by a vector of link availability coefficients specifying, for each link, the fraction of its nominal (maximum) capacity available in this state, and by a traffic coefficients vector specifying, for each demand, the proportion of its nominal traffic to be realized in the considered state. Our routing strategy allows for adjustment (thinning or thickening) of the reference path-flows. For a given nominal value x of a path-flow, its thickening is limited to τx where τ is a given constant greater than or equal to 1. Thus, in each state, the value of every path-flow can range from 0 to τ times its reference value. It turns out that the corresponding link cost minimization problem (where link capacities and state-dependant path-flows are decision variables) is NP-hard. We present a non-compact linear programming formulation of the problem together with a solution algorithm based on path generation. We illustrate the effectiveness of the introduced routing strategy by presenting numerical results for a set of representative network examples.**

Keywords-survivable networks; multiple partial link failures; multicommodity flow; linear and mixed integer programming; path generation.

I. INTRODUCTION

In this paper, we study a routing strategy for demand protection called Flow-Adjustment Routing (FAR) together with the corresponding network optimization problem. FAR aims at protecting traffic demands against Multiple Partial Link Failures (MPLF) by appropriate adjustment of the reference (nominal) path-flows. Strictly speaking, FAR is not a rerouting strategy because no paths can be created to restore the affected flows. Instead, the nominal path-flows are thinned or thickened according to the current state of the links. To account for MPLF, we consider a nominal state and a set of link availability states $\mathcal{S}$ (containing the nominal state) and a finite set A fractional numbers. For each link $e \in E$ and each availability state $s \in \mathcal{S}$, the corresponding link availability coefficient $\alpha_e^s \in A$ specifies the fraction of the nominal capacity of link e that is available in state s $(0 \le \alpha_e^s \le 1)$. FAR assumes that the nominal path-flows (i.e., path-flows defined for the nominal state with all links fully available) can be thinned or thickened to adapt to capacity fluctuations but not restored on paths not used in the nominal state. On top of this, we assume that the demand volumes to be realized in the availability states different from the nominal state are possibly reduced as compared to the nominal traffic. In the following, we use the terms *availability states* and *failure states* interchangeably.

For the so-specified setting, we study the corresponding optimization problem referred to as Flow-Adjustment Problem (FAP). FAP aims at minimizing the cost of links under the following constraints: (i) the nominal path-flows and the state-dependent path-flows satisfy the nominal and the state-dependent traffic demand requirement, respectively, (ii) path-flows obey the maximum thickening assumption of the protection strategy, and (iii) for each link and each availability state, the link load does not exceed the currently available link capacity. As FAP is NP-hard (because a special case of FAP shown to be NP-Hard is studied by Tomaszewski et al. [13]), its Linear Programming (LP) formulations (see Section III) are unavoidably non-compact and require path generation to be solved to optimality. For generating paths we need to apply a mixed-integer pricing problem—here the difficulty of FAP is manifested.

The introduced model is original. In fact, not much work has been done in survivable network optimization under the MPLF assumption. To the best of our knowledge, only the so called global rerouting (restoring flows from scratch in surviving capacity) has been studied in this context [1] – a strategy quite impractical in the considered wireless framework. It happens that multiple failures have so far been considered in survivable network design almost always (i.e., besides global rerouting) assuming total link failures $(\alpha_e^s \in \{0,1\})$. The work done here is substantial (again, see [1][5] and the references therein) but this case is, unfortunately, not relevant for our framework.

The rest of this paper is organized as follows. In the next section, we give motivation behind the considered flow-adjustment strategy. In Section III, we introduce the notation and formulate the basic FAP model. Section IV describes a path generation algorithm necessary to find optimal solutions for FAP. In Section V, we present results of a numerical study that illustrates a potential value of the considered protection strategy in terms of the cost of the resulting network in comparison with global rerouting. In Section VI, we present the performance of the restoration process using simulations. Finally, in Section VII, we present concluding remarks.

II. FLOW ADJUSTMENT- A SIMPLE PROTECTION STRATEGY FOR MULTIPLE PARTIAL FAILURES

The flow-adjustment routing strategy for MPLF proposed in this paper extends the Flow Thinning Routing strategy (FTR) presented in [2][3]. Both FTR and FAR are inspired by the idea of Elastic Rerouting (ER) presented in [4] and Path Diversity Protection (PDP) [1], [5]. We recall that both ER and PDP assume total link failures, i.e., failure scenarios which admit only binary vectors α_e^s characterizing the availability states (referred to as the failure states in this case) in $\mathcal{S}$ (i.e., $A = \{0,1\}$), that is, when links fail, then their entire capacity is lost. PDP is a protection strategy where in a failure state $s \in \mathcal{S}$ path-flows through the failing links are simply disconnected, and the surviving path-flows must be sufficient to realize the demand volumes, possibly decreased with respect to nominal demand volumes. ER allows for decreasing the flows of unaffected demands, as well as for increasing (to a certain threshold) path-flows of affected demands.

In this paper, we follow the concept of ER, but no distinction will be made between unaffected and affected demands. Hence, our strategy is allowed to thin or thick the nominal path-flow on any routing path. Thus, FAR assumes that each demand is in general routed over several paths, not necessarily disjoint, with over-dimensioned nominal path-flows to ensure an assumed level of demand survivability. Contrary to conventional end-to-end restoration strategies, no flow is rerouted to recover from a failure. In fact, it seems that allowing only for thinning makes the resulting protection strategy less complicated for network implementations. Our strategy is an extension of FTR in which the path-flows are allowed only to be decreased. Instead, FAR admits both thinning and thickening allowing for less costly networks as compared with FTR. Yet, FAR and FTR are similar from the mathematical modeling point of view, especially the mixed-integer pricing problem.

To clarify the idea of how FAR works, we wish to emphasize a few points. First, note that a common pool of link capacities is used for the nominal path-flows and in the remaining availability states. Hence, the selected routing paths carrying the flows are dimensioned so that the total traffic realized by the demand's path-flows could in general be greater than the nominal traffic. The most important feature of FAR is handling partial failures without any flow rerouting at all. In other words, no paths besides the nominal paths are used for handling other availability states. Therefore, the proposed approach results in using a sort of limited dynamic routing, adapted to the network states. To summarize, for each demand there is a fixed set of nominal routing paths carrying nominal flows. In an availability state in general only a part of the total nominal demand flow will be realized on these paths, depending on the available capacity and the required demand restoration ratio. Consequently, the restoration will be practically done by thickening some of the path-flows, and no new (re)routing paths are allowed.

III. FAP: FLOW-ADJUSTMENT PROBLEM

The basic problem considered in this paper is referred to as FAP and is as follows. We minimize the cost of link capacity assuming that in the nominal state of network operation all demand volumes are realized by means of (nominal) path-flows. When the network is subject to a failure from a given set of failure states (we assume that a failure state consists of partial failures of multiple links) then the demand volumes, possibly reduced, are realized for the duration of the failure state by appropriate thinning or thickening of the nominal flows. The detailed formulation of FAP will be given in Subsection III-B.

A. Notation

The considered network is modeled using a graph $\mathcal{G}(\mathcal{V},\mathcal{E})$, undirected or directed, composed of a set of nodes $\mathcal{V}$ and a set of links $\mathcal{E}$. In the sequel, we will always consider directed graphs unless stated explicitly otherwise. Thus, each link $e \in \mathcal{E}$ represents a directed pair (v,w) of some nodes $v,w \in \mathcal{V}$, and is assigned a non-negative unit capacity cost ξ_e which is a parameter, and a capacity reservation y_e which is an optimization variable. The cost of the network is given by the quantity $C = \sum_{e\in\mathcal{E}} \xi_e\, y_e$. The demands are represented by the set $\mathcal{D}$. Each demand $d \in \mathcal{D}$ is associated with a directed pair of nodes (end-nodes of d) $(o(d);\, t(d))$ for some $o(d), t(d) \in \mathcal{V}$; a volume h_d^0 (a parameter) has to be sent from $o(d)$ to $t(d)$ (demand volumes and link capacities are expressed in the same units). Also, each demand d is assigned a set of admissible paths $\mathcal{P}_d$ composed of selected elementary paths from $o(d)$ to $t(d)$ in graph $\mathcal{G}$. (Recall that an elementary path does not traverse any node more than once.) Paths from $\mathcal{P}_d$ are used to realize the demand volume h_d^0 by means of path-flows $x_{dp}^0, p \in \mathcal{P}_d$, which are optimization variables.

The given sets of admissible paths define the link-path incidence coefficients $\delta_{edp}, e \in \mathcal{E}, d \in \mathcal{D}, p \in \mathcal{P}_d$, where $\delta_{edp} = 1$ if path $p \in \mathcal{P}_d$ traverses link $e \in \mathcal{E}$ (i.e., if $e \in p$, treating the paths as subsets of links: $p \subseteq \mathcal{E}$), and $\delta_{edp} = 0$ if path $p \in \mathcal{P}_d$ does not traverse link e. It is important to note that the sets of admissible paths $\mathcal{P}_d, d \in \mathcal{D}$, are parameters in the FAP problem formulation considered in the sequel, although in general it assumes that all possible elementary paths can potentially be used if this is required to reach the optimum.

Network links are subject to (partial) failures. The failure-less state (with all links fully available) is called the nominal state and is denoted by 0, and the flows $x_{dp}^0, p \in \mathcal{P}_d$

are referred to as nominal flows. The set of failure states is denoted by $\mathcal{S}$ (we call set $\mathcal{S}$ the failure scenario). Each failure state $s \in \mathcal{S}$ is specified by a vector of link availability ratios $\alpha^s = (\alpha_e^s, e \in \mathcal{E})$, where $0 \le \alpha_e^s \le 1$ for $e \in \mathcal{E}$. The link capacity available in state s is assumed to be equal to $\alpha_e^s y_e$. Hence, α_e^s is the fraction of capacity y_e that survives in state s. Certainly, in state 0 all the ratios α_e^0 are equal to 1. In general, in a failure state more than one link can have its availability ratio less that 1 so in fact we are considering multiple partial failures of the network links.

When a failure state $s \in \mathcal{S}$ affects the network, in general not all the nominal flows $x_{dp}^0, d \in \mathcal{D}, p \in \mathcal{P}_d$ can be realized anymore as the available link capacity is decreased. It is assumed that the demand volumes to be realized in state $s \in \mathcal{S}$ can be decreased, to values $h_d^s, d \in \mathcal{D}$. The demand volumes assumed for a failure state must be realized by means of the nominal flows that are appropriately thinned (decreased) or thickened (increased) so to fit to the reduced link capacity. The thinned nominal flows for state $s \in \mathcal{S}$ are denoted by $x_{dp}^s, d \in \mathcal{D}, p \in \mathcal{P}_d$. These flows are allocated to the admissible paths for the duration of the failure state. The state-dependent flows $x_{dp}^s, s \in \mathcal{S}, d \in \mathcal{D}, p \in \mathcal{P}_d$ are optimization variables. The relation, for each demand $d \in \mathcal{D}$, is defined by a given demand-dependent flow control factor τ_d, where $\tau_d \ge 1$. Note that when $\tau_d = 1$, then, the reference path-flows of demand d can only be thinned. Still, when $\tau_d > 1$, they can be as well thickened, but only up to the factor τ_d so that, $x_{dp}^s \le \tau_d x_{dp}^0, s \in \mathcal{S}, d \in \mathcal{D}, p \in \mathcal{P}_d$.

B. *Formulation of FAP*

FAP assumes that in each failure state $s \in \mathcal{S}$, only a part h_d^s of the nominal volume h_d^0 has to be realized for each demand $d \in \mathcal{D}$. This is achieved by thinning or thickening the nominal flows x_{dp}^0 to values x_{dp}^s, $(p \in \mathcal{P}_d)$ so that the links capacities $\alpha_e^s y_e, e \in \mathcal{E}$ available in state s are not exceeded. For given sets of admissible paths $\mathcal{P}_d, d \in \mathcal{D}$, problem FAP can be represented by the following path-flow linear programming (LP) formulation involving variables $x_{dp}^0\ (d \in \mathcal{D}, p \in \mathcal{P}_d)$, $x_{dp}^s\ (s \in \mathcal{S}, d \in \mathcal{D}, p \in \mathcal{P}_d)$ and $y_e (e \in \mathcal{E})$:

$$\min \quad C = \sum_{e \in E} \xi_e y_e \tag{1a}$$

$$[\lambda_d^0 \ge 0] \quad \sum_{p \in \mathcal{P}_d} x_{dp}^0 \ge h_d^0,\ d \in \mathcal{D} \tag{1b}$$

$$[\pi_e^0 \ge 0] \quad \sum_{d \in \mathcal{D}} \sum_{p \in \mathcal{P}_d} \delta_{edp} x_{dp}^0 \le y_e, e \in \mathcal{E} \tag{1c}$$

$$[\lambda_d^s \ge 0] \quad \sum_{p \in \mathcal{P}_d} x_{dp}^s \ge h_d^s,\ d \in \mathcal{D}, s \in \mathcal{S} \tag{1d}$$

$$[\pi_d^s \ge 0] \quad \sum_{d \in \mathcal{D}} \sum_{p \in \mathcal{P}_d} \delta_{edp} x_{dp}^s \le \alpha_e^s y_e, e \in \mathcal{E}, s \in \mathcal{S} \tag{1e}$$

$$[\sigma_{dp}^s \ge 0] \quad x_{dp}^s \le \tau_d x_{dp}^0, d \in \mathcal{D}, p \in \mathcal{P}_d, s \in \mathcal{S} \tag{1f}$$

$$\text{all variables } x^0,\ x^s, y \text{ continuous},\ x^s \ge 0. \tag{1g}$$

In the formulation, the quantities in brackets on the left-hand sides are dual variables associated with the constraints (see Section I.2.2 in [5]). All these variables are, by assumption, nonnegative. Objective (1a) minimizes the total cost of links. Constraint (1b) makes sure that for each demand its paths have jointly sufficient capacity to satisfy the demand volume assumed for the nominal state. Constraint (1c) does not allow the nominal link loads to exceed the nominal link capacities. Next, constraint (1d) assures that in each failure state $s \in \mathcal{S}$, the adjusted flows are sufficient to realize the (possibly reduced) volume of each demand $d \in \mathcal{D}$. Then, constraint (1e) makes sure that in each state $s \in \mathcal{S}$, the surviving capacity of each link $e \in \mathcal{E}_s$ is not exceeded. Finally, constraint (1f) relates the state-dependent path-flows to the reference flows.

IV. PATH GENERATION

Formulation (1) is a link-path LP formulation. It is non-compact because of exponentially many path-flow variables x as we potentially consider all possible paths in the admissible path-sets $\mathcal{P}_\mathrm{d}, d \in \mathcal{D}$.

Thus, in order to consider all possible routing paths in graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$ in FAP, we need to apply the technique of linear programming known as column generation [7], [8], called Path Generation (PG) in our context. With PG, starting from some initial path-sets $\mathcal{P}_\mathrm{d}, d \in \mathcal{D}$, we generate new paths (corresponding to variables/columns $x_{dp}^0, d \in \mathcal{D}, p \in \mathcal{P}_d$ and $x_{dp}^s, s \in \mathcal{S}, d \in \mathcal{D}, p \in \mathcal{P}_d$), and iteratively add them to the path-sets. As discussed below, this is done by solving an appropriate pricing problem using, as parameters, optimal dual variables associated with constraints (1b)-(1f), i.e., an optimal solution $\lambda^*, \pi^*, \sigma^*$ of the problem dual to FAP formulated in the next subsection.

A. *Dual LP formulation of FAP*

The problem dual to LP (1) is as follows (see for example [1]):

$$\max W = \sum_{d \in \mathcal{D}} \Big(h_d^0 \lambda_d^0 + \sum_{s \in \mathcal{S}} h_d^s \lambda_d^s \Big) \tag{2a}$$

$$\pi_e^0 + \sum_{s \in \mathcal{S}_e} \alpha_e^s \pi_e^s \le \xi_e, e \in \mathcal{E} \tag{2b}$$

$$\lambda_d^0 + \sum_{s \in \mathcal{S}} \tau_d \sigma_{dp}^s \le \sum_{e \in \mathcal{E}} \delta_{edp} \pi_e^0, d \in \mathcal{D}, p \in \mathcal{P}_d \tag{2c}$$

$$\lambda_d^s \le \sigma_{dp}^s + \sum_{e \in \mathcal{E}_s} \delta_{edp} \pi_e^s, s \in \mathcal{S}, d \in \mathcal{D}, p \in \mathcal{P}_d \tag{2d}$$

$$\text{all variables } \lambda, \pi, \sigma \text{ continuous and nonnegative.} \tag{2e}$$

Let $\mathcal{D}(\mathcal{P})$ denote the problem defined by (2) for a given set of admissible paths $\mathcal{P} = \bigcup_{d \in \mathcal{D}} \mathcal{P}_d$ and let $\Pi(\mathcal{P})$ denote the (dual) polyhedron defined by constraints (2b)-(2e). Essentially, path generation is related to the so called dual separation problem. The problem consists in trying to find, for each demand d $\in \mathcal{D}$, a path $q(d)$ between $o(d)$ and $t(d)$ such that adding the constraints (2c)-(2d) for $q(d)$ to formulation (2) makes the current optimal solution of $\mathcal{D}(\mathcal{P})$ infeasible for $\mathcal{D}(\mathcal{P} \cup \{q(d)\})$ (see for example [1]). If there is no demand for which a path exists, then the current set $\mathcal{P}$ is sufficient to find the optimum of FAP admitting all possible admissible paths. The problem of finding paths $q(d)$, $d \in \mathcal{D}$ is called the pricing problem.

B. Pricing problem

Suppose λ, π, σ form an optimal solution of the dual problem $\mathcal{D}(\mathcal{P})$ defined by (2). Then, to be sure that π and λ form an optimal solution also for the dual problem with all possible paths, we need to check whether for each demand $d \in \mathcal{D}$, and for each path q in graph $\mathcal{G}(\mathcal{V}, \mathcal{E})$ between the nodes $o(d)$ and $t(d)$, there exist nonnegative numbers $\sigma^s, s \in \mathcal{S}$ such that:

$$\lambda^0 + \sum_{s \in \mathcal{S}} \tau \sigma^s \leq |q|^0 \tag{3a}$$

$$\lambda^s \leq \sigma^s + |q|^s, s \in \mathcal{S} \tag{3b}$$

$$\sigma^s \geq 0, s \in \mathcal{S} \tag{3c}$$

Above, $|q|^0 = \sum_{e \in q} \pi_e^0$ and $|q|^s = \sum_{e \in q} \pi_e^s, s \in \mathcal{S}$ denote the state-dependent dual length of path q (note that to simplify the notation we do not use the link-path incidence coefficients δ_{eq} here).

Certainly, for all paths $p \in \mathcal{P}_d$ the above inequalities fulfilled by $\sigma^s = \sigma^s_{dp}$ are a part of the considered optimal solution of (2). So the question now is how to find a path q outside the assumed set $\mathcal{P}_d$, if any, for which inequalities (3) are infeasible with respect to variables $\sigma^s, s \in \mathcal{S}$. In fact, in path generation it is advantageous (to speed up the PG algorithm, see Subsection III-D) to find, for each $d \in \mathcal{D}$, not only a path (if any) in $\hat{\mathcal{P}}_d$ that just separates the current dual solution λ, π, but rather a path $q \in \hat{\mathcal{P}}_d$ for which the dual constraints (2c) and (2d) are maximally violated by the considered dual solution λ, π (see [7], [8], [9]). This is especially true when finding such a path is not substantially more complex than finding an arbitrary path that violates the dual constraints. In our setting, the (negative) measure of violation of the dual constraints corresponding to path q is equal to

$$\|q\| = \left(\tau^{-1}|q|^0 - \sum_{s \in \mathcal{S}_q} |q|^s\right) - \left(\tau^{-1}\lambda^0 + \sum_{s \in \mathcal{S}_q} \lambda^s\right) \tag{5}$$

provided it is negative. The quantity $\|q\|$, is referred to as the generalized dual length of path q. Thus, the pricing problem for demand $d \in \mathcal{D}$ can be specified as:

$$\min_{q \in \hat{\mathcal{P}}_d} \|q\| \tag{6}$$

The so-formulated pricing problem (6) is difficult because of the particular form of the dual length $\|q\|$. Nevertheless, the problem can be stated as a binary program using formulation (7). In the formulation, binary variables $u_e, e \in \mathcal{E}$, specify the path q we are looking for: $q = \{e \in \mathcal{E}: u_e = 1\}$. Binary variables $z^s, s \in \mathcal{S}$, in turn, identify the set $\mathcal{S}_q$ corresponding to the so defined path q: $\mathcal{S}_q = \{s \in \mathcal{S}: z^s = 1\}$. Besides, $\delta^+(v)$ and $\delta^-(v)$ denote the sets of all links outgoing from, and all links incoming to, respectively, node $v \in \mathcal{V}$, and o is the originating node of the considered demand and t is its terminating node.

$$\min \quad L = \sum_{e \in \mathcal{E}} \left(\tau^{-1}\pi_e^0 + \sum_{s \in \mathcal{S}_e} \pi_e^s z^s\right) u_e - \tau^{-1}\lambda^0 - \sum_{s \in \mathcal{S}} \lambda^s z^s \tag{7a}$$

$$\sum_{e \in \delta^+(o)} u_e - \sum_{e \in \delta^-(o)} u_e = 1 \tag{7b}$$

$$\sum_{e \in \delta^+(v)} u_e - \sum_{e \in \delta^-(v)} u_e = 0, \ v \in \mathcal{V} \setminus \{o, t\} \tag{7c}$$

$$M z^s \geq \lambda^s - \sum_{e \in \mathcal{E}_s} \pi_e^s u_e, s \in \mathcal{S} \tag{7d}$$

$$u_e \in \{0,1\}, e \in \mathcal{E}, \ z^s \in \{0,1\}, s \in \mathcal{S} \tag{7e}$$

where M is a "big M" constant. Constraints (7b) and (7c) assure that variables u_e that are equal to 1 form a path from o to t. Constraints (7d) force each variable $z^s, s \in \mathcal{S}$, to be equal to 1 when the length, with respect to π^s, of the path q defined by variables u is smaller than λ^s. If we for a while assume that also $z^s = 0$ when the length, with respect to π^s, of path q is greater than or equal to λ^s, then it is clear that the objective function computes the value of the quantity $\|q\| = \tau^{-1}(|q|^0 - \lambda^0) - \sum_{s \in \mathcal{S}_q}(|q|^s - \lambda^s)$ (see definition (5)). The optimal solution u, z, L of (7) defines the optimal path $q = \{e \in \mathcal{E}: u_e = 1\}$ we are looking for, with L equal to its reduced cost.

C. Path Generation algorithm

The path generation algorithm for FAP is as follows:

Algorithm 1. Flow-adjustment problem

Step 1: Initialization
Define initial feasible path-sets $\mathcal{P}_d, d \in \mathcal{D}$.

Step 2: Solving
Solve the dual problem $\mathcal{D}(\mathcal{P})$ given by (2) to obtain dual variables λ and π.

Step 3: Update
For each $d \in \mathcal{D}$ solve the pricing problem (7). If the optimal objective L is negative, then add the resulting path q to the path-sets $\mathcal{P}_d$. If for any demand no new path has been added then stop: the resulting path-sets are sufficient to solve FAP to optimality. Otherwise, go to Step 2.

End

Figure 1. Path generation algorithm for FAP

V. NUMERICAL RESULTS

In this section, we present the results of a computational study illustrating the performance of FAR. The undirected network instances used in our tests and listed in Table 1 are taken from SNDlib [10].

TABLE I. NETWORK DESCRIPTION

Network	*Nodes*	*Links*	*Demands*
Net_10 (dfn-bwin)	10	45	90
Net_11 (di-yuan)	11	42	22
Net_14 (nobel-us)	14	21	91
Net_17 (nobel-germany)	17	26	121

In the following subsections, we will compare the Global Rerouting strategy (GR), the FTR strategy, and the FAR strategy in terms of cost-effectiveness. Recall that in a non-nominal link availability state, GR is allowed to restore flows for all demands in the available capacity from scratch, and that FTR is equivalent to FAR with $\tau = 1$. For the experiments reported in this section, we assume a uniform availability ratio α for all the affected links in a given availability state, i.e., $\alpha_e^s = \alpha$ for all $s \in \mathcal{S}$ and $e \in \mathcal{E}_s$ (where $\mathcal{E}_s$ denotes the subset of links affected in state s), and $\alpha_e^s = 1, s \in \mathcal{S}, e \in \mathcal{E} \backslash \mathcal{E}_s$. Also, we assume the demand satisfaction ratio $\beta = 1$, i.e., $h_d^s = \beta h_d^0 = h_d^0$ for all $d \in \mathcal{D}$ and $s \in$. In the comparisons, C_{FA}^{α} (respectively C_{FT}^{α}) and C_{GR}^{α} will denote the optimal value of the network cost for FAR (respectively, the network cost for FTR and GR) with the availability ratio fixed to α. GapFA (respectively, GapGR) gives the relative gain of the cost indicated by C_{FA}^{α} (respectively, C_{GR}^{α}) with respect to C_{FT}^{α} for a given availability ratio α : $GapFA = \frac{C_{FT}^{\alpha} - C_{FA}^{\alpha}}{C_{FT}^{\alpha}}$ and $GapGR = \frac{C_{FT}^{\alpha} - C_{GR}^{\alpha}}{C_{FT}^{\alpha}}$.

A. *Minimum network cost for single partial link failures*

We first consider the single partial link failures, as a reference to compare FAR with other rerouting strategies. We assume that each link can fail but one at a time, and when it fails its availability ratio is equal to α. Hence, the availability states can be identified with the links. In Figures 2-5, we present GapFA and GapGR as a function of α for 19 selected cases, varying α from 95% to 5%.

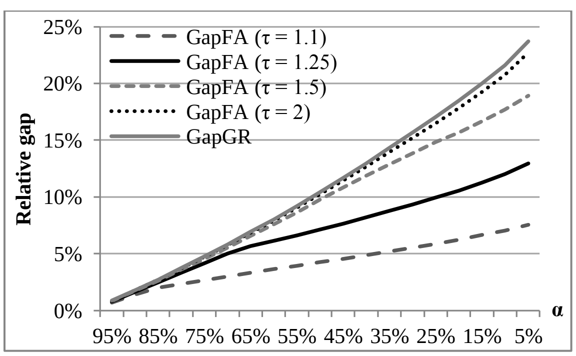


Figure 2. Relative gap between FAR, FTR and GR strategies for Net_10.

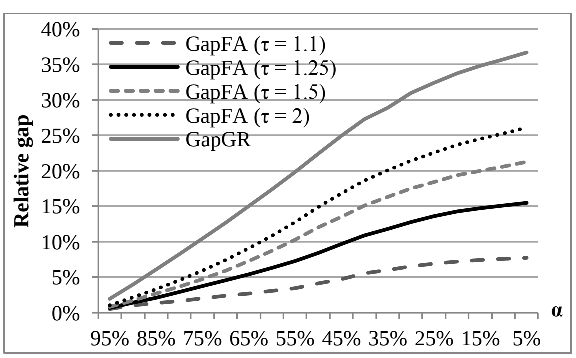


Figure 3. Relative gap between FAR, FTR and GR strategies for Net_11.

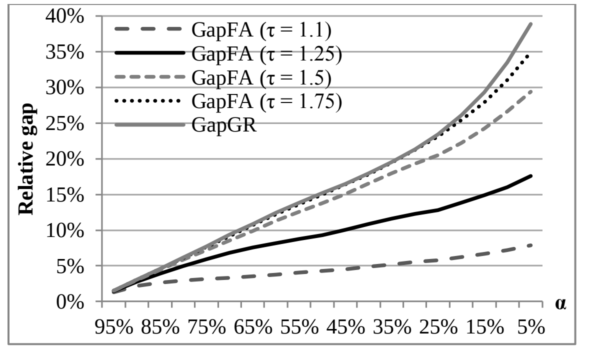


Figure 4. Relative gap between FAR, FTR and GR strategies for Net_14.

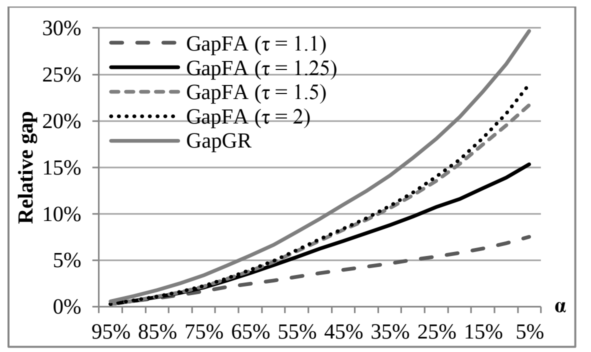


Figure 5. Relative gap between FAR, FTR and GR strategies for Net_17.

As illustrated by Figures 2 to 5, the overall cost of the network obtained when allowing thickening is substantially lower than that obtained using flow-thinning only, and this remains true for all considered availability scenarios and all networks.

It turns out that network topology and demand density characteristics have a significant impact on the efficiency of the flow-adjustment routing strategy. Net_10 and Net_14 have a high number of demands compared to their number of nodes (Net_10 has a full traffic matrix and Net_14 has a full undirected traffic matrix). For these networks the link cost optimized for FAR is close to the cost optimized for GR already for relatively low values of parameter τ (1.75 to 2). In contrast, Net_11 and Net_17 have a limited number of demands compared to their number of nodes and the optimal network cost for FAR requires a high value of parameter τ to meet the results of GR. We finally notice that for a sparse network with a high number of demands (as Net_17), allowing path thickening has a limited impact on the network cost for $\tau > 2$.

B. *Minimum network cost for single partial node failures*

We now consider single partial node failures (each node can fail but one at a time). This kind of failures represents a local perturbation in a network affecting several links at the same time. In this case, the availability states correspond to the nodes, and the link capacities in a failure state s are given by αy_e if e is incident to the failing node, and to y_e otherwise. In Figures 6-9, we present GapFA and GapGR as a function of α for 19 selected cases, varying α from 95% to 5%.

We notice that the graphs have similar shapes for all the considered networks. Indeed, the gain in the network cost using the flow-adjustment strategy increases until a certain threshold (which seems not to be dependent on the value of τ), and next decreases to 0% for full node failures (α=5%.) This shows that the flow-thinning strategy remains efficient for node failures for the extreme cases as sufficiently low or high perturbation levels. However, the gap between these two strategies and the global rerouting strategy is significant and reaches 80% to 90%, depending on the network, for a low availability ratio α=5%. (Recall that for $\tau \to +\infty$, the network cost for FAR converges to that of GR.)

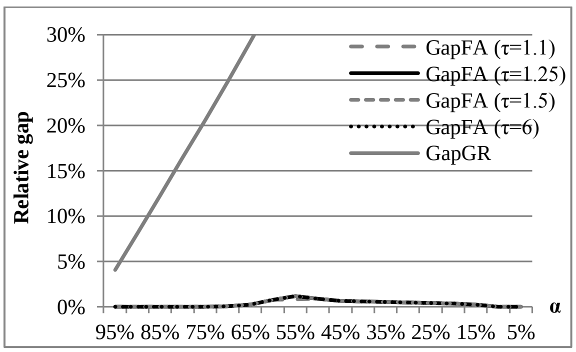


Figure 6. Relative gap between FAR, FTR and GR strategies for Net_10.

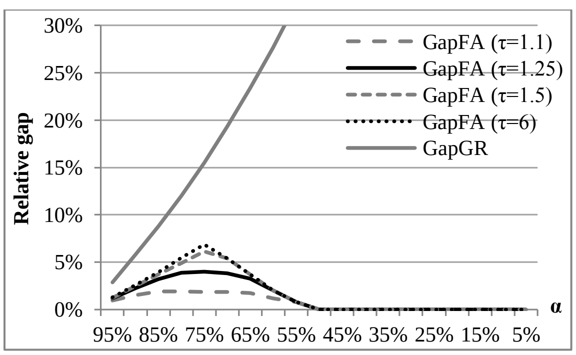


Figure 7. Relative gap between FAR, FTR and GR strategies for Net_11.

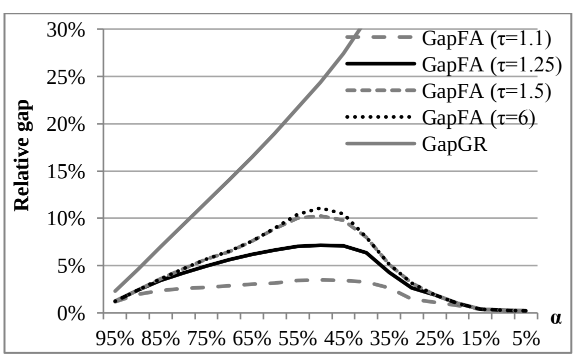


Figure 8. Relative gap between FAR, FTR and GR strategies for Net_14.

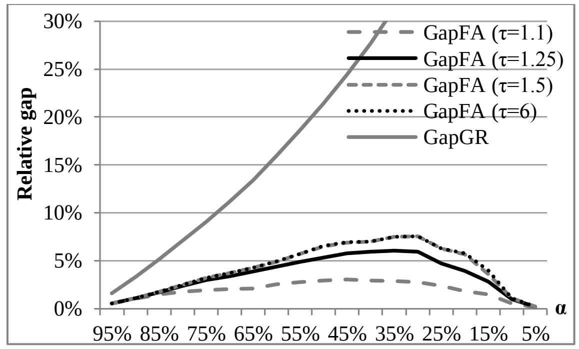


Figure 9. Relative gap between FAR, FTR and GR strategies for Net_17.

Observe that whereas sparse networks (as Net_14 and Net_17) display a decrease of the network cost from 8% to 10% with $\tau < 2$ (compared to flow-thinning), dense networks (as Net_11) have a limited decrease of the cost (maximum 5%). In fully meshed networks (as Net_10), it is virtually impossible to improve the network cost—the gain is less than 1%. However, further investigations are required to analyze this effect.

C. *Range of the perturbation*

Finally, we study the range of the perturbation, i.e., the number of paths which have their flow adjusted when a failure occurs.

We have two routing paths update processes: thinning and thickening. Figures 10-11 show the average number of paths that will have their flow adjusted, for all failure states with a fixed capacity availability ratio α set to 50% for single link failures (Figure 10) and for single node failures (Figure 11). In these figures, the percentage of paths which has to be thinned (resp. thickened) is represented in solid (resp. dashed) bars.

The figures show that FAR requires modifying flows on almost every path when a failure occurs. The percentage of "thickening operations" depends on the value of τ and exhibits a similar behavior for all networks.

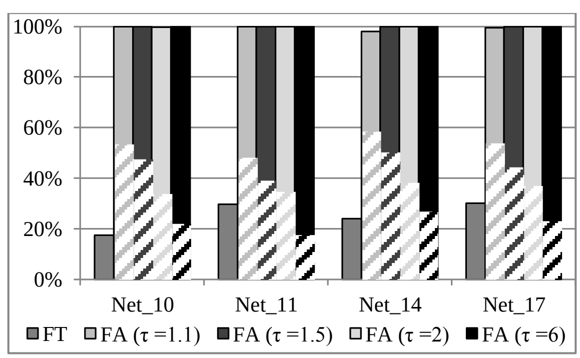


Figure 10. Fraction of paths to be thinned (solid bar) and thickened (dashed bar) with respect to the total number of paths per link failures.

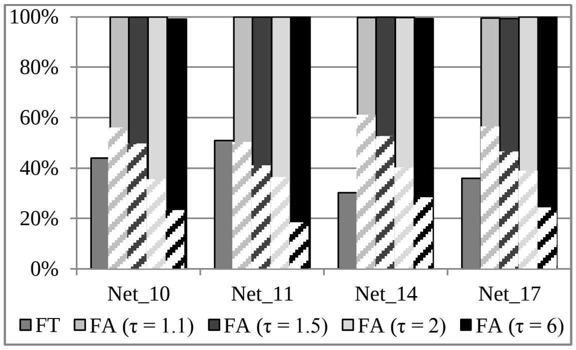


Figure 11. Fraction of paths to be thinned (solid bar) and thickened (dashed bar) with respect to the total number of paths per node failures.

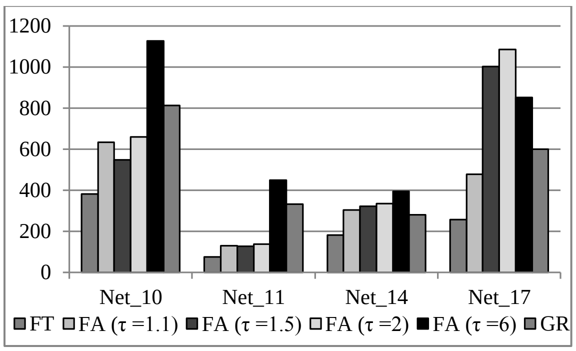


Figure 12. Average number of distincts paths used by FAR, FTR and GR per single link failures.

Figure 12 displays the number of distinct paths used by the other strategies: FTR and GR. We first notice that FTR requires less paths than FAR, and the gap increases with τ. Now we compare the number of paths used by FAR and GR. When τ is low, FAR requires less paths than GR. The difference decreases for higher values of τ, and for $\tau = 6$, for all networks, GR uses less paths than FAR to achieve an optimal solution. This is mainly due to the fact that FAR uses paths with very low value in the nominal state to be able to increase them in a failure state. In regard to scalability and management cost, the above observations suggest that FAR should be used with small values of τ. Another way to limit the number of paths per demand used by this scheme is to modify the formulation (1) by adding specific constraints restricting the number of routing paths per demand, (which would surely have an extra computational cost).

VI. FAILURE RECOVERY PROCESS

The main interest in the flow-thinning strategy stems from the simplicity of the path-flow handling process. Indeed, the reaction to a particular availability state basically consists in decreasing the flow on (some of) the perturbed paths. In the following, we assume that a signaling protocol sends a message from the end nodes of a link to the source nodes of the paths passing through this link when its capacity decreases and reaches a certain threshold. Hence, the time required to recover from a failure state is equal to the time required for the signaling messages to traverse the longest path from the end nodes of the perturbed links to the source node of the disturbed demands. In the following, we study the FAR restoration process.

A. Simulation of the FAR flow adjustment process

The flow adjustment process in FAR is not as simple as in FTR. This process is composed of two simultaneous stages managed by the source and the destination of the traffic demands [12]. The source nodes of the demands will first decrease the flow of some concerned paths, in order to make room for enlarging the flows on some other paths. Next, the destination nodes can increase the flow of the latter paths. Finally, we do not ensure full synchronization as this can be time consuming; hence, some routing paths may need a certain time to become fully operational. This will depend on the number of paths to restore, and on the quantity of flow required to be added to these paths.

B. Simulation results

We study the evolution of the ratio of demands that is perturbed when a failure occurs, and the time required for complete restoration by doing a basic simulation. This simulation is called "basic" for 2 reasons: we first assume that the buffer size is not modified by the perturbation (which is not correct for TCP where a failure is managed using congestion-avoidance algorithm) and we also consider that the time to pass through any link is the same, equal to 1 unit.

Figure 13 reports the ratio of perturbed demands for a fixed link failure as a function of the time, for network Net_14 with $\alpha = 0{,}5$. With FAR there are about 20% of demands perturbed for this link failure situation. Then, the bandwidth of some paths is decreased to allow the bandwidth of some other paths to be increased. This leads to further demands to be temporarily perturbed with about 55% of perturbed demands after 3 units of time. Nevertheless, the process converges very fast comparing to GR which reroutes all demands, perturbed or not.

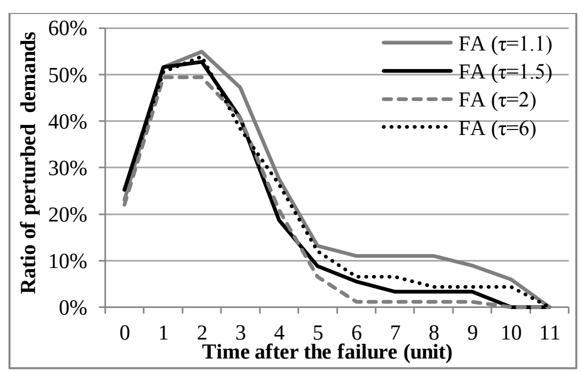


Figure 13. Evolution of the ratio of perturbed demands for Net_14 (α=0,5).

Finally, we notice that the ratio of perturbed demands remains too high compared to that with the flow-thinning strategy.

 ISBN: 978-1-61208-365-0

VII. CONCLUSION AND FUTURE WORK

In this paper, we have studied flow adjustment routing—a routing strategy for demand protection which allows for limited path-flow thickening on top of a commonly understood flow thinning mechanism. FAR is capable of handling multiple partial link failures that are observed in wireless networks or in upper layers of wired communication networks. FAR requires less capacity in the network as compared with a pure Flow-Thinning Strategy, and is cost-wise very close to Global Rerouting for some networks. Our computational results show that FAR achieves encouraging results in terms of the investment cost, at least for the sets of availability states consisting of partial single link failures or single node failures.

We have noticed that the FAR restoration process affects a large number of path flows in the network and may lead to additional perturbation at the very beginning of the process if thinning and thickening operations are not coordinated. Hence, some non-perturbed demands may be affected for a short time when some bandwidth needs to be released from its paths. Making a distinction between paths of perturbed and non-perturbed demands could help to avoid this. On one hand, paths of non-perturbed demands should not be allowed to decrease their total flow more than their traffic requirement. On the other hand, paths of perturbed demands should be able to thin or thick their bandwidth. This leads to a restricted flow-adjustment routing strategy which is nothing else than an extension of the elastic robust rerouting strategy [11], with some constraints relaxed, applied to multiple partial link failures. Moreover, in its current form, FAR and FTR to a less degree, could require significant implementation effort as a large volume of paths are concerned and an important quantity of information is required to maintain all the connections at the routing nodes; this may impact the scalability of the strategy. These issues need further investigation and will be the subject of future work.

ACKNOWLEDGMENT

The work of French authors was carried out in the framework of the Labex MS2T, which was funded by the French Government, through the program ”Investments for the future” managed by the National Agency for Research (Reference ANR-11-IDEX-0004-02). M. Pioro was supported by National Science Centre (Poland) under grant 2011/01/B/ST7/02967 “Integer programming models for joint optimization of link capacity assignment, transmission scheduling, and routing in fair multicommodity flow networks.”

REFERENCES

[1] M. Pióro and D. Medhi, “Routing, Flow, and Capacity Design in Communication and Computer Networks”, Morgan-Kaufman, 2004.

[2] M. Pióro, D. Nace, and Y. Fouquet, “An optimization model for communication networks with partial multiple link failures”, In Proceedings Fifth International Workshop Networks Design and Modeling, (RNDM 2013), 2013, pp. 83-90.

[3] M. Pióro, D. Nace, and Y. Fouquet, “On Protected Traffic Routing in Wireless Networks with Partial Multiple Link Failures”, In Proceedings Eight Conference on Broadband, Wireless Computing and Applications, (BWCCA 2013), 2013, pp. 22-28.

[4] I. Shinko, D. Nace, and Y. Fouquet, “A study on a distributed rerouting scheme”. In Proceedings Advanced Information Networking and Applications (AINA 2013), Workshop NetMM, 2013, pp. 1461-1466.

[5] S. Orlowski and M. Pióro, “On the complexity of column generation in network design with path-based survivability mechanisms”, Networks, 59 issue 1, 2012, pp. 132-147.

[6] H. Anderson, “Fixed Broadband Wireless System Design”, John Wiley & Sons, 2003.

[7] L. Lasdon, “Optimization Theory for Large Systems”, MacMillan, 1970.

[8] M. Minoux, “Mathematical Programming: Theory and Algorithms”, John Wiley & Sons, 1986.

[9] G. L. Nemhauser and L. A. Wolsey, “Integer and Combinatorial Optimization”, John Wiley & Sons, 1988.

[10] S. Orlowski, R. Wessäly, M. Pióro, and A. Tomaszewski, “SNDlib 1.0 – survivable network design library”, Networks 55 issue 3, 2010, pp. 276-286.

[11] Y. Fouquet, D. Nace, M. Pióro and I. Shinko, “Elastic routing: a distributed variant, implementation issues, and numerical results”, In Proceedings Eighth International Conference on P2P, Parallel, Grid, Cloud and Intenet Computing, (3PGCIC 2013), 2013, pp. 98-104.

[12] RFC2205, “Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification”, IETF, 1997.

[13] A. Tomaszewski, M. Pióro, and M. Zotkiewicz, “On the complexity of resilient network design”, Networks 55 issue 2, 2010, pp. 108-118.

Agent Supported QoS Management

Wojciech Kamieniecki
PhD Studies, Department of Informatics
University of Economics in Katowice
Katowice, Poland
email: w.kamieniecki@gmail.com

Malgorzata Pankowska
Department of Informatics
University of Economics in Katowice
Katowice, Poland
email: pank@ue.katowice.pl

***Abstract*— Nowadays, the rapidly developing science of services focuses on service management, which has to take into account the available resources and the user's wishes concerning the desired quality and costs. Quality of Service (QoS) management is perceived as a special aspect of distributed systems management. This area of management is concerned with finding appropriate QoS characteristics for the different system components in a distributed information system application and reserving the corresponding resources in such a way as to achieve the required functionality of the given application and to optimize the overall business organization performance. In this paper, we present a consistent set of concepts concerning QoS modelling for agent technology application and give an example of how that concept can be used.**

Keywords-service economy; Service Level Agreement; Service Level Objective; Quality of Service; agent technology.

I. Introduction

Nowadays, business organizations realize functionality as systems that are composed of services. This includes even mission critical processes of the business. Hence, the quality of such systems including their composition and services is increasingly important. However, it is a challenge to establish high quality in this context because the dynamics and distribution of functionality increase the potential points of failure. Different approaches exist to ensure quality, but they typically act within a restricted scope, such as network layer or software design. This paper presents the usage of Multi-Agent System (MAS) for Quality of Service (QoS) management and computerized network management. Thereby, it supports the selection of approaches to improve quality and finally helps to find a suitable solution for a given situation. The paper consists of two main parts. The first part covers a discussion on the service management, Service Level Agreement (SLA) construction and quality of service. Next, the applied agent technology is explained and the results of the application of agent system prototype for dynamic QoS management are presented and evaluated.

II. Service Science

In literature, service science is an emerging trans-discipline that integrates marketing and behavioural science, operations research and management science, governance and political science, game theory and learning science, psychology and cognitive science, industrial engineering and system science, management of information systems and computer science, organization theory and administrative science, economics, law and historical science, foresight studies and design science [1]. The principal goal of service science is to catalogue and understand service systems, and to apply that understanding to advancing the service developers' ability to design, improve and scale service systems for practical business and social purposes. Services are considered as value co-creation that results from communication, planning, or other purposeful and knowledge-based interactions between distinct service system entities, such as individuals and business units [2]. The service science discipline is to establish service systems and value propositions as foundational concepts, to create data sets to understand the nature and behaviour of service systems and to create modelling and simulation tools for service systems. From the marketing and management science perspective, the services are intangible, heterogeneous, inseparable, and perishable. Services cannot be touched, transported or stored. Each service is unique, instantly generated, rendered and consumed. Services appear in relation to processes and Information Technology (IT) user needs, and the service provider implements these processes to enable the desired changes in the user world. Services require application of specialised competencies (knowledge and abilities) through actions, processes and performance to benefit. They involve a degree of influence of the service provider on the service recipient.

A. Service Management

Service management is defined as a set of specialized organizational capabilities for providing value to customers in the form of services. The service value consists of two principal elements: utility or fitness for purpose and warranty or fitness for use [3]. Utility is determined by the service's functionality and warranty is determined by service quality and performance. Utility is perceived by the customer from the attributes of the service that have a positive effect on the performance of tasks associated with desired outcomes. Service warranty is determined by sufficient capacity or magnitude and is defined in terms of continuity and security.

Nowadays, information technology supports service automation, which has a particularly significant impact on the performance of service assets, such as management, organization, people, processes, and knowledge. Advances in artificial intelligence, machine learning and rich-media technologies have increased the capabilities of software-based service agents to handle a variety of tasks and interactions. Automated systems present a good basis for

 ISBN: 978-1-61208-365-0

improving service processes and they are a means for capturing the knowledge required for a service process. The automation of service processes helps to improve the quality of service, reduce costs and minimize the risks by reducing complexity and uncertainty of service management.

B. *Service Level Management*

The Service Level Management (SLM) approach was developed for years to combine the services providers' capabilities with service users' requirements. To manage service providers' responsibilities effectively, SLM implements Service Level Agreements (SLAs) with Operational Level Agreements (OLAs), and Underpinning Contracts (UCs) with third party suppliers [4]. OLAs is a non-contractual, service-oriented document describing services and service standards, with responsibilities and obligations where appropriate. The scope of issues considered within SLM is huge and the typical topics include: service performance against SLA, incident and problem reviews, business and customer feedback, issues' escalation and contract review summaries, service demand management, expected major changes which affect services, key business events over the service period, service improvement programmes, best practice assurance and standards' compliance. SLA is a basis for the specification and development of Information Technology (IT) service. It enables the monitoring of real time conformance of the service performance and related metrics to the SLA requirements. SLA supports service reconfiguration and adjustment to minimise SLA violations. By definition, SLA is an agreement, while the actual service is specified, designed and implemented in a technical context. There are some strong requirements for SLA modelling [5]. SLA is specified in a specific language, i.e., SLAng, RBSLA, to ensure integration of the SLA management framework with other IT systems for providing the service to the user. SLAs are described in a language that is technology neutral and platform independent. The management of SLAs and exchange of SLA specific information is automated to ensure a more proactive monitoring of the runtime service systems. There are different models of SLA lifecycle [6]. Generally, the SLA lifecycle covers the following stages of an SLA development: service and SLA template development, SLA negotiation, service preparation, service execution, assessment of SLA and the QoS, as well as assessment of the overall service, service termination and decommission [7]. SLA is a representation of all features a user should expect to receive via a service. An SLA is a concrete representation or codification of an agreement, which consists of the following sections:

- Purpose describing the motives behind the SLA creation.
- Parties involved in the SLA and their representative roles, i.e., provider and user.
- SLA validity period.
- SLA scope defining the services covered in the agreement.
- Restrictions to ensure that requested service levels will be provided.
- Service Level Objectives (SLOs) representing the levels of service that both the service user and the service provider agree on. They typically include a set of QoS indicators.
- Penalties for not meeting the agreed SLOs, such as getting discounts or having the right to terminate the contract.
- Exclusions specifying what is not covered in the SLA.
- Administration processes to assess the SLA objectives and describe the responsibility of the service provider [8].

According to [9], an SLA includes some guarantee terms, where each term codifies an obligation (see Figure 1). The performative aspects of the obligation are encapsulated by the QoS object, while service utility is captured by the business value. In order to ensure that obligations are met and the service is delivered as agreed, the service delivery must be monitored. Therefore, a set of monitoring policies is developed and implemented.

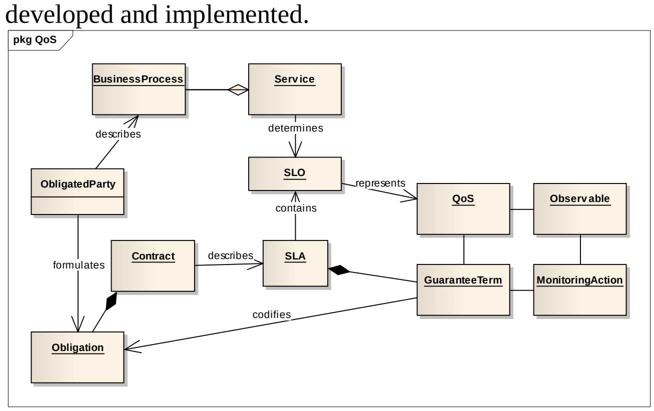


Figure 1. Service Level Agreement within Service Level Management.

Service Level Agreement (SLA) describes agreed service functionality, cost and qualities. An SLA is an agreement regarding the guarantee of a service. It defines mutual understandings and expectations of a service between the service provider and service users. It consists of sections describing the commitments to service quality and service levels that the service provider has to guarantee. SLAs contain Service Level Objectives (SLOs) that represent the Quality of Service (QoS) goals, e.g., storage, bandwidth or response time. Service providers need to comply with QoS requirements, specified in SLA and contracts, which determine the revenues and penalties on the basis of the achieved performance level.

C. *Quality Management*

Generally, in service science, quality can be considered in a few different ways [10]. On one hand, Quality as a functionality characterizes the design of a service and can be measured by comparing the service against other services offering similar functionalities. Quality as conformance, on the other hand, can be monitored for each service individually, and usually requires the user's experience of the service in order to measure the promise against the delivery.

 ISBN: 978-1-61208-365-0

Quality as reputation is regarded as a general reference to a service's consistency over time in offering both functionality and conformance qualities, and can therefore be measured through the other two types of quality [10]. Thiadens analyses the product, the process, IT facilities and the business organization qualities [11]. Zeginis [12] proposed considered qualities as measurable and as unmeasurable. Measurable qualities could include accuracy, availability, capacity, costs, latency, provisioning-related time, scalability, whereas unmeasurable qualities cover interoperability of communicating entities, modifiability, security, as well as complementary dimensions, i.e., assertion-based monitoring, event-based monitoring, history-based monitoring. Service measure system contains information on the current system configuration and runtime information on the metrics that are part of the SLA. The system measures SLA parameters, such as availability or response time, either from inside, by monitoring resource metrics directly from managed resources, or from outside the service provider's domain, e.g., by analysing the client transactions.

D. *Quality of Service*

In a service contract or agreement, a service is defined by its context or functions, its terms and conditions, and is normally set by the agreement between the service user and the service provider. QoS is determined in relation to the fulfilment of the service agreement. According to the International Standard ISO/IEC 13226:1998 the QoS Framework is a structural collection of concepts and their relationships which describes QoS and enables the partitioning of, and relationships between, the topics relevant to QoS in information technology to be expressed by common means of description [13]. In ISO/IEC 10746-2, QoS is a set of qualities related to the collective behaviour of one or more objects. Depending on the established context and specified requirements, the QoS parameters may be of different kinds, e.g., a desired level of characteristic, a maximum or minimum level of a characteristic, a measured value, a signal to take an action, a request for operations, or the results of operations [13]. In the domain of service science and particularly in SLM, the QoS management functions are designed to assist in satisfying users' QoS requirements. The activities of QoS management include the establishment of QoS for a set of QoS characteristics, monitoring the QoS values, maintaining the actual QoS as close as possible to the QoS target, control of QoS targets, enquiry upon some QoS information and alerts in the case of events related to the QoS management [14]. Hardy considers three kinds of quality of service [15]. In the technical design, the intrinsic QoS which includes characteristics of the connection made through the network and provisioning the network accesses, terminations, and switch-to-switch links, relative to the expectations of the person who designs and operates the system. The perceived quality of service is what will determine whether the user will find the service acceptable when it is delivered, and the assessed quality of a service, which results when the user who pays for the service determines whether the quality of service was good enough to warrant its continued use.

III. Application of Agent Technology for QoS

Nowadays, the multi-agent systems (MAS) concern many aspects of human living. MAS can be successfully used in the transportation area [16][17] or in a hospital system [18]. The flexibility of MAS gives the opportunity to create a new type of intelligent system. Properties of agents are as follows: reactiveness, goal orientation, autonomy, adaptability, ability to communicate, capacity for cooperation and learning ability. Those properties of agents make this type of system distinguished and unique in IT. Agents are autonomic entities in the system, but through their learning abilities and communication skills they are able to create a complex system.

QoS may be used in a computer network as one of determinants of quality of a network. Actually, the QoS can be used to divide all network connections into specific groups, based on traffic flow definition: single transfer of information between computer units, like workstations, servers, etc., through the network. Each of this group has its own priority. Priority is used to calculate the portion of bandwidth which should be assigned to specific connections. This simple algorithm applies to management of traffic flows inside IT infrastructure. All models of QoS algorithm have the same common feature, i.e., static approach in defining the policy. The consistency of QoS policy is hard to achieve, because there is no possibility to track all changes of traffic flows in real-time by an administrator or even groups of administrators. In this situation, the static QoS will not be a sufficient solution from business perspective. The MAS for QoS [19] is a new approach to solve the problem of ad-hoc high priority business flows. The agents gather the users' requirements and based on those information they are capable of creating the optimal policy. Moreover, thanks to trend analysis, the agent is able to change the initial priority. The most important thing is that the agents notice the changes of users' requirements and react to them in real time. Agent, as the autonomic element in the system, can decide which traffic connection should be prioritized. Thus, a group of agents may create a system focused on ensuring users' satisfactions. It should be emphasized, that MAS was designed to solve complex problems, like managing the quality of network service in dynamic infrastructure, gathering and calculating huge amount of date, etc.

The approach presented in this section is the contribution of the authors only. Nevertheless, some of the parts of agent algorithm can be similar to other approaches due to open standard of QoS and agent's definition.

During the work on the prototype, we tried to find a similar approach to compare the effectiveness of these models, however without success. There are some of approaches how to use the MAS for QoS, like [20][21[22], nevertheless, they are not describing the real usage of MAS for QoS in simulated environment. Therefore, it is not possible to compare this model to any other, because each of them are focused on different aspects of managing the QoS. MAS for QoS can be divied into few elements: sniffer, analyser, generator and negotiator. Each of the elements is the independent part of the system. However, we must keep in mind that the analyser cannot work without data from sniffer subsystem. The sequence of agents' actions are sniffering the network traffic, analysing it, generating the new QoS policy. In case when an agent decides that some part of the traffic flows is important, the agent can negotiate higher preferences of that traffic flows with his neighbours. Due to a possible problem with MAS performance, we decided to implement some part of the agent into the database.

The policy is the output of agent's work and it is related only to the specific agent within MAS, so we can assume that the policy is created according to traffic flows which were observed by the agent in a proper time period. The policy is created by the agent on the basis of current traffic flows and the historical occurrences. Moreover, the policy includes the information on what portion of bandwidth and priority should be assigned to a particular traffic flow. The priority is used to distinguish the importance of traffic flows and this is the main factor in MAS for QoS. Taking into account that information, the agent is able to create the optimal policy. MAS for QoS has the possibility to use the network administrator's knowledge and creates the initial knowledge database, based on this information. Network administrator can furnish agent with information about critical traffic flows that have significant impact on business. Information defined by the administrator and observed by the agent is collected in the knowledge database.

In each company, we can distinguish at least one business process. Pall defined the business process as "the logical organization of people, materials, energy, equipment, and procedures into work activities designed to produce a specified end result (work product)" [23]. Business form is created by a set of processes forms – in the way which a business unit/units carries out the business. The business process can be described by a proper process flow. By means of the flow, the management can factorize the complex process. Moreover, priority is a common property of business processes.

Business process priority, as a common property of business processes, defines which business process has high impact on organization. However, managing processes and their priorities inside the company demands not only wide knowledge about all the processes but expert analytics skills too. Nowadays, management tries to do that with the help of expert systems, distributed analytic systems, etc. Multi-agent system is one of the examples of using analytic system to help user in decision making area.

A. *Case Study Description*

The MAS for QoS can be used in every computer network. However, the more complex the computer network is, the more efficient is the policy created by an agent. In our case study the computer network, closed test environment (Figure 3) consists of 5 routers, 12 workstations, 7 internal servers and more than 50 external servers. In our case study, the MAS is built by 5 autonomous agents. The MAS will achieve optimal results when agents will be installed on network devices only. Thanks to this approach all agents have the wide knowledge about traffic flows and all business flows inside the organization. Moreover, the agent can learn the habits of users and try to create a policy that reflects all users' needs. One of the most typical business flows (Figure 2) in an organization is creating a report for management. From organization's perspective the business flow is not complex at all. However, from a technical point view, the flow is more complex (Figure 3).

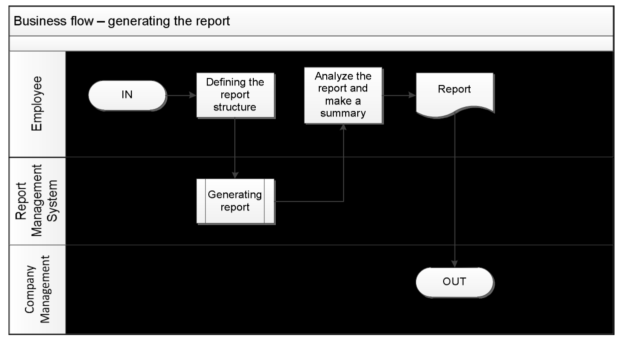


Figure 2. Business flow – generating the report.

The administrator is faced with prioritizing the connections inside an IT infrastructure. The common challenge for all IT infrastructure is the occurrence of multiple connections at the same time. Thus, generally it can be stated that many IT infrastructures face prioritizing the connections in real time. The priority is a percentage of bandwidth assigned to particular traffic connection. The higher the priority is, the more bandwidth will be assigned to the connection. To solve this problem the administrator can implement the QoS. Thanks to this solution, there is a possibility to create a static policy to assure that some connections will have a higher priority than others. Nevertheless, creating a static policy is a suboptimal solution, because the specific traffic/business flow may exist for a short period of time only. In the static policy, the common issue is not using the full available bandwidth. Moreover, continuously changing the policy can have significant impact on business and administrators' works. In such a case we can use MAS for QoS. Thanks to the flexibility of the MAS, there is an opportunity to manage the QoS for a computer network, especially in a highly dynamic environment. The new approach considers to use the historical and current information for creating the policy by agent and the human role can be reduced to minimum. Improving the computer network by MAS has an influence not only on the technology area but also on business processes built on it. The main goal of MAS for QoS is to adjust the traffic priority to actual users' needs. To perform appropriate tests a traffic generator was created. The generator generates the traffic, which reflects as far as possible the network traffic generated by employees or users in similar real network. Moreover, the test computer network (Figure 3) is very similar to computer network used in small companies. Despite the fact that the tests were done

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-365-0

in test environment, the result of these tests can be compared with those that have been done in real environment, thanks to similarity of both environments and network traffics. The results shown in this section are presented from one agent perspective for better visibility. The realized test lasted 2 hours and during it agent noticed that 200 unique traffic flows occurred 5044 times and at least once the priority was changed for them. The agent, as an independent unit with the knowledge database of traffic flows, modified the priority of traffic flows 1781 times. It means that agent changed 26% of traffic flows priorities of total observed traffic flows during test. From business perspective, the agent can have significant influence on the business flows inside the company. The business flows describe all interaction between users, assets, etc. and have real impact on company profits. The longer the agent will work, the better the policy will be matched to the current needs of users and the quality of business flows will be improved.

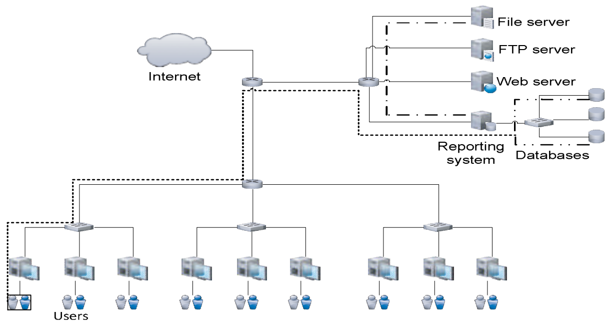


Figure 3. Business flow from technical perspective.

B. *Research Results*

In the prototype, the agent has the possibility to use traffic flows defined by an administrator. This information will be treated as the initial knowledge database by the agent. The agent can use the initial knowledge database in two ways: a defined priority of traffic cannot be changed or it is treated as the initial value, i.e., it can be changed by the agent over time. The first option might be used for traffic with real high impact on business flows. However, in this approach the agent reserves specific bandwidth for irrelevant traffic flow, which importance should be decreased over time. From business perspective this is a suboptimal allocation of resources, which could be used for increasing profits. A wrong allocation of network resources can disturb the businesses processes inside company. Internet surfing, connection to internal file servers or databases are all examples of those groups. The second option should be used in a dynamic environment, where there is a possibility of changing priorities of business flows. Both solutions can be adopted in every IT infrastructure, but only the second gives the opportunity to use the agent to improve and to create the most accurate policy to users' needs.

In Figures 4 and 5, it can be observed how the priority of traffic flow was changed over time for the same type of business flow – generating the report. The agent adjusted the priority to real usage and needs of users. Figure 4 presents how the priority was changed to the highest value and changed back to the lowest value (initial value for all traffic flows) over time. The traffic flow had a high priority, between 4 and 5, for over 1 hour. The situation is different on Figure 5. In the beginning of traffic occurrence, the agent decreased the priority of traffic flow to the lowest value and then increased it to a higher value. The agent used the priority value defined by the administrator as an initial value only. Unfortunately, as it was observed, using the initial value as the final could be the cause of creating a suboptimal policy. In such case, the agent will not take into account the current needs of users.

To summarize the example result, the agent registered 464 unique traffic flows and only 8 of them were defined by the administrator. The average priority with defined traffic flows is 2,17 and without defined traffic flows - 2.06. For 200 unique traffic flows the priorities were changed and the agent noticed 5044 occurrences of those traffic flows. For the rest of traffic flows (264), the agent did not change the initial priority value. 77 of unique traffic flows, which had not been defined by the administrator, had the highest priority at least once. It means that 16,6% of traffic flows had the highest priority value, so those connections had the biggest allocation of resources and they were the most preferable ones in a specific period of time.

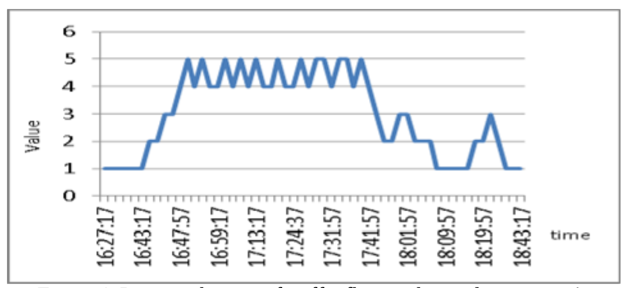


Figure 4. Priority changes of traffic flow without administrator's definitions.

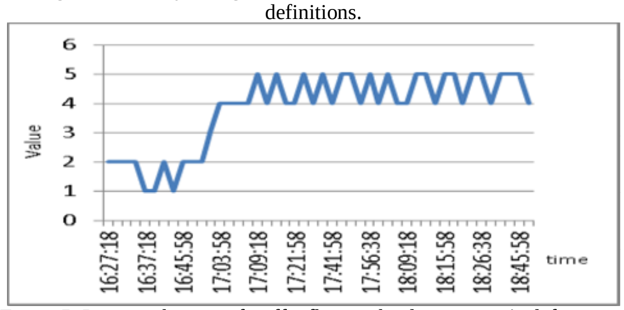


Figure 5. Priority changes of traffic flow with administrator's definitions.

Without the MAS for QoS, only 2 traffic flows defined by the administrator have a priority higher than 1. In the research of usage, it was attempted to prove that improving the quality of network connection can have significant impact on business processes. If the connection is faster than normal, the execution of business process can be finished faster than it was estimated in the beginning. Nowadays, there is no possibility that the administrator could create complex policy in a very short time. However, the

 ISBN: 978-1-61208-365-0

administrator has an opportunity to use the MAS for maintaining the QoS in a computer network. The MAS for QoS guarantees that policies created by agents will be more adjusted to users' actual needs than created manually by administrator. Moreover, the biggest advantage of using MAS for QoS is the time in which the policy will be created. The administrator should have at least 10-30 minutes to create a policy while the agent needs only 3-5 seconds.

The test of MAS for QoS was performed on environment similar to the one which was presented in Figure 3. One of the biggest challenges is to protect the MAS for QoS against any abnormal traffic's behaviour, like maintenance or administrator traffic. The MAS for QoS distinguishes the network traffic and chooses the traffic used by users only. Moreover, the administrator of this system has the opportunity to define the traffic which should be analysed by agent. This approach allows to avoid any incorrect politics created by the prototype.

IV. Conclusions and Future Work

MAS for QoS introduces a new approach on how to adjust the quality of traffic flows, which has real impact on the business flows inside a company. The quality in a network is especially important for the new generation of Internet applications, such as Voice over IP, video-on-demand and other consumer services. By introducing the dynamic quality for traffic flows, the MAS for QoS can change the network parameters for particular traffic flows in real time. Thanks to this approach, the agent is capable of changing the quality of connections only for those that really need it, based on his knowledge database.

The presented work will be further developed and extended. There are many alternative approaches for building scalable computer networks which could be used in MAS for QoS. Thanks to using different types of computer networks, we will have an opportunity to improve the agent's work - agent code optimization. More generally, more work needs to be done to improve an agent's statistical algorithms in the analytic module, which are used to generate the policies by the agent.

References

[1] J. C. Spohrer, S. K. Kwan, and H. Demirkan,"Service science: on reflection," in New Business Models and Value Creation: A Service Science Perspective, L. Cinquini, A. Di Minin, and R.Varaldo, Eds. Milan: Springer , 2011, pp.7-24.

[2] H. Demirkan, J. C. Spohrer, and V. Krishna, "Introduction of the Science of Service Systems" in The Science of Service Systems, H. Demirkan, J.C.Spohrer, and V. Krishna, Eds. New York: Springer, 2011, pp. 1-13.

[3] "ITIL Service Strategy", London: TSO, 2007.

[4] "Best Practice for Business Perspective: The IS View on Delivering Services to the Business, ITIL The key to Managing IT Services", London: TSO, 2004.

[5] T. Tlhong, J. S. Reeve, "Modeling and Management of Service Level Agreements for Digital Video Broadcasting (DVB) Services," in Self-organizing Systems, D.Hutchison, R.H.Katz, Eds. Berlin: Springer, 2007, pp. 288-294.

[6] J. Happe, W. Theilmann, A. Edmonds, K. T. Kearney, A Reference Architecture for Multi-Level SLA Management, Service Level Agreements for Cloud Computing, P. Wieder, J. M. Butler, W. Theilmann, R. Yahyapour (eds.) Springer New York, 2011, pp. 13-26.

[7] A. Tenschert, I. Kotsiopoulos, B. Koller, "Text-Content-Analysis based on the Syntactic Correlations between Ontologies" in Economic Models and Algorithms for Distributed Systems, D. Neumann, M. Baker, J.Altmann, O.F.Rana, Eds. Basel: Birkhauser, 2010 , pp. 161-180.

[8] Ch. Zeginis, "Monitoring the QoS of Web Services using SLAs - Computing metrics for composed services", University of Crete, Computer Science Department, Heraklion, March 2009, available December 2013 at *http://* www.csd.uoc.gr/~zegchris/master_thesis.pdf.

[9] E. Badidi, "A Cloud Service Broker for SLA-based SaaS Provisioning," Proceedings of International Conference on Information Society (i-Society 2013) Shoniregun Ch.A. IEEE Toronto Section, Toronto, 2013, pp. 64-69.

[10] "SLA@SOI, Empowering the Service Economy with SLA-aware Infrastructures, Deliverable D.A5.a", 2009, available January 2014 at http://sla-at-soi.eu/.

[11] V. Deora, J. Shao, W. A. Gray, N. J. Fiddian, "A Quality of Service Management Framework Based on User Expectations," in Service-Oriented Computing ICSOC 2003, LNCS 2910 M. E. Orlowska, S. Weerawarana, M. P. Papazoglou, J. Yang, Eds. Berlin: Springer-Verlag, 2003, pp. 104–114.

[12] Ch. Zeginis, "Monitoring the QoS of Web Services using SLAs - Computing metrics for composed services", University of Crete, Computer Science Department, Heraklion, March 2009, available December 2013 at http:// *www.csd.uoc.gr/~zegchris/master_thesis.pdf.*

[13] T. Thiadens, Manage IT! Dordrecht: Springer, 2005.

[14] Information technology - Quality of service: Framework, International Standard, ISO/IEC 13236: 1998 , Geneve.

[15] W. C. Hardy, QoS: Measurement and Evaluation of Telecommunications Quality of Service, Chichester: John Wiley and Sons, Ltd. 2001

[16] D. Sislak, P. Volf, M. Pechoucek: "Agent-Based Cooperative Decentralized Airplane-Collision Avoidance" in IEEE Transactions on Intelligent Transportation Systems, vol. 12, no.1, 2011, pp. 36-45.

[17] K. Tumer, A. Agogino, "Distributed Agent-Based Air Traffic Flow Management" in IFAAMAS, 2007, pp. 330-337.

[18] T. O. Paulussen, et al.: "Agent-Based Patient Scheduling in Hospitals", Multiagent Engineering. Theory and Applications in Enterprises, S. Kirn, O. Herzog, P. Lockemann, O. Spaniol: Springer 2006, pp. 255-275.

[19] W. Kamieniecki, „Konkurencyjnosc dynamicznego modelu Quality of Service" in Konkurencyjnosc podmiotow gospodarczych w warunkach niepewnosci, WSZMiJO, Katowice 2011, pp. 4-8.

[20] M. Liu, S. Xu, S. Sun, "An agent-assisted QoS-based routing algorithm for wireless sensor networks" in Journal of Network and Computer Applications, vol. 35, issue 1, 2012, pp. 29-36.

[21] T. Rajendran, P. Balasubramanie, "An agent-based dynamic web service discovery framework with QoS Support" in International Journal of Engineering Research and Industrial Applications, vol. 2, no V, 2009, pp. 1-13.

[22] S. S. Manvi, P. Venkataram, "QoS management by mobile agents in multimedia communication" in Database and Expert Systems Applications, 2000. Proceedings. 11th International Workshop on, IEEE, 2000, pp. 407-411.

[23] G. A Pall, Quality Process Management: Prentice-Hall, 1987

Ontology-based Management of a Network for Distributed Control System

Dariusz Choiński, Michał Senik, Bartosz Pietrzyk
Silesian University of Technology
Faculty of Automatic Control, Electronics and Computer Science
Gliwice, Poland
e-mails:{dariusz.choinski@polsl.pl, michal.senik@polsl.pl, bartosz.pietrzyk@student.polsl.pl}

***Abstract*—In this paper, we propose an ontology-based analysis and management of a domain in which initially unspecified number of Industrial Automation (IA) data servers compatible with Open Platform Communication (OPC) specification are available for processing. The result of the performed analysis is an ontology-based Multi-Agent System (MAS) compatible with the Foundation for Intelligent Physical Agents (FIPA) specification that is capable of reliable management in a nondeterministic environment conditions in which not only data servers can change over time in number, but their hierarchical data structures as well. The first step of the presented analysis involves explicit knowledge formalization by means of a Unified Modeling Language (UML). The goal is to obtain complete, hierarchically structured, constrained, human readable ontology in a UML class diagrams format, representing both topology of the domain and its dynamic process control data. The second step is to translate the obtained UML class diagram into First Order Logic (FOL) expressions. The goal is to establish more detailed domain knowledge as well as to check consistency and assure confidence of the derived UML class diagram. The third step is to explicitly formalize the domain ontology in a machine interpretable extensible markup language (XML) schema (XSD), based on the derived UML class diagram. The goal is to have a possibility of automatic generation of hierarchically structured, class source code that, together with parent UML model and FOL expressions, will serve as a baseline for the domain integration system development.**

Keywords-Network management; Multi-Agent Systems; Ontology; FOL; FIPA; OPC; XML; hybrid systems; concurrent programming.

I. DOMAIN INTEGRATION SYSTEM CONCEPT

In the presented domain integration systems, there is a predefined number of database servers, storing both historical and real-time hierarchical data and a nondeterministic number of OPC Data Access (DA) IA servers, serving as source of real-time, process control data. Each server can be accessed by numerous different client applications. OPC standard [1] was established as a method for efficient communication between automation devices and systems. One of the basic specifications is the OPC DA which defines the communication between the client and the server hosting the real-time process data. Data Access Clients have access to data from the automation system via Data Access Servers. The communication interface between the client and the server is completely independent of the physical data source. The OPC DA specification also defines two main structures for describing data shared by the server. These are the namespace (Namespace) and the OPC objects. The namespace provides hierarchically structured, control process data. The structure of the OPC objects is flat and is created by the client application. The OPC object, within the established structure, is attributed to identifiable characteristics, such as: the value of the corresponding variable, the time of measurement, the quality measurement and others [2][3]. Cooperation with OPC DA servers is established through the Java Native Interface (JNI) wrapper, which is based on the native OPC DA library. Cooperation with database servers is established through the NHibernate database entity framework wrapper [4].

The presented domain integration system concerns usage of partially autonomous, proactive and self-managed MAS as an integration solution. Resulting from such an approach, there is a number of different types of agents that have to cooperate together, performing their highly specialized set of activities, in order to perform integration tasks correctly [2][3][4]. The idea of cooperation, as communication between agents, using serialization of speech acts, requires the creation of an ontology that allows partitioning of the message by the agent, so that the intentions of the objectives are clear and unambiguous. At the same time, it should be a feature of the ontology which is easily processed by both man and machine. Therefore, the rationale for the MAS domain integration system development is an OPC-based ontology. The structure of the transmitted information is particularly important in the use of Multi-Agent technology in control and design of control systems. The set of concepts, which in this case is a description list of the data points, used and controlled variables in the whole process of designing the control system and its software is practically constant. What changes, mainly, is the structure of mutual connections and the structure of the information used for decision making and activities related to the control. An obvious advantage of the system of agents that communicate using messages based on a universal definition of a FIPA standard [5] is the ability to remotely boot services, regardless of the particular software implementation. Within the commonly used protocols in the domain, it is necessary to know the structure of instances of the individual objects performing services or storing information and for the MAS this knowledge is formalized by means of ontology.

The rest of this paper is organised as follows. The second section presents a high level, abstract description of an automation system analysis based on Petri Nets and ontologies. The third section proposes a solution to validate the obtained ontologies' UML class diagrams by means of additional FOL formulas. The fourth section presents general rules of conversion from UML class diagrams to FOL formulas. The fifth section presents a sample conversion from ontology-based, UML class diagrams to corresponding FOL formulas, proving the correctness of obtained ontology.

II. DYNAMIC DOMAIN EVENTS RESPONSE

Resources, as a part of the greater domain, are usually treated as a source of a variety of different pieces of information that need to be integrated and analyzed in order to be meaningful. These data are usually stored in a resource's hierarchical memory structures. The process of the fast data collection and analysis of those pieces of information is an essential activity for each integration system resulting in a proper and efficient domain control and maintenance. Both the data structure and the resource allocation are essentially dynamic, and thus, can change over time. The inability to synchronize automatically with each other causes confusion and various different data integrity problems. It is worth mentioning that the synchronization process always depends on various different reconfiguration and reorganization processes. To achieve such an autonomous and proactive domain integration system, additional detailed analysis of a domain from the perspective of each underlying integrated resource is required. The performed analysis ought to treat a resource as a finite state machine and result in explicitly defined state set that would cover its whole functionality. It is important to notice that those states must not lead to the integration system deadlock in any way as each state should have its transition conditions, predecessor and successor states clearly defined. To achieve this, a states reachability graph has to be created, and, since Petri Nets [6] is a widely accepted tool to perform such an analysis, it is a fairly easy and straightforward task (Figure 1).

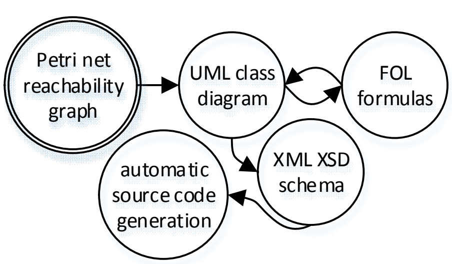


Figure 1. Iterative approach to domain integration system engineering.

However, this is only the initial step towards domain integration system creation. Since Petri Nets is still just a human only interpretable tool; a more sophisticated and expressive tool, such as ontology, is required. Ontology possesses enough capabilities to formalize the gathered domain knowledge in both human and machine readable format. It can describe both static properties of the system and its runtime states in which the system can reside, as well as the conditions of transitions between those states. Ontology can model anything starting from the tiniest domain element to vast hierarchies of domain resources. Based on the ontology, parts of the domain integration system can share their knowledge and cooperate to solve integrated system's problems [2][3]. Technically, ontology is a set of very simple and much more complex rules, such as concepts, predicates and actions, which can be created in many available programming languages, such as Java, C# or XML [2][3]. Each ontological expression can be organized in a hierarchical structure, which means that simpler entities can be nested in more complex ones.

III. ONTOLOGY-BASED ANALYSIS AND ENGINEERING

In the proposed domain, integration system ontology is a fundamental element serving as a formal domain and its integration system specification, communication medium and domain integration system implementation base. Based on such an ontology, a detailed analysis can be performed, which allows to obtain peek quality of a domain integration system. Ontology-based analysis and engineering activities, however, require a good and comprehensive visual tool that could enhance ontology expressiveness and improve obtained results quality. For many experts in this field, UML and its class diagrams especially, have gained much credit. However, UML class diagrams along with their many useful features tend to contain also a lot of implicit knowledge that concerns declaration of classes and their methods, classes' generalization and accessibility level. Implicit, hidden knowledge always causes unnecessary problems during domain analysis and its integration system implementation. This is even more concerning, knowing that, in time, UML class diagrams, tend to grow uncontrollably fast in their size and complexity, which introduces a problem of domain knowledge maintenance. To eliminate or at least to reduce the impact of these problems, ontology-based UML class diagrams can be greatly enhanced with support of FOL [7]. By doing so, each single class and their hierarchies can be additionally supported with numerous FOL assertions.

Combined together, UML class diagrams and FOL assertions can produce a more complete, detailed and complementary description of a domain and its integration system. Such an approach to ontology engineering allows us to prove its soundness and check its consistency level, which in turn allows for the pre implementation domain integration system validation assuring its foundations. It is worth mentioning that the presented ontology-based analysis and engineering are essentially iterative activities, which also means that they end when enough confidence

 ISBN: 978-1-61208-365-0

and knowledge about the integrated domain has been gathered and formalized explicitly (Figure 1).

However, for the ontology to be reused during domain integration system implementation and communication processes, it has to be defined in a machine interpretable format. A widely accepted solution to this problem would be to reuse XML XSD schema as it possesses enough expressive power to be not only analyzed by a machine but by a human as well. Because the ontology was modeled by means of UML class diagrams, it is also the most reasonable and convenient approach since translation to XML XSD schema is rather straightforward and well documented. However, the resulting XML XSD schema is still just a static representation of an ontology, which is just a static description of a domain and as such, XML XSD schema can only be reused as data validation tool during runtime. The true potential of reusing XML XSD schema is perhaps the possibility of automatic source code generation (Figure 1). In such a case, XML XSD schema stands as a template for the ontology class hierarchy source code creation, which can only improve consistency and interoperability amongst various different domain integration system elements.

For the sake of this paper and analysis of the domain integration system, it was decided to focus only on a simplified part of the system that involves various different OPC DA servers, host machines and operating agents.

IV. General Rules of UML to FOL Transition

However, before any implementation, automatic source code generation, XML XSD schema creation and any FOL analysis, a set of general rules of conversion between UML class diagram model and FOL expressions has to be specified. Generally, in order to speak about FOL sentences predicates, such as class, argument, argument type, multiplicity, association and natural number has to be introduced (1).

$$NatNum, C, T, A, R, S, a, f, r \tag{1}$$

UML class diagrams, much alike the ontologies, allow for declarative modeling of the static structure of a domain, in terms of concepts and their relationship [7]. Single class in each UML class diagram denotes a set of objects with common features and in FOL it will be represented as a unary predicate C (1). Common features of each class are expressed by means of its underlying attributes. Each attribute is characterized by name, type and multiplicity and in FOL it is represented as a binary predicate a (1). To represent the type of an attribute in FOL a unary predicate T (1) will be used. Each attribute characterizes with multiplicity. Even single valued attribute has one. In order to express multiplicity, first of all, a natural number unary predicate NatNum (1) has to be specified [8].

$$\begin{gathered} NatNum(0) \\ \forall\ n.NatNum(n) \Rightarrow NatNum(S(n)) \\ \forall\ n.0 \neq S(n) \\ \forall\ m,n.m \neq n \Rightarrow S(m) \neq S(n) \end{gathered} \tag{2}$$

Natural numbers in FOL (2) can be characterized by means of one natural number constant symbol 0 and one successor unary predicate S (1) (2). For each n value, if n is natural number so is S(0), S(S(0))and S(…(S(n)). Natural number will help us in defining multiplicities [7] for each available class attribute for which the FOL expression (3) holds.

$$\forall\ x \exists\ y.C(x) \wedge a(x,y) \Rightarrow T(y) \tag{3}$$

An expression (3) states that for each x instance of class C there exists such value y of type T related to instance x by means of an a attribute. The multiplicity [7] of attribute a is denoted by FOL expression (4), which states that for each instance x of class C there exists such value y of type T that references to x by means of an attribute a that has at least i and at most j values.

$$\begin{gathered} \forall\ x,i,j,\exists\ y.C(x) \wedge T(y) \wedge a(x,y) \\ \wedge NatNum(i) \wedge NatNum(j) \\ \Rightarrow (i \leq \#\{y|a(x,y)\} \leq j) \end{gathered} \tag{4}$$

Hierarchical relationships between different classes are modeled by means of an association relationship which is very much alike attribute but differs in the level of accessibility. While an attribute models properties that are local to a class, an association models properties that are shared amongst different classes. An association [7] can be a binary or a n-ary relation, thus what holds for the binary association holds also for n-ary one. In FOL, association between various different classes without association class defined is represented as a n-ary predicate A (1) for which the FOL expression (5) holds. An expression (5) states that association instances have to be of correct classes.

$$\begin{gathered} \forall\ i,n,x_0,x_n.\ NatNum(n) \wedge NatNum(i) \\ \wedge A(x_0,x_n) \Rightarrow \wedge_{i=0}^{n} C_i(x_i) \end{gathered} \tag{5}$$

An association between different classes that has related association class is represented by a unary predicate A and n binary role names predicates $r_0 \ldots r_n$ (6)(7)(8).

$$\forall\ x,i \exists\ y.A(x) \wedge NatNum(i) \wedge r_i(x,y) \Rightarrow C_i(y) \tag{6}$$

$$\begin{gathered} \forall\ x,i \exists\ y,y'.A(x) \wedge NatNum(i) \\ \wedge r_i(x,y) \wedge r_i(x,y') \Rightarrow y = y' \end{gathered} \tag{7}$$

$$\begin{gathered} \forall\ x,x',i,n \exists\ y_i,y_{n.A}(x) \wedge A(x') \wedge NatNum(i) \\ \wedge NatNum(n) \wedge \wedge_{(i=0)}^{n}(r_i(x,y_i) \wedge r_i(x',y_i)) \\ \Rightarrow x = x' \end{gathered} \tag{8}$$

An assertion (6) types the association. It specifies that for each instance of association class A, instance value y that relates to x by means of role r_i is of specific class type C_i. An assertion (7) refers to the fact that there exists only one instance value y for each single role r_i of A. An assertion (8) specifies that there is only one instance of association class that faithfully represents one particular relation. Special kind of a binary association between two classes that corresponds to a containment relationship is an aggregation. It specifies that each containing class owns a set of contained classes instances (9). An aggregation [7] relationship does not need an additional association class, thus in FOL it can be specified as a binary relation (9).

$$\forall\ x \exists\ y.A(x,y) \Rightarrow C_1(x) \wedge C_2(x) \tag{9}$$

In the object-oriented domain, the notions of inheritance and polymorphism are very important. Both are often used interchangeably and both refer to the notion of generalization. Generally, class hierarchy is a result of a composition of several generalizations (10).

$$\forall\ x,i,n.\mathrm{NatNum}(i) \wedge \mathrm{NatNum}(n) \wedge \wedge_{(i=0)}^{n}(C_i(x_i)) \Rightarrow C(x) \tag{10}$$

Class hierarchies usually form complex structures and usually during domain integration system analysis it is often required to formalize various different and smaller class subcategories. To do that, it is important to specify both class disjointness (11) and completeness (12) notions [7]. Disjointness refers to the notion that single object cannot be an instance of two different subclasses at the same time. Completeness refers to the fact that each subclass is also an instance of at least one superclass.

$$\forall\ x,i,j,n.\mathrm{NatNum}(n) \wedge \mathrm{NatNum}(i) \wedge \mathrm{NatNum}(j) \wedge \wedge_{(i=0)}^{n} C_i(x) \Rightarrow \wedge_{((j=0),(j\neq i))}^{n} \neg C_j(x) \tag{11}$$

$$\forall\ x,i,n.\mathrm{NatNum}(n) \wedge \mathrm{NatNum}(i) \wedge C(x) \Rightarrow \vee_{(i=0)}^{n} C_i(x) \tag{12}$$

The methods, static or instance, are the executable part of each class. Each such method defines class competencies and the body of those methods represents how the class and its instances interact with a domain. Class methods are functions from the class or class instance to which a method is associated and possibly additional parameters to instances or simple values [7]. In FOL, a class method is represented by a n-ary predicate f (13) with up to f_x+f_i+f_o arguments, where f_x is an instance of the parent class, f_i is the number of input parameters and f_o is the output of the method. Therefore, it is easy to deduce that an instance method without input parameters will be defined by a binary predicate with f_x+f_o number of arguments. FOL predicate f has to additionally satisfy a set of assertions that will explicitly specify method consistency (14) and correct typing of method's input and return parameters (13). Both assertions, as a result, allow capturing explicitly notions of overriding and overloading that in UML class diagrams are rather hidden from ones perspective.

$$f_{x,p_0,\ldots,p_m,r} \tag{13}$$

$$\forall\ x \exists\ p_0,\ldots,p_m,r.C(x) \wedge \mathrm{NatNum}(m) \wedge f_{x,p_0,\ldots,p_m,r} \Rightarrow \wedge_{(i=0)}^{m}(P_i(p_i)) \wedge R(r) \tag{14}$$

$$\forall\ x \exists\ p_0,\ldots,p_m,r,r'.C(x) \wedge R(r) \wedge R(r') \wedge \mathrm{NatNum}(m) \wedge f_{x,p_0,\ldots,p_m,r} \wedge f(x,p_0,\ldots,p_m,r') \Rightarrow r=r' \tag{15}$$

V. Domain Integration system Analysis

Based on the general rules of transition between UML class diagram and FOL, further domain integration system analysis can be performed that might reveal the flaws of the obtained model. The presented analysis results, however, were not generated automatically by means of any additional tool as no such tool is currently available. Each given FOL formula was manually derived during additional domain integration system UML class diagram analysis proving its soundness, correctness and consistency. Such an approach allows decomposing complex analysis problems into simpler ones; thus, it helps to describe integration issues in more details. Without such an approach, no scalable, open and reconfigurable domain integration system could be engineered. For the sake of better understanding, in the presented work, only a simple part of domain integration system was chosen. The part that was selected incorporates four different, hierarchically related to each other, concepts representing general domain characteristics (16), various different PC-based and IA-based workstations (17), industrial OPC DA servers (19) and intelligent, autonomous software agents (18).

MAXISConcept class (16) (Figure 2) is a general, domain ontology, integration system, abstract base class that defines a few different common methods (16) that have to be inherited and overridden on each ontology subclass level to meet specific ontology subclass requirements and to be used it has to be inherited.

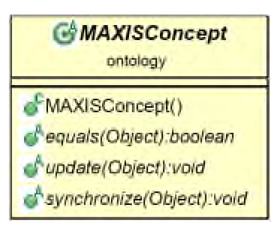


Figure 2. MAXISConcept class.

$$
\begin{gathered}
\mathrm{MAXISConcept}(x) \\
\mathrm{MAXISConcept} \\
\\
\mathrm{equals}_{x,\mathrm{Object},\mathrm{boolean}} \\
\mathrm{update}_{x,\mathrm{Object}} \\
\mathrm{synchronize}_{x,\mathrm{Object}}
\end{gathered} \tag{16}
$$

HostConcept class (17) (Figure 3) models a workstation machine on which OPC DA servers and agents can be deployed. It derives MAXISConcept class and overrides its methods to provide their specific implementation it also defines two members HostName and HostIp accessible through public getter and setter methods.

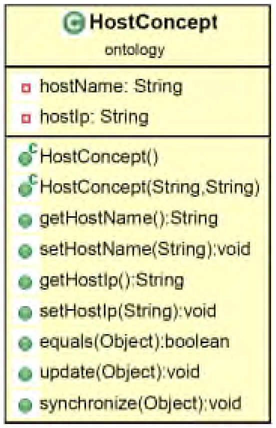


Figure 3. HostConcept class.

$$
\begin{gathered}
\mathrm{HostConcept}(x) \\
\mathrm{HostConcept}, \mathrm{HostConcept}_{\mathrm{String},\mathrm{String}} \\
\mathrm{SetHostName}_{x,\mathrm{String},\mathrm{void}} \\
\mathrm{GetHostName}_{x,\mathrm{void},\mathrm{String}} \\
\mathrm{SetHostIp}_{x,\mathrm{String},\mathrm{void}} \\
\mathrm{GetHostIp}_{x,\mathrm{void},\mathrm{String}} \\
\\
\forall\ x \exists\ y.\mathrm{HostConcept}(x) \wedge \mathrm{hostName}(x,y) \\
\Rightarrow \mathrm{String}(y) \\
\forall\ x \exists\ y.\mathrm{HostConcept}(x) \wedge \mathrm{hostIp}(x,y) \\
\Rightarrow \mathrm{String}(y) \\
\\
\forall\ x \exists\ y.\mathrm{HostConcept}(x) \wedge \mathrm{String}(y) \\
\Rightarrow 0 \leq \{y \mid \mathrm{hostName}(x,y)\} \leq 1 \\
\forall\ x \exists\ y_1, y_2.\mathrm{HostConcept}(x) \wedge \mathrm{String}(y_1) \\
\wedge \mathrm{String}(y_2) \wedge \mathrm{hostName}(x,y_1) \\
\wedge \mathrm{hostName}(x,y_2) \Rightarrow y_1 = y_2 \\
\\
\forall\ x \exists\ y.\mathrm{HostConcept}(x) \wedge \mathrm{String}(y) \\
\Rightarrow 1 \leq \{y \mid \mathrm{hostIp}(x,y)\} \leq 1 \\
\forall\ x \exists\ y_1, y_2.\mathrm{HostConcept}(x) \wedge \mathrm{String}(y_1) \\
\wedge \mathrm{String}(y_2) \wedge \mathrm{hostIp}(x,y_1) \\
\wedge \mathrm{hostIp}(x,y_2) \Rightarrow y_1 = y_2
\end{gathered} \tag{17}
$$

AgentConcept class (18) (Figure 4) relates to the notion of intelligent, autonomous software agent that can cooperate with other different agents exchanging various different ontological messages under certain conditions in the given domain area solving assigned tasks according to designed functionality. It derives HostConcept class providing more specific implementation for each inherited method and is univocally characterized by its AgentLocalName class member.

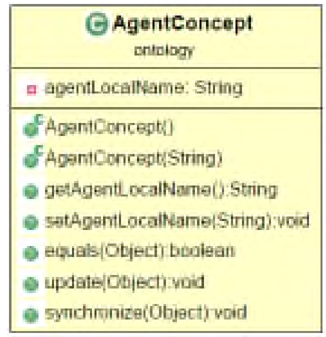


Figure 4. AgentConcept class.

$$
\begin{gathered}
\mathrm{AgentConcept}(x) \\
\mathrm{AgentConcept}, \mathrm{AgentConcept}_{\mathrm{String}} \\
\mathrm{SetAgentLocalName}_{x,\mathrm{String},\mathrm{void}} \\
\mathrm{GetAgentLocalName}_{x,\mathrm{void},\mathrm{String}} \\
\\
\forall\ x \exists\ y.\mathrm{AgentConcept}(x) \wedge \\
\mathrm{agentLocalName}(x,y) \Rightarrow \mathrm{String}(y) \\
\\
\forall\ x \exists\ y.\mathrm{AgentConcept}(x) \wedge \mathrm{String}(y) \\
\Rightarrow 1 \leq \{y \mid \mathrm{agentLocalName}(x,y)\} \leq 1 \\
\\
\forall\ x \exists\ y_1, y_2.\mathrm{AgentConcept}(x) \wedge \mathrm{String}(y_1) \\
\wedge \mathrm{String}(y_2) \wedge \mathrm{agentLocalName}(x,y_1) \\
\wedge \mathrm{agentLocalName}(x,y_2) \Rightarrow y_1 = y_2
\end{gathered} \tag{18}
$$

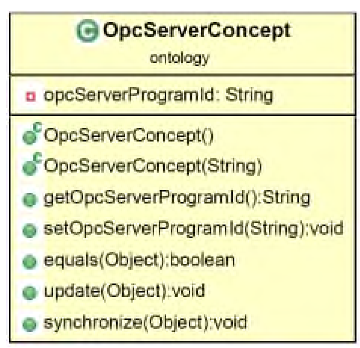


Figure 5. OpcServerConcept class.

OpcServerConcept class (19) (Figure 5) relates to the OPC DA industrial server that provides various different real-time data from an underlying process. Similar to the

AgentConcept class, OpcServerConcept class also derives HostConcept class providing more specific implementation for each inherited method. OpcServerConcept class defines OpcServerProgramId member to univocally distinguish operating OPC DA server.

$$
\begin{gathered}
\mathrm{OpcServerConcept}(x) \\
\mathrm{OpcServerConcept}_{\mathrm{String}} \\
\mathrm{SetOpcServerProgramId}_{x,\mathrm{String},\mathrm{void}} \\
\mathrm{GetOpcServerProgramId}_{x,\mathrm{void},\mathrm{String}} \\[1em]
\forall x \exists y.\mathrm{OpcServerConcept}(x) \wedge \\
\mathrm{opcServerProgramId}(x,y) \Rightarrow \mathrm{String}(y) \\[1em]
\forall x \exists y.\mathrm{OpcServerConcept}(x) \wedge \mathrm{String}(y) \\
\Rightarrow 1 \leq \{y \mid \mathrm{opcServerProgramId}(x,y)\} \leq 1 \\[1em]
\forall x \exists y_1, y_2\, \mathrm{OpcServerConcept}(x) \wedge \mathrm{String}(y_1) \\
\wedge \mathrm{String}(y_2) \wedge \mathrm{opcServerProgramId}(x,y_1) \\
\wedge \mathrm{opcServerProgramId}(x,y_2) \Rightarrow y_1 = y_2
\end{gathered}
\tag{19}
$$

Class hierarchy always imposes numerous constraints, which are implicit in UML class diagram model (Figure 6), however, to improve readability, each such constraint can be defined explicitly (20).

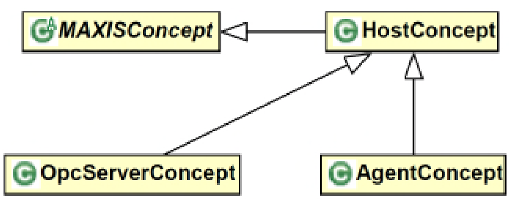


Figure 6. Simple domain integration system class hierarchy.

$$
\begin{gathered}
\forall x.\mathrm{HostConcept}(x) \Rightarrow \mathrm{MAXISConcept}(x) \\
\forall x.\mathrm{AgentConcept}(x) \Rightarrow \mathrm{HostConcept}(x) \\
\forall x.\mathrm{OpcServerConcept}(x) \Rightarrow \mathrm{HostConcept}(x) \\[1em]
\forall x.\mathrm{AgentConcept}(x) \Rightarrow \neg \mathrm{OpcServerConcept}(x) \\
\forall x.\mathrm{OpcServerConcept}(x) \Rightarrow \neg \mathrm{AgentConcept}(x) \\[1em]
\forall x.\mathrm{HostConcept}(x) \Rightarrow \mathrm{AgentConcept}(x) \\
\vee \mathrm{OpcServerConcept}(x)
\end{gathered}
\tag{20}
$$

VI. CONCLUSION

UML class diagrams are fundamental during engineering of each domain integration system. However, each such diagram tends to hide many simple but important facts therefore, an additional tool that can precisely capture such implicit knowledge has to be introduced. The presented analysis focuses on a precise, detailed specification and hierarchical relationship of each domain element, showing an easy way to produce a comprehensive and complementary description of an integrated domain using both UML class diagrams and FOL expressions. Such analysis is not a trivial task as it requires multiple iterations to obtain satisfactory results and thus confidence about integrated domain details. However, the goal of this analysis is not simply to obtain multiple FOL assertions and better UML class diagrams. The main goal is to produce a most detailed description of a scalable, open and reconfigurable domain integration system that can faithfully operate under nondeterministic conditions. To achieve this, resulting ontology-based UML class diagram has to be transformed into a machine interpretable format. The most reasonable solution to this problem is to translate the UML class diagram into XML XSD schema, which in turn can be straightforwardly reused during both implementation and runtime.

ACKNOWLEDGMENT

This work was supported by the National Science Centre under grant No. 2012/05/B/ST7/00096 (D. Choinski) and by the Human Capital Operational Programme co-financed by the EU from the financial resources of the European Social Fund-project no. POKL. 04. 01. 02-00-209/11 (B. Pietrzyk)

HUMAN CAPITAL
NATIONAL COHESION STRATEGY

EUROPEAN UNION
EUROPEAN
SOCIAL FUND

REFERENCES

[1] F. Iwanitz and J. Lange, OPC–Fundamentals, Implementation and Application. Huthig Verlag Heidelberg, 2006.

[2] D. Choinski and M. Senik, 2010. "Collaborative Control of Hierarchical System Based on JADE." In: Y. Luo (ed.), CDVE 2010, LNCS. vol. 6240, Springer, Heidelberg, pp. 262-269.

[3] D. Choinski and M. Senik, 2011. "Multi-Agent oriented integration in Distributed Control System." In: J. O'Shea et al. (eds.), KES-AMSTA 2011, LNAI. Vol. 6682, Springer, Heidelberg, pp. 231-240.

[4] D. Choinski and M. Senik, "Multi-Agent System for Adaptation of Distributed Control System." ICINCO 2012, pp. 206-211.

[5] F. Bellifemine, G. Caire, and D. Greenwood, Developing Multi-Agent Systems with JADE. John Wiley & Sons, Chichester, 2007.

[6] J. L. Peterson, Petri net theory and the modeling of systems. Prentice Hall, 1981.

[7] D. Berardi, D. Calvanese, and D. G. Giacomo, "Reasoning on UML class diagrams." Artif. Intell. 168(1-2): pp. 70-118, 2005.

[8] S. Russel and P. Norwig, Artificial Intelligence a Modern Approach, 3rd ed. Prentice Hall, 2010.

 ISBN: 978-1-61208-365-0

Fairness Improvement of Multiple-Bottleneck Flow in Data Center Networks

Kenta Matsushima, Yuki Tanisawa and Miki Yamamoto
Faculty of Engineering Science
Kansai University
3-3-35 Yamate-cho, Suita-shi, Osaka, Japan
Email: k506903, k284455, yama-m@kansai-u.ac.jp

***Abstract*—Quantized Congestion Notification (QCN), discussed in IEEE 802.1Qau, is one of the promising layer 2 congestion control methods for data center networks. Data center network fundamentally has symmetric structure and links are designed to have high link utilizations. So, data center flows probably pass through multiple bottleneck links. QCN reduces its transmission rate with each congestion notification feedback reception, which might cause excessive regulation of transmission rate. We have already proposed QCN with Bottleneck Selection (QCN/BS) for multicast communications in data center. QCN/BS is originally proposed for multicast communications, but it can also be applied to unicast communication with multiple bottleneck points. QCN/BS selects the worst congestion level and the transmission rate of the sending device is calculated exclusively according to feedback from the selected switch. In this paper, we preliminary evaluate QCN/BS in unicast communications with multiple bottleneck points. Our preliminary evaluation reveals that QCN/BS can resolve this excessive rate regulation problem but has new fairness problem for long-hop flow. To resolve this fairness problem, we integrates QCN/BS and our proposed Adaptive BC_LIMIT. In Adaptive BC_LIMIT, parameter BC_LIMIT is adaptively decided so that the time interval between QCN rate increase is independent of transmission rate. With rate increase interval independent of transmission rate defined in the original QCN as well as rate decrease dependent on it defined in our proposed Adaptive BC_LIMIT, convergence of fair rate allocation among flows sharing a bottleneck link is accelerated. Our simulation results show that our proposed integration of QCN/BS and Adaptive BC_LIMIT significantly improves fairness problem for unicast communications with multiple bottleneck points in data center networks.**

Keywords–data center; QCN; congestion control; fairness.

I. Introduction

Efficient networking is extremely important when a large number of servers are connected in a high-speed, high-capacity network, which is typical situation of data centers supporting cloud computing. Many large-scale data centers implement both a storage area network (SAN) and a local area network (LAN). A SAN generally uses a Fiber Channel for high reliability. Fiber Channel technology is more expensive than Ethernet technology, and the management cost of maintaining the two types of network is high. Thus, the integration of LANs and SANs with Ethernet technology has been under standardized by the IEEE 802.1 Data Center Bridging Task Group [1]. The convergence of data center networking is expected to yield low power consumption and simplify hard wiring [2].

With LAN/SAN integration, conventional SAN performance, i.e., high reliability with low frame loss, will be provided on Ethernet technology. A multi-hop Ethernet configuration is generally used to accommodate the large number of end systems (servers) in current data center networks. Consequently, heterogeneous traffic causes congestion in traffic hot spots. Quantized Congestion Notification (QCN) [3] [4] is one of the promising congestion control methods for data center networks. QCN can keep queue length at a low value because the sending device determines a transmission rate according to feedback from a switch.

Data center network generally has symmetry structure, e.g., Fat Tree [5] and VL2 [6]. Currently, traffic engineering techniques for data center networks, such as MicroTE [7] and Penalized Exponential Flow-spliTing algorithm (PEFT) in data center [8], have been proposed to improve oversubscription environment in data center networks. Purpose of these traffic engineering techniques is generally minimizing maximum link utilization, which might increase the number of highly utilized links in data center networks. Symmetric structure with highly utilized links introduces quite different traffic feature from current wide area Internet, multiple bottlenecks on a path. QCN is feedback-based congestion control and reduces transmission rate with each feedback reception. With multiple bottleneck links, QCN might cause excessive rate regulation due to feedback frames sent by multiple bottleneck points.

This excessive feedback problem typically occurs in multicast communications. We have already proposed Quantized Congestion Control with Bottleneck Selection (QCN/BS) [9] which resolves Loss Path Multiplicity (LPM) problem [10]. In QCN/BS, the sending device identifies the transmission rate of each bottleneck point and selects the lowest one. Our preliminary evaluation in this paper shows that QCN/BS can improve somewhat fairness problem caused by excessive rate regulation but we discovers curious fairness problem for long-hop flow. In multiple bottlenecks situation, frame departure process from a highly utilized bottleneck link (in QCN, link utilization generally grows up to 0.99 [3]), is groomed. This means inter-arrival time to a next bottleneck link of this flow is almost discrete (exactly it is not discrete due to 0.99 utilization and frame length fluctuation: with 1.0 utilization and fixed frame size, it is completely discrete). When discrete arrival is mixed with a fluctuated flow, i.e., flow encountering the first bottleneck point, discrete arrival sees slightly large queue length. This slight difference in measured queue length causes slightly more feedback reception in long-hop flow.

The original QCN rate calculation algorithm has a tendency of keeping unfair situation [11]. We proposed adaptive BC_LIMIT [11] where parameter BC_LIMIT is adaptively decided according to current transmission rate of flows (details of adaptive BC_LIMIT is explained in section III). This parameter setting accelerates convergence of fair rate allocation among flows sharing a bottleneck link. In this paper, we integrate our proposed two algorithms, QCN/BS and Adaptive BC_LIMIT, in order to resolve unfair problem suffered in long-hop flow. Our simulation results show that our proposed

 ISBN: 978-1-61208-365-0

integrated algorithm significantly improves fairness among flows in multiple-bottleneck situation.

The paper is structured as follows. In Section II, we review the QCN and QCN/BS algorithm and show preliminary performance evaluation of QCN and QCN/BS for multiple-bottleneck flow. Section III gives detailed description of our proposed integrated QCN/BS. In Section IV, we present the simulation results. Section V concludes our paper.

II. QCN/BS for Multiple Bottleneck Points

A. QCN

QCN is a Layer 2 congestion control method for multi-hop Ethernet, and its standardization is discussed mainly in IEEE 802.1 Qau. The QCN algorithm is based on a congestion notification from a switch. A QCN switch observes current queue length and calculates a feedback value when a data frame arrives. When congestion occurs, as identified by the calculated feedback value, the switch sends a feedback frame with a certain probability to the source. When a feedback frame is received, the source decreases the transmission rate according to the feedback value. If no feedback frame is received, the transmission rate is increased according to the three-phase rate increase algorithm.

The QCN algorithm works at Reaction Points (RPs) and Congestion Points (CPs). RPs and CPs represent QCN source and switch dynamics, respectively. These behaviors have been described in greater detail in [12].

The CP Algorithm

The CP calculates its feedback value as follows:

$$F_b = (Q_{eq} - Q) - w(Q - Q_{old}), \tag{1}$$

where F_b is the feedback value, Q is the current queue length of the corresponding switch, Q_{eq} is the target queue length, Q_{old} is the queue length at the time of the previous feedback transmission, and w is a constant weight value.

The first component on the right side of 1 shows how much smaller the current queue length is than the target queue length, the second component shows how much the queue length has decreased.

When a CP receives a data frame with a negative feedback value, it returns the feedback value to the corresponding RP. To avoid incurring overhead, the CP returns the feedback value with a certain probability.

The RP Algorithm

The behavior of the RP is shown in Figure 1. The rate increase phase is divided into three sub-phases: Fast Recovery, Active Increase, and Hyper-Active Increase. Each RP maintains four

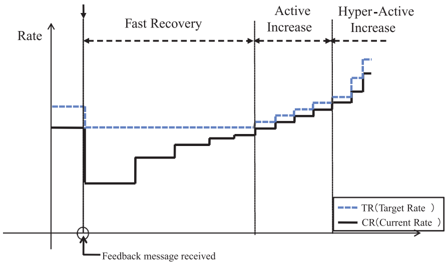


Figure 1. behavior of the RP.

variables for its rate control: Current Rate (CR), Target Rate (TR), Byte Counter, and Time Counter. CR is the current transmission rate, and TR is the transmission rate that is the goal for CR; it is always larger than or equal to CR. The Byte Counter is incremented by 1 whenever the RP sends a mixed byte value (denoted BC_LIMIT = 150 KB in pseudo QCN code [12]). The Time Counter is also incremented by 1 whenever a mixed amount of time has passed (15 ms in [12]). The behaviors of RPs are described below.

Rate Decrease. Whenever a feedback frame is received, the RP first activates the rate decrease phase, and both the Byte Counter and Time Counter are initialized, i.e., reset to 0. Just after receiving feedback, TR and CR are changed as follows:

$$\begin{cases} TR \leftarrow CR \\ CR \leftarrow CR(1 - G_d|F_b|), \end{cases} \tag{2}$$

where G_d is a constant that satisfies $G_d|F_{b_{max}}| = 0.5$.

Fast Recovery. In the Fast Recovery phase, CR is increased rapidly just after rate reduction if no feedback is received. Whenever the Byte Counter or Time Counter is incremented by 1 (after the RP sends data frames of BC_LIMIT KB or the timer spends 15 ms) CR is recovered as follows:

$$CR \leftarrow \frac{1}{2}(CR + TR). \tag{3}$$

Active Increase. When the Byte Counter or the Time Counter reaches 5, the Fast Recovery phase transits to the Active Increase phase. The rate increase in this phase is slower than that in the Fast Recovery phase because the transmission rate might be very close to the rate at which congestion occurred (and feedback was received). In this phase, whenever the Byte Counter or Time Counter is incremented by 1, TR and CR are changed as follows:

$$\begin{cases} TR \leftarrow TR + R_{AI} \\ CR \leftarrow \frac{1}{2}(CR + TR), \end{cases} \tag{4}$$

where R_{AI} is a fixed value (5 Mbps). During this phase, whenever the RP sends half of BC_LIMIT (75 KB) or the timer records 7.5 ms, the Byte Counter and Time Counter are incremented by 1.

Hyper-Active Increase. If no feedback is received after Fast Recovery and Active Increase phases, considerable bandwidth might be left unused. For example, this occurs, when one or more sessions that share a bottleneck switch are closed, and their unused bandwidth is available for other sessions. In this case, unused bandwidth should be rapidly consumed by existing session(s). In the Hyper-Active Increase phase, R$_{AI}$ in 4 is replaced by a higher value (50 Mbps) to achieve the rapid growth of consumed bandwidth. Hyper-Active Increase starts when both Byte Counter and Time Counter reach 5.

B. QCN/BS

In multicast communications, multiple bottleneck points (switches) might be observed on tree-shaped multicast transmission path. Taking the ideal protocol for tracking the most congested path under changing network conditions discussed in the LPM problem paper [10] into consideration, we proposed modified QCN for a flow with multiple bottleneck points, QCN/BS [9].

In QCN/BS, the most congested switch is selected. The transmission rate of the sending device is calculated from

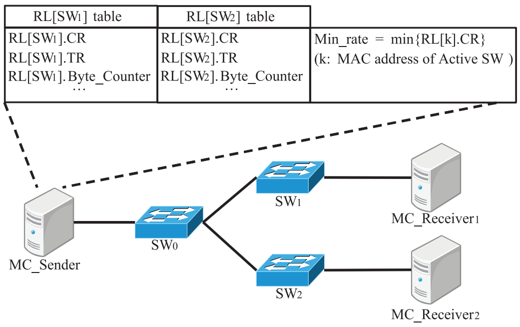


Figure 2. Overview of QCN/BS.

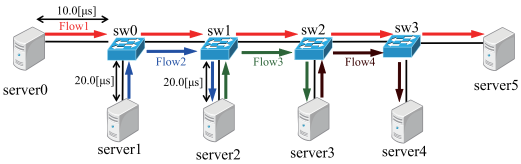


Figure 3. Multiplebottleneck Topology.

the feedback frames sent by the selected switch. The sending device stores the transmission rates for all switches on its multicast tree. To limit the number of transmission rates that the sending device has to manage, only the rates for congested switches should be stored. New transmission rates are calculated for all feedback frames received. The sending device selects the lowest transmission rate, which means it selects the most congested switch. Switches can be identified by their MAC address, which is stored in a feedback frame field.

Figure 2 is a schematic diagram of QCN/BS. In conventional QCN, the source (RP) maintains table based Rate Limiter (RL) for congestion control. The RL table maintains CR, TR, Byte Counter, and Timer Counter data. In QCN/BS, to determine the location of the worst switch congestion, the RL table also needs to maintain RL entries for all congested switches. Each switch is identified by a MAC address. The source (RP) can identify each congested switch and calculate its transmission rate independently.

For QCN/BS, the source (RP) has been modified as follows.

- When a feedback frame arrives

A new transmission rate is calculated for the congested switch, identified by its MAC address. The initial value of the QCN/BS RL table is set as initial value of the convention QCN RL table [12].

- When a data frame is transmitted

In QCN/BS, the source updates transmitted bytes for all entries ($RL[i].Byte\_Counter$ for all congested switches i); when the Byte Counter reaches a certain value, the transmission rate is increased.

In QCN/BS, the sending device does not need to identify whether a flow is multicast or unicast because QCN/BS only selects a single bottleneck. This means that QCN/BS can be applied to multiple bottlenecks on a unicast path.

TABLE I. Simulation Parameters.

Simulator	ns-2.33
Bandwidth	10[Gbps]
the number of Seeds	20
RTT	100[μs]
Packets size	1500[byte]
Queue length	100[pkts]
Qeq	22[pkts]

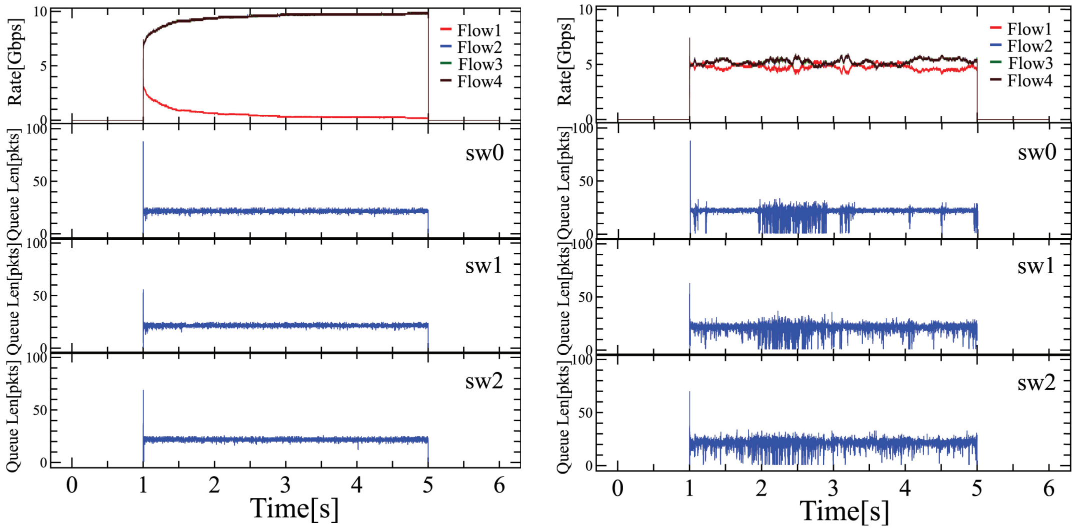
C. Preliminary Evaluation

In this section, we preliminary evaluate QCN and QCN/BS in unicast communications with multiple bottleneck points. We use ns2 [13] as the simulation tool. Figure 3 shows the simulation model. Flow 1 passes through 3 bottleneck links each of which is respectively shared with flow2, 3 and 4. All links have identical bandwidth and operate 10Gbps. sw0, sw1 and sw2 are independent bottleneck switches and the CP implemented in these three switches return feedback to the RP of the corresponding sending devices (server0, 1, 2 and 3). RTT of all flows is 100μs and the propagation delay of each link is depicted in this figure. Other simulation parameters are listed in Table I. We use greedy model where transmission rate of the sending device is exactly defined by the QCN algorithm. For the detailed parameters of QCN, we used the parameters recommended in [12].

Figure 4 (a) and (b) show the transmission rate characteristics of the original QCN and QCN/BS, respectively. These figures also show the queue length characteristics of three bottleneck switches. In the original QCN, transmission rate of Flow 1 (red line) is suppressed just after flow is initiated (1.0[sec]). Other flows (Flow 2, 3 and 4) can obtain remained bandwidth, i.e., their transmission rates are significantly higher than Flow1 (Flow 2, 3 and 4 has almost the same transmission rate and these curves in this figure are eventually overlapped). In QCN/BS, transmission rate of Flow 1 is generally close to other flows, which means link bandwidth is fairly shared between one-hop flow and three-hop flow having multiple bottlenecks on its path. Queue length of QCN/BS is slightly fluctuated but no significant overshoot is observed. From congestion control viewpoint, it is good behavior because queue length is kept low. As shown in Table II, link utilization of QCN/BS is generally high, which means QCN/BS does not over-regulate the transmission rate.

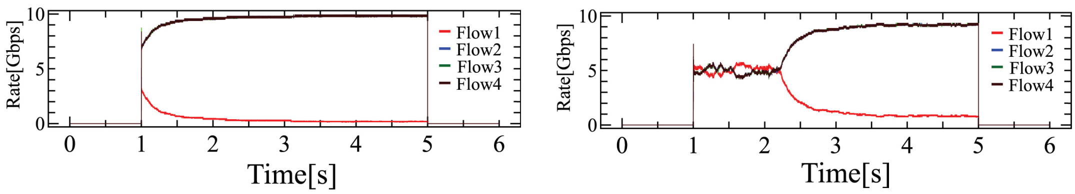
We evaluate the original QCN and QCN/BS for 20 different seeds. For the original QCN, transmission rate of Flow 1 is significantly regulated in all 20 seeds, i.e., all other 19 seeds have almost the same results as Figure 5(a). QCN/BS has good shape (close to other flows) in 7 seeds. However, in our simulation results for QCN/BS, other 13 seeds show too much regulated transmission rate of Flow 1. Figure 5 shows transmission rate characteristics for one of these 13 seeds. So, QCN/BS occasionally improves multi-bottleneck fairness issues in QCN but is a little far from the satisfied solution.

Table III shows the number of received feedback frames for each flow(these results are obtained for the same simulation seed as Figure 5). Flow 1 receives more feedbacks than other flows even though its transmission rate is the lowest (as shown in Figure 5, Flow 1 has the lowest rate). Figure 6 shows CDF of queue length of QCN/BS at each congested switch observed by each flow. At switch 0, flow 1 and 2 observes almost the same queue length. However, at switch 1 and 2, flow 1 observes



(a) originalQCN (b) QCN/BS

Figure 4. Characteristic originalQCN and QCN/BS queue lengths and transmission rate.



(a) originalQCN (b) QCN/BS

Figure 5. Characteristic originalQCN and QCN/BS.

TABLE II. Bottleneck link utilization.

	QCN	QCN/BS
Link Utilization	0.999726	0.999338

slightly larger queue length than one-hop flow (flow 3 and 4 at sw1 and 2, respectively). This curious situation of observing larger queue length is the reason for unfair bandwidth sharing. We try to explain why this situation happens only for Flow 1 by using Figure 7. QCN stabilizes queue length of bottleneck link around pre-defined target queue and enables high link utilization, such as over 0.99. Output process of this highly utilized link (over 0.99) is spaced out with fixed frame length. For a multi-hop flow, an output process of a link is an input process of the subsequent switch. So, input process of flow 1 in sw2 and sw3 is normalized with fixed frame length. Transmission rate of flow 3 and 4 in Figure 5 is defined by QCN rate control and is slightly fluctuated. When their transmission rate is slightly smaller than flow 1, flow 1 might see slightly larger queue size as shown in Figure 7. Flow 1 might see slightly shorter queue size when their (flow 3 or 4's) transmission rate is slightly larger. So, all flows have a possibility to see slightly larger queue length. QCN/BS selects the worst congested switch and adjusts its transmission rate as a calculated rate for feedbacks sent from this selected switch. This behavior causes unfair condition for long-hop flows when compared with short-hop flows even though their observed queue length has similar tendency. For a long-hop flow, eventual decrease of queue length at one switch cannot enforce increase of its transmission rate when another switch is selected and dominates QCN transmission. However, a short-hop flow, such as flow 3 and 4 can increase its transmission rate when it observes decreased queue length. This difference for rate increase behavior brings unfair condition for long-hop flow.

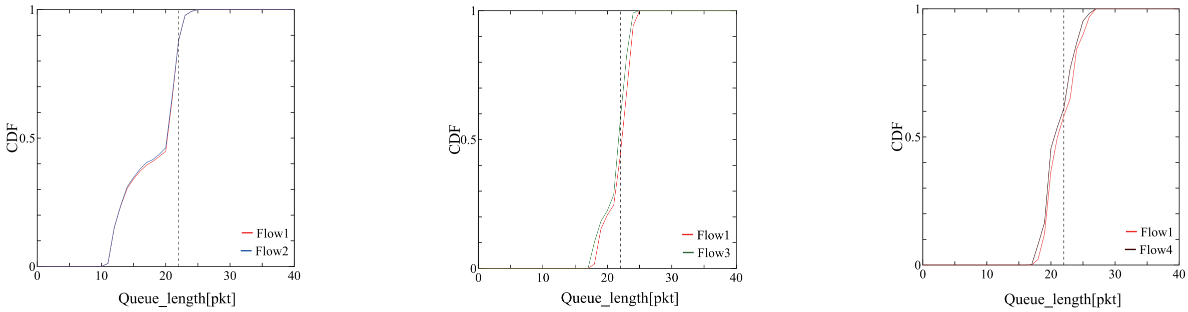
III. Integrated QCN/BS

In this section, we propose QCN/BS integrated with Adaptive BC_LIMIT for resolving fairness issues for long hop flow in multiple bottleneck situation. First, we explain Adaptive BC_LIMIT.

A. *Adaptive BC_LIMIT*

When QCN occasionally falls into flow imbalance (unfair) situation, original QCN algorithm tends to maintain a state of this flow imbalance [11]. This is because the increase and decrease in its transmission rate depends on the flow's transmission rate. In all three increase phases, the transmission rates in 3 and 4 are increased when the counters incremented. Byte Counter is incremented whenever a fixed byte amount is transmitted. Therefore, an RP whose current rate is high tend to have a small interval for rate increases, and an RP with a low transmission rate has a long interval. Thus, RPs having a high transmission rate increase their transmission rate more rapidly than those with a low rate, and an unfair flow state might be maintained.

To improve this undesirable rate increase behavior, we proposed Adaptive BC_LIMIT [11]. In Adaptive BC_LIMIT,



(a) sw0 (b) sw1 (c) sw2

Figure 6. CDF of queue length observed by each flow.

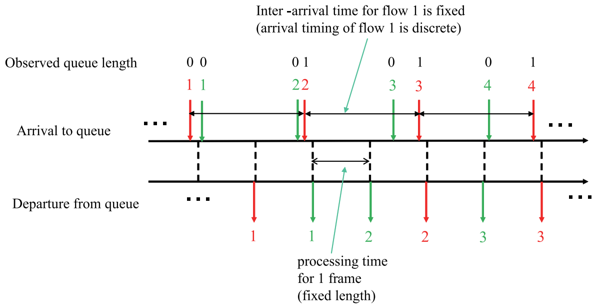


Figure 7. Discrete arrival sees slightly larger queue length.

TABLE III. The number of received feedback frames.

	flow1	flow2	flow3	flow4
sw0	6	13	0	0
sw1	27	0	14	0
sw2	26	0	0	14

the value of BC_LIMIT is defined as follows,

$$BC\_LIMIT = K * Current\_Rate, \tag{5}$$

where parameter K is set to $2.4 * 10^{-4}$ as defined in our former paper [11].

In Adaptive BC_LIMIT, the time interval between rate increases is independent of the current rate of a flow. This means the opportunities for rate increases are almost the same for all flows, even if their transmission rates (throughput) differ. Flows with a high transmission rate have more opportunities to receive feedback frames leading to rate decreases. This is because a feedback frame is transmitted (with a certain probability) back to the source when a data frame arrives at the CP. Two features of Adaptive BC_LIMIT, i.e., rate increases independent of transmission rate and rate decreases dependent on it, accelerate convergence to fair rate allocation among flows sharing a bottleneck link.

B. QCN/BS Integrated with Adaptive BC_LIMIT

When multiple bottleneck points are located on unicast path, long-hop flow might see slightly larger queue length and suffers throughput degradation. And QCN algorithm itself tends to keep unfair situation as explained in the previous subsection. When QCN algorithm is replaced to Adaptive BC_LIMIT, unfair condition might be instantly improved to fair condition.

Algorithm 1 QCN/BS integrated with Adaptive BC_LIMIT algorithm

<u>Rate Increase Phase</u>
When data transmitted
$BC\_LIMIT[SW_i] = BC\_LIMIT[SW_i] - transmitted\_data$
if $BC\_LIMIT <= 0$ **then**
  Byte Counter is incremented by 1
  $BC\_LIMIT[SW_i] = K * RL[SW_i].CR$ (Adaptive BC_LIMIT)
end if
When timer is expired
Time Counter is incremented by 1
When Byte Counter or Time Counter is incremented
if Byte Counter < 5 && Time Counter < 5 **then**
  In Fast Recovery
else
  if (Byte Counter => 5 && Time Counter < 5) || (Byte Counter < 5 && Time Counter => 5) **then**
    In Active Increase
  else
    if Byte Counter => 5 && Time Counter => 5 **then**
      In Hyper Active Increase
    end if
  end if
end if
- -
<u>Rate Decrease Phase</u>
When RP receives feedback from SW_i
if SW_i already has table $RL[SW_i]$ **then**
  $RL[SW_i].Byte\_Counter$ and $RL[SW_i].Time\_Counter$ are initialized
  $BC\_LIMIT[SW_i] = K * RL[SW_i].CR$ (Adaptive BC_LIMIT)
  $RL[SW_i].CR$ decreases as in the conventional QCN
else
  RP creates a new table $RL[SW_i]$
end if
for all SW_i **do**
  if $Min\_rate > RL[SW_i].CR$ **then**
    $Min\_rate = RL[SW_i].CR$
  end if
end for
$Transmission\_rate = Min\_rate$

Inspired by this idea, we propose, in this paper, integration of QCN/BS and Adaptive BC_LIMIT to resolve fairness problem of long-hop flow in multiple bottleneck condition. Algorithm 1 shows our proposed QCN/BS integrated with Adaptive BC_LIMIT. As shown in this algorithm, transmission rate for each switch sending feedback frame(s) is managed at

 ISBN: 978-1-61208-365-0

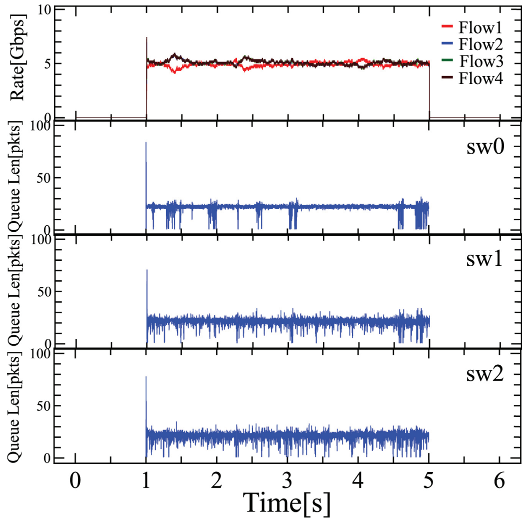


Figure 8. Characteristic QCN/BS integrated with Adaptive BC_LIMIT queue lengths and transmission rate.

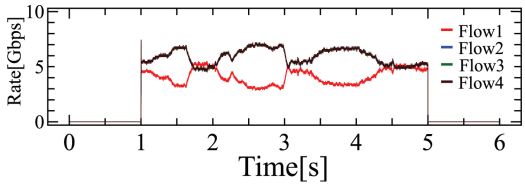


Figure 9. Characteristic QCN/BS integrated with Adaptive BC_LIMIT transmission rate.

the source (RP). In transmission increase phase, transmission rate is increased every time transmitted bytes reach BC_LIMIT (this BC_LIMIT is adaptively computed as shown in (5)). The transmission rate of the sender (RP) is defined as the lowest transmission rate among its managed rates (for all congested switches).

IV. Performance Evaluation

In this section, we evaluate our proposed QCN/BS integrated with Adaptive BC_LIMIT. We use the same simulation model and parameters as section II. Figure 8 shows transmission rate and queue length characteristics of QCN/BS integrated with Adaptive BC_LIMIT (simulation seed is the same one as Figure 5). With integration with Adaptive BC_LIMIT, transmission rate of Flow1 is improved towards fair bandwidth allocation. Adaptive BC_LIMIT stabilizes all flows transmission rate towards fair situation, which improves fair bandwidth allocation to Flow 1. Among 20 simulation seeds, we only find 3 seeds which has slight worse situation. Figure 9 shows the worst case among these 3 seeds. As shown in this figure, even though imbalance between Flow1 and other flows can be observed in short time period, it can be regained towards fair condition. Other 17 seeds give quite good fair condition as shown in Figure 8.

V. Conclusion

QCN/BS is layer 2 congestion control applicable to multiple bottleneck points. Originally it has been proposed for multicast communications where multiple bottlenecks are generally observed on multicast tree, but QCN/BS can be applied to unicast communications with multiple bottleneck points. In the paper, we preliminary evaluate QCN and QCN/BS for unicast communications in multiple-bottleneck situation. Our evaluation results show that QCN/BS occasionally improves fairness issues but cannot resolve unfair condition to long-hop flow completely. We reveal that the reason for this fairness issue is that long-hop flow observes slightly longer queue and receives more congestion feedbacks. To resolve this unfair situation, we integrate QCN/BS with Adaptive BC_LIMIT, which accelerates stabilization towards fair condition. Our simulation results show that our proposed integrated QCN/BS can significantly improve fairness issues for long-hop flow in multiple bottleneck situation.

References

[1] "IEEE 802.1 Data Center Bridging Task Group." http://www.ieee802.org/1/pages/dcbridges.html. [retrieved : may 2014]

[2] R. Hays and H. Frasier, "40G Ethernet Market Potential," IEEE 802.3 HSSG Interim Meeting, Apr. 2007.

[3] M. Alizadeh, et al., "Data Center Transport Mechanisms: Congestion Control Theory and IEEE Standardization," in Proc. Annual Allerton Conference, Sep. 2008, pp. 1270-1277.

[4] "IEEE802.1 Qau." http://www.ieee802.org/1/pages/802.1au.html. [retrieved : may 2014]

[5] M. Al-Fares, A. Loukissas, and A. Vahdat, " A Scalable, Commodity Data Center Network Architecture," in Proc. ACM SIGCOMM, Seattle, WA, USA, Aug. 2008, pp. 63-74.

[6] A. Greenberg, et al., "VL2: a Scalable and Flexible Data Center Network, " in Proc. ACM SIGCOMM, Barcelona, Spain, Aug. 2009, pp. 51-62.

[7] T. Benson, A. Anand, A. Akella, and M. Zhang, "MicroTE: Fine Grained Traffic Engineering for Data Centers," in Proc. ACM CoNEXT 2011, Tokyo, Japan, Dec. 2011, pp. 6-9.

[8] F. Tso and D. Pezaros, " Improving Data Center Network Utilization Using Near-Optimal Traffic Engineering," IEEE Trans. on Parallel and Distributed Systems, June 2013, Vol.24, No.6, pp. 1139-1148.

[9] Y. Tanisawa, Y. Hayashi, and M. Yamamoto, " Quantized Congestion Notification for Multicast in Data Center Networks," in Proc. International Conference on Cloud Networking(IEEE CLOUDNET 2012), Paris, France, Nov. 2012, pp. 51-56.

[10] S. Bhattacharyya, D. Towsley, and J. Kurose, "The Loss Path Multiplicity Problem in Multicast Congestion Control," in Proc. IEEE INFOCOM, Mar. 1999, pp. 856-863.

[11] Y. Hayashi, H. Itsumi, and M. Yamamoto, " Improving Fairness of Quantized Congestion Notification for Data Center Ethernet Networks," DCPerf 2011(The 1st international Workshop on Data Center Performance), Minneapolis, USA, June. 2011, pp. 20-25.

[12] R. Pan, "QCN Pseude Code Version 2.1." http://www.ieee802.org/1/files/public/docs2008/au-pan-qcn-serial-hai-2-1-0408.zip. [retrieved : may 2014]

[13] NS2, Networks Simulator, 1991. Available at http://www.isi.edu/ns-nam/ns/ [retrieved : may 2014]

Multi-layer Power Saving System Model Including Virtualization Server and Many-core Server

Joon-young Jung, Dong-oh Kang, Heong-jik Lee, Jang-ho Choi, Chang-seok Bae
Human Computing Research Section
Electronics and Telecommunications Research Institute
Deajeon, Korea
e-mails: {jyjung21, dongoh, leehj, janghochoi, csbae}@etri.re.kr

***Abstract*— Electric power has become an important part of our life and the power consumption is increasing rapidly. In data center, the power consumption is also increasing and it is essential to reduce the power consumption. Therefore, this paper proposes the requirement functions, the platform, and the structure of a Multi-layer Power Saving System (MPSS), including virtualization servers and many-core servers. Nowadays, the servers in data centers are sufficiently powerful to support many virtual machines. Therefore, the proposed system should be able to manage virtualization servers. We implement this system to monitor and control the power consumption using Intelligent Platform Management Interface (IPMI), the Advanced Configuration and Power Interface (ACPI), and the Dynamic Voltage and Frequency Scaling (DVFS). Through experimental results, the power consumption is reduced about 23%, when the Time-based Dynamic Power Management (TDPM) policy is used.**

Keywords-Data Center; Green IT; Management Server; Power Saving; Virtualization Server.

I. INTRODUCTION

There have been many studies to improve energy efficiency. Alonso et al. [1] presented a holistic approach to have a more efficient consumption behavior without lowering the threshold of comfort that consumers are used to. Power consumption is also increasing in data centers. Therefore, it is becoming a key design issue in data centers [2]. Even if the peak performance is required during short intervals, it should be supported for customer satisfaction using a lot of servers in the data center. Even if system components are not always required to be in the active state, it should be ready for customer satisfaction. So, an energy-efficient server has the ability to enable and disable these components [3]. The Dynamic Power Management (DPM) reconfigures clusters to provide the requested services with minimum active components and loads dynamically [4][5]. The Voltage and Frequency scaling can reduce the power consumption because the consumption energy of a processor is proportional to V^2 and F, where V and F are the operating voltage and frequency, respectively. The Dynamic Voltage Scaling (DVS) controls the operating voltages and frequencies of the processors according to their workload intensities. The DVF works well in web servers typically because they have a very large capacity compared to the average workload [6]. When a server is idle, it uses about 60% less power than when it is in use. And servers commonly work at around a 5% to 20% utilization rate because of the response time. An average of 10% of the servers in data centers were unused [7]. Vondra et al. [8] presented Time Series Forecasting, which enabled to predict the load of a system based on past observations. The prediction can be used to decide how many servers to turn off at night.

Modern servers in data centers are powerful enough to use virtualization to present many smaller virtual machines, where each machine runs a separate operating system [9]. In a virtualization system, several users connect to a single server and use applications independently [10]. The technology for a server virtualization exists. A hypervisor is the hardware virtualization technique that allows multiple operating systems to run concurrently on a host computer. Thus, multiple users can work together with a Virtual Machine (VM) and Input/Output (I/O) devices simultaneously. Nowadays, the virtualization server is generally used for efficiency in the data center. However, energy saving policies have not considered the virtualization server [14][15]. Therefore, this paper proposes 3-tier Power Saving System (3-PSS) to reduce the power consumption in the data center which includes virtualization servers and many-core servers. The 3-PSS can monitor and control the power consumption of guest OSs in virtualization servers.

The rest of the paper is organized as follows. In Section II, we propose MPSS modeling. In Section III, we provide the implementation. Section IV provides the experimental result, and some concluding remarks are finally given in Section V.

II. MPSS MODELING

A. MPSS Functions

There are several mandatory functions for the MPSS, as shown in Figure 1. The monitoring manager should monitor the power consumption of the servers in the data center. The power consumption data are also saved to analyze the power consumption pattern. The maximum value is used to decide a power capping value. The power consumption of the VM, single server, rack, cluster, and data center levels may be monitored. The emergency condition should be handled by using the power threshold alerting function. Whenever the target power budget cannot be maintained, an alert message is sent to the user.

The policy manager analyzes power consumption data. It is possible to forecast the power consumption using the historical data. The policy manager can dynamically make and change the policy to reduce the power consumption. The policy may be classified by workload, such as CPU-intensive, I/O-intensive, and memory-intensive workload. The policies may be used to save the power consumption in the data center [16].

The control manager should control the energy resources. It controls the power consumption of VM, node, rack, cluster, and data center using Intelligent Platform Management Interface (IPMI), the Dynamic Voltage and Frequency Scaling (DVFS), and the Advanced Configuration and Power Interface (ACPI).

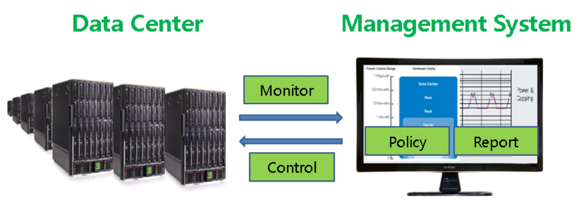


Figure 1. MPSS mandatory functions.

The reporting manager shows the power consumption at the VM, node, rack, cluster, and data center levels. This can be used for detailed analysis of the power consumption behavior of a particular workload or at a particular time interval. The report should be shown periodically and can show the power consumption data as a combination of location and service.

B. *MPSS Platform*

As shown in Figure 2, MPSS platform consists of the server platform, the power management interface, and the DPM platform. The server platform consists of the hardware, the host Operating System (OS), the hypervisor, and the guest OS.

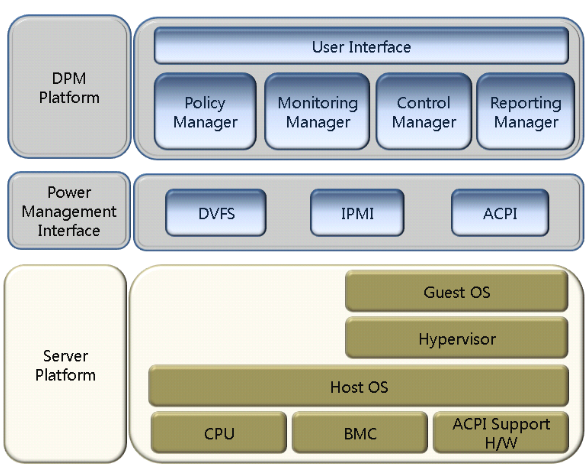


Figure 2. MPSS platform.

The Baseboard Management Controller (BMC) provides the intelligence behind intelligent platform management. The BMC manages the interface between the system management software and the platform management hardware. A hypervisor or Virtual Machine Monitor (VMM) is a piece of computer software, firmware or hardware that creates and runs virtual machines. The proposed platform in Figure 2 is type 2. Type 2 hypervisors are easy to use because they typically require no modification of the guest OS. The power management interface connects with the server platform to monitor and control the power consumption by using IPMI, ACPI, and DVFS. The IPMI is a standardized computer system interface used by system administrators to manage a computer system and monitor its operation [11]. The ACPI establishes industry-standard interfaces by enabling OS-directed configuration, power management, and thermal management of mobile, desktop, and server platforms [12]. DVFS may refer to dynamic voltage scaling and dynamic frequency scaling [13]. Dynamic voltage scaling changes the voltage value used in a component depending upon the circumstances. Dynamic frequency scaling changes the frequency of a microprocessor either to conserve power or to reduce the amount of heat generated by the chip. Voltage and frequency scaling are often used together to save power. The DPM platform consists of the policy manager, monitoring manager, control manager, and the reporting manager.

C. *MPSS Structure*

MPSS structure is shown in Figure 3. One power management server cannot monitor and control all nodes in the data center because there are lots of nodes in the data center. Therefore, MPSS has a 3-layer hierarchy structure, that is, it has a DPM master server, a DPM group server, and nodes.

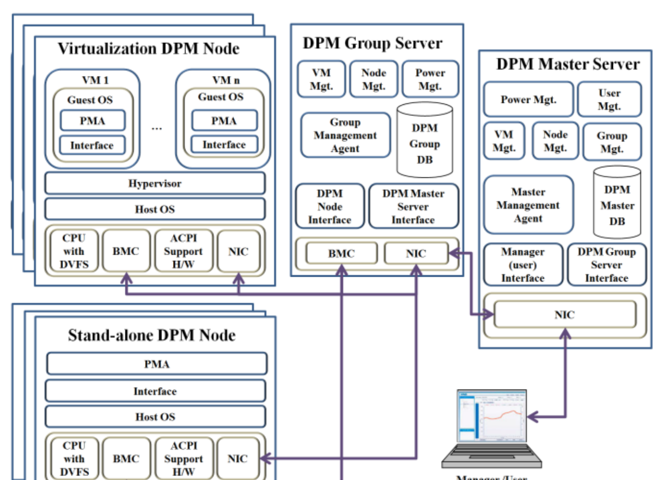


Figure 3. MPSS structure.

A DPM group server can monitor and control hundreds of nodes, which consists of virtualization DPM nodes and stand-alone DPM nodes. The DPM master server can monitor and control nodes through the DPM group server.

 ISBN: 978-1-61208-365-0

The DPM master server manages the power consumption for VMs, nodes, racks, and clusters in the data center using IPMI, ACPI, and DVFS.

A virtualization DPM node is detailed in Figure 4. It contains hardware and software components, including a BMC board, the ACPI support hardware, a CPU with DVFS, a Network Interface Card (NIC), a hypervisor and several VMs. Several VMs can be run in a DPM node. Each VM has a Power Management Agent (PMA), that includes DVFS, IPMI and ACPI modules, to save the power consumption and control resources. Each VM also has a hardware interface layer that connects the PMA and hardware using the hypervisor. The VM uses a group server interface to connect with a DPM group server. Each VM sends power consumption information and receives control messages through this interface. Each DPM node has a BMC board and uses OpenIPMI library to collect power consumption information. The DPM group master manages and periodically requests DPM nodes information. The DPM group server sends this information whenever the DPM master server requests it. The DPM master server monitors and collects DPM nodes information in the Data Base (DB). The DPM master server platform with Policy Based Management (PBM) and DPM analyzes the monitored data and controls nodes in the data center via IPMI, ACPI, and DVFS.

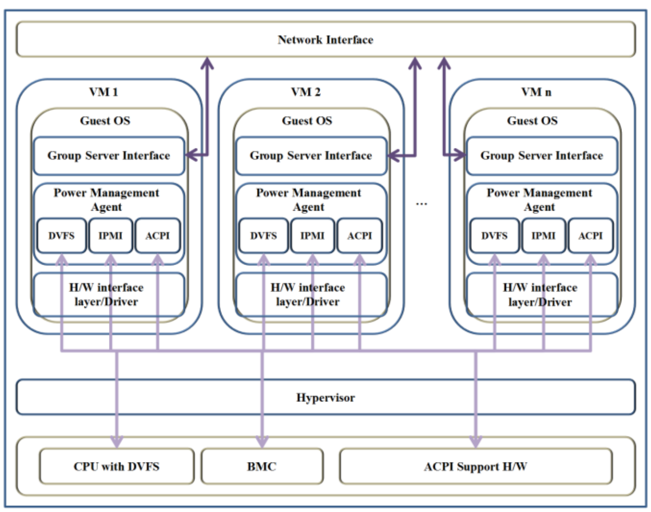


Figure 4. Block diagram of virtualization DPM node.

The PBM manages policies and rules that save the power consumption. It can make a policy by using historical data automatically. System manager can make a policy directly via a user-friendly user interface. DPM monitors energy resources in real time and controls them dynamically in order to save the power consumption. The user monitors and controls the data center using the web-based User Interface (UI) program. All commands except the system on/off command, which uses a BMC interface, make use of the TCP/IP packet.

III. IMPLEMENTATION

We implemented the power saving system in the data center. The DPM master server can monitor nodes in the data center, as shown in Figure 5.

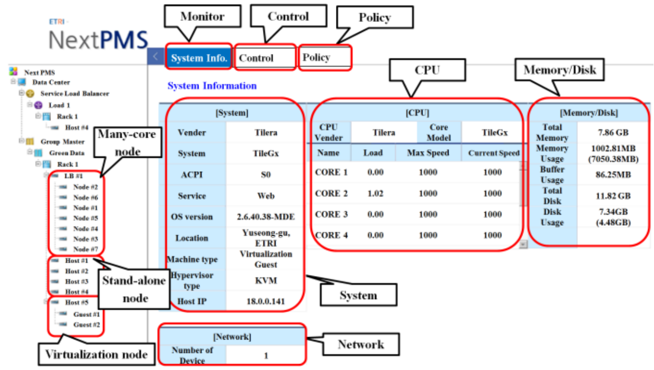


Figure 5. Node system information.

There are three kinds of nodes, that is, the many-core node, the stand-alone node, and the virtualization node. If one node is selected, the system information of that node, CPU, memory, network, and disk, is described in detail. The usage information of that node can be monitored, as shown in Figure 6.

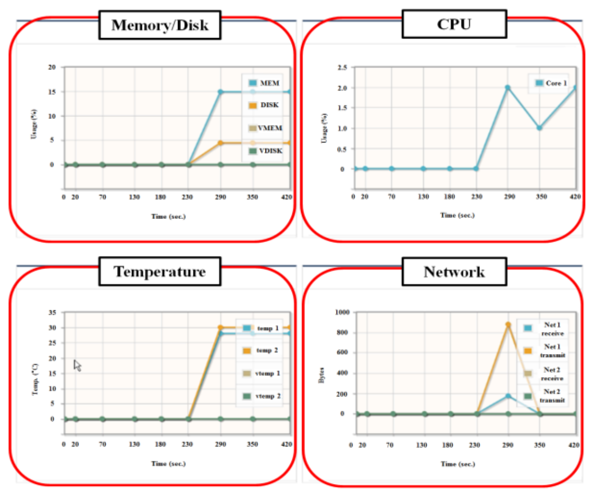


Figure 6. Node usage information graph.

The nodes in the data center can be controlled to save the power consumption, as shown in Figure 7.

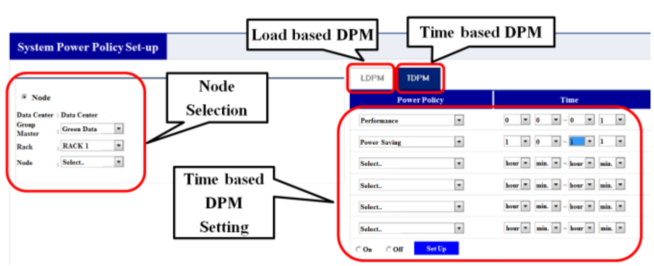


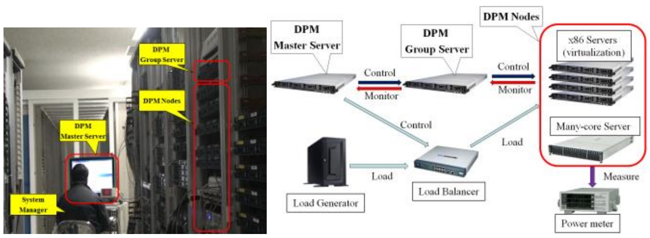
Figure 7. TDPM control interface.

 ISBN: 978-1-61208-365-0

The selected node can be controlled by the LDPM and the TDPM policies. The node can be turned off using the IPMI command, and turned on using the IPMI over LAN command.

IV. Experimental Results

The 3-PSS is tested in the data center, as shown in Figure 8. The DPM nodes consist of stand-alone nodes, virtualization nodes, and many-core nodes. The DPM group server connects with DPM nodes using 1Gbps LAN.



(a) Test environment (b) Test configuration

Figure 8. 3-PSS test.

The DPM master server monitors and controls DPM nodes through the DPM group server. A load generator makes loads and sends those loads to a load balancer which distributes loads to DPM nodes. The load balancer is controlled by the DPM master server.

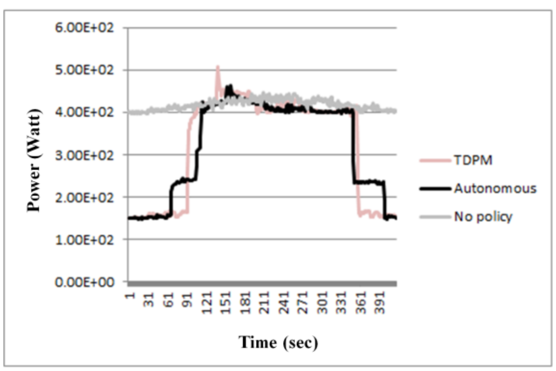


Figure 9. The result of time based DPM test.

Figure 10. The load scheme for time based DPM test.

We test TDPM with four x86 nodes. The result of the TDPM test is shown in Figure 9. The load increases for 4 minutes and then decreases for 3 minutes, as shown in Figure 10. We make these loads using the Apache JMeter. These loads scenario supposes that 7 users request Web services every 30 seconds for 210 seconds. We use Linux Stress tool to consume the power of Web servers when loads are requested from the Apache JMeter.

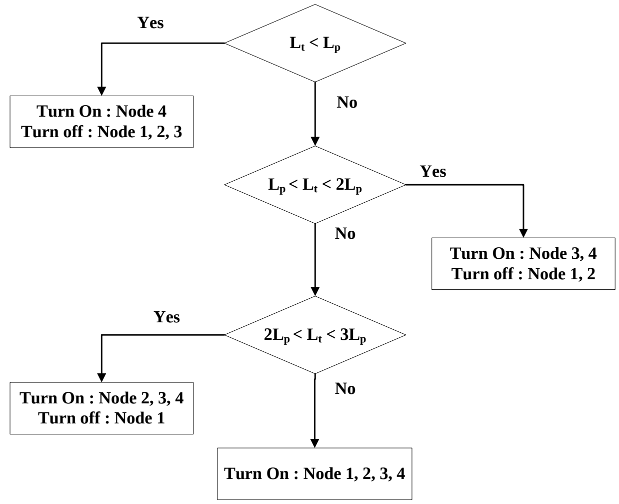


Figure 11. The autonomous policy based on load.

When the TDPM policy is used, one node is on while three nodes are off from 0 to 92 seconds, all four nodes are on from 92 to 348 seconds, then finally, one node is on and three nodes are off from 348 to 420 seconds. When the autonomous policy is used, the load profile (L_p), which is the loads that can be treated one node, is predefined by the DPM master server. The DPM master server monitors the total loads (L_t), which is the loads that be generated by the load generator, and controls the DPM nodes to save power consumption. The autonomous policy of this experiment is shown in Figure 11. If $L_t < L_p$, the DPM mater server turns on the node 4 and turns off the node 1, node 2, and the node 3. If $L_p < L_t < 2L_p$, it turns on the node 3 and the node 4 and turns off the node 1 and the node 2. If $2L_p < L_t < 3L_p$, it turns on the node 2, node 3, and the node 4 and turns off the node 1. If $3L_p < L_t$, it turns on all nodes. The results of the autonomous policy is that one node is on from 0 to 62 seconds and from 396 to 420 seconds, two nodes are on from 62 to 106 seconds and from 345 to 396 seconds, three nodes are on from 106 to 113 seconds, and four nodes are on from 113 to 345 seconds. In this case, the power used is over 400 watts, when the policy is not used. However, the reduction in power consumption is about 23%, when the TDPM policy or the autonomous policy is used.

V. Conclusion and Future Work

For saving the power consumption in the data center, we considered the MPSS functions and propose the 3-PSS platform, and structure for the data center including virtualization servers and many-core servers. We implemented this system to monitor and control the power consumption using IPMI, ACPI, and DVFS. Through experimental results, the power consumption has been found to be reduced by about 23%, when the TDPM or the autonomous policy is used.

For further work, we plan to develop MPSS without performance degradation. The performance is an essential factor in the data center. Therefore, the performance degradation should not occur due to the power consumption saving. We will also estimate the number of nodes that can be managed by a single server.

ACKNOWLEDGMENT

This work was supported by the IT R&D program of MSIP/IITP, [10040696, Development of energy saving green server under 1mW/MIPS for cloud service].

REFERENCES

[1] I. G. Alonso, M. R. Fernández, J. J. Peralta, and A. C. García, “A Holistic Approach to Energy Efficiency Systems through Consumption Management and Big Data Analytics,” International Journal on Advances in Software, vol. 6, numbers 3 & 4, 2013, pp. 261–271.

[2] E. N. Elnozahy, M. Kistler, and R. Rajamony, "Energy-Efficient Server Clusters," Proc. 2nd Workshop Power-Aware Computing Systems, 2003, pp. 179–196.

[3] L. Benini, A. Boliolo, and G. D. Micheli, “A Survey of Design Techniques for System-Level Dynamic Power Management”, IEEE Transactions on VLSI Systems, vol. 8, no. 3, June 2000, pp. 299–316.

[4] J. Lorch and A. Smith, “Software strategies for portable computer energy management,” IEEE Personal Commun., vol. 5, June 1998, pp. 60–73.

[5] L. Benini and G. De Micheli, Dynamic Power Management: Design Techniques and CAD Tools. Norwell, MA: Kluwer, 1998.

[6] P. Bohrer, et al., “The Case for Power Management in Web Server,” Power-Aware Computing, January 2002, pp. 261–289.

[7] P. Foster, PC and Server Power Management Software, Pike Research, 1Q 2010.

[8] T. Vondra and J. Sedivy, “Maximizing Utilization in Private IaaS Clouds with Heterogenous Load through Time Series Forecasting,” The International Journal on Advances in Systems and Measurements, vol. 6, numbers 1&2, 2013, pp. 149–165.

[9] P. Barham, et al., “Xen and the art of virtualization,” Proc. ACM Symposium OSP, 2003, pp. 164–177.

[10] J. Nieh, S. J. Yang, and N. Novik, "A comparison of thin-client computing architectures," Technical Report CUCS-022-00, November 2000.

[11] Intel, Hewlett-Packerd, NEC, and Dell, “Intelligent Platform Management Interface Specification Second Generation,” October 2013.

[12] Intel, Hewlett-Packerd, Microsoft, Phoenix, and Toshiba, “Advanced Configuration and Power Interface Specification revision 5.0,” December 2011.

[13] L. Sueur, Etienne, and G. Heiser, "Dynamic voltage and frequency scaling: The laws of diminishing returns," Proc. of the 2010 international conference on Power aware computing and systems. USENIX Association, 2010, pp. 1-8.

[14] Elnozahy, Mootaz, M. Kistler, and R. Rajamony. "Energy conservation policies for web servers," Proc. of the 4th conference on USENIX Symposium on Internet Technologies and Systems, vol. 4, 2003, pp. 8-8.

[15] Kephart, et al., "Coordinating Multiple Autonomic Managers to Achieve Specified Power-Performance Tradeoffs," International Conference on Autonomic Computing, vol. 7, June 2007, pp. 24.

[16] C. Wissam, and C. Yu, "Survey on power management techniques for energy efficient computer systems," Laboratory Report, Mobile Computing Research Lab, 2002.

Trans-Organizational Role-Based Access Control in Android

Secure Mechanism for Verifying User-Role Assignments of Organizations

Jason Paul Cruz and Yuichi Kaji
Nara Institute of Science and Technology, Graduate School of Information Science
Nara, Japan
E-mail: jpmcruz@ymail.com, kaji@is.naist.jp

***Abstract*—The role-based access control (RBAC) is a natural and versatile model of the access control principle. In the real world, it is common that an organization provides a service to a user who owns a certain role that was issued by a different organization. However, such a trans-organizational RBAC is not common in a computer network because it is difficult to establish both the security that prohibits malicious impersonation of roles and the flexibility that allows small organizations/individual users to fully control their own roles. To solve this problem, this study proposes a mechanism that makes use of the hierarchical ID-based encryption scheme and the challenge-response authentication protocol. The proposed mechanism contributes to achieve both the security and the flexibility and it provides additional features that are common in physical communication but are not obvious in the cyberworld. This study also reports a prototyping system that is implemented on Android-enabled mobile devices. The proposed system employs the needed cryptographic mechanisms, and new technologies, namely, near-field communication and two-dimensional codes, are employed to realize locally closed communication between devices.**

Keywords-role-based access control; trans-organizational role; information security; ID-based encryption; service coalition; Android.

I. INTRODUCTION

The role-based access control (RBAC) [1] is a widely accepted framework that describes the access control relation among users and services. In RBAC, users are associated with roles, and roles are associated with services. This framework is compatible with the access control requirements of real-world organizations and is employed in the computer systems of many organizations/companies. However, it must be noted that RBAC is a versatile framework, and roles are often used in a trans-organizational manner. For example, students are often allowed to be admitted to a museum with discounted admission fee. In this example, the “student” role that is issued by an organization (school) is used by another organization (museum) to determine if a guest is eligible to receive a certain service (discounted admission). This kind of trans-organizational use of roles is, unfortunately, not common in computer networks. Even if one has a certain role that is issued by an organization, there is no way to convince a third-party organization that he/she really has that role.

To realize a trans-organizational RBAC mechanism in a computer network, two issues should be considered; the security and the flexibility. With regard to security, the mechanism should prevent malicious users from disguising their roles. This requirement is naturally accomplished in real-world services with the use of physical certificates, such as passports and ID-cards, which are difficult to forge or alter. This problem, however, is not obvious in a computer system. Digital certificates [2] can be utilized as an analogue of physical certificates, but the use of digital certificates is not favorable from the viewpoint of realization cost, which can discourage small companies and non-profit organizations from participating in the framework. Another less sophisticated approach to the security problem is to let a service-providing organization (the museum in the above example) inquire a role-issuing organization (school) about the user-role assignment. This approach works fine in some cases [3], but a focal point of this approach is the necessity for the agreed beneficial relationship among organizations. Consequently, it is difficult for a new organization to join the partnership, severely restricting the trans-organizational utilization of roles.

The current study aims to develop a practical mechanism that realizes the trans-organizational utilization of roles. First, we extend the model of RBAC to represent the trans-organizational usage of roles. This simple extension clarifies the components and requirements that are needed in the framework of trans-organizational RBAC. Then, we investigate a realization of a user-role assignment that is secure (users cannot disguise roles), user-oriented (users can disclose their roles to any organization), and open (anyone can verify if a user has a certain role that is managed and issued by another organization). The crucial point of this realization is to make use of hierarchical ID-based encryption (HIBE) [4][5], which allows an arbitrary string to be used as a public encryption key. Our key idea is to define correspondence between the roles and keys of HIBE and to employ a challenge-response authentication protocol that will be used for verifying if a user really has an asserted role. The hierarchical nature of HIBE makes our scheme suitable for the trans-organizational utilization of roles, and furthermore, allows flexible role management operations, such as the endorsement and delegation of roles. A prototype system of the proposed trans-organizational RBAC will also be introduced. For the usability of the trans-organizational RBAC, it is highly desirable for a user to be able to carry

 ISBN: 978-1-61208-365-0

his/her roles all the time. To verify the practicality of the proposed scheme, we implemented the proposed system on Android-enabled mobile devices. The implementation contains the realization of cryptographic functions that are essential for handling cryptographic keys and the development of a scheme that allows two devices to perform the challenge-response authentication by utilizing local and closed communication. The prototype demonstrates that the proposed scheme is simple, lightweight, and completely practical for realizing the trans-organizational RBAC. The rest of this paper is organized as follows. Section II introduces the RBAC and the different models associated with it. Section III discusses the technical aspects of HIBE. Section IV presents the structure, procedures, and features of the proposed framework. Section V discusses the realization and implementation of the proposed system in Android-enabled devices. Section VI provides the conclusion and future work.

II. Models for the Role-Based Access Control

In the simplest model of the RBAC [1], the access structure is defined by three sets and two relations. In this paper, we use U for the set of *users*, R for the set of *roles*, and S for the set of *services*. A *user-role assignment*, UA, is a subset of $U \times R$, and a *role-service assignment*, SA, is a subset of $R \times S$. A user u is eligible to access a service s if and only if there is a role r such that $(u, r) \in \mathrm{UA}$ and $(r, s) \in \mathrm{SA}$. The access control should be made in such a way that services are provided to eligible users only. In general, the user-role assignment UA is defined by an entity that issues roles in R, and the role-service assignment SA is defined by an entity that provides the services in S. In this paper, the former is called a *role-issuing entity*, and the latter is called a *service-providing entity*. If RBAC is utilized in a single organization, then we can regard that the role-issuing entity and the service-providing entity are the same identical organization, and that the service-providing entity should have no difficulty referring to the user-role assignment. In this case, the eligibility of a user u to a service s can be easily determined.

On the other hand, in the real world, there are many cases wherein a service-providing entity is a different organization from a role-issuing entity. As stated in the previous section, a school issues the "student" role to its students, and an external organization, such as a museum, provides services to users who hold the "student" role. In this case, the service-providing organization (museum) is a completely independent organization from the role-issuing organization (school), and the service-providing organization is not expected to refer to the user-role assignment that was defined by the role-issuing organization. To discuss such a situation, we first consider an extended model of RBAC.

The *trans-organizational RBAC* is defined similarly to the usual RBAC, but a set O of *organizations* is defined in addition to the sets of users, roles, and services. Furthermore, the set R of roles is partitioned into several subsets, with each subset of R associated with an element in O, that is, $R = R_{o_1} \cup \cdots \cup R_{o_n}$, where $o_1, \ldots, o_n \in O$ and $o_i \cap o_j = \emptyset$ if $i \neq j$. To make the relation among roles and organizations explicit, a role r in R_{o_i} is written as $o_i.r$. Similarly, the user-role assignment UA is partitioned into disjoint subsets; $\mathrm{UA} = \mathrm{UA}_{o_1} \cup \cdots \cup \mathrm{UA}_{o_n}$, where $\mathrm{UA}_{o_i} \subset U \times R_{o_i}$. Obviously, $o_i.r \in R_{o_i}$ means that the role $o_i.r$ is managed by the organization o_i, and the assignment of users to $o_i.r$ is fully controlled by that organization o_i. In the trans-organizational RBAC, upon a request from a user u to a service s, the service-providing organization needs to check if there is an organization $o_i \in O$ and a role $o_i.r \in R_{o_i}$ such that $(u, o_i.r) \in \mathrm{UA}_{o_i}$ and $(o_i.r, s) \in \mathrm{SA}$. Assuming that the user u declares the role $o_i.r$ to utilize, then all the service-providing organization needs to do is check if $(u, o_i.r) \in \mathrm{UA}_{o_i}$ or not. However, it should be noted that the role-issuing organization o_i can be a different organization from the service-providing organization in general. The confirmation of $(u, o_i.r) \in \mathrm{UA}_{o_i}$, which is sometimes called an *authentication*, is not as obvious for the service-providing organization as in the single-organization case. If the confirmation cannot be established, then a malicious user may try to access a service by asserting a role that the user does not actually have.

It is essential in the trans-organizational RBAC to realize a secure authentication mechanism, and this problem can be solved using two approaches. The first approach is to utilize digital certificates that are protected by the digital signatures of the role-issuing entities. This kind of certificate is sometimes called an attribute certificate [2] and is regarded as a digitalized version of physical certificates, such as ID-cards. The problem in this approach is the maintenance cost of the public-key infrastructure (PKI) [6][7]. Different from written signatures, continuous efforts are essential to keep digital signatures secure and functional. PKI is widely recognized as expensive, and this cost issue prevents small organizations from participating in a PKI-based framework. The second, rather political, approach to the authentication problem is to arrange a mutual agreement between role-issuing organizations and service-providing organizations. If several organizations share an identical benefit, then they can set up a partnership and mutually disclose their user-role assignments. A good example of this approach can be found in the Shibboleth project [3], but we need to remark that this framework is essentially a semi-closed one. An organization will not be allowed to join the partnership if that organization cannot offer recognizable benefits to the organizations involved, consequently limiting the trans-organizational utilization of roles.

III. Hierarchical ID-Based Encryption

A public-key encryption is a cryptography that utilizes two different keys for encryption and decryption. In a typical public-key encryption, such as RSA [8], a user sets up his/her key pair by himself/herself. One of the keys in the key pair is called an encryption key and is disclosed to the public. The other key is called a decryption key and is kept secretly by the user. In many cases, the keys are constructed from randomly selected information, which means that the

 ISBN: 978-1-61208-365-0

keys look like random data. A separate mechanism, such as PKI, is needed to associate public encryption keys with users. However, PKI makes the system complicated and costly [6][7].

An ID-based encryption [4] is a special public-key encryption. Different from the usual public-key encryption, a user first chooses his/her encryption key. An interesting point in the ID-based encryption is that, under an appropriate setting, one's identity, such as an e-mail address, can be used as an encryption key. After choosing the encryption key, the user submits the encryption key to a trusted authority which we call a *key generator*. The key generator examines the eligibility of the user and then, upon confirmation of the user's eligibility, computes the decryption key that corresponds to the submitted encryption key. Different from the usual public-key encryption, the correspondence between users and encryption keys becomes obvious if the identities of users are chosen as the encryption keys. Consequently, the costly mechanism of PKI is not needed in the framework of ID-based encryptions [4].

The HIBE [5] is an extension of the ID-based encryption wherein identities and functions of the key generator are realized in a hierarchical manner. In this paper, we write a hierarchical identity (abbreviated simply as ID) by a sequence of strings $S = s_1.s_2.\dots.s_n$, where n is a non-negative integer called a *level* of S, and s_i with $1 \le i \le n$ is a string. If an ID $S = s_1.s_2.\dots.s_n$ is a prefix of $S' = s'_1.s'_{\prime}.\dots.s'_{n'}$, then we say that S is a *super-ID* of S' and S' is a *sub-ID* of S. In HIBE, an ID can be regarded as an encryption key by itself, although, it is sometimes convenient to distinguish IDs from encryption keys explicitly. In the following discussion, we write ek_S and dk_S for the encryption and decryption keys that correspond to the identity S, respectively. In the original ID-based encryption, all decryption keys are solely generated by a trusted key generator. In HIBE, however, the generation of decryption keys is made in a hierarchical manner; the key pair $(\mathrm{ek}_S, \mathrm{dk}_S)$ for a level-one ID $S = s_1$ is generated by a designated key generator which we call a *root key generator* and is issued to an appropriate user who is eligible to hold the key pair. A user who has a key pair $(\mathrm{ek}_S, \mathrm{dk}_S)$ for an ID S can generate a key pair $(\mathrm{ek}_{S'}, \mathrm{dk}_{S'})$ for an ID S' that is a sub-ID of S. The functions used in HIBE are described below. There is complicated mathematics behind these functions, but we omit them because they are not the subject of this study. The main body of HIBE consists of the following four procedures:

Initialize() is a procedure that is executed by the root key generator in the initialization of the HIBE system. This procedure determines the public and secret parameters used in the system. The secret parameter is kept secretly by the root key generator, and the public parameter is disclosed to the public. The value of the public parameter is used in the following three procedures, although we do not write them explicitly in the notation for simplicity.

KeyGenerate($\boldsymbol{S}$, $(\mathbf{ek}_{S'}, \mathbf{dk}_{S'})$) is a procedure that computes the decryption key for the given ID S. More precisely, the procedure generates dk_S if S is a sub-ID of S' and $\mathrm{dk}_{S'}$ is a correct decryption key of S'. If not, the procedure fails to compute dk_S. We remark that dk_S cannot be computed if one does not know a correct decryption key of a super-ID of S.

Encrypt($\boldsymbol{k}, \boldsymbol{m}$) encrypts data m by using k as an encryption key.

Decrypt($\boldsymbol{k}, \boldsymbol{c}$) decrypts data c by using k as a decryption key.

If $(\mathrm{ek}_S, \mathrm{dk}_S)$ is a key pair that is correctly generated by KeyGenerate and $c = \mathrm{Encrypt}(\mathrm{ek}_S, m)$ is an encryption of m constructed by using the encryption key ek_S, then $\mathrm{Decrypt}(\mathrm{dk}_S, c)$ returns m.

HIBE is useful when used in a challenge-response authentication protocol. Consider a scenario that involves two people, a *prover* and a *verifier*. The prover asserts himself/herself as a genuine user with an identity S, but the verifier is not sure if this assertion is true or not. In this case, the verifier can determine if the prover is genuine or not by executing the following steps. First, the verifier chooses a random message m, and then encrypts m by using the encryption key ek_S for the asserted ID S. The obtained ciphertext $c = \mathrm{Encrypt}(\mathrm{ek}_S, m)$, which is called a *challenge*, is passed to the prover. The prover is requested to decrypt c by using the decryption key dk_S that a genuine user should possess. If the prover returns m as the result of the decryption, then he/she succeeds to make a correct *response* and is authorized as a user with the identity S. If the response is wrong, then the prover is rejected. Through this challenge-response protocol, the verifier is able to determine if the prover has the ID S. At this point, it should be noted that the ID S is indeed a hierarchical identity; the fact that the prover posseses the decryption key dk_S means that somebody who had a certain super-ID of S authorizes the prover to have the identity S. In other words, with the challenge-response protocol, the prover confirms a "chain of trust" that originates from the root key generator. This scenario is favorable in an open system with many unspecified users.

IV. Proposed Scheme

A. Overview

We now consider an authentication mechanism that is suitable for the trans-organizational utilization of roles. Our idea is to represent roles by hierarchical identities that work as encryption keys of HIBE. For example, if we would like to define a "student" role of A-university, then a hierarchical identity, such as "A-univ.student", is introduced and used as an encryption key of HIBE. Decryption keys are managed so that users with a role r possess the correct decryption key dk_r of r. A service-providing organization can verify if a user has the role r by examining the user by using the challenge-response protocol with r used as an encryption key of HIBE. Note that the service-providing organization does not have to know anything about r beforehand and does not have to make any contract or inquiry to the role-issuing organization that has assigned r to the user because r itself is used as an encryption key. This feature makes it easy to verify the user-role assignment of users even if the role is issued by another organization. In the proposed framework, there is no essential difference between users and role-issuing organizations because they both receive valid key pairs from superordinate entities and they both have the ability to generate new roles and corresponding key pairs by utilizing their keys in possession. However, for an easy understanding of the proposed framework and for simplicity, we will distinguish users from role-issuing organizations and introduce three component procedures that are needed for defining a user-role assignment. In the following, we extend the hierarchical notions of IDs to roles. If r_1 is a super-ID of another ID r_2, then the role represented by r_1 is a *super-role* of the role represented by r_2. The term *sub-role* is defined in the same way.

B. Procedures

Fig. 1 shows the overall structure of the proposed model. In this model, we assume the existence of a designated root key generator that is trusted by all users and organizations. The root key generator executes Initialize() of HIBE and determines the public and secret parameters. The public parameter is disclosed to the public and should be accessible to all users and organizations. The root key generator secures the secret parameter and uses it to generate key pairs for level-one roles.

1) Setting up an organization

An organization o_1 chooses its identity string, say S_{o_1}, and requests the root key generator to approve that the organization uses S_{o_1} as its identity. If the root key generator approves the request, it computes the decryption key $\mathrm{dk}_{S_{o_1}}$ and sends this key to o_1 by using a secure communication channel. As a result, o_1 possesses a correct key pair $(\mathrm{ek}_{S_{o_1}}, \mathrm{dk}_{S_{o_1}})$ of its identity S_{o_1}. The organization o_1 then defines the set R_{o_1} of roles it should manage. All roles in R_{o_1} must be sub-roles of S_{o_1}, where the identity S_{o_1} is regarded as a "role". Note that o_1 can compute the decryption key of any role $o_1.r \in R_{o_1}$ by utilizing the function $\mathrm{KeyGenerate}(o_1.r, (\mathrm{ek}_{S_{o_1}}, \mathrm{dk}_{S_{o_1}}))$, because o_1 knows the correct key pair $(\mathrm{ek}_{S_{o_1}}, \mathrm{dk}_{S_{o_1}})$ and $o_1.r$ is a sub-ID of S_{o_1}.

On the other hand, organizations other than o_1 cannot compute the decryption key of the role $o_1.r$ because the trusty key generator does not disclose $\mathrm{dk}_{S_{o_1}}$ to other organizations. Identities of roles in R_{o_1} can be open to the public, but the corresponding decryption keys must be kept secret by organization o_1.

2) Defining a user-role assignment

To assign a role $o_1.r$ to a user u, the organization o_1 gives the key $\mathrm{dk}_{o_1.r}$ to user u by using a secure communication channel. User u records $\mathrm{dk}_{o_1.r}$ as the decryption key of the role $o_1.r$, and keeps the key secure.

3) Verifying a user-role assignment

Assume that a user u visits a service-providing organization o_2 and asserts that he/she has the role $o_1.r$ that was assigned by the role-issuing organization o_1. The organization o_2 needs to verify if the assertion of user u is true or not. The verification can be done by using the challenge-response protocol; the organization o_2 chooses a random data m and requests user u to decrypt $c = \mathrm{Encrypt}(\mathrm{ek}_{o_1.r}, m)$. Note that we are using HIBE, and the encryption key $\mathrm{ek}_{o_1.r}$ is the same as (or easily derived from) the hierarchical identity $o_1.r$ of the asserted role. If the user really has the role $o_1.r$, then he/she must possess the decryption key $\mathrm{dk}_{o_1.r}$ that is provided by the organization o_1 and should be able to decrypt the challenge c. Remark that the service-providing organization o_2 can verify if the user u holds the role $o_1.r$ without querying the role-issuing organization o_1 and that user u has little chance to disguise his/her role.

C. Managing Roles

1) Personalization of roles

In the proposed framework, the relation between users and roles is represented by the possession of cryptographic keys by users. This approach involves a possible security risk; a leakage of keys. If, for example, a role r is assigned to several users, then all those users have the same key dk_r. If one of those users is unconscious of security, then he/she may let other persons use the key dk_r. Such an inappropriate usage of keys can obstruct fair and reliable access control. To deter such irresponsible behavior of users, a role-issuing organization can "personalize" a role by appending an additional string to the identity of roles. Assume for example that there are several students in A-university. In this case, instead of using a general role, such as "A-univ.student", the university can define personalized roles, such as A-univ.student.Alice and A-univ.student.Bob, and provide

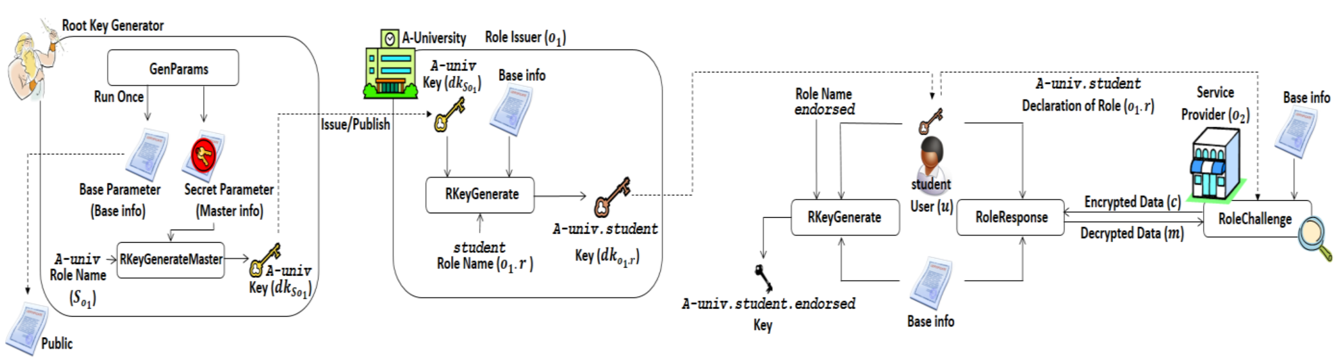


Figure 1. Overview of the proposed structure.

decryption keys of these roles to Alice and Bob, respectively. With this kind of personalization, a student will be more conscious of leaking/losing his/her key to another person because he/she will have the risk of being identified and subsequently punished for irresponsible behavior. The theft/loss of keys remains a risk, but such risk also exists for ID-cards used in the real world. We cannot say that the proposed framework is “more secure than” but we may say it is “as secure as” the real-world role management.

2) Hierarchical issuance of roles

In the proposed scheme, there is no essential difference between organizations and users. A user can compute decryption keys from the key that he/she already has and issue a new sub-role of the role that he/she already has. This function can be used to realize some personal activities that are not considered in the conventional RBAC approach. One possible example is the endorsement of another person. In the real world, an endorsement among individuals sometimes plays an important role. Semi-closed organizations, such as academic societies and golf clubs, have the tradition or policy that a newcomer must be endorsed or referred by a current member. This mechanism can be realized using the proposed scheme. Consider for example that Alice is an authorized member of XYZ golf club and is given a personalized role “XYZ-golf.member.alice” and its corresponding decryption key. If Alice would like to endorse Bob to the club, then she can generate a new sub-role “XYZ-golf.member.alice.endorsed” and its corresponding decryption key. By providing the decryption key to Bob, Bob can demonstrate that he is really endorsed by Alice. Using the HIBE and the challenge-response authentication, the club does not have to inquire Alice for the verification of the endorsement. Besides personal endorsement, we conjecture that a broad range of personal relations can be implemented by utilizing the hierarchical roles.

V. REALIZATION

The proposed scheme was implemented in Android-enabled mobile devices. In the proposed scheme, the user-role assignments are represented by possession of decryption keys by users. A role-issuing organization does not have to construct and maintain large databases for recording the user-role assignments, and it does not have to be bothered by inquiries of other organizations with regard to user-role assignments. The created Android application implements all the functions of the HIBE and the proposed scheme for ease of use and accessibility.

The prototype contains several functions that correspond to components in Fig. 1. The functions of the root key generator mainly consist of two operations: GenParams and RKeyGenerateMaster. GenParams utilizes the Initialize() function of HIBE and generates the public and secret parameters, where the public parameter is disclosed to the public. An organization o_i that would like to participate in this system chooses its identity, say S_{o_i}, and asks the root key generator to compute the decryption key $\mathrm{dk}_{S_{o_i}}$. The root key generator utilizes RKeyGenerateMaster to compute $\mathrm{dk}_{S_{o_i}}$, which needs the information of the secret parameter and hence this function is accessible to the root key generator only. The generated key $\mathrm{dk}_{S_{o_i}}$ is transferred to the organization o_i through general communication means, such as Wi-Fi, Bluetooth, Android Beam, and NFC. The role-issuing organization o_i now has the key pair $(\mathrm{ek}_{S_{o_i}}, \mathrm{dk}_{S_{o_i}})$ for the ID S_{o_i}. By using the function of RKeyGenerate, this key pair, and the public parameter that has been disclosed, the organization o_i can compute valid key pairs of sub-IDs of S_{o_i}. A user receives, possibly many, keys from organizations, each of which corresponds to a role in an organization. The user safely stores these keys in his/her device and accesses them for the RKeyGenerate and RoleResponse functions. RoleResponse provides the function of the prover for the challenge-response authentication and interacts with the RoleChallenge function that is invoked by a service-providing organization.

The cryptographic operations used in these functions are performed using the Java Pairing-Based Cryptography (JPBC) library [9], which is a collection of classes and methods for handling underlying pairing-based cryptosystems. Over JPBC, we implemented the HIBE that was proposed by Gentry [5].

The most complicated but important communication in the proposed scheme is the challenge-response authentication between a user and a service-providing organization. Several messages must be exchanged between two devices, and we provide two different schemes to realize this communication, namely, the use of near-field communication (NFC) and quick-response (QR) codes.

NFC is a contactless technology used to transmit small amounts of data across short distance. NFC has three modes of operation, and this study tackles only P2P mode. NFC messages in Android are handled using the NFC Exchange Format (NDEF). In the proposed Android application, the Intent Filters that listen to the intent action of NfcAdapter.ACTION_NDEF_DISCOVERED were added to the RoleChallenge and RoleResponse activities to be able to receive NFC data [10][11]. Only the MIME type of text/plain was included in the application as we are only concerned with passing and receiving data of type string. Given that at least two activities have the same intent filter that responds to an NFC tap, users are, by default, prompted to select which application in the mobile device to use, making the application tedious to use. To solve this problem, the foreground dispatch system was utilized. The foreground dispatch system is used to make a particular activity have priority over other activities. This allows a particular activity to become the default receiver when it is on the foreground.

QR Code is a type of 2D barcode that is capable of handling different types of data [12]. This code can accommodate high capacity of data in a small area, which is sufficient to include the challenge-response data in one code symbol. The camera hardware of mobile phones can be used as scanners for QR codes generated for the challenge/response actions. For this implementation, the camera hardware of the device was programmed and the ZXing (“zebra crossing”) library, which is an open-source library that supports the decoding and generation of barcodes, was used to obtain the data [13]. This feature allows the interaction of two users without NFC-capable devices and without the Internet.

Typically, the challenge-response authentication is carried out as follows:

1. A user, the prover, opens the application and goes to the "Role Response" option. Then, the prover selects the base file that contains the public parameter and the role file that contains the role he/she wants to use.
2. A service-providing organization, the verifier, opens the application and goes to the "Role Challenge" option. To start the verification process, the verifier selects the same base file and either types the role indicated by the prover or obtains the role automatically via NFC (first tap). Once the role is received, a random challenge data is created.
3. The verifier then sends this challenge data to the prover via NFC (second tap) or by generating a QR code for the prover to scan.
4. After receiving the challenge data via NFC or scanning of the Challenge QR Code, a random response data is calculated and created in the prover's device based on the role file selected.
5. The prover then sends this response data to the verifier, again, via NFC (third tap) or by generating a QR code for the verifier to scan.
6. After receiving the response data via NFC or scanning of the Response QR Code, the Role Challenge indicates if the assumed role is verified or is a mismatch.

Several screen shots of the prototype are shown in Fig. 2. Another possibility for the realization of the user-side system is through the use of smartcards that are compatible with the NFC technology [14].

VI. Conclusion and Future Work

A trans-organizational RBAC is considered and extended to represent the trans-organizational usage of roles. The proposed scheme provides a secure mechanism for verifying the user-role assignments of organizations. The proposed scheme was developed on Android-enabled mobile devices for ease of use and accessibility. Compared to other similar approaches, the proposed scheme provides more flexibility and autonomy while maintaining security. This mechanism allows the realization of many collaborative right managements that are common in physical communication but are difficult to implement over computer networks. Even with the given advantages, the proposed scheme remains subject to the classical issue of compromised secret keys; the proposed scheme is based on the assumption that keys are managed appropriately and protected well. If dk_S is compromised for an unfortunate reason, the keys of the sub-roles of S should be redeployed. This problem can be mitigated by utilizing the personalized and fixed-term roles, but it is encouraged in general to provide more protection for the keys of roles of higher-level. Taking such issue into consideration, future research will focus on the inclusion and integration of expiration dates on the roles. Moreover, the prototype will be expanded to non-Android devices, such as iPhones and Windows mobile devices, for interoperability.

References

[1] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," IEEE Computer, 29, 2, pp. 38–47, 1996.

[2] S. Farrell and R. Housley, "An internet attribute certificate profile or authorization," RFC 3281, 2002.

[3] The Shibboleth System, accesible online: http://shibboleth.internet2.edu/ [accessed: 2014-05-08].

[4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Proc. of the Advances in Cryptology (CRYPTO) 2001, pp. 213–229, 2001.

[5] C. Gentry and A. Silverberg, "Hierarchical ID-based cryptography," Proc. of the Advances in Cryptology (ASIACRYPT) 2002, pp. 548–566, 2002.

[6] C. M. Ellison et al., "SPKI certificate theory," RFC 2693, 1999.

[7] P. Gutmann, "Simplifying public key management," IEEE Computer, 37, 2, pp. 101–103, 2004.

[8] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, 21, 2, pp. 120–126, 1978.

[9] A. De Caro and V. Iovino, "jPBC: Java pairing based cryptography," Proc. Of the IEEE Symposium on Computers and Communications (ISCC) 2011, pp. 850–855, 2011.

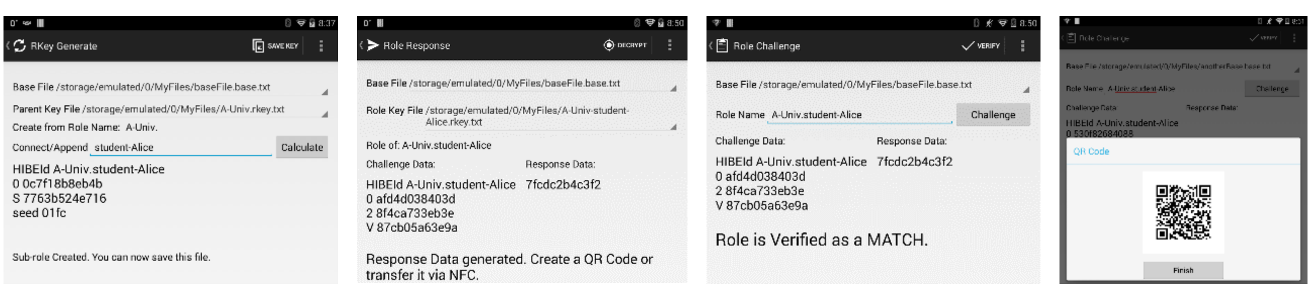
[10] R. Meier, "Professional Android 4 Application Development," John Wiley & Sons, Inc., Indianapolis, pp. 693–700, 2012.

[11] S. Komatineni and D. MacLean, "Pro Android 4," Apress, pp. 858–870, 2012.

[12] http://www.qrcode.com/en/ [accessed: 2014-05-08].

[13] https://github.com/zxing/zxing [accessed: 2014-05-08].

[14] M. Scott, N. Costigan, and W. Abdulwahab, "Implementing cryptographic pairings on smartcards," Proc. of the Cryptographic Hardware and Embedded Systems, pp. 134–147, 2006.



(a) (b) (c) (d)

Figure 2. (a) RkeyGenerate, (b) Role Response, (c) Role Challenge, and (d) QR Code functions of the application.

Scalable and Self-configurable Eduroam by using Distributed Hash Table

Hiep T. Nguyen Tri, Rajashree S. Sokasane, Kyungbaek Kim
Dept. Electronics and Computer Engineering
Chonnam National University
Gwangju, Republic of Korea
e-mails: {tuanhiep1232@gmail.com, sokasaners@gmail.com, kyungbaekkim@jnu.ac.kr}

Abstract—**In the recent years, the number of increased Wi-Fi networks and Wi-Fi-enabled devices shows how fast Wi-Fi technology is growing. Since a single network provider is usually not able to ensure Wi-Fi coverage for its own users across many geographic locations, we need Wi-Fi roaming. Eduroam is a Wi-Fi roaming system, which allows a user of a domain to access wireless resources in another domain with the unique credential of the user managed in the original domain. The authentication process in Eduroam is based on the hierarchical tree structured Remote Authentication Dial-In User Service (RADIUS) servers over wide area networks. Existing RADIUS-based tree structure of Eduroam is not self-configurable; joining/leaving of node is not automatically handled by the existing approach and it takes high communication delay as well. In order to improve the scalability of Eduroam with self-configurable feature and reduce communication delay as compared with tree structure-based Eduroam, we hereby proposed a Scalable & Self-configurable Eduroam by using Distributed Hash Table (DHT). Through a prototype implementation, we showed that the proposed system supports high scalability and high fault tolerance.**

Keywords-DHT; Eduroam; RADIUS server; Wi-Fi roaming.

I. INTRODUCTION

Wi-Fi technology has become increasingly popular due to its flexibility and mobility; as a result, the need of Wi-Fi roaming systems is increasing. The Eduroam [1] is a secure roaming system between educational institutions. The Eduroam allows users to access the Internet with their own credentials at visiting institution during roaming. The Eduroam principle is based on the fact that the user's authentication is done by the user's home institution, whereas the authorization decision allowing access to the network resources is done by the visited network. The authentication process of Eduroam is based on hierarchical tree structured RADIUS servers. However, hierarchical tree structure approach in Eduroam causes long communication delay, and also exposes a single point of failure because every authentication traffic flows through the tree hierarchy even though it is only of interest to a leaf RADIUS server. To overcome these issues of tree structured Eduroam, we developed a Flat Layer RADIUS server model with Eduroam in our previous work [9]. The Flat Layer RADIUS server model effectively reduces communication delay and avoids single point of failure.

In the Flat Layer RADIUS server model, we assumed that every node in the network must know about all other nodes in the network. In the Flat Layer RADIUS server model, each node (RADIUS server) directly communicates with each other, without using any intermediate RADIUS proxy servers. To evaluate the performance of the Flat Layer RADIUS server model and compare with tree structure model, we setup experiments by using open source based freeRADIUS (version 2.1.8) and ubuntu (version 10.04.4) as RADIUS server. Table I shows the authentication time comparison between the tree structure and the Flat Layer RADIUS models. Note that the authentication time includes request forwarding process, authentication process, network latency and response forwarding process. Table II shows request processing time of three stages in authentication process. From Table I, we can observe that Flat Layer RADIUS server model takes less authentication time than RADIUS-based tree structures.

TABLE I. AUTHENTICATION TIME (μS)

	Tree structure		Flat Layer RADIUS model
	3 hops away	*2 hops away*	
Request Forwarding Process	1155	711	273
Authentication Process	330	237	242
Response Forwarding Process	559	278	134
Network latency	620823	402997	201330

TABLE II. REQUEST PROCESSING TIME

Process/machine	Time in μs
Request Forwarding	357
Authentication	270
Response Forwarding	162

However, the Flat Layer RADIUS server model may face the scalability issue. If a node operation, such as joining or leaving the network, takes place all nodes in the network need to be updated to stay up-to-date with latest membership information of the network. If the number of nodes in the network goes up, the data transfer between all nodes lead to overhead and updating operation to all nodes takes much time, it may cause for bottleneck. Flat Layer RADIUS server model works well with small scale, but when the members in the network are going to be increased the maintenance cost is also increased with it.

Recently, to resolve scalability issues in many distributed systems, DHTs have been largely adopted as a useful substrate to the design and specification of scalable and self-configurable distributed systems. The basic operation in DHT-based systems is lookup (key), which returns the node controlling the region of the space corresponding to that key. In the lookup structure, DHT nodes form an overlay network where each node has a number of neighbors. One lookup (key) messages are then routed through the overlay network to the node responsible for that key.

In this paper, we propose Scalable and Self-configurable Eduroam by using DHT, in order to improve the scalability of Eduroam and make it self-configurable in case of joining/leaving node operation takes place frequently. In the proposed system, RADIUS servers run on DHT substrate and they form a DHT-based RADIUS network. A RADIUS server manages a single domain. It uses the domain name as a key and uses its IP address and port number as the concatenated string for a value in the DHT-based network. In the DHT-based RADIUS network, node joins and leaves are handled automatically by obeying the updating rules of DHT. When a client sends an authentication request, RADIUS server which receives the request will forward it to the corresponding RADIUS server through a DHT lookup operation with the target domain name of the request.

We implement the DHT-based RADIUS network for scalable and self-configurable Eduroam by modifying the freeRADIUS server with the bamboo DHT substrate. Through the extensive evaluation and the implementation, we observe that the proposed system is scalable and self-configurable. The paper is organized as follows. Section II describes Eduroam, DHT and our previous work on the Flat Layer Approach. Section III explains the detailed design of the proposed system. Next, we evaluate proposed system in Section IV. Finally, Section V concludes the paper.

II. BACKGROUND

This section provides an overview of the Eduroam, authentication process and related protocols, such as RADIUS and DHT.

A. Eduroam

Eduroam was originally proposed by TERENA (Trans-European Research and Education Networking Association) [1]. Eduroam allows students, researchers and staff from home institutions to obtain Internet connectivity when visiting other institutions. The Eduroam principle [1] is based on the fact that the user's authentication is done by the user's home institution, whereas the authorization decision allowing access to the network resources is done by the visited network. Eduroam is based on the most secure encryption and authentication standards in existence today [1]. It gives an access to authorized users only.

The Eduroam is based on hierarchical structured RADIUS proxy servers and IEEE 802.1X. Figure 1 shows an example of the RADIUS proxy tree in Eduroam. When a user accesses an Access Point (AP) in the network of visited institution, authentication information is transmitted from visited institution to user's home institution through RADIUS proxy tree [2]. If the authentication is successful, the user can access the network of visited institution.

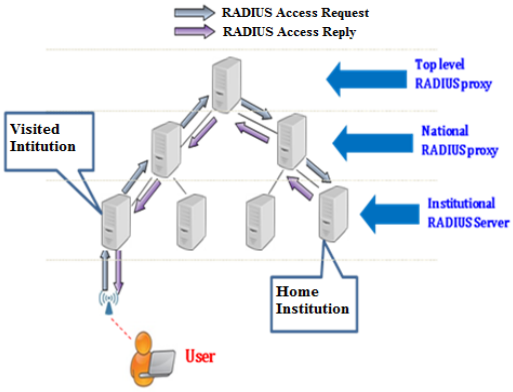


Figure 1. RADIUS-based tree structure in Eduroam.

When a user tries to log on to the wireless network of a visited Eduroam-enabled institution, the user's authentication request is sent to the user's home institution. This is done via a hierarchical system of RADIUS servers. The user's home institution verifies the user's credentials and sends to the visited institution (via the RADIUS servers) the result of such verification.

B. Ditributed Hasht Table

In a peer-to-peer system, every node in the system plays the same role; each node has a piece of system data. In this case, looking up data has an important role in the distributed system. DHT provides a lookup service to help peer-to-peer system or other distributed applications to locate data more efficiently. DHT uses a key that is generated by hashing function to locate node which contains the value [4][5][6].

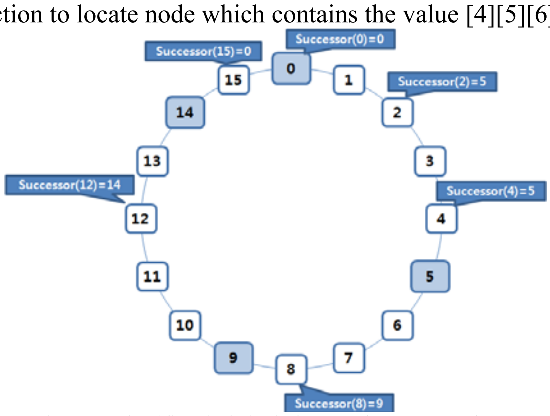


Figure 2. Identifier circle includes 4 nodes 0, 5, 9 and 14.

In a basic consistent hashing approach, nodes and value keys are hashed onto a circle ring, shown in Figure 2. The value keys are assigned to the nearest peer in the clockwise direction. Each node in the network maintains a routing table, which contains references of other nodes. In Pastry [6], the leaf set contains information about the closest node in identifier space. Routing table contains information of nodes whose identifier shares the present node’s identifier in the first n digits and whose $(n+1)^{th}$ digit has one of the 2b-1 possible value. The neighborhood set contains information of the closest (according the proximity metric) nodes.

When there is a request to lookup data which is mapped to a key, firstly, Pastry lookups in leaf set. If the key identifier is within range of leaf set the message will be forwarded to the closet node in leaf set; otherwise, Pastry lookups routing table. The message is forwarded to a node that shares a common prefix with the key at least by one more digit. If there is no node in routing table satisfying that condition, the message will be forwarded to the node that shares a prefix with the key at least as long as the local node. The node is chosen in a set, is built from leaf set, routing table and neighborhood set.

DHT is conventional and popularly used in Peer-to-Peer system; BitTorrent [10][11][12][13][15] are examples of system or research related to DHT. DHT is also considered to support the Domain Name System (DNS) [12][13][15]. DNS which is used to translate domain name into IP address is a hierarchical distributed naming system [14]. Each node or leaf has resource records which contain domain name information. The tree is divided into zones. Each zone contains one or many domains. The tree begins at root zone. When a client wants to look up a domain name, the client sends request to root. Based on resource records, the root returns information of next node. If the node is responsible for the domain name, the node will return the IP address and the lookup process will end; otherwise, the node will return the information of next node. Cox implemented and evaluated DDNS, which is a system that is based on Chord and has the same function of DNS [15]. DDNS is self-configurable, so DDNS eliminates the pain of name server administration. DDNS also inherits good load balancing and fault tolerance. As we can see, DNS has the similar structure with Eduroam. Therefore, combination of DHT and Eduroam puts forward a promise to improve scalability and self-configuration to the Eduroam system.

C. Flat Layer Approach

In order to improve the performance of the authentication process in Eduroam, a Flat Layer approach was proposed by Sokasane and Kim [9]. In the Flat Layer RADIUS server model, the authentication delay is reduced because the visited institution server directly forwards the request to the home institution server. Flat Layer approach also helps system to avoid single point of failure problem.

Figure 3 depicts the structure of Flat Layer approach. When the visited institution RADIUS server receives an authentication request from user proxy by AP, the RADIUS server checks the user information in its database. If the domain name contained in the authentication request is a local domain, the authentication request will be handled locally; otherwise, the visited institution's RADIUS server will forward the authentication request directly to the home institution RADIUS server, based on the domain name information provided in the request. In order to direct forwarding authentication request to home institution server, each RADIUS server in system must know the information of all other RADIUS servers in the system. So, the total hop count message that passes through to reach the destination is just one. Consequently, authentication delay is reduced.

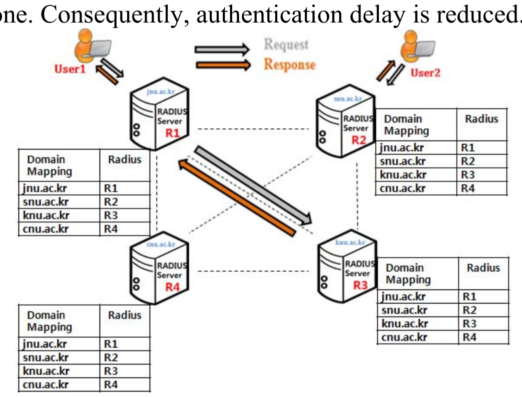


Figure 3. Flat Layer Approach.

Even though the Flat Layer approach reduces the authentication delay as well as avoids single point of failure, it has some disadvantages. The first disadvantage is scalability problem. As we said before, each RADIUS server must know the information of all other RADIUS servers present in the system. If a new RADIUS server joins or leaves, all RADIUS servers need to update their information. If there are a large number of RADIUS servers in system, the cost of updating information is very big.

III. PROPOSED SYSTEM

Although Eduroam is the secure roaming system between research and educational institutions, it has some disadvantages, especially with its RADIUS-based tree structure. Every authentication traffic flows through the whole hierarchy [3] even though it is only of interest to a leaf RADIUS server that causes high communication delay. Also, the existing RADIUS-based tree structure is not self-configurable and raises scalability issues.

To mitigate the disadvantages of Flat Layer RADIUS server model, we proposed a peer-to-peer based Eduroam approach. In this section, we will present proposed system in detail.

In DHT, data is distributed across nodes by using the hash function, and a routing scheme is implemented to efficiently look up the node on which data item is located. In DHT-based RADIUS server model, each node knows information about related nodes only. DHT provides a protocol for looking up the node in which data item is located [7]. DHT has some advantages, such as scalability, availability [5], self-configuration, and it only affects a set of nodes rather than every other node in system. When a new node joins the system, the system will redistribute data. The new node is automatically configured to build its routing table. This process will affect only a small set of nodes in the system, instead of affecting all nodes in the system. It helps to reduce the cost of data transferred.

In our proposed system, we consider DHT as lookup service. Figure 4 shows the architecture of proposed system. The system includes AAA servers (RADIUS) and DHT agents (or DHT nodes), which are parts of DHT system. In the proposed system, RADIUS server contains domain information of related domain(s) only rather than all domain(s) information present in the system. DHT agents play a very vital role. A DHT agent works as lookup service, which responds with the information of requested domain(s). In the proposed system, the DHT agent is responsible for finding appropriate domain information and sending it to visited institutions RADIUS server, then RADIUS server of visited institution sends user information to user's home institutions RADIUS server to get verification of user.

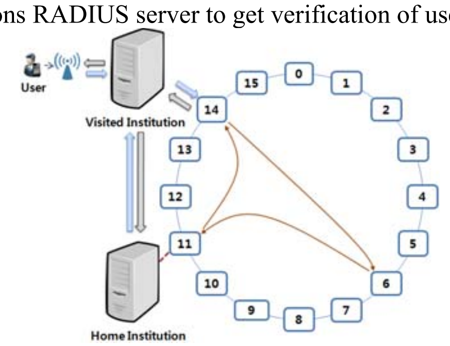


Figure 4. Architecture of Scalable and Self-configurable Eduroam.

The workflow of the proposed system is as follows (see Figure 6). While roaming, when a user wants to access the network of visiting institution through the credentials of home institution, the user needs to send an authentication request with user@domain.name format. At this point, the RADIUS server checks the domain name that user requested for; if the domain name of the authentication request is local domain name of the authentication server, authentication server will find it in database of local server. The database can be a database server or just a configuration file. If the username exists in the database, authentication server will respond Accept-Accept message otherwise authentication server respond Accept-Reject. If the domain name of the authentication request is not a local domain name of the authentication server; this is the case when a user wants to access the visited institution server. The visited institution's RADIUS server does not contain the user information; so, the visited institution RADIUS server needs to forward the message to the home institution's RADIUS server, where the user information is kept. After that, the visited institution's RADIUS server will send lookup request to the node called visited DHT node of DHT system. Each node in the DHT system contains a unique domain name regarding the domain name of the user. The visited DHT node employs the lookup function of the DHT system to send a lookup message to the home DHT node that hold home institution's information. The home DHT node will send a response message which contains the home institution server information to the visited DHT node. And then, the visited DHT node sends the response message to the visited institution's RADIUS server. The visited institution's RADIUS server forwards the authentication request to the home institution's RADIUS server based on the information that the DHT system returns. In the home institution's RADIUS server, the process is almost same with the first case except the response message is returned to the client through the visited institution's RADIUS server.

In the next sub-sections, we will discuss more detail about AAA server and DHT agent.

A. *Implemeting AAA server*

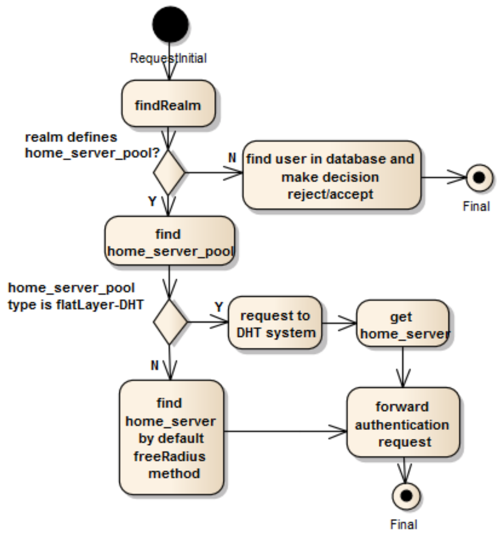


Figure 6. Work flow of DHT-based RADIUS server module.

In the Eduroam system, the freeRADIUS is used as an AAA server. The authentication process of the freeRADIUS is as follows; firstly, the freeRADIUS finds the correct realm based on the domain name given in the request.

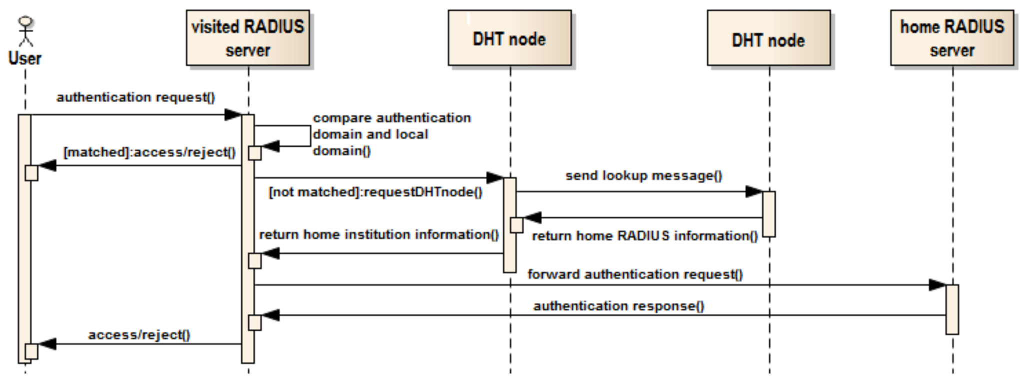


Figure 5. Proposed system flow.

 ISBN: 978-1-61208-365-0

Realm is an object that contains information to make the decision, either the request is forwarding to the other domain or to handle it locally. If the founded realm does not contain any server pool information, the requested domain name is the local domain and it should be handled by the local server; otherwise, the freeRADIUS finds the server pool for the requested domain name. The server pool contains information of the candidate home institution servers. In the home server pool, the candidate home servers and its type (property- that controls how home servers are chosen) are listed. By default, the type property can be assigned to one of the 6 values including fail-over, load-balance, client-balance, client-port-balance and keyed-balance. Based on the type value, server can choose the appropriate home institution server to forward the request.

With the backward compatible purpose, if in the case, we need to request to the DHT system to get information of the home institution server, we decided to assign a new value to the home server pool type. We added a module in the freeRADIUS, which is responsible for requesting and getting results from the DHT system. If the type property of home_server_pool object is "flatLayer-DHT", then the newly added module will be executed. Figure 5 shows the work flow of the DHT-based RADIUS server module in the proposed system.

B. Implementing DHT agent

A DHT agent node is a part of DHT-based system, which works as lookup service of the proposed system. We decided to use bamboo-dht [8] as a routing layer to implement the DHT agent. Figure 7 shows the architecture of DHT agent. The freeRADIUS service module is responsible for receiving the requests from the freeRADIUS and returning the results. Bamboo routing is a routing layer module that provides routing API. After receiving a request from the freeRADIUS, the freeRADIUS service uses the bamboo routing layer to send a lookup message to the DHT node, which holds the information of the home institution's server. When the destination DHT node receives the lookup message, the destination DHT node send a response message directly to the source DHT node, by using information attached in the lookup message. The source DHT node uses the message information to return to the freeRADIUS.

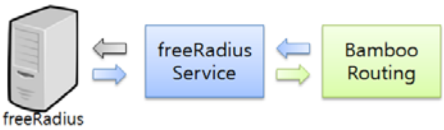


Figure 7. DHT agent architecture.

In this system, the domain name works as an identifier of each DHT node. Therefore, DHT system uses the domain name instead of the IP address and port to make an identifier. When a DHT node tries to join the system, it will send a joining request to the gateway node. The gateway node will send a message to the DHT node, that is identified by the domain name of the joining request and wait for the response. If the gateway node receives the response message within time out, the gateway node will reject the joining message. This will help to eliminate conflicting identifier in the DHT system.

IV. Evaluation

In order to evaluate our proposed system, we setup an environment in which we used 4 VMware machines. Each machine has CPU 3.4 GHz single core, 1 GB RAM and is running 64-bit ubuntu OS (version 10.04.4). We installed edited freeRADIUS (version 2.1.8) and bamboo-DHT which was modified based on the version released on March 3, 2006. On each machine we deployed the number of DHT nodes and the freeRADIUS with different configurations.

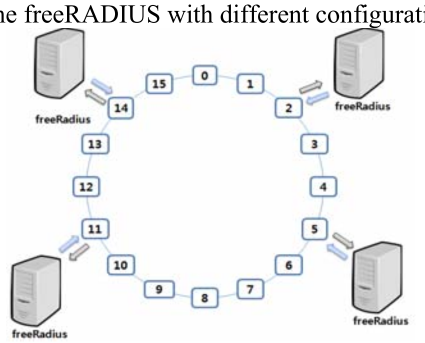


Figure 8. Evaluation architecture.

To evaluate the scalability of system, we conducted some experiments with the different number of the DHT nodes and the freeRADIUS nodes to obtain the hop count number. Figure 8 shows an example of test-bed system. Since visited institution's server forwards the request directly to the home institution's server, there is a difference between the number of DHT nodes and freeRADIUS nodes. Concretely, the number of freeRADIUS nodes increases from 3 to 10 and the number of the DHT nodes increases from 5 to 800.

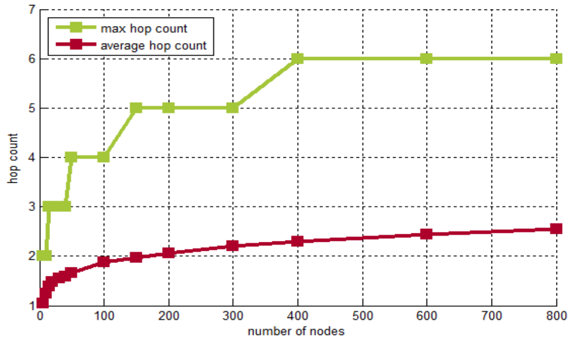


Figure 9. DHT look up hop count.

Figure 9 shows the number of hop count which is required to reach up to the destination DHT node. We can observe that the number of hop count is directly proportional to the number of nodes, but the increase speed of hop count is inversely proportional to the number of nodes. Although the number of nodes is up to 800 but the average hop count is 2.55.

Figure 10 shows the join time. The join time is a time period that a node needs to join completely the RADIUS network. During the join time, a node is unavailable. To

 ISBN: 978-1-61208-365-0

measure the join time, we continuously start DHT nodes up to 800 and check the time when the node is available. From Figure 10, one can observe that the join time becomes more fluctuated with more number of nodes. The maximum join time is less than 1 second even though the number of DHT nodes increases up to 800.

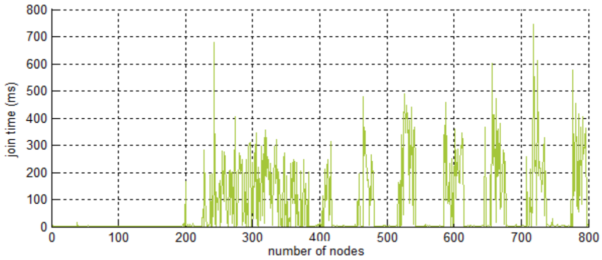


Figure 10. DHT node join time.

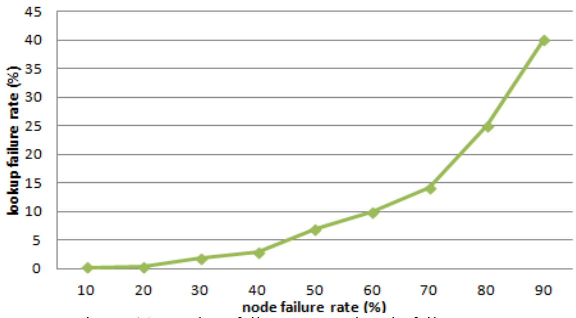


Figure 11. Lookup failure rate and node failure rate.

In order to test fault-tolerance of the system, we experimented in a network, which includes 800 DHT nodes. We simulated node's failure. We used a simple node failure model, which considers the crashing of node or the network failure. In the node failure model, all the failure nodes are simulated simultaneously. After simulated node's failure, we immediately sent successively lookup requests to the available DHT nodes, and we counted the number of failed lookup requests and total requests and calculated the lookup failure rate along with the node failure rate. The value of lookup timeout in this experiment is 10 seconds. Figure 11 shows the result of lookup failure rate and node failure rate. The lookup failure rate increases fast if the node failure rate is more than 40%. If the node failure rate is less than 40%, the lookup failure rate is small (<3%). The possibility of simultaneous failure of nodes is 40%, in reality is very small. Even though the failed node rate is 90%, the system is able to recover after just 1-2 minutes by itself.

V. CONCLUSION

In this paper, we presented experimental results of the Eduroam system that adopts DHT as a lookup service. The proposed system is scalable and self-configurable. We also evaluated fault-tolerance of the system. In the proposed system, the RADIUS servers run on DHT substrate and they form a DHT-based RADIUS network. A RADIUS server manages a single domain.

The proposed system should have a stable node which plays as a role of a gateway which will be used while new nodes join the system. When a new node wants to join, it requires connecting to one available node in the system. The proposed system has to face the problem of handling routing function when there are a huge number of nodes leaving the system.

AKNOWLEDGEMENT

This research was supported by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (NIPA-2014-H0301-14-1014) supervised by the NIPA(National IT Industry Promotion Agency).

REFERENCES

[1] Eduroam. https://www.eduroam.org [accessed: 2014-04-29]

[2] Y. Miyamoto, Y. Yamasaki, H. Goto, and H. Sone, "Optimization System of IP Address Using Terminal ID in eduroam" in Proceedings of 2011 IEEE/IPSJ International Symposium on Applications and the Internet, July. 2011, pp. 342 – 346, ISBN: 978-1-4577-0531-1.

[3] K. Wierenga and L. Florio, "eduroam: Past, Present and Future", Computational Method in Science and Technology, vol. 11 (2005), pp. 169-173, 2005.

[4] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, "A scalable content-addressable network", In Proc. ACM SIGCOMM'01, San Diego, CA, Aug. 2001, pp. 161-172.

[5] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan. "Chord: A scalable peer-to-peer lookup service for Internet applications", In Proc. ACM SIGCOMM'01, San Diego, CA, Aug. 2001, pp. 149-160.

[6] A. Rowstron and P. Druschel. "Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems", Proceeding Middleware '01 Proceedings of the IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg, 2001, pp. 329-350, ISBN:3-540-42800-3.

[7] Distributed Hash Table. http://en.wikipedia.org/wiki/Distributed_hash_table [accessed: 2014-04-29]

[8] The Bamboo Distributed Hash Table. http://bamboo-dht.org/ [accessed: 2014-04-29]

[9] R. Sokasane and K. Kim. "Flat Layer RADIUS Model: Reducing Authentication Delay in eduroam", In Proceedings of the 2nd International Conference on Smart Media and Applications, Kota Kinabalu, Malaysia, Oct. 2013, pp. 161-168.

[10] K. Kim and D. Park. "Efficient and Scalable Client Clustering for Web Proxy Cache" IEICE Transactions on Information and Systems, vol. E86-D, no. 9, Sept. 2003, pp. 1577-1585.

[11] K. Kim. "Lifetime-aware Replication for Data Durability in P2P Storage Network" IEICE Transactions on communications, vol. E91-B, no. 12, Dec. 2008, pp. 4020-4023.

[12] V. Pappas, D. Massey, A. Terzis, and L. Zhang "A Comparative Study of the DNS Design with DHT-Based Alternatives" In Proceedings of IEEE INFOCOM'06, Barcelona, Catalunya, Spain Apr. 2006, pp. 1-13, ISBN: 1-4244-0221-2.

[13] Y. Doi, "DNS meets DHT: Treating Massive ID Resolution Using DNS Over DHT", International Symposium on Applications and the Internet, Trento, Italy, Feb. 2005, pp. 9-15, ISBN: 0-7695-2262-9.

[14] Domain Name System. http://en.wikipedia.org/wiki/Domain_Name_System [accessed: 2014-04-29]

[15] R. Cox, A. Muthitacharoen, and R. Morris. "Serving dns using a peer-to-peer lookup service", In Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS), Cambridge, MA, Mar. 2002, pp. 155-165, ISBN:3-540-44179-4.

Integrated Learning Environment for Smart Grid Security

Kewen Wang, Yi Pan, Wen-Zhan Song
Department of Computer Science
Georgia State University
Atlanta, USA
kwang12@student.gsu.edu, {yipan, wsong}@gsu.edu

Weichao Wang
Department of SIS
UNC Charlotte
Charlotte, USA
weichaowang@uncc.edu

Le Xie
Department of Electrical and Computer Engineering
Texas A&M University
College Station, USA
Lxie@ece.tamu.edu

***Abstract*— Cyber Security of smart grids becomes more and more important to our everyday life for its wide implication in power systems, a critical infrastructure in a modern society. Many universities and corporations have put efforts in this field. However, there has been lack of emphasis on educational front of this important area. We believe that simulation systems designed for research purposes in the smart grid security should also be incorporated in education. Hence, this paper presents an integrated learning environment for the education of smart grid security. The core components of this environment are smart grid simulator and a learning website. Based on this learning environment, we design course projects and learning materials in teaching, so that students can better grasp the knowledge of smart grid security.**

Keywords-Cyber Security; Smart Grid Education; Learning Environment.

I. INTRODUCTION

With the widespread applications of smart grid, its security has raised significant interest and concerns among industries and academia [1]. A Department of Homeland Security report [2] shows that the vulnerability in smart meters and smart controllers could allow attackers to remotely compromise thousands of such devices and cause rolling blackout, which is a great threat to our everyday life. Significant efforts have been put on the research of such critical infrastructure services, with the example of several critical infrastructure research centers being established nationwide [3].

In contrast with strong emphasis on research in smart grid cyber security, the education programs fall behind in many aspects. For example, there is a lack of smart grid simulation software which provides a platform covering the essential components of corresponding security educational programs for teachers and students. Although some systems about the cyber security of smart grid become available for research purposes [4][5][6][7], few of them are suitable for education purposes because their software environment and programming interfaces are not available to students and instructors. The lack of this learning environment brings a huge difficulty for the education on smart grid security, which could train many people into fast developing industry [8][9] of smart grid and teach students necessary knowledge in this field.

Thus, it will be beneficial to solve this problem by developing a learning environment for the security of smart grid. In this paper, we propose an integrated smart grid learning environment for the purpose of smart grid security education and describe several course projects and learning materials using this learning environment. Section II presents the overview of this learning environment; Section III describes the details of the course projects using this learning environment; Section IV illustrates the learning materials available in the environment; Section V concludes the paper.

II. OVERVIEW OF LEARNING ENVIRONMENT

This learning environment mainly consists of two components: smart grid emulator and a learning website. This smart grid emulator is named Smart-Grid Common Open Research Emulator (SCORE). It provides a platform for emulating smart grid environment [10], and running real smart grid applications by applying virtualization techniques. This emulator SCORE needs to be installed in Linux environment, and operated by some related commands.

This process of installation and operation may be not easy for the students without computer science background, so we design a website for users to facilitate the access to this smart grid emulator. This website shown in Figure 1 provides an easy interface for user to practice in smart grid environment without considering complicated software environment. It is convenient for students to apply smart grid simulation environment to run specified power grid model and obtain related power and communication security knowledge under this model. After registration through the website shown in Figure 2, users can access the emulator that need be installed in Linux environment. It presents the registration information required.

 ISBN: 978-1-61208-365-0

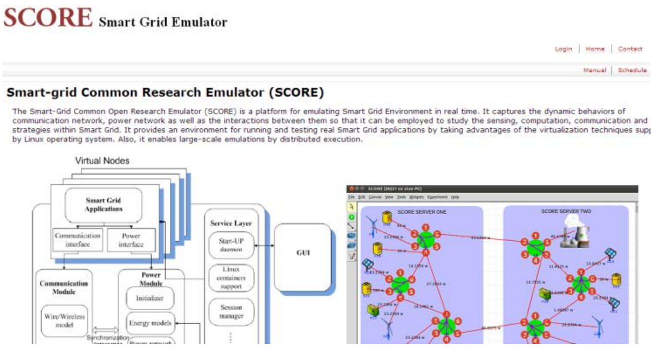


Figure 1. Website Display.

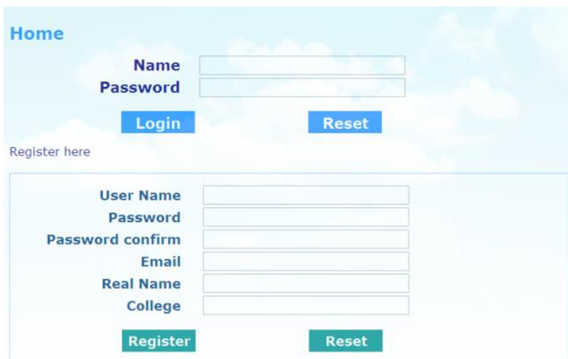


Figure 2. User Registration.

III. COURSE PROJECTS DESIGN

In this learning environment, we design several course projects to help students grasp related knowledge. In the projects, students are required to modify or write programs in the smart grid emulator to simulate the malicious attacks and obtain the resulting files showing the power network information. Moreover, in some projects, students are required to design counter attack plan to defend against such attacks.

A. *Grid Topology Attack Project*

After registering, user can access the schedule webpage shown in Figure 3. By clicking a time slot grid in this page, a new window will pop up to let user input some related information about reservation shown in Figure 4. After clicking "save" button, this task specified by the user will run in access the grid emulator during the time slot.

In this reservation window shown in Figure 4, a user can upload a configuration by clicking the "Choose File" button. If the user does not specify a file to upload, the system will use a default configuration file to run the smart grid emulator. Actually, this configuration file is *.imn type file. It is used to specify the grid topology information including node, power line and communication link information.

The alteration of this file could result in the change of the topology of the power grid, which is also the consequence of grid topology attack. In this project, we simulate the attack of damaging the current smart grid topology [11], by changing its topology configuration files. This project is shown in Figure 6. A new topology configuration of smart grid will result in a new smart grid topology.

During the running of smart grid, user can download the resulting log files, which display the dynamic power flow and network information. By clicking the reserved job in the schedule webpage shown in Figure 3, a new window will pop up to show the information of this running task shown in Figure 5. It displays the information about the task, and provides a link "ResultFile" to download the resulting log files.

Because a power system needs to balance demand and supply, some alterations of such configuration files may lead to the fluctuation of the whole power grid, which could be observed from its resulting log files.

Students are required to tamper with some topology configuration files and find out its impact on the stability of the whole power grid through comparing resulting log files before and after configuration files changing.

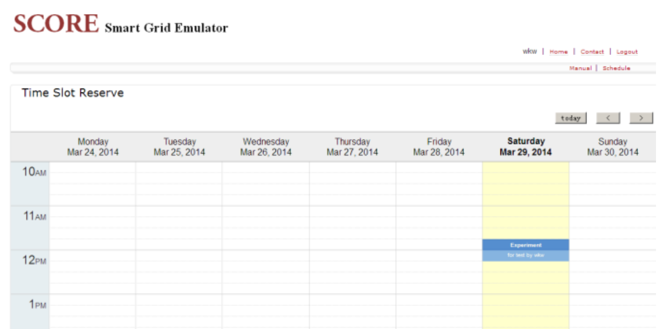


Figure 3. Schedule.

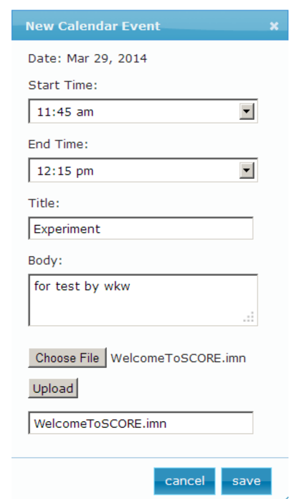


Figure 4. Time Slot Reserve.

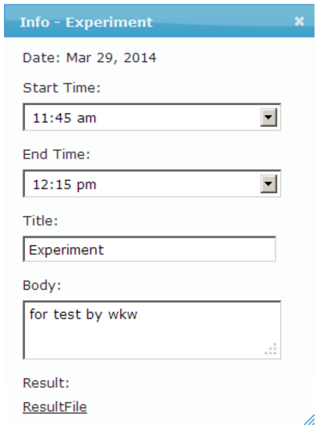


Figure 5. Result Information.

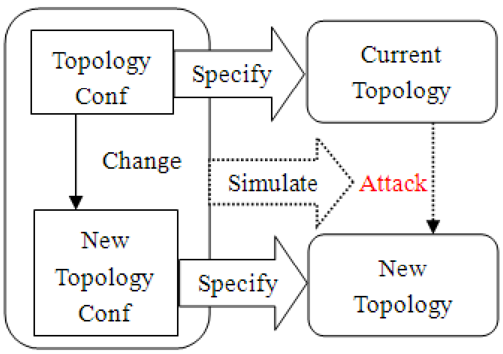


Figure 6. Topology Attack Project.

B. *Energy Model Attack Project*

Energy model specifies how the electrical appliances consume or supply the electrical power. Furthermore, user can customize energy model and run the system with your specified energy model by writing energy model programs and adding it to smart grid programs. It is possible to execute the energy model attack by overwriting the current energy model programs with the customized energy model programs. For example, modify the energy model to increase the power consumption of some electrical appliances may lead the whole power out of supply.

In this project, we implement the attack of altering the energy model of smart grid elements such as generator by modifying current energy model. This process is shown in Figure 8. Students are required to modify the sample program written in C++ to implement a new energy model. The main part of the sample program is shown in Figure 7. This sample program is running in the Smart grid emulator SCORE, and it specifies the energy model for appliances in the Smart Grid. Users can modify this sample code to implement their customozed energy model.

```
int main(intargc, char**argv) {
stringself_id = string(argv[1]); //use this to get the node id.
pid_tpid;
pid = getpid();
EnergyDaemoned(self_id); // init aenergydaemon using the node id.
        while (1){
        /* You can use the interfaces in EnergyDaemon.h
         * to implement your energy modeland interact with
     * the emulation environmenthere
    * The following is just a simple example.*/
                srand ( pid+ time(NULL) );
                intupdateInterval=rand() % 10 + 1;
                sleep(updateInterval);
                srand(updateInterval+pid+time(NULL));
                doubledesiredEnergy=rand()%50+1;
    //This sets the desired energy rate of the energy model.

        ed.setDesiredEnergy(desiredEnergy);sleep(5);

        ed.setDesiredEnergy(desiredEnergy);sleep(10);}
                return 0;
                }
```

Figure 7. Energy Model Sample Program.

Because the programs written by students may not execute correctly, instructors need correct the errors in the programs and submit it to the emulator. Similarly to the previous project, students can reserve a time slot and submit a task by specifying the topology configuration file containing customized energy model. And user can also download the resulting log files to observe the differences of the real-time power flow information between using previous and customized energy model.

Moreover, carefully designed alterations on selected energy models could keep the whole power system stable, which makes this attack not easy to be detected. In this project, students are required to design two suits of attack plans: one need change energy models of some elements to make the power grid system instable, and the other plan need change some energy models of a few elements and keep the system stable. Also, students are required to download the corresponding resulting log files to analyze the power flow and network information.

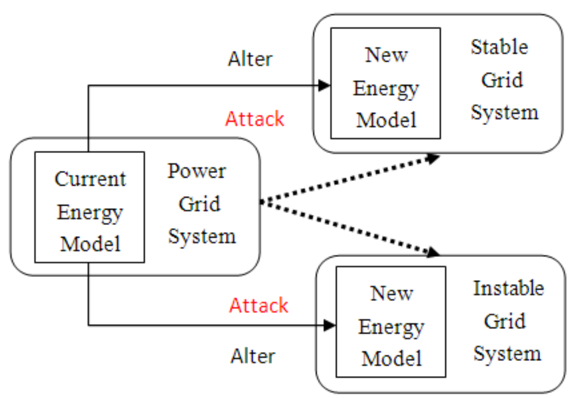


Figure 8. Energy Model Attack Project.

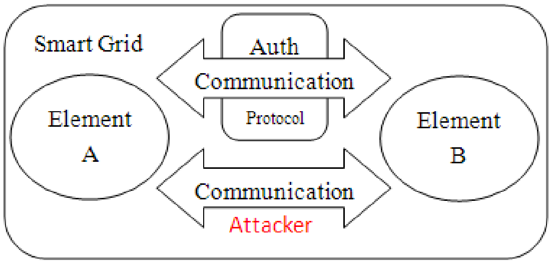


Figure 9. Authentication Protocol Project.

C. Authentication Protocol Project

Besides, we design an authentication protocol project to help students understand how authentication works in the smart grid environment. This project is shown in Figure 8.

Authentication is a critical component in network security, and it is widely taught in the course of network security. The authentication protocol in smart grid could be used to protect user data in the advanced smart meters to be safely collected by power corporations. And authentication is critical to prevent attackers to remotely control users' intelligent electrical appliances. Most important is the protection of the power grid control system, which needs authentication to access. It is necessary to apply authentication protocol to prevent malicious attack of the power grid control system.

In smart grid, authentication process can be skipped to reduce communication overhead, and this property could be used by attackers to bypass the authentication protocol. In Figure 8, attacker could get the communication between element A and element B in smart grid without authentication.

In this project, students are required to finish a search survey about the authentication in smart grid, and choose a senior to design a plan to execute such kind of attack. Moreover, students are taught the method to defend such attack from the experience of common network security and the features of smart grid. Students are required to propose a plan to defend against this kind of attack, and demonstrate why it could be feasible under the circumstance of smart grid.

IV. LEARNING MATERIALS

In addition, this website provides a platform to share learning materials like course presentation slides, related documents and source codes. We also design some flash videos in the web pages to introduce the overview of smart grid and its security; to explain complicated security policies, infrastructure stability and data privacy in smart grid; and to show how attacks and counter-attack work in smart grid environment. Students can access this website to obtain an in-depth grasp of smart grid security. Based on these learning materials, we have developed some course topics to cover the main aspects of smart grid security.

A. Overview of Smart Grid and Its Cyber Security

This is the introduction to the overall architecture of the smart grid including both the physical power system and the communication system. For power system, we will introduce the functions of the energy generation components, the distribution and transmission mechanisms, and the load control and demand response algorithms. For the communication system, we will cover various communication networks in smart grid, the Advanced Metering Infrastructure (AMI), and major smart grid industry standards.

The mutual impacts between the power system and the communication system will the emphasized in the materials. The cyber security of smart grid will provide the discussion of the problems such as the attacks in power system and communication system. Since many traditional security measures such as authentication, authorization, and accounting demonstrate unique properties in smart grid, we will re-introduce these concepts based on the new application environments.

Moreover, students can access the website to run the specified task and download the resulting log files. By observing these log files, students will have a clearer picture about the dynamical power flow information in smart grid. As a special emphasis, we will demonstrate how cyber attacks can lead to catastrophic results in physical power systems.

B. Network Security and Infrastructure Stability in Smart Gird

This section provides an in-depth coverage of the information network infrastructure in smart grid and its security. We will first describe the roles of wide area (WAN), local area (LAN), and home area networks (HAN) in smart grid. The advantages and disadvantages of different techniques to provide last-mile access connection to end users through power line communication, wireless networks, or cellular systems will be presented. Many network attacks in Internet have their companions in smart grid, and we will these kinds of attacks in details.

Since the power system needs to maintain a balance between the demands and supply in real-time, we will demonstrate how network attacks in the cyber system can impact the infrastructure stability of the whole power grids.

Moreover, the course projects of grid topology attack and energy model attack could assist the understanding of the attacks in smart grid. From these two projects, students could practice the simulated attack in smart grid and analyze these attacks' impact on the stability of power grid system.

C. Data Security and Privacy in Smart Grid

This section provides an in-depth coverage of the threats to confidentiality and privacy of the data in smart grid. We will first describe the data collection, aggregation, processing, transmission, and storage procedures in the AMI. Since different network protocols may be used at different stages of data processing, we will discuss the vulnerabilities during the data format transformation procedures.

 ISBN: 978-1-61208-365-0

In this section, we will introduce several concrete examples of data manipulation [12][13][14], such as data injection attacks [15][16]. Since data transmitted in smart grid without sanitization may lead to disclosure of sensitive information of end users, we will also introduce the countermeasures to preserve user privacy. Besides, the course project of authentication protocol will help students better understand the data privacy in smart grid and the importance of authentication in smart gird.

D. Examples. False data injection attack

We present a potential class of cyber attack, named false data injection attack, against the state estimation in deregulated electricity markets. With the knowledge of the system configuration, we show that such attacks will circumvent the bad data measurement detection equipped in present Supervisory Control and Data Acquisition (SCADA) systems, and lead to profitable financial misconduct such as virtual bidding the ex-post Locational Marginal Price (LMP).

An attacker could manipulate the nodal price of Ex-Post market while being undetected by the system operator. Combining with virtual bidding, such attack could bring financial profit to the attacker. A heuristic is developed to compute the optimal injection of the attacker, which can be formulated as a convex optimization problem and thus solved efficiently by the attacker.

We illustrate examples of financial virtual bidding misconducts, which are direct consequences of false data injection attack against the EMS state estimators. Figure 10 shows the topology of the IEEE 14-bus system. There are a total of five generators in this system. Table I describes two scenarios that are simulated. In both cases, a small subset of transmission line flow sensors are compromised by false data injection attack.

A malicious attacker aims at gaining profit from virtual bidding. At the pair of the nodes that are pre-specified in the third column of Table I, an attacker purchases and sells the same amount of virtual power in Day-ahead market at nodes j_1 and j_2, respectively. Based on historical trends, the attacker purchases at the lower price node and sells at the higher price node 3. In real-time market, the attacker then executes false data injection attacks on the selected sensors in order to remove a subset of congested lines. To illustrate the effect of the attacks on ex-post market clearing prices, we assume that the load forecast at day-ahead is perfect. In other words, if there were no cyber attacks, the day-ahead LMP will be the same as the ex-post LMP.

In Case I, only one transmission line (from bus 1 to bus 2) is congested. The attacker chooses to buy virtual power at bus4 and sells virtual power at bus 3 in day-ahead market. By compromising two line flow sensors with false data injection, the transmission line congestion gets relieved, leading to a system-wide uniform ex-post market price. Figure 11 shows the LMPs with and without the cyber attacks. Based on (12), the profit of such transaction is about \$1/MWh.

In Case II, there are three congested lines in the day-ahead market in Figure 12. By compromising three line flow sensors, the desired attack pair of nodes (buses 1 and 2) result in the same LMP in ex-post market. The reason is that the cyber attacks maliciously lower the estimated line flow information, thereby setting the shadow prices of the actual congested lines to be zero. The profit of such transaction is about \$8/MWh. In Table II, we compare the attack efforts and expected financial profits for both cases. We use the norm infinity of z_a with respect to the norm infinity of z as an indicator of the attack efforts. As the system congestion becomes more complex, the potential of gaining financial profits by maliciously placing false data attack is also higher.

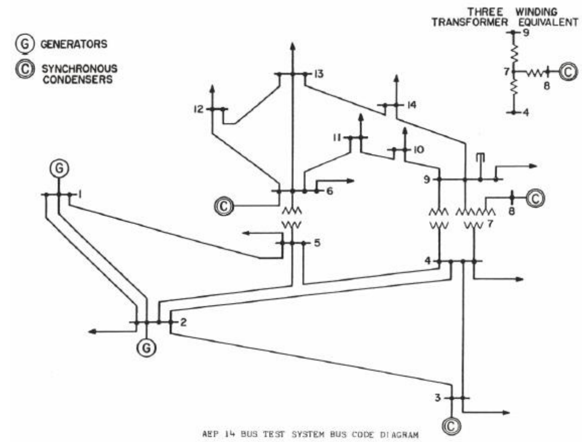


Figure 10. IEEE standard 14-bus system.

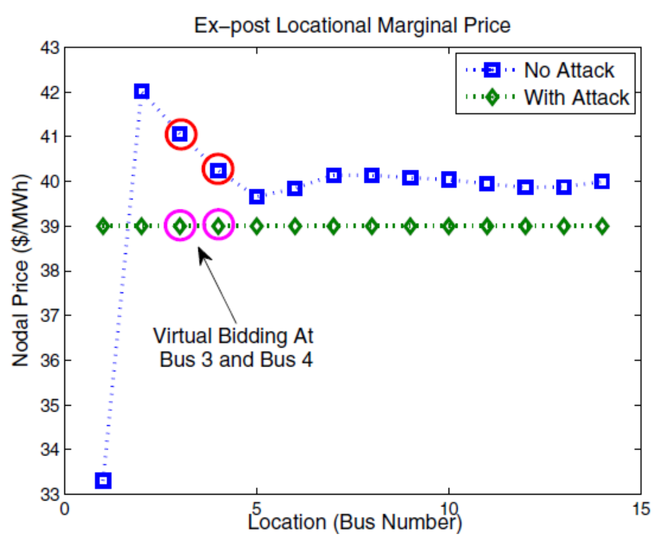


Figure 11. LMP with and without cyber attacks (only one line congestion).

TABLE I. CASE DESCRIPTION

	congested lines in day-ahead (from bus-to bus)	virtual bidding nodes	compromised sensors
Case I	1-2	3 and 4	line flow sensors 1-2, 3-4
Case II	1-2, 2-4, 2-5	1 and 2	line flow sensors 1-2, 2-3, 2-4

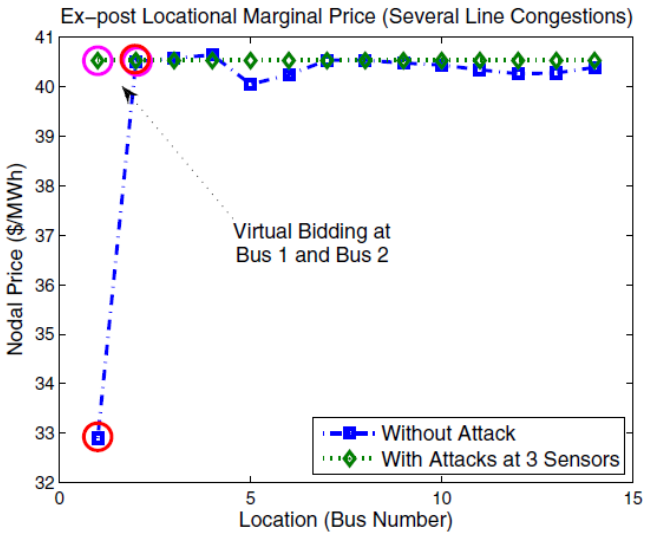


Figure 12. LMP with and without cyber attacks (three congested lines).

TABLE II. ATTACK EFFORTS AND PROFITS ($\varepsilon = 1MW_H$)

	relative efforts $\frac{\| z_a \|_\infty}{\| z \|_\infty}$	**profits (% of transaction cost)**
Case I	1.53%	2.50%
Case II	1.21%	9.76%

V. CONCLUSION AND FUTURE WORK

In this paper, we proposed a web-based smart grid learning module for students. It is shown to be beneficial for students to grasp the knowledge of security measures in smart grids and participate in the practice of smart grid security through instructive learning materials and delicately designed course projects in this learning environment.

Currently, we are working to provide friendly user interface and display course project results in graphics, especially the interaction parts in this website that provide the interface for students to access this learning environment. For example, the design of the reminding windows during the operations in the website will be improved for students to more easily apply the course project in this platform.

Moreover, an ongoing effort is to evaluate the student feedback and learning outcome from this proposed new module for smart grid security. This part will include designing the evaluation questions to measure the effect of the platform after practice of students, analyzing the feedback from students' answers to these questions to find out the defects and of this platform and improve the whole learning environment based these feedbacks.

REFERENCES

[1] Subcommittee on Smart Grid of the National Science and Technology Council. A policy framework for the 21st century grid: Enabling our secure energy future. Executive Office of the President, National Science and Technology Council, 2011.

[2] DHS Industrial Control System Cyber Emergency Response Team (ICS-CERT). Schneider electric quantum ethernet module multiple vulnerabilities.ICS-ALERT-11-346-01,2011.

[3] DHS. National infrastructure protection plan: Partening to enhance protection and resiliency. Department of Homeland Security, 2009.

[4] T. Godfrey, et al. "Modeling smart grid applications with co-simulation." Smart Grid Communications (SmartGrid -Comm), 2010 First IEEE International Conference on. IEEE, 2010, pp. 291-296.

[5] V. Liberatore and A. Al-Hammouri. Smart grid communicat- ion and co-simulation. In IEEE Energy Tech, 2011, pp. 1-5.

[6] H. Lin, S. Sambamoorthy, S. Shukla, J. Thorp, and L. Mili, "Power system and communication network co-simulation for smart grid applications." Innovative Smart Grid Technologies (ISGT), 2011 IEEE PES. IEEE, 2011, pp. 1-6.

[7] J. Nutaro, P. Kuruganti, M. Shankar, L. Miller, and S. Mullen, "Intergrated modeling of theelectric grid, communications, and control." International Journal of Energy Sector Management, 2(3), pp. 420-438, 2008.

[8] KEMA. The u.s. smart grid revolution: Kema's perspectives for job creation. Prepared for the GridWise Alliance, 2009.

[9] M. Lowe, H. Fan, and G. Gereffi, "US Smart Grid: Finding New Ways to Cut Carbon and Create Jobs." Centre on Globalization, Governance and Competitiveness, Duke University (2011).

[10] S. Tan, W. Song, Q. Dong, And L. Tong, "Score: Smart-grid common open research emulator." Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conference on. IEEE, 2012, pp. 282-287.

[11] D. Choi, L. Xie, "Impact analysis of locational marginal price subject to power system topology errors." SmartGridComm 2013, pp. 55-60.

[12] S. Cui, et al. "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions." Signal Processing Magazine, IEEE 29.5 (2012), pp. 106-115.

[13] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid." Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on. IEEE, 2011, pp. 244-248.

[14] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid." Cyber-Physical Systems (ICCPS), 2012 IEEE/ACM Third International Conference on. IEEE, 2012, pp. 183-192.

[15] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets." Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on. IEEE, 2010, pp. 226-231.

[16] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations." Smart Grid, IEEE Transactions on 2.4 (2011), pp. 659-666.

 ISBN: 978-1-61208-365-0

A SAML Metadata Broker for Dynamic Federations and Inter-Federations

Daniela Pöhn, Stefan Metzger, and Wolfgang Hommel
Leibniz Supercomputing Center
Munich Network Management Team
85748 Garching n. Munich, Germany
Email: [poehn,metzger,hommel]@lrz.de

***Abstract*—We present the design and concept for a new service to enable multi-tenant information and communications technology (ICT) service user authentication and authorization (AuthNZ) management in the research and education environment, called Géant-TrustBroker. Géant-TrustBroker complements eduGAIN, an umbrella inter-federation established on top of the national higher education federations in more than 20 countries world-wide by the pan-European research and education network GÉANT. Motivated by real-world limitations of eduGAIN, Géant-TrustBroker enables on-demand establishment of dynamic virtual federations, reducing the manual workload for the participating organisations by a high level of automation. Manual interaction is only necessary when organisational trust-building measures, such as signing a formal contract between providers, are necessary. Furthermore, the efforts of converting user information attributes to the format of a service provider is reduced by a conversion rule repository. We contrast Géant-TrustBroker with other state-of-the-art approaches and present its core workflow and the internal technical architecture.**

Keywords*–*Federated Identity Management; SAML; Shibboleth; Inter-Federation; Trust-Management.

I. Introduction

Any medium-sized and large organisation, e. g., universities or business companies, provide several ICT services to their employees, students, and also partners and guests. To access, e. g., email, web collaboration and printing services, a unique identifier, usually an username, is assigned to each user. All required information about users is provided by authoritative Lightweight Directory Access Protocol (LDAP) servers or relational database management systems for a centralized Identity & Access Management (I&AM) solution. This allows a simple provisioning procedure for new users and a deprovisioning process in the case of employees leaving a company.

Inter-organisational identity management is necessary when either an organisation's member shall access external services, for example, because a service, such as email, has been outsourced to a third party provider, or when members of several organisations shall work together on a common project, such as a research project, which involves multiple universities and external partners. Existing solutions for authentication and authorisation infrastructures (AAI) are either based on the accept-all-comers concept of OpenID without any formal trust or the rigid bilateral trust model of Security Assertion Markup Language (SAML). Different implementations, like Shibboleth and Identity Federation Framework of the Liberty Alliance, are based on SAML. While many national research and education networks (NRENs) operate large infrastructures for authentication and authorisation based on SAML, many federations in the industrial sectors consist of only very few members. NRENs' AAIs differentiate between organisations providing services for users, i. e., Service Providers (SPs), and home organisations, so called Identity Providers (IDPs). While geographic and industrial-sector-specific borders for federations are not imposed by Federated Identity Management (FIM) technology itself, they have become a reality due to the historic evolution and growth of FIM's use in both industry and higher education institutions. Most sectors and countries run their own federation. For instance, the DFN-AAI [1] interconnects universities and research institutes in Germany. Since research collaborations are not limited to national borders and researchers are professionally mobile, the problem of international and cross-sector collaboration is exacerbated. Neither a researcher from country A nor an employee of an industry partner from country B can access an ICT service operated by a university in country C based on existing national AAIs.

Different ad-hoc approaches exist to handle this problem. Either local user accounts are created for all project participants at each service, which obviously does not scale well for larger projects; or a new federation is set up specific for the given project or community. Either solution increases the overall complexity for IDP and SP operators and their manual working tasks. Also, this compromises user convenience and efficiency because of longer account set-up waiting times and the need to handle separate credentials for each service. Therefore, Inter-FIM is the next evolutionary step and, currently, a still young research discipline. Most conceptual, technical and organisational issues result from two main characteristics of today's federation solutions:

- An organisation's membership in a federation usually requires contracts, e. g., either with all other federation members in an ad-hoc federation or federations with a central operator, which can be either a large company in an hub-and-spoke federation or an independent entity as it can be seen in identity networks. The IDP must, for example, provide high quality user data to avoid SP misuse based on fake accounts, while the SPs must commit themselves to obey privacy and data protection principles.
- Federations must be built on common technical grounds, i. e., besides the same federation technology, e. g., SAML, the data format used by all IDPs and SPs must be harmonized, resulting in the so-called federation schema. This schema defines the syntax and semantics of information provided by the IDPs about their users. These attributes typically include name, email address and language preferences of the users.

One big, world-wide federation is an utopia, because common technology, common membership criteria and one single user data format could not be achieved with thousands of organisations [2]. Instead, existing federations are often integrated into a higher-level umbrella inter-federation. eduGAIN [3] is a successful attempt to span the NRENs' country-specific AAIs across the pan-European research network GÉANT and beyond, including already more than 20 federations. eduGAIN provides the communication endpoints information, which are used to identify and technically trust an entity, i. e., SP or IDP. These so called metadata entries include X.509v3 certificates and other relevant information in Extensible Markup Language (XML) files. Aggregating the metadata of several federations with a Metadata Distribution Service (MDS) [4] results in a huge, in eduGAIN currently around 30.000 lines of code, inter-federation XML metadata file, which significantly slows down processing the metadata at each IDP and SP in practice. Either the slowed down processing must be compensated through new hardware investments or it leads to significantly reduced usability of the end users. Entities establish static bilateral trust relationships, while the Interoperable SAML Profile [5] addresses the exchange of SAML messages. As described above, putting federations under the umbrella of an inter-federation leads to inter-federation data schemas that are the common denominator of all involved federations. In turn SPs, which require certain user attributes not included in the inter-federation data schema, cannot be used with their full functionality. Furthermore, the additional contracts required between federations and their members make the overall inter-federation more complex and cumbersome to manage. With the growth of the inter-federation, the minimalistic data schema, the significant technical effort for each participating organization, and the additional contractual complexity limit the advantages of the concept.

Our new approach, named Géant-TrustBroker (GNTB), is developed as a part of the EC-funded Géant GN3plus research project and shifts from a static, manual model to a more dynamic, fully automated fashion based on SAML, which is used in the research and education communities and is easier to extend. The new, on-demand establishment of trust by dynamic exchange of metadata is more scalable than current approaches. GNTB therefore creates dynamic, virtual federations that overcome many organisational and technical issues of other Inter-FIM approaches. The prototype will be developed based on Shibboleth, the most common implementation of SAML. In Section II, we present the current state of the art and contrast it with the Géant-TrustBroker service described in Section III. Section IV then details GNTB's internally used data model, API calls, and technical details on the conversion rule repository. The paper is concluded by an outlook to how eduGAIN and GNTB will collude and a summary of the results achieved so far.

II. Related Work

As huge metadata files affect performance of the inter-federation, Dynamic SAML [6] simplifies the discovery of other entities. For initial trust establishment, the metadata consumer validates the signature using a root certificate and establishes the trust, though trust continues to lie in pre-established contractual arrangements. Despite the dynamic character, the entities have to manually convert the user information, which are exchanged, or use a data schema that is the common denominator.

The Metadata Query Protocol by Young, currently submitted as Internet Engineering Task Force (IETF) Draft [7], suggests how to retrieve metadata from entities using simple Hypertext Transfer Protocol (HTTP) GET requests. Therefore it solves the problem of huge aggregated metadata files, but otherwise has the same drawbacks as Dynamic SAML: manual work for attribute conversion, attribute filter, and the initial trust establishment. The Metadata Query Protocol is one piece of the Metadata Exchange Protocol (MDX), where entities pick a registrar for their metadata and receive attributes from partner entities from one or more aggregators. In analogy to the DNS protocol, the aggregators and registrars are linked in order to exchange metadata with each other. Similar to MDX, the Public Endpoint Entities Registry (PEER) project [8] implemented a public endpoint entities registry supporting both SAML and non-SAML protocols. Though PEER moves from a huge metadata aggregator to a central system, where administrators can register their domain, many manual steps are needed, for example, to generate an attribute filter adjusted to the IDP. The generic framework of Dynamic Identity Management and Discovery System (DIMDS) [9] has the purpose to achieve minor user involvement in the identity management by creating a new DIMDS account. All user attributes are stored unencrypted in a central system, which can affect the privacy of users. Furthermore, DIMDS does not distinguish between IDPs and SPs, though not all IDPs are SPs as well and vice versa. The same problem appears in Federated Attribute Management und Trust Negotiation (FAMTN) [10], where it is assumed that each SP in the federation can act as an IDP. Internal users of the FAMTN system are supposed to perform negotiations by exploiting their single sign-on (SSO) ID without repeating identity verifications, though the SSO ID can be misused for attacks. It might appear that a provider needs less or more attributes, leading to violations of data minimalization or further negotiations between providers. IdMRep [11] shifts from pre-configured cooperations to dynamic trust establishment by a distributed reputation-based mechanism based on local Dynamic Trust Lists (DTLs) [12] and external reputation data. DTLs can, e. g., receive recommendations from other entities, but this mechanism does not work for an entity, which is new in a federation or inter-federation. Because of the amount of data processing required for all external and internal trust information especially in inter-federations, this results in yet another bottleneck in practice. Furthermore, the problem of different attributes, syntax, and semantics is not considered. In contrast, the proposed solution of the Credential Conversion Service for eduGAIN (eCCS) [13] focuses on the conversion of credentials. eCCS makes use of a special credential conversion service, which translates source credentials into target credentials, based on attributes from the SChema for Academia (SCHAC) [14] and eduPerson [15] schemas, which are described in the DAMe project. Though conversion rules within the inter-federation eduGAIN are concurrently written manually, the proposal concentrates on the two schemas SCHAC and eduPerson. The solution is not scalable for more schemas and other attributes, which are needed within certain research communities, like Distributed European Infrastructure for Supercomputing Applications (DEISA) and Partnership for Advanced Computing in Europe (PRACE), and several other inter-organizational projects.

III. GÉANT-TRUSTBROKER

Put simply, Géant-TrustBroker is an on-demand repository for SP and IDP metadata and conversion rules, which can be re-used by IDPs to fulfill attribute requirements for using a service. GNTB therefore simplifies the discovery of other entities and the establishment of technical trust, while it improves the scalability of metadata release. Furthermore, GNTB provides different means for the creation of dynamic virtual federations. GNTB is currently tailored for SAML, the widespread FIM standard used in R&E federations, but could be extended to support other FIM protocols as well. The GNTB core service enables the exchange of user information across federation borders with the following main characteristics:

- GNTB provides SP and IDP metadata on-demand. As opposed to distributing the complete aggregated metadata of all SPs and IDPs participating in an inter-federation, e. g., eduGAIN, GNTB supplies IDPs only with the metadata of SPs, which are used by at least one of their users and vice versa.
- GNTB automates the technical configuration steps to integrate new metadata when an IDP's user requests a service for the first time.
- Additionally, GNTB enables the re-use of data conversion rules. Instead of supporting only a small common subset of user attributes, the exchange of data conversion rules enables more complex and project-specific data schemas.

Especially the last two characteristics eliminate the previously manual workload for SP and IDP administrators and avoid long waiting times for the end users before they can use the service of a new SP. In general, two different workflow types have to be differentiated:

- The core workflow establishes the technical trust relationship between two entities, i. e., a SP and an IDP, triggered by the users themselves. The workflow is close to the regular SAML workflow in order to seemlessly integrate GNTB in current implementations and federations.
- Management workflows, which allow SPs and IDPs to register, update, and delete their metadata as well as conversion rules. To simplify the design of the core workflow, the metadata registration step is required before the GNTB core service can be used. However, metadata registration could also be integrated in the core workflow in the future.

To explain the GNTB core workflow in further detail, assume that user Alice from IDP I in federation $f1$ wants to make use of a web-based application service from SP S in federation $f2$ as depicted in Figure 1. The authentication form at S presents Alice, as often seen in a FIM scenario, a list of already trusted IDPs. As I and S have no bilateral relationship established yet, Alice cannot choose I from this list directly, but because S is registered at GNTB, Alice can trigger the GNTB core workflow. Using standard SAML mechanisms, Alice is redirected to the GNTB website automatically. From

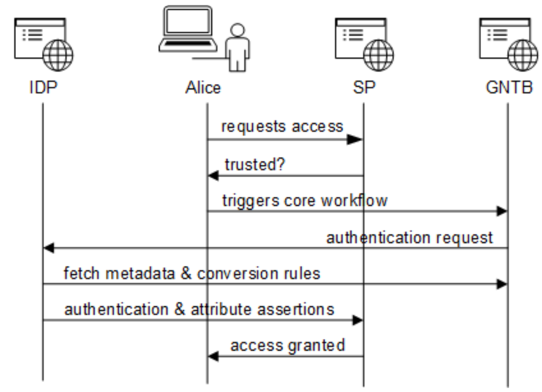


Figure 1. GNTB's core workflow.

the list of already registered IDPs, Alice has to pick the one she wants to use. GNTB passes the information about the chosen IDP back to S to determine whether an user from IDP I is considered acceptable. If Alice inadvertently, e. g., because she missed it on the list, has chosen an IDP, which S already trusts, a regular FIM authentication workflow is instanced without any further involvement of GNTB. S then sends the initial SAML user authentication request to GNTB, which temporarily stores it. This intermediate step is necessary to authenticate Alice in order to prevent malicious users to add arbitrary IDPs' metadata to any SP and vice versa. GNTB then redirects Alice automatically to her chosen IDP I for authentication. During this step GNTB acts like an SP towards I. Assuming that S is acceptable and Alice has been authenticated successfully, I fetches the metadata for S from GNTB. Based on this kind of information, I can automatically update its metadata configuration, reducing the former manual workload. Because the providers S and I do not belong to the same federation, they usually use different schemas, which requires appropriate attribute conversion. I has to check whether suitable rules are available at GNTB. Based on such rules, I's local attribute resolver configuration has been updated automatically and enables the creation of appropriate attribute filters, i. e., definitions, which user attributes it will sent to S on request; this primarily ensures privacy protection. In the next step, Alice is redirected to GNTB and afterwards back to I to respond to the temporarily stored authentication request of S. Since Alice has already been authenticated, I can immediately send a SAML authentication assertion and Alice's browser is redirected back to S. Because SAML assertions usually have to be signed by the sending entity, S requires and fetches Is metadata from GNTB, which includes the public key(s) in order to verify the signature. For further authentication requests S stores Is metadata to its local configuration. In the last step, S requests a SAML attribute assertion that provides detailed, but filtered user information. After the technical trust establishment, GNTB is not involved anymore and therefore does not interfere with existing entity configuration using other add-ons. However, GNTB supports retrieving updated metadata automatically.

IV. BROKERED TECHNICAL TRUST IN DYNAMIC FEDERATIONS

The Géant-TrustBroker service is the central part of our approach and important for establishing technical trust between

Copyright (c) IARIA, 2014. ISBN: 978-1-61208-365-0

two entities and reusing conversion rules. The data model includes a multi-federation namespace that is the basis for registering the list of user attributes required for using the service, while a data access layer facilitates the registration of entities, users, or uploading conversion rules.

A. *Géant-TrustBrokers internal data model*

As a central point of any Inter-FIM environment, metadata enables exchanging information about the communication endpoints and to ensure the authenticity of the sender. Therefore, this kind of information needs to be stored centrally at GNTB. A technical implementation imposes particular requirements on an interface for up- and downloading signed metadata files, the possibility to extract information from these files, and some kind of version control. We investigated other resource registry solutions for federations different approaches exist, e. g., the

- SwitchAAI Resource Registry tool, which makes use of a relational database management system;
- DFN-AAI, which stores the metadata files directly in the filesystem using PHP- and XSLT processing afterwards; and
- PEER project, which integrated a version control system.

Alternatively, a high-performance XML database, e. g., eXist would be an option. As GNTB should provide its service to different federations and communities, the metadata content varies, making the sole usage of a relational or XML database too complicated for reproducing metadata in a simple, efficient way. On the other hand, a version control system adds additional value to the service. Thus, we combine both approaches – a relational database and a versioning file system – because GNTB needs further information about an entity, e. g., to which organization a provider entity belongs to, in which repository container its metadata file is stored, or to record its current status. Additionally, to ensure that only authenticated and authorized administrators can manage their metadata or uploaded conversion rules, a simple GNTB user management is implemented. The database schema consists of the following information:

- Organizations: Each organization consists of one or more IDP or SP entities.
- Providers: Besides its unique name (entity_ID), entity type (i. e., IDP, SP) and its current status (e. g., valid, invalid, deactivated) information about the last attribute change and the location of the metadata file are stored.
- Users: Information about the authorized users, like username, hashed password, given name, surname, and email address of the contact person and their technical role.
- Conversion rules: Metadata about conversion rules, like description, its owner (e. g., the IDP, which uploads the rule), timestamp of the last change, status, and location of the rule file.
- Groups: Communities and federations, which can be the target or source group for conversion rules. Target means that the conversion rule can be re-used by one or several groups of IDPs or, respectively, one single IDP. Source is the opposite: the conversion rule was written for the needs of one specific SP or group of SPs, which all require identical attributes. One entity could be member of several groups, e. g., one federation, one inter-federation, and several projects.
- Relationships between a) IDPs and SPs, b) IDPs and conversion rules, c) rules and groups. The relationship between an IDP and an SP indicates a successful technical trust establishment using the GNTB core workflow described above and has to be stored at GNTBs database. This and analogous the information about the IDP and conversion rule relationship enable to notify administrators about metadata or rule changes. The last table contains information about a specific rule and by which target (single entity or group of entities) it is re-used. Thus we have to store only one copy of a conversion rule in the repository.

B. *Géant-TrustBroker's data access layer*

The database tables are filled up by different application programming interface (API) functions provided by GNTB data access layer (GNTB API). These functions can be split into three categories: account handling, provider entity handling, and conversion rule handling.

1) Account handling: As GNTB requires authentication of users as a precondition before any metadata or rule related configuration is possible, to prevent successful malicious intent of the user, some kind of user management is essential. For Géant-TrustBroker a basic access authentication (HTTP authentication) based on username and password, as often seen in FIM scenarios, is acceptable from a security perspective. But to avoid plain-text credentials in IDP- or SP-located scripts, a certificate based authentication method can also be used. User management provides the required functions to support the generally known lifecycle phases (e. g., creation, update, and deletion) of a GNTB account. API functions can be used to add, update, or delete the $username$, $password$ (i. e., its hash value) and the optionally stored $given\_Name$, $surname$ and $emailaddress$ entries of the entity administrator to the database.

2) Provider entity handling: At the first time contact between an entity and GNTB, metadata information is usually not yet registered, except if it has been automatically taken over from a federation or inter-federation, e. g., by a central Metadata Distribution Service, as it could be an option in the inter-federation eduGAIN. The registration procedure is possible either Uniform Resource Locator (URL) or file-based. In the first case, an entity is registered by providing a metadataURL to fetch a metadata XML file from there; otherwise, an entity provider uploads this file manually. The uploaded metadata is validated by specific XML Schema Definition (XSD) files, which validates the structure of the XML file. The ownership can be confirmed by HTTP validation, i. e., creating a resource in the root of the HTTP service for the domain with the name of a random parameter string given by GNTB, certificate validation of the uploaded metadata or by simply verifying educational domain names by email. As described in the core workflow above, a SP typically checks its trust relationship to the IDP chosen by the user. The API provides an appropriate *gntb_Ent_CheckTrustToIdp(Entity_ID[SP], Entity_ID[IDP])* function for this purpose. If an IDP is considered acceptable, the core workflow continues to establish the technical trust by invoking the API function *gntb_Ent_EstabTrust(Entity_ID[SP, Entity_ID[IDP])*. The administrators can set up further options, like notification of changed metadata and certificate expiration, update its metadata and delete technical trust relationships.

3) Conversion rule handling: Service providers may expect attributes, which may not be part of the IDP's schema, i. e., the IDP cannot provide these attributes out of the box. In order to send them, IDP administrators utilize so called user attribute data conversion rules, which will be used to extend the local attribute-resolver.xml definition. In the first step, raw attributes are pulled by a DataConnector from an IDP-internal data store, e. g., LDAP server or user management database, and then prepared for release in an attribute definition consisting of the definition of the attribute itself and the so called conversion rules. Typical attribute conversions encompass

- renaming: the attribute is used with the same format, but another name. A simple example of renaming a source attribute *gecos* to a new *displayName* attribute would look like this:

```
1 <resolver:AttributeDefinition id="displayName"
  xsi:type="Simple" xmlns="urn:mace:[...]"
  sourceAttributeID="gecos">

2 <resolver:AttributeEncoder [...]
  name="urn:mace:dir::displayName" />

3 <resolver:AttributeEncoder [...]
  name="urn:oid:2.16.840.1.113730.3.1.241"
  friendlyName="displayName" />

4 </resolver:AttributeDefinition>
```

- transforming: this is typically used for timestamps or dates, if the internally format is different from that of the SP;
- splitting: regular expression can be used to extract partial information from an attribute;
- merging: inter-connects two source attributes, e. g., givenName and surname, into a new one, e. g., commonName.

These conversion functions can be cascaded, i. e., one rule to prepare the attribute for internal use, then another one referencing the internal rule for the federational or communities schema, which can afterwards have a dependency to another schema. Administrators can re-use those conversion rules by utilizing the GNTB conversion rule repository. These XML files can be uploaded and should be searchable as well as reusable by other IDPs. The data access layer provides the function *gntb_Conv_FetchRule(Name)* to download an appropriate conversion rule. The definitions within the rule are added to the local configuration (metadata-resolver.xml) by scripts. Due to the fact that XML include tags would not work according to [16], as XInclude requires schema support in the original schema to mark where things can be included, and we want to reduce the manual work for administrators, local assembling of configuration files is reasonable. We define source groups, which is one SP or a group of SPs needing specific attributes. The target group is one IDP or a group of IDPs, that can use this conversion rule. As mentioned above, conversion rules can be applied to different sources and targets, if a rule is applicable for different groups, i. e., federations, communities or project partners as well. For example, one conversion rule named 01203_2.xml was written from an IDP I belonging to the federation $DFN - AAI$, which is an example for a target group. If the source of this rule was SP B in the federation $SWITCH - AAI$, an IDP C in the Austrian federation $ACOnet$, noticing that the rule 01203_2.xml can be used for their federation as well, can fetch the rule, updated its configuration and therefore this Austrian IDP C applies rule 01203_2.xml for the Austrian federation.

V. Conclusion and Future Work

Géant-TrustBroker enables the on-demand, user-triggered exchange of metadata and user attribute data conversion rules across identity federations' borders. Concurrently the scalability of the metadata exchange in federations and inter-federations is improved. GNTB supports the fully automated technical setup of FIM-based AuthNZ data exchange and therefore increases the automation of the former manual implementation efforts required by administrators of SPs and IDPs. Consequently, users can immediately start using a new service outside of their federation and have no waiting time until the administrators have finished the manual setup process.

The Géant-TrustBroker core workflow, which is based on the IDP Discovery Protocol and Profile [17], will be formally specified as an IETF Internet-Draft and submitted for standardisation as IETF Request for Comments (RFC). The GNTB prototype and implementation of the workflows for the FIM software package Shibboleth will be made availabe as open source and used for pilot operations in 2016.

Further research questions relate to the combination of technical and behavioural trust for the establishment of dynamic virtual federations as well as to quality assurance, i. e., measure for Level of Assurance (LoA) guarantees, of entities in the dynamic virtual federations, which will be focused in 2015 during GN4 phase 1.

Acknowledgment

The research leading to these results has received funding from the European Communitys Seventh Framework Programme under grant agreement no 605243 (Multi-gigabit European Research and Education Network and Associated Services - GÉANT).

The authors wish to thank the members of the Munich Network Management (MNM) Team for helpful comments on previous versions of this paper. The MNM-Team, directed by Prof. Dr. Dieter Kranzlmüller and Prof. Dr. Heinz-Gerd Hegering, is a group of researchers at Ludwig-Maximilians-Universitt München, Technische Universitt München, the University of the Federal Armed Forces, and the Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities.

References

[1] "DFN-AAI – Authentication and authorization infrastructure," 2014, URL: https://www.aai.dfn.de/en/ [accessed: 2014-03-04].

[2] "Interfederation and Metadata Exchange: Concepts and Methods," 2009, URL: http://iay.org.uk/blog/2009/05/concepts-v1.10.pdf [accessed: 2014-03-04].

[3] "Géant: eduGAIN Homepage," 2014, URL: http://www.geant.net/service/eduGAIN/Pages/home.aspx [accessed: 2014-03-04].

[4] "mds.edugain.org," 2014, URL: http://mds.edugain.org/ [accessed: 2014-03-04].

[5] "Interoperable SAML 2.0 Web Browser SSO Deployment Profile," 2009, URL: http://saml2int.org/profile/current [accessed: 2014-03-05].

[6] P. Harding, L. Johansson, and N. Klingenstein, Dynamic Security Assertion Markup Language. IEEE, 2008.

[7] "Metadata Query Protocol - draft-young-md-query-01," 2013, URL: http://datatracker.ietf.org/doc/draft-young-md-query/?include_text=1 [accessed: 2014-03-05].

[8] "PEER 0.11.0: Python Package Index," 2013, URL: https://pypi.python.org/pypi/peer/0.11.0 [accessed: 2014-03-05].

[9] K. Lampropoulos and S. Denazis, "DIMDS: A Dynamic Identity Management and Discovery System," in Proceedings of the INFOCOMP Workshop 2009, IEEE, Rio de Janeiro, Brasil. IEEE, 2009, pp. 1–2, ISBN: 978-1-4244-3968-3.

[10] A. Bhargav-Spantzel, A. C. Squicciarini, and E. Bertino, "Trust Negotiation in Identity Management," IEEE Security and Privacy, vol. 5, no. 2, Mar. 2007, pp. 55–63. [Online]. Available: http://dx.doi.org/10.1109/MSP.2007.46

[11] P. AriasCabarcos, F. Almenárez, F. GómezMármol, and A. Marín, "To Federate or Not To Federate: A Reputation-Based Mechanism to Dynamize Cooperation in Identity Management," Wireless Personal Communications, 2013, pp. 1–18. [Online]. Available: http://dx.doi.org/10.1007/s11277-013-1338-y

[12] F. Almenárez, P. Arias, A. Marín, and D. Díaz, "Towards Dynamic Trust Establishment for Identity Federation," in Proceedings of the 2009 Euro American Conference on Telematics and Information Systems: New Opportunities to Increase Digital Citizenship, ser. EATIS '09. ACM, 2009, pp. 25:1–25:4. [Online]. Available: http://doi.acm.org/10.1145/1551722.1551747

[13] G. López, O. Cánovas, D. Lopez, and A. Gómez-Skarmeta, "Extending the Common Services of eduGAIN with a Credential Conversion Service," in Computer Security – ESORICS 2007, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007, vol. 4734, pp. 501–514. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-74835-9_33

[14] "Download SCHAC Releases," 2011, URL: http://www.terena.org/activities/tf-emc2/schacreleases.html [accessed: 2014-03-05].

[15] "LDIFs - MACE-Dir: eduPerson/eduOrg LDIFs," 2012, URL: https://spaces.internet2.edu/display/macedir/LDIFs [accessed: 2014-03-05].

[16] "Shibboleth – Users – include files for xml config," 2011, URL: http://shibboleth.1660669.n2.nabble.com/include-files-for-xml-config-td6206245.html [accessed: 2014-03-13].

[17] "Identity Provider Discovery Service Protocol and Profile - Committee Specification 01," 2008, URL: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-idp-discovery.pdf [accessed: 2014-05-08].

 ISBN: 978-1-61208-365-0

Intrusions Detection System Based on Ubiquitous Network Nodes

Lynda Sellami
Department of Computer Science
Bejaia University, Algeria
slynda1@yahoo.fr

Djilali Idoughi
Laboratory of Applied Mathematics
Bejaia University, Algeria
djilali.idoughi@gmail.com

Abderrahmane Baadache
Laboratory of Modeling and Optimization Systems
Bejaia University, Algeria
abderrahmane.baadache@gmail.com

***Abstract*—Ubiquitous computing allows to make data and services within the reach of users anytime and anywhere. This makes ubiquitous networks vulnerable to attacks coming from either inside or outside the network. To ensure and enhance networks security, several solutions have been implemented. These solutions are inefficient and/or incomplete. Solving these challenges in security with new requirement of Ubicomp, could provide a potential future for such systems towards better mobility and higher confidence level of end-user services. We investigate the possibility to detect network intrusions, based on security nodes abilities. Specifically, we show how authentication can help build user profiles in each network node. Authentication is based on permissions and restrictions to access to information/services on ubiquitous network. As a result, our idea realizes a protection of nodes and assures security of network.**

Keywords-ubiquitous computing; intrusion detection system (IDS); security

I. INTRODUCTION

The goal of the current research in distributed computing is to abstract the physical location of users and remote resources [1][2]. Such an environment is exposed to serious security threats that can reach people and equipment, as well as data and programs in the virtual world. Therefore, the traditional mechanisms that focus only on digital security become inefficient. It is important to detect security breaches when they occur. This is made possible by intrusion detection mechanism.

Intrusion Detection Systems (IDS) allow to quickly implement new security policies to detect and react as quickly as possible against attacks occurring in a network [3].

IDS have already been used in classic and traditional environments for overcoming intrusion problems [3]. Our goal is to present some IDSs that have been developed for ubiquitous environments and examine their limits in different areas of Ubicomps.

In this article, we propose an IDS that aims to overcome the problems of intrusions in ubiquitous environments. We explore our approach for detecting intrusions (attacks) that occur in ubiquitous environments.

The rest of the paper is organized as follows: Section II presents a state of work already done on intrusion detection in ubiquitous environments. In Section III details our proposal. Finally, conclusion and perspectives are described in Section IV.

II. RELATED WORK

The use of networks and information systems as tools becomes necessary for the proper functioning and growth of enterprises. The multitude of network usage by known or unknown persons (users), turns the networks into potential targets for attacks. Users can exploit the vulnerabilities of networks and computer systems to access information or to undermine their good functioning.

The security of these networks, targeted by attackers, is an issue of paramount importance. For this, IDSs have been widely discussed for solving the problems of intrusions in networks. Several solutions that have been adopted in order to overcome the problems of attacks.

A. Ubiquitous Environments

An Intrusion Detection System can be considered as an application, in which individuals and organizations often express the need and objective of protecting their systems against intrusions.

To face the problem of security and the new requirements of the Ubicomp, we introduce and describe the main research work in this direction.

1) SUIDS (for Service-oriented and User-centric Intrusion Detection System): This is an IDS for ubiquitous environments; it is a system for intrusion detection of oriented services. SUIDS is suitable for users and deals with smart homes and offices [4][5]. It adopts a new mechanism-oriented service geared to verify and represent user and protect a variety of devices in the network against intrusions.

SUIDS treats the issue of heterogeneity of pervasive networks in three categories, which are principal nodes, service nodes and user nodes. SUIDS organizes the system hierarchically in three levels. The first level corresponds to the domain manager node. The second level contains the principal nodes. The third level is dedicated to service users nodes. To detect intrusions, SUIDS builds on the events of user behavior.

The detection algorithm uses a chi-square test to determine abnormalities. The chi-square test is applied for each specific parameter.

Figure 1 presents Hierarchical System for Smart-Home:

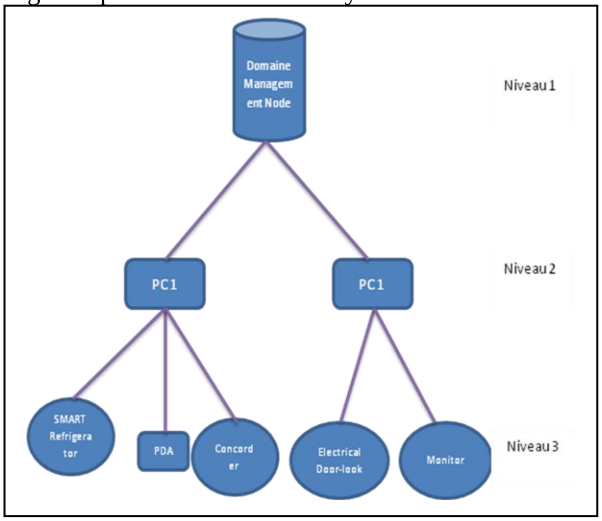


Figure 1. Hierarchical System for Smart-Home [4].

2) IDS for IP-Based ubiquitous sensor netwoks: RIDES (for Robust Intrusion Detection System for IP-Based Ubiquitous Sensor Networks) [6] is a hybrid system of intrusion detection. It combines the signatures of attacks and the discovery of anomalies (behaviors) for detecting intrusions. It uses a distributed algorithm of pattern matching for the intrusion detection based on signatures. To ensure the detection of intrusion based anomalies, RIDES employs a technique of classification based on the notation of SPC (Statistical Process Control) technique called CUSUM chart.

3) An application-oriented solution: That enforcement-led approach to security is presented by Robinson [7], as a background of research related to security in ubiquitous computing. It offers a good balance between theory, technology and scenarios. It is a method of generalized research-oriented application and it is applied on a thesis about intrusion detection. This approach is composed of four (4) steps. Step 1 is responsible for identifying the scope and objectives to be achieved. Step 2 provides the design strategy for achieving the objectives of the application. Step 3 provides hardware and software which can be extended or establishes mechanisms to achieve the objectives. Step 4 evaluates theory and technology proposals based on objectives and identified constraints.

4) Intrusion detection for wireless sensor networks based cluster: The objective of this approach is to detect and prevent intrusions in sensor networks [8]. Singh et al. [2] have implemented the MAC (Media Access Control), address of intruders attacking networks.

The sensor network is composed of a static Base Station (BS) and clusters. The BS is located away from sensors, and the clusters are composed of a number of dynamic sensor nodes.

Each cluster leader collects data, compresses and transmits them to the Base Station [2]. The Base Station keeps track of the healthy state of all nodes in each cluster by checking information sent by each cluster head to MAC address [2].

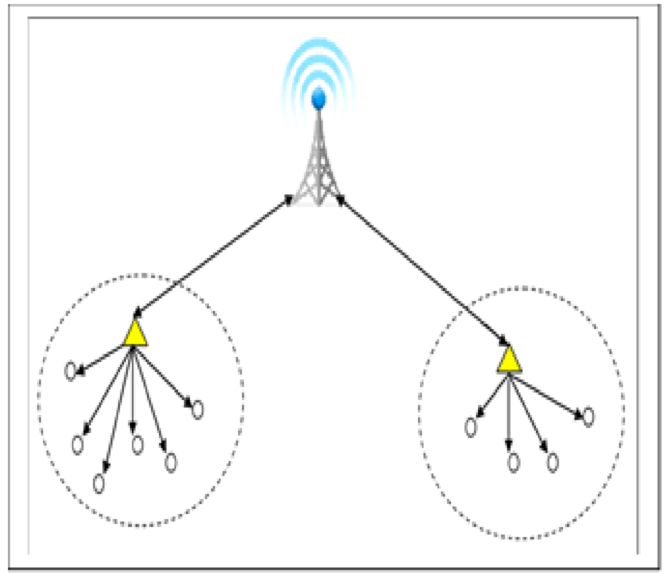


Figure 2. Data communication between base station and heads of clusters [2].

5) Distributed PCA (Principal Components Analysis) approach for intrusion detection in sensor networks: Loo et al. [9] present a new approach for distributed intrusion detection called PCADID, for attacks detection in wireless sensor networks.

The sensor array is partitioned into groups of sensor nodes. In each group, a selected control node cooperates with other control nodes in order to build a normal comprehensive profile of the network [9].

The authors have used two (2) approaches [9]:

- An approach based on the PCA centralized approach, called PCACID. Here each control node establishes a normal profile of its own network traffic using PCA (Principal Components Analysis).
- An approach based on the PCA distributed approach, called PCADID. Here each control node using the APC establishes its own normal sub-profile for its traffic network, and sends it to other control nodes. Each control node constructs the normal profile of the network

6) Policy of intrusion detection for ubiquitous sensors networks: Xu et al. [10] propose an intrusion detection policy for ubiquitous sensors networks. Their approach consists of three (3) units:

- Unit of data collection: Each sensor node listens to communications among neighboring nodes. The streamed packets are transmitted to the processing unit.
- Unit of data processing: The header of packets received by the playback unit is interpreted and analyzed; the values are then updated in the list of verification data.
- Handling policy: Compare the current activity of the sensors node with the threshold values. If the behavior violates these values, the node is identified as compromised.

B. Limits and New Motivations

The majority of IDSs developed for ubiquitous environments are designed for specific areas of application or for application scenarios, which limit their generalizations for all areas of Ubicomp. We deal with the following problems already presented in field of mobile ad hoc networks [11] and wireless network [12]: (1) centralization of detection, (2) transition to SMS communications, (3) excessive consumption of energy, (4) capacity limitation of sensors (hardware), and (5) reconfiguration problem when changing the architecture and the components. The IDSs developed for Ubicomp are insufficient or incomplete, and they need improvements and/or adaptation.

TABLE I. IDSs LIMITS OF UBICOMPS

IDS	Inconveniences
SUIDS	-The principal nodes are far from the service nodes. They need more energy -The network connections are consumed in communication with service nodes -Intrusions that occur during transmission may go unnoticed. -Existence of the concept of centralized detection can not be applied to larger areas (administrative building). -This solution is not applicable to other areas of applications of ubiquitous where we need a mass of information to convey and treat -Risk of false positives that generates too alarms and treatments.
Application-led	-This document provides a general methodology to search applications oriented in Ubicomp. -It is applied on application scenarios -The solution may not work on all instances of an application or other applications with different requirements. -The notion of reconfiguration and adaptation must be added.
Cluster-based	- It is based on a central controller
ACP-based	-It is necessary that each control node up-to-date has normal profile for PCACID, -It is necessary that each control node up-to-date sounds under normal profile and cooperate with other control nodes to update the overall normal profile of the network. -The normal behavior of the network (sensors) changes over time
Policy detection	-Overload sensor nodes through the collection, analysis, transmission and detection.

III. PROPOSITION

In this research, we propose an IDS for identifying intrusion from legitimate users in ubiquitous systems.

A. Description of the Proposal

The ubiquitous network consists of several nodes (devices, hosts, sensors, etc.). It is difficult or impossible to have a global view of ubiquitous network since they are on very large scale. For supporting the scalability of ubiquitous networks, we focus on network nodes. Each node has knowledge of closest neighbors surrounding it. Considering a node and its neighbors allow to extend our approach to a large number of nodes.

Therefore, each treatment applied to a node will be applied to its neighbors.

It is assumed that each node of the ubiquitous network is provided with the collection unit, and the detection and analysis unit. In the case of adhesion of a new node to the network, its neighbors send him the two units after an existence test.

Each node of the network has permissions and privileges, allowing to perform a number of processing and communication with other nodes on the network. Nodes use an adapted routing protocol so that they can route messages among them.

B. Overview of the Proposition

Figure 3 illustrates the functioning of our proposal; it consists of four parts, namely, data source, behavior, control, and action.

Data flow is defined by the node (sensor, network packets, users query, etc.). The behavior of the node is constructed from the data stream. To detect anomalies in the behavior of nodes (users), a unit of control and analysis is used to compare the actual behavior with the normal profile. When an abnormality is detected, an alarm is sent to the node to help solve this problem. An abnormality corresponds behavior which derived from normal (deviation), or unintended (unexpected).

1) *Detection approach:* There are two ways of detecting intrusions, (1) through known attack patterns to match with, misuse detection, and (2) through expected normal behaviors and identifying deviations as intrusion, anomaly detection. In our case, we have used the anomaly detection technique for identifying intrusions. This, obviously, requires defining the expected normal behaviors of the user that use the service of network. Each node creates its normal profile.

2) *Normal profile:* Each user accesses a ubiquitous network with authentication, which limits access to information/services offered by the network. Authentication uses the notions of permissions and restrictions of the network. This permissions and restrictions allow to build normal profiles of users.

Each node collects information to determine the vector of restrictions, and permissions for network access. These feature vectors (restrictions and permissions) are the normal traffic profile of nodes. Let $V_{i,k}(0)$ be the feature vector of node i of size n, that represents the number of features (privileges and restrictions). The number of features is the same for all nodes.

Such that: $V_{i,k}(0) = (v_{i,1}, v_{i,2}, v_{i,3}, ..., v_{i,n})^{T,}$ and n is the number of characteristics of the node i.

C. Intrusion Detection Approach

Figure 3 shows the functioning of our approach:

1) The node presents the data source.

2) Normal node profile is built based on the permissions and restrictions of the node. This construction of the profile is achieved by a unit of construction of normal profile.

3) A collection unit is responsible for capturing information (data), which allows to build the current behavior a node.

4) A unit of analysis and control is responsible for comparing the current behavior with the normal profile of a node. In case of deviation the behavior of a node from its normal profile, an action is sent to the node.

5) The action is the behavior of the IDS to a possible intrusion; an alarm is transmitted to inform the node and its neighbors of the intrusion and that correction of the problem is required.

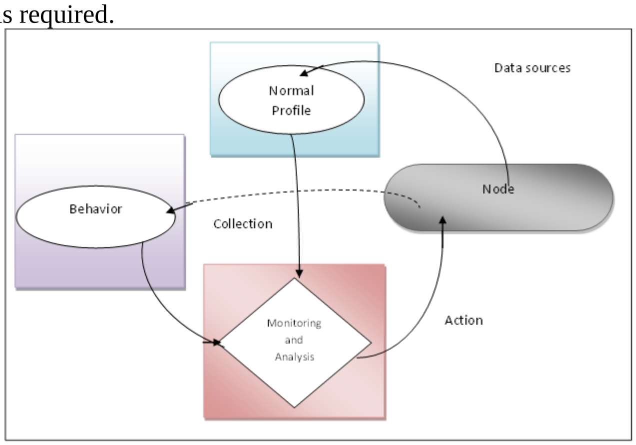


Figure 3. Step to the detection.

1) Normal profile.

Normal profile is constructed taking into account the activities of the user, as the preferred tool, work habits, typing speed, etc. In our approach the construction of normal profile is focused on: frequency; program CPU, I/O, other resources, and denied executions. We create profile based-on legitimate user data and represent a user's typical behavior.

User can have permissions and restrictions, which are representing by a vector of features. For example, a record (01100000100000000001100001001110100000) is a vector of features (permissions and restrictions), where *1* is the permission, and *0* is the restriction.

2) Anomaly

All user-based anomaly detection schemes for intrusion detection are intrusive behaviors is, by its very nature, anomalous [13]. User is acting in an abnormal manner then the actions of that user can be classified as intrusive. Behaviors can be determined to be abnormal through a comparison against a user profile that represents a user's typical behavior.

Users establish a profile based-on the number and types of commands they employ. Thus, if a system can discern this profile, and commands are employed "outside" of this profile, then the system should flag this action as a potential intrusion. Commands are presented by authentication of user, which appear in the same sequence.

User profile can take on many forms, is based upon either an individual's behavior and/or the typical behavior of the individuals in a functional group. Any time that the system is not operating in a normal manner there is an increased likelihood that an intruder is (or was) present on the system. For example, a record:

(00100000010000110000110000100111010001 0) is abnormal vector of features.

D. Intrusion Detection

The detection phase identifies abnormal vectors. At each time interval (t), each node collects a feature vector $V_{i,\,k}(t)$. This feature vector represents the behavior of a node in this time interval.

Detection of abnormal vector is based on the vector of normal profile $V_{i,\,k}(0)$ previously established.

To determine abnormalities, we calculate the distance between $V_{i,k}(0)$ and $V_{i,k}(t)$ using:

$$\sum_{\kappa=1}^{n} \left| Vi,\kappa(0), \mathrm{V}i,\kappa(t) \right| \tag{1}$$

Such that n is the number of characteristics of the node *i*.

At each node, we calculate the distance of projection of each feature vector $V_{i,k}(t)$. We class $V_{i,k}(t)$ abnormal, if the projection distance calculated exceeds a predefined threshold:

$$\begin{cases} d\big(Vi,\kappa(0),Vi,\kappa(t)\big) = 0 \textit{ : Normal} \\ d\big(Vi,\kappa(0),Vi,\kappa(t)\big) \geq 0 \textit{ : Anomaly} \end{cases} \tag{2}$$

E. Application Example

In a Smart Office, we have a set of nodes that have access to services and information.

The Smart Office has a central manager, whose management tasks are to access services and information in the network.

The number of nodes connected to the Smart Office is very large, which limits the work of central manager and encumbers management nodes.

Our idea is based on nodes and their behaviors. Each node accesses the services and information of Smart Office with network authentication. This authentication allows the authorizations and restrictions of services and information to nodes.

Generally, an intruder accesses the network via a node with the objective to access network services. Network protection depends on the protection of each node.

As a possible scenario to demonstrate the system design, we assume that Marc works in a Smart Office. He uses his PC to work and access network services and information requiring an authentication and access control mechanism. This authentication gives Marc the right to print, consult the database and send emails. Marc cannot update database, share data, or use the scanner. All tasks accomplished by Marc are tracked. Then his privileges are: print, consult the database and send emails, while his restrictions are: update

 ISBN: 978-1-61208-365-0

database, share data and use scanner. The normal behavior of Marc is expressed by all these restrictions and privileges. This allows to build the vector features $V_{i,k}(0)$ with an initial time 0.

$V_{i,k}(0)$ = {print, consult, email, update, share, scan}

Such that I = name of the node (Marc), and k = number of privileges and restrictions (= 6).

1) Intrusion Detection

When connecting to the smart office, the profiling unit built the feature vector corresponding to the normal profile of Marc based on his privileges and restrictions.

In a time interval (t), the collection unit collects information about the current behavior of Marc, this allows to build the feature vector $V_{i,k}(t)$ corresponding to his current behavior. This vector shows the values of privileges and restrictions that Marc had accessed during this time interval.

The unit of analysis and detection calculates the distance between $V_{i,k}(t)$ and $V_{i,k}(0)$ to class the abnormal vectors (behavior):

If $d(Vi,\kappa(0),Vi,\kappa(t))=0$: Normal behavior (3)

Else : Anomaly

Our idea allows checking all what comes from nodes, for monitoring the behavior of the user (node). The analysis and detection is performed in each node independently of the other nodes.

2) Positioning of the solution

IDSs shown in the related work are developed for sensor networks, which limits their generalization to ubiquitous networks. We also have the problem of overload sensors, and update database the profiles and signatures.

Our solution is based on the authentication by the permissions and restrictions of access to information and services on ubiquitous network. As such, there is no need to update database of the normal profile.

TABLE II. COMPARISON OF IDSS

IDSs	**Features**	
	Construction of normal profile	***Data source***
SUIDS	Learning phase	Event Registration
Application-led	Learning phase	Data packets
Cluster-based	Learning phase	Network packets
ACP-based	Learning phase	Network packet
Our approach	Based on permissions and restrictions to access network.	Permissions and restrictions

As the table shows, all works presented in the related work section are supported on the normal profile; require a learning phase for the construction of the normal profile. This phase limits the scalability of the solutions (support of new nodes). In our approach the construction of the normal profile does not require the learning phase, it based on permissions and restrictions to access network.

For the data source, our approach uses the permissions and restrictions of the node, and other approaches are based on networks or data packet.

In our solution, the detection is done on each node individually of its neighbors, limiting the cooperation in the detection. This is what we focus on. The design of schemes for achieving complete or partial cooperation is a topic of future research.

IV. CONCLUSION AND FUTURE WORK

The principal objective of this work was to ensure the safety of ubiquitous networks. We developed an approach to detect intrusions; our approach allows to monitor the safety of nodes and the network. It consists in searching anomalies that could lead to possible attacks, and to take action against such attacks.

We then described our approach; we introduced a new way of constructing the normal profile of users based on authentication. This approach allows a more flexible analysis and detection, which avoids the update of the database of the normal profile. We interest to the behavior of the node to the network.

Our idea realizes a protection of nodes and assures security of network. This protection is proved by authentication abilities to build user profile.

The problem is still open, while the nodes act individually with their neighbors, limiting the cooperation in detection. In some case which attacks are complexes, the node will not be able to identify intrusion and intruder.

This article is a work in progress, presenting ideas to be developed in our future work.

As future work, we will complete the intrusion detection architecture, investigate the methods to analyze audit data for intrusion detection, formulate and evaluate our intrusion detection approach.

REFERENCES

[1] OECD, “Guidelines on the protection of privacy and transborder flows of personal data,” http://www.oecd.org/, 2013, [accessed June 2014].

[2] S. K. Singh, M. P. Singh, and D. K. Singh, “Intrusion Detection Based Security Solution for Cluster-Based Wireless Sensor Networks,” International Journal of Advanced Science and Technology, vol. 30, May. 2011, pp. 83-95.

[3] K. Sellami, R. Chelouah, L. Sellami, and M. Ahmed-Nacer, “Intrusion Detection Based on Swarm Intelligence using mobile agent,” International Conference on Swarm Intelligence: Theoretical advances and real world applications (ICSI 2011), Cergy, France, June. 2011, pp. 1-3.

[4] B. Zhou, Q. Shi, and M. Merabti, “A novel service-oriented and user-centricintrusion detection system for ubiquitous networks, ” Proceedings of IASTED International Conference on Communication, Network and Information Security (CNIS’05), Nov. 2005, Phoenix, Arizona, USA, pp. 76-81.

[5] B. Zhou, Q. Shi, and M. Merabti, “ A Framework for Intrusion Detection in Heterogeneous Environments,” Proc. IEEE Consumer Communications and Networking Conference (CCNC 06), vol. 2, Jan. 2006, Las Vegas, Nevada, USA, pp. 1244-1248.

[6] S. O. Amin and al, “RIDES: Robust Intrusion Detection System for IP-Based Ubiquitous Sensor Networks,” Journal of Sensors, vol. 9, no. 6, May. 2009, pp. 3447-3468, doi:10.3390/s90503447.

[7] P. Robinson, “An Application-led Approach for Security Research in Ubicomp,” The Third International Conference on Pervasive Computing, Munich, Germany, May. 2005.

[8] P.F. Tiako and L. Gruenwald, "Collaboration framework for data compensation in sensor networks," In Proceedings of the 2008 IEEE International Conference on Electro/Information Technology, May. 2008, pp 504-509.

[9] C. Loo, M. Y. Ng, M. Palaniswami, and C. Leckie, “APC-based Distributed Approche for Intrusion Detection in WSNs,” International Journal of Distributed Sensor Networks, vol. 2, no.4, Dec. 2006, pp. 313-332.

[10] J. Xu, J. Wang, S. Xie, W. Chen, and J. U. Kim, “Study on intrusion detection policy for wireless sensor networks”, International Journal of Security and Its Applications, vol. 7, no. 1, January. 2013, pp. 1-6.

[11] I. Parker, J. L. Undercoffer, J. Pinkston, and A. Joshi, “On Intrusion Detection in Mobile Ad Hoc Networks,” 23rd IEEE International Performance Computing and Communications Conferenc , Workshop on Information Assurance, April. 2004, pp. 1-6.

[12] F. Adelstein, P. Alla, R. Joyce, and G. G. Richard, “Physically Locating Wireless Intruders,” Proc. IEEE 2004 IAS Conference, Las Vegas, Nevada, vol. 1, April. 2004, pp. 482—89.

[13] J. Marin, D. Ragsdale, and J. Sirdu, “A hybrid approach to the profile creation and intrusion detection,” In DARPA Information Survivability Conference &amp, Exposition II (DISCEX'01), Vol. 1, IEEE 2001, pp. 69-76.

Fast Person Identification Using JPEG2000 Compressed ECG Data

Yi-Ting Wu*, Hung-Tsai Wu†, and Wen-Whei Chang‡
Institute of Communications Engineering
National Chiao-Tung University
Hsinchu, Taiwan
e-mail: *jay79227@gmail.com, †htwu.nctu@gmail.com, ‡wwchang@cc.nctu.edu.tw

***Abstract*—The use of electrocardiogram (ECG) signals in biometric systems has been an active research topic for over a decade. In wireless telecardiology applications, compressed ECG packets are often required for efficient transmission and storage purposes. Nonetheless, compressed ECG data must be decompressed first before applying existing biometric techniques that work on the original signal. To achieve a faster patient care, we propose a new biometric technique which performs person identification in compressed-domain using one-lead ECG signals. First, we apply a preprocessor which converts one-dimensional (1-D) ECG signals to 2-D image matrices and compresses them by the JPEG2000 image coding standard. Features relating to ECG morphology were extracted directly from the JPEG2000 code-stream and then applied for indexing person identity by texture content in a known enrollment database. Experiments on standard ECG databases demonstrate the validity of the proposed compressed-domain ECG biometric system with an accuracy of 95.72%.**

Keywords–ECG Biometric; Person Identification; JPEG2000 Image Coding Standard.

I. INTRODUCTION

Electrocardiogram (ECG) signal is a recording of the electrical activity of the heart and is a clinical diagnosis tool for cardiac diseases. Typical features are linked to the peaks and time durations of the P-QRS-T waves representing the heart activity in terms of depolarization and repolarization of the atria and ventricles [1]. In wireless telecardiology applications, ECG data forwarded by the user to the hospital needs to be verified and authenticated to guard against spoof attack. Recently, some proposals have suggested the possibility of using ECG as a new biometrics modality for person identification [2]-[9]. Comparing with other biometric traits such as fingerprints and voice, the ECG of a human is more universal and secure. The validity of using ECG biometric is supported by the fact that ECG can only be obtained through a sensor placed around the user and forgery is difficult as the unique shape of the ECG signal is affected by the physiological and geometrical differences of the heart in different individuals.

Basically, ECG biometrics can be achieved by comparing the enrollment ECG template and recognition ECG template. Based on the features that are extracted from ECG signals, we can classify ECG biometric methods as fiducial-based [2]-[5], non fiducial-based [6]-[8], or a hybrid [9]. Among them, Discrete Wavelet Transform (DWT) techniques have shown effective for extracting discriminative features in ECG biometric recognition [6][7]. Irrespective of underlying methods used for the generation of the templates, most of the existing ECG biometrics work on uncompressed raw ECG signals [2]-[9]. However, in remote telecardiology scenarios, ECG data are often kept in compressed format for efficient transmission and storage purposes. Many ECG data compression methods have been proposed, including direct time-domain methods and transformation methods [10][11]. Most of the ECG data compression methods adopt one-dimensional (1-D) representations for ECG signals and focus on the utilization of the intra-beat correlation between adjacent samples. Since the ECG signals have both intra- and inter-beat correlation, better algorithms have been proposed to get the most of benefit from both types of correlation [12][13]. These methods generally start with a preprocess which converts 1-D ECG signals to 2-D data arrays through the combined use of QRS detection and period normalization. The constructed 2-D ECG data arrays are then ready to be further compressed by the vector quantization [12] or the JPEG2000 image coding standard [13]. In such scenarios, then the compressed ECG data must be fully decompressed before applying existing biometric techniques. Apart from posing threat to the emergency patient, delay in authentication can be an unnecessary burden on the hospital system, as the hospital may have thousands of enrolled patients and decompression of all their ECG packets is an enormous work. This drawback can be avoided by directly reading the compressed ECG data to obtain unique features that can identify an individual. The key advantage of the proposed compressed-domain ECG biometric system is smaller template size and faster biometric matching compared with existing biometric systems. In addition, most of the literatures have concentrated their research on obtaining healthy subjects in their experiments. By contrast, we will look into the effects of diseased subjects on the recognition rate of an ECG biometric system.

The rest of this paper is organized as follows. Section II describes the ECG fundamentals and presents a preprocessor which converts 1-D ECG signals to 2-D image matrices. Section III gives an overview of the JPEG2000 encoding algorithm. Details of the algorithms for the proposed ECG biometric system are provided in Section IV. Section V presents the simulation results for the healthy and diseased subjects using standard ECG databases. Finally, Section VI gives our conclusions.

II. 2-D ECG COMPRESSION

To begin, we apply a preprocessor, which can be viewed as a cascade of two stages. In the first stage, the QRS complex in each heartbeat is firstly detected for segmenting and aligning 1-D ECG signals to 2-D image matrices and in the second stage, the constructed matrices are compressed by JPEG2000 [14]. Figure 1 shows the block diagram of the 2-D ECG compression scheme proposed by Bilgin [13].

A. ECG Data Sources

The ECG data for the experiments are obtained from the QT Database [15] that contains ECG recordings collected from healthy subjects and patients with various heart diseases. First, 10 healthy subjects from the MIT-BIH Normal Sinus Rhythm

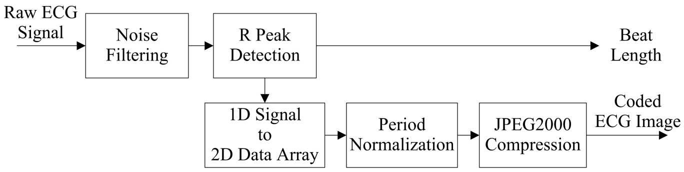


Figure 1. Block diagram of the ECG JPEG2000 compression scheme [13].

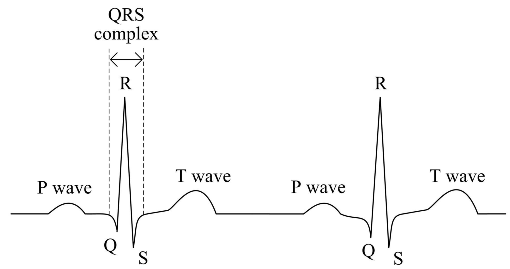


Figure 2. Typical ECG wave pattern in time-domain.

Figure 3. ECG image matrix for record sel17453m of the QT Database.

Database are used in the experiments and denoted as dataset D1. Subjects that are added to the system to determine the effects of the diseased ECG consist of 10 records from the MIT-BIH Arrhythmia Database, 10 records from the MIT-BIH Supraventricular Arrhythmia Database, and 10 records from the Sudden Cardiac Death Holter Database. For convenience, these three groups of diseased subjects are denoted as dataset D2, D3, and D4, respectively. Each of these records is 15 minutes in duration and are sampled at 250 Hz with a resolution of 11 or 12 bits/sample. The ECG waveform of a normal heartbeat consists of a P wave, a QRS complex, and a T wave [1]. The P wave corresponds to the sequential depolarization of the right and left atria. The QRS complex is produced when the ventricles depolarize and squeeze the blood from the right ventricle to the aorta. The T wave occurs due to ventricular repolarization. A typical representation of the ECG waveform is shown in Figure 2. It can be seen that an ECG signal tends to exhibit considerable similarity between adjacent heartbeats, along with short-term correlation between adjacent samples. Thus, by dividing an ECG signal into heartbeat segments with lengths equal to the beats, there should be a large correlation between individual segments.

B. 2-D Image Matrix Construction

ECG itself is 1-D in the time-domain, but can be viewed as a 2-D signal in terms of its implicit periodicity. The QRS complex is the most characteristic wave in an ECG waveform and hence, its peak can be used to identify each beat. First of all, raw ECG signals are filtered to remove various noises. Afterwards we apply the Biomedical Signal Processing Toolbox [16] to detect the R peak of each QRS complex. Then, an ECG signal is divided into heartbeat segments and each segment is stored as one row of a 2-D data array. Having constructed the data array as such, the intra-beat correlation is in the horizontal direction of the array and the inter-beat correlation is in the vertical direction. Since the heartbeat segments may have different lengths, each row of the data array is period normalized to a fixed length of $N_p = 200$ samples via cubic spline interpolation. This choice was based on the observation that the average heartbeat length is about 0.8 second, which corresponds to 200 samples for a 250-Hz sampling frequency. Accordingly, the original heartbeat length was represented with 9 bits and transmitted as side information. Finally, we proceed to construct image matrices of dimension 200×200 by gathering together 200 rows of the data array and normalizing the amplitude of each component to an integer ranging from 0 to 255. A typical example of an ECG image matrix is shown in Figure 3. The constructed gray-scale ECG image matrices are then ready to be further compressed by the JPEG2000 still image coding standard.

III. JPEG2000 ENCODING ALGORITHM

Although the JPEG2000 coding standard was originally developed for still image compression, its applicability to ECG data compression has been proposed in [13]. Compared with the original JPEG coding standard, the wavelet-based JPEG2000 provides advanced features in scalability and flexibility. In addition, JPEG2000 supports Region of Interest (ROI) coding so that different parts of an image can be coded with different fidelity. The JPEG2000 encoding process consists of the following operations: 1) a preprocessing step which includes tilling, DC-level shifting and color space transform, 2) 2-D DWT followed by quantization, and 3) entropy coding and bit-stream organization. The fundamental building blocks of JPEG2000 are shown in Figure 4. The encoder begins with a preprocessor which divides the source image into rectangular blocks called tiles. For each tile, the DC level of image samples is shifted to zero and color space transform is performed to decorrelate the color information. Then, the 2-D DWT is carried out for each color component of a tile. Successive dyadic decompositions are applied and each of these splits high and low frequencies in the horizontal and vertical directions into four subbands. Among them, the subband corresponding to the lowest frequency in the two directions is used as a starting point for the next decomposition. This process is repeated for N levels until no significant gains in compression efficiency can be obtained. In total, $(3N+1)$ subbands are obtained with respect to an N-level 2-D wavelet decomposition.

The 2-D DWT can be viewed as a cascade of 1-D DWT in the horizontal direction and 1-D DWT in the vertical direction. Specifically, the 1-D DWT is based on the lifting scheme described in [17]. First, source data $x[n]$ are split into even samples $s_0[n] = x[2n]$ and odd samples $d_0[n] = x[2n+1]$. Then, the detailed coefficients $d_i[n]$ and the approximation

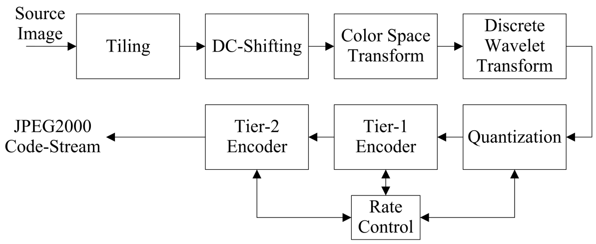


Figure 4. Fundamental building blocks of a JPEG2000 encoder [14].

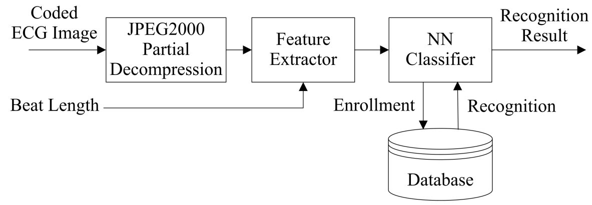


Figure 5. The proposed ECG biometric system.

coefficients $s_i[n]$ at the i-th iteration are calculated as follows:

$$d_i[n] = d_{i-1}[n] - \sum_k P_i[k] s_{i-1}[n-k], i = 1, 2, \ldots, N-1$$
$$s_i[n] = s_{i-1}[n] + \sum_k U_i[k] d_i[n-k], i = 1, 2, \ldots, N-1, \quad (1)$$

where P_i and U_i represent a predictor and an updater, respectively. Finally, both the detailed and approximation coefficients are normalized. For notational convenience, let $x_j(m,n)$ represent the wavelet coefficient located at position (m,n) in the j-th subband. After the 2-D DWT, a uniform quantizer is applied to quantize each wavelet coefficient $x_j(m,n)$ by an index $\bar{x}_j(m,n)$ as follows:

$$\bar{x}_j(m,n) = \text{sgn}(x_j(m,n)) \left\lfloor \frac{|x_j(m,n)|}{\Delta_j} \right\rfloor, \quad (2)$$

where Δ_j denotes the quantizer's step size. The last step in JPEG2000 compression consists in entropy coding with two tier encoders. In the tier-1 encoder, quantized indexes of each subband are split into code-blocks, which are then compressed using a context-based entropy coder. The tier-2 encoder truncates the bit-streams of each code-block to meet the targeted compression ratio, and combines them with additional headers to form the JPEG2000 code-stream.

IV. Proposed ECG Biometric Algorithm

Person identification is essentially a pattern recognition problem consisted of two stages: feature extraction and classification. Under the JPEG2000 framework, the person identification problem is analogous to a Content Based Image Retrieval (CBIR) problem. Concerning compressed-domain techniques, the JPEG2000 code-stream is subjected to partial decoding and then the energies from all subbands are used as the feature set. We also introduce a new method for feature extraction that involves the application of the Principal Component Analysis (PCA) for dimensionality reduction. In the classification stage, the query ECG image is compared with the enrollment database, and output the person identity that best matches the query with respect to some distance measurement criterion. Figure 5 shows the block diagram of the proposed ECG biometric system.

A. Feature Extraction in DWT Domain

Feature extraction is the first step in applying CBIR to ECG biometrics and one that conditions all the subsequent steps of system implementation. For arbitrary image databases of natural scenes, color and texture features are considered most important. Since 1-D ECG signals are converted to gray-scale images, we shall focus on the texture features that characterize smooth, coarse and regularity of the specific image. One effective tool to texture analysis is the DWT as it provides good time and frequency localization ability. Its multi-scale nature also allows the decomposition of an ECG into different scales, each of which represents particular coarseness of the signal. Furthermore, DWT coefficients in JPEG2000 can be obtained without involving a full decompression, as partial decoding of the JPEG2000 code-stream would suffice the needs. This is a favorable property as the inverse DWT and subsequent decoding processes could impose intensive computational burden. Different texture features such as energy, significance map, and intensity histogram at the output of wavelet filter-banks have been successfully applied to wavelet-based image retrieval [18]-[20]. In general, any measures that provide some degree of class separation should be included in the feature set. However, as more features are added, there is a trade-off between classification performance and computational complexity.

We began by using the energies from all subbands as a first step towards an efficient characterization of texture in compressed ECG images. This is because that the energy distribution along the frequency axis over scale and orientation has been shown effective for texture characterization in image retrieval [19][20]. For each subband, the reconstructed wavelet coefficients $\tilde{x}_j(m,n)$ are computed as follows:

$$\tilde{x}_j(m,n) = [\bar{x}_j(m,n) + r \cdot \text{sgn}(\bar{x}_j(m,n))] \cdot \Delta_j, \quad (3)$$

where $\bar{x}_j(m,n)$ represents the decoded quantizer indexes and the bias parameter r is set to be zero here. Then, the energy of the j-th subband is defined as

$$E_j = \frac{1}{M_j N_j} \sum_{m=1}^{M_j} \sum_{n=1}^{N_j} \tilde{x}_j^2(m,n), \quad (4)$$

where M_j and N_j represents the row and column dimension, respectively. Another feature of interest is the average time elapse between the current and previous R peaks, referred to as the RR-interval. Certain ECG arrhythmias, such as premature ventricular contraction and atrial premature beats, are related with premature heart beats that provide shorter RR-intervals than other types of ECG signals. Changes in the RR-interval plays an important role in characterizing these types of arrhythmias. Notice that the RR-interval can be calculated from the beat lengths which are transmitted as side information along with the JPEG2000 code-stream. In total, $(3N+2)$ features are used to form a Biometric Identification Vector (BIV), including the RR-interval and $(3N+1)$ subband energies.

The second feature set is obtained by applying PCA on the subband whose frequency is the lowest in both horizontal and vertical directions. This choice is based on the fact that human eyes are more sensitive to low frequency components than high frequency components. As one of the most commonly used dimension reduction techniques, PCA finds the most representative set of projection vectors such that the projected samples retain the most information about the original data samples. To begin, the M wavelet coefficients in the lowest frequency subband of a training dataset are used to compute the covariance matrix $\mathcal{C}$. Following an eigenvalue decomposition, we obtain an eigenvalue matrix D and its corresponding eigenvector matrix V with its column vectors sorted in the descending order of eigenvalues. Finally, column vectors of V are used as a basis set for projection of the data in the directions of sorted eigenvectors. Let $\mathbf{x}_l$ represent the data vector consisting of M wavelet coefficients in the lowest frequency subband taken from the l-th ECG image. The PCA procedure can be expressed as

$$\mathcal{C} = \sum_{l=1}^{N_t} (\mathbf{x}_l - \bar{\mathbf{x}})(\mathbf{x}_l - \bar{\mathbf{x}})^T = VDV^T, \tag{5}$$

where N_t is number of ECG images used in the training dataset and $\bar{\mathbf{x}}$ represents the mean vector of all $\mathbf{x}_l$. Then, the data vector $\mathbf{x}_l$ is projected on the eigenvectors by taking the inner product according to $\mathbf{y}_l = V^T \mathbf{x}_l$. In this work, the PCA was applied on $M = 49$ coefficients of the lowest frequency subband and seven principal components were selected corresponding to retaining approximately 99% of the total variability in the training dataset. Together with the RR-interval, only eight features are used to form a BIV for the second feature set.

B. Enrollment and Recognition

The proposed person identification system can be divided into two stages: enrollment and recognition. During the enrollment stage, a number of BIVs of each enrolled user were taken as a representation of the user and enrolled into a database. In the recognition stage, the ECG signals of an unknown subject are acquired and then compressed by JPEG2000. Afterwards, the feature extraction procedure results in a query BIV to be compared with all the BIVs enrolled in the database. Accordingly, the system outputs the person identity of an enrolled BIV which best matches the query BIV with respect to a distance measurement criterion. In this work, the Standard Euclidean Distance (SED) is adopted to measure the respective similarity between the query BIV $\mathbf{q}$ and each enrolled BIV $\mathbf{e}$. Mathematically, the SED is denoted by $d_{\mathbf{q},\mathbf{e}}$ and can be expressed as

$$d_{\mathbf{q},\mathbf{e}} = \sqrt{\sum_{i=1}^{L} (\frac{\mathbf{q}(i) - \mathbf{e}(i)}{\sigma_i})^2}, \tag{6}$$

where L is the length of the BIV, $\mathbf{q}(i)$ and $\mathbf{e}(i)$ denote the i-th component in the corresponding BIV, and the scale factor σ_i represents the standard deviation computed from the i-th component of all enrolled BIVs. As the data belonging to the same class should be close in the feature space, a Nearest-Neighbor (NN) classifier is used to search for the minimum SED value and assigns its corresponding person identity as the recognition result.

V. Experimental Results

Computer simulations were conducted to evaluate the performance of the proposed compressed-domain approaches for person identification. Two ECG biometric systems based on JPEG2000, denoted by PA1 and PA2, are presented and investigated. They both applied a preprocessor for construction of the 2-D ECG image matrices in the JPEG2000 format and used an NN classifier for subsequent person identification. Unlike the PA1 which was performed using subband energy-based feature set, the PA2 extracted the wavelet coefficients from the lowest frequency subband and represented in a lower dimensional space using PCA. 10 normal subjects and 30 diseased subjects from the QT Database are chosen to represent a wide variety of QRS and ST-T morphologies. The JPEG2000 codec used here was the open-source software JasPer version 1.900.0 [21]. ECG images were compressed in a lossy mode using Daubechies 9/7 filter with 5-level of decomposition, while the dimension of each tile and code-block is set to be 200×200 and 64×64, respectively. Besides, the parameter value of coding rate ρ is set to be 0.15 and 0.08 in order to achieve the compression ratio of 10 and 20, respectively.

A preliminary experiment was first conducted on normal and diseased ECG signals to examine the performance of 2-D compression by JPEG2000 [13]. Typically, the performance is evaluated in terms of the compression ratio (CR) and the percent root mean square difference (PRD). The CR is defined as

$$\text{CR}=\frac{N_{ori}}{N_{com}}, \tag{7}$$

where N_{ori} and N_{com} represent the total number of bits required for the original and compressed ECG data, respectively. The PRD is used to evaluate the reconstruction distortion and is defined by

$$\text{PRD}(\%) = \sqrt{\frac{\sum_{k=1}^{K} [x_{ori}(k) - x_{rec}(k)]^2}{\sum_{k=1}^{K} x_{ori}(k)^2}} \times 100, \tag{8}$$

where K is the total number of original samples in the record and x_{ori} and x_{rec} represent the original and reconstructed ECG signals, respectively. Table I presents the average results for 2-D compression of various ECG records using JPEG2000 with coding rate $\rho = 0.15$ and $\rho = 0.08$. As should be expected, the PRD performance of the system is related to the severity of disease. For the coding rate of $\rho = 0.08$, the individual PRD performances of the ECG records vary from 5.11% to 7.31% depending on the characteristics of normal and pathological ECG signals. Although the 2-D compression method shows good results for normal ECG signals, it may suffer from irregular rhythms mainly due to the QRS detection stage. In order to exploit the inter-beat correlation, the ECG signal is QRS detected and then segmented according to the detected fiducial points. As a consequence, the performance of 2-D ECG compression algorithms is affected by the accuracy of the QRS detection scheme. Compared with normal subjects, the worse performance of diseased subjects may be attributed to the fact that the number of QRS false detections may increase significantly in the presence of noise and varying QRS morphology.

The next step is to evaluate the recognition performance of the proposed ECG biometric system on different datasets. The system performance is evaluated in terms of the recognition rate, which is normally defined as the ratio of the number of correctly identified subjects to the total number of testing subjects. First of all, the proposed biometric systems were individually tested on datasets from D1 to D4. Table II presents the recognition rate performances associated with various datasets for the case where the ECG images are subjected to JPEG2000

 ISBN: 978-1-61208-365-0

TABLE I
AVERAGE CR AND PRD PERFORMANCES FOR JPEG2000 WITH RATE $\rho = 0.15$ AND $\rho = 0.08$.

Rate ρ		D1	D2	D3	D4
0.15	CR	14.28	9.88	10.72	10.64
	PRD	3.08%	3.54%	3.32%	3.10%
0.08	CR	21.66	17.36	19.70	19.20
	PRD	5.11%	7.31%	7.24%	7.25%

TABLE II
RECOGNITION RATES (%) OF THE PROPOSED METHODS.

Dataset	JPEG2000 ($\rho = 0.15$)		JPEG2000 ($\rho = 0.08$)	
	PA1	PA2	PA1	PA2
D1	96.18	99.98	95.45	99.99
D2	87.66	91.95	87.73	91.53
D3	91.48	95.50	91.54	95.46
D4	84.87	91.85	83.95	92.18
D1, D2	90.19	94.97	90.25	94.20
D1, D2, D3	89.98	96.39	89.16	95.92
D1, D2, D3, D4	89.55	95.72	89.39	95.66

encoding with coding rate $\rho = 0.15$ and $\rho = 0.08$. Data in the table have been averaged over 1000 trials per subject. For each subject, we randomly selected four compressed ECG images for feature extraction and one BIV results for each ECG image. Among them, the first two BIVs of each subject are used for training in the enrollment stage, and the other two BIVs are used for testing in the recognition stage. The results clearly demonstrate the improved performance achievable using PA2 in comparison to that of PA1. By the method PA2 with $\rho = 0.15$ applied individually on datasets from D1 to D4, the recognition rate was 99.98% for normal subjects, 91.95% for arrhythmia subjects, 95.50% for supraventricular arrhythmia subjects, and 91.85% for sudden cardiac death subjects. To elaborate further, we also investigate the performance of PA2 when normal and diseased subjects are jointly enrolled and tested. With this in mind, the initial 10 normal subjects are combined with an additional 10, 20, and 30 diseased subjects and the system is retrained and tested again. The results in Table II show a correct recognition rate of 94.97% when the system PA2 is jointly tested on datasets D1 and D2. When 10 other subjects from dataset D3 were added into the database, recognition rate was 96.39%. Lastly, 95.72% was achieved with the entire database containing 10 normal subjects and 30 diseased subjects. As the table shows, the additional inclusion of 30 diseased subjects only dropped the recognition rate by 4.26%. This clearly demonstrates that the proposed system PA2 is robust enough to handle the inclusion of diseased ECG in the biometric database.

VI. CONCLUSIONS

This paper proposed a fast method of ECG biometric recognition that directly uses the compressed ECG data in JPEG2000 format. Under the JPEG2000 framework, the person identification problem is analogous to a context-based image retrieval problem. In this work, we have compared the performances of two feature sets for texture characterization in compressed ECG images. The first feature set uses the energies of all subbands, whereas the second feature set is obtained by applying PCA on the wavelet coefficients of the lowest frequency subband. Also, we look into the effects of diseased subjects on the recognition rate of a compressed-domain ECG biometric system. The proposed ECG biometric system has been tested on standard ECG databases and high recognition accuracy is achieved with a low feature dimension.

ACKNOWLEDGMENT

This research was supported by the National Science Council, Taiwan, ROC, under Grant NSC 102-2221-E-009-030-MY3.

REFERENCES

[1] M. S. Thaler, The Only EKG Book You'll Ever Need, 7th ed. Philadelphia, PA: Lippincott Williams & Wilkins, 2012.

[2] L. Biel, O. Pettersson, L. Philipson, and P. Wide, "ECG Analysis: A New Approach in Human Identification," IEEE Trans. Instrum. Meas., vol. 50, no. 3, Jun. 2001, pp. 808-812.

[3] S. Israel, J. Irvine, A. Cheng, M. Wiederhold, and B. Wiederhold, "ECG to identify individuals," Pattern Recognit., vol. 38, 2005, pp. 133-142.

[4] T. W. D. Shen, W. J. Tompkins, and Y. H. Hu, "Implementation of a one-lead ECG human identification system on a normal population," J. Eng. Comput. Innovations, vol. 2, no. 1, Jan. 2011, pp. 12-21.

[5] I. Odinaka et al., "ECG biometric recognition: A comparative analysis," IEEE Trans. Inform. Forensic Secur., vol. 7, no. 6, Dec. 2012, pp. 1812-1824.

[6] C. C. Chiu, C. M. Chuang, and C. Y. Hsu, "Discrete Wavelet Transform Applied on Personal Identity Verification with ECG Signal," Int. J. Wavelets Multi., vol. 7, no. 3, May 2009, pp. 341-355.

[7] S. A. Fattah, C. Shahnaz, A. S. M. M. Jameel, and R. Goswami, "ECG Signal Based Human Identification Method Using Features in Temporal and Wavelet Domains," in Proc. TENCON 2012, Nov. 2012, pp. 1-4.

[8] D. Hatzinakos, K. Plataniotis, and J. K. M. Lee, "ECG Biometric Recognition Without Fiducial Detection," in Proc. IEEE Biometrics Symposiums (BSYM), Sep. 2006, pp. 1-6.

[9] Y. Wang, F. Agrafioti, D. Hatzinakos, and K. Plataniotis "Analysis of human electrocardiogram ECG for biometric recognition," EURASIP J. Adv. Signal Process., vol. 1, Jan. 2008, pp. 1-6.

[10] S. M. S. Jalaleddine, C. G. Hutchens, R. D. Strattan, and W. A. Coberly, "ECG data compression techniques - a unified approach," IEEE Trans. Biomed. Eng., vol. 37, no. 4, Apr. 1990, pp. 329-343.

[11] B. Wang and G. Yuan, "Compression of ECG data by vector quantization," IEEE Eng. Med. Biol. Mag., vol. 16, no. 4, Jul./Aug. 1997, pp. 23-26.

[12] C. C. Sun and S. C. Tai, "Beat-based ECG compression using gain-shape vector quantization," IEEE Trans. Biomed. Eng., vol. 52, no. 11, Nov. 2005, pp. 1882-1888.

[13] A. Bilgin, M. W. Marcellin, and M. I. Altbach, "Compression of electrocardiogram signals using JPEG2000," IEEE Trans. Consum. Electron., vol. 49, no. 4, Nov. 2003, pp. 833-840.

[14] D. S. Taubman and M. W. Marcellin, JPEG 2000: Image Compression Fundamentals, Standards, and Practice. Norwell, MA: Kluwer, 2001.

[15] The QT Database. [Online]. Available from: http://physionet.org/physiobank/database/qtdb/ 2014.05.04

[16] M. Aboy et al., "A biomedical signal processing toolbox," in Proc. Biosignal 2002, Jun. 2002, pp. 49-52.

[17] I. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting steps," J. Fourier Anal. Appl., vol. 4, no. 3, 1998, pp. 245-267.

[18] J. R. Smith and S. F. Chang, "Transform features for texture classification and discrimination in large image databases," in Proc. IEEE Int. Conf. Image Process., Nov. 1994, pp. 407-411.

[19] A. Teynor, W. Müller, and W. Kowarschick, "Compressed domain image retrieval using JPEG2000 and gaussian mixture models," Visual Information and Information Systems, Visual Information and Information Systems, Lecture Notes in Computer Science, vol. 3736, 2006, pp. 132-142.

[20] M. N. Do and M. Vetterli, "Wavelet-Based texture retrieval using generalized Gaussian density and Kullback-Leibler distance," Proc. IEEE Trans. Image Process., vol. 11, no. 2, Feb. 2002, pp. 146-158.

[21] The JasPer Project Home Page. [Online]. Available from: http://www.ece.uvic.ca/~frodo/jasper/ 2014.05.04

Teaching Networking: A Hands-on Approach that Relies on Emulation-based Projects

António Nogueira, Paulo Salvador
DETI - University of Aveiro/Instituto de Telecomunicações
Aveiro, Portugal
e-mail: {nogueira,salvador}@ua.pt

***Abstract*—Computer networking is an inescapable reality of our days, being part of the curricula proposed by almost all universities. Effective learning and teaching of networking, however, require students to gain hands-on experiences in developing projects, which will help them to understand basic concepts as well as the strengths and limitations of the technology. At our university, we devised a new approach to teach networking concepts by requiring students to develop emulation-based projects in parallel with traditional theoretical classes and practical classes involving real networking equipment. The effectiveness of this teaching methodology was evaluated formally by the students' opinions and classification marks, and informally, in discussions within the teaching team. This paper describes the global philosophy behind this new teaching methodology, as well as its implementation approach and obtained results. The evaluation results that were achieved, representing a clear improvement of past results, allow us to conclude that the proposed approach is very promising. In fact, the emulation-based hands-on approach is able to motivate students and smooth their learning curve since they are close to reality and, at the same time, have the freedom to work everywhere at anytime and are free from boring physical connectivity problems.**

Keywords-Practical teaching; networking project; emulation; GNS3.

I. Introduction

Computer networking became an indispensable part of our daily life. Many books have been written on this topic, which is being taught in both undergraduate and graduate level courses. Although students learn a lot of concepts in traditional courses, they do not have enough hands-on experience with real networks or in-depth understanding of how things work in practice. In order to circumvent these shortcomings, many universities developed lab-based networking courses [1][2][3], which are very useful to teach concepts but are not able to cover as much material as traditional courses due to the lack of time and resources. Most of the times, these labs do not scale to hundreds of students. Besides, in the austerity days we are facing it is very difficult to buy expensive networking equipment in order to equip one or several functional laboratories.

Therefore, we need to design new networking experiments that are focused on teaching essential networking topics, while taking availability of resources into account. Simulation and emulation seem to be good compromises between the need to use virtual environments and the connection to the real world that should not be broken. There are several networking software tools that can be used to analyze, emulate and simulate computer networks. Among the different possibilities, Graphical Network Simulator, version 3 (GNS3) was the chosen emulation environment [14]; it is basically a hardware emulator (called a hypervisor) that creates a virtual environment on a host computer (running Windows, Linux or Mac). By running Cisco Internetwork Operating System (IOS) software on the hypervisor, the student can create complex networking scenarios with the real look and feel of hardware devices because he is interacting with the real IOS that is running on virtualized routers.

Based on this rationale, we devised a new approach to teach networking concepts by requiring students to develop emulation-based projects in parallel with traditional theoretical classes and practical classes involving real networking equipment. In this paper, we describe our experience of introducing an emulation-based project as a key pedagogical method for teaching advanced computer networks in a specific course, named Networks Architecture, which belongs to the third year of the undergraduate level. A three-threaded teaching approach was adopted for this course, comprising: (i) theoretical classes; (ii) practical classes, where real networking equipment is used and (iii) a network project that allows students to gain practical experience and a deeper understanding of the key concepts of network protocols and technologies.

The lecture and practical threads use face-to-face teaching, group work and discussion, allowing a deep interaction between students and teachers. In the network project, students are typically organized in groups of two people and have several tasks to accomplish ”after hours”: after designing and dimensioning a medium to large size corporate network, they have to configure and test it in GNS3.

The effectiveness of this teaching approach was extensively evaluated, formally by the students' opinions and classification marks and informally in discussions within the teaching team. The quite good evaluation results that were achieved, particularly when compared to results from previous years, allowed us to conclude that this approach is very promising. The hands-on approach is very important to motivate students, because they can “feel” the network and, at the same time, have the freedom to work

 ISBN: 978-1-61208-365-0

everywhere, anytime, and get rid of the cables and connectivity problems.

The remaining part of the paper is organized as follows: Section II discusses some teaching issues that should be taken into account when planning a computer networking course; Section III briefly discusses some relevant network simulation and emulation tools; Section IV presents the network project that was designed, including its description, tasks and resolution strategy; Section V presents the most relevant outcomes; finally, Section VI presents the main conclusions.

II. TEACHING ISSUES

Besides the continuous changing nature of computer networking and the heterogeneity in students' backgrounds, there are some other obstacles of teaching and learning this subject. First of all, the underlying principles are complex and very abstract to many students (they do not find an easy connection to reality).

Besides, the layered approach that is frequently adopted is considered inadequate by most of them, since there is not a clear identification of the functionalities of the different layers, as well as a clear separation between them.

Since most students lack practical experience, they have difficulties to understand common networking problems and overcome difficulties. Providing a hands-on practical experience to students is also problematic because some academic environments do not have the adequate resources. Networking labs are still quite expensive.

The sequence of subjects' coverage can also affect learning. Traditionally, top-down [4] and bottom-up [5] approaches have been intensively used, both on Computer Science and Engineering courses. However, a non-linear path on the coverage sequence seems to be the best choice in most situations.

In order to address some of these concerns, we changed the pedagogical approach that was usually followed in the Networks Architecture course by introducing an emulation-based project in parallel with traditional theoretical and practical classes. Besides the two hours/week theoretical classes and the three hours/week laboratorial classes (where students interact with real networking equipment), the network project adds two more hours/week to the course workload in order to allow students to gain a deeper understanding of the key concepts of network protocols and technologies. The project is developed by groups of two students and spans from the first to the last week of the course (usually, this period corresponds to 15 weeks). The project evaluation is based on a practical demonstration and an oral examination (so, group elements can get different marks) and the obtained mark has a weight of 40% in the global course mark (the weights of the theoretical exam and the lab activities are equal to 40% and 20%, respectively).

III. NETWORK SIMULATION AND EMULATION TOOLS

The deployment of real networks is not practical and can be really expensive depending on the size of the network and the number of computers, routers, switches or other network devices that have to be used. Nowadays, there are many software tools that can be used to perform network simulation and some of them can recreate exactly any detail of a real network. This allows an easy network deployment, with the benefits of saving space, money and time.

A. Network Simulator

Network Simulator (NS), developed by research laboratories and top research universities and funded by National Science Foundation (NSF), has been the major software simulation tool for network research for more than 20 years. Its most popular version, NS2, is a discrete-event simulator in which the routing algorithms are written in C++ as pre-built into the library, while events are configured using OTcl language [6]. Due to the unpopularity and the slow learning curve of OTcl, NS is seldom used in classroom teaching.

The last version of NS, NS3 [7], is under the General Public License (GPL) and provides free download of its source codes. The core of NS3 is written in C++ and has a Python scripting interface. Protocol entities are designed to be closer to real computers and NS3 includes support for virtualization, using lightweight virtual machines [7].

B. OMNeT++

Similarly to NS2 and NS3, OMNeT++ is also a public-source, component-based network simulator with Graphical User Interface (GUI) support [8]. Its primary application area is communication networks. OMNeT++ has generic and flexible architecture, which makes it successful also in other areas like Information Technology (IT) systems, queuing networks, hardware architectures, or even business processes.

OMNeT++ components are called modules and are programmed in C++. The components are then assembled into larger components and models by using a high-level language. The simulation kernel can be embedded into all kinds of different users' applications.

C. OPNET

OPNET is the commercial counterpart of NS [9]. It has a rich set of modelers that support the latest wireless and emerging network technologies. The user friendly interfaces are intuitive to use for creating network topologies, configuring and simulating network traffics, and collecting and visualizing data. The OPNET IT Guru academic version is free for teaching and research in academia. Many universities are adopting OPNET in teaching general networking courses because it has intuitive user interfaces and lab manuals for popular textbooks.

Both NS and OPNET are excellent tools for conducting research or teaching general network concepts. However, their configuration process is very different from the real-world networking or security devices that are dominated by Cisco appliances.

D. Cisco Packet Tracer

Cisco Packet Tracer is a network simulation software developed by Cisco to support its Networking Academy Program. This software provides visual network simulation and allows creating networks with an almost unlimited number of devices. The configuration of the network devices is made through a command-line interface, similarly to real equipment. It also provides tables, diagrams and other visual representation and offers a multiuser functionality that permits multiple users to work on the same project through the Internet [10].

Packet Tracer has two operation modes: the real-time mode that shows how real devices behave and the immediate network response to any network change; the simulation mode, which is directed to background concepts and allows controlling time intervals, data transfer rates and bandwidth and manipulate the propagation of data packets through the network. This software supports the possibility of inserting interface cards into modular routers and switches, creating virtual networks over real ones.

The most important limitations of Packet Tracer are related to its performance and to the lack of support for some important advanced networking mechanisms and protocols.

E. NetSim

Network Simulator (NetSim) is a Cisco network simulator developed by Boson, a company that provides material to prepare students for IT certification exams from Cisco, Microsoft CompTIA, and others [11]. It uses the Boson's proprietary Network Simulator, Router Simulator and EROUTER software technologies to simulate a real network and is available on three different versions, each one with specific characteristics and directed to a different certification.

NetSim supports up to 42 routers and 6 switches, on a total of 200 devices on the network. It simulates network traffic using virtual packet technology and provides Telnet or Console modes to interact with the network devices. This software is not open-source, which is a clear handicap for educational purposes.

F. Graphical Network Simulator v3

GNS3 [12] was introduced many years ago, when an open-source hypervisor called Dynamips was written to emulate Cisco routers. Dynamips was intended to emulate Cisco IOS hardware and was fairly complicated to use. So, a GUI was added to manage the process of the hypervisor, which is exactly what is called GNS3. So, GNS3 is the front-end for multiple hypervisors, including Dynamips and Qemu, with the latter being used to emulate hardware used by the Cisco Adaptive Security Appliance (ASA) firewall.

While Dynamips is responsible for the back-end operation of emulating routers with real IOS images, GNS3 uses Dynagen as the text-based front-end to establish communication with Dynamips [12]. GNS3 also supports other machine emulators and virtualizers like Qemu [16], Virtualbox [17] or Pemu [18]. This allows a user to simulate networks with a wide diversity of devices, like Cisco ASA and Private Internet eXchange (PIX) firewalls, Cisco IPS, Juniper routers or hosts (based on different operating systems, like Linux, Windows, MacOS X).

So, GNS3 affords anyone with a computer a way to practice network topologies. But it goes beyond that: users can quickly set up routers and firewalls, using simple drag-and-drop actions on the screen. It is easy to add Ethernet connections between devices or add hardware modules to routers in the virtual GNS3 topology for more complex network designs.

Another relevant advantage of GNS3 is the possibility of connecting the virtual network to the real world, with real devices, besides the ability to perform packet capture and analysis using Wireshark [13].

Layer 2 Ethernet switching inside of a GNS3 topology is limited to the switchport modules that can be added to the virtual routers inside GNS3, which do not support the full layer 2 switching capabilities that a physical switch would provide.

GNS3 also has some other limitations: its throughput is limited to 1000 packets per second in the virtual environment, it can consume a large amount of real and virtual memory and it can achieve high Central Processing Unit (CPU) usage levels [14]. Although GNS3 already includes some tools to prevent this memory and CPU usage levels, we should always take into account that the higher the number of routers and network devices, the higher will be the consume [15].

In summary, we can say that, in spite of these limitations, GNS3 is one of the most valuable tools for practicing, proof-of-concept design, protocol analysis and verification.

IV. Network Project

In order to address the different topics of the Networks Architecture course, we devised a network project that could be solved incrementally and whose solution could be implemented in GNS3. In line with the course objectives, the most relevant topics that should be studied and implemented in this project are: definition of Virtual Local Area Networks (LANs), Internet Protocol, version 4 (IPv4) and IPv6 addressing, internal routing based on the Routing Information Protocol (RIP), RIP next generation (RIPng), Open Shortest Path First, version 2 (OSPFv2) and OSPFv3 routing protocols, multicast routing, Quality of Service (QoS) mechanisms, IPv4/IPv6 transitions mechanisms, Internet Protocol Security (IPSec), Access Control Lists (ACLs) and network management based on scripting.

A. General Problem Description

Let us suppose that we want to design, implement and test the communications infrastructure of a medium to large size company. We will start by presenting the problem enunciation that was proposed to students of the Networks Architecture course.

Company Example, Inc. has a strong Research and Development (R&D) component and will expand its facilities in Aveiro (currently, they are composed by a single building), with two new three-floor (adjacent) buildings. The company will also create two new branches, one in Lisbon and another in San Jose, California. The old Aveiro network should not be changed, but its connectivity with the new buildings and with the Internet should be assured.

The first floor of each building is reserved for the production zone; the second floor of the first building is reserved for sales and client support and the last floor of the first building is reserved for the administration offices; floors 2 and 3 of the second building are reserved to R&D.

Let us suppose that each production floor has: (i) 12 production points (machines/robots), (ii) 3 technical verification zones (machines/terminals), (iii) a meeting/reception room and (iv) a videoconference room. The sales and client support floor has: (i) 50 sales rooms, (ii) 2 meeting rooms to contact clients via videoconference and (iii) 50 workplaces for client support. Each R&D floor has: (i) 20 laboratories, each with at least 8 workplaces, (ii) 4 rooms reserved to engineering development, (iii) a lounge top workers/visits. The administration floor should support 20 persons and includes 2 videoconference rooms.

At the Lisbon and San Jose branches, the company will have single 2 floor buildings, with the first floor being reserved for R&D laboratories (25 researchers per lab) and the second floor being reserved for local administrative services (15 persons).

The company will have communication services (data, voice and video) implemented over IP, as well as a video-surveillance system and 3 internal Internet Protocol Television (IPTV) channels.

Finally, the company has two datacenters (services and storing) in Aveiro and San Jose that will support the different activities: administration/planning (management archive), R&D (scientific archive and data processing) and public services to employees and general community via Internet.

B. *Objectives*

For the three new networks of the Example, Inc. branches, students have to:

- Present the Open Systems Interconnection (OSI) Layer 2 networks subdivision (VLANs design).
- Define the public IPv4 addressing scheme (assuming that the company owns network 193.2.2.0/24 in Portugal and network 195.1.1.0/26 in the USA) and the private IPv4 scheme and the respective translation mechanisms.
- Define the IPv6 addressing scheme (assuming that the company owns network 2002:C:C::/48 in Portugal and network 2001:F:F::/48 in the USA).
- The company has two Internet access contracts with Portuguese ISPs PT1 and PT2 for the Aveiro and Lisbon sites, respectively.
- All network sites should include a wireless network divided in two distinct VLANs, with distinct permissions. All network sites should also have internal IPTV channels. We can assume that each site has its own independent multicast video server.
- ISP PT2 does not support IPv6 addressing/routing. Propose and implement a solution that allows full IPv6 connectivity between the Portuguese network sites of the company in case of a complete failure of ISP PT1 (the default IPv6 connectivity provider).
- In order to guarantee the confidentiality of some communications, students should configure a Virtual Private Network (VPN) IPSec between the company sites and define the respective routing policies (i.e., which traffic should be transported by the VPN). Besides, they should configure a secure connection between the old and the new datacenters in the Aveiro site.
- Based on the underlying structure and configurations, students should define and configure mechanisms of traffic differentiation that implement the QoS policies that are necessary for the network services in operation.
- Students should also develop a scripting system that can be used to support network monitoring and management. In a first phase, the system should identify all network equipments (routers and switches), their interfaces and the corresponding link loads.

C. *Specific Tasks*

In order to achieve the above mentioned goals, students have to perform several specific tasks:

- Design the logical network architecture and the corresponding physical mapping.
- Define the characteristics/capabilities of the different network equipments.
- Define the (virtual) local networks.
- Define the IPv4 and IPv6 addressing schemes.
- Make some extra definitions (like for example budget, non-network equipments, etc.).
- Configure the access layer and define the interconnection/addressing of the terminal equipments.
- Configure the IPv4 unicast routing.
- Configure the IPv6 unicast routing.
- Implement private addressing translation mechanisms.
- Configure the multicast IPv4 and IPv6 routing.
- Implement QoS policies.
- Configure the IPv4/IPv6 transition mechanisms.
- Configure internal secure connections and external secure connections between branches (as well as the corresponding routing mechanisms).
- Write monitoring scripts (in bash language).
- Perform some extra configurations (control access rules, Dynamic Host Configuration Protocol (DHCP) server, user VPN server, etc.).

Although these tasks can be solved in a slightly different order, students should be aware that some of them are dependent on others. So, this list of tasks is given to students, in order to guide them in their starting efforts.

D. *Resolution Strategy*

As happens in most situations, the best strategy to solve this exercise is to split it into sub-exercises.

 ISBN: 978-1-61208-365-0

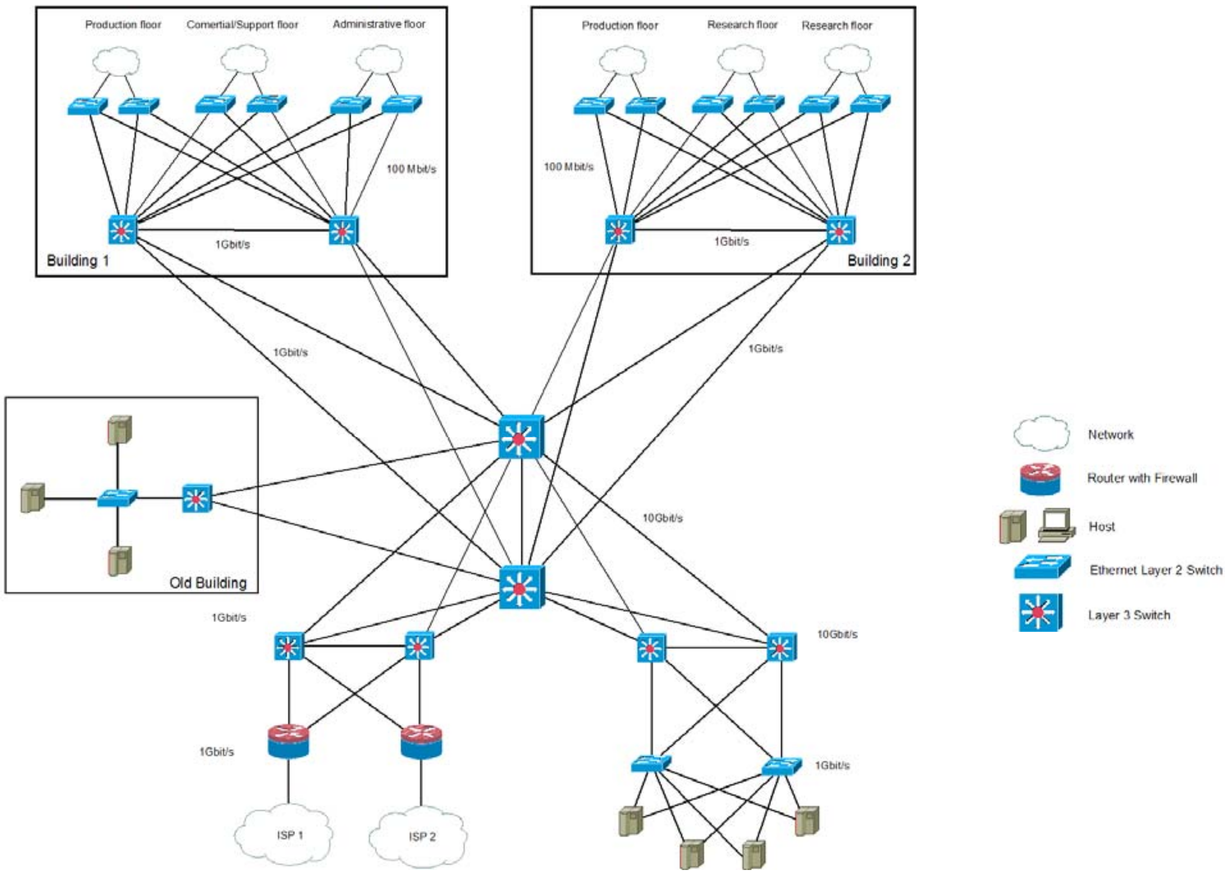


Figure 1. Network topology for the Aveiro site.

Actually, this approach has two main advantages: each sub-problem is easier to address and the computational resources that it will require (using GNS3) are substantially lower than the resources that would be needed to solve the complete problem.

So, the first step should be to look at each company site, designing, configuring and testing its own network. Following this approach, Figs. 1, 2 and 3 illustrate the topologies of the networks that could be designed for the Aveiro, Lisbon and San Jose sites, respectively. In this design phase, a correct definition and dimensioning of the access, distribution and core layers is crucial for the remaining phases of the project. In this phase, the students, usually, interact a lot with their teachers in order to find the best solution. After this effort, the definition of the different VLANs and the addressing issues are the most relevant topics that have to be addressed.

These high-level networks (corresponding to the company sites) are implemented and tested separately in GNS3: obviously, a last experiment should be dedicated to the interconnection of these networks, where each one corresponds to the communications infrastructure of a different company site.

On the other hand, the students must also specify the design and implementation details of the network corresponding to each floor, which were represented as generic clouds in the higher level network diagrams of Figs. 1, 2 and 3. As an example, Fig. 4 presents the network topology for the Research floor infrastructure. Quite similar topologies should be designed for the other floors.

Besides specifying the network equipments (type, model, characteristics, number of the interfaces, interfaces types, etc.), students have to present and discuss the network topology of these lower level networks. Obviously, this refinement process should be repeated until the desired level of detail is achieved.

After completing the design and dimensioning phases, the project enters in the implementation phase: here, all network connections, equipments, configuration details, GNS3 performance mechanisms (like the *Idle PC* feature), should be conveniently addressed. Troubleshooting methodologies are crucial in this phase. Usually, this phase also implies a lot of interaction between students and teachers.

Finally, the testing phase is used to validate the implemented network(s), eventually changing some of the decisions that were previously taken. So, this is a closed-loop process that can go through several iterations.

 ISBN: 978-1-61208-365-0

V. Evaluation

The effectiveness of the three-thread teaching approach was evaluated in several ways: informally, in discussions within the teaching team, and formally by the students' opinions and classification marks.

Regarding the first evaluation criteria, the merits of this teaching methodology were consensual among the teaching team. Actually, everyone felt that students were more engaged with the course and spent a higher number of hours studying and working on these networking topics. So, the satisfaction degree of the teaching team was quite high.

The students' opinions were obtained through a written questionnaire that is part of the Quality Assurance Plan of our university. The most important results obtained are the following: the global satisfaction with the course was rated by students with 7.11 out of 8, while the appropriateness of the proposed activities to the course objectives was rated with 7.38 out of 8. These results are generally very good, and when compared to the results obtained for the same items in the previous Academic year of 2012 (6.68 and 7.02, respectively), allow us to conclude that a very positive evolution was achieved.

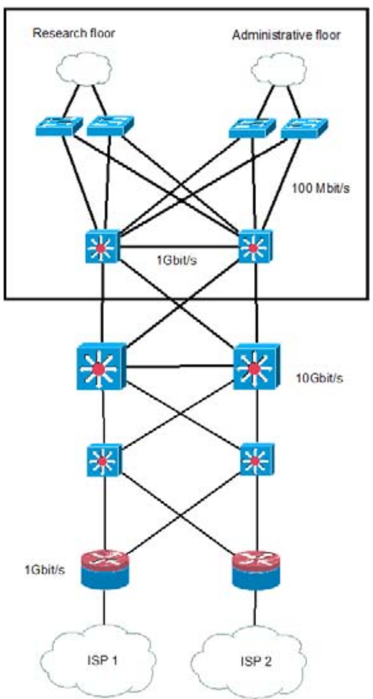


Figure 2. Network topology for the Lisbon site.

Finally, we should look at the course classification marks. Figures 5 and 6 show the marks obtained in 2012 and 2013, respectively, for a total number of students equal to 54 in 2012 and 50 in 2013. The number of students that failed in this course decreased from 25.93% in 2012 to 10.00% in 2013. This is a very relevant result, since we were able to substantially increase the success rate of this course. If we look at the average mark obtained by well-succeeded students, we can see that it increased from 12.1 (out of 20) in 2012 to 12.53 in 2013. Although only two students were able to achieve a classification of 17 (Very Good) in 2013, the most important slice of students was able to reach a quite satisfactory mark of 13 out of 20.

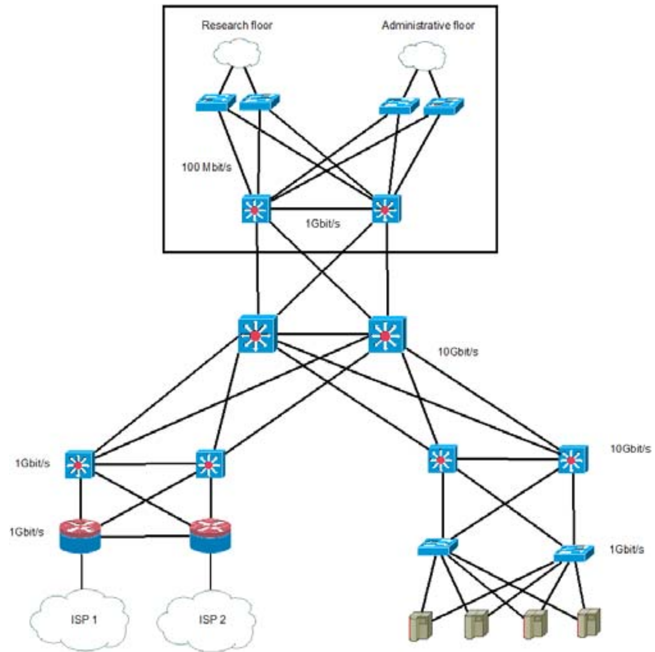


Figure 3. Network topology for the San Jose site.

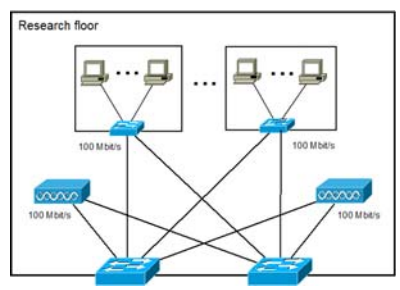


Figure 4. Network topology for the Research floor of the Aveiro site.

Regarding the marks that were obtained in the emulation-based project itself, we can say that they were quite high: with few exceptions, all students were able to obtain marks of 16 and higher (out of 20), marks that are typically higher than the ones they are able to obtain in the theoretical exam. This is clearly related to the practical nature of this component and to the interest that this type of work clearly induces in students.

The quite good results that were achieved in the different evaluation criteria, particularly when compared to the results from the previous year (where no project was proposed to students), allow us to conclude that this multi-thread teaching approach is very promising.

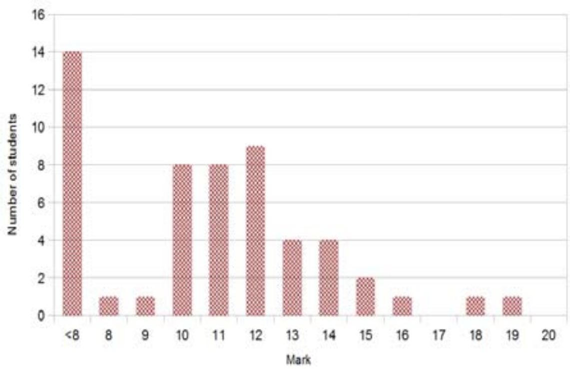


Figure 5. Classification results of the Networks Architecture course - 2012.

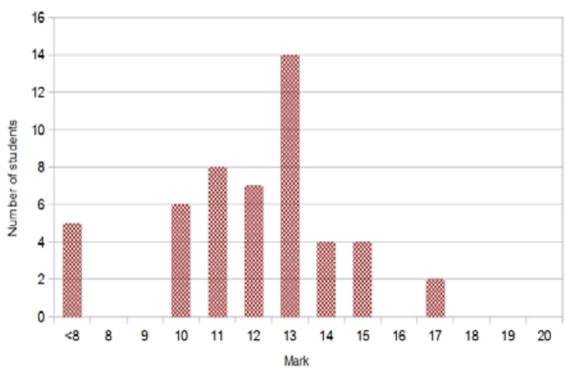


Figure 6. Classification results of the Networks Architecture course – 2013

The hands-on approach promoted by face-to-face lab classes and emulation-based networking projects is very important to motivate students, because they can "feel" the network and, at the same time, have the freedom to work anytime and everywhere and get rid of the cables and connectivity problems.

VI. CONCLUSIONS

This paper describes our experience of introducing an emulation-based project as a key pedagogical method for teaching advanced computer networks. A three-threaded teaching approach was adopted in a third-year undergraduate course, comprising theoretical classes, practical classes involving real networking equipment and a network project that allows students to gain practical experience and a deeper understanding of the key concepts of network protocols and technologies.

The effectiveness of the used teaching approach was evaluated formally by the students' opinions and classification marks and informally through discussions within the teaching team. The quite good evaluation results that were achieved, particularly when compared to results from previous years, allowed us to conclude that the proposed approach is very promising. In fact, the hands-on approach can motivate students because they are more engaged to reality but, at the same time, have the freedom to work everywhere and do not suffer from physical connectivity problems.

ACKNOWLEDGMENT

This work was supported by Fundação para a Ciência e a Tecnologia (FCT) of Portugal, under the auspices of project PEst-OE/EEI/LA0008/2013.

REFERENCES

[1] D. E. Comer, "Hands-On Networking with Internet Technologies", Prentice Hall Inc., 2002.

[2] W. J. Dewar and S. S. Sethi, "A Laboratory for Teaching Computer Networks", IEEE Transactions on Education, vol. 38, no. 2, 1995, pp. 145-149, doi: 10.1109/13.387216.

[3] M. El-Kharashi, G. Darling, B. Marykuca, and G. C. Shoja, "Understanding and Implementing Computer Network Protocols Through a Lab Project", IEEE Transactions on Education, vol. 45, no. 3, 2002, pp. 276-284, doi: 10.1109/TE.2002.1024621.

[4] J. Kurose and K. Ross, "Computer Networking: A Top-Down Approach Featuring the Internet", Second Edition, Addison Wesley Longman, 2003.

[5] A. Tanenbaum, "Computer Networks", Fourth Edition, Prentice Hall PTR, 2003.

[6] NS2, "NS2 official website", [Online]. Available from: http://www.isi.edu/nsnam/ns/ [Retrieved: April 2014].

[7] NS3, "NS3 official website", [Online]. Available from: http://www.nsnam.org/documents.html [Retrieved: April 2014].

[8] OMNeT, "OMNeT++ official website", [Online]. Available from: http://www.omnetpp.org/ [Retrieved: April 2014].

[9] OPNET, "OPNET Modeler", [Online]. Available from: http://www.opnet.com/ [Retrieved: April 2014].

[10] Cisco Systems, "Cisco Networking Academy", [Online]. Available from: http://www.cisco.com/web/learning/netacad/index.html. [Retrieved: April 2014].

[11] Boson, "Netsim – Network Simulator", [Online]. Available from: http://www.boson.com/netsim-cisco-network-simulator [Retrieved: April 2014].

[12] J. Harry, "Using the GNS3 Network Simulator", [Online]. Available from: http://www.trainsignal.com/blog/using-gns3-network-simulator [Retrieved: April 2014].

[13] Wireshark, "Wireshark", [Online]. Available from: http://www.wireshark.org/ [Retrieved: April 2014].

[14] GNS3, "Introduction to GNS3", [Online]. Available from: http://www.gns3.net/documentation/gns3/introduction-to-gns3/ [Retrieved: April 2014].

[15] GNS3, "Memory and CPU Usage", http://www.gns3.net/documentation/gns3/memory-and-cpu-usage/ [Retrieved: April 2014].

[16] QEMU, "QEMU – Open Source Processor Emulator", [Online]. Available from: http://wiki.qemu.org/ [Retrieved: April 2014].

[17] VirtualBox, "VirtualBox", [Online]. Available from: https://www.virtualbox.org/ [Retrieved: April 2014].

[18] PEMU, "PEMU – Free Cisco PIX Firewall Emulator/Simulator", [Online]. Available from: https://www.fir3net.com/Cisco-PIX [Retrieved: April 2014].

Computing Optimised Result Matrices for the Processing of Objects from Knowledge Resources

Claus-Peter Rückemann
Westfälische Wilhelms-Universität Münster (WWU),
Leibniz Universität Hannover,
North-German Supercomputing Alliance (HLRN), Germany
Email: ruckema@uni-muenster.de

Abstract—**The aim of this paper is to discuss and summarise the main results on computing optimised result matrices from the practical creation of long-term multi-disciplinary and multilingual knowledge resources. Structuring big data is the essential process, which has to preceed creating and implementing algorithms. The knowledge resources implement structure and features and can be integrated most flexibly into information and computing system components. Main elements are so called knowledge objects, which can consist of any content and context documentation and can employ a multitude of means for description and referencing of objects used with computational workflows. Core attributes are a facetted universal classification and various content views and attributes. Developing workflow implementations for various purposes requires to compute result matrices from the objects and referred knowledge, e.g., from geosciences, archaeology, physics, and information technology. The purposes can require individual processing means, complex algorithms, and a base of big data collections. Advanced discovery workflows can easily demand large computational requirements for High End Computing (HEC) resources supporting an efficient implementation. This paper presents some major methodologies and statistics instruments, which have been developed and successfully integrated. The combination of instruments and resources allows to flexibly compute optimised result matrices for discovery processes in information systems, expert and decision making components, search engine algorithms, and fosters the further development of the long-term knowledge resources.**

Keywords–Knowledge Processing; Result Matrix; Optimisation; Computing; Statistics; Classification; UDC; Big Data; High End Computing; Knowledge Resources; Knowledge Discovery.

I. Introduction

Knowledge resources are the basic components in complex integrated systems. Their target is mostly to create a long-term multi-disciplinary knowledge base for various purposes. Request and selection processes result in requirements for computing result matrices from the available information and data. Optimisation in the context of result matrices means "improved for a certain purpose". Here, the certain purpose is given by the target and intention of the application scenario, e.g., requests on search results or associations. Therefore, improving the result matrices is a very multi-fold process and "optimising result matrices" primarily refers to the content and context but in second order also to the workflows and algorithms. The major means presented here contributing to the optimisation are classification and statistics, based on the knowledge resources. The employed knowledge resources can provide any knowledge documentation and additional information on objects and knowledge references, e.g., from natural sciences and decision making. Any data used in case studies is embedded into millions of multi-disciplinary objects, including dynamical and spatial information and data files.

It is necessary to develop logical structures in order to govern the existing unstructured and structured big data today and in future, especially in volume, variability, and velocity and to keep the information addressable on long-term. Preparing and structuring big data is the essential process, which has to preceed creating and implementing algorithms. The systematic, methodological, and "clean" big data knowledge preparation and structuring must generally be named as largest achievement in this context and can be considered by far the most significant overall contribution [1]. The creation and optimisation of respective algorithms is of secondary importance, the more the data must be considered for long-term knowledge creation as, e.g., the benefits of most of those implementations depend on a certain generation of computing and storage architectures, which change all few 4–6 years.

Workflows based on these objects and facilities have been created for different applications. The knowledge resources can make sustainable and vital use of Object Carousels [2] in order to create knowledge object references and modularise the required algorithms [3]. This provides a universal means for improving coverage, e.g., dark data, and quality within the workflow. Secondary resources being available for data, information, and knowledge integration, besides Integrated Information and Computing System (IICS) applications, allow for workflows and intelligent components on High End Computing (HEC) and High Performance Computing (HPC) resources [4], [5]. This paper presents the up-to-date experiences with selected components for structures and workflows.

This paper is organised as follows. Section II introduces the previous work with methodologies and components used, Sections III and IV present the implemented means and statistics fundamentals integrated. Sections V, VI, and VII discuss the implementation environment and evaluate main results, and summarise the lessons learned, conclusions and future work.

II. Methodologies and components employed

The data used here is based on the content and context from the knowledge resources, provided by the LX Foundation Scientific Resources [6], [7]. The LX structure and the classification references based on UDC [8], [9] are essential means

 ISBN: 978-1-61208-365-0

for the processing workflows and evaluation of the knowledge objects and containers. Both provide strong multi-disciplinary and multi-lingual support.

An instructive example for an archaeological and geoscientific use case, deploying knowledge resources, classification, references, and Object Carousels has been recently published [2]. With this research the presentation complements the use case by an important methodology, statistics for intermediate result matrices, usable in any associated workflow. In order to get an overview, the following practical example for a specific workflow as part of an application component shows how result matrices for requests can be computed iteratively.

1) Application component request,
2) Object search (i.e., knowledge objects, classification, references, associations),
3) Creation of intermediate result matrices,
4) Iterative and alternating matrix element creation (i.e., based on intermediate result matrices, object search, referenced content, classification, and statistics),
5) Creation of result matrix,
6) Application component response.

The workflow will mostly be linear if the used algorithms are linear and the data involved is fixed in number and content.

The knowledge objects are under continuous development for more than twenty-five years. The classification information has been added in order to describe the objects with the ongoing research and in order to enable more detailed documentation in a multi-disciplinary and multi-lingual context.

Classification is state-of-the-art with the development of the knowledge resources, which implicitly means that the classification is not created statically or even fixed. It can be used and dynamically modified on the fly, e.g., when required by a discovery workflow description. Representations and references can be handled dynamically with the context of a discovery process. So, the classification can be dynamically modelled with the workflow context. The applied workflows and processing are based on the data and extended features developed for the Gottfried Wilhelm Leibniz resources [10].

Mathematical statistics is a central means for data analysis [11], [12]. It can be of huge benefits when analysing regularities and patterns when used for machine learning with information system components [13]. It is a valuable means deployed in natural sciences and has been integrated in multi-disciplinary humanities-based disciplines, e.g., in archaeology [14]. The span of fields for statistics is not only very broad but statistics itself goes far beyond a simple “tool” status [15].

Methodological means, which have been created in order to be deployed for regular use are workflows improving result quantity and result quality, various filters, universal classifications, statistics applications, manually documented resources' components, integration interfaces for knowledge resources, comparative methods, combination of several means. The methodologies with the knowledge resources are based on computational methods, processing, classification and structuring of multi-disciplinary knowledge, systematic documentation, long-term knowledge creation, vitality of data concepts, sustainable resources architecture, and collaboration frameworks. In the past, many algorithms have been developed and implemented [6], [7] for supporting different targets, e.g., silken criteria, statistics, classification, references and citation evaluation, translation, transliteration, and correction support, regular expression based applications, phonetic analysis support, acronym expansions, data and application assignments, request iteration, centralised and distributed discovery, and automated and manual contributions to the workflow.

A. Structure and classification

The key issues for computing result matrices from knowledge resources are that they require long-term tasks on efficiently structuring and classifying content and context. The classification, which has shown up being most important with complex multi-disciplinary long-term classification with practical simple and advanced applications of knowledge resources is the Universal Decimal Classification (UDC) [16]. According to Wikipedia currently about 150,000 institutions, mostly libraries and institutions handling large amounts of data and information, e.g., the ETH Library (Eidgenössische Technische Hochschule), are using basic UDC classification worldwide [17], e.g., with documentation of their resources, library content, bibliographic purposes on publications and references, for digital and realia objects. Just regarding the library applications UDC is present in more than 144,000 institutions and 130 countries [18]. Further operational areas are author-side content classifications and museum collections.

UDC allows an efficient and effective processing of knowledge data. UDC provides facilities to obtain a universal and systematical view on the classified objects. UDC in combination with statistical methods can be used for analysing knowledge data for many purposes and in a multitude of ways. With the knowledge resources in this research handling 70,000 classes, for 100,000 objects and several millions of referenced data then simple workflows can be linear but the more complex the algorithms get the workflows will mostly become non-linear. They allow interactive use, dynamical communication, computing, decision support, and pre- and postprocessing, e.g., visualisation. The classification deployed for documentation [19] is able to document any object with any relation, structure, and level of detail as well as intelligently selected nearby hits and references. Objects include any media, textual documents, illustrations, photos, maps, videos, sound recordings, as well as realia, physical objects, such as museum objects. UDC is a suitable background classification, for example: The objects use preliminary classifications for multi-disciplinary content. Standardised operations used with UDC are coordination and addition (“+”), consecutive extension (“/”), relation (“:”), order-fixing (“::”), subgrouping (“[]”), non-UDC notation (“*”), alphabetic extension (“A-Z”), besides place, time, nationality, language, form, and characteristics.

B. Statistics implementation for the knowledge resources

A vast range of statistics, e.g., mathematical statistics, can be deployed based on the knowledge resources. The application of mathematical statistics benefits from an increased number of probes or elements. Probes can result from measurements, e.g., from applied natural sciences and from available material. In many cases, without further analysis a distribution or result may seem random. If the accumulation of an occurrence may indicate a regularity or a rule then this may correlate with a statistical method. Many cases require that statistical results have to be verified for realness. This can be done checking against experience and understanding and using mathematical means, e.g., computing probabilities based on probes.

Statistics have been used for steering the development of the resources. Classification and keyword statistics support the optimisation of the quality of data within the knowledge resources. Counts of terms, references, homophones, synonyms and many more support the improvement of the discovery workflows. Comparisons of content with different language representations increase the intermediate associated result matrices for a discovery process. The created knowledge resources' architecture is very flexible and efficient because the components allow a natural integration of multi-disciplinary knowledge. The processes of optimising a result matrix differ from a statistical optimisation by the fact that statistics is only one of the factors within the workflows.

III. Implemented knowledge resources' means

The goals for the combination of statistics and classification are, for example:

- Creating and improving result matrices.
- Decision making within workflows.
- Further development of knowledge resources.
- Extrapolation and prediction.

The implementation for the required flexible workflow creation and levels is shown in the following sketch (Figure 1).

Workflow
Sub-workflow . . . Sub-workflow
Sub-subworkflow . . . Sub-subworkflow
[. . . any level . . .]
Algorithm . . . Algorithm
Resources interface . . .

Figure 1. Workflow-algorithm sketch of the implementation.

The architecture is non-hierarchical. Any workflows can be applied in chains. Each workflow can use sub-workflows, these can use sub-subworkflows and so on. Each workflow can call or implement algorithms, e.g., for discovery processes, evaluation, and statistics. The workflows and algorithms can use or implement interfaces to the resources. The ellipses indicate that any step can be called or executed in parallel on HEC resources, e.g., in data-parallel or task-parallel processes, in any number of required instances.

An example for this is a "multi-probe parallelised optimisation" workflow, which generates an intermediate result matrix and uses the elements in order to create additional results, all of which are combined for an overall optimised result matrix. The intermediate result matrices are deploying statistical, numerical methods, and various algorithms on base of additional knowledge and information resources.

As implementations of statistics are based on counting and numbers the statistics sub-workflows can deploy everything, e.g., any feature or attributes, which can be counted. Sources and means of statistics and computation are:

- Dynamical statistics on the internal and external content and context (e.g., overall statistics, keyword-, categories-, classification-, and media-statistics).
- Mathematics and formula on statistics from the content.
- Elements' statistics (structuring, content, references).
- Statistics based on UDC classification.
- UDC-based statistics computed from comparisons and associations of UDC groups and descriptions.
- Statistics based on any combination of classification, keywords, content, references, context, and computation.

Workflows based on the statistics can be type "semi-manually" or "automated". Besides the major processing and optimisation goals descriptive statistics can be done with each workflow or sub-workflow. Any change of the means supported within a workflow can contribute to the optimisation of the result matrix. Suitable and appropriate means have to be determined for best supporting the goals of the respective step in the workflow. The implementation considers measuring the optimisation by quantity and quality of attributes and features, on intelligence-based and learning processes. With either use there is no general quality measure. Possible quality measures depend on purpose, view, and deployed means. In addition, the decision on these measures can be well supported by statistics, e.g., comparing result matrices from different workflows on the same request. Learning systems components can be used for capturing the success of different measures. The knowledge resources can contain equations and formulary of any grade of complexity. Due to the very high complexity level of the multi-disciplinary components it is necessary to use the basic instances for a comparison in this context of matrix statistics.

The following passages show basic excerpts of statistics objects (LaTeX representation) being part of the implemented knowledge resources. These statistics methods/equations are selected and shown mainly for two reasons: The selected methods are taken from the knowledge objects contained in the resources. These methods are used for result matrix calculations and compared with the evaluation in this research.

IV. Statistics: Fundamentals and application

Statistics on itself can rarely give an overall decisive answer on a question. Statistic means merely can be used as tools for supporting valuations and decisions. Statistics, probability, and distributions are valuable auxiliaries within workflows and integrated application components, e.g., on numbers of objects, spatial or georeferences, phonetic variations, and series of measurement values. Probability and statistics measures are used with integrated applications, e.g., with search requests, with seismic components (e.g., Median and Mean Stacks), which can also be implemented on base of the resources.

 ISBN: 978-1-61208-365-0

A. Basic algorithms applied with knowledge resources

The mean value, arithmetic mean or average M for n values is given by

$$M = \frac{1}{n}\sum_{\nu=1}^{n} x_\nu \tag{1}$$

Calculating the mean value is described by a linear operation. The median value or central value is the middle value in a size-depending sort order of a number of values. For making a statement on the extent of a group of values, the variance ("scattering") can be calculated, with the mean deviation m and the squared mean deviation m^2.

$$m^2 = \frac{1}{n}\sum_{\nu=1}^{n}(x_\nu - M)^2 = \overline{(x-M)^2} \tag{2}$$

For any value this holds $m^2(A) = m^2 + (M - A)^2$ When applying statistics, especially when calculating the propagated error, the following definition of the variance is used:

$$m^2 = \frac{1}{n-1}\sum_{\nu=1}^{n}(x_\nu - M)^2 \tag{3}$$

The mean deviation $\zeta(A)$ is defined as:

$$\zeta(A) = \overline{|x-A|} \text{ for which holds } \zeta(A) = \text{min. for } A = Z \tag{4}$$

The probable deviation or probable error ρ with the probable limits Q_1 and Q_3 is defined as:

$$\rho = \frac{Q_3 - Q_1}{2} \tag{5}$$

The relative frequency h_i is defined as:

$$h_i = \frac{n_i}{n}, \text{ then it holds } \sum_{i=1}^{k} h_i = 1 \tag{6}$$

where n_i is the class frequency, which means the number of elements in a class of which the middle element is x_i.

B. Distributions deployed with knowledge resources

A continuous summation results in the cumulative frequency distribution

$$H_i = \sum_{j=1}^{i} h_j \tag{7}$$

which gives the relative number for which holds $x \leq x_i \cdot H_i$ is a function discretly increasing from 0 to 1. The presentation results in a summation line. With steady variables, for which at an interval width of Δx the quotient $h_i/\Delta x$ nears a limit, one can calculate a frequency density $h(x_i)$ and for the summation frequency $H(x)$:

$$h(x_i) = \lim_{\Delta x \to 0}\frac{h_i}{\Delta x} \quad \text{and} \quad \frac{dH(x)}{dx} = h(x) \tag{8}$$

With statistical distributions the Gaussian normal distribution is of basic importance.

$$h(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}x^2} \tag{9}$$

$H(x)$ can not be given "closed". It can be shown that

$$K = \int_{-\infty}^{+\infty} h(x)dx = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{+\infty} e^{-\frac{1}{2}x^2}\, dx = 1 \tag{10}$$

The Binominal distribution $w_k(s)$ is defined by

$$w_k(s) = \binom{k}{s} p^s q^{k-s} \tag{11}$$

The sum of the two binominal coefficients is equal to $\binom{k+1}{s}$. This is described by Pascals' Triangle. It holds:

$$M = \sum_{s=0}^{k} w_k(s)\cdot s = kp \quad \text{and} \quad m = \sqrt{kqp} \tag{12}$$

Accordingly, the mean error of the mean value decreases proportional to $1/\sqrt{k}$. This describes the error propagation law.

$$h(X) = \frac{1}{\sqrt{2\pi}m} e^{-\frac{1}{2}\left(\frac{X-M}{m}\right)^2} \quad \text{for } -\infty < X < +\infty \tag{13}$$

From this Gaussian curves, binominal distributions, correlation coefficients and advanced measures can be developed.

C. Application of fundamental theorems of probability

The probability p is defined by:

$$p(x_i) = \lim_{n\to\infty} h_i = \lim_{n\to\infty}\frac{n_i}{n} \tag{14}$$

The classical definition of p_{classic} is:

$$p_{\text{classic}} = \frac{\text{number of favoured cases}}{\text{number of possible cases}} \tag{15}$$

The following can be said if independence is supposed. $\vee$ means the logical OR, $\wedge$ the logical AND.
Either-OR: If $E_1, E_2, \ldots, E_m$ are events excluding each other and the respective probabilities are $p_1, p_2, \ldots, p_m$, then the probability for *either* E_1 *OR* E_2 *OR* ... *OR* E_m is:

$$p(E_1 \vee E_2 \vee \ldots \vee E_m) = p_1 + p_2 + \ldots + p_m \tag{16}$$

As-well-as: If $E_1, E_2, \ldots, E_m$ are event pairwise independent from each other then the probability of E_1 *as well as* E_2 *as well as* ... *as well as* E_m is:

$$p(E_1 \wedge E_2 \wedge \ldots \wedge E_m) = p_1 \cdot p_2 \cdot \ldots \cdot p_m \tag{17}$$

 ISBN: 978-1-61208-365-0

V. Implementation for the Result Matrix Cases

A. Measures for optimisation and purposes

The measures for optimisation are on the one hand object of the services and workflows but on the other hand they can be of concern for the knowledge resources themselves.

Conforming with the goals, measures for optimisation mean fitness for a purpose, e.g., search for a regularity with statistics and result matrices. After a search for regularities any statistical procedure benefits from checking against experiences and associating the procedure and result with a meaning. In many cases, e.g., "relevance" means numbers, uniqueness, proximity for objects, content, and attributes, e.g., terms.

Optimisation can be achieved by various means, e.g., by intelligent selection, by self-learning based optimisation, and by comparisons and statistics. The first measures include manual procedures and essences of results being stored for learning processes. They can also deploy comparisons and statistics, which also mean probability and distributions. This case study is focussed on comparisons and statistics applied with the knowledge resources. The subject of the statistics deals with the collection, description, presentation, and interpretation of data. Especially, the methodology can be based on computing more than the minimal number of comparisons, computing more than the minimal number of distributions, computing result matrices considering the mean of several distributions or extreme distributions. In the case of "relevance", information on weighting may come from sources of different qualities.

The general steps with the knowledge resources, including external sources, can be summarised as: Knowledge resource requests, integrating search engine results (e.g., Google), integrating results more or less randomly, without explicit considerate classification and correlation between content and request, comparing the content of search result matrix elements with the knowledge resources result matrix containing classified elements, statistics on an accumulation of terms, selecting accumulated terms, elimination of less concentrated results, selecting the appropriate number of search results.

B. Sources and Structure: Knowledge resources

The full content, structure, and classification of the knowledge resources have been used. In the context of the case discussed here, the sources, which have been integrated and referenced with the knowledge resources consist of:

- Classical natural sciences data sources.
- Environmental and climatological information.
- Geological and volcanological information.
- Natural and man-made factor/event information.
- Data sets and compilations from natural sciences.
- Archaeological and historical information.
- Archive objects references to realia objects.
- Photo and video objects.
- Dynamical and non-dynamical computation of content.

The sources consist of primary and secondary data and are used for workflows, as far as content or references are accessible and policies, licenses, and data security do not restrict.

C. Classification and statistics in this sample case

Table I shows a small excerpt of resulting main UDC classification references practically used for the statistics with the knowledge resources in the example case presented here.

Table I. Universal Decimal Classification of statistics features with the knowledge resources (excerpt).

UDC Code	*Description*
UDC:3	Social Sciences
UDC:310	Demography. Sociology. Statistics
UDC:311	Statistics as a science. Statistical theory
UDC:311.1	Fundamentals, bases of statistics
UDC:311.21	Statistical research
UDC:311.3	General organization of statistics. Official statistics
UDC:5	Mathematics. Natural sciences
UDC:519.2	Probability. Mathematical Statistics
UDC:531.19	Statistical mechanics
UDC:570.087.1	Biometry. Statistical study and treatment of biological data
UDC:615.036	Clinical results. Statistics etc.

The small unsorted excerpts of the knowledge resources objects only refer to main UDC-based classes, which for this part of the publication are taken from the Multilingual Universal Decimal Classification Summary (UDCC Publication No. 088) [8] released by the UDC Consortium under the Creative Commons Attribution Share Alike 3.0 license [20] (first release 2009, subsequent update 2012).

As with any object the statistics features can be combined for facets and views for any classification subject. On the other hand statistics objects from the resources can be selected and applied. The listing (Figure 2) shows an excerpt intermediate object result matrix on statistics content.

```
ANOVA        [Statistics, ...]:
             Analysis of Variance.
BIWS         [Whaling]:
             Bureau of International Whaling Statistic.
GSP          [Geophysics]:
             Geophysical Statistics Project.
Median       [Statistics]:
             In the middle line.
             s. also Median-Stack
Median-Stack [Seismics]:
             Stacking based on the median value of
              adjacent traces.
MSWD         [Mathematics]:
             Mean Square Weighted Deviation.
MSA          [Abbbreviation, GIS]:
             Metropolitan Statistical Area.
MOS          [Abbreviation]:
             Model Output Statistics.
MCDM         [GIS, GDI, Statistics, ...]:
             Multi-Criteria Decision Making.
SHIPS        [Meteorology]:
             Statistical Hurricane Intensity Prediction
              Scheme.
SAND         [Abbreviation]:
             Statistical Analysis of Natural resource
              Data, Norway.
```

Figure 2. Intermediate object result matrix on "statistics" content.

Learning from this: The classifications used for this intermediate matrix are based on contributions from more than one discipline. The elements themselves do not necessarily have to contain a requested term because the classification contributes. Several steps may be necessary in order to improve the matrix, e.g., selecting disciplines, time intervals on the entries, references, and associations. Because different content carries different attributes and features the evaluation can be used in comparative as well as in complementary context.

The implemented knowledge resources means of statistics and computation described above are integrated in the workflows, including classification, dating, and localisation of objects. In addition, probability distributions, linear and non-linear modelling, and other supportive tools are used within the workflow components.

D. Resulting numbers on processing and computing

The processing and computational demands per workflow instance result from the implementation scenarios. The following comparison (Table II) results from a minimal workflow request for a result matrix compared to a workflow request for a result matrix supporting classification views referring to UDC, supporting references and statistics on intermediate results. Both scenarios are based on the same number of elements and entries and can be considered atomic instances in a larger workflow. Views and result matrices can be created manually and automated in interactive and batch operation.

TABLE II. PROCESSING AND COMPUTATIONAL DEMANDS: 2 SCENARIOS, BASED ON 50000 OBJECT ELEMENTS AND 10 RESULT MATRIX ENTRIES.

Scenario Workflow Request for Result Matrix	*Value*
"`geosciences archaeology`" (minimal)	
Number of elements	50,000
Number of result matrix entries (defined)	10
Number of workflow operations	15
Wall time on one core	14 s
"`geosciences archaeology`" (UDC, references, statistics)	
Number of elements	50,000
Number of result matrix entries (defined)	10
Number of workflow operations	6,500
Wall time on one core	6,700 s

As the discussed scenarios are instances this means workflows based on n of these instances will at least require n-times the time for an execution on the same system. It must be remembered that the parallelisation will have a significant effect when workflows are created based on many of these instances when required in parallel. Without modifying the algorithms of the instances, which mostly means simplifying, the positive parallelisation effect for the workflows can be nearly linear. Besides the large requirements per instance with most workflows there are significant beneficial effects from parallelising even within single instances as soon as the number of comparable tasks based on the instances increases. A typical case where parallelisation within a workflow is favourable is the implementation of an application creating result matrices and being used with many parallel instances, e.g., with providing services. The number of 70,000 elementary UDC classes currently results in 3 million basic elements when only considering multi-lingual entries – without any combinations. With most isolated resources only several thousand combinations are used in practice each. The variety and statistics are mostly deployed for decision processing, increasing quantity, and increasing quality. Many of the above cases require to compute more than one data-workflow set to create a decision. A review and an auditing process are mandatory for mission critical applications. The computational requirements can increase drastically with the computation of multiple workflows. Each workflow will consist of one or more processes, which can contain different configurations and parameters. Therefore, creating a base for an improved result matrix starts with creating several intermediate result matrices. With a ten process workflow, e.g., the possible configurations and parameters can easily lead to computing a reasonable set of thousands to millions of intermediate result matrices.

The objects and methods used can be long-term documented as knowledge objects. Nevertheless, there is explicitely no demand for a certain programming language. Even multiple implementations can be done with any object. The workflows and algorithms with the cases discussed here have been implemented as objects in Fortran, Perl, and Shell. Anyhow, the implementation of algorithms is explicitely not part of any core resources. It is the task of anyone having an application to do this and to decide on the appropriate means and methods.

VI. CASE RESULTS AND EVALUATION

Computing result matrices is an arbitrary complex task, which can depend on various factors. Applying statistics and classification to knowledge resources has successfully provided excellent solutions, which can be used for optimising result matrices in context of natural sciences, e.g., geosciences, archaeology, volcanology or with spatial disciplines, as well as for universal knowledge. The method and application types used for optimisation imply some general characteristics when putting discovery workflows into practice regarding components like terms, media, and other context (Table III).

TABLE III. RESULTING PER-INSTANCE-CALLS FOR METHOD AND APPLICATION TYPES ON OPTIMISATION WITH KNOWLEDGE DISCOVERY.

Type	*Terms*	*Media*	*Workflow*	*Algorithm*	*Combination*
Mean	500	20	20	50,000	3,000
Median	10	5	2	5,000	50
Deviation	30	5	5	200	20
Distribution	90	40	15	20	120
Correlation	15	10	5	20	90
Probability	140	15	20	50	150
Phonetics	50	5	10	20	50
Regular expr.	920	100	50	40	1,500
References	720	120	30	5	900
Association	610	60	10	5	420
UDC	530	120	20	5	660
Keywords	820	100	10	5	600
Translations	245	20	5	5	650
Corrections	60	10	5	5	150
External res.	40	30	5	5	40

Statistics methods have shown to be an important means for successfully optimising result matrices. The most widely implemented methods for the creation of result matrices are intermediate result matrices based on regular expressions and

 ISBN: 978-1-61208-365-0

intermediate result matrices based on combined regular expressions, classification, and statistics, giving their numbers special weight. Based on these per-instance numbers this results in demanding requirements for complex applications – On numerical data: Millions of calls are done per algorithm and dataset, hundreds in parallel/compact numeric routines. On "terms": Hundred thousands of calls are done per sub-workflow, thousands in parallel/complex routines, are done.

Most resources are used for one application scenario only. Only 5–10 percent overlap between disciplines – due to mostly isolated use. Large benefits result from multi-disciplinary multi-lingual integration. The multi-lingual application adds an additional dimension to the knowledge matrix, which can be used by most discovery processes. As this implemented dimension is of very high quality the matrix space can benefit vastly from content and references.

VII. Conclusion and Future Work

A number of structuring elements and workflow procedures have been successfully implemented for processing objects from knowledge resources, which allow optimising result matrices in very flexible ways.

First, long-term multi-disciplinary and multi-lingual knowledge resources can provide a solid source of structured content and references for a wealth of result matrices. The long-term results confirm that for the usability the organisation of the content and the data structures are most important and should have the overall focus compared to algorithm adaptation and optimisation. Nevertheless, the computational requirements may be very high but compared against the long-term data creation issues, they should be regarded secondary from the scientific point of view.

Second, employing a classification like UDC has shown to be a universal and most flexible solution with statistics for supporting long-term multi-disciplinary knowledge resources.

Third, computing optimised result matrices from objects of universally classified knowledge resources can be efficiently supported by various statistics and probability measures. With the quality and quantity of matrix elements this can also improve the decision making processes within the workflows.

The research conducted provided that advanced discovery will have to go into depth as well as into broad surface of the context of the multi-disciplinary and multi-lingual information in order to effectively improve the quality for most workflows. Many of these workflow processes can be very well parallelised on HEC resources. A typical case where parallelisation is required is the implementation of an application creating result matrices and used with many parallel instances. This introduces benefits for the applicability of the discovery facing big data resources to be included. The integration of the above strategies and means has proven an excellent method for computing optimised result matrices. Future work will be focussed on the workflow processes and standardisation and best practice for container and resources' objects.

Acknowledgements

We are grateful to all national and international partners in the GEXI cooperations for their support and contributions. Special thanks go to the scientific colleagues at the Gottfried Wilhelm Leibniz Bibliothek (GWLB) Hannover, especially Dr. Friedrich Hülsmann, for prolific discussion, inspiration, and practical case studies.

References

[1] A. Woodie, "Forget the Algorithms and Start Cleaning Your Data," Datanami, 2014, March 26, 2014, URL: http://www.datanami.com/datanami/2014-03-26/forget_the_algorithms_and_start_cleaning_your_data.html [accessed: 2014-04-03].

[2] C.-P. Rückemann, "Sustainable Knowledge Resources Supporting Scientific Supercomputing for Archaeological and Geoscientific Information Systems," in Proc. Third INFOCOMP 2013, Nov. 17–22, 2013, Lisbon, Portugal, 2013, pp. 55–60, ISSN: 2308-3484, ISBN: 978-1-61208-310-0.

[3] C.-P. Rückemann, "High End Computing for Diffraction Amplitudes," in Proceedings ICNAAM 2013, Rhodes, Greece, vol. 1558. AIP Press, 2013, pp. 305–308, ISBN: 978-0-7354-1184-5, ISSN: 0094-243X, DOI: 10.1063/1.4825483.

[4] U. Inden, D. T. Meridou, M.-E. C. Papadopoulou, A.-C. G. Anadiotis, and C.-P. Rückemann, "Complex Landscapes of Risk in Operations Systems Aspects of Processing and Modelling," in Proc. Third INFOCOMP 2013, Nov. 17–22, 2013, Lisbon, Portugal, 2013, pp. 99–104, ISSN: 2308-3484, ISBN: 978-1-61208-310-0.

[5] P. Leitão, U. Inden, and C.-P. Rückemann, "Parallelising Multi-agent Systems for High Performance Computing," in Proc. Third INFOCOMP 2013, Nov. 17–22, 2013, Lisbon, Portugal, 2013, pp. 1–6, ISSN: 2308-3484, ISBN: 978-1-61208-310-0.

[6] "LX-Project," 2014, URL: http://www.user.uni-hannover.de/cpr/x/rprojs/en/#LX (Information) [accessed: 2014-01-12].

[7] C.-P. Rückemann, "Enabling Dynamical Use of Integrated Systems and Scientific Supercomputing Resources for Archaeological Information Systems," in Proc. INFOCOMP 2012, Oct. 21–26, 2012, Venice, Italy, 2012, pp. 36–41, ISBN: 978-1-61208-226-4.

[8] "Multilingual Universal Decimal Classification Summary," 2012, UDC Consortium, 2012, Web resource, v. 1.1. The Hague: UDC Consortium (UDCC Publication No. 088), URL: http://www.udcc.org/udcsummary/php/index.php [accessed: 2014-01-12].

[9] "UDC Online," 2014, http://www.udc-hub.com/ [acc.: 2014-01-12].

[10] C.-P. Rückemann, "Archaeological and Geoscientific Objects used with Integrated Systems and Scientific Supercomputing Resources," International Journal on Advances in Systems and Measurements, vol. 6, no. 1&2, 2013, pp. 200–213, ISSN: 1942-261x.

[11] Y. Dodge, The Oxford Dictionary of Statistical Terms. Oxford University Press, 2006, ISBN: 0-19-920613-9.

[12] B. S. Everitt, The Cambridge Dictionary of Statistics, 3rd ed. Cambridge University Press, Cambridge, 2006, ISBN: 0-521-69027-7.

[13] C. M. Bishop, Pattern Recognition and Machine Learning. Springer, 2006, ISBN: 0-387-31073-8.

[14] R. D. Drennan, Statistics in Archaeology, 2008, in: Pearsall, Deborah M. (ed.), Encyclopedia of Archaeology, pp. 2093-2100, Elsevier Inc., ISBN: 978-0-12-373962-9.

[15] D. Lindley, "The Philosophy of Statistics," Journal of the Royal Statistical Society, 2000, JSTOR 2681060, Series D 49 (3), pp. 293–337, DOI: 10.1111/1467-9884.00238.

[16] "Universal Decimal Classification Consortium (UDCC)," 2014, URL: http://www.udcc.org [accessed: 2014-01-12].

[17] "Universal Decimal Classification (UDC)," 2014, Wikipedia, URL: http://en.wikipedia.org/wiki/Universal_Decimal_Classification [accessed: 2014-01-12].

[18] A. Slavic, "UDC libraries in the world - 2012 study," universaldecimalclassification.blogspot.de, 2012, Monday, 20 August 2012, URL: http://universaldecimalclassification.blogspot.de/2012/08/udc-libraries-in-world-2012-study.html [accessed: 2014-01-12].

[19] C.-P. Rückemann, "Integrating Information Systems and Scientific Computing," International Journal on Advances in Systems and Measurements, vol. 5, no. 3&4, 2012, pp. 113–127, ISSN: 1942-261x.

[20] "Creative Commons Attribution Share Alike 3.0 license," 2012, URL: http://creativecommons.org/licenses/by-sa/3.0/ [accessed: 2014-01-12].

Research on Classification of Fiber Intrusion Signal Based on Supported Vector Machines

Jie Zhu
Department of Electronic Engineering
Shanghai Jiao Tong University
Shanghai, China, 200240
zhujie@sjtu.edu.cn

***Abstract*—The widely use of optical fiber gives rise to the need of its protection and intrusion detection. An optical fiber system in which the optical path satisfies the structure of sagnac loop can easily form a distributed fiber senor. With the photo-elastic effect, when intrusion happens, there will be optical signals created in the fiber, and with optical and electrical methods, one can get the intrusion related signals for analysis. After obtaining the signals, we use differential phrase demodulation method to demodulate the signals. With the demodulated signals, the feature vector of the signals can be extracted through time-frequency analysis. Then, supported vector machine (SVM) is used to classify 3 different types of intrusion. For better accuracy of classification, we use wavelet de-noising to do the noise elimination. Field experiments showed that the system is reliable and of good accuracy.**

Keywords-fiber sensor; differential phrase demodulation; supported vector machine; Time-Frequency analysis; wavelet de-noising.

I. INTRODUCTION

Optical fiber now is widely used in our life, such as cable television network, telephone switching network, Internet, and so on. It permits transmission over longer distances and at higher bandwidths than other forms of communication. As it is so widely used, it is vulnerable to different kinds of intrusion. But, with photo-elastic effect, optical fiber can serve as distributed fiber sensor, and this creates convenience for fiber intrusion detection and recognition. By processing the signal given by the "fiber sensor", we can get the information of the intrusion, and then, we are able to classify intrusion with machine learning method. In this paper, *Supported Vector Machine* (SVM) [1] is chosen for classification.

SVM became popular some years ago for solving problems in classification, regression, and novelty detection. Compared with the method of neural network [2] and other machine learning methods, SVM requires less training samples, and this feature meets our requirement in this case.

In order to improve the performance of classification, we focus on the choice of feature vector and noise elimination. In Section IV, 17 features are chosen to form the feature vector after comparison test. In Section V, wavelet de-noising is applied to further enhance accuracy rate of classification

II. METHOD OF SIGNAL ACQUISITION

To perform the fiber intrusion signal recognition, firstly, we should make our optical path satisfy the structure of Sagnac loop [3] just by adding a feedback module and an interference/multiplexing module to our commonly available fiber system. Then, the distributed fiber sensor system is formed as follows:

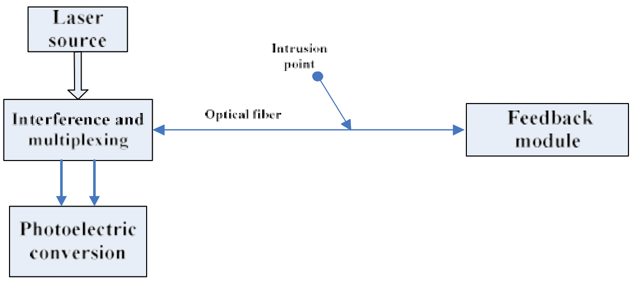


Figure 1. Distributed fiber sensor system.

Once intrusion happens, after photoelectric conversion, we can get the pair of coherent electrical signals $x(t)$, $y(t)$ in the form of (1):

$$\begin{cases} x(t) = A\cos(\Delta\varphi(t) + \alpha) - A\cos\alpha \\ y(t) = B\cos(\Delta\varphi(t) + \beta) - B\cos\beta \end{cases} \quad (1)$$

Here, $\Delta\varphi(t)$is the signal that contains the intrusion information. A and B are amplitude coefficients. The phrases α, β are produced by the interference module [4].

Conduct differential, multiplication, and integration on $x(t)$ and $y(t)$, we get $\Delta\varphi(t)$ with amplitude coefficient $AB\sin(\alpha-\beta)$as follows:

$$AB\sin(\alpha-\beta)\,\Delta\varphi(T) = \int x'(t)*y(t) - x(t)*y'(t) + A\cos\alpha * y(t) - B\cos\beta * x(t) \quad (2)$$

$\Delta\varphi(T)$ is the signal that contains intrusion information, which we desire to obtain.

 ISBN: 978-1-61208-365-0

III. SUPPORTED VECTOR MACHINE

SVM became popular some years ago for solving problems in classification, regression, and novelty detection. It was originally designed for binary classification. In this paper, we use one-against-one method [5] to implement our multiclass classification problem. An SVM learns the decision boundary between two classes by mapping the training sample vectors onto a higher dimensional space, and then, determining an optimal separating hyper-plane [6]-[7], as shown in Figure 2.

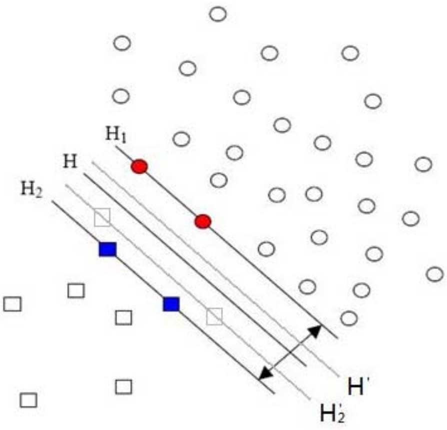


Figure 2. Optimal separation of two linear separable classes by hyper-plane

In Figure 2, "○" represents the class one and the "□" represents the class two. A good choice for classification is the hyper-plane that leaves the maximum margin between the two classes, where the margin is defined as the sum of the distances of the hyper-plane from closest point of the two classes, like the H_1 and H_2 in the above Figure.

Considering the training feature vectors of two classes,

$$(x_i, y_i), x_i \in R^n, y_i \in \{-1, +1\} \tag{3}$$

SVM algorithms will find a pair of parallel optimal hyper-planes, defined as follows:

$$\begin{aligned} H_1 &: y = \boldsymbol{\omega} \cdot \mathbf{x} - b = +1 \\ H_2 &: y = \boldsymbol{\omega} \cdot \mathbf{x} - b = -1 \end{aligned} \tag{4}$$

to separate the two classes, so that the margin, i.e. the distance between two hyper-planes, is the largest. This is the sum of the shortest distance $2/\| \boldsymbol{\omega} \|$ from the hyper-plane to the closest positive and negative examples. The training vectors on the hyper-lanes are called support vectors [8]. The hyper-planes are located by solving the optimization problem:

$$\min \| \boldsymbol{\omega} \|^2 + C \sum \xi_i \tag{5}$$

subject to

$$\begin{aligned} \boldsymbol{\omega} \cdot \mathbf{x} - b &\geq +1 - \xi_i \\ \boldsymbol{\omega} \cdot \mathbf{x} - b &\leq -1 + \xi_i \end{aligned} \tag{6}$$

If $\xi_i = 0$, the two classes are linearly separable and there are no data points between H_1 and H_2. If $\xi_i > 0$, the two classes are not linearly separable; for the data violating the maximum margin condition, a penalty controlled by $C > 0$ is given to balance margin maximization and classification errors. Using Wolfe duality theory [9], the problem can be transformed to the following dual problem:

$$\max \sum_i^N \alpha_i - \frac{1}{2} \sum_{i,j} \alpha_i \alpha_j y_i y_j \boldsymbol{X}_i \cdot \boldsymbol{X}_j \tag{7}$$

subject to

$$\sum_i^N \alpha_i y_i = 0 \tag{8}$$

$$0 \leq \alpha_i \leq \mathrm{C} \tag{9}$$

Therefore:

$$\boldsymbol{\omega} = \sum_i^N \alpha_i y_i \mathbf{X}_i \tag{10}$$

In the case where a linear boundary is inappropriate, the SVM can map the input vector into a high dimensional space through function $\psi(x)$, where it can construct a linear hyper-plane in the high dimensional space, then kernel function can be expressed as

$$k(\boldsymbol{X}_i \boldsymbol{X}_j) = \boldsymbol{\psi}(\boldsymbol{X}_i) \cdot \boldsymbol{\psi}(\boldsymbol{X}_j) \tag{11}$$

That is, the dot product in that high dimensional space is equivalent to a kernel function of the current space [10].

IV. CLASSIFICATION OF INTRUSIONS

In field experiment, three types of intrusion are conducted, namely, Type 1: Excavating with shovel near where the cable is buried, Type 2: Beating directly on the optical fiber with hand, Type 3: Beating the fiber cable with shovel. Examples of the time domain waveforms and spectrums of the 3 types of intrusions are shown as follows (Figure 3, Figure 4, and Figure 5):

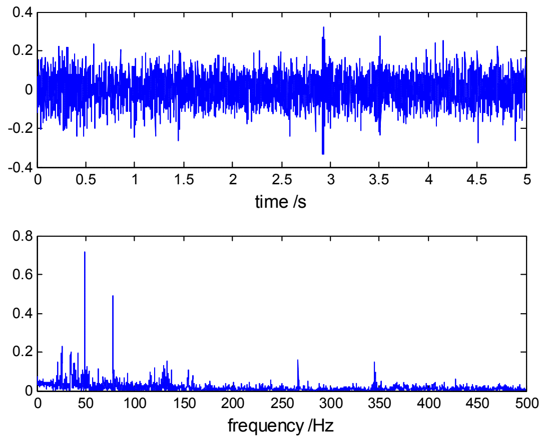


Figure 3. Excavating with shovel (type 1).

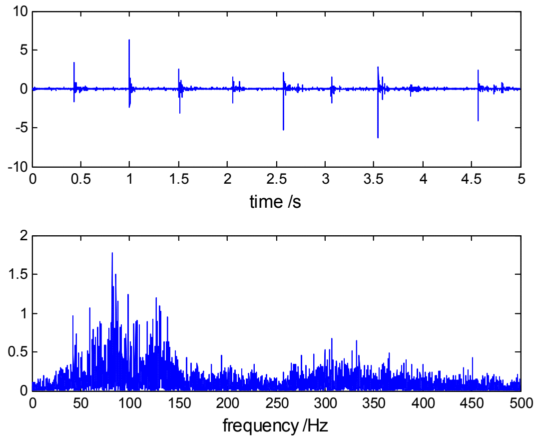


Figure 4. Beating directly on the optical fiber (type 2).

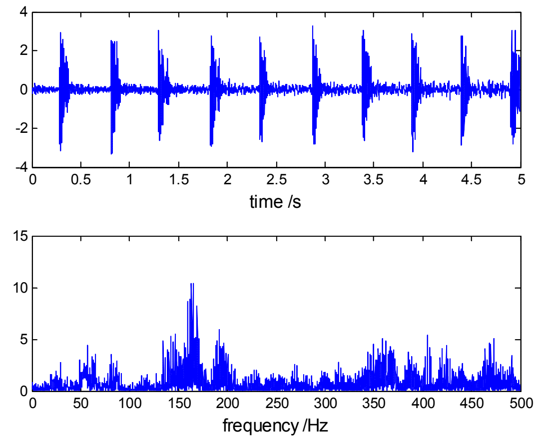


Figure 5. Beating the fiber cable (type 3).

In order to use SVM to do the classification, we must first extract the feature vector. In this paper, we do both time and frequency analysis to get the feature vector suitable for our classification system.

A. Time domain analysis

For every frame of data, in time domain, we compute the following 5 values as components of feature vector.

(1) Maximum value of signal magnitude
(2) Minimum value of signal magnitude
(3) The number of peaks whose height exceed half the maximum magnitude
(4) Average signal magnitude
(5) The ratio of maximum signal magnitude to the average of signal magnitude

B. Power spectrum analysis

For every frame of data, we compute its autocorrelation function, and then, do FFT (Fast Fourier Transformation) to get its power spectrum. We get the following 6 feature values:

(1) The frequency of the highest peak in the power spectrum
(2) The height of the highest peak in the power spectrum
(3) The frequency of the second highest peak in the power spectrum
(4) The height of the second highest peak in the power spectrum
(5) The ratio of the height of the highest and second highest peak in the power spectrum
(6) The number of peaks whose height exceed half the height of the highest peak in the power spectrum

Then, using the energy distribution information we get the following 6 feature values.

(1) The ratio of the energy of the highest peak to the energy of the whole power spectrum
(2) (2)-(6): The ratio of energy in frequency bands 0-99Hz, 100-199Hz, 200-299Hz, 300-399Hz, 400-499Hz respectively to the energy of the whole power spectrum

With the total 17 features, the feature vector can be constructed and used for SVM classification. We use these features to set the optimal parameters C and G in SVM by 10 fold cross-validation and Grid method. In Figure 6, the blue line has the lowest accuracy, 80%, and the red line have the highest accuracy, 93.5%; so, we could select the optimal parameters in the red line. After selecting the optimal parameters, we could get the final accuracy of classification by SVM, like in Figure 7 and Figure 10.

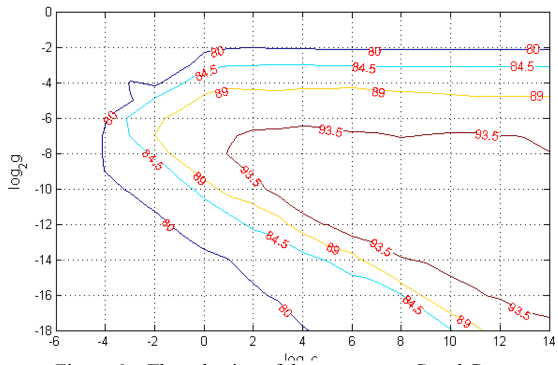


Figure 6. The selection of the parameters C and G

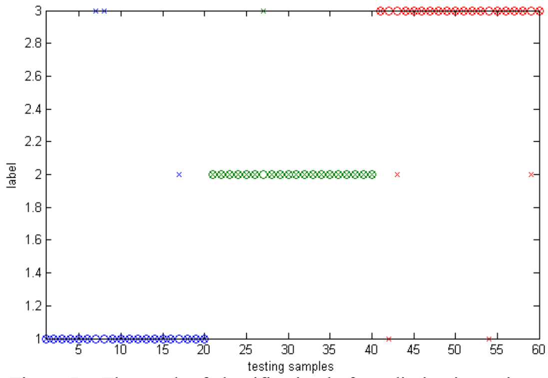


Figure 7. The result of classification before eliminating noise

TABLE I. CLASSIFICATION RESULT

Type 1		Type 2		Type 3	
1	1	2	2	3	3
1	1	3	2	1	3
1	1	2	2	2	3
1	1	2	2	3	1
1	1	2	2	3	3
1	1	2	2	3	3
3	2	3	2	3	3
3	1	2	2	3	3
1	1	2	2	3	2
1	1	2	2	3	3

Figure 7 is result of the classification before eliminating noise, and then, we convert it to be a table as the Table I. In this Figure, “O” is for label of testing samples and “X” is for the prediction label of testing samples. We randomly choose 40 samples from each type of intrusion as training data, and randomly choose 20 samples from the left of each type as testing data. Using one-against-one method to do the multiclass classification, in testing samples of Type 1, there are two misclassifications that mistake Type 1 for Type 3 and one misclassification that mistakes Type 1 for Type 2; in testing samples of Type 2, there are two misclassifications that mistake Type 2 for Type 3; in testing samples of Type 2, there are two misclassifications that mistake Type 3 for Type1 and two misclassifications that mistake Type 3. The accuracy of classification is 85%.

Marking the time domain features as Group 1, power spectrum features as Group 2, and energy distribution features as Group 3, we, respectively, use Group 1, Group 2, Group 3 , Group (1,2), Group (1,3), Group (2,3)’s features to consist the feature vector, and conduct training and testing with the same data set and method as above. The result is shown in Table II:

TABLE II. CLASSIFICATION RESULT

	G1	G2	G3	G1, 2	G1, 3	G2, 3
accuracy(%)	63. 3	78. 3	76. 7	81. 6	80	83. 3

From the result shown in Table Ⅱ, one can see that absence of any group will result in decline of the classification accuracy, so, we use 3 groups together to form the feature vector.

V. WAVELET DE-NOISING

In Section IV, the SVM classification result is not so satisfying and we tried to choose some other time-frequency features to consist the feature vector, but, the improvement is limited. In this situation, de-noising is needed for the improvement of our classification.

In this paper, we adopt the wavelet-based de-noising [11]. Firstly, the wavelet transform performs a correlation analysis; therefore, the output is expected to be maximal when the input signal most resembles the mother wavelet. Secondly, if a signal has its energy concentrated in a small number of wavelet dimensions, its coefficients will be relatively large compared to any other signal or noise that its energy spread over a large number of coefficients. Thirdly, shrinking the wavelet transform will remove the low amplitude noise or undesired signal in the wavelet domain, and an inverse wavelet transform will then retrieve the desired signal with little loss of details.

The noise in the signals $x(t), y(t)$ in (1), that we get after photoelectric conversion, has similar properties as white noise, so, as the most popular method for white noise, de-noising, wavelet de-noising is used in this paper.

We use soft-threshold, choose sym8 in the Symlets family [12], as our wavelet base and do 6 level of decomposition. The choosing of wavelet base and the depth of decomposition level is a compromise between de-noising performance and efficiency [13]. Figure 8 and Figure 9 show the de-noising results of time and frequency domain, respectively.

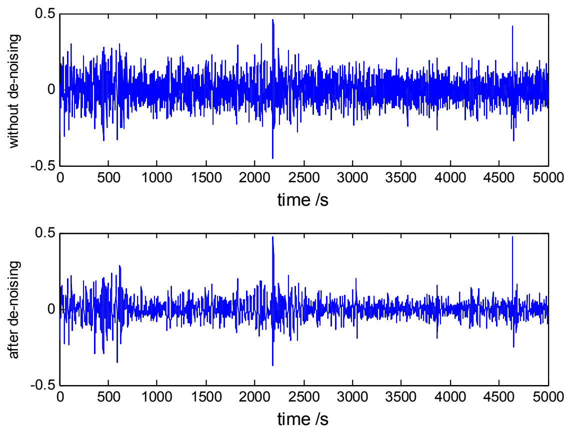


Figure 8. Time domain comparison.

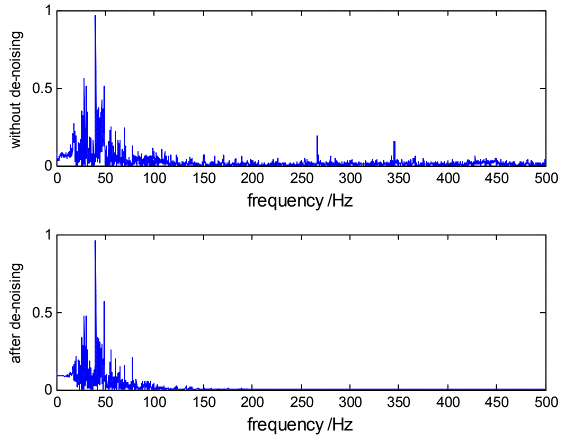


Figure 9. Spectrum comparison.

Using the same feature vector, same training and test data set as in Section IV, we get the following SVM classification result.

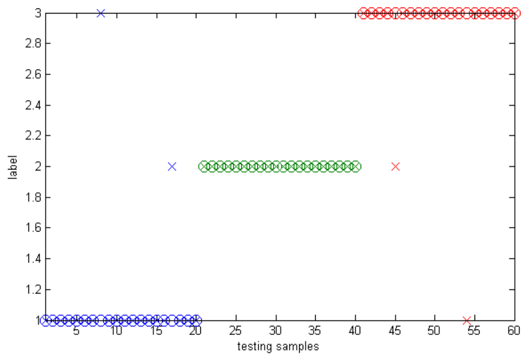


Figure 10. The result of classification after eliminating noise

TABLE III. CLASSIFICATION RESULT WITH DE-NOISING

Type 1		Type 2		Type 3	
1	1	2	2	3	3
1	1	2	2	3	3
1	1	2	2	3	3
1	1	2	2	3	1
1	1	2	2	2	3
1	1	2	2	3	3
1	2	2	2	3	3
3	1	2	2	3	3
1	1	2	2	3	3
1	1	2	2	3	3

Figure 10 is result of the classification after eliminating noise, and then, we convert it to be a table, as the Table III.

In this Figure, “O” is for label of testing samples and “X” is for the prediction label of testing samples. The accuracy of classification reaches 95%. From the comparison of the results of two trials (one with wavelet de-noising and one without), we can see that wavelet de-noising is quite effective for the improvement of classification accuracy.

VI. CONCLUSION AND FUTURE WORK

In this paper, we focused on the improvement of performance of SVM-based fiber intrusion signal recognition system. Three different types of intrusion are experimented, and kinds of time-frequency features are tried to serve as components of feature vector for SVM. Finally, 17 kinds listed in Section IV are chosen. Wavelet de-noising is used to enhance the performance of classification, and the improvement is obvious. Further research is needed to improve the composition of feature vector and find better de-noising methods to make the classification more accurate.

REFERENCES

[1] R.J. Kuo and C.M. Chen, “Evolutionary-Based Support Vector Machine”, Industrial Engineering and Engineering Management (IEEM), 2011, pp. 472-475.

[2] E. Byvatov, U. Fechner, J. Sadowski and G. Schneider, “Comparison of Support Vector Machine and Artificial Neural Network Systems for Drug/Nondrug Classification”, J. Chem. Inf. Comput. Sci., 2003, vol. 43, no. 6, pp. 1882-1889.

[3] A. Owen, G. Duckworth and J. Worsley, “OptaSense: Fibre Optic Distributed Acoustic Sensing for Border Monitoring”, Intelligence and Security Informatics Conference (EISIC), European, 2012, vol. 59, pp. 362-364.

[4] Changyu Shen, Jinlei Chu, Yanfang Lu, et al. “High Sensitive Micro-Displacement Sensor Based on M-Z Interferometer by a Bowknot Type Taper”, Photonics Technology Letters, IEEE, 2014, vol. 26, pp. 62-65.

[5] Chih-Wei Hsu and Chih-Jen Lin, “A comparison of methods for multiclass Support Vector Machines,” IEEE Trans. Neural Networks, vol. 13(2), 2002, pp. 415- 425.

[6] I. Guyon, J. Weston, S. Barnhill, and V. Vapnik, “Gene selection for cancer classification using support vector machines,” Mach. Learn. , Jan. 2002, vol. 47, no. 1-3, pp. 389-422.

[7] C.-H. Li, H.-H. Ho, Y.-L. Liu, B.-C. Kuo, and J.-S. Taur, “An automatic method for selecting the parameter of the normlized kernel function to support vector machines,” *J. Inf. Sci. Eng.*, Jan. 2012, vol. 28, no. 1, pp. 1-15.

[8] A. Pattle and D. S. Chouhan, “SVM kernel function for classification,” Advances in Technology and Engineering (ICATE), 2013, pp. 1-9.

[9] P. Wolfe, “A duality thorem for non-linear programming”, Q. Appl. Math. 19, 1961, pp. 239-244.

[10] Changxue Ma, Randolph, M.A; Drish, J, “Distributed fiber optic acoustic sensor for leak detection,” Proceedings ICASSP-2001, vol. 1, pp. 381-384.

[11] G. Garg, V. Singh, J.R.P. Gupta and A.P. Mittal, “Optimal algorithm for ECG denoising using Discrete Wavelet Transforms”, ICCIC, 2010, pp. 1-4.

[12] V. P. Dimri, N. Vedanti and S. Chattopadhyay, “Fractal analysis of aftershock sequence of the Bhuj earthquake: A wavelet-based approach”, Current Science, May 2005, vol. 88, no. 10.

[13] Tae Hwan Lee and Byung Cheol Song, “De-noising algorithm using sparse 3D transform-domain collaborative filtering and adaptive soft thresholding”, ISCE, 2011, pp. 128-131.

A Constraint-Based Graphical Approach to Modelling Construction Systems:

An alternative to discrete-event simulation

Ian Flood
Rinker School, College of Design, Construction and Planning,
University of Florida,
Gainesville, Florida, USA
flood@ufl.edu

***Abstract* — An essential part of the planning and control of any construction system is the development of a model of the project's key processes. The Critical Path Method (CPM) is the most widely used process modelling method in construction since it is simple to use and reasonably versatile. Most other modelling techniques have limited scope being aimed at specialized types of project. Linear scheduling, for example, provides excellent visual insight into the performance of a system but is limited to modelling construction processes that progress along a line, such as tunnels and highways. Discrete-event simulation is the most versatile of all modelling methods, but it lacks the simplicity in use of CPM and for this reason has not been widely adopted in practice. This paper demonstrates an alternative modelling approach designed to provide the visual insight of linear scheduling, the modelling versatility of simulation, and yet be relatively simple to use and understand. The principles and use of the approach are demonstrated in application to three example construction industry projects.**

Keywords – interactive modeling, discrete-event simulation, process modeling, graphical constraint-based modeling, visualization.

I. INTRODUCTION

The last 100 years has seen the development and application of a wide range of methods for modelling construction processes. An analysis of the genealogy [1] of these tools shows that they can be grouped into three main categories: the Critical Path Methods (CPM); the linear scheduling techniques; and discrete-event process simulation. Most other tools are either an enhancement or an integration of these methods. For example, 4D-CAD and nD-CAD planning methods [2] [3], where one of the dimensions is time, are strictly CPM models hybridized with 3D-CAD for visualization purposes.

Each of the three main groups of modelling method are, unfortunately, only relevant to a restricted range of construction planning problems. The CPM methods (the most popular in construction) are well suited to modelling projects at a relatively general level of detail, but are limited in terms of the types of interactions they can consider between tasks [4]. Moreover, CPM models become cumbersome when used to model repetitive processes, and provide little understanding of the interactions between repetitive tasks. When presented in Gantt Chart format, a CPM model provides some visual insight into how a system's logic affects its performance (thus suggesting more optimal ways of executing work) but this is limited to event-based logical dependencies and their impact on time-wise performance.

Linear scheduling, on the other hand, is targeted at projects where there is repetition at a high level, such as high-rise, tunnelling, and highway construction work (see, for example, Matilla and Abraham [5]). These models are very easy to understand and represent the system's logic and its performance within an integrated framework. Consequently, they provide the modeller with strong visual insight that can help identify more optimal ways of achieving the project's production goals. For example, they show in graphic form how the relative progress of repetitive tasks can lead to conflict, both in terms of time and physical interference between productive resources (such as crews and equipment). However, linear scheduling cannot be used to model non-repetitive work, and it includes some simplistic assumptions which often make it difficult to model real-world repetitive processes. For example, velocity diagrams (a linear scheduling technique) cannot easily represent operations that follow different paths, such as two underground utility lines that interact at a cross-over point but otherwise follow different routes.

Finally, discrete-event simulation (see, for example, Halpin and Woodhead [6]; Sawhney et al. [7]; Hajjar and AbouRizk [8]) is very versatile in that it can in principle model any type of interaction between tasks and any type of construction process (including repetitive and non-repetitive work). However, the effort involved in defining and validating a simulation model means that in practical terms it is best suited to systems that cannot be modelled sufficiently accurately using CPM or linear scheduling. In addition, simulation models provide no direct visual indication of how a system's logic determines its performance. That is, performance is an output from the model after it has been fully developed; it is not an integral

 ISBN: 978-1-61208-365-0

part of the model and therefore its dependence on the model's logic is not directly apparent.

Most projects include a variety of processes some of which may be best modelled using CPM while others may be better represented by linear scheduling or simulation. However, it is not normally practical to expect planners and plan-users to employ more than one modelling method to manage a project. In any case, using several tools that are not fully compatible makes it impossible to seek a globally optimal solution to a planning problem. On the other hand, the alternative approach of using one tool to represent all situations (typically CPM) compromises a user's ability to plan and control work optimally.

Ideally, what is needed is a single tool that is well suited to modelling the broad spectrum of repetitive and non-repetitive construction work, is highly versatile, provides insight into better ways of organizing work, and is easy to use. This paper goes back to basics and proposes a new modelling paradigm, *Foresight*, that addresses the above issues. Section II introduces the principals of the *Foresight* modelling system. Sections III to V provide three case studies demonstrating the application of *Foresight* to construction projects that would otherwise best be modelled using discrete-event simulation: a simple earthmoving operation, a tunnelling operation; and an underground utility laying operation.

II. PRINCIPAL MODELING CONCEPTS OF FORESIGHT

The goal in developing the new approach to modelling was to attain the simplicity of CPM, visual insight of linear scheduling, and the modelling versatility of simulation. In addition, hierarchical structuring of a model (see for example, Huber et al. [9] and Ceric [10]) and interactive development of a model were identified as requisite attributes of the new approach since they facilitate model development and aid understanding of the organization and behaviour of a system.

The three principle concepts of the Foresight modelling approach are as follows and illustrated in Figure 1:

Attribute Space. This is the environment within which the model of the process exists. Each dimension defining this space represents a different attribute involved in the execution of the process, such as time, cost, excavators, skilled labour, number of repetitions of an item of work, permits to perform work, and materials. The attributes that make-up this space are the resources that are used to measure performance and/or that could have a significant impact on performance.

Work Units. These are elements that represent specific items of work that need to be completed as part of the project. They are represented by a bounded region within the attribute space. A unit can represent work at a high level (such as 'Construct Structural System'), a low level (such as 'Erect Column X') or any intermediate level. Collectively, the work units must represent all work of interest but should not represent any item of work more than once. Work units may exist in different subsets of attribute space.

Constraints and Objectives. Constraints define the relationships between the work units and the attribute space, either directly with the attribute space (such as constraint 'a' in Figure 1) or indirectly via relationships with other work units (such as constraints 'b', 'c', and 'd' in Figure 1). These constraints effectively define the location of the edges of the work units. A constraint can be any functional relationship between the borders of the work units and/or the space within which they exist. Practical examples include: (i) ensuring that crews at different work units maintain a safe working distance; (ii) ensuring that the demand for resources never exceeds the number available; (iii) determining the duration for a task based on the number of times it has already been repeated; and (iv) ensuring that idle time for a task is kept to a minimum. The objectives are the specific goals of the planning study, such as to maximize profits or to complete work by a deadline (such as constraint 'd' in Figure 1). Fundamentally, they are the same thing as constraints, albeit at a higher level of significance, and therefore are treated as such within the proposed new modelling system.

There are two secondary concepts of the Foresight modelling system, both concerned with its structure:

Nesting. Work units can be nested within other work units (such as work unit 'D' in Figure 1 which is shown to be within work unit 'C' which is respectively part of 'E'), or overlap with each other (such as work units 'A' and 'B'). Nesting of work units can be defined explicitly, allowing the model to be understood at different levels of abstraction, increasing its readability, reducing the likelihood of errors in the design of the model, and

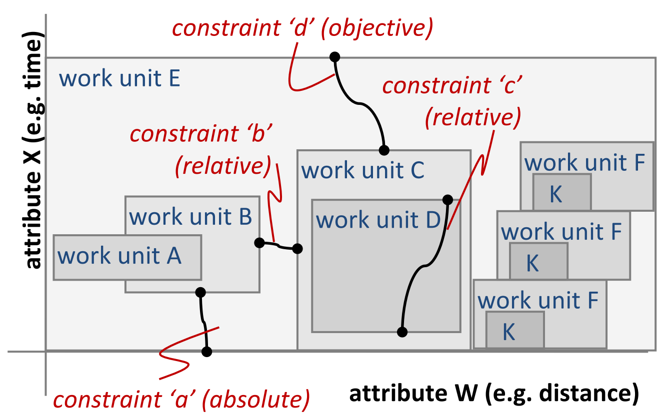


Figure 1. Schematic illustrating the three principal concepts of Foresight.

 ISBN: 978-1-61208-365-0

reducing the amount of work required to define and update a model.

Repetition. Work units can be repeated (such as work unit F in Figure 1) and can be implemented at any level within the nesting hierarchy, thus minimizing the amount of work required to define a model. Repetition of a work unit will include a repetition of all relevant constraints and its nested work units and their constraints.

A specification of *Foresight* is that model development be implemented interactively. That is, the visual presentation of a model is updated and all constraints are resolved as the work units and constraints are either edited or added to the model. This way, the modeller can see immediately the impact of any changes or additions that are made. Another point to note is that these models are presented as a plot of the work units within at least two dimensions of the attribute space. This form of presentation allows the progress of work to be visualized within the model's functional structure. This is an extrapolation of the way in which linear scheduling models are presented, and has the advantage of allowing the user to visualize directly how the performance of the model is dependent on its structure. These points will be illustrated in the following three example applications.

It should be noted that *Foresight* is, strictly speaking, a simulation system in that it requires the use of a three-phase simulation algorithm to resolve its constraints.

III. SIMPLE EARTHMOVING OPERATION

The first system to be modelled is that of a simple earthmoving system comprising an excavator used to load dump trucks. Figure 2 shows a CYCLONE [6] simulation process diagram of this system for a situation where there are three trucks (each of 5 cu-yds capacity), and one excavator (with a 1 cu-yd bucket). The excavator must therefore perform five cycles to load a truck.

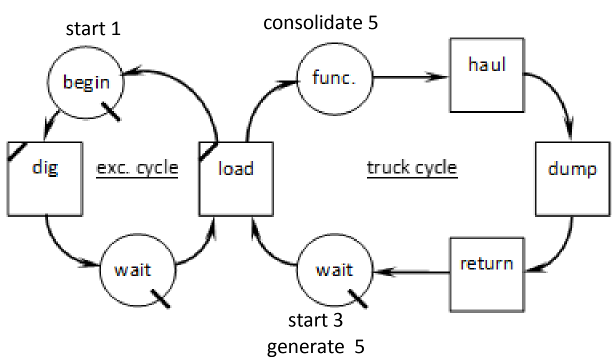


Figure 2. CYCLONE simulation process diagram for a simple earthmoving operation.

This model, once defined within the computer and validated, would be run several times to gain measures of performance of the system, such as production rates and queue length distributions.

The *Foresight* representation of this system is presented in Figure 3. Part (a) of this figure shows the hierarchical form of the model (without the main constraints added) whereas part (b) shows the model in its normal format with all constraints added representing, for example, work unit durations, and precedence. Parts (c) and (d) of Figure 3 show the model using the variables trucks versus time, and excavators versus time respectively. Figure 3(c) only shows the model to the 2nd level in its hierarchy, even though the truck activities go down to the 3rd level, to allow a more generalized understanding of its performance. Likewise, Figure 3(d) shows the activities of the excavator down to the 4th rather than 5th level. These plots effectively show the demand for these productive resources over time, indicating any idle time and thus possible imbalance in the resource combinations. Appropriate statistics concerning these factors can be readily extracted.

Several important differences between CYCLONE and Foresight can be understood by comparing the model representations of Figs. 2 and 3. First, it should be understood that CYCLONE requires the complete logic of the model (as represented by the CYCLONE diagram of Figure 2) to be finalized before the system's performance can be predicted in a simulation run. In contrast, the Foresight model integrates the structure and logic of the model and the estimated performance of the system within a single format (as represented by Figure 3(b)). This gives Foresight a couple of significant advantages. First, as elements are added to the model and its parameters altered, the impact of these edits on the estimated performance of the system are seen immediately - the model does not have to be completed before the simulation results are produced. This is a similar advantage to that seen in other graphically based planning tools such as Linear Scheduling. The second advantage is that in a Foresight model, the way in which the logic and structure of the model affect the performance of the system is directly visible, which in turn assists in the optimization of the design of the system - this point will be illustrated in the next case study of a sewer-tunneling operation.

IV. TUNNELLING OPERATION

The second study is concerned with modelling the construction of a 2 m internal diameter sewer, where tunnelling is through clay and the lining is formed from concrete ring segments. The example is used to illustrate the steps in developing a *Foresight* model for a problem that, given its complexities, should otherwise be modelled using simulation methods.

A component oriented approach should be adopted when developing a *Foresight* model, such that each work unit represents the construction of a physical component or sub-

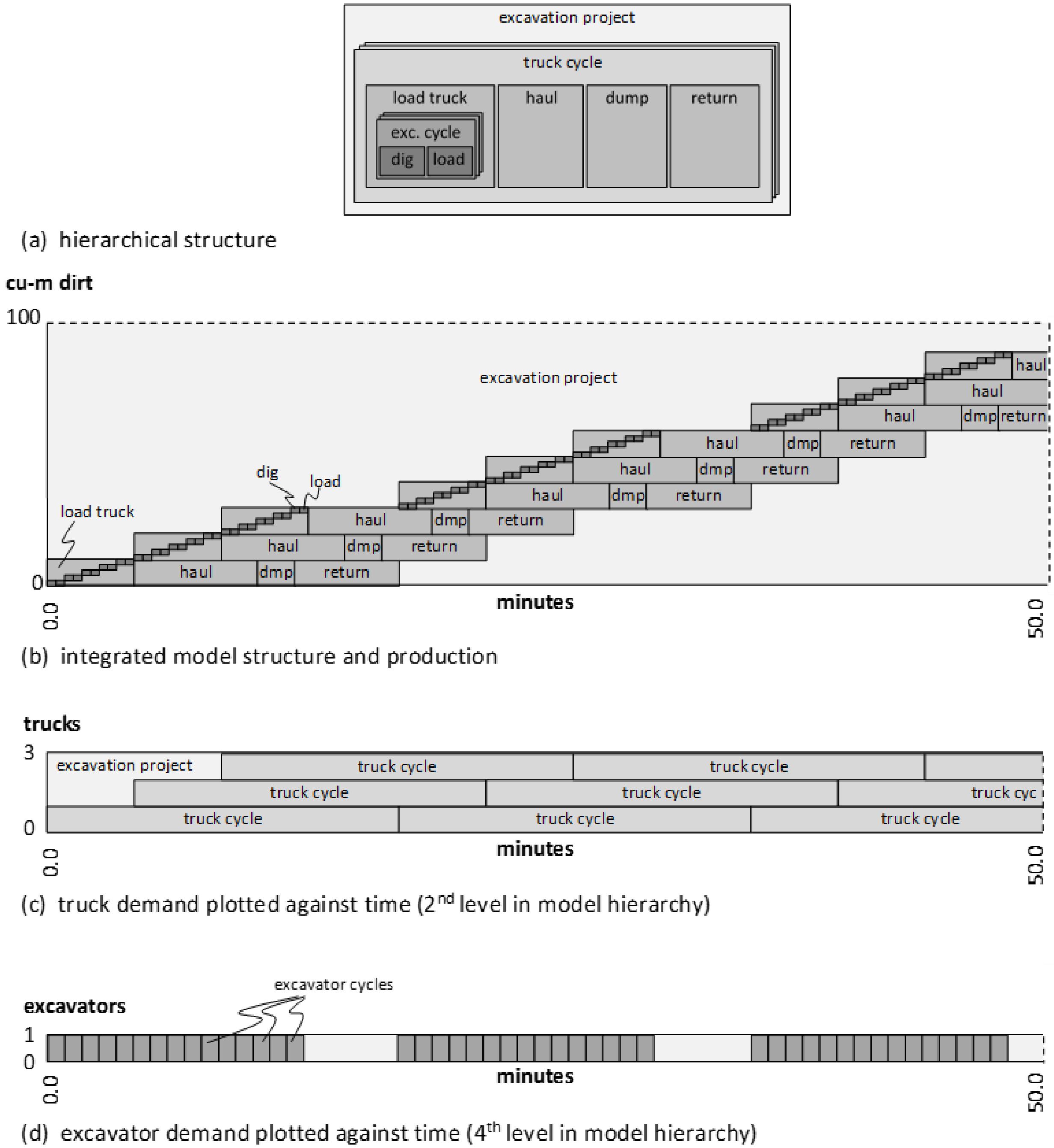


Figure 3. Foresight model of a simple earthmoving operation.

component of the facility under construction. A top-down, hierarchical approach is an effective strategy for developing these models, starting with the highest level component (the complete facility) and then breaking it down into its constituent components. Figure 4 shows the hierarchical structure of the Foresight model of the tunnelling operation. At the lowest level in this breakdown are the work units *Excavation* representing the cutting of 1 m length of the tunnel, and *Concrete Lining* which involves placing and grouting concrete ring segments in the 1 m cut. *Excavating* and *Concrete Lining* are repeated 3 times thereby constructing a 3 m length of tunnel, which is then followed by *Light Track* which lays a 3 m length of track used to carry a manually propelled train for removal of spoil and delivery

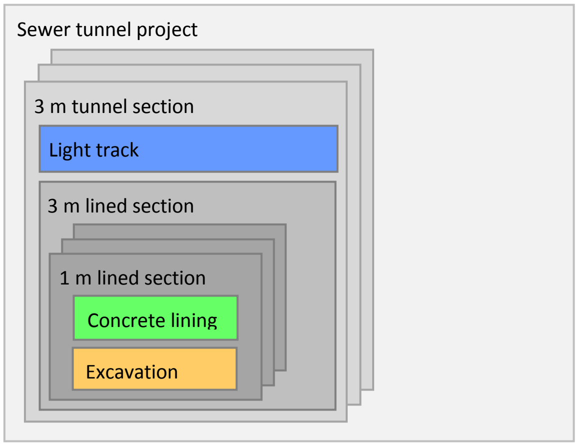


Figure 4. Foresight hierarchical model structure representing a tunneling operation.

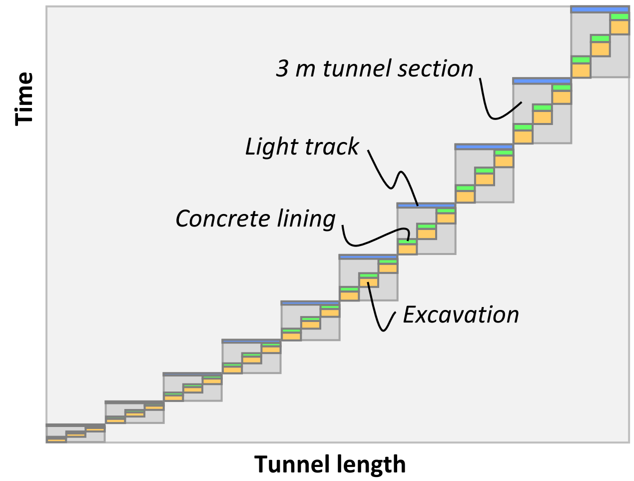


Figure 5. Tunnelling model with constraints added.

of concrete ring segments. If two crews are used for the project then the model shown in Figure 4 would be duplicated (once for each crew) and placed within a parent work unit.

The work unit at the second highest level represents the process of constructing a 3 m section of tunnel, and will be repeated for the length of the tunnel.

Addition of constraints can occur as work units are added to the model. For the tunnel model, the main constraints would be as follows:

- The work units representing *3 m tunnel sections* are positioned serially both in the *Time* and *Tunnel Length* dimensions.
- The work unit representing the *Sewer tunnel project* extends in the *Tunnel Length* direction to a value equal to the tunnel length.
- The *3 m tunnel section* work units start at the left side of the *Sewer tunnel project* work unit and extend all the way to (but not beyond) the right side of the *Sewer tunnel project* work unit.
- The *1 m lined section* work units are positioned serially both in the *Time* and *Tunnel Length* dimensions.
- The *1 m lined section* work units span from the left to right side of their *3 m tunnel section* work unit.
- *Excavation* and *Concrete lining* are positioned sequentially in the *Time* dimension.

Completion of any *Foresight* model requires addition of the constraints. For the tunnelling model, this includes adding functions specifying the individual heights of the *Excavation*, *Concrete lining*, and *Light Track* work units, indicating their respective durations, the result of which is shown in Figure 5. For convenience, only the first 30 m of tunnel construction is shown. Note, the progress of the project follows a curve, which results from the fact that the duration to remove spoil and bring concrete ring segments to the tunnel face increases with tunnel length. Such a dependence can be readily established as a function of the position along the length of the tunnel.

There are many refinements that may be made to this model to provide more accuracy and/or greater detail to allow decisions to be made about equipment types to be employed. Additional detail may involve, for example, further decomposition of the *Excavation*, *Concrete lining* and *Light track* works units. *Excavation* may contain work units representing digging at the tunnel face, loading the light train, hauling the spoil from the tunnel, dumping the spoil, and returning the light train. Other attributes may be added, such as crew members, allowing these to be shared between different work units concurrently.

To illustrate the visual power of these models, consider the problem where two separate crews will be employed for tunnelling, each starting at the same point but heading in opposite directions. If crew-performance records indicate that 1 crew tends to operate about 50% faster than the other then we would want to find a starting location that would minimize the total project duration. If the tunnel was 60 m in length and employed two crews starting at the midpoint, with the slower crew heading to the left and the faster crew heading to the right, then the model would appear as shown in Figure 6. It can be seen from this chart that the faster crew should probably start 3 m or 6 m to the left of the midpoint to minimize the project duration – both choices could be tested quickly. Alternatively, an additional dimension could be added to the model representing starting the crews at different positions along the tunnel length, thus providing an automated sensitivity analysis of project duration versus starting point for the crews.

V. UNDERGROUND UTILITY LAYING OPERATION

A *Foresight* model of an electrical cable laying project, complete with constraints, is shown in Figure 7. The operation is typical of the type of process that would be

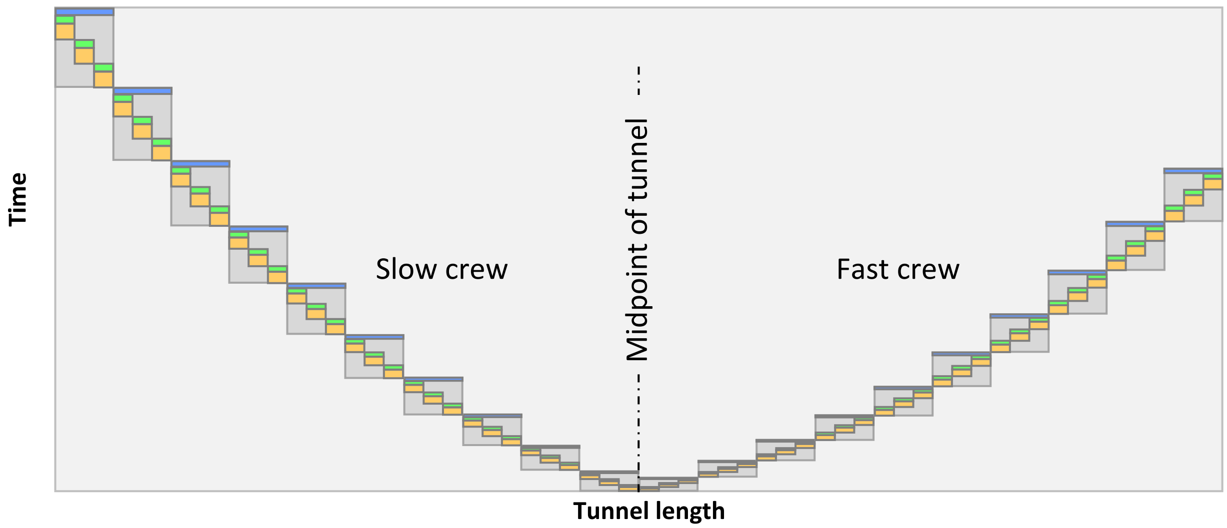


Figure 6. Tunnelling model with two crews starting at centre and heading in opposite directions.

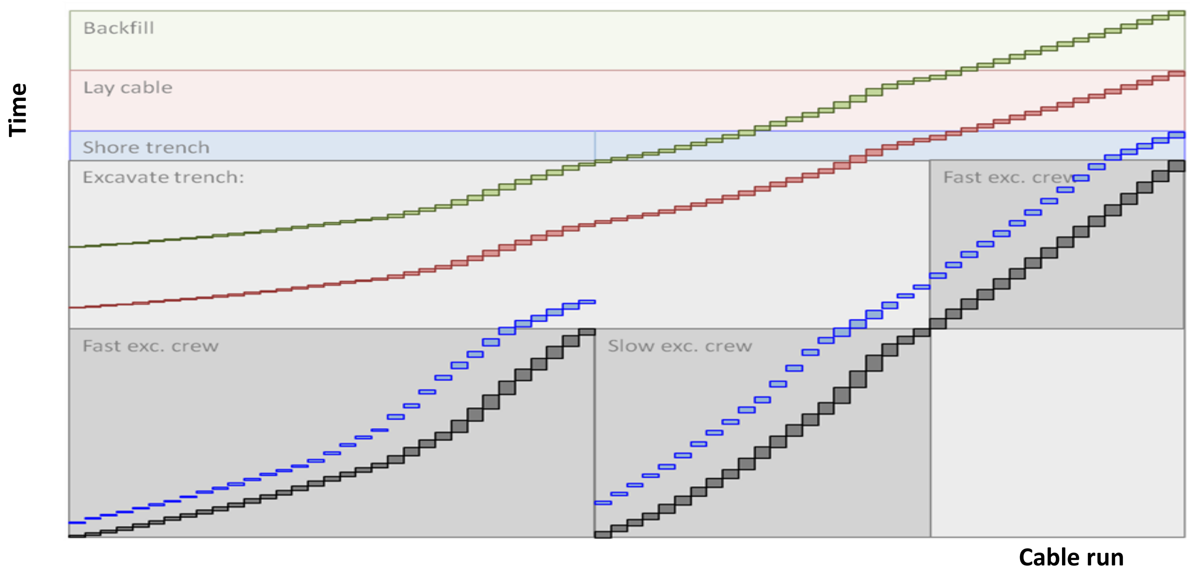


Figure 7. Underground electrical cable laying operation.

modelled using linear scheduling except that it includes some logical features that are beyond conventional linear scheduling methods.

The project comprises four main tasks: *Excavate trench*; *Shore trench*; *Lay Cable*; and *Backfill*, each of which is colour coded. The smaller sized work units represent work on 1 m lengths of the project while the larger work units are essentially summaries of each task. Important feature of this model are:

- There are two crews available for excavation work and two crews available for shoring. The first excavation crew is faster than the second and will leap frog them when they reach their starting point.
- *Shore trench* has two constraints relative to *Excavate trench*, a minimum and a maximum permissible distance. The minimum working distance is for safety and to prevent interference between the crews. The maximum distance is to minimize the chances of the trench collapsing before being shored. In this example, the Shore trench crew must spend some time idle to ensure that the minimum distance constraint is not violated. If they operated considerably slower then the excavation crew would have had to spend time idle to ensure the maximum distance buffer was not violated.
- A constraint is imposed on both *Lay cable* and *Backfill* that prevents gaps between their work units within the model (effectively meaning they cannot spend time

 ISBN: 978-1-61208-365-0

idle). This constraint reduces the amount of time their crews are employed on the project. As a consequence, *Lay cable* and *Backfill* are forced to start later.

VI. Conclusions

In this paper the author has proposed a new approach, named *Foresight*, for modelling construction processes built on concepts relevant to contemporary project planning. The principles upon which *Foresight* is based provide it with the versatility necessary to model the broad spectrum of construction projects that until now have required the use of several different modelling tools. The resultant models are highly visual in form, representing the progress of work within the model structure. This provides insight into how the design of a process will impact its performance, and suggests ways of optimizing project performance.

Research is on-going developing detailed models using this method for a variety of project types. The objective of these studies is to determine the successes and limitations of the proposed planning method in the real-world, and to determine refinements that will increase its value as a modelling tool.

References

[1] I. Flood, R.R.A. Issa, and W. Liu, “A New Modeling Paradigm for Computer-Based Construction Project Planning”, Proc. Joint Intntl. Conf. on Cmptg. and Decision-Making in Civil and Building Engineering, Montreal, Canada, ASCE, June 2006, pp 1-11.

[2] B. Koo and M. Fischer, “Feasibility Study of 4D CAD in Commercial Construction”, Journal of Construction Engineering and Management, ASCE, 126(4), 2000, pp 251-260.

[3] R.A. Issa, I. Flood, and W. O’Brien, (Eds.), 4D CAD and Visualization in Construction: Developments and Applications, A. A. Balkema Publishers, Steenwijk, 2003.

[4] R.B. Harris and P.G. Ioannou, “Scheduling Projects with Repeating Activities”, Journal of Construction Engineering and Management. ASCE, 124(4), 1998, pp 269-276.

[5] K.G. Matilla and D.M. Araham, “Linear-Scheduling: past research efforts and future directions”, Engineering, Construction, and Architectural Management, Blackwell Science Ltd, 5(3), 1998, pp 294-303.

[6] D.W. Halpin and R.W. Woodhead, Design of Construction and Process Operations, John Wiley and Sons, Inc., New York, NY, 1976.

[7] A. Sawhney, S.M. AbouRizk, and D.W. Halpin, “Construction Project Simulation using CYCLONE”, Canadian Journal of Civil Engineering, 25(1), 1998, pp 16-25.

[8] D. Hajjar and S.M. AbouRizk, “Unified Modeling Methodology for Construction Simulation” Journal of Construction Engineering and Management, ASCE, 128(2), 2002, pp 174-185.

[9] P. Huber, K. Jensen, and R.M. Shapiro, "Hierarchies of Coloured Petri Nets", Proc. 10th Int. Conf. on Application and Theory of Petri Nets, (LNCS 483), Springer-Verlag, 1990, pp 313-341S.M.

[10] V. Ceric, “Hierarchical Abilities of Diagrammatic Representations of Discrete-Event Simulation Models”, Proc. 1994 Winter Simulation Conference, (Eds. J. D. Tew, S. Manivannan, D. A, Sadowski, and A. F. Seila), 1994, pp 589-594.

 ISBN: 978-1-61208-365-0