

17<sup>TH</sup> ANNUAL EUROMEDIA CONFERENCE

2012

BUCHAREST, ROMANIA

APRIL 18-20, 2012

Organized by

ETI

University POLITEHNICA of Bucharest

Sponsored by

EUROSIS

LMS

BITE

University of Skovde

Higher Technological Institute  
Tenth of Ramadan City

Ghent University

HOSTED BY

JW Marriott Hotel  
Bucharest, Romania





# **EUROMEDIA'2012**

FEATURING

SEVENTEENTH ANNUAL SCIENTIFIC CONFERENCE  
ON WEB TECHNOLOGY, NEW MEDIA  
COMMUNICATIONS AND TELEMATICS THEORY  
METHODS, TOOLS AND APPLICATIONS

Dan Stefanoui

and

Janetta Culita

APRIL 18-20, 2012  
BUCHAREST, ROMANIA

A Publication of EUROSIS-ETI

Printed in Ghent, Belgium

## **EXECUTIVE EDITOR**

**PHILIPPE GERIL  
(BELGIUM)**

**Editor**

**Professor Dan Stefanoui  
Politehnica University of Bucharest, Bucharest, Romania**

### **Local Programme Chair**

Janetta Culita, Politehnica University of Bucharest, Bucharest, Romania

## **International Programme Committee**

### **WEBTEC Programme Committee**

Riadh Ben Halima, LAAS-CNRS, Université de Toulouse, Toulouse Cedex, France  
Boguslaw Butrylo, Bialystok Technical University, Bialystok, Poland  
Khalil Drira, LAAS-CNRS, Université de Toulouse, Toulouse Cedex, France  
Tom Guérout, LAAS-CNRS, Université de Toulouse, Toulouse Cedex, France  
Markus Koch, Orga Systems GmbH, Paderborn, Germany  
Jens Lichtenberg, Ohio University, Athens, USA  
Assoc. Prof. Wenji Mao, Chinese Academy of Sciences, Beijing, China P.R.  
Thierry Monteil, LAAS-CNRS, Université de Toulouse, Toulouse Cedex, France  
Lorenzo Motta, Ansaldo Segnalamento Ferroviario s.p.a. Genova, Italy  
Dr. Carlos E. Palau, Universidad Politecnica de Valencia, Valencia, Spain  
Prof. Paola Salomoni, Universita di Bologna, Bologna, Italy

### **MEDIATEC Programme Committee**

**Track Chair:** Dr. Ignazio Infantino, Phd, ICAR-CNR, Palermo, Italy

#### **IPC**

Ass. Prof. Ali Arya, Carleton University, Ottawa, Ontario, Canada  
Prof. Helena Barbas, CENTRIA-UNL, Lisbon, Portugal  
Dr Jonathan Dukes, O'Reilly Institute, Trinity College, Dublin 2, Ireland  
Jehan Francois Paris, University of Houston, Houston, USA  
Florin Pop PhD, University POLITEHNICA of Bucharest, Bucharest, Romania  
Prof. Marco Rocchetti, Universita' di Bologna, Bologna, Italy

### **COMTEC Programme Committee**

Prof. Dr. Marwan Al-Akaidi, Arab Open University, Kuwait  
Christos Bouras, University of Patras, Patras, Greece  
Sophie Chabridon, Institut Télécom, Télécom SudParis, Evry Cedex, France  
Prof. Chris Guy, The University of Reading, Reading, United Kingdom  
Ph. D. Oryal Tanir, Bell Canada, Montreal, Canada

### **APTEC Programme Committee**

Assoc. Prof. Viorel Nicolau, "Dunarea de Jos" University of Galati, Romania  
Dr.ir. Johan Opsommer, Belgacom - BUS, Brussels, Belgium  
Prof. Jeanne Schreurs, Hasselt University, Diepenbeek, Belgium  
Ass. Prof. Ramiro Velazquez, Universidad Panamericana, Aguascalientes, Mexico

# INTERNATIONAL PROGRAMME COMMITTEE

## E-TEC Programme Committee

Ciprian Dobre PhD, University Politehnica Bucharest, Bucharest, Romania  
Jose Machado, University do Minho, Braga, Portugal  
Paulo Novais, University do Minho, Braga, Portugal  
Prof. Selwyn Piamuthu, University of Florida, Gainesville, FL, USA

## Workshops

### Cloud Computing

Prof. Dr. Jan Broeckhove, RUCA-UA, Antwerp, Belgium

### Knowledge Management, E-Business management and E-Mobility

Prof. Ricardo Chalmeta, Universidad Jaume I, Castellon, Spain  
Jeanne Schreurs, Hasselt University, Diepenbeek, Belgium

### In-Car Applications

Assoc Prof. Petr Hanacek, Brno University of Technology, Brno, Czech Republic

### Virtual Reality Applications

Pieter Jorissen, Karel de Grote-Hogeschool, Hoboken, Belgium  
Mircea Popovici, Ovidius University, Romania  
Prof. Marcos A Rodrigues, CCRC Sheffield Hallam University, Sheffield, UK

### Medical Imaging Systems

#### General Chair

Joao Manuel R. S. Tavares, FEUP, University of Porto, Porto, Portugal

#### General Co-Chair

Daniela Iacoviello, Department of Computer and System Sciences "A. Ruberti", Sapienza University of Rome, Italy

## International Programme Committee

Adélia Sequeira, Instituto Superior Técnico, Portugal  
Alberto De Santis, Università degli Studi di Roma "La Sapienza", Italy  
Aledir Silveira Pereira, São Paulo State University, Brazil  
Ana Mafalda Reis, University of Porto, Portugal  
Anton Vernet, University Rovira i Virgili, Spain  
Arrate Muñoz Barrutia, University of Navarra, Spain  
Begoña Calvo Calzada, University of Zaragoza, Spain  
Bernard Gosselin, Faculte Polytechnique de Mons, Belgium  
Christos E. Constantinou, Stanford University School of Medicine, USA  
Dinggang Shen, UNC-CH School of Medicine, USA  
Emmanuel A. Audenaert, Ghent University Hospital, Belgium  
Enrique Alegre Gutiérrez, University of León, Spain  
Fiorella Sgallari, University of Bologna, Italy  
Jorge M. G. Barbosa, University of Porto, Portugal  
Lyuba Alboul, Sheffield Hallam University, UK  
Mahmoud El-Sakka, The University of Western Ontario London, Canada  
Manuel González Hidalgo, Balearic Islands University, Spain  
Maria Elizete Kunkel, Universität Ulm, Germany  
Maria Petrou, Imperial College London, UK  
Miguel Velhote Correia, University of Porto, Portugal  
Paola Lecca, The Microsoft Research - University of Trento, Italy  
Petia Radeva, Autonomous University of Barcelona, Spain  
Renato Natal Jorge, University of Porto, Portugal  
Sabina Tangaro, National Institute of Nuclear Physics, Italy  
Teresa Mascarenhas, University of Porto, Portugal  
Vassili Kovalev, University of Surrey, UK  
Yongjie Zhang, Carnegie Mellon University, USA  
Zeyun Yu, University of Wisconsin at Milwaukee, USA

## **INTERNATIONAL PROGRAMME COMMITTEE**

### **Cybersecurity**

Fernando de la Cuadra y de Colmenares, ONTINET.COM

### **Computer Graphics**

Roberto de Beauclair Seixas, IMPA, Rio de Janeiro, Brazil  
Philippe Geril, ETI, Ostend, Belgium

### **Student Track**

Goreti Marreiros, Instituto Superior de Engenharia, Porto, Portugal

# **EUROMEDIA 2012**

© 2012 EUROSIS-ETI

Responsibility for the accuracy of all statements in each peer-referenced paper rests solely with the author(s). Statements are not necessarily representative of nor endorsed by the European Simulation Society. Permission is granted to photocopy portions of the publication for personal use and for the use of students providing credit is given to the conference and publication. Permission does not extend to other types of reproduction nor to copying for incorporation into commercial advertising nor for any other profit-making purpose. Other publications are encouraged to include 300- to 500-word abstracts or excerpts from any paper contained in this book, provided credits are given to the author and the conference.

All author contact information provided in this Proceedings falls under the European Privacy Law and may not be used in any form, written or electronic, without the written permission of the author and the publisher.

All articles published in these Proceedings have been peer reviewed

EUROSIS-ETI Publications are ISI-Thomson and IET referenced

Legal Repository: Koninklijke Bibliotheek van België, Keizerslaan 4, 1000 Brussels, Belgium

CIP 12.620 D/2011/12.620/1

**For permission to publish a complete paper write EUROSIS, c/o Philippe Geril, ETI Executive Director, Greenbridge NV, Wetenschapspark 1, Plassendale 1, B-8400 Ostend Belgium**

EUROSIS is a Division of ETI Bvba, The European Technology Institute, Torhoutsesteenweg 162, Box 4, B-8400 Ostend, Belgium

Printed in Belgium by Reproduct NV, Ghent, Belgium

Cover Design by Grafisch Bedrijf Lammaing, Ostend, Belgium

EUROSIS-ETI Publication

**ISBN: 978-90-77381-69-4**

**EAN : 978-90-77381-69-4**

## PREFACE

The EUROMEDIA conference is the annual EUROSIS meeting aimed at exploring the latest in state-of-the art multimedia research, technology, management and art. As in previous years, the conference seeks to bring together researchers and practitioners in academia and industry, who are interested in exploring and exploiting new and multiple media to create new capabilities for human expression, communication, collaboration, and interaction. EUROMEDIA covers a broad range of topics, from multimedia computing: theory to practice, over underlying technologies to applications. The present event is no exception, providing an ideal forum for the presentation and exchange of research relating to the design and use of state-of-the-art multimedia and networked systems.

The EUROMEDIA 2012 conference, which is held at the JW Marriott Hotel, Bucharest from April 18-20, 2012, runs concurrently with the ECEC and FUBUTEC conferences, this year covers presentations in the field of Cloud Computing, Online Communities, Learning and Diagnosis, Telecom Systems and Secure Telecom Systems.

Next to the regular presentations contained in this book, the conference also features invited presentations by Herman Van der Auweraer, LMS International, Heverlee, Belgium on “Innovation Engineering by Simulation” and by Professor Valentin Cristea of the University POLITEHNICA of Bucharest, Bucharest, Romania on “Challenges and Trends in Software Service-Based Systems”, plus a tutorial by Ignazio Infantino from ICAR-CNR, Palermo, Italy on “Detection of Human Activities and Human Intentions through Cognitive Architecture”.

We also would like to thank Philippe Geril, whose continued dedication and hard work as the conference organiser has enabled us to maintain the standard expected of the EUROMEDIA 2012 conference, to EUROSIS for the opportunity to be involved in the organization of EUROMEDIA 2012, to the University POLITEHNICA of Bucharest and LMS for their support of the event, to all members of the Scientific Committee for their reviews and significant contribution for the high quality standards of EUROMEDIA 2012, to all sessions chairs for their effort for the smooth running of all scientific sessions of EUROMEDIA 2012, to our Keynote and Invited Lecturers and to all Authors for sharing their excellent works during EUROMEDIA 2012 and last but not least to all attendees that enrich and validate the purposes of EUROMEDIA 2012.

Prof. Dan Stefanoui  
University POLITEHNICA Bucharest  
EUROMEDIA'2012  
General Conference Chair





<b>Preface .....</b>	<b>IX</b>
<b>Scientific Programme .....</b>	<b>1</b>
<b>Author Listing .....</b>	<b>109</b>

## CLOUD COMPUTING

### **ReC<sup>2</sup>S: Reliable Cloud Computing System**

Alecsandru Patrascu, Catalin Leordeanu, Ciprian Dobre and Valentin Cristea .....	5
---	---

### **Temperature monitoring and control with cloud instrumentation**

Petru Adrian Cotfas, Daniel Cotfas, Ramona–Georgiana Oros, Doru Ursutiu and Cornel Samoila .....	14
---	----

### **Social Cloud for personalized information retrieval**

Alexandru Agape .....	18
-----------------------	----

### **Digua: Minifier and Obfuscator for Web Resources**

Alex Ciminian and Ciprian Dobre .....	21
---------------------------------------	----

## ONLINE COMMUNITIES

### **Customized modulation of VLE into an online parallel and classified Virtual community for educators: Arab Open University's experience**

Haifaa Elayyan and Hussien Mansour .....	29
--	----

### **Computer Technology: A Tool in the hand of the Artist?**

Canan Hastik and Arnd Steinmetz .....	35
---------------------------------------	----

### **Social Shopping Adviser: Recommendation platform based on mobile services**

Elena Burceanu, Ciprian Dobre and Valentin Cristea .....	39
--	----

## LEARNING AND DIAGNOSIS

### **Supporting Learning-By-Doing Situations by Semantic Technologies**

Danail Dochev and Gennady Agre .....	49
--------------------------------------	----

### **Using a cognitive model to include human emotions and intentions in Human-Machine Interaction**

Ignazio Infantino, Giovanni Pilato, Riccardo Rizzo and Filippo Vella .....	54
--	----

## CONTENTS

<b>Computer Aided Diagnosis Methods Based on Fractal and Spatial Series Analysis for Kidney CT Images</b>	
Andreea Udrea and Mihai Tanase .....	59

## TELECOM SYSTEMS

<b>Benchmark Analysis for Advanced Distributed Data Storage for Heterogenous Clusters</b>	
Catalin Negru, Florin Pop, Ciprian Dobre and Valentin Cristea.....	67

<b>Proposal of a Smooth Channel Switching Mechanism for P2P Streaming and its Application</b>	
Naomi Terada, Eiji Kominami, Atsuo Inomata, Kazutoshi Fujikawa, Eiji Kawai and Hideki Sunahara .....	73

<b>Wireless Router as a Physical Access Control System (WRPACS)</b>	
Dragos George Comaneci, Silvia Cristina Stegaru and Ciprian Dobre .....	78

<b>Application of Vehicle Ad-hoc Networks in Traffic Control Systems</b>	
Benny M Nyambo, Goodbye Mavata and Gerrit K. Janssens .....	85

## SECURE TELECOM SYSTEMS

<b>Toward a Secure Data sharing Peer to Peer Network based on Geometric and Semantic Distances</b>	
Ana-Delia Sâmbotin and Mugurel Ionuț Andreica .....	93

<b>Security Communication Layer for Public Distributed Reporting Services</b>	
Decebal Popescu, Ciprian Dobre, Florin Pop, Nirvana Popescu and Valentin Cristea.....	100

# **SCIENTIFIC PROGRAMME**



# **CLOUD COMPUTING**



# ReC<sup>2</sup>S: Reliable Cloud Computing System

Alecsandru Patrascu, Catalin Leordeanu, Ciprian Dobre, Valentin Cristea  
Faculty of Automatic Control and Computers,  
University Politehnica of Bucharest  
email: [alecsandru.patrascu@cti.pub.ro](mailto:alecsandru.patrascu@cti.pub.ro),  
{[catalin.leordeanu](mailto:catalin.leordeanu@cs.pub.ro), [ciprian.dobre](mailto:ciprian.dobre@cs.pub.ro), [valentin.cristea](mailto:valentin.cristea@cs.pub.ro)}@cs.pub.ro

## KEYWORDS

Cloud Computing, resource management, scheduling, reliability, security

## ABSTRACT

In our research we focus on providing essential characteristics such as performance, availability, reliability and security for cloud computing systems, which are becoming more and more popular. In this paper we accurately describe the capabilities that our project provides to its end-users and also specify all the functional and non-functional requirements that the application implements. We also describe some of our design choices for our solution, along with how we intend to integrate our solution into other existing virtualization solutions and cloud computing software.

## INTRODUCTION

Cloud Computing to put it simply, means Internet Computing. Cloud computing (Vaquero et al. 2009) is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

This cloud model (Keahey et al. 2009) promotes availability and is composed of five essential characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service); three service models (cloud software as a service (SaaS), cloud platform as a service (PaaS) and cloud infrastructure as a service (IaaS)); and, four deployment models (private cloud, community cloud, public cloud and hybrid cloud). Key enabling technologies include: (1) fast wide-area networks, (2) powerful, inexpensive server computers, and (3) high-performance virtualization for commodity hardware.

The cloud computing model offers the promise of massive cost savings combined with increased IT agility. It is considered critical that government and industry begin adoption of this technology in response to difficult economic constraints. However, cloud computing tech-

nology challenges many traditional approaches to datacenter and enterprise application design and management. Cloud computing is currently being used. However, security, interoperability, and portability are cited as major barriers to broader adoption.

The Internet is commonly visualized as clouds; hence the term “cloud computing” for computation done through the Internet. With cloud computing users, for example, can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Besides, databases in the cloud are very dynamic and scalable.

Cloud computing is unlike grid computing, utility computing, or autonomic computing. In fact, it is a very independent platform in terms of computing. The best example of cloud computing is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computers through the Internet.

We are going to talk in detail about the capabilities of the application that we are going to develop. The main goal of this paper is to present a unified and self-contained platform and framework on top of which end-users can develop custom application in a secure and reliable mode. The users will benefit from the full power of the cloud computing framework in order to reach their desired performance and security degree.

## RELATED WORK

Many projects tackle the problem of dynamically overlaying virtual resources on top of physical resources by using virtualization technologies, and do so with different resource models. These models generally consider overhead as part of the virtual resource allocated to the user, or do not manage or attempt to reduce it. A common assumption in related projects is that all necessary images are already deployed on the worker nodes. Our requirements for dynamic deployment of advanced reservations (AR) and as soon as possible (ASAP) workspaces make it impossible to make this assumption.

Amazon Elastic Compute Cloud (EC2) (Ama 2011) is a central part of Amazon’s cloud computing platform,

Amazon Web Services (AWS). EC2 allows users to rent virtual computers on which to run their own computer applications and allows scalable deployment of applications by providing a web service through which a user can boot an Amazon Machine Image to create a virtual machine, which Amazon calls an “instance”, containing any software desired. A user can create, launch, and terminate server instances as needed, paying by the hour for active servers, hence the term “elastic”. EC2 provides users with control over the geographical location of instances which allows for latency optimization and high levels of redundancy. For example, to minimize downtime, a user can set up server instances in multiple zones which are insulated from each other for most causes of failure such that one backs up the other.

The XGE (Fallenbeck et al. 2006) project extends Sun Grid Engine so it will use different VMs for serial batch requests and for parallel job requests. The motivation for their work is to improve utilization of a university cluster shared by two user communities with different requirements. By using the suspend/resume capabilities of Xen virtual machines when combining serial and parallel jobs, the XGE project has achieved improved cluster utilization when compared against using backfilling and physical hardware. However, the XGE project assumes that two fixed VM images are predeployed on all cluster nodes.

The VIOLIN and VioCluster (Ruth et al. 2005) projects allow users to overlay a virtual cluster over more than one physical cluster, leveraging VM live migration to perform load balancing between the different clusters. The VioCluster model assumes that VM images are already deployed on potential hosts, and only a “binary diff” file (implemented as a small Copy-On-Write file), expressing the particular configuration of each instance, is transferred at deploy-time. This approach is less flexible than using image metadata, as COWs can be invalidated by changes in the VM images. Furthermore, our work focuses on use cases where multiple image templates might be used in a physical cluster, which makes it impractical to supply all the templates on all the nodes.

The Maestro-VC (Kiyancilar et al. 2006) system also explores the benefits of providing a scheduler with application-specific information that can optimize its decisions and, in fact, also leverages caches to reduce image transfers. However, Maestro-VC focuses on clusters with long lifetimes, and their model does not schedule image transfer overhead in a deadline-sensitive manner, and just assumes that any image staging overhead will be acceptable given the duration of the virtual cluster. Our work includes short-lived workspaces that must perform efficiently under our model.

The Shirako (Irwin et al. 2006) system developed within the Cluster-On-Demand project uses VMs to partition a physical cluster into several virtual clusters. Their interfaces focus on granting leases on resources to users,

which can be redeemed at some point in the future. However, their overhead management model absorbs it into resources used for VM deployment and management. As we have shown, this model is not sufficient for AR-style cases.

The In-VIGO (Adabala et al. 2005) project proposes adding three layers of virtualization over grid resources to enable the creation of virtual grids. Our work, which relates to their first layer (creating virtual resources over physical resources), is concerned with finer-grained allocations and enforcements than in the In-VIGO project. Although some exploration of cache-based deployment has also been done with VMPlant, this project focuses on batch as opposed to deadline-sensitive cases.

## CONTEXT

Cloud computing is cost-effective and the cost is greatly reduced as initial expense and recurring expenses are much lower than traditional computing. Maintenance cost is reduced as a third party maintains everything from running the cloud to storing data. The cloud is characterized by features such as platform, location and device independence, which make it easily adoptable for all sizes of businesses, in particular small and mid-sized. However, owing to redundancy of computer system networks and storage system cloud may not be reliable for data, but it scores well as far as security is concerned. In cloud computing, security is tremendously improved because of a superior technology security system, which is now easily available and affordable. Yet another important characteristic of cloud is scalability, which is achieved through server virtualization.

The main form of abstracting the hardware resources, and also the main method of providing the scheduler with information is the lease. The concept of leases is also used in other systems available. Basically, a lease is like a renting contract existing between the user that requests certain resources and the system that offers them. This contract specifies the duration of the renting and is based on the fact that the user will be responsible in that for the resources allocated.

The information that is going to be retained in these leases varies from system to system, but mostly they contain details regarding the processor, the memory that is going to be allocated. More exactly, our scheduler will accept leases that contain the following information, which will be joined together under a lease id: processor architecture, processor vendor, processor speed, processor number of cores, memory size, storage capacity, network bandwidth, network protocol, lease start time, lease end time, lease duration.

## GENERAL SYSTEM ARCHITECTURE

The system presented in the following paper has a modular architecture. All modules are described in detail.



It is easy to see that the whole ecosystem is actually pluggable and it can be extended with other modules or plugins.

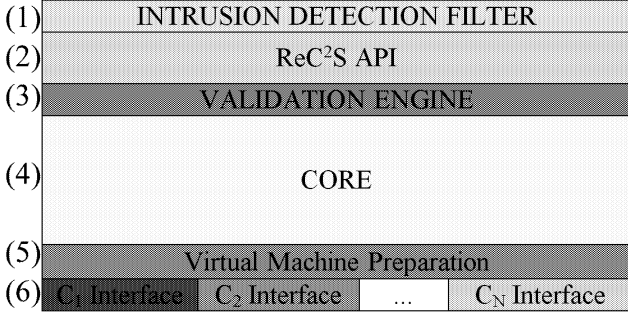


Figure 1: Components of the system

The entire system is composed from 6 layers. We present them briefly to offer a general idea of the components and how they fit in. In the following chapters we present each of them in detail.

The first layer is responsible for filtering the requests that come from outside the cloud. It basically checks the legality of a certain request to the cloud system.

The second layer is the API layer. The API represents a set of primitives that are offered to the user and permits interaction with the cloud systems. It is presented as a web front-end and a static API. For example an authenticated user can request to start/stop/restart a certain virtual machine, can push a job to the cloud system or a specific virtual machine, can retrieve answers from the job that he pushed, etc.

The third layer is responsible for checking that the actions that the user specified or requested are actually eligible for executing. The main goal is security - anomaly request detection.

The fourth layer and the most important one is the core of the system. It is responsible with interaction with the cloud systems that he manages. It does a load balancing of the requests it receives, both in the same autonomous system or inter autonomous systems and it runs a lease based scheduler.

The fifth layer is responsible with the preparation of the virtual machines that are going to be loaded. This includes finding the appropriate virtual image in the content repository, and, if necessary, installing different software stacks inside.

The sixth layer is responsible for communication directly to a specific cloud system interface.

### Intrusion detection filter

This module is the entry point in our system and it is responsible with its security. It is designed in such way that it can detect attacks that originate from outside. It detects malicious actions like flooding and DoS/DDoS attacks.

### ReC²S API

This module offers a way to the user to interact with the system. In our current evolution state we provide means to add new leases. The requests are registered and sent to validation, to the proper module. In order to be more interactive, we provide a graphical user interface, in the form of a webpage.

This module is split in two separate layers. The first one represents a REST-full API implementation and the second one the proper implementation. In our implementation, the API wrapper must permit the use of the following actions:

- setting the lease details. In this section, the user must provide a series of information about the lease that he's creating, like:
  - processor architecture. The user can choose between a 32 or 64 bit architecture. This is important because in this way he can take advantage of different optimization and speedups available to certain processors;
  - processor vendor. The user can choose between Intel or AMD processor type. Also this is important for certain applications that are optimized for a specific vendor;
  - processor speed. This is the actually speed of the CPU;
  - number of processor cores. This is the number of processor/cores that the virtual machine(s) from this lease will have available;
  - memory size. This is the amount of RAM available to the virtual machine(s);
  - storage capacity. This is the amount of disc space required for the virtual machine(s) to run;
  - network bandwidth. This is the speed of the virtual network card that the virtual machine(s) will have;
  - lease start time. This is important when adding a lease because it impacts the way in which the virtual machine(s) are added and started. This time is used in the different scheduling policies inside the core. The user can choose between a determinate or infinite time for the virtual machine(s). An infinite time is the same as having a persistent lease. The determinate time can be a certain timestamp in the future or even a certain event (ex: the user wants to start a lease when data is ready to be processed);
  - lease time end. This is important when adding a lease because it impacts the way in which the virtual machine(s) are ran, stopped and

preempted. This time is used in the different scheduling policies inside the core. Also the user can choose between a determinate or infinite (persistent) lease;

- lease duration. This, in conjuncture with the preemptible part can be used in help of the users that are not running very important tasks and they can permit the virtual machine to be paused and resumed for running more important leases. Also, this is a good way of reducing cost and achieving the desired elasticity. The user can choose between a timed or infinite (persistent) lease;
  - preemptible. This offers the user the chance to make his lease prone to pausing and resuming if the scheduler decides to do that.
- setting the virtual machine(s) details. In this section, the user can customize settings for the virtual machine(s) that is (are) going to be run with this lease, like:
    - minimum instances. This is the minimum of virtual machines that the user wants at a certain period, and their number mustn't never get below this value;
    - maximum instances. This is the maximum number of the virtual machines that the user wants in heavy load periods. The scheduler must be careful when using this feature to start the machines when a heavy load is detected and stop the extra virtual machines when not needed. This is good for the user because it helps in achieving desired elasticity;
    - the type of the template. This is the operating system that every virtual machine involved in a lease must run. It's implemented as a lease in order to maintain an uniform view of the virtual machines for the scheduler. Currently, the only base template in use is Ubuntu Server 10.04. Later, these templates will be enriched with other Linux operating systems, or even let the user upload their own virtual machine template;
    - network configuration. This is the IP or IP pool of the virtual machine(s) that is going to be used by the user to connect to them.
  - setting the packages that the users want to deploy on each virtual machine. This lets the user to auto-install some software on each of the running virtual machine(s). This can include a Java/Python/MPI/etc development framework, a database, etc;

- saving the request for future uses. This is useful for the user because he can save the settings made to the lease, and also the lease itself for future uses.

After adding a lease, the user can access its details and information like:

- lease administration. This permits the user to stop, pause or restart the lease at his desire;
- alerts. This permits the user to have him attention on events like: before starting the lease with T minutes, on lease start, on lease stop, when the scheduler decided when to start the lease.

## API action validation

This module receives requests to add new leases in system. Every new request is checked for consistency and validated. If the request is legit and the user making the request is authenticated, the new lease is transformed in a job for our system and it's properly inserted in the job queue.

## Core

This module is the most important from the entire system. The core is composed from 4 sub-modules. We present each of them briefly in order to make a good idea of the core module.

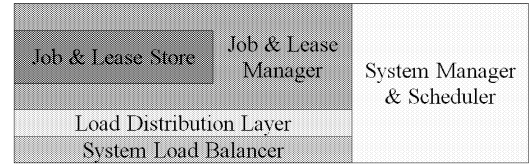


Figure 2: System core

The job and lease manager mainly consists of a form of data replication and partition. It provides real-time data aware routing, elastic data access and caching. The job and lease store is basically a sub-module of the lease manager that is responsible for storing in a reliable way the things that the cloud system manager and scheduler will process.

The load distribution layer is a sub-module responsible with horizontal scaling the requests received from the scheduler. It runs an application framework in order to decouple the code from the existing underneath runtime. The system load balancer is responsible for vertically scaling the requests received from the scheduler.

The system manager and scheduler is the most important sub-module. Its main purpose is the scheduling of jobs and leases efficiently between the virtual machines. It also discovers new instances of new services

and virtual machines managers, load balancers, load distributions. It has a pluggable interface in order to be scalable.

#### *Job and lease store*

This is the sub-module that stores all lease requests from the outside. These requests are stored as objects in the queue. This sub-module can be implemented in a lot of ways, but at our current stage is implemented as a message queue. When choosing a particular queuing system we analyzed features like: the speed of the sub-system, support for different programming languages (Java, C, C++, etc), standard compliant, data security, data replication, support for different frameworks (Spring, etc), support for different communication protocols (TCP, SSL, UDP, multicast, etc). All these requirements were filled successfully by the open-source library, Apache ActiveMQ.

#### *Job and lease manager*

This is the sub-module that connects the entire core part to the job and lease store. This is implemented in a generic form and has to provide access methods like getting an element from the store, putting an element to the store. Because the underneath store can be implemented in different ways and using different architectures, this sub-module should be implemented in a plug-and-play manner, using a pluggable system, so that every access to the store should be made using a specific plugin.

Every plugin must register to the manager. We recommend this approach in order to avoid having to re-deploy and restart the manager every time a store is added, or the store API is changing. If this is not a problem for the environment, the whole sub-module can be stopped, modified and then started again.

As we have said above, the manager must provide an interface to the outside world. In our current implementation we used the following ones:

- `addLease(L)`. This call will add to the specific store the lease `L`. This call must return to the caller a proper value that will reflect if the lease is added to the store and it's ready to be processed, or if the adding the lease to the store has failed. This return value is necessary in order to the caller to take proper actions: either inform the user that everything is good and to wait for the access to the virtual machine(s) that he requested or retry adding the lease to the store;
- `getNextLease()`. This call will return to the caller the next lease that is going to be processed, if it exists. If the store doesn't have any leases the caller must get an empty store alert in order to retry to call this until there are available leases to process.

In order for this manager to work properly it provides

real-time data aware routing. The only abstraction being the underneath store, starting from the upper layers, the system has proper knowledge of the leases that are requested and offered to the caller. This is necessary for providing elastic data access, meaning that the sub-module itself must be capable of auto-balancing in case of high network traffic. Also this shall happen if the stores that it manages are heavily loaded and/or the requests are coming in too fast for one manager to handle. Caching must be another important feature that this module has to handle. The leases requested from the underneath store are kept in cache for a certain period of time. We have chosen this approach to fulfill the needs for the persistent leases. This case is rarely found in practice because only few of the users want the lease to be persistent due to the high cost of the resources.

#### *Load distribution layer*

This is be the layer responsible with horizontally scaling our work loads. This is done automatically and in the process of this analysis, the number of workstations is taken in account. If their number changes over the execution of our system, the entire algorithm is re-run to reflect the current situation.

#### *System load balancer*

This is the layer responsible with vertically scaling our work loads. This is done also automatically. There is a connection between this layer and the load distribution layer. To be clearer, we give a simple example of how the two of them work together. Let's assume that we run our system over an infrastructure consisting in four servers, all the same. The system load balancer detects that the hardware capabilities are the same and will report it to the load distribution layer. Then, the load distribution layer sees that it has four servers available, and after receiving updates from the system load balancer, it will split the entire work load in four parts and will submit them to each server. Now, let's assume that a server will be replaced by one, twice as powerful. The load distribution layer will still see four servers, but it will get a notification from the system load balancer that one of the servers is two times more powerful than the remaining three. Therefore, it will split the work load into five parts and it will submit two parts to the newer and powerful server and to the rest of the others, one part for each.

#### *Scheduler*

In order for the scheduler to function properly a scheduling scheme has been composed. Depending on the leases and the task, they are split in the following scheduling types and the scheduler has three operating modes:

- Using advanced reservations. This forms the base of the leasing strategies. It reflects fixed resources that are going to be allocated.

- Using a best-effort strategy. This is formed from another four sub-strategies

- *Preemptible*. The virtual machines can be started, stopped, paused and resumed at a given time. This process can be somehow compared with the preemption of processes made in the operating system, only that in our case the processes are replaced with virtual machines. To maintain a good system consistency an external clock must be used, to prevent messages loosing between the virtual machines when they are stopped.

To be more precise, in the following lines we will talk about this strategy and comparing it with a process. Let's assume that we have a virtual machine running, not exchanging data with any other virtual machine. When the scheduler decides to preempt it, for later reloading or to move it to another network node, it just calls the properly "Pause Virtual Machine" function. Then, the virtual machine is stopped and it's ready for restore.

But if we have a machine that exchanges data with another virtual machine and it depends on it to function properly, when the scheduler decides to preempt it, all this chain of virtual machines must be stopped in the same time to avoid data loss. The same happens when they are restored - the scheduler must restore them in the same time, again to avoid data loss.

- *Non-preemptible*. This type of scheduling is also known as "right now allocation". In order to achieve this, a series of information regarding the virtual machine and the place in which the virtual machine will run is required. The scheduler needs data like the actual size of the files that compose the virtual machine, the transfer speed to the destination network and the time needed for the virtual machine to start. For example, if the user wants a lease of one machine, starting in 2 minute, the scheduler must find the appropriate free server to start the virtual machine, and start to transfer the virtual machine template as soon as possible so that at the end of the 2 minute, a virtual machine will be ready for deployment. Also, if the template is copied in place sooner than the starting point, it is no problem because it can wait for the user to start using it. A problem appears if the starting point of the lease is sooner than the time needed to transfer the virtual machine image from the repository to the destination. This can be resolved by using virtual machines caches. This part will be resolved in the future by a different module of the system.

- *Deadline*. This type of scheduling is also known as "you can allocate anytime, but no longer than T", where T is a fixed time. In order to achieve this, the scheduler must know how much time will the lease last so that he can allocate it before this.
- *Negotiated*. Depending on the moment in time when the user wants to start the lease. (Now: 100\$, after 1h: 50\$, after 2h: 20\$, etc)

- Using an urgent lease. This is going to be used when instant resources must be allocated

In order to deploy efficiently through different virtual machines operating systems a process driver must be used. To make this task easier we use Apache Ant because of its support for multiple architectures and operating systems.

The whole system is seen as in the figure 3.

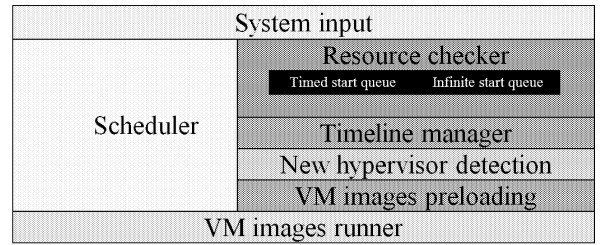


Figure 3: Scheduler architecture

We've mentioned the "System input" layer because in order to work, our system must have entries that contain leases to process. This is a connection layer between the core and the underneath lease storage.

When the input reaches the system it is analyzed and sent to the "Resource Checker" module. This is responsible with checking the availability of resources specified in the lease on the physical systems. It also checks if the system can sustain this requirements on the whole lease duration. This decision is influenced by the current state of the managed systems. It must also keep a safe guard for the required elastic expansion of the virtual machines involved in the allocation of the lease. If this module decides that the lease is safe to be allocated it saves the lease on a special queue, implemented as a priority queue, the "Timed start queue" from the above. If it decides that the physical system cannot hold the lease it saved the lease on another special queue, also implemented as a priority queue, the "Infinite start queue" from the above. The thing that differences the two queues is that in the moment the lease is inserted in the latest, the lease start time is modified to infinite, so that it can start as soon as the system has free resources. Another thing that this module uses is the "Timeline manager", which acts as a global clock and it manages the two queues mentioned above. Mainly its functionality is that, at every defined moment in time, in our

case at every minute, to check first for existing leases in the timed start queue. If it finds one, it is automatically deployed on a destination hypervisor chosen from the one attached to the virtual machine runner layer. It also checks if resources are available to run the lease from the infinite start queue.

The “New hypervisor detection” layer is responsible with detection of new hypervisor that are going to be attached and used when running the leases.

The “VM image preloading” layer is responsible with the initialization of the virtual machine image, or cloning an existing one. The initialization creates a new virtual machine from an existing configuration and installs the software stacks chosen by the user. The cloning function just duplicates an existing configuration.

The “VM image runner” is responsible with running the previously created and configured virtual image, on the destination hypervisor. The user will be granted access to the virtual machine at this step.

The core is composed from the “Scheduler” layer. Historically, scheduling was and it’s going to be a hard and tricky problem in computer science. Scheduling is concerned with the allocation of scarce resources to activities with the objective of optimizing one or more performance measures. Depending on the situation, resources and activities can take on many different forms. Resources may be machines in an assembly plant, CPU, memory, I/O devices, etc. The form that we are going to study in deeper is called online scheduling.

In our online scheduling form, that we have entitled “ReC2Sched”, the scheduler receives jobs during different periods of times. The most interesting part is that it must take decisions without knowing some of the details of the jobs or knowing what will happen in the future. This means that the decisions he is going to make will not be optimal, but with proper algorithms and heuristics this entire process will tend to that.

In our research for the most suitable scheduling algorithms we studied a couple of them.

- randomized algorithms: these algorithms are based on a Monte-Carlo approach and take their decision based on a pseudo-random choice;
- semi-online algorithms:
  - Shortest Job First - is a scheduling policy that selects the waiting lease with the smallest execution time to execute next. This is advantageous because it’s simple to use and implement and because it maximizes the average amount of time each lease has to wait until its execution is complete. SJF is rarely used outside of specialized environments because it requires accurate estimations of the time of all leases that are waiting to execute. Estimating the

running time of queued leases is done using a technique called “aging”;

- Shortest Remaining Processing Time - is a scheduling method that is a preemptive version of the Shortest Job Next scheduling. In this algorithm, the lease with the smallest amount of time remaining until completion is selected to execute. Since the currently executing process is the one with the shortest amount of time remaining by definition, and since that time should only reduce as execution progress, leases will always run until they complete or a new lease is added that requires a smaller amount of time. This policy is advantageous because short leases are handled very quickly. The system also requires very little overhead since it only makes a decision when a lease completes or a new lease is added, and when a new lease is added the algorithm only needs to compare the currently executing lease with the new lease, ignoring all other leases currently waiting to execute;
- First In First Out - is basically an abstraction in ways of organizing and manipulation of data relative to time and prioritization. This expression describes the principle of a queue processing technique or servicing conflicting demands by ordering process by first-come, first-served (FCFS) behavior: what comes in first is handled first, what comes in next waits until the first is finished, etc;
- High Density First - The algorithm Highest Density First always runs the job with the highest density, which is the weight of the job divided by the initial work of the job;
- Round Robin - this is one of the simplest scheduling algorithms for leases, which assigns time slices to each lease in equal portions and in circular order, handling all leases without priority (also known as cyclic executive). Round-robin scheduling is both simple and easy to implement, and starvation-free. This kind of policy may not be desirable if the leases size are highly variable. A lease that produces large jobs would be favored over other leases. This problem may be solved by time-sharing, i.e. by giving each job a time slot or quantum (its allowance of CPU time), and interrupt the job if it is not completed by then. The job is resumed next time a time slot is assigned to that lease;
- Shortest Elapsed Time First - this algorithm devotes all the resources to the job that has been processed the least. In the case of ties, this amounts to round robin on the jobs that

have been processed the least. While round robin perhaps most intuitively captures the notion of fairness, shortest elapsed time first can be seen as fair in an affirmative action sense of fairness.

Besides implementing our custom scheduling algorithm, for performance comparison we have chosen to implement custom FIFO and SJF algorithms. We present them bellow.

The first engine is FIFO. This is a simplistic implementation and it processes leases as soon as it arrives. SJF additionally does a lease sort depending on the time of running. In our tests, the times obtained with these two engines were not sufficient to satisfy our need for speed. This lead us to the implementation of our custom algorithm, specially created for our problems. It is different because it does fast lookups into the lease storage unit and it analyses them in advance (we have used in our implementation a 2 minute processing time in advance). Also, our algorithm is a hybrid between the previous two and also is an adaptive algorithm. As a novelty, we are using a 0.5 second computation step. In each step a number of leases is choses to be scheduled.

### Virtual machine preparation

This module is intended as a layer between the core and the actual cloud specific API. The most important tasks that it does are:

- get the decision made by the scheduler;
- analyze it and create a deployment plan. The deployment plan must contain the virtual machine image that is going to be loaded, the software stack that is going to be installed and the appropriate installation script, if such option is chosen by the user;
- preload using the cloud API the image to the chosen location;
- run the installation script. When choosing a certain framework to run our script we analyzed features like: system independent implementation, the ability to run all kind of tasks (creating a folder, deleting a folder, calling certain specific commands). All these requirements were filled by the open-source project Apache Ant

### Cloud specific interface

This module is intended as an abstraction layer between our system and the cloud platforms existing on the market. In order to be more scalable and also maintain a high degree of abstraction, an interface is provided and every implementation of the specific API must implement this. This module acts as a plugin manager, with

the proper API being inserted at run-time in a plug-and-play way.

For our implementation, as we said at the beginning of the paper, we started with VMware ESXi. VMware ESXi has been designed to be easily adapted to any infrastructure and easily extended with new components. The result is a modular system that can implement a variety of Cloud architectures and can interface with multiple datacenter services.

## RESULTS AND OPTIMIZATIONS

To optimize the speed of deployment of the virtual machines requested on a specific lease, we configured a list of virtual machines with predefined software stacks. For example we have in the repository virtual machines templates containing already-installed databases, and different other frameworks. This has a great impact on the entire system because deployment is made faster. This time is won from the time used by the virtual machines images to install the specific software stacks.

To test the scheduler and the system as a whole we have tested all three scheduling algorithms. The scenario was as follows. Suppose that we have 8 users logged in in our system. They each submit a lease, but all with the same time of start. This scenario is a common found in actual production environments.

The hardware platform used was composed from an AMD Phenom II X6, with 8GB RAM, RAID0 configured hard-disks running VirtualBox as hypervisor and an Intel DualCore, 4GB RAM as the scheduler. The network used is 10/100 MB.

In case of FIFO we obtained the following results:

#	Lease creation time (s)	Resource lookup time (s)	Lease lookup time (s)	Virtual machine clone time (s)	Create time (s)
1	9.939	0.100	0.560	9.029	0.250
2	9.940	0.098	0.560	9.029	0.253
3	9.948	0.098	0.560	9.029	0.261
4	9.927	0.097	0.560	9.029	0.241
5	9.926	0.101	0.560	9.029	0.236
6	9.939	0.095	0.560	9.029	0.255
7	9.931	0.098	0.560	9.029	0.244
8	9.951	0.098	0.560	9.029	0.264

In the first column we see the order in which the leases were ran. This is 1, 2, 3, 4, 5, 6, 7 and 8. On the second column we can see the total lease time spent in creation of a lease.

Thanks to our included Virtual Machine preloader, before the actual lease are created, the virtual machine template ( 800MB) is transferred to the destination. This took about 82 seconds in our test environment.

The total time spent was  $(\sum Leasecreationtime) + 82 = 156.735seconds$

In case of SJF we obtained the following results:

#	Lease cre- ation time (s)	Resource lookup time (s)	Lease lookup time (s)	Virtual ma- chine clone time (s)	Create time (s)
2	9.940	0.098	0.560	9.029	0.253
4	9.927	0.097	0.560	9.029	0.241
7	9.931	0.098	0.560	9.029	0.244
1	9.939	0.100	0.560	9.029	0.250
3	9.948	0.098	0.560	9.029	0.261
8	9.951	0.098	0.560	9.029	0.264
5	9.926	0.101	0.560	9.029	0.236
6	9.939	0.095	0.560	9.029	0.255

We can see from the above table that the lease are picked to be run in a different order, 2, 4, 7, 1, 3, 8, 5 and 6. The total time spent in this case was  $(\sum Leasecreationtime) + 82 = 155.947seconds$

In case of ReC2Sched we have obtained the following:

#	Lease cre- ation time (s)	Resource lookup time (s)	Lease lookup time (s)	Virtual ma- chine clone time (s)	Create time (s)
1	9.768	0.055	0.560	9.029	0.124
2	9.767	0.056	0.560	9.029	0.122
3	9.767	0.056	0.560	9.029	0.122
4	9.772	0.056	0.560	9.029	0.127
5	9.764	0.056	0.560	9.029	0.119
6	9.766	0.055	0.560	9.029	0.122
7	9.771	0.057	0.560	9.029	0.125
8	9.766	0.055	0.560	9.029	0.122

We can easily conclude that the times are lower than the previous two engines. Also, because the lease are running in parallel, the total time was  $Max(startleasetime + delay) + 82 = 92.264seconds$  which is the lowest obtained in our test.

## CONCLUSIONS AND FUTURE WORK

In this paper we presented a solution to provide reliability and security for Cloud users. Our approach takes the form of a complete framework on top of an existing Cloud infrastructure and we have described each of its layers and characteristics. Furthermore, the experimental results prove its efficiency and performance.

As future work we intend to further optimize the scheduling algorithms, as well as the other layers of the framework. We also intend to offer more complex security solutions which would greatly improve the usability

of the system. Further testing using more complex scenarios with other existing Cloud infrastructures would also help us to further improve our solution.

## Acknowledgments

The research presented in this paper is supported by national project: “TRANSYS - Models and Techniques for Traffic Optimizing in Urban Environments”, Contract No. 4/28.07.2010, Project CNCIS-PN-II-RU-PD ID: 238.

## REFERENCES

2011. *Amazon Elastic Compute Cloud (EC2)*. URL <http://aws.amazon.com/ec2/>.
- Adabala S.; Chadha V.; Chawla P.; Figueiredo R.; Fortes J.; Krsul I.; Matsunaga A.; Tsugawa M.; Zhang J.; Zhao M.; Zhu L.; and Zhu X., 2005. *From virtualized resources to virtual computing grids: the INVIGO system*. In *Future Generation Computer Systems*.
- Fallenbeck N.; Pinch H.; Smith M.; and Freisleben B., 2006. *Xen and the art of cluster scheduling*. In *Proceedings of the 1st International Workshop on Virtualization Technology in Distributed Computing*. IEEE.
- Irwin D.; Chase J.; Grit L.; A.Yumerefendi; Becker D.; and Yocum K., 2006. *Sharing networked resources with brokered leases*. In *USENIX Technical Conference*.
- Keahey K.; Tsugawa M.; Matsunaga A.; and Fortes J., 2009. *Sky Computing*. *IEEE Internet Computing*, 13, no. 5, 43–51. ISSN 1089-7801.
- Kiyancilar N.; Koenig G.; and Yurcik W., 2006. *Maestro-VC: A paravirtualized execution environment for secure on-demand cluster computing*. In *Proceedings of the 6th IEEE International Symposium on Cluster Computing and Grid*. IEEE.
- Ruth P.; McGachey P.; and Xu D., 2005. *VioCluster: Virtualization for dynamic computational domains*. In *Proceedings of the IEEE International Conference on Cluster Computing*. IEEE.
- Vaquero L.; Rodero-Merino L.; Caceres J.; et al., 2009. *A break in the clouds: towards a cloud definition*. *ACM SIGCOMM Computer Communication Review*, 39, no. 1, 50–55. ISSN 0146-4833. doi:<http://doi.acm.org/10.1145/1496091.1496100>.

# Temperature monitoring and control with cloud instrumentation

Petru Adrian Cotfas  
Faculty of Electrical Engineering  
and Computer Sciences  
Transilvania University of Brasov  
Bulevardul Eroilor 29, Brasov  
500035, Romania  
pcotfas@unitbv.ro

Daniel Cotfas  
Faculty of Electrical Engineering  
and Computer Sciences  
Transilvania University of Brasov  
Bulevardul Eroilor 29, Brasov  
500035, Romania  
dctotfas@unitbv.ro

Ramona Georgiana Oros  
Faculty of Material Science and  
Engineering  
Transilvania University of Brasov  
Bulevardul Eroilor 29, Brasov  
500035, Romania  
oros\_ramona@yahoo.com

Doru Ursutiu  
Faculty of Electrical Engineering  
and Computer Sciences  
Transilvania University of Brasov  
Bulevardul Eroilor 29, Brasov  
500035, Romania  
udoru@unitbv.ro

Cornel Samoila  
Faculty of Material Science and  
Engineering  
Transilvania University of Brasov  
Bulevardul Eroilor 29, Brasov  
500035, Romania  
csam@unitbv.ro

## KEYWORDS

Industrial processes, dynamic programming, system engineering, software engineering, real time.

## ABSTRACT

The main directions of scientific and technical revolution of recent years can be considered: development of new materials with predetermined properties, the knowledge structure of matter and mastery of this structure, the development of biotechnologies and the most important, informatization. The last one had effects not because nowadays computers are used in all fields, but especially because of the high level of technical - economic performance, diversification and ultra-specialization of all kind of processes, from medical to military but also industry. Thus, the development of high quality products requires rigorous control of the production process in terms of process variables involved. For this a WiTAG system is going to be used, as the main component of the controlling system.

## STATE OF THE ART

Talking about industrial processes like heating, melting, welding or drying leads also to talks related with special equipment used for such processes. According to this are defined the used parameters for the control and management of the processes.

Having as example a heating process the essential condition to realize the final product and achieve optimal conditions, is to keep the temperature between recommended limits.

Control and adjustment of parameters when the heating equipment is working can be achieved by using specialized devices, properly arranged in a control loop. For such implementation Transilvania University of Brasov came with the idea to used wireless technologies.

In general, wireless sensors are small systems widely used in measuring instruments. Some of these sensors are manufactured using very new and advanced technologies such as neural networks or fuzzy logic, even accounting for embedded software on the chip.

Nowadays, most of the systems available on the market used for temperature monitoring as wireless systems are not totally wireless. They include wireless communication but it is realized only between the central point of information of measurement and/or processing and the user's PC. The relationship between measuring instruments and systems to be monitored and controlled is done by wired connections as well as centralized data system.

The specific feature of wireless sensors used in these experiments (Figure 1) is the combination of three main elements that compose them:

- Measuring transducer (thermocouple, temperature sensor, etc.).
- Intelligence (hardware that can make decisions according to the directions taken in memory);
- Communication capabilities (transmission system - wireless reception).

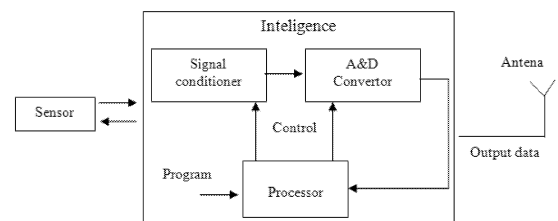


Figure 1 Block diagram of a wireless sensor

As can be seen in the Figure 1, the sensor is controlled by a microprocessor. In this way it is able to assimilate large amounts of data, to take autonomous decisions and thus to act adequately to achieve its objectives in any environment,



even if it is permanently changing.

This paper, presents the concept of a wireless temperature system with embedded intelligence, small dimensions, energy-range of 3 to 5 years, Internet access and control. This subject is also related with the concept of cloud instrumentation. Using this new innovative idea can be connected many sensors or equipment's over the Internet.

## MONITORING AND CONTROL APPLICATION

### Hardware development

For wireless measuring and control of temperature was used a laboratory furnace, embedded in the following systems (Figure 2):

- 1 laboratory furnace;
- 1 wireless systems for temperature measurements (WiTag);
- 1 router (Access Point);
- 1 PC.

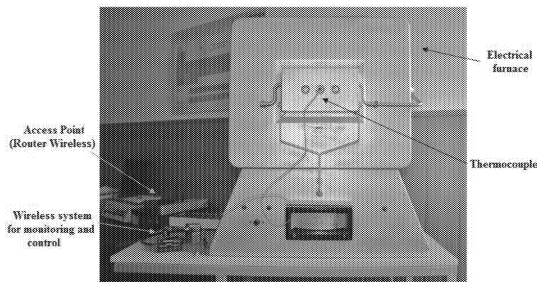


Figure 2. Practical hardware system

The central part of the WiTag system is represented by TAG4M system (Figure 3). This is an ultra-low power system that has an internal processor, analog and digital inputs and outputs, sensors on board and can transmit wireless information through an Access Point to a PC used as virtual instrument. The only thing that is required is to set a specific name and password for the router, the same that the TAG has in its memory.

The core 32-bit processor (or CPU) runs on a 44 MHz external clock. Sensor measurement operation is controlled by an external 32 KHz oscillator. The CPU incorporates full 802.11 PHY, MAC and encryption engine.

Taking in consideration the characteristics of the system had to be realized the following tasks: 1 analog input of voltage (14 bits, 0 – 10 V),

- 3 analog inputs of voltage (14 bits, [-200mV;+500mV]),
- 1 analog input of current (4 – 20mA),
- 4 digital outputs DIO,
- 1 sensor of temperature that is on board (thermistor 10K +/- 1C<sup>0</sup>)

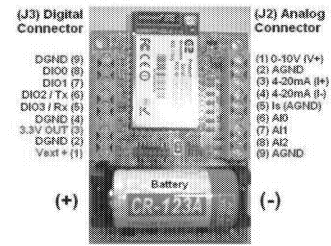


Figure 3 The TAG4M system

To have an accurate measurement due to the fact that the temperature limits can be high enough was used an external temperature sensor, a K type thermocouple, connected to the TAG. This type of sensors is used in general to control industrial applications where the temperature is between 0 – 1000 Celsius degrees.

### Software development

The software was realized by the authors of this publication in LabVIEW. The decision to choose LabVIEW as development environment first of all came from the idea that it is well known software for the development of virtual instruments useful in any field, especially in industry and second of all in our opinion it is the most suitable software for such applications.

Any application developed in LabVIEW consists of two distinct parts, closely interrelated: the user interface (Control Panel) is virtual instrument and the diagram that is the application.

In this case where developed two independent interfaces: one interface for the temperature monitoring and the other one for the control part. Their structure is similar in image and as functionality.

Monitoring interface (Figure 4) structure is easy to use because the information is organized in clusters. First, the user is informed about the identification data of the wireless system, such as MAC and IP address. Next, the user can set the time in which to carry out measurements and can choose which type of thermocouple to be used from a list populated with all types of thermocouples. For these input values, exist also output values representing by the current value of the measured temperature, which is displayed in a numeric and also graphical indicator.

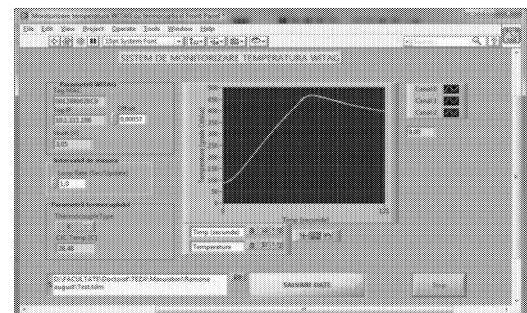
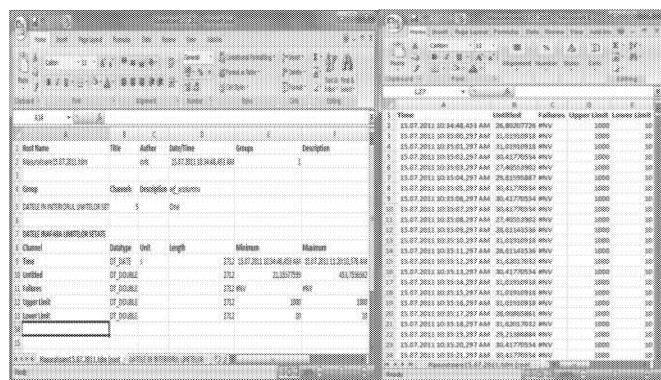


Figure 4 User interface for temperature monitoring

For reading data stored during temperature monitoring process, has developed a user interface. Within this, the user can select the file that wants to read from the database and the data inside will be displayed graphically. There is also the possibility to save data during the monitoring process or in a certain time depending on the user's desire. Saved data can be found in a database on user PC and includes two tabs, in the first tab are displayed general information regarding the equipment that is performing measurements (name, MAC and IP address) figure 5a, while the second one contains the actual measured data and how long it took the user to realize the measurements. Figure 5b.



a. b.

Figure 5 Saved file format (a. General information, b. Measurement information)

Control interface has a similar structure to monitoring interface. First, the user is informed about the identification data of the wireless system, such as MAC and IP address. Further, it can set the furnace so that the tuning parameters to be completed in one of three possible operating modes: P (Proportional), PI (Proportional Integral) and PID (Proportional Integral Derivative), Figure 6. The parameters represent the most frequent ways of operating for heating equipment's.

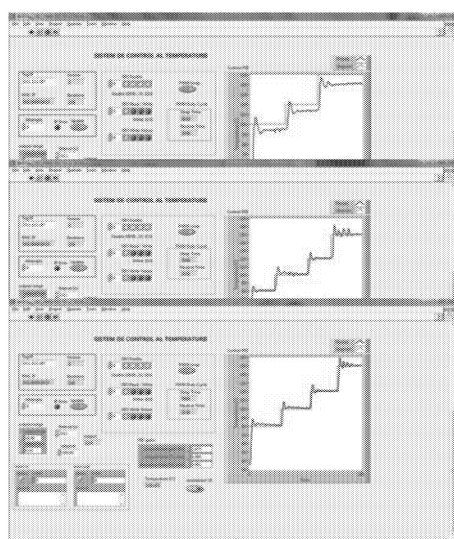


Figure 6 Control interface for temperature control during P, PI, PID processes

## CONCLUSIONS

The main idea of this development was to realize a temperature monitoring and control system for using remote technologies.

This research work proves that the wireless system developed (hardware and software) is able to manage in very accurate manner, temperature monitoring and control in P, PI and PID situations.

The final result of this research work proved that the system is able to:

- permit permanent and simultaneous monitoring from a control point by a single operator or heating a large number of processes;
- reconfigure the control point processes separately or simultaneously;
- to offer cheaper communications costs, given the current conditions on the evolution of Internet connection;
- reduce the costs of monitoring the process / month, i.e. the need for a small number of operators;
- possibility to keep journals of values, status and alarms for all monitored elements of the process; journals of actions taken by the operator;
- offers a friendly graphical user interface that simplifies operation and offers tabular and graphical report generation for any period. It can be: mean values and consumer quality, alarms, status items, actions of all others;

Using such systems leads to lower operating and maintenance costs and increase performance. But also, partial or total automation of the technological process provides:

- accuracy and uniformity in the operation of machinery;
- quality products;
- better working conditions, reducing the physical effort;
- increased productivity, a very important indicator of economic results - financial (reducing the number of persons);
- specific consumption of raw materials, energy within the limits of technical documentation.

## REFERENCES

- ALTGAUZEN, A. P. – *Instalatii electrotermice industriale*, Editura Tehnică, Bucuresti, 1975
- ALTMAN, W. – *Process Control for Engineers and Technicians*, IDC Technologies, 2005
- DUNN, W. C – *Fundamentals of Industrial Instrumentation and Process Control*, McGraw Hill, 2005
- HALIT, E. – *Wireless Sensors and Instruments Networks, Design and Applications*, Taylor & Francis Group, ISBN 978-0-8493-3674-4, Boca Raton, FL, USA, 2006
- KALANI, G. – *Industrial Process Control – Avances and Applications*, Elsevier Science, 2002
- KONAR, A. – *Computational Intelligence Principles and Application*, Springer Verlag, 2005
- NATIONAL INSTRUMENTS – *PID Control Toolset User Manual*, 2001
- OROS, R. G., JINGA, V., SAMOILĂ, C., URSUȚIU, D. - *New Technologies – WITAG for temperature and pressure monitoring in critical areas of chemical equipments*, Republica Cehă, Mai 2010

SAMOILĂ, C., DRUGĂ, L., STAN, L. – *Cuptoare și instalații de încălzire*, Editura Didactică și Pedagogică, București, 1983

TRINKS, W. – *Industrial furnances*, McGraw – Hill, New York, 1976

#### **WEB REFERENCES**

<http://www.g2microsystems.com/>

<http://www.tag4m.com/>

# Social Cloud for personalized information retrieval

Alexandru Agape

University Politehnica of Bucharest  
email: alexandru.agape@gmail.com

## KEYWORDS

Social Cloud, personalized information retrieval, web 3.0, social network, volunteer computing

## ABSTRACT

In this paper we propose a new distributed architecture for personalized information retrieval systems built on top of existing social networks. We show how volunteer computing can be applied to commercial applications by introducing a new Social Cloud based model for designing web information systems. By means of a multi-agent simulation we show the effectiveness of our approach.

## INTRODUCTION

Following the fast growth of world wide web (Berners-Lee et al. 1992) computer scientist around the world passionate by the internet focused their work on building the next generation of the web, the so called Web 2.0 (Lewis 2006). It harnesses the Web in a more interactive and collaborative manner, emphasizing peers' social interaction and collective intelligence, and presents new opportunities for leveraging the Web and engaging its users more effectively (Murugesan 2007). Web 2.0 new technologies allowed users to easily add new data to the web. Along with this, a new concept rose: Web 3.0 - giving meaning to that data, personalization and intelligent search among other things. Some argue that Web 3.0 is where "the computer is generating new information", rather than humans. Therefore, besides fast algorithms and efficient implementations, huge computing resources are needed. Designing a new generation web information system that would scale with the number of users requires a new development model, the same as Web 2.0 applications needed the asynchronous programming model to achieve its goals. Technological advances led to powerful personal computers. We propose a software architecture to make use of these resources (most of the time unused) and help one developing and deploying scalable web 3.0 applications without the need of expensive data centers or servers. We emphasize the role of Social cloud model for the future of the web by showing how volunteer computing can be embedded in a commercial web 3.0 application.

In the proposed distributed architecture the application server is used only for distributing tasks, storing and verifying results while the actual processing takes place on the machines of the users. The particularities of personalized information retrieval systems make them suitable for this kind of architecture. Small clusters (highly connected groups) of users would work together in processing data needed by all of them, and benefit of the results together. In order to keep user experience at a high level, we propose splitting the data processing in two or more phases, first one being faster but not very accurate and used for providing the user initial results while the main processing step is running.

To our knowledge, this is the first application architecture on top of Social Cloud proposed. We consider it the first design that shows the usefulness of the Social Cloud model, as the previous proposed ones are focused on the user and not on the application developer. It is also the first proposal of using volunteer computing in commercial applications, by forcing users to use their machines for computing their results. The role of the application server is reduced from executing tasks to only translating tasks in terms of computations to be done. The approach it is different from standard desktop applications because results of computations done by a user are shared with some of the other users.

## RELATED WORK

Introduced in Sarmenta (2001), volunteer computing is a form of distributed computing that allows "high-performance parallel computing networks to be formed easily, quickly, and inexpensively by enabling ordinary Internet users to share their computers idle processing power". Social Volunteer Computing (McMahon and Milenkovic 2011) is integrated within a social network and brings together volunteers, submitters, developers and facilitators. Chard et al. (2010) proposed leveraging the pre-established trust formed through friend relationships within a Social network to form a dynamic *Social Cloud*. This is a scalable computing model in which virtualized resources contributed by users are dynamically provisioned among a group of friends. Independently, Mohaisen et al. (2011) investigated recently a new type of computing paradigm they also called Social Cloud

that is more close to our view of what the Social Cloud should be. Similar to the conventional grid-computing paradigm, users can outsource their computational tasks to peers and use friends for storage. But it also exploits the trust exhibited in social networks as a guarantee for the good behavior of the workers in the system.

The problem with existing Social Cloud usage scenarios is that users sharing computational power usually join the cloud because they need more resources to run their tasks, so most of the time one will be running own tasks and wouldn't have resources to share. Our model is different of all of the above. Nodes of the social cloud share their resources implicitly by communicating with the central server and work together to solve tasks relevant to all implied parts. We don't deal with peer-to-peer communication. We make joining the cloud easy and attractive by hiding it in the application. We aim our work at Web 3.0 applications creators, and provide them a model to develop scalable computing intensive applications without the need of large computational resources.

## GENERAL ARCHITECTURE

Our system design includes three types of components:

- **central node** is a server hosting the application that translates high level task into computing tasks, distributes them among interested nodes, aggregates and store results and feedback, and serve results to the initial query to the user.
- **client nodes** are computers of the users, with limited availability, that process user query, solve computing tasks, display results to the user and gather feedback to improve results.
- **additional computing nodes** (optional) are processing servers provided by the application owner to verify results or increase processing power of the cloud.

Simple as it is, our system design is depicted in Figure 1. The data center appears as a separate entity connected to the central server, to make it clear that the application server would still need to be powerful and with a high storage capacity. We added the server corresponding to the underlying social network together with a sketch of the entire network. We marked the nodes corresponding to users inside the social cloud. The data flow tries to minimize amount of traffic: communication with the social network server is done directly by the node that needs the data. The central server takes queries from clients, distributes tasks and gathers results. This data is afterward stored in the database and served as response to user queries.

To show an example of a real world application using our model, we consider a query based image retrieval application on top of Facebook. In order to get a powerful system, there are two approaches to be

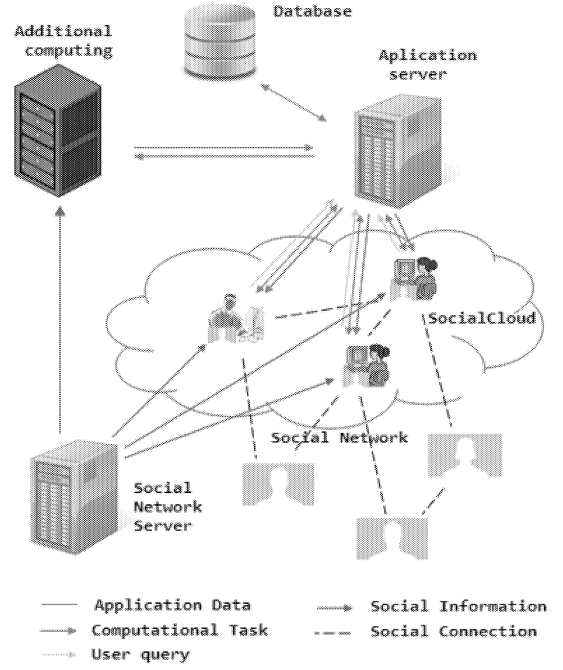


Figure 1: System architecture

combined: natural language processing and image analysis. First one would consist in retrieving all tags and comments for each photo, and index them. This would require some power but can't be considered a computing intensive task. On the other hand, analyzing one image, extracting features and running specific detectors (automatically assigning labels) is more expensive and qualifies for a second step of processing. A good system would include displaying intermediate results (those based on NLP in our example) and would prioritize the big tasks according to the results of those. The user can browse the results, and give feedback to the system in order to clean the results list for future times when he will issue the same query.

One other trending concept of Web 3.0 easy to embed in our model is crowdsourcing (Davis and Lin 2011). This refers to the situation where you use other agents to solve your tasks, and is achieved in our model by the feedback functionality. Another strong point of our model is that we don't have to deal with privacy issues because peers share only computation results, and through the central server.

## MULTI-AGENT SIMULATION

We build a simulation of the application described in the previous section. We consider a multi-agent system with pairwise connections between agents (the friendship relation). At the beginning only a small number of agents are considered to be part of the social cloud. Each agent has some data attached.

Dataset	Nodes	Edges	Citation
Karate	34	578	Zachary (1977)
Wikivote	7115	103689	Leskovec et al. (2010)
Slashdot	77360	905468	Leskovec et al. (2010)
Epinions	75879	508837	Richardson et al. (2003)

Table 1: Social networks datasets

Dataset	Small tasks				Big tasks			
	Best	Privacy	Greedy	Server	Best	Privacy	Greedy	Server
Karate	0.36	0.36	0.39	0.30	1.64	2.06	3.03	1.06
Wikivote	0.38	0.38	0.49	0.21	2.16	2.92	3.66	4.70
Slashdot	0.4	0.4	-	0.23	3.63	5.11	-	13.31
Epinions	0.39	0.39	-	0.24	3.45	5.07	-	12.09

Table 2: Average waiting time

The application needs to process the data of all the friends of an user of the application. As in the example, we consider two types of tasks depending on size.

Task allocation is an important point of the application we don’t tackle in this paper. Instead we consider the followings situations, two using a greedy task allocator (based on the number of nodes that need the result):

- **Best** — describes an upper bound of the performance of the system, considering that once it joined the cloud, a client node performs computations till the end of the simulation.
- **Privacy** — once an agent has all the needed results (for the computations it shares), it exits the cloud. The model considers a “God” task allocator and computes an upper bound of the performance for this more common approach.
- **Greedy** — similar to previous but with the greedy allocator. We could test this approach only for small datasets.

## RESULTS

We run the simulation on four different datasets representing real social networks that are summarized in Tabel 1. We evaluate the performance of our model for each of the three approaches and compare to the baseline solution of using a client-server architecture (modeled to have a power of 20% of the sum of computing power of all the users). We measure the average waiting time for an user till his preliminary and full results are available. Table 2 summarizes the simulation results. They show that our model doesn’t introduce big average delay in displaying results as compared to the traditional approach, and can even outperform it (with fewer hardware resources and less power consumption). Also, it seems that task allocation algorithms and privacy issues don’t have a high impact on performance.

## CONCLUSIONS

We proposed a Social Cloud based model for designing scalable Web 3.0 applications built on top of social networks, particularly personalized information retrieval systems. Giving meaning to data and personalization requires huge computing power. Our solution to this problem reclaims the unused computing power available to the user. We identified the application type that would benefit mostly from our design and proved the effectiveness of our design by means of a multi-agent simulation.

## ACKNOWLEDGMENTS

This work was supported by The Faculty of Automatic Control and Computers, University Politehnica of Bucharest.

## REFERENCES

- Berners-Lee T.; Cailliau R.; and Groff J.F., 1992. *The World-Wide Web. Computer Networks and ISDN Systems*, 25, no. 4-5, 454–459.
- Chard K.; Caton S.; Rana O.; and Bubendorfer K., 2010. *Social Cloud: Cloud Computing in Social Networks*. In *ICCC*. 99–106.
- Davis J. and Lin H., 2011. *Web 3.0 and Crowdsourcing*. In *AMCIS*.
- Leskovec J.; Huttenlocher D.P.; and Kleinberg J.M., 2010. *Predicting positive and negative links in online social networks*. In *WWW Proceedings*. 641–650.
- Leskovec J.; Lang K.J.; Dasgupta A.; and Mahoney M.W., 2009. *Community Structure in Large Networks*. *Internet Mathematics*, 6, no. 1, 29–123.
- Lewis D., 2006. *What is web 2.0? ACM Crossroads*, 13, no. 1, 3.
- McMahon A. and Milenkovic V., 2011. *Social Volunteer Computing*. *JSCI*, 9, no. 4, 34–38.
- Mohaisen A.; Tran H.; Chandra A.; and Kim Y., 2011. *SocialCloud: Using Social Networks for Building Distributed Computing Services*. *CoRR*, abs/1112.2254.
- Murugesan S., 2007. *Understanding Web 2.0. IT Professional*, 9, no. 4, 34–41.
- Richardson M.; Agrawal R.; and Domingos P., 2003. *Trust Management for the Semantic Web*. In *ISWC Proceedings*. 351–368.
- Sarmenta L.F.G., 2001. *Volunteer Computing*. Ph.D. thesis, MIT, Cambridge, USA.
- Zachary W.W., 1977. *An information flow model for small groups*. *JAR*, 33, no. 4, 452–473.

# DIGUA: MINIFIER AND OBFUSCATOR FOR WEB RESOURCES

Alex Ciminian and Ciprian Dobre  
Department of Computer Science  
Politehnica University of Bucharest  
Spl. Independentei, 313  
Bucharest, Romania

E-mail:  
[alex.ciminian@gmail.com](mailto:alex.ciminian@gmail.com)  
[ciprian.dobre@cs.pub.ro](mailto:ciprian.dobre@cs.pub.ro)

## KEYWORDS

Digua, minification, web, front-end, javascript, css.

## ABSTRACT

This paper presents Digua, a standalone library for minifying web resources. It is designed to be used for reducing file sizes of CSS, JavaScript and HTML files. A side-effect of minifying these resources is code obfuscation.

The novel approach in our solution is the fact that it can minify all elements of a website, and not just one type of resource. Also, it can detect the correlation between HTML, JavaScript and CSS and perform an all-round minification, therefore saving more bytes. There are no similar solutions available on the market today, technology-wise and functionality-wise. The main challenge is to preserve the code's functionality. It is hard to ensure that this type of operation will function across an almost infinite variety of websites, but we have taken steps to mitigate these risks through a flexible benchmark system.

## INTRODUCTION

The speed of the Internet has become the focus-point of many companies today. Serving content and applications as efficiently as possible is a challenge most developers have to face at the present moment. Faster load times usually contribute to a better overall user-experience that in turn leads to more content consumption online. This generates more revenue for content publishers as well as for advertisers so it is no wonder that big Internet companies are investing heavily in both creating and promoting tools that promise a faster online experience.

Our project is tied to the developer space of Internet speed. More precisely, we address optimizations in the front-end, because it has been estimated by analyzing HTTP traffic (Souders, S 2008) that for most web applications the user waits 80% of the time for the page's resources to be loaded. The other 20% is spent waiting for backend computation and for the html to be served.

We propose a solution that reduces file sizes in order to make web pages load faster. We do this by leveraging industry best practices (Souders, S 2007) (Souders, S 2009)

and offering users the possibility of applying these practices automatically to their projects. The solution is production-ready and can be used in multiple ways: through the command line, integrated in build environments (e.g. Ant, Maven). Further developments will make usable through a GUI or plugged into an application server as a filter. One of the project's objectives is to make it as easy as possible to integrate the minifier in a variety of workflows.

## STATE OF THE ART

There are multiple techniques that have the goal of reducing a website's load time and bandwidth usage. Minification is one of these; it is the process of removing all unnecessary characters from source code, without changing its functionality. These unnecessary characters usually include white space characters, new line characters, comments, and sometimes block delimiters, which are used to add readability to the code but are not required for it to execute.

Minification can be distinguished from the more general concept of data compression in that the minified source can be interpreted immediately without the need for an uncompression step: the same interpreter can work with both the original as well as with the minified source.

The reference implementations we compared our solution to are the YUI Compressor [Yah08], the Google Closure Compiler [Goo10], Dojo ShrinkSafe [Too07], Packer [Edw07], JSMIn [Cro03] and CSSMin [Scy04]. These are the most widely used tools in the industry today.

Among these, the YUI Compressor and Google Closure set of tools are the only ones that provide a wider range of options and supported formats when minifying web resources. Other tools focus on single file formats and are less configurable.

Packer is the most atypical tool from the ones analyzed. It is based on encoding the source JavaScript in Base62, a positional notation [Wik11] that yields very good compression results. However, this does come at a cost - there is time spent on the client 'unpacking' the original source code, and sometimes it may be more than the time saved downloading the file! This is highly dependent on the type of hits the application is expected to receive. If visitors

are expected to return often, packer is disadvantageous because of the extra CPU load it incurs on decompression.

## ARCHITECTURE OF THE SOLUTION

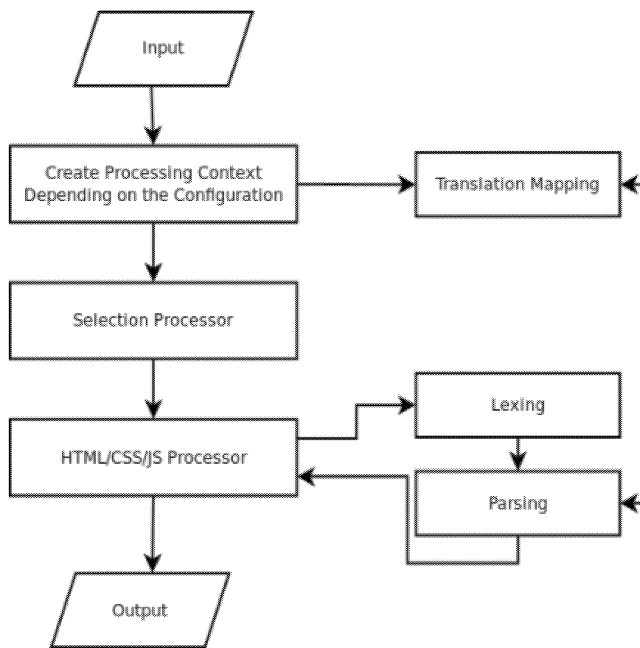


Figure 1: Program Flow

### Input and output

The input and output operations are abstracted through a set of classes that implement the `Source` interface in our project. They are flexible and genericized, thus make Digua usable in a variety of contexts. The project currently supports `File`, `Directory` and `String` Sources (for direct text input). There are plans to implement `ServletRequestSources` so that the library can be plugged into an application server as a `Filter` (as specified in the Java Servlet API reference [Or11]).

### Context

The context holds references to the input and output sources for a transformation and the map of translated variable names. It also can be passed a reference to a parent context from which a common map of translated variables can be read and the processors can be kept in sync. The context also holds references to two Sources that determine how the input and output are handled. A context must be passed in each processor.

### Lexers and Parsers

The lexers and parsers are automatically generated from our grammars via ANTLR. While the Lexer is left as is, the parsers are heavily modified and contain the logic that does the actual minification of the code. All Parsers inherit from the `DiguaParser` abstract class which makes the Context available inside inheriting parsers and contains the common token filtering and output logic.

The minification rules are passed inside the grammars. For example, let's take the case of minifying HTML colors. In CSS, the colors can be specified in hex format or, for a few of them, as plain English color names. To make all paragraphs on a page red, one could have a rule like `p { color: #ff0000; }`. The hex color can be written in condensed form as `#f00`, or even better, as `red`. This simple optimization can save up to 4 bytes for each declaration. An example on how this is achieved can be seen in this gist[Cim12].

### Processors

The processors are the classes doing the core work. They take the input, process it, and output the results. The source and destination are determined through the context being passed into the process method specified by the processor interface.

For processors that use lexing and parsing, the lexer and parser are referenced internally, through their respective classes. The processors may host content specific methods (for example, function translation is specific to JavaScript) that can be used in the parser and lexer (the processor is itself passed as a property for those classes). The abstract `ParserProcessor` is extended by all classes that use parsing. It instantiates the respective lexer and parser classes at runtime, so there is no need to duplicate the interface method `process` in the specific classes that extend it (`HTMLProcessor`, `JavaScriptProcessor`, `CSSProcessor`).

We also implemented several "utility" processors. The `SelectionProcessor` can choose the right type of processor based on the content type of the input. The `SerialProcessor` can be used to chain processor calls, for example to output minified CSS directly from a LESS preprocessor file. The `ParallelProcessor` can be used to speedup the minification time for multiple files by processing them in separate threads. Figure 2 shows the tree structure of the processors.

### Translators

The translators determine the names of the variables, ids, functions etc. after minification. There are several strategies for translating variable names and are all configurable. Digua can translate only local variable names and not modify the global ones. It also can generate random variable names in the minified version thus obfuscating the source. Alternatively, it has the option of generating sequenced variable names, which make the source, if unminified, easier to understand.

The translation of names is being kept consistent by a shared map, per processor. For example, in the case of processing a full directory, there would be several Translators invoked (for JavaScript: a translator for local variables, one for global variables, one for function names)



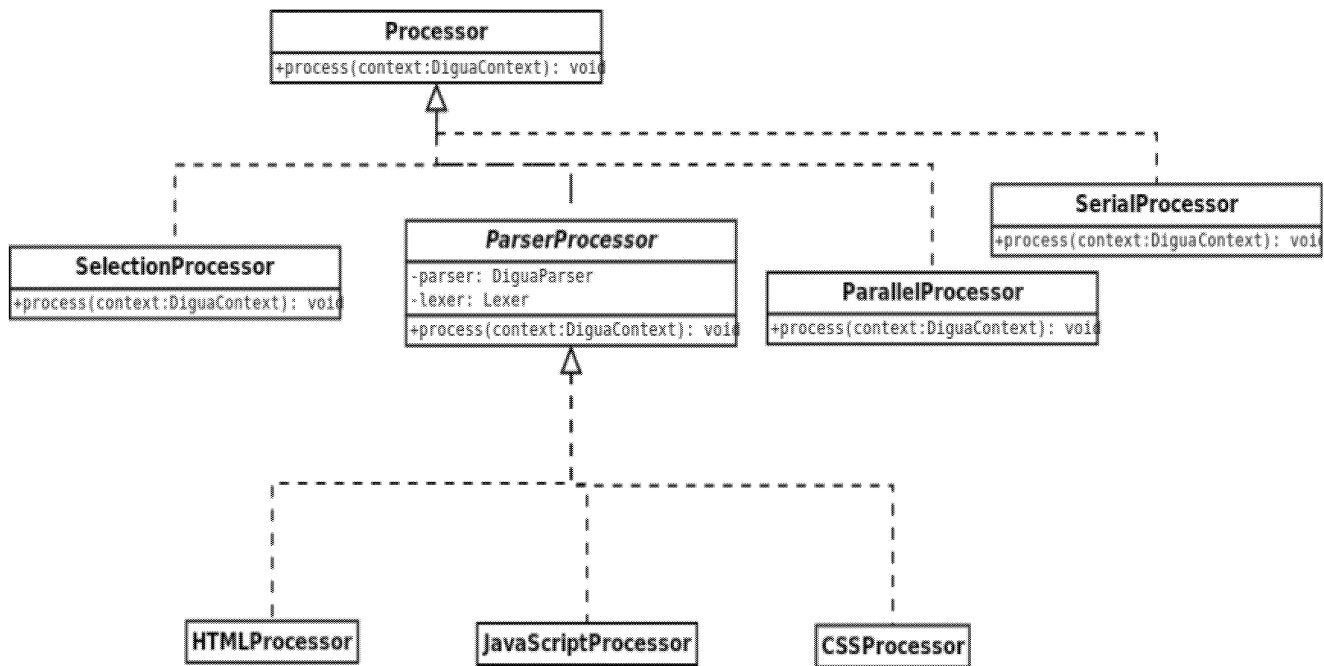


Figure 2: Processors Diagram

but only one translations map which would be held in the parent context of the application.

### Technologies Used

The main part of the project is written in Java. To generate the parsers and lexers we used the ANTLR library. The available grammars for HTML, CSS and JavaScript were tuned for the scope of our minifier.

We implemented the project's build system with Apache Maven. This allows for automatic dependency resolution and enables the project to be integrated easily in modern builds. Also, by using Maven we provide seamless integration with the Eclipse IDE, since you can generate the project files from the POM.

The benchmarking is done by running a shell script that in turn calls a python script configured through JSON. We used git to retrieve the actual tag for the source code we compressed and validated, but we also ran tests on custom HTML, CSS and JavaScript.

### Contributing to the Project

All the code associated with this project is open-source (released under the Apache 2.0 License) and is hosted on SourceForge. By having the project on SourceForge [BC11] we also make use of their hosted apps like MediaWiki as documentation, Mantis as a bugtracker, code versioning via SVN and a presentation website for the project.

### CASE STUDIES

There are two different directions we approached when evaluating our solution. The first one was comparative: we wanted to see how Digua fared against the top open-source libraries that have the same objective. The second one was absolute: we wanted to see what kind of performance improvement a user would hope to have by using our solution on a complete webpage. This second approach could not be included as a comparative test, since Digua is the only library offering this functionality.

We compared our solution against the libraries we mentioned in section 2. None of them provide the full functionality that Digua offers, but we crafted our tests around the features that our competitors support.

The benchmarking was done using a python script (open-source, available in the project's repository). The script is externally configurable through a JSON file; new tests or new frameworks for the comparison may be added just by modifying that file.

### Compressing jQuery

The first test features the reduction in file size obtained by each library when run against the latest stable jQuery source code file. The file was initially 161.5 KB in size. The test results are depicted in figure 3.

Dean Edwards' packer library fares best when compressing jQuery. This is because packer actually encodes the source JavaScript in Base62 and does not perform the tokenization that all other libraries, including Digua, perform. The tradeoff between the reduction in size and cost in computation time can prove to be a drawback, especially if you fewer fresh visitors than returning ones.

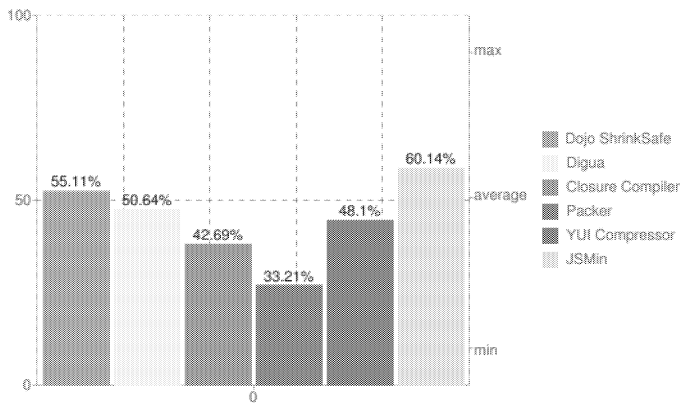


Figure 3: jQuery minification comparison

There were no validation tests run for the jQuery minification because of a bug in the way the tests on the library are run. In short, the jQuery project is made up of multiple source files that get 'built' into the resulting framework file. There is currently no way to run the tests on a single-file source (whether it be minified or in its initial state), although the test suite claims to work in this situation. This is a bug we reported to the jQuery core dev team and will probably be fixed in future releases.

### Compressing prototype.js

This test was similar to the one performed on jQuery, the only difference is that it was run on the Prototype JavaScript framework. The original source file measured 126.7 KB. The same procedure was followed: checkout the latest stable tag from source control, build the source and run the minifiers against it.

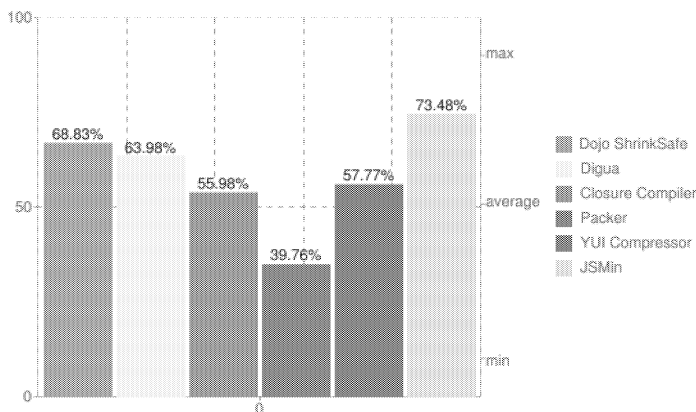


Figure 4: Minifying prototype.js

The main difference is that the prototype test suite could be run against the minified source, so we were able to validate our result as being correct. This is important moving forward, especially for the introduction of new features.

### Compressing a Wordpress Theme's Stylesheet

We tested CSS compression against the only two other libraries in our benchmark that offer this functionality (YUI and CSSMin).

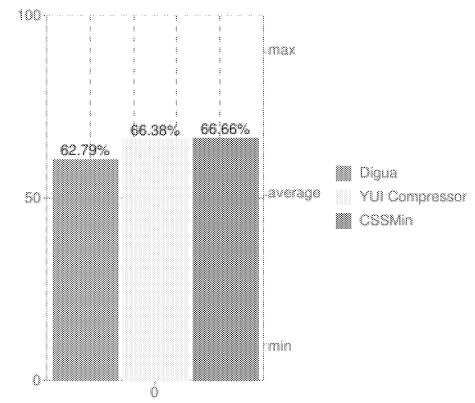


Figure 5: Minifying a Wordpress Theme Stylesheet

The results listed in Figure 5 show that there is not much room for improvement here, all libraries fared more or less the same. Also, there was no point in trying to validate the compression as it does not make much sense without an HTML context file on which to apply the styles. The target for compression was a rather large (16 KB) stylesheet file for the Glassical Wordpress CSS theme.

### Full Webpage Compression Tests

We ran two benchmarks for full webpage compression. In the first scenario we tried to think of a typical website that loads the minified jQuery source but also tries to load several unminified plugins. No minification was assumed on the part of stylesheets and HTML. The results are promising (Figure 6: the overall reduction in size is of almost 35%. The initial size was 107.7 KB. This is significant, and considering there is almost no difficulty involved it is by far worth the effort.

The second benchmark was for a website that already minifies its external resources, but does not run a solution over all its components. We took the Smashing Magazine homepage as an example - they are a leading resource for web developers and have extensive coverage of best practice techniques. We saved the webpage locally and ran digua over all the downloaded resources. This resulted in an almost 5% drop in overall size (we excluded the images from this calculation, as they were not processed in any way). Although, in the context of serving compressed resources this may not amount to much it may be significant for websites that have millions of pageviews per month.

### CONCLUSIONS

The architecture of the library is easily extensible. New input and output sources can be added so that it can fit in any context, whether it be inside an application server, in the command line, in a graphical interface or in a web environment. To improve processing, hooks can be added in the grammar and functions may be implemented in the Processor classes (as described in the color minification example). To provide better obfuscation, additional translators may be implemented that yield even harder to understand code than the Random one present in the

project. The minification is designed out to be configurable, although the interface for configuration is not currently exposed to the user.

The benchmarking we implemented will prove to be very valuable in the long run because it is very easily extensible - new tests can be added just by modifying the configuration file. The automatic reporting provides easy to read results in a matter of seconds (almost all the charts in this paper were generated by the benchmarking script).

The comparative tests will help us improve Digua by showing us which libraries do a better job of compressing certain resources thus pointing out certain features we can implement so that it will yield better results. The available automated validation is going to help in implementing these new features, because it can quickly confirm that they do not break the minification process and will speed up development time.

While it still lags behind the industry leaders (Google, Yahoo!, packer) when it comes to minifying JavaScript, Digua's overall performance makes it a good choice as a minification tool. As speed is beginning to be seen as a feature, minification is being implemented on a larger and larger scale. Digua's versatility when it comes to the way it can be executed we hope will determine people to use it.

The project is open-source and will remain that way. A large part of this document, after it is processed, will be used as documentation for developers wanting to contribute to the project. We hope to attract as many interested people as possible because that is the best way to make the project grow and to improve its performance as much as possible.

## FUTURE WORK

One important feature that currently the project is lacking would be to implement an external way of configuring the minification process. This would be available to the end-user without forcing him to modify the library's source code in any way. The code is designed well in this respect, but there is still a lot of logic to be implemented. For example, if one was to specify a JavaScript file as an input to Digua and that file contained a comment in the form:

```
/*@Digua.include ( 'other.js' ) */
/*@Digua.transform.variables.global=false */
```

It should also trigger the minification of the other.js file, but without transforming global variable names.

## Integration with CSS preprocessors

Another feature that is currently lacking is integration with CSS preprocessors, such as LESS or SASS. These could be used with the SerialProcessor and would allow seamless integration for developers that rely on these tools to keep their stylesheets maintainable.

This is a feature that has not been implemented by any other library among the ones which we studied, although Google's Closure tool suite offers a CSS preprocessor of its own.

## Graphical User Interface

The previous version of Digua also contained a graphical user interface, but the architectural changes in the present version have made it incompatible with the project's current state. A future development would be rewriting the GUI code. Although initially written to function with Swing, using SWT would make it easy to integrate with the Eclipse IDE. Distributing it as an IDE plugin would make it more attractive to developers and could increase the project's adoption.

## Performance Enhancements

Implementing new features for minification may prove to further reduce file sizes. The groundwork is laid out for this, including benchmarking, validation and easy way to develop features so we hope to further increase the performance of the project in the near future.

## ACKNOWLEDGEMENTS

A special thank you goes out to **Adrian Ber** who started this project in 2009 and wrote the first two versions completely on his own. His support was essential for the code contributions made in this new version and in the writing of this paper.

The research presented in this paper is also supported by the national project: "TRANSYS Models and Techniques for Traffic Optimizing in Urban Environments", Contract No. 4/28.07.2010, Project CNCISIS-PN-II-RU-PD ID: 238.

## REFERENCES

- Souders, Steve. 2007.  
*High Performance Web Sites*. O'Reilly Publishing, CA.
- Souders, Steve. 2009.  
*Even Faster Web Sites*. O'Reilly Publishing, CA
- Souders, Steve 2008 "High-Performance Web Sites"  
*Communications of the ACM* 51, December 2008, p36-41.

## WEB REFERENCES

- [BC11] Adrian Ber and Alex Ciminian. *Patu Digua Open-Source Project*. <http://digua.sourceforge.net/>, 2011..
- [Cim12] Alex Ciminian. *Usage Example: Hacking the CSS Grammar*. <https://gist.github.com/1738814>, 2012.
- [Cro03] Douglas Crockford. *Jsmín*.  
<http://www.crockford.com/javascript/jsmin.html>, 2003.
- [Edw07] Dean Edwards. *Packer*.  
<http://dean.edwards.name/packer/>, 2007.

[Goo10] Google. *Closure compiler*.  
<http://code.google.com/closure/compiler/>, 2010.

[Ora11] Oracle. *Java servlet technology*.  
<http://www.oracle.com/technetwork/java/javase/servlet/index.html>, 2011.

[Scy04] Joe Scylla. *CSSmin*.  
<http://code.google.com/p/cssmin/>, 2004.

[Too07] Dojo Toolkit. *Dojo shrinksafe*.  
<http://shrinksafe.dojotoolkit.org/>, 2007.

[Wik11] Wikipedia. *Positional Notation*.  
[http://en.wikipedia.org/wiki/Positional\\_notation](http://en.wikipedia.org/wiki/Positional_notation).

[Yah08] Yahoo! *YUI compressor*.  
<http://developer.yahoo.com/yui/compressor/>, 2008.

# **ONLINE COMMUNITIES**



# *CUSTOMIZED MODULATION OF VLE INTO AN ONLINE PARALLEL AND CLASSIFIED VIRTUAL COMMUNITY FOR EDUCATORS*

## *Arab Open University's experience*

Haifaa Elayyan  
Arab Open University  
ITC department lecturer  
Kingdom of Saudi Arabia  
helayyan@arabou.edu.sa

Hussien Mansour  
Arab Open University  
ITC department lecturer  
Kingdom of Saudi Arabia  
hmansour@arabou.edu.sa

### **KEYWORDS:**

Open learning, VLE, social networking services e-assessments, e-learning technologies, data mining concept and quality assurance.

### **ABSTRACT**

Arab Open university as an educational institution adopting the opening learning concept uses Virtual Learning Environment (VLE) , also known as Learning Management System ( LMS) as Virtual online platform for students to mainly build richly collaborative communities to deliver contents to students. This community assesses this learning process and provides many monitoring systems for quality assurance based on pedagogical model [1]. This paper argues the potentiality of running a well integrated parallel VLE associated with the students VLE but for educators as social networking service , they need to be well prepared with the essential e-learning knowledge and technologies assessed with all VLE e-assessments support to form an easily imported/exported repository to regulate their activities , conduct online workshops and lesson , monitoring systems for evaluation and classification forms using the concept of data mining; associative classifier , add of human resources inside the VLE, which is not being used inside the VLE before to maintain a complete record for quality assurance teaching progress purposes.

### **INTRODUCTION**

Virtual learning environments are web applications, which can be running on a server and are accessed by using a web browser that all VLE users and most importantly tutors and students can access the system from any place with an Internet connection.

This VLE gives educators a suite of tools to create a course website and provide access control so only enrolled students and tutors who teach this course currently in the running semester can view it [2]. The suit of tools also offers a wide variety of tools that can make a course more effective. They

provide an easy way to upload and share materials, hold online discussions and chats, give quizzes and surveys, gather and review assignments, and record grades only for students enrolled and tutors who teach this course in that semester . So the limitation of the usage is what we are targeting in our experience. For instance, the Limitation controls the access of other tutors from other courses to access and get benefits from the group discussions as long as they don't teach the course in the current semester.

In this research paper we attempt to build a cooperative community for all educators by using the facility of building a course cyber that can be accessed by all tutors for other purposes than just to assessing student, regardless they do teach this course or not .

The Arab Open University is a pioneer educational institution that adopted the open learning concept and has dedicated itself to form this concept and enhance it with advanced e-technologies. One of these e-technologies is an Open Source Course Management System called Learning Management systems Moodle, also called a Virtual Learning Environment (VLE). Such environments become very popular among educators around the world as a tool for creating online dynamic web sites for their students. As many institutions AOU, uses LMS as a platform to present a well formed, active virtual online community for students to participate and mainly to conduct fully online courses, use the activity modules (such as forums, databases and wikis) to build richly collaborative communities to deliver content to students. This community assesses learning outcomes using assignments or quizzes which based on pedagogical model.

These dynamic web sites are completely meant for students. LMS is being used to present a well formed , active virtual online community for students to participate in wide range of activities and mainly to conduct fully online courses, use the activity modules (such as forums, databases and wikis) to build richly collaborative communities to deliver content to students. This community assesses learning outcomes using assignments or quizzes which based on pedagogical model.

Modulation of the VLE for educational purposes takes it to the modulation of course WebPages and e-contents for full control and management of online assessments and evaluation of student's performance.

The main purpose of using these e-technologies is to upgrade the education progress, not to replace teachers. Unfortunately, tutors are missed in such platform as their access is limited to the courses they teach each semester while most of tutors who are with long experience in teaching can be an information reference for the beginners to share experiences and advices with other important facilities for tutors only to share and feedback. The new application can be done easily inside the same LMS used for students' assessments by dedicating a course webpage to be a gathering course for interaction among tutors; in our experiment we called it IT TUTOR Forum and it was directed to the IT department as a first experiment.

Following section explains in details how LMS serve students and tutors with regular use, taken the experience of AOU as an example.

#### ARAB OPEN UNIVERSITY: VIRTUAL LEARNING ENVIROMENT (VLE)

AOU uses Moodle as Learning Management System which is internet-based application as an interactive platform, controlling and managing material distributions, assignments, communications and so many other aspects of instructions for their courses for quality assurance as it is a vital for open learning institution like AOU. We can list a number of LMS features and how they might be useful:

Beside that LMS is friendly and easy to use, and popular with large user community and development bodies; LMS is flexible in terms of: Multi-language interface, advanced Customization, Separate group features, and pedagogy.

The users of AOU platform will be able to create files, connecting to websites related to a course and managing the e-contents of these courses. Further, the availability of a suit of *Activities' tools* related to creating interaction mediums such as: Discussion forums, Chat rooms, Quizzes, Messaging system, Submitting assignments and homework, Grading, Manage users logs, course catalogs, and activity reports , Manage competency (e-Tests, e-Assignments), allow personalization (user profiles, custom news, recent activity, RSS), Enable monitoring activities (QA, accreditation, external assessment) [3].

All the above mentioned features reflect the usefulness of LMS, these features are eventually directed to serve students and evaluate their assessments more than tutors whom their responsibilities are to guide students all through the semester to enhance the learning progress. However, our concern is to take care of those tutors, feed their expertise, make their

knowledge up to date, holding online orientation sessions, involve them in the decision-making process on the academic topics and other concerns are the purpose of creating the IT TUTOR FORUM.

#### ARAB OPEN UNIVERSITY NEW APPLICATION: IT TUTOR FORUM

Tutors who are the main educators in our LMS should grip our attentions and host our concerns. Hence, they need to be well prepared and have the essential knowledge to guarantee efficiency in their tutoring performance. A similar above mentioned application used for students targeting tutors and the impact of such experience are what this paper presents. Student improved assessments as described previously can be used to create a parallel adjustable environment and produce Internet-based global design to support a social constructionist framework in the same LMS used for students but for Tutors . Different fronts can be achieved with such application specially that AOU rely on part timer tutors whose their background is associated only with the offered courses per semester. Such community can provide tutors with customized human resources using activity module called database module , which can be customized in terms of fields, presets that record tutors' personal information ,photos, upload their resumes , their academic achievements and categorized and classified evaluation . Forming such an easily imported and exported repository which is mainly meant to regulate their activities , monitoring, and maintain a complete record for quality assurance teaching progress purposes [4] , also, such online community will help to prepare tutors and adopt them to work efficiently in LMS's frame by conducting online workshops for example , how to grade assignments , what a virtual class is and how to use it, how to write a sufficient feedback. Having bulletin board for regulations , announcements and reminders that are only for tutors, exchange experiences, discuss their concerns and forward their general complains as well as communicating with others by having a general group forums which is a built in activity module. Worthy to mention the valuable information can be retrieved from their questionnaire feedback and impact will be used in general statistics used for quality assurance purposes.

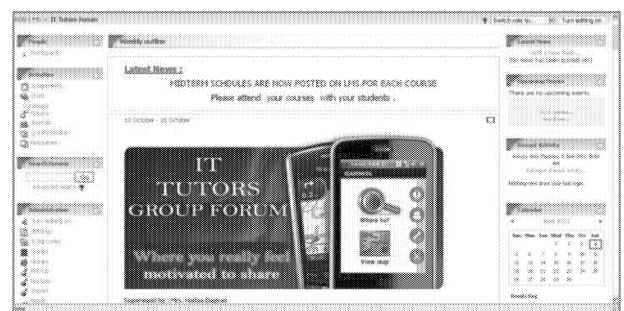


Figure 1. IT TUTOR FORUM



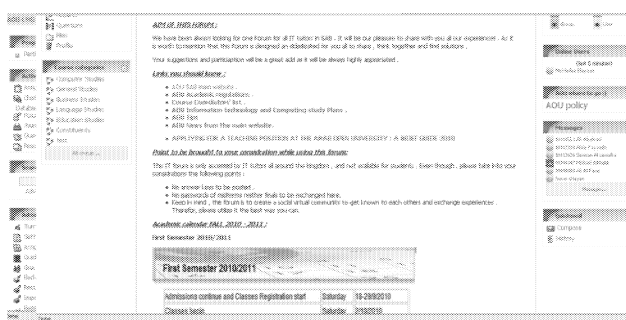


Figure 2. Aims of IT TUTOR FORUM

## IT TUTOR FORUM ASPECTS:

### Motivation of this new application:

The tutor forum is a course webpage customized for tutorship purposes. Groups that are allowed to access this webpage are only tutors who are teaching in the IT department as their first experience. They were added as non-editing teachers to run this webpage besides the other courses they teach in that semester.

Tutors were introduced to the idea and motivation of this customized webpage, and encouraged by continuous invitation to participate and share with other tutors who teach the same or different courses. As being a webpage inside a platform, the IT tutor forum is supported with all activity tools and features as mentioned before but this time it is for tutors only. We have been always looking for one Forum for all IT tutors in AOU. It will be our pleasure to share with all tutors our experiences as course coordinators. It is worthy to mention that this Forum is designed an dedicated for all tutors to share, think together and find solutions out of course limitations. All tutors were encouraged to post their suggestion and participations which will be a great addition as it will always be highly appreciated by the whole IT team.

### Updated lists:

As course coordinators responsible about running courses on LMS, we need to keep updating the tutors with all details that may not be related directly to the course tutor teaches such as, Course Coordinators' list of IT course as it changes every semester, study plan, AOU teaching tips and provide them with guide for applying for teaching position if they are interested in full time jobs.

### Reminding aspect:

This IT forum is only accessed by IT tutors all around the AOU, and not available for students. Even though, tutors were asked to take into consideration the following points:

- No answer keys to be posted.
- No passwords of midterms neither finals to be exchanged here.
- Keep in mind, the forum is to create a social virtual community to get known to each other and exchange experiences. Therefore, please utilize it the best way you can.

### Detailed information aspect:

The IT tutor forum is provided with all the details that cannot be exchanged where, as they are related to course coordinators and tutors who are not related to any course in specific. So information such as the explanation about the coordination system in AOU cannot be shared in any other IT course pages except here.

Not only coordination system, information about Monitoring of the Educational Process: is also necessary to be passed to tutors and explained here and will be archived for all tutors they may access any time.

In a multi-branch, as well as a multi-campus university like AOU, it is crucial to establish a set of explicit and well-defined measures to be implemented in all branches. The creation and implementation of such measures is fundamental to all aspects of the teaching-learning process, particularly with regard to testing, for it is through examining the performance of students on exam papers and other forms of assessment that an establishment can make sure which course objectives have been attained and which have not. Keeping such information will save time and efforts for course coordinators to explain every time for the tutors who just joined the AOU staff for example.

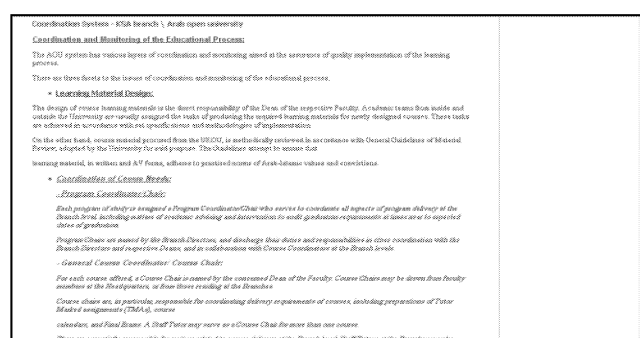


Figure 3: Detailed information

For example IT tutor forum provides well detailed information about assessments being based on three main types of written work:

1. Tutor-Marked Assignments (TMAs)
2. Mid-Term Assessment (MTAs) (formerly quizzes)

### 3. Final Exams (FEs) .

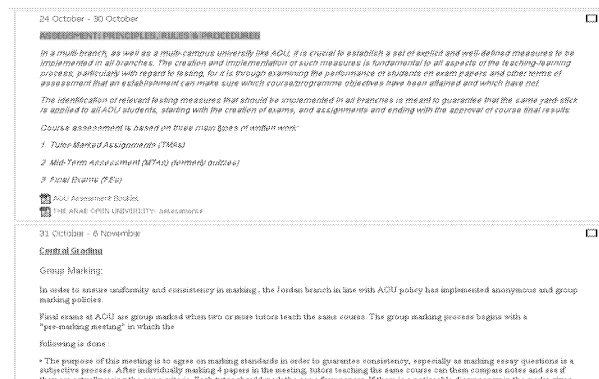


Figure 4: Rules of e-assessments

Many files can be uploaded and shared with tutors explaining about how to deal with these assessments and how to grade a TMA for example. Rules about Plagiarism for example can be also detailed here with examples and way to deal with. Explain the software AOU is using which is copy catch software and give online workshops and training how to use it

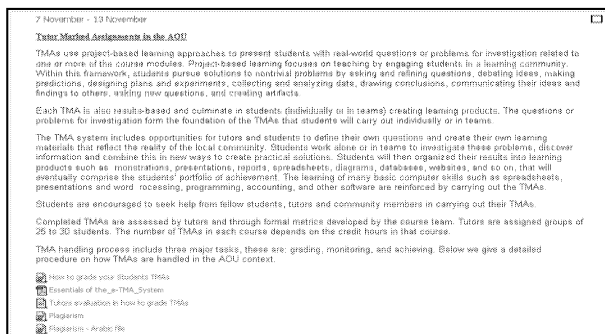


Figure 5: Share files with tutors .

The IT Tutor forum also took advantage of its database features to create the following two new ideas inside the LMS:

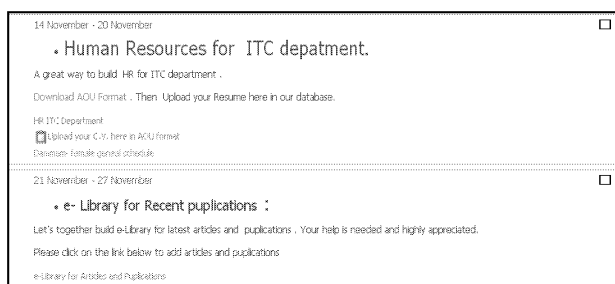


Figure 6: IT TUTOR FORUM databases

### Human resources:

The Online Human resources inside the LMS for part time tutors, by using the database feature of creating a template of AOU C.V. and asks tutors to fill and upload their pictures and also upload their copies certificates if they are needed. Figures 6 and 7 depict some sample from HR model.

To achieve the security for this level, tutors are actually divided into separate groups so they do not have access to the other C.Vs

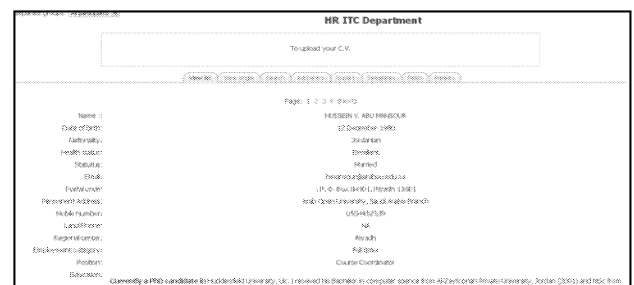


Figure 7 .Human resources database .



Figure 8 . Human resources : uploading pictures .

### e- Library for Recent publications:

Encouraging tutors to build an e-Library with the latest articles and publications specially about open learning for example, to post and collect recent publications they think are worthy to share. Figures 8 and 9 depict samples from AOU e-Library.

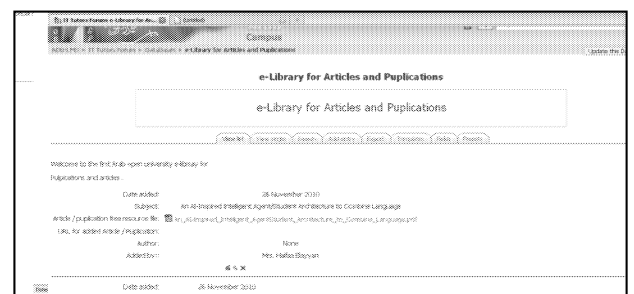


Figure 9: e- Puplication database

Figure 10: e-publication sharing and uploading .

## General Discussions and Questionnaire

The IT tutor forum is also uses the general discussion facilities to have a social networking discussing general issues or specific for any of IT courses. As well, questionnaire facility was used for example at the beginning of the semester to make sure that all tutors for example got their package at the proper time. The Questionnaire tool has a wonderful measurement that helps to assess the questionnaire for enhancement purposes.

Figure 11. Questionnaires and general discussions .

(a)

(b)

Figure 12: (a) & (b) Sample of the questionnaire

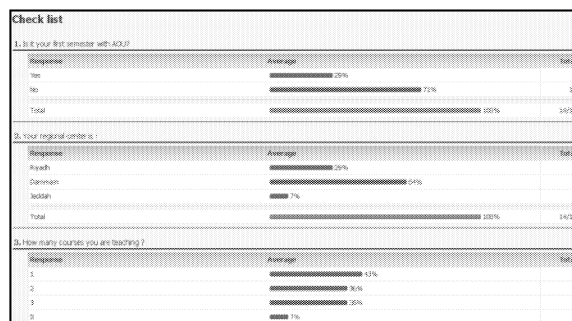


Figure 13. Assessing the result of the questionnaire

## RESULTS

Having the IT tutor forum for one semester has increased the rate tutors access the LMS, to go through a new experience they all enjoyed, participated and helped each other in the same platform they are asked to help students. Sharing the experience was a motivating reason to increase the logs and posts for each tutor. As an example, we have chosen Mrs. Mona who teaches the M211 course and has logged 1352 records as shown below:

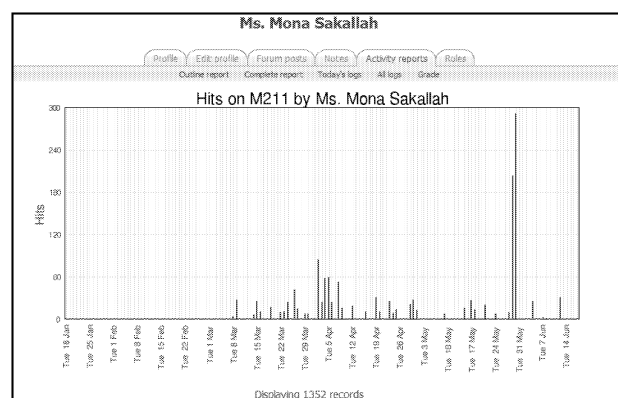


Figure 14: Logs record for regular course

Meanwhile she has accessed and enjoyed the experience of the IT tutor forum with its 4638 records

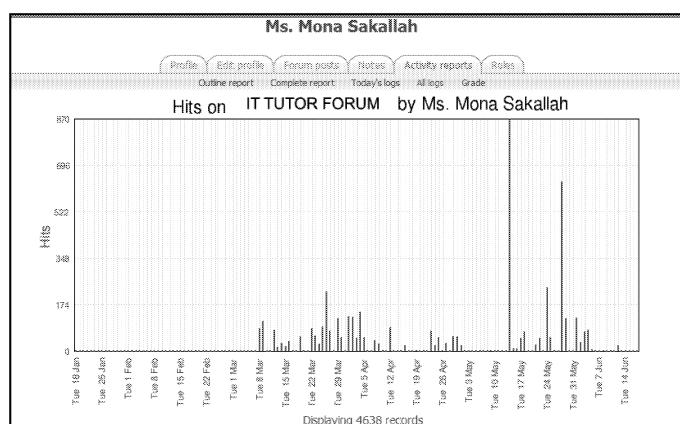


Figure 15: Logs record for IT tutor forum .

## CONCLUSION

IT tutor forum is a new application of using the LMS targeting educators in the purpose of providing them with information and get them ready for the education progress having a social community for them to communicate and share their ideas and talents. IT Tutor Forum is a monitoring and e-measurement systems of tutors' progress on such a platform that can easily integrated with an electronic evaluation form as specified in [5] which for sure comes for quality assurance aspects.

## BIOGRAPHY

Haifaa Elayyan, is an ITC lecturer and coordinator who works for the Arab Open University. She is a committed researcher with a solid background in web systems and has a lot of interest and high ambitions in e- technologies and e-solutions.

## REFERENCES

- Abdel-Elah Al-Ayyoub, Essentials of the e-TMA System for the Arab Open University, Arab Open University.
- JEP31004-2003, "Open Learning Modules and Technologies", an EC funded project jointly implemented with AOU, JU, and PSUT - Jordan, AU – Spain, IDEC - Greece, ORT – France, AIESEC – The Netherlands, and PLOCDIV – Bulgaria.
- Haifaa Elayyan , Saleh Al Saleem , eFundamental design of TMA activity module , <http://www.dline.info/jitr/ci.php>
- Jihad Al-Sadi, Bayan Abu Shawar, Taleb H. Sarie: Quality Assurance Procedures: New Enhancements to the Learning Management System at AOU. CSREA EEE 2006: 265-271
- Professor Taleb Sarie , The Arab Open University, Arab Open University, Jordan ,
- [www.moodle.org](http://www.moodle.org)

# COMPUTER TECHNOLOGY - A TOOL IN THE HAND OF THE ARTIST?

Canan Hastik and Arnd Steinmetz

University of Applied Science  
School of Media  
Haardring 100

D-64295 Darmstadt, Germany

E-mail: canan.hastik@h-da.de and arnd.steinmetz@h-da.de

## KEYWORDS

Demoscene, Digital Art, Multimedia, Preservation, Real-time

## ABSTRACT

Experimenting around with new media is essential for artistic work and the creation of new art forms. Looking at the Computer Demoscene, a European subculture, gives an insight into a generation of ambitious hobbyists who took up the heritage of the American hacker culture. Artists express themselves by experimenting with computer technology. With their practices of real-time-generated images and sound this youth culture scene extends the boundaries of technology. In the following, the scene will be analyzed to outline characteristics and criteria for ensuring a preservation of the artifacts of this sub-cultural art form.

## INTRODUCTION

The expression "tool in the hands of the artist" has a tradition. Currently there is lively debate in art history taking place, as to whether the computer can be understood as a "tool of practical art" (Institut f. Mathematik u. Informatik 2012), as a "production and presentation device" (Serexhe 2011), as "an artistic means of expression" (Klüttsch 2007), "a processed material" (Botz 2011) or an experience to "feel of materiality" (Heikkilä 2011). At the same time the idea of an artist only owning a software license as a tool has been established (Serexhe 2012). This discourse has an impact on the overall understanding and awareness of the value of computer-based creativity and the identification of sustaining and preserving artistic work and its components and will also have for future generations.

Only through deep understanding of a born-digital artwork, the use of materials and tools, the creative process and the social context, it is possible to develop solutions for a sustainable preservation and conservation strategy. Thus, the technical and semantic aspects of the Computer Demoscene representing complex dynamic media objects are being discussed.

## TECHNOLOGY RELATED SUBCULTURE

Niche cultures arise, driven by technical development, forming their own norms, values and specific practices. It is

not unusual for historiography that historical milestones are neglected because of commercial interests. Documentation often is incomplete or inconsistent. The same applies to niches in contemporary media arts like the Computer Demoscene which requires more attention than it currently receives. Only few research publications exist (Silvast and Reunanen 2004).

## The Computer Demoscene

The Computer Demoscene is one example for a subculture that still appears on the edge of the scientific domain. With its "Demo art" this creative subculture developed its own artistic expression. Having a deep knowledge on the machines and patience on examination, artists program and develop their artwork using sophisticated mathematical operations for manipulation and editing. The multimedia work "Demo" that arises consists of text, images and audio data encoded in zeros and ones.

The Computer Demoscene spread in the days of the Commodore 64 which has been "the most popular platform for a long time" (Stamnes 2012). In the early 80s a young anarchistic subculture emerged from hobby programmers and the Demoscene has become a community that creatively uses computer technology (Hitzler and Niederbacher 2010). Until the 90s the scene was closely associated with the "Cracker Scene". Demo artists initially developed small presentations in the form of concise thematic introductions for cracked home computer games. This so-called "Crack-Intro" was a start screen with logo of the cracker group, text messages and graphics as well as music. To complement their skills Demo Artists formed groups of programmers, graphics artists and musicians to demonstrate what they can get out of the given hardware. Over time artworks of real-time graphics, motion graphics and visual arts with more complex effects and a variety of elements were designed. Several forms of the Demo art originated which will be described and progressively analyzed below.

## CHARACTERISTIC OF DEMOSCENE WORKS

To conceive the defining characteristics of the Computer Demoscene a short historical overview will be given.

### Chronological Milestones

The roots of the scene go back to the beginning of

Computer-generated art in the early 50s. For a long time the works of the pioneers B. Laposky and H.W. Franke had been representative for achievements in this field (Goodman 1987). In the early 60s C. Csuri used computer technology to generate the first real-time animation. His artwork "Hummingbird" is exemplary for successful programming and the usage of computer technology as a medium for art (Csuri 2012). In the 70s computer technology reaches the masses with wide spread gaming platforms and games. When starting a copied game in the 80s, the "Cracker-Intro" also called "Crack-Intro" or "Cracktro" came up. A classic Cracktro composed of a logo, a colored font, various effects using the background color, a marquee with information on the game and greetings to friendly cracker groups. In most cases it also had music. Soon these artifacts became more spectacular than the games. While the scene always took advantage of advanced technology, various types of Demoscene artworks evolved. Each type can primarily be classified based on technical aspects.

### **Demoscene Material**

A sampling survey of the largest web repository (Pouet 2000) of news, groups and productions shows that Demoscene artworks basically can be categorized in "Cracktros", "Intros", "Demos" and "Wild". Intros are small presentations with one or two screens whereas Demos have more than two screens. Competition oriented Intros are being subdivided additionally based on size limits. Originally they were as large as a cracker could make room for the hack. Today's PC Demos may have over 80 megabytes in size (Breakpoint 2010). Demos subdivide into platforms they are designed for. Restrictions occur through size limitation and this classification is indicative to an important quality criterion and is regarded as a constructive challenge within the scene. The general rules defining these restrictions are not standardized. On top of that some products cannot explicitly be assigned to only one category or are not being categorized at all. This especially applies for PC-based and Wild Demo art works.

In total the use of over 70 different platforms can be counted, reaching from classic platforms like Commodore 64, Amiga and Atari ST to game consoles, handhelds, mobile phones, operating systems and graphical user interfaces. Usually the activity is proportional to the actual distribution range of the platform, but also the access to appropriate development software plays a role. For the development of Demo art the "hackability" of the platform is fundamental. With much effort Demo artists analyze and reverse-engineer the hardware, based on the Demoscene rule that "the hack value of a display hack is proportional to the esthetic value of the images times the cleverness of the algorithm divided by the size of the code" (Displayhack 2012).

The category "Wild" accounts for about ten percent of the sum of Demo art works and includes insane hardware hacks and developments like reverse-engineering CPUs to figure out the opcodes, development of flashcards and coding emulators (Team Pokeme 2005). Much smaller categories are procedural graphics, executable and tracked music,

games, video and web browser releases.

### **ELABORATED DEMO ARTISTS**

Cracktros, Intros and Demos are typically executable programs. Basically they have the following main characteristics (Borzyskowski 2000): They are not available for sale, they demonstrate capabilities of the graphic and musical artist and visual effects are generated in real-time. The source code of the executable computer program is not standardized and cannot be reproduced by commercial software. The complexity of these individual artworks is not comprehensible to an outsider. Neither does a non-programmer have access to the difficulty nor the programming skills in the field of undocumented hardware features, for example the creation of tricks to work around limitations of the GPU. Therefore Demo art is exemplary for technical and audio-visual sophistication and the difficult reproducibility. In this context a scene specific habit and creation process has been developed which is outlined below.

### **Sophisticated Programming**

Laposky's early experiments with analog switching systems are fundamental for the demonstration of the creative use of technology. Instead of oscillating voltages Csuri programmed functions and manipulated mathematical instructions with attributes. Like in Demo art sophisticated algorithms are used to display, manipulate or move objects on the screen. The more complex objects are being displayed the more impressive the demonstration will appear. A competition based on the realization of always more complex and elaborate programming tricks was started because of the limited options given by classical platforms. Object to object records were broken, better written calculation routines became faster and more efficient or new effects were discovered. The development of specific effects and designs depends on the technical skills of the artist dealing with the machine and the Demoscene's specific handling of the existing repertoire of resources.

Focusing on programming it is not easy to make Demo art technically impressive these days and pushing the limits by just combining effects with elaborate transitions. Most methods seem to be already "on the edge" but artists still try to push the boundaries even further. Graphics artists had access to a wide range of tools, features and effects. These were limited to the original color graphics modes and the specifications of the used hardware. Again through outstanding programming achievements and pioneering spirit existing limitations could be exceeded. For example special routines allow displaying up to 128 colors instead of the original 16 colors on a C64 screen (C64 Picture Gallery 1999). The musical productions were also influenced by the available software. However, it was not uncommon to improve them and make these add-ons available for free within the scene. These production techniques resulted in graphics designers and musicians working closely together with programmers in groups to enrich and optimize their artworks. These "Demogroups" consisted of up to twenty members.

Faster processors and more computing resources became available and programming changed - away from a hardware-oriented programming style to solving more abstract mathematical problems. The use of tools for the development of eye-catchers got popular. Nevertheless, it is expected that Demo artists will demonstrate their skills by pursuing the principle to generate “flashy bits written in custom assembly language and breaking every rules” (Shatz 1993). Still, there are various approaches of developing modular Demo editors or environments. To mention an example which represents a reflection of the basic principles of the scene in dealing with resources and materials: A specially developed editor (farbrausch 2000) allows generating all textures from the corresponding parameters and demonstrates how it is possible to compile all the space-consuming data out of a set of parameters rather than integrating readily painted bitmaps as textures in the Demo data file. Thus all materials like graphics, polygon models and music is generated by program code. Running for over ten minutes and generating 1.8 gigabytes of data, the executable program is only 64 kilobytes small (Fr-08: .the .product 2000). However editors, emulators or virtualization environments are definitely being used amongst Demoscene artists.

From the impressive artifacts that challenge the computer hardware the most, also compositional principles and styles have emerged and are maintained until today (Hartmann 2010; Tasajärvi 2004).

### **Established Aesthetics**

The structure of Demo art works is characterized by the use of classic elements. Objects got scaled up and down, rotated, deformed, moved and typically presented in fast-paced or even dancing scroll effects or animation. Graphics were animated using programmed routines. Animations were used on complex mathematically described objects and geometric shapes. Some classic old-school effects like the raster line interrupt and the Copper bar effect, both background effects that will display vertical and/or horizontal stripes of different resolution and color number on the screen, became typical for a composition. Other classic effects are tunnel flights, plasma, fire and 3D-effects. With the widespread use of PCs from the mid 90s and the related variety of hardware the community focused on computationally more intensive algorithms. A new era of the Computer Demoscene began. In contrast to home computers, Demo art on a PC may or may not work on another PC or the program code may be differently interpreted. Demo art development was changing; not only the technical masterpiece and the effects had to convince the audience, but also screen composition, color schemes and innovative ideas. Classic effects had to be reinvented or went out of fashion.

Currently the most significant contribution to the discussion about the aesthetics strategies and styles in Demo art is the doctoral thesis by D. Botz.

### **CRITERIA FOR THE PRESERVATION**

It can be observed that the use of new platforms will

always be based on the use of an existing repertoire. On the one hand active inventory, the backup and transfer of classical effects and principles of composition to new platforms is being practiced. On the other hand the new platform is used for more efficient implementation of established aesthetics. In this context new styles and principles are being developed. Besides that some artwork is ported to other platforms.

Demo art material contains static data like text, image, data lists, audio and video encoded in complex dynamic media archive files. Hundreds of different formats are available and mostly only the artists themselves have access to the original source code of the real artwork.

This leads to another important quality criteria and principle of the Demoscene: the factor “real-time”. By limiting the hardware and the size of the executable file not only comparability can be achieved but also the use of too many pre-computed animations will be avoided (Reunanen 2010). In fact, only with the knowledge of specific hardware requirements the “performance” of Demo artwork can be judged and can no longer be traced if it is isolated from the data storage medium and random access memory. But having videos of Demo art products ensures accessibility for the public.

The technical parameters which are specific for the design of Demo art are an important feature of the scene and its use of resources.

### **CONCLUSION**

The almost overwhelming variety of designs and forms of Demo art and the lack of historical distance to identify trends make it difficult to provide a classification and establishment of this creative and cultural activity. In addition to this multi-faceted Demo art objects the diverse usage of platforms challenges the development of sustainable preservation concepts and conservation strategies. Apparently, technology comes before the artistic inspiration and Demo art is no longer existent if the platform is untended. Through porting, versioning and citation the scene itself hands down materials referred to “classic” or “old-school” design principles and compositions and make them open to the public. Development environments, editors, programming languages or software applications which complement or simplify the creative process are understood as tools. These are mostly available for free.

The outlines of the technical and creative aspects make clear that the conditions of production have led to a characteristic Demoscene artwork practice. This practice is fundamentally related to applied mathematics. It should be noted that Demoscene artists have chosen a particularly complex set of tools with computer technology as a medium. Therefore Demoscene artists practice a particular cultural technique which stands for sustainability, tangibility, creativity and craftsmanship. The creativity is basis to create innovative works and the craftsmanship represents technical skills as a form of expression. Only through the right expression Demo art can be mediated.

The objective gets even more relevant when it comes to aspects of portability or interaction. Interactivity is not only a topic for the related field of electronic games, a small number of Demos also has interactive components. These criteria will be discussed in another paper.

## REFERENCES

- Botz, D. 2011. "Kunst, Code und Maschine. Die Ästhetik der Computer-Demoszene", Transcript Verlag, Bielefeld, ISBN:978-3-8376-1749-8.
- Goodman, C. 1987. "Digital Visions: Computers and Art". Abrams, New York. ISBN: 978-0810923614.
- Hartmann, D. 2010. "Computer Demos and the Demoscene: Artistic Subcultural Innovation in Real-Time". In *Proceedings of the 16th International Symposium of Electronic Art*, Funke, J. et al. (Ed.) Revolver Publishing, Berlin, ISBN: 978-3-86895-103-5.
- Hitzler, R. and Niederbacher, A. 2010. „Leben in Szenen. Formen juveniler Vergemeinschaftung heute“. VS Verlag, Wiesbaden, ISBN:978-3-531-15743-6.
- Klütsch, C. 2007. "Computergrafik: ästhetische Experimente zwischen zwei Kulturen. Die Anfänge der Computerkunst in den 1960er Jahren". Springer, London, ISBN: 978-3-211-39409-0.
- Reunanen, M. 2010. "Computer Demos – What Makes Them Tick?", Licentiate Thesis, Aalto Univ., Helsinki.
- Shatz, P. 1993. "Walkthroughs and Flybys", Waite Group Press, Corte Madera, ISBN: 1-878739-40-9.
- Serexhe, B. 2011. "Substanz und Ethik in der Konservierung digitaler Medienkunst", ICOM Deutschland. Mitteilungen 2011, Vol. 18, No.33, 8-10.
- Serexhe, B. 2012. "Digitale Herausforderungen". Digital Art Works: The Challenges of Conservation, 4-8.
- Tasajärvi, L. 2004. "Demoscene: The Art of Real-Time". Even Lake Studios, Helsinki.
- [Online] Available at [http:// stubber. math-inf.uni-greifswald.de/mathematik+kunst/ computer. html](http://stubber.math-inf.uni-greifswald.de/mathematik+kunst/computer.html), (Accessed 15 January 2012).
- Stamnes, B. 2012. "State of the Demoscene: 1991-2011". [Online] Available at <http://blog.subsquare.com/state-of-the-demoscene-in-numbers>. (Accessed 15 March 2012).
- Silvast, A. and Reunanen, M. 2004. "Demoscene Research Bibliography: Scientific Material Concerning the Demo Culture". [Online] Available at [http://www.kameli.net/demoresearch2/?page\\_id=4](http://www.kameli.net/demoresearch2/?page_id=4) (Accessed 15 March 2012).
- Team Pokeme 2005. [Online] Available at "Shizzle". <http://pouet.net/prod.php?which=16376>. (Accessed 15 March 2012).
- Pouet 2000. "Your online demoscene ressource". [Online] Available at <http://www.pouet.net/> (Accessed 15 March 2012).

## BIOGRAPHIES

**CANAN HASTIK** studied information & science engineering at the University of Applied Sciences in Darmstadt. Since 2011 she is a PHD student in the postgraduate research study program in corporation with CIT-Cork Institute of Technology, Ireland. She is a scientific assistant at IKUM – Institute on Communication and Media. Her main research interests are preservation and accessibility of complex multimedia objects in the field of electronic games and art, usability and knowledge representation.

**ARND STEINMETZ** is holding the chair of Multimedia Application and Technology inside the School of Media at the University of Applied Sciences (UAS) in Darmstadt, Germany and is adjunct Professor at the CIT-Cork Institute of Technology, Ireland. He is director of IKUM – Institute on Communication and Media at the UAS Darmstadt. As that his research interest is oriented in multimedia/media metadata structures and media technology and applications. He is currently leading research in two of the largest media archival programs of Germany's Federal Art Foundation (Motion Bank and Pina Bausch Archive). He is member of IEEE, ACM, GI and FK TG.

## WEB REFERENCES

- Borzyskowski, G. 2000. "The Hacker Demo Scene and Its Cultural Artefacts". [Online] Available at [http://www. schreib. net/ play/demos/ what/borzyskowski](http://www.schreib.net/play/demos/what/borzyskowski), (Accessed 24 January 2012).
- Breakpoint 2010. "Competitions and Events". [Online] Available at <http://breakpoint.untergrund.net>, (Accessed 21 January 2012).
- Csuri, C. 2012. "Early Computer Art". [Online] Available at <http://www.csuri.com/index.php/2008/12/early-computer-art/#more-382>, (Accessed 25 January 2012).
- C64 Picture Gallery 1999. "A Brief Description Of Graphic Modes". [Online] Available at <http://www.studiostyle.sk/dmagic/gallery/gfxmodes.htm>, (Accessed 21 January 2012).
- Displayhack 2012 "Displayhack – What is it?" [Online] Available at <http://www.displayhack.org/2011/about/>, (Accessed 15 January 2012).
- Fairlight 1987. "Beat it! – Jammin' II". [Online] Available at <http://noname.c64.org/csdb/release/index.php?id=27058> (Accessed 15 January 2012).
- Farbrausch 2000. "Fr-08: .the .product ". [Online] Available at [http://www. theproduct. de](http://www.theproduct.de), (Accessed 15 January 2012).
- Heikkilä, V.-M. 2011. "Materiality and the demoscene: when does a platform feel real?". [Online] Available at [http://www.pelulamu.net/countercomplex/ computationally-minimal-art](http://www.pelulamu.net/countercomplex/computationally-minimal-art), (Accessed 15 January 2012).
- Hurricane 1989. "100 Bobs". [Online] Available at <http://kestra.exotica.org.uk/demo.php?id=1975> (Accessed 15 January 2012).
- Institut f. Mathematik u. Informatik 2012. "Der Computer als Werkzeug der praktischen Kunst und der Kunstwissenschaft".



# Social Shopping Adviser: Recommendation platform based on mobile services

Elena Burceanu, Ciprian Dobre and Valentin Cristea  
Department of Computer Science  
University POLITEHNICA of Bucharest  
Spl. Independentei, 313, Bucharest  
Romania

E-mails: elena.burceanu@cti.pub.ro, {ciprian.dobre, valentin.cristea}@cs.pub.ro

## KEYWORDS

Recommendation, shopping assistant, mobile services, relevance score.

## ABSTRACT

As nowadays society is a consumer orientated one, choosing which goods to buy is a very common and time consuming activity. Developing an intelligent, social based recommendation system is a good way to overcome the problem of products information overload. Social recommendations for products refers to the fact that consumers trust a product more if there is a review (of any kind) for it, confirmed by many other users (in psychology this is known as Social Proof). Moreover, if the users that confirms it shares common 'tastes' with the consumer, not only that he/she will consider the product more reliable, but the 'good' will also match his preferences with a high probability and, therefore, he/she will prefer to buy the verified product. A social shopping adviser is what the following paper proposes. We present implementation details, together with experimental results designed to evaluate the system in a first prototype implementation.

## 1. INTRODUCTION

We live in a market-oriented society, where customers are constantly looking for the products that best satisfy their needs. Customers need information about products, they want to make the most informed decisions about the place to buy from, or which product to choose from many alike. Depending on person and product, customers might base their decisions on reviews given by (possibly familiar) people, or they might be willing to search for public information. The result is, nevertheless, a large amount of information that, today more than ever, can be near-impossible to sort and filter by humans, filled with irrelevant data or conflicting opinions. Many times we face decisions regarding what a product to choose (in a supermarket, for example) from a dozen possible similar choices - and all search engine results and/or opinions obtained on social recommending networks did little to help (many times contradicting results or opinions even harden the effort). All this make it difficult to find suggestions that would suit our needs. And even if we manage to filter the information and get accurate information about products, they might be coming from persons having opinions quite different from our own. Such evidence motivates the research of novel approaches based on 'trust' and 'tags based recommendation' in a social network context (Cantador, *et al*, 2010)(Sigurbjörnsson&van Zwol, 2008). The idea is to

let recommendations come only from close friends (where the term 'friend' is, even today, a disputed one, since the relation between two people can be established using different metrics, depending on the architecture of the social network and the targeted performances or objectives).

In this paper we present Social Shopping Adviser (SSA), a client-server system for recommending (in a social network context) products that have assigned a bar-code. Using modern-day technology, we aim to help the customer put in front of choosing between a large diversity of (almost) similar products or insufficiently described ones (regarding the aspects the customer wants to hear about). The client is overwhelmed with ads, and spends a lot of time choosing which product to buy, hoping to make the best decision for every decision he/she has to take. The mobile application uses barcode scanner data to find personalized recommended information relevant for each user.

We propose several novel contributions. First, we classify product information as: *relative data* (subjective data that depends on user preferences, such as 'what my friends like' or 'what tags am I am interested in') and *immutable data* (for instance 'what price has that product in a specific shop', 'what tags are associated with a product' or 'how does it look like'). Second, the system dynamically builds a *social network*, transparent to users, used only for product recommendation. This removes the privacy invasion feeling, usually given by a regular social network. Third, the system uses only a *small granularity* for each detail of a product. For example, when a user reviews a detail for some product, e.g. an incorrect photo of the product, he/she can vote only for the picture, not for all set of information, because the location or tags of the products might be correct. This way the wrong information is taken out of the system (with negative votes) without affecting good pieces of information. This leads to less effort from the clients to 'fill in' the correct details.

The rest of this paper is organized as follows. We first present several recommendation products related to the proposed system. We present the advantage of SSA, followed by a presentation of its architecture (in Section 3) and relevant implementation details (in Section 4). In Section 5 we present evaluation results for the proposed system. Section 6 gives the conclusions and presents future work.

## 2. RELATED WORK

The recommendation systems can roughly be divided in four categories (Kazienko&Kolodziejwski, 2006). Demographic

recommendation systems classify users by location (based on the user profile - statically and dynamically created based on history). Products are organized in classes and the user is interested in items from a class close to his profile. In collaborative recommendation systems the user manually gives ratings to items. There are recommended items with high ratings explicitly delivered by similar users (by profiles). The content-based recommendation systems are concerned with similarities between products. The products that are recommended are related to the recently (re)viewed ones, regardless of user preferences. Finally, in case of statistical approaches, the user is presented with products having a high score given by some statistical method (the best buy, the best rated, etc).

Such algorithms can offer either too weak or too powerful personalization (single session or taking into account user history). The problem with too personalized ones (collaborative and demographic) is that they require the user to register and fill in his personal data (which requires time, and raises privacy issues on the transactions).

Collaborative and content-based methods face the sparseness issue. If the user has an identity valid only in a session, there is too little information to process, and the recommendation is poor. Statistical and collaborative methods are not able to recommend new items to the user. The remedy for these disadvantages of recommendation methods consists in the use of hybrid systems.

Folksonomies, derived from the practice and method of collaboratively creating and managing tags to annotate and categorize content (Kazienko&Kolodziejewski, 2006)(Lee, *et al*, 2002), can also be used to perform collaborative tagging (Cao&Li, 2007), social classifications, social indexing, and social tagging. Recommending systems that use collaborative data can successfully be based on a folksonomy. In this case the score is created according to the vocabulary of the users, not that of the experts or of the program designers. Lee *et al* (2002) proposed a learning agent that does not recognize a consumer, but uses the information that user inputs in the system when he/she searches for suggestions. But the only problem aimed to be solved with the proposed solution is that of a customer that can identify the type of product he/she uses and describe its features. A customer profile, based on his past activity, is enough only for recommending frequently-purchased products. For others (such a laptop or a digital camera) expert advices are required (Cao&Li, 2007). The problems that occur are the synonyms, ambiguous words and phrases instead of words. Such systems have also to cope with the added noise to the search (in which case the quality or relevance of the results becomes questionable).

Several shopping recommendation application are also available today. TheFind (TheFind, 2012) is integrated with databases from lots of stores and offers more than an application (sign in, user profile based on static data, website support, integrated with Facebook friends and likes). But this is different from the solution proposed in this paper by the fact that TheFind is product orientated (not user orientated), and the social network is imported from Facebook (the system uses only social friends, not 'preferences' friends), not created ad-hoc, based on user

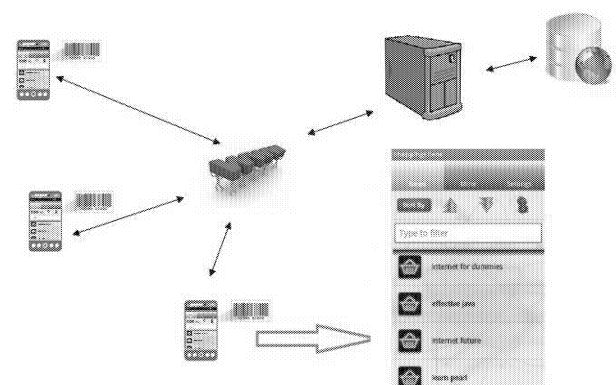
preferences. In TheFind the relations are static, compared with our proposed solution, where relations are dynamically and constantly modified.

Facebook Ads (FaceBookAds, 2012) is a shopping recommendation system based on diversity and decentralization of information. Based on semantic web technologies, the system classifies ads based on user's profile, in a non-intrusive way. The problem with these ads is that the heuristics are not exact, and the advertisers constantly push their ads disregarding the user's profile. Our proposed system uses complex information. The problem of information validity is solved by letting the users vote for every suspicious part of it. This way, you can walk through details provided for a product (from different users), and vote (positive or negative) for this reviews (given tags, price, location, etc). Also one can see comments for a product, comments that can add another detail level (information that is not integrated in the current details structure).

Comparing SSA with Amazon.com gives also common different points in algorithms main heuristics. Amazon is based mainly on the facts that people who bought an specific item also bought other specific ones and that people who rated an item highly also rated other items highly. Differences in using are that in order to access information from Amazon, you need to be logged in. Also, the database needs to be statically populated. Moreover, the user identity on Amazon is public; anyone can see the reviews posted by someone. Even if both approaches uses a preferences network, the one from Amazon starts from the product: who bought/rated high this also bought/rated high this, while the solution from this paper brings in a concept oriented on the user: when someone rate high other person's input in the system (not an item), the unidirectional friendship is increased. Nevertheless, our solution doesn't use semantics yet and Amazon does.

### 3. ARCHITECTURE

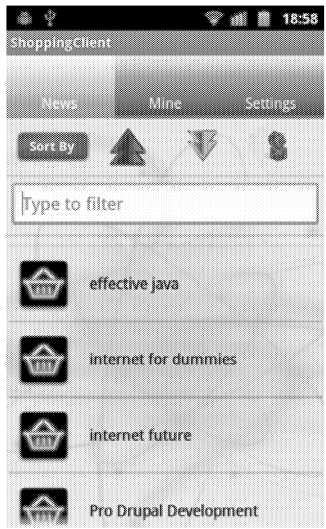
Our proposed system, SSA, dynamically constructs the relations between tags and trust. The end-results is a dynamic, ad-hoc social network of users (see Figure 1). Product recognition is accomplished using barcode scanning, using the client's device camera. The central server is responsible with all information management (products and users). The data is matched against the profile of each user, such that to be relevant to each user. All recommendation and trust algorithms run on this server.



Figures 1: The system architecture.

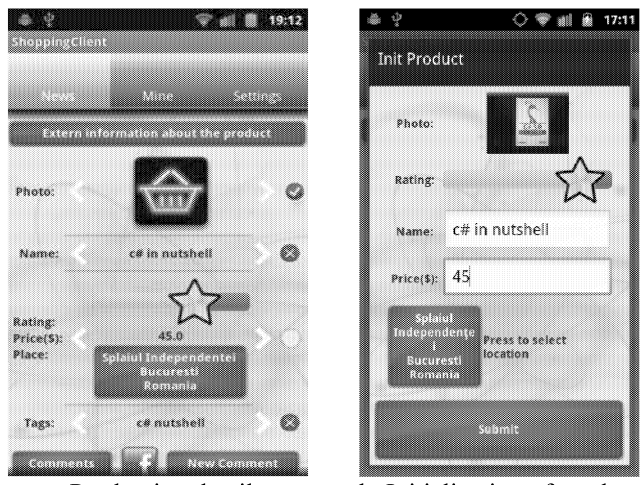
In this architecture the server is connected to a product database. Clients exchange data with the server directly from their mobile smartphones. They can interrogate the server (over the Internet), make a change in their personal settings, or submit a new vote for a review of an item.

A first prototype implementation of the mobile client-side application was developed over the Android platform. The application is composed of three main views: list of products retrieved from the server, the details of a scanned product, and user settings. Figure 2 shows a list of products, as retrieved from the server based on the trust recommendation algorithms and the current client context in the social network. From the upper buttons, the list can be either sorted or filtered.



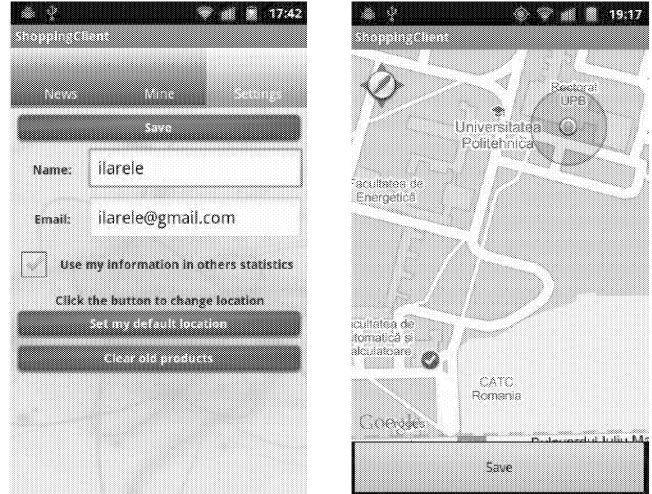
Figures 2: The list of products returned from the server.

Next, the user can scan the barcode of a certain product and communicate with the server to find relevant details about that particular item (Fig. 3a). He/she can click on any product and see details about a particular item. The details of a product are ordered according to the number of points (score) of each information, computed using the algorithm presented in the next Section. The user can train the system and insert details about products (Fig. 3b).



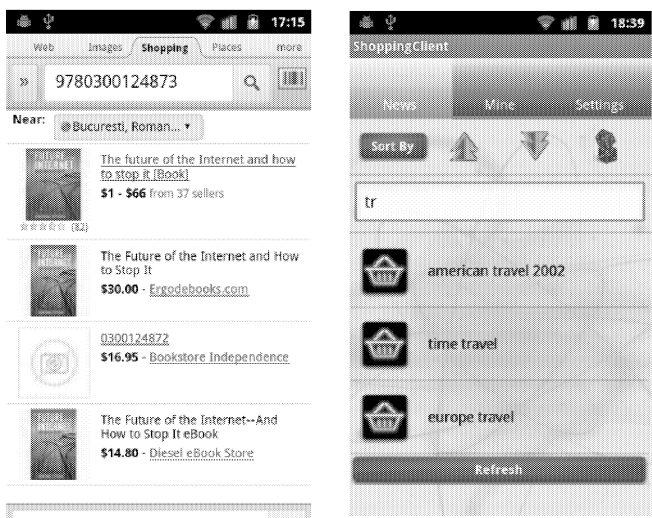
a. Production details. b. Initialization of product details.  
Figures 3: Product dialog.

The user can specify settings such as the name and email (optional fields, used when showing comments about products), his/her current location and the privacy settings (if he/she allow for activity recordings, or the set of preferences to be used to compute trust over the social network) (Fig. 4a). A location-based dialog (Fig. 4b) can also be used to specify a search for a certain products within a designated area, or the information inserted by the user (pictures of a product) can be augmented with location information.



a. Settings dialog. b. Location dialog.  
Figures 4: Personalized details.

The general data for a product refers to the information that does not depend on the user. For each product a picture (the quality of the picture may vary, but the one with the highest number of votes will represent the product) is required to better describe it. Also each product has a name, possible location data (where was spotted by users), rating, price (the price and rating are associated with different buying locations, but the price can also relate to a certain period of time – the price of a product from a specific location can vary in time), and tags.



a. Google product search. b. Filtered items.  
Figures 5: Searching for products.

The user can insert several details. The picture of the product is recorded using the device's camera. For setting the location, a map view activity can be used, with the default location being the current user location. Other fields (such as

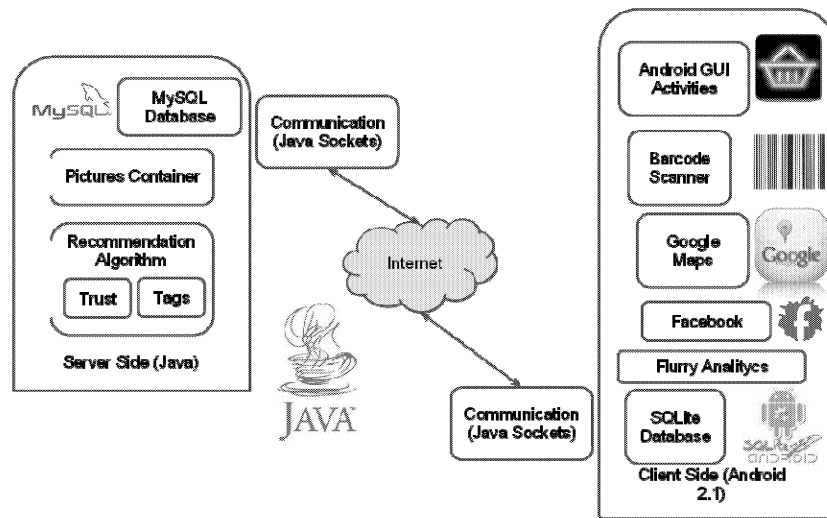
the rating, price, name, tags) can also be set by the user. He/she can even add comments for a particular product, or can be posted on Facebook directly from the mobile application.

The list of products retrieved from the server (Fig. 2) contains a brief description of the product description (picture and name). When touching a product the user is presented with advanced details about that product. He/she can find information about the product from an external source (via Google Product Search - Fig. 5a) or local to application (entered in the system by users of the application).

Every product detail can have multiple values, as inserted by different users. The ones showed in the dialog are those

having the highest rating. The user has the possibility to iterate through those values (back and forward) to the next value. He can filter the products (by name or tags, Fig. 5b) and sort them (by date, location, price - ascending/descending or random).

On the server side there are three main modular modules: a picture container (for storing the images associated with different products), a database (the prototype uses MySQL), and the trust and recommendation module (responsible with the execution of the algorithms, and the management of the trust relations in the virtual social networks, as well as tagged preferences). Those modules can be easily replaced by similar ones for testing different implementations (Fig. 6).



Figures 6: Modular Architecture and APIs.

The communication with the server is only initiated by the client. Pushing messages from server to a mobile device is expensive for the back-end because it needs a periodic scanning from the client (through a service running in the background). This implies a persistent connection to the Internet. Both the connection and the background scanning discharge the battery with a high rate. So, to avoid this major problem for nowadays mobile devices, the server never pushes information to the client. For an update, the client sends a request and waits for answers.

#### 4. IMPLEMENTATION DETAILS

The tag recommendation algorithm builds clusters of related tags. These clusters are computed based on the relation between tags (computed as the percentage of common occurrences in a description divided by the total number of occurrences for the first tag).

The virtual social network is dynamically built using the computing preferences of each user. The relations between users are used to compute the trust between any two users. The network cannot be modified manually, thus increasing the security level. The friendship between two users is computed as the 'friendship product' along the shortest path, and as an average weight for paths of the same length.

The resulted points for a product approximate the degree of interest that the user has for that product (how good it scales his/her needs for information about the product).

The server manipulates two types of data. The *relative* (subjective) one refers to which products a user might be interested in (not interesting in buying it, the user might want to know 'not' to buy a particular product). The score for this data is computed by the recommendation algorithm.

The *absolute* data refers to the details of a product for which the 'correct' value cannot vary too much between users: the picture of the product (if there are several pictures for one product, the user is presented with the most accurate one), the location and price (in a location, there should be only one single price for a specific product, in a certain time window). Also the associated tags should be clear (even if there are more sets of 'correct' tags, they are voted and the user will easily see the first entries from the list).

The recommendation algorithm is split in two parts: the first one selects the products, and the second one sorts them based on their score. The filtered products are the first  $n$  products to be shown to the user and are used as a base for the two main algorithms that rate products. The tag recommendation and the trust algorithms are used to decide the order of the products in the list returned to a specific client.

The static algorithm is the one that gives the details of the products, sorted by the voted results. When the user asks for a new detail of a specific kind, for a specific item, the returned result is chosen only based on number of votes for him (not in relation with the social network).

Next we present the tag recommendation and the trust algorithms, as well as the modality to combine them together.

#### 4.1. The tags recommendation model

The algorithm is executed: 1) when a product is saved with more than one tag associated (to update the relation between tags); 2) when the user adds a scanned product with tags (the tags points are incremented in the user tags list); and 3) when a user votes for a picture (selecting either location, rate, price) or a name (even if the vote is positive or negative, the tag score is incremented, because it means the user is interested in that product).

The server retrieves all products in the same cluster and sorts them according to their modification dates, and the relations between tags. For each product the client votes and product id are kept synchronized. Next, the server retrieves the tags associated with the user's preferences (based on its previous votes) and the product information. Only the tags that are rated positive are considered in this step. The algorithm iterates through the product tags and finds the ones related to the user's votes. For each of them, it searches for similar tags (in the same cluster), and normalizes the score, using the value of the common references for two tags divided by the total occurrences of the first tag (intuitively, this corresponds to the probability of the two products to be of interest to the user in the same search). In the end all products are sorted by their semantic relevance to the client.

In the prototype implementation, the recommendation score is computed based on the scores from the network of friends and from the score obtained by the tag preferences. The score of the product is  $score = score_{trust} + score_{tagsrecommendation}$ , where  $score \in [0, 2]$ .

The tags preferences are computed similarly. For each user, there is a list of (tag, points), updated based on votes, on the following actions: on taking picture (if an user take a picture for a product means that he/she is interested in that product, so in the product tags) and on voting for location, picture, name. The algorithm complexity is  $O(maxTagsPerProduct * (maxTagsPerUser + maxPrefTags))$ .

In order to reduce the noise from the results, we also eliminate some entries when computing the points for a product. This means that not only some results will weight very little, but they will not be considered at all. So, if the percentage of a tag is too small (below 1%), its contribution in the score computation is removed.

#### 4.2. Trust model

Similar to the tags recommendation, the relation between two users is formed whenever a user votes for other user's review. In this case, the friendship relation between the users is updated (positive or negative) (e.g. if user *A* votes for a

picture that *B* submitted, then in *A* friends list *B*'s rating is increased).

The relation between a user and a product (the interest degree) is updated whenever a user adds or comments a product (in this case he/she's interest on that product doubles), and when the user places a vote (the user's preference score is incremented by one).

The friendship network is asymmetric, so if *B* is a friend with *A*, user *A* is not necessarily a friend of *B*. If user *A* votes a detail (picture, name, tags or location group) about a product entered in the system by user *B*, then user *A* is added to the user's *B* friend list with the proper rate (the vote rate is added to the current rate that *A* has in *B*'s list).

Given a product id (*idProd*) and a user id (*toId*), the trust algorithm first finds the users interested in a certain product. It computes an average of the trust between the initial users and each of his friends. This last value is computed like:

Table 1: The algorithm for computing application permissions.

```
Set fromUserFriends ← fromUser.friends.
    entrySet();
fa (Entry friendEntry : fromUserFriends) {
    String friendId ← friendEntry.getKey();
    if (friendId == toId) {
        Float friendPoints ← friendEntry.getValue();
        Float interesRate ← getInteresRate(toId,
            idProd);
        if (interesRate > 1) interesRate = 1;
        friendPoints ← friendPoints /
            users.get(toId).numberContributions;
        if (friendPoints > 1) friendPoints = 1;
        return friendPoints * interesRate;
    }
}
nextLevelFriends.add(friendEntry);
...
```

The algorithm goes through the graph of friends in a breath first order, starting from the client id who's friends we are interested in. If any of them is the destination user, the algorithm finds the points that determines what is the relation between that user and the product (*interesRate*) and multiplies it with the 'friendship' that labels the edge in the graph (*friendPoints/allFriendsPoints*). Then we go on the other levels:

Table 2: The algorithm for computing application permissions (the case of subsequent levels).

```
float secondSum ← 0;
int secondNo ← 0;
fa (Entry secondLevel : nextLevelFriends) {
    String secondId ← secondLevel.getKey();
    Float secondPoints ← secondLevel.getValue();
    Float interesRate ← getInteresRate(toId,
        idProd);
    if (interesRate > 1) interesRate = 1;
    secondPoints ← secondPoints /
        users.get(toId).numberContributions;
    if (secondPoints > 1) secondPoints = 1;
    secondSum += secondPoints *
        getTrustFromTo(secondId, toId, idProd,
            alreadyChecked) * interesRate;
}
```

```

    secondNo++;
}
if (secondNo == 0) return 0;
return secondSum / secondNo;

```

The friends from next levels are 'friends of the friends'. Their score is computed in a similar way with the first level friends. The difference consist in the fact that their friendship points are computed as the parent trust, multiplied with last edge value (the score along a path is the product of the edges). The score is normalized:  $score_{trust} \in [0, 1]$ . The algorithm only measures the trust in a friend 'taste'. The algorithm complexity is  $O(maxFriendshipLevel * \log maxFriendshipLevel)$ .

## 5. EVALUATION AND RESULTS

To evaluate the system, we considered several book products. In the first evaluation scenario we considered the case of a user performing several operations: registering into the system, scanning, saving the list of items, taking picture, updating location, submitting reviewers, and updating data associated with certain books.

In the second evaluation scenario we cleared the database, added using the mobile application 30 books from three different domains (Computers, Cooking and Travel), created seven user profiles, used the existent books, checked the recommended products to see if they match the user's wanted profile. Finally, in the last evaluation scenario, the group of test subjects was divided in two. The first group was asked to search for the information on books using a popular search engine. The other one was asked to perform the same queries using the SSA mobile application.

### 5.1. Usability

The users selected for these experiments are students within the Computer Science Department of at University Politehnica of Bucharest. They were selected based on their expertise, such that to cover a statistically wide range of

possible profiles. The users were split in two study groups, one was asked to search for information using other means, while the second group was using the proposed system. In the end, the users completed a questionnaire, with questions regarding the relevance of the obtained information, ease of use and access, the design of the application, etc. The conclusion of the usability test was that the application is able to select information that is closer to the user's own interests, and much faster than similar competing solutions. The main drawbacks, for now, were identified with the message fields (e.g., inappropriate error messages or status, or the absence of further use of contextual information).

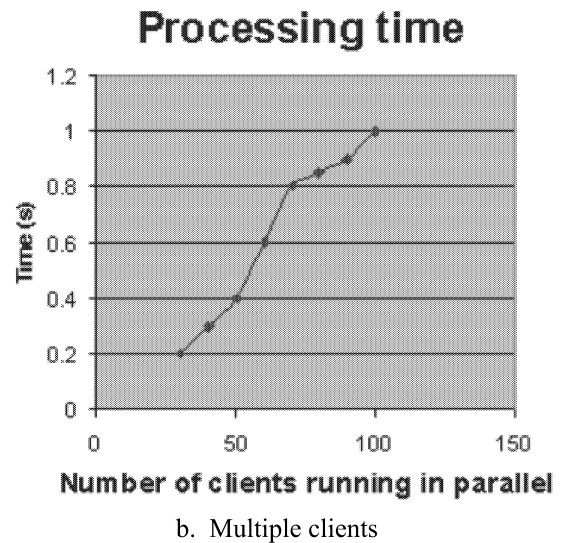
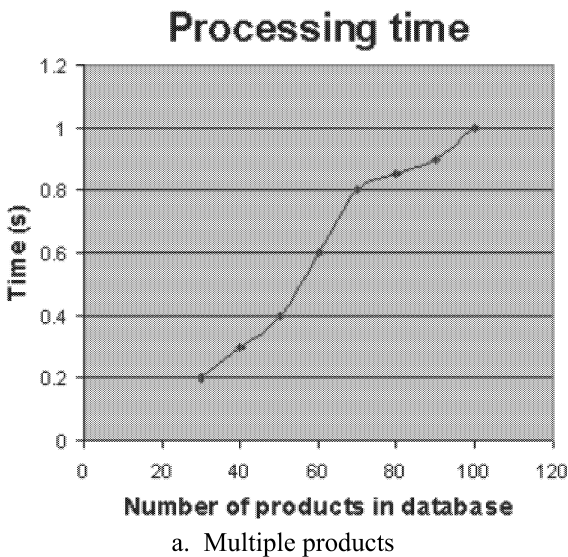
### 5.2. System's performance

Next we evaluated the performance of the system using the Flurry Analytics framework (Flurry, 2012). The monitoring framework is able to provide aggregated usage and performance data. It is a robust analysis tools because it helps exactly identifying issues (errors raised and clear details about them).

The propagation delay for a new preference depends on the synchronization with the database, and it is really small, the change is visible in a future interrogation. Once the number of users is increased, the processing time grows. This is due to the fact that in the prototype implementation the server is not distributed, and it does not scale on large amount of data (Fig. 7a). Running multiple clients in parallel also affects the response time (Fig. 7b).

For a regular utilization scenario (recommendation request, vote for 3 properties, iterate through 5 characteristics) the measured traffic was of approximately 5 KB. Using the application 20 times per day, and 3 days per week, we get 300KB. Assuming an average pricing model over a mobile operator, this leads to an operation cost of approximately 0.02 euro per week.

The delay for serving a request is composed of  $timerequest + timeprocessing + timeresponse$ . The first and the last terms



Figures 7: Experimental results.



depend on the connection quality. The processing time depends on the load on server and on database size and indexes. For the current implementation, with 30 books in database, the complete processing was accomplished in approximately 0.2 seconds.

## 6. CONCLUSIONS AND FUTURE WORK

In this paper we proposed a system to replace the regular methods of choosing between available products on the market. The system is able to recommend products based on the real needs of the customers. It is able to aggregate data from multiple sources and form a transparent social network between users. Using barcodes, a database and a recommendation algorithm a customer can find details about a product (such as locations and prices, pictures, etc.) or he/she can obtain recommended products, based on his preferences. We proposed several algorithmic approaches for computing the recommendation scores, and for managing the list of users and products. The results show the feasibility of the system to exceed the possibilities of modern search engines, and help the user find personalized information about products.

As future work, we intend to investigate the addition of a distributed server and database to address the scalability issue. Also, for a better recommendation algorithm, we want to investigate the addition of the distance within in a social network (friends of friends) and different friend lists for each domains ('I have similar tastes in books, but not in travels'). In terms of security, the server will also be extended to include mechanisms to protect it from receiving corrupted data (e.g. a client giving more votes than allowed, a client changing his id and acting as multiple users).

## ACKNOWLEDGEMENTS

The research presented in this paper is supported by national project: "TRANSYS – Models and Techniques for Traffic Optimizing in Urban Environments", Contract No. 4/28.07.2010, Project CNCSIS-PN-II-RU-PD ID: 238. The work has been co-funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Romanian Ministry of Labour, Family and Social Protection through the Financial Agreement POSDRU/89/1.5/S/62557.

## REFERENCES

- Cantador, I., A. Bellogín, and D. Vallet. 2010. 'Content-based recommendation in social tagging systems'. In *Proceedings of the fourth ACM conference on Recommender systems (RecSys '10)*. ACM, New York, NY, USA, 237-240.
- Sigurbjörnsson, B., and R. van Zwol. 2008. Flickr tag recommendation based on collective knowledge. In *Proceedings of the 17th international conference on World Wide Web (WWW '08)*. ACM, New York, NY, USA, 327-336.
- Flurry official website, last accessed February 3, 2012, from <http://www.flurry.com>.
- Kazienko, P., and P. Kolodziejski. 2006. 'Personalized integration of recommendation methods for e-commerce'. *Journal of Computer Science and Applications*, 2006.
- Lee, W.P., C.H. Liu, and C.C. Liu. 2002. 'Intelligent agent-based systems for personalized recommendations in internet commerce'. *Expert Systems with Applications*, 22(4), pp. 275-284.
- Cao, Y., and Y. Li. 2007. 'An intelligent fuzzy-based recommendation system for consumer electronic products'. *Expert Syst. Appl.*, 33(1), pp. 230-240.
- TheFind official website, last accessed February 2, 2012, from <http://www.thefind.com/>.
- Facebook Ads, last accessed February 3, 2012, from <http://www.facebook.com/home.php>.

## BIOGRAPHIES

**ELENA BURCEANU** finished her Bachelor studies within the University POLITEHNICA of Bucharest. Her research interests include distributed mobile applications and social collaborative systems. Currently she pursues her Master studies within the Distributed Systems track, with the University POLITEHNICA of Bucharest.

**CIPRIAN DOBRE** PhD, is lecturer with the Computer Science and Engineering Department of the University POLITEHNICA of Bucharest. The main fields of expertise are Grid Computing, Monitoring and Control of Distributed Systems, Modeling and Simulation, Advanced Networking Architectures, Parallel and Distributed Algorithms. His research activities were awarded with the Innovations in Networking Award for Experimental Applications in 2008 by the Corporation for Education Network Initiatives (CENIC).

**VALENTIN CRISTEA**, PhD, is the Head of the Computer Science and Engineering Department of University POLITEHNICA of Bucharest. He teaches courses on Distributed Systems and Algorithms. As a PhD supervisor he directs thesis on Grids and Distributed Computing. Valentin Cristea is Director of the National Center for Information Technology of UPB and leads the laboratories of Collaborative High Performance Computing and eBusiness..





# **LEARNING AND DIAGNOSIS**



# SUPPORTING LEARNING-BY-DOING SITUATIONS BY SEMANTIC TECHNOLOGIES

Danail Dochev and Gennady Agre

Institute of Information and Communication Technologies – Bulgarian Academy of Sciences

Sofia 1113, Bulgaria

E-mail: [dochev@iinf.bas.bg](mailto:dochev@iinf.bas.bg), [agre@iinf.bas.bg](mailto:agre@iinf.bas.bg)

## KEYWORDS

Computer Assisted Instruction, Learning-by-doing,  
Semantic Technologies

## ABSTRACT

The paper deals with the organisation of specific learning-by-doing activities by learner's authoring of analytical materials. These 'learning-by-authoring' activities are facilitated by semantic technologies to support the learners in the access and filtration of appropriate information objects and their subsequent analysis during the authoring process. The discussed framework for a TEL environment is experimented in a concrete domain - Bulgarian Iconography with educational uses in a set of humanitarian disciplines. The paper discusses briefly the information support for the learners, based on domain ontological modelling, in development of dedicated multimedia collection for analysis and in adequacy evaluation of the selected representative subset of objects. An example of a concrete learning task is presented.

## INTRODUCTION

The constructivism approach to human learning prevails in many contemporary research and development efforts in the area of Technology Enhanced Learning /TEL/. They address the creation of different pre-defined learning situations to facilitate active learners' participation. Nevertheless such dealing is too general and hence necessarily simplified. Active learning is relatively easy accomplished when learning facts, simple procedures and practical skills. This becomes more complicated in case of more "artificial" academic education, concerning more theoretic, conceptual matters, when formation and interpretation of abstract concepts is aimed for. This is the case when studying e.g. theoretical physics, mathematics, logics, philosophy etc. (Pasin and Motta 2007; Dzbor et al. 2007). This is valid to a great extent also for education in humanities, irrespective of the significant volume of necessary accompanying factual knowledge. The learners in such disciplines are often not directly engaged (or are engaged in lesser extent) with phenomena and perceptions from the real world, as in learning experimental sciences or technological disciplines. They have to work more with models – world representations as well as with digital presentations of artefacts. As computer systems give rich possibilities to present, access and apply models and digital

objects it seems natural these peculiarities to be supported adequately by TEL facilities.

There is common agreement among the researchers in the areas of pedagogy, psychology, cognitive science etc. (Driscoll 2000) that the most important generic skills to be developed in learners are: a/ analysis; b/ argumentation; c/ interpretation. These skills are interrelated as the analysis requires interpretation and the argumentation depends on the abilities to analyze and correctly interpret phenomena from the subject under study.

Due to the specificity of humanitarian disciplines (theoretic frameworks with not fully defined concepts and notions; significant impact of linguistic, cultural and subjective factors on the understanding and explanation of phenomena; different, even contradictory interpretations of phenomena, which should not be neglected in the learning process) the interpretative component of the learning is of a special importance for the education in humanities. From information viewpoint the interpretation is connected with the abilities to make associative links to independent information sources, to formulate assertions on their base and to make inferences from the available knowledge.

Such deliberations reveal some new desired functionalities of the TEL systems: in addition to ensuring appropriate presentation of the necessary built-in knowledge and facilitating the retrieval of information objects from information repositories they should offer to the learners more direct information help in the irrevocable basic learning phases of analysis and synthesis – desirably on individual, as well as on group level. The present paper deals with specific learning-by-doing activities - learner's authoring of analytical materials, facilitated by applying semantic technologies to support the learners in the access and filtration of necessary information objects to be analysed during the authoring process, as well as in the evaluation of outcomes.

## LEARNING-BY-AUTHORING ACTIVITIES

### Learning Situation

The work presented in this paper is organised under current national research project SINUS "Semantic Technologies for Web Services and Technology Enhanced Learning" (Dochev and Agre 2009) which targets are:

1/ Development of an environment for extending, binding and using heterogeneous multimedia digital libraries /DL/, accessible as web services.

The task under consideration is to develop ontology-based upgrades of existing DLs, where the semantic information is presented implicitly (in the data base structure) or explicitly (by ontology-based metadata used for semantic annotations). The upgrade has not to modify the original DL structure, information content and annotations. This line of investigation is not in the scope of the present paper.

2/ Development of specialized e-learning facilities, allowing learning by-doing through learners' authoring of specific learning materials by intensive use of multimedia DLs.

These facilities aim to support the analytical and to a certain extent the interpretative skills of the learners in a given humanitarian field by authoring of analytical materials in well defined learning situations. These 'learning-by-authoring' activities consist in development of educational scholarly essays/course theses/ projects for pre-assigned by the teacher analyses of the objects under study, created in three steps:

1/ Constructing limited-sized dedicated multimedia collection from DL with semantically annotated resources.

2/ Analysis of the selected collection by comparison and debate of certain objects characteristics. The analysis may require modification/enrichment of the developed collection.

3/ Development of the analytical essay as a multimedia document.

The intended target groups of the SINUS environment cover academic users (students, following different courses from the subject under study and their lecturers) and non-academic users. The students from formal education forms are expected to have a middle or higher level of knowledge about the domain and to intend to use the environment to improve their domain knowledge. They will actively search for digital learning resources and use them to achieve their learning goals by development of analytical scholarly essays, thematic projects, course or diploma theses etc. The lecturers should receive information support in preparing concrete learning tasks for their students (development of analytical materials for different purposes, based on appropriate selection of available digital resources), as well as in preparing exemplary learning resources and recommendations for students work on different levels.

The considered non-academic users do not work professionally in the subject domain, but have long-term interest in the area and are willing to extend their knowledge by self-education in the context of life-long learning. They normally are also interested to form their own specialised collections, annotated for their own use and/or sharing through social networks. It is supposed that such users are acquainted and work actively with the techniques for search of resources in Internet-based environments.

A specific user group of the environment consists of developers of semantic and learning resources – developers of domain ontologies, annotators of multimedia resources in digital repositories, authors of previously prepared semantically annotated learning resources.

Besides the learning applications the main functions of the environment would be useful to researchers in the subject domain for search of information material directly

connected with their investigations and development of specialised personalised virtual thematic collections of digital materials. The environment functionality for the last two user groups is outside the scope of the present paper.

A previous paper (Dochev et al. 2011) discusses the learning setting and the supported learning goals, and the information support for the collection development with the built-in system knowledge it needs. Below is briefly presented how the environment may guide and consult the learners, considering the normal shortage, inaccuracy and even incorrectness of the initial learners' knowledge for the domain and also for the accessible materials and available information support.

### Checking Possible Errors during the Collection Development

During the collection development the learner's input to the system consists of a query/set of queries in order to obtain desired multimedia objects, presumably satisfying requirements corresponding to the assigned task. Thus the learner may select:

- several objects, which all have the same desired characteristics;
- sets of objects, each of the sets having distinctive characteristics.

In the first case the (intermediate or final) result of the search has to be checked against the following conditions:

1. correctness – if the search result contains ONLY objects with the desired characteristics;
2. completeness - if the search result contains ALL the objects from the repository with the desired characteristics.

These checks are based on a simple model of the learners' errors when executing a task "find all the objects, corresponding to the described condition/s". This model fits with the classical Information Retrieval characteristics Precision and Recall. In order to apply the model the learning environment has to compare the intermediate or final search result of the learner against the conditions fixed in an *exemplary teacher's query/set of queries* for the given (sub)task.

The finalization of the collection development is often achieved by additional selection of several information objects from the intermediate search result to form a subset of representative (according to the learner) objects with characteristics, necessary for the further analysis. Besides the desired characteristics the learning task may define also a desired minimal size of particular subset. The coverage of necessary characteristics in the selected subset together with eventual qualitative requirements will be checked by the learning environment against the *formalized inner presentation of the learning task* formulated by the teacher. Such checks allow the environment to evaluate if the developed by the learner dedicated task-focused collection of multimedia objects contains sufficiently rich and various illustrative material to back-up the analyses. E.g. for the learning domain presented in the next section the environment may check the number of specific objects, the sufficient coverage of: iconographic schools, time periods, iconographic techniques, the sufficient diversity of object

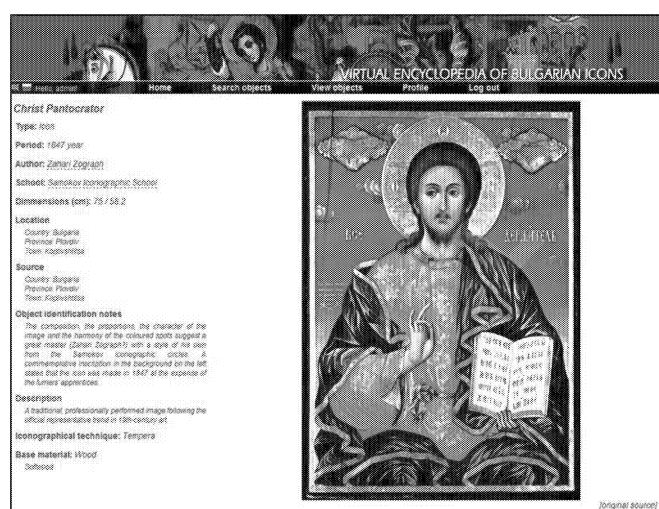
with desired characteristics etc. These checks are based on the built-in domain knowledge codified in domain ontology/ies. According the results of the checking recommendations to the learner to modify/upgrade the collection will be issued.

### Information Support for Collection Analysis

After the formation of a collection, satisfying the conditions of the assigned learning task the next phase of the analytical essay development consists in collection analysis - comparison of collection objects in order to determine their common or differing characteristics. The task under consideration here is to enrich search results visualization by explicitly controlled and content-based sorting of found objects and by explicitly controlled and content-based display of additional descriptive (metadata based) information.

The following system operations may facilitate the comparison of collection objects:

- Grouping of the collection elements according to defined value/s of a (set of) characteristic/s;
- Partitioning on subgroups according to defined characteristic or set of characteristics;
- Finding partitioning according to common value/s of a (set of) characteristic/s (the values are not pre-defined);
- Finding partitioning according to common (set of) characteristic/s (the characteristics are not pre-defined);
- Ordering objects according a characteristic value (e.g. chronologically);
- Registering the identity and the difference of the selected elements according pre-defined characteristics.



**Figure 1: An object from the “Virtual Encyclopaedia of the Bulgarian Iconography”**

## AN APPLICATION EXAMPLE

### Learning Domain

The discussed framework for a TEL environment, facilitating learning-by-authoring for the presented learning

tasks, is experimented in a concrete humanitarian domain - Bulgarian Iconography, which has educational uses in a set of disciplines like iconography, arts, history, culture studies, theology, etc. As source material for experimentation are used objects from the digital library “Virtual Encyclopaedia of the Bulgarian Iconography” (Figure 1) (Pavlova-Draganova et al., 2007) <http://bidl.cc.bas.bg/index.php?lang=en>.

The semantic annotation and search of digital objects is based on the domain Ontology for Bulgarian Iconographic Objects (Staykova and Dochev 2009). It is implemented as a set of a basic ontology, reflecting only features implicitly built in the structure of the DL, and additional small connected ontology of iconographical techniques. This approach to semantic modelling of the domain allows keeping intact the content, annotation and access method of the used DL and in the same time enables to enrich the semantic access to the DL information objects by additional descriptive (ontological) features through attachment of additional specialized ontologies.

**Table 1. Ontology concepts**

#### *Iconographical Object*

*Icon*

*Wall Painting*

*Miniature*

*Vitrage*

*Mosaic*

*Plastic Iconographical Object*

*Iconostasis*

*Throne*

...

*Author*

*Iconographical Clan*

*Iconographical School*

...

*Object Date*

*Object Period Date*

*Object Dating*

*Object Location*

*Monastery*

*Church*

*Chapel*

*Private Collection*

*Museum*

*Gallery*

....

*Canonical Type Character*

*Apostle*

*Deacon*

*Jesus Christ*

*The Virgin Mary*

...

*Iconographical Scene*

...

*Iconographical Technique*

...

*Gilding*

*Base of Gilding*

*Type of Gilding*

*Primer*

*Type of Primer*  
*Filler*  
*Condition of Primer*  
*Thickness of Primer*  
*Lacquering*  
*Type of Lacquering*  
*Condition of Lacquering*  
*Evenness of Lacquering*  
*Thickness of Lacquering*  
 ...

Table 1 presents a partial list of the ontology concepts to give a shallow impression for the experimented ontology coverage.

### An Exemplary Learning Task

The example presents structured formulation of a concrete learning task, extracted from the SINUS project use-case scenarios (Draganov et al., 2010). Structured textual formulation of the learning task is shown in Table 2. This table is cited from a previous paper (Dochev et al., 2011), which also contains a formalisation of the textual description in form of queries (presented in pseudo-language), used in the environment to help in the execution of the steps of collection development and evaluation of the adequacy of the selected by the learner representative subset of objects for further comparison of their significant characteristics.

**Table 2. Description of a learning task and recommendations**

Task	Make critical art analysis of the chronological development of the iconographic image of Jesus Christ in the Bulgarian iconographic schools.
Step	<b>1. Select collection of objects for the analysis.</b>
Recommendations	The selected objects have to satisfy the following criteria:
Basic:	Select at least 6 iconographical objects with the person of Jesus Christ in compositions with one main figure. All iconographical objects have to be in good current condition.
Optional:	At least one object from eminent author or founder of iconographic school. At least one primitive iconographical object and at least one iconographical object from the period of Bulgarian renaissance.
Step	<b>2. Make analysis of the collection.</b>
Recommendations	Examine the selected objects, comparing: <ul style="list-style-type: none"> <li>the cloths, gestures, proportions of the person of Jesus Christ;</li> <li>objects, other persons, Christian symbols;</li> <li>background, other elements around the image of Jesus Christ.</li> </ul> Search for changes – appearance or lack of elements (objects, symbols, persons), changes in background, clothes etc.

Step	<b>3. Register the results of the critical art analysis as a project.</b>
Recommendations	The project to be formed as multimedia document containing the selected iconographic images together with explanatory text before/after each image.

In the environment all the queries are formed by means of user-friendly interface, permitting the user to express her/his criteria for search, grouping, visualization etc. in the terms of ontological concepts by convenient consecutive guidance through a system of menu and submenu. In the implementation a query consists logically of the following parts:

a/ Ontological-based presentation of the query, generated by the learner through a Graphical User Interface (providing uniform way to search information and to activate services in the environment).

b/ Internal system representation - a SPARQL expression. SPARQL is an RDF Query language for data bases. This internal presentation was chosen to facilitate the access to semantic repositories as well as the comparison of semantic queries.

c/ Additional user-oriented presentation helping the inexperienced users to understand the meaning of current or previous queries. It is a simplified natural-language-like presentation based on appropriately verbalized labels of the ontology objects and relations.

In fact the interface-generated ontological-based query presentation is the primary one, while the other two presentations are “inferred”- produced automatically from it.

According to the learning task example above the collection development is natural to be made in successive steps, each time making the requirements more precise by refinement queries on current intermediate result/s. In order to help the learner to create refinement queries the system has to memorize and display when necessary elements of the learner’s interaction history. The history consists of pairs: query and corresponding search results, stored in a dynamic semantic repository (OWLIM, 2011). For query visualization the search results plus textual presentation of queries (c) are used. The query-results pairs are used also for checks of developed collection correctness against the (internal presentation of) teacher’s queries.

### CONCLUSIONS AND DIRECTIONS FOR FUTURE WORK

The paper discusses an approach to learning-by-doing activities through learners’ authoring of analytical materials in specific learning settings. An experimental learning environment applying this approach and using semantic information technologies is under development, addressing the area of Bulgarian iconography, studied in a set of humanitarian disciplines (iconography, arts, history, culture studies, theology, etc.). The environment objectives and specific learning tasks are briefly described. The discussion is focused on the current work to reveal and implement by Semantic Web techniques the necessary knowledge to guide

and help the learner's actions in developing limited-sized dedicated collections of multimedia objects, adequate to the pre-assigned learning tasks and then in comparing specific characteristics of the selected objects for the needs of developed analytical materials. By analysing the intermediate/final results of the incremental collection development against the pre-formulated teachers' criteria in ontological terms the environment helps the learner by warnings about errors and shortages.

The evaluation of learners' generated analytical materials is a challenging task. Learning environments may help in this step applying the internal knowledge models which describe the authoring process, the requirements towards analysed objects, and recommendations for the structure and characteristics of the results. In the design work on SINUS environment the attention to evaluation of intermediate and final results is focused not on assessment phases, but on monitoring the process and helping the learners to create analytical essays/projects according to teachers' mental picture what is a good analytical essay. The 'pedagogical' knowledge built in the environment in fact reflects such mental picture.

The current investigations and experiments led to the following possible future work directions:

- Facilitating the generation of semantic search queries by use of multilingual ontology-backed terminological lexicons. This facility should permit access to DL with foreign-language interface, supposing the use of semantic annotation and terminological lexicon, backed by the same ontology.
- Use of text processing techniques to obtain automatically formalised learning task descriptions from the original teacher's text description. The formalised task descriptions will enable to detect possible learners' errors during the collection development and to issue warnings about the coverage of concepts and desirable characteristics in the analytical essays.
- Use of text processing and data mining techniques to monitor and support the preparation of analytical essays with appropriate argumentation, structure and balance (e.g. checking by full-text analysis the availability of necessary basic concepts in the text and the sufficient coverage of their different ontological instances).
- Use of full-text analysis of textual descriptions of the DL information objects to detect domain ontology concepts in order to facilitate the objects semi-automatic semantic annotation.

## ACKNOWLEDGEMENTS

The work on this paper was funded partially by the Bulgarian National Science Fund project D-002-189 SINUS "Semantic Technologies for Web Services and Technology Enhanced Learning".

## REFERENCES

- Dochev D. and G. Agre, 2009. Towards Semantic Web Enhanced Learning. In *Proc. of the Int. Conf. on Knowledge Management and Information Sharing*, Funchal, Madeira, pp. 212-217.
- Dochev D., G. Agre, R. Pavlov, 2011. An Approach to Learning-By-Doing through User Creation of Learning Content. In: *Al-Saedy H. (Ed.). Proc. of 16th Annual Media and Web Technology Conference EUROMEDIA'2011*, London, April 2011, pp. 9-12.
- Draganov, L., D. Paneva-Marinova, L. Pavlova-Draganova, R. Pavlov, 2010. Use Case for Creative Learning-by-Authoring. In: *Proc. of the International Conference on e-Learning and the Knowledge Society*, August, 2010, Riga, Latvia, pp. 191-196.
- Driscoll, M., 2000. *Psychology of Learning for Instruction*. Needham Heights, MA, Allyn & Bacon.
- Dzbor M., A. Stutt, E. Motta, T. Collins, 2007. Representations for Semantic Learning Webs: Semantic Web technology in learning support. *Journal of Computer Assisted Learning* Vol. 23, pp. 69-82.
- Pasin M., E. Motta, 2007. Supporting Philosophers' Work through the Semantic Web: Ontological Issues. In: *SWEL Workshop of Ontologies and Semantic Web Services for IES, AIED 2007*, July 2007, Marina del Rey, CA, USA; pp. 80-90.
- Pavlova-Draganova, L., V. Georgiev, L. Draganov, 2007. Virtual Encyclopaedia of Bulgarian Iconography, *"Information Technologies and Knowledge"*, vol.1, №3, pp. 267-271.
- Staykova K. and D. Dochev, 2009. Ontology "Bulgarian Iconographical Objects" - Creation and Experimental Use, *"Cybernetics and Information Technologies"*, Vol. 9 (2009), №1, pp. 25-37.

## WEB REFERENCES

- OWLIM, 2011. <http://www.ontotext.com/owlim> (last accessed 25 Dec. 2011).

## AUTHOR BIOGRAPHIES

DANAIL DOCHEV is Associated Professor in the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences. His main research interests are: Knowledge-based Systems, Technology Enhanced Learning, Intelligent Organisation of Digital Content.

GENNADY AGRE is Associated Professor in the Institute of Information and Communication Technologies at the Bulgarian Academy of Sciences. His main research interests are: Machine Learning, Data Mining, Semantic Web Technologies.

# Using a cognitive model to include human emotions and intentions in Human-Machine Interaction

Ignazio Infantino, Giovanni Pilato, Riccardo Rizzo, Filippo Vella  
National Research Council of Italy  
ICAR-CNR, V.le delle Scienze edif. 11,  
90128, Palermo (PA)  
Italy  
E-mail: [name.surname]@cnr.it

## KEYWORDS

Human-Computer Interfaces, Affective computing,  
Cognitive Architecture, Robotics

## ABSTRACT

Detection and understanding of human intentions and emotions are relevant aspects of human-machine interaction, and the paper deals with a possible approach based on a cognitive framework named SeARCH-In (Sensing-Acting-Reasoning: Computer understands Human Intentions). The paper describes how the PSI cognitive model is implemented by visual perception capabilities, and managing semantic knowledge through a suitable ontology. The proposed implementation will be able to recognize user faces, to recognize and track human postures by visual perception. The ontological knowledge approach is employed for human behavior and expression comprehension, and the stored user habits are used for building a semantically meaningful structure for perceiving human intentions.

## INTRODUCTION

A cognitive architecture should be a basic the infrastructure of an intelligent system that manages, through appropriate knowledge representation, perception, and in general the processes of recognition and categorization, reasoning, planning and decision-making (Langley et al., 2009). In order for the cognitive architecture to be capable of generating behaviors similar to humans, it is important to consider the role of emotions. In this way, reasoning and planning may be influenced by emotional processes and representations as happens in humans. Ideally, this could be thought as a representation of emotional states that, in addition to influencing behavior, also helps to manage the detection and recognition of human emotions. Similarly, human intentions may somehow be linked to the expectations and beliefs of the intelligence system.

In a wider perspective, the mental capabilities (Vernon et al., 2007) of artificial computational agents can be introduced directly into a cognitive architecture or emerge from the interaction of its components. The approaches presented in the literature are numerous, and range from cognitive testing of theoretical models of the human mind, to robotic architecture based on perceptual-motor components and purely reactive behaviors - see Comparative

Table of Cognitive Architectures (BICA, 2011). The aim and long-term goal is the detailed definition of the Artificial General Intelligence-AGI (Goertzel and Pennachin, 2007), i.e. the construction of artificial systems that have a skill level greater or equal of humans in certain scenarios.

In the wider context of capturing and understanding human behavior (Pantic et al., 2006), it is important to perceive (detect) signals such as facial expressions, body posture, and movements while being able to identify objects and interactions with other components of the environment. The techniques of computer vision and machine learning methodologies enable the gathering and processing of such data in an increasingly accurate and robust way (Kelley et al., 2010). If the system captures the temporal extent of these signals, it can also make predictions and create expectations of their evolution. In this sense, we mean of detecting human intentions, and in a simplified manner, they are related to elementary actions of a human agent (Kelley et al., 2008). Over the last few years the approach pursued in the field of Human-Computer Interface (HCI) has changed, shifting to human centered design for HCI, namely the creation of systems of interaction made for humans and based on models of human behavior (Pantic et al., 2006). The Human-centered design, however, requires thorough analysis and correct processing of all that flows into man-machine communication: the linguistic message, non-linguistic signals of conversation, emotions, attitudes, and any other of information transmission, i.e. facial expressions, head movements, non-linguistic vocalizations, movements of hands and body posture, and finally it is necessary to recognize the context in which information is transmitted. In general, the modeling of human behavior is a challenging task and is based on the various behavioral signals: affective and attitudinal states (e.g. fear, joy, inattention, stress); manipulative behavior (actions used to act on objects environment or self-manipulative actions like biting lips), culture-specific symbols (conventional signs as a wink or a thumbs-up); illustrators actions accompanying the speech, regulators and conversational mediators like nodding the head and smiling.

In the case of human-machine interaction, one of the most important aspects to be explored in the detection of human behavior is the recognition of the intent (Kelley et al., 2008): the problem is to predict the intentions of a person by direct observation of his actions and behaviors. In practice we try to infer the result of a goal-directed mental activity that is not observable, and characterizing precisely the



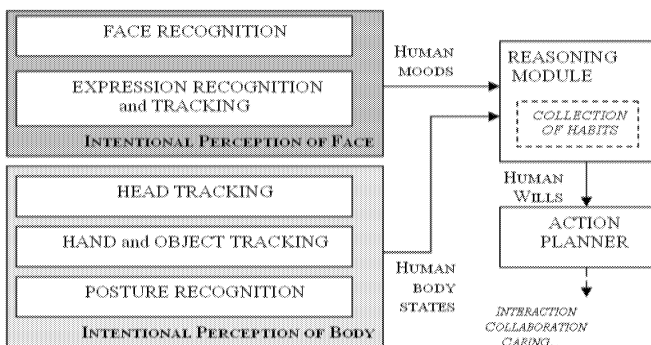
intent. Humans recognize, or otherwise seek to predict the intentions of others, using the result of an innate mechanism to represent, interpret and predict the actions of the other. This mechanism probably is based on taking the perspective of others (Gopnick and Moore, 1994), allowing you to watch and think with eyes and mind of the other.

Moreover, detection of human emotions plays many important roles in facilitating healthy and normal human behavior, such as in planning and deciding what further actions to take, both in interpersonal and social interactions. Currently in the field of human-machine interfaces, systems and devices that can recognize, process, or even generate emotions (Cerezo et al., 2008). The "affect recognition" often requires a multidisciplinary and multimodal approach (Zeng et al., 2009), but an important channel, rich with information, is facial expressiveness (Malatesta et al., 2009).

In the following, we described a cognitive framework that processes visual perception, manages semantic knowledge through a suitable ontology, and detects and recognizes human intentions.

## THE INTENTIONAL FRAMEWORK SeARCH-IN

SeARCH-In (Sensing-Acting-Reasoning: Computer Understands Human Intentions) is a vision based framework oriented towards human-machine interactions (see Figure 1). In this paper, an improvement of the system described in (Infantino et al., 2008, Infantino 2012) is presented, choosing a new cognitive model that uses emotions, and including 3D vision capabilities. The implemented system is able to recognize user faces, and to recognize and track human postures by visual perception. The described framework is organized on two modules mapped on the corresponding outputs to obtain intentional perception of faces and intentional perception of human body movements.



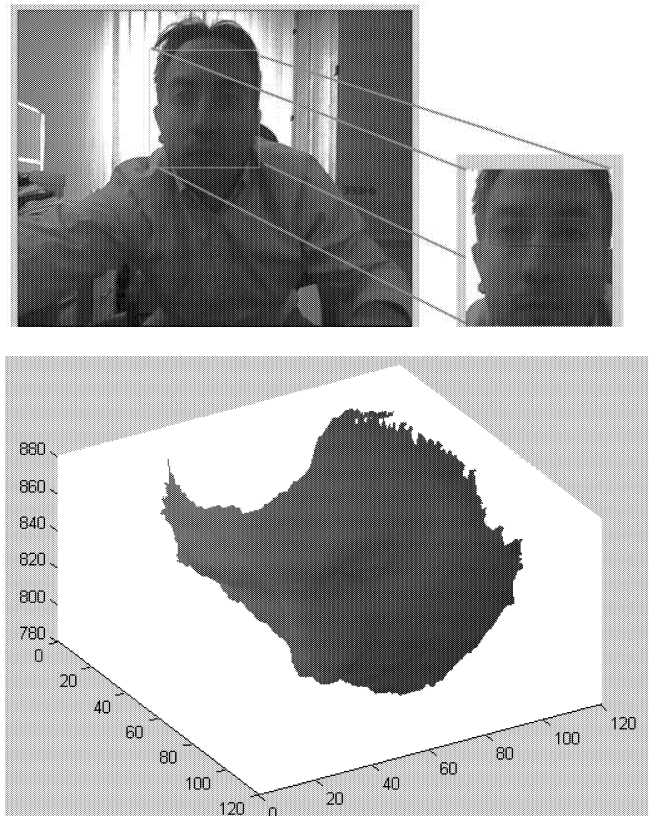
Figures 1: SeARCH-In architecture

The vision module is designed to be part of the complete cognitive architecture, and knowledge management and reasoning is allowed by a suitable OWL-DL ontology. In particular, the ontological knowledge approach is employed for human behavior and expression understanding, while stored user habits are used for building a semantically meaningful structure for perceiving human wills. A

semantic description of user wills is formulated in terms of the symbolic features produced by the intentional vision system. The sequences of symbolic features belonging to a domain specific ontology are employed to infer human wills and to perform suitable actions. The perception that regards the agent is generated from the observation of a human being who acts in an unstructured environment: human face, body, actions, and appearance are the object of humanoid in order to interact with him. The interaction is intended to be based on emotional and affective aspects, on the prediction of intents recalled from the memory. Furthermore, the perception concerns, in a secondary way for the moment, the voice and the objects involved in the observed action.



Figures 2: The proposed architecture has been tested on the NAO robotic platform.



Figures 3: Example of face and features extraction, 3D reconstruction for expression recognition.

The face and body are the elements analyzed to infer the affective state of the human, and for the identity recognition. The face is identified in the scene observed by the cameras of the robot using the algorithm proposed in (Viola and Jones, 2004), and its OpenCV implementation. The implementation of this algorithm is widely used in commercial devices since it is robust, efficient, and allows real-time use. The human body is detected by the Microsoft Kinect device, which, at the moment, is external to the robot, but shares the data on the network. From the artificial agent point of view, the Kinect device is in effect one of its sensor, and the software architecture integrated it as the other sensors. Again, we are using a commercial device that ensures accurate 3D perceptive results in real time. This sensor produces both a color image of the scene, and a depth map, and these two representations are aligned (registered), allowing you to associate each pixel with the depth estimated by IR laser emitter-detector pair. Through other software libraries, it is possible to obtain the human posture, like a reconstructed skeleton defined as a set of points in three dimensional space corresponding to the major joints of the human body (see Figure 4). In the region of the image where face is detected, two sets of algorithms are simultaneously run. The first group is used to capture the facial expression, identifying the position and shape of the main characteristic features of the face: eyes, eyebrows, mouth, and so on. The recognition of the expression is done using the 3D reconstruction (Hao and Huang, 2008), and identifying the differences from a neutral expression prototype (see Figure 3). The second group allows the recognition, searching a match in a database of faces, and using the implementation (API NaoQi, ALFaceDetection module) already available to the NAO humanoid robot (see Figure 2).



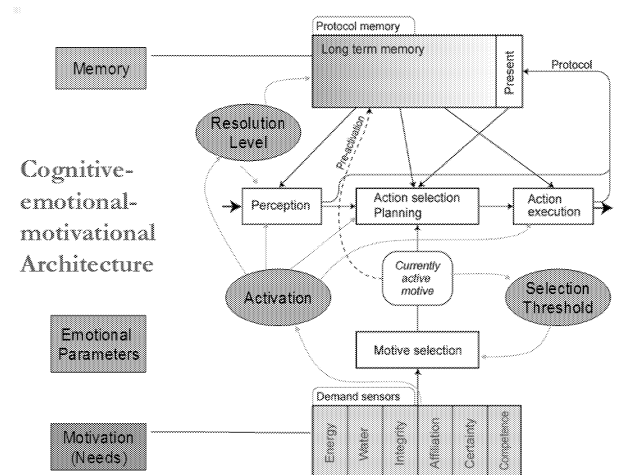
Figures 4: Example of 3D reconstruction of human skeleton by Kinect device.

## INTENTIONS IN PSI COGNITIVE MODEL

Among cognitive architectures, we choose the PSI model (Bartl and Drner, 1998) because involves explicitly the concepts of emotion and motivation in cognitive processes.

In particular we choose the MicroPsi implementation (Bach et al., 2006) that is an integrative architecture based on PSI model, has been tested on some practical control applications, and also in simulations of artificial agents in a simple virtual world. Similar to LIDA, MicroPsi currently focuses on the lower level aspects of cognitive process, but it does not handle directly advanced capabilities like language and abstraction. A variant of MicroPsi framework is included also in CogPrime (Goertzel, 2008). This is a multi-representational system, based on a hyper-graph with uncertain logical relationships and associative relations operating together. Procedures are stored as functional programs; episodes are stored in part as "movies" in a simulation engine.

Considering the architecture of PSI and the intentional vision agent created by the SEARCHIn framework, you can make some considerations on the perception of the intentions of a human being, the recognition of his identity, the mechanism that triggers of sociality, how memory is used, the symbolic representation of actions and habits, and finally the relationship between the robot's inner emotions and one observed.

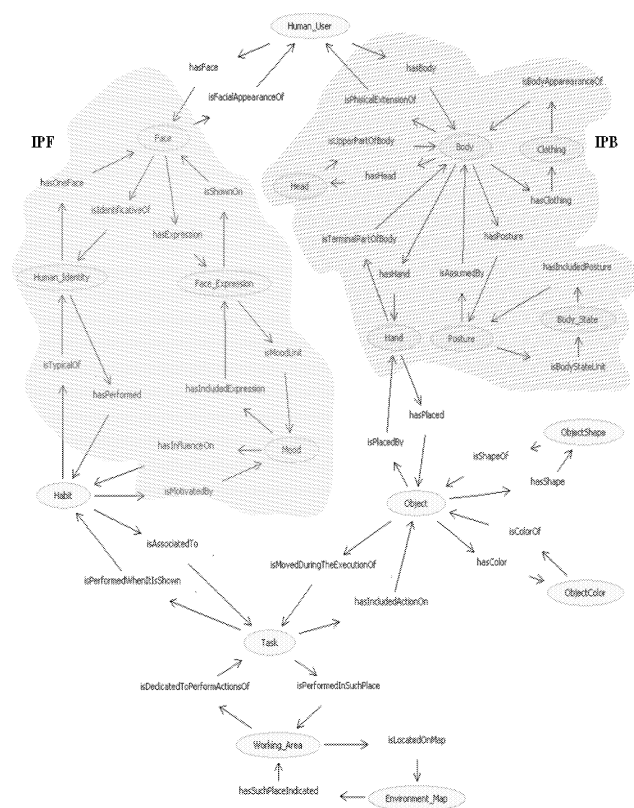


Figures 5: Cognitive-emotional-motivational schema of the PSI cognitive architecture (Bartl and Drner, 1998)

The PSI model requires that the internal emotional states modulate the perception of the robot, and are conceived as intrinsic aspects of the cognitive model. The emotions of the robots are seen as an emergent property of the procedure of modulation of the perceptions, behavior, and global cognitive process. In particular, emotions are encoded as configuration settings of cognitive modulators, which influence the pleasure/ distress dimension, and on the assessment of the cognitive urges. The idea of social interaction based on affect recognition and intentions simply leads to a first practical application of cognitive theory PSI. The detection and recognition of a face meets the need for social interaction that drives the humanoid robot, consistent with the reference theory which deals with social urges or drives, or affiliation. The designed agent includes discrete levels of pleasure/distress: the greatest pleasure is associated with the fact that the robot has recognized an individual,

and has in memory the patterns of habitual action (through representations of measured movement parameters, normalized in time and in space, and associated with a label); the lowest level of pleasure is obtained when it detects a not identified face, showing a negative affective state, and a lack of recognition of the observed action.

It is possible to implement a simple mechanism of emotional contagion (Gaglio et al., 2011), which executes the recognition of human affective state (limited to an identified human), and tends to set the humanoid on the same mood (positive, neutral, negative). The Nao may indicate his emotional state through the coloring of some leds placed in eyes and ears, and communicates its mood changes by default vocal messages to make the human aware of its status (red is associated with a state of stress, green with neutral state, yellow with euphoria, blue with calm).



Figures 6: SearchIn Ontology (see Infantino et al., 2008). Gray areas indicate Intentional Perception of Faces module (IPF) and Intentional Perception of Body module (IPB).

The symbolic explicit representation provided by the PSI model requires that the objects, situations, plans are described by a formalism of executable semantic networks, i.e. semantic networks that can change their behaviors via messages, procedures, or changes to the graph. In previous work (Infantino et al., 2008), it has been defined a reference ontology (see Figure 6) for the intentional vision agent which together with the semantic network allows for two levels of knowledge representation, increasing the communicative and expressive capabilities.

The working memory, in our example of emotional interaction, simply looks for and identifies human faces, and

contains actions for random walk and head movements to allow it to explore space in its vicinity until it finds a human agent to interact with. There is not a world model to compare with the one perceived, even if the reconstructed 3D scene by depth sensor could be used, and compare it with a similar internal model in order to plane exploration through anticipation in the cognitive architecture. The long-term memory is represented by the collection of usual actions (habits), associated with a certain identity and emotional state, and in relation to certain objects. Again, you might think to introduce simple mechanisms to capture affordances of objects, or introduce a motivational relevance related to the recognition of actions and intentions.

## CONCLUSIONS AND FUTURE WORK

We have shown how to combine cognitive architectures, visual perception processing, and a semantic structure for a system capable of detecting human intentions. Currently we are testing new modules to add to the described architecture in order to improve its cognitive capabilities. In particular we are interested in introducing of introspective or self-observing capabilities, and in implementing mechanism to build the semantic bridge between perception and concepts.

## REFERENCES

- Aylett, R. author of the figure available at [www.macs.hw.ac.uk/~ruth/psi-refs.html](http://www.macs.hw.ac.uk/~ruth/psi-refs.html)
- Bach, J.; Drner, D., and Vuine, R. (2006). Psi and MicroPsi. A Novel Approach to Modeling Emotion and Cognition in a Cognitive Architecture. Tutorial at ICCM 2006 available at <http://www.macs.hw.ac.uk/EcircusWeb/webContent/>.
- Bartl, C., and Drner, D. (1998). PSI: A theory of the integration of cognition, emotion and motivation. F. E. Ritter, & R. M. Young (Eds.), Proceedings of the 2nd European Conference on Cognitive Modelling, pp. 66-73.
- BICA (2011), Comparative Table of Cognitive Architectures <http://bicasociety.org/cogarch/architectures.htm>
- Cerezo, E.; Baldassarri, S; Hupont, I. and Seron, F. J. (2008). "Affective Embodied Conversational Agents for Natural Interaction", Affective Computing, Jimmy Or (Ed.), ISBN: 978-3-902613-23-3, I-Tech Education and Publishing.
- Gaglio, S; Infantino, I; Pilato, G.; Rizzo, R.; and Vella, F. (2011). "Vision and emotional flow in a cognitive architecture for human-machine interaction", Intl. Conf. Biologically Inspired Cognitive Architectures (BICA) 2011, Washington, USA, November 3-5 2011 (Frontiers in Artificial Intelligence and Applications, vol. 233, 2011, ISBN 978-1-60750-958-5)
- Goertzel, B. (2008). OpenCog Prime: Design for a Thinking Machine. Online wikibook, at <http://opencog.org/wiki/OpenCogPrime>.
- Goertzel, B. and Pennachin, C.. (2007). *Artificial General Intelligence*. Springer-Verlag, Berlin, Heidelberg.
- Gopnick, A. and Moore, A. (1994). "Changing your views: How understanding visual perception can lead to a new theory of mind," in Children's Early Understanding of Mind, eds. C. Lewis and P. Mitchell, 157-181. Lawrence Erlbaum
- Hao, T., and Huang, T.S. (2008). 3D facial expression recognition based on automatically selected features. Computer Vision and Pattern Recognition Workshops, 2008. CVPRW '08. IEEE Comp. Society Conf. pp.1-8.
- Infantino, I. (2012). "Affective human-humanoid interaction through cognitive architecture", *The Future of Humanoid*

- Robots: Research and Applications*, Riadh Zaier (Ed.), ISBN: 978-953-307-951-6, InTech.
- Infantino, I.; Lodato, C.; Lopes, S. and Vella, F. (2008). Human-humanoid interaction by an intentional system, In proc. of 8th IEEE-RAS International Conference on Humanoids 2008, pp.573-578, 1-3 Dec. 2008.
- Kelley, R.; Tavakkoli, A.; King, C.; Nicolescu, M.; Nicolescu, M. and Bebis, G.. (2008). Understanding human intentions via hidden markov models in autonomous mobile robots. In Proceedings of the 3<sup>rd</sup> ACM/IEEE international conference on Human robot interaction (HRI '08). ACM, New York, NY, USA, 367-374.
- Kelley, R.; Tavakkoli, A.; King, C.; Nicolescu, M. and Nicolescu, M. (2010). "Understanding Activities and Intentions for Human-Robot Interaction", *Human-Robot Interaction*, Daisuke Chugo (Ed.), ISBN: 978-953-307-051-3, InTech.
- Langley, P.; Laird, J. E.; and Rogers, S. (2009). "Cognitive architectures: Research issues and challenges". *Cognitive Systems Research*, 10, 141-160.
- Malatesta, L.; Murray, J.; Raouzaïou, A.; Hiole, A; Caamero, L. and Karpouzis, K. (2009). Emotion Modelling and Facial Affect Recognition in Human-Computer and Human-Robot Interaction, State of the Art in Face Recognition, Julio Ponce and Adem Karahoca (Ed.), ISBN: 978-3-902613-42-4, I-Tech Education and Publishing.
- Pantic, M.; Pentland, A.; Nijholt, A. and Huang, T.S. (2006). Human Computing and Machine Understanding of Human Behavior: A Survey, in proc. Of Eighth ACM Int'l Conf. Multimodal Interfaces (ICMI '06), pp. 239-248.
- Vernon, D.; Metta, G. and Sandini G.. (2007) "A Survey of Artificial Cognitive Systems: Implications for the Autonomous Development of Mental Capabilities in Computational Agents". *IEEE Transaction on Evolutionary Computation*, vol. 11, n. 2, pp. 151-180.
- Viola, P., and Jones, M. J. (2004). "Robust Real-Time Face Detection". *International Journal of Computer Vision*, vol. 57, no 2, pp. 137-154.
- Zeng, Z.; Pantic, M.; Roisman, G.I. and Huang, T.S. (2009). "A Survey of Affect Recognition Methods: Audio, Visual, and Spontaneous Expressions". *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.31, no.1, pp.39-58.

## BIOGRAPHY

**IGNAZIO INFANTINO** is a senior research scientist at the Institute of High Performance Computing and Networking (ICAR), of the National Research Council of Italy (CNR). He obtained Laurea degree and PhD on Computer Engineering at University of Palermo. His research interests are in the fields of computer vision, robotics, cognitive architecture, human-computer interaction, image processing.

# COMPUTER AIDED DIAGNOSIS METHODS BASED ON FRACTAL AND SPATIAL SERIES ANALYSIS FOR KIDNEY CT IMAGES

Andreea I. Udrea and Mihai Tanase  
Department of Automatic Control and Computer Science  
University Politehnica of Bucharest  
Spl. Independentei, Bucharest,  
Romania  
E-mail: udrea.andreea@yahoo.com

## KEYWORDS

Fractal dimension, correlation dimension, CT image analysis.

## ABSTRACT

The goal of this paper is to present a set of algorithms developed based on fractal and spatial series analysis that can be applied to computer aided diagnosis for discrimination between normal and modified kidney tissue. These algorithms were tested on 120 computer tomography (CT) images of normal, benign and malign affected renal tissue. Two of the algorithms provide useful numerical results that can be gathered to form statistics and provide a classification of the kidney tissue in normal and malign affected, while the third method can be used for enhanced visualization that proves its usefulness in the case of images that can not be classified. The conclusions of the study on the selected set of CT images are that distinction between normal and malign tissues can be done with high accuracy and significantly better results are obtained from CT images taken with contrast substances while using the correlation dimension. The enhancing procedure can give insights on the problem at hand when the statistics fails.

## INTRODUCTION

Time series analysis and fractal analysis are known techniques in clinical science and in connection to chaos theory (Bassingthwaite et al. 1994), (Cambel 1993).

Usually, fractal analysis refers to a collection of methods for the description and quantization of *geometric features* of irregular forms and patterns. It was largely applied for the study of biological systems and subsystems at microscopic and macroscopic scale (Dobrescu and Vasilescu, 2004) because of their fractal-like structure. Its most known measure is the fractal dimension used to provide information on the irregularity of an object contour or self similarities in a texture.

On the other hand, time series analysis deals with one dimensional time series that are sets of values of a single variable function,  $x(t)$  – usually measured as function of time (*dynamic features*). The study of time series requires a nonlinear approach. The development of numerical methods

was motivated by deterministic chaos which has been demonstrated to be present within many real systems in chemistry, physics, biology, medicine, electronics.

The usual studied time series in medicine are recordings of the electrical activity – electrocardiograms, electroencephalograms and physiological parameters – blood pressure, breathing.

In the domain of pathological anatomy, one deals with static – not varying with respect to time – structures like CT images and frozen tissues samples. In this case, we consider measurements with respect to a one-dimensional spatial axis – instead of temporal axis so that methods of nonlinear dynamical analysis can be applied as well (Mattfeldt 2004).

## MATERIALS AND METHODS

For this study, a series of 120 CT images were used. Fifty of them contain malign modified kidney tissue, fifty images – present normal kidney tissue and the rest of 20 – 4 images groups of benign affections.

A set of algorithms that are developed based on fractal and time series analysis and are applied to the study of renal CT images is presented. Based on them, a classification between modified and normal kidney tissues is made and also a method for enhance visualization of CT images is proposed. We consider a series of CT images containing the kidney tissue that have fractal – like tissue structures. The basic idea is to find and, if possible, categorize the anomalies that affect the kidney's tissue by studying time (spatial) series associated to the image and their fractal dimension. If the results are not conducting to a prognosis, an enhanced visualization tool can be employed by the physician to better inspect the image.

The first method computes the fractal dimension in the box-counting sense. The nonlinear analysis of time-spatial series is based on Takens embedding procedure, which allows the reconstruction of the attractor and the computation of the correlation dimension associated to the attractor of the studied tissue. This method was extended for two dimensional series called here spatial series.

The enhance visualization method is based on weighted fractal dimension and a filtering algorithm and outputs a colored map obtained based on the grey scale CT image.

## Box-Counting method and dimension

The box counting method provides a measure – fractal (box-counting) dimension ( $d_f$ ) for the complexity of the texture of the kidney tissue. The fractal dimension is computed using the box-counting algorithm because, in comparison to other methods, it offers two major advantages: it is easy to implement and can be applied for images no matter how complex.

The  $d_f$ , derived from the *Hausdorff* coverage dimension, is given by the following approximation:

$$d_f = \lim_{s \rightarrow 0} \frac{\log(N(s))}{\log(1/s)}, \quad (1)$$

where: -  $N(s)$  is the number of squares with side length  $s$  that contain information when grid covering the image.

Relation (1) is the equation of the slope  $d_f$  of the regression line associated to the points  $(\log(N(s)), \log(1/s))$  for different values of the square's side -  $s$ . The standard Box-Counting algorithm assumes to determine the  $d_f$  in accordance with the dependence of the texture upon the used scale factor. It consists transforming the grey scale image in binary image, successively covering it with squares with equal sides ( $2, 2^2, 2^3, \dots$ ) and counting every time the squares that contain some part of the analyzed object. The points of coordinates  $(\log(N(s)), \log(1/s))$  are approximately positioned in a line and its slope is the fractal dimension in "box-counting" sense.

A general problem of this method is the use of an ad hoc threshold when creating the binary image. This fact leads to incomplete or "noisy" object in the binary image and sometimes importantly affects the  $d_f$  value.

## Weighted box-counting dimension for image enhancement

This algorithm is based on the fact that in the CT images a higher density of the tissue is equivalent to lighter gray. The idea is to associate to every pixel a weight proportional to its gray level. We resume the essential of the algorithm below. Let us consider an image. We cover the image with square boxes as in the standard Box-Counting algorithm. Let  $s_k$  be the size of the box used in covering at step  $k$  (therefore we have to compute  $N(s_k)$  at this step). Let  $(x, y)$  be the coordinate of the upper-left corner of one of these boxes (let this be the box  $B_i^k$ ). We define  $m_i^k$  as the maximum of the weight values of the pixels contained in this box.

$$m_i^k = \max\{w_{i,j} \mid (i,j) \in ([x, y] \times [x + s_k - 1, y + s_k - 1]) \cap \mathbb{Z} \times \mathbb{Z}\}$$

where  $w_{i,j}$  is the weight associated to the pixel at  $(i,j)$  coordinates. Let  $W_i^k = [m_i^k / s_k] + r_i^k$ , where if  $s_k \mid m_i^k$  then  $r_i^k = 1$  else  $r_i^k = 0$ . Therefore  $N(s_k) = \sum_i W_i^k$ .

Next, the computation formula for  $d_w$  is the similar to the one in the classical algorithm. We shall refer to the number  $d_w$  as the Weighted Box Counting Dimension or WBCD.

Let us consider an image and let  $A$  be a pixel on it. Let  $K$  be a square centered at  $A$ . By using the previous algorithm we compute the WBCD of the square  $K$  and we associate a color to the pixel  $A$  according to this WBCD (the function which associates the color is a key part of the algorithm). In this way we obtain a map of level lines (we shall refer to this map as the Fractal Dimension Classification Map or FDCM). This leads to a classification of different tissues according to the associated color. Different structures must have different colors. The use of the FDCM in diagnosis requires a database with sufficient images.

## The CT image associated time series, its attractor and the correlation dimension

By investigating time series, one can observe the behavior and properties of dynamical systems.

A dynamical system  $T: N \times M \rightarrow M$  is said to be a discrete dynamical system if there is a map  $f: M \rightarrow M$  such that:

$$T(n, x) = (f \circ f \circ \dots \circ f)(x) = f^n(x), \\ \forall n \in \mathbb{N}, \forall x \in M.$$

A nonempty set of states  $K \subset M$  is called an attractor or attracting set for the system  $T$  if the following properties hold:  $K$  is closed,  $K$  is invariant, there is a neighborhood  $U$  of  $K$  such that:  $\lim_{t \rightarrow \infty} d(T(t, x), K) = 0, \forall x \in U$ .

A real valued map  $F: M \rightarrow \mathbb{R}$  is interpreted as a measure on the state space. If  $\forall t, s \in S$  are fixed ( $s$  is called delay) and  $x \in M$  is a fixed state, then a sequence of measurements:

$$F(T(t, x)), F(T(t + s, x)), F(T(t + 2s, x)), \\ \dots, F(T(t + (d-1)s, x))$$

is called a time series starting from  $(t, x)$  associated to the system  $T$ . If  $T$  is a discrete dynamical system defined by the map  $f$ , then the associated time series starting from  $(0, x)$  is:

$$F(x), F(f(x)), F(f^2(x)), \dots, F(f^n(x)).$$

One can reconstruct the attractor of a dynamical system from the time series generated by the system, by using the Takens Embedding Theorem (Takens 1981, Peitgen et al. 2000). The theorem was written for an infinite time series, but it can be implemented for a long enough finite series also. We present a version of Takens theorem: Let  $T: R \times M \rightarrow M$  be a smooth dynamical system of class  $C^2$  on  $M$  and let  $F: M \rightarrow \mathbb{R}$  be a measure of class  $C^2$ . Let  $t \in R$  be a fixed moment and let  $\tau > 0$  be a delay. If  $K$  is a compact invariant set of  $T$  and if  $b$  is the box-counting dimension of  $K$ , then the map:  $H: K \rightarrow \mathbb{R}^{2b+1}$  defined by:

$$H(x) = (F(T(t, x)), F(T(t - \tau, x)), \dots, F(T(t - 2b\tau, x)))$$

is generically injective.

Presuming that the fractal dimension of the attractor is known, the attractor can be reconstructed from a univariable time series in a higher dimensional space (that is at least twice plus one its fractal dimension). In practice,  $b$  is unknown, so, there are a series of methods for reconstructing the attractor without knowing its dimension. The correlation dimension -  $d_C$  - is a simple way to distinguish a random signal from a signal generated by a possibly chaotic set. The  $d_C$  for a closed curve is 1 and for a two-dimensional surface is 2. The correlation dimension is calculated using formula (2):

$$C(\varepsilon) = \varepsilon^{d_C}, \varepsilon \rightarrow 0 \Rightarrow d_C = \lim_{\varepsilon \rightarrow 0} \frac{\ln C(\varepsilon)}{\ln \varepsilon} \quad (2)$$

$C(\varepsilon)$  is called the correlation integral and is defined by expression (3):

$$C(\varepsilon) = \lim_{N \rightarrow \infty} \frac{1}{N^2} \sum_{i,j=1}^N H(\varepsilon - |y_i - y_j|), \quad (3)$$

where:  $H(x)$  - is the Heaviside function,  $H(x) = \begin{cases} 1, x > 0 \\ 0, otherwise \end{cases}$ ;

$\varepsilon$  - maximal Euclidian distance allowed between pairs of points;  $y_i$  - is a point in the embedded phase space constructed from a single time series according to Takens theorem:  $y_i = (x_i, x_{i+\tau}, x_{i+2\tau}, \dots, x_{i+(d_E-1)\tau})$ ;  $d_E$  - the dimension of the embedding space;  $i = N - \tau(d_E + 1)$  number of embedding vectors;  $N$  - initial time series length. So,  $C(\varepsilon)$  gives the proportion of the number of pairs of points in the embedding space with the Euclidian distance less than a specified small  $\varepsilon$ .

In order to perform nonlinear analysis on a CT normal or modified tissue image, a series of steps must be made. First, from a CT slice, the region containing the tissue to be analyzed must be isolated; a matrix containing values of each pixels shade is obtained (the value can vary between 0 and 255 corresponding to different shades of grey; 0 stands for black and 255 for white).

The time (spatial) series is generated in the following manner: the matrix resulting from the original image is cut in horizontal strips of 1, 4, 8, ... pixels, with respect to the initial image dimension and precision; all strips are put together one after another and generate one single strip associated to the image; the time (spatial) series -  $x(t)$  - is generated by computing either the mean value or the maximal (dominant) value of each columns of pixels within the strip. As result of this procedure, the time (spatial) series associated to the section of the analyzed tissue is obtained.

Having the associated series, the next step of the procedure implies calculating the correlation dimension of the attractor. This value is the discrimination criterion.

The delay or lag value -  $\tau$  - used to create the delayed embedding must be chosen carefully. A small value of the delay generates correlated vector elements, while large delay values yield to uncorrelated data and a random distribution in the embedding space. The delay can be chosen with good results as the moment of time where the autocorrelation function of the reconstructed series decays to  $1/e$  of its initial value:

$$RN(\tau) < RN(1)(1 - 1/e). \quad (4)$$

Generally, the lag value was found between 4 and 10, while the used search interval is [1, 20].

The minimum allowed embedding dimension is the dimension where the number of so called false nearest neighbors drops under a certain percent. A false neighbor is a point that under a certain higher dimensional embedding is projected near a point that that in the previous embedding was not in its vicinity.

In order to implement this procedure, each point of the delayed series is tested by taking its closest neighbor in  $d_E$  dimensions, and computing the ratio of the distances between these two points in  $d_E + 1$  dimensions and in  $d_E$  dimensions. If this ratio is larger than a certain threshold  $th$ , the neighbor was false (this threshold is taken large enough to take in consideration points that exponential divergence

due to deterministic chaos):  $\frac{\|y_{i,d_{E+1}} - y_{j,d_{E+1}}\|}{\|y_{i,d_E} - y_{j,d_E}\|} > th$  where  $\|\cdot\|$

is the Euclidian distance (Grassberger and Procaccia 1983).

Next, the correlation dimension is calculated over a range of different  $\varepsilon$  - values and embedding dimensions higher than the first assuring a decreased number of false neighbors.

The  $d_C$  differs from one embedding dimension to another due to the noise in the data, but there is a particular region, usually called the *scaling region* where  $d_C$  stabilizes (Hegger et al. 1999). This is the interval where a mean value for the correlation dimension of an attractor is calculated.

## RESULTS AND STATISTICS

We start the analysis procedure by presenting a comparative study between the 2 kidneys of the same patient, one healthy while the second presenting a malign tumor.

In Table 1, on each row there are the images of correspondent sections in the kidneys and the values for the box-counting dimension and mean correlation dimension.

It can be observed that both dimensions for the unaffected kidney tissue vary accordingly to the complexity of the tissue in the analyzed section (in the middle of the kidney more complex than in the extremities). Generally, the  $d_f$  and  $d_C$  of the modified tissue varies correspondingly to the dimension of the affected region and the complexity of the tissue at the analyzed level with clearly larger differences in the case of  $d_C$ .

The same procedure was applied to all the 120 CT's. Statistical methods were performed in order to test the trustworthiness of these two different types of discrimination methods.

For the statistical analysis, descriptive and comparison procedures were performed. The subjects were divided in two samples each containing 50 CT images (normal and modified, respectively).

### Statistical results for box-counting method

For each sample, the average, standard deviation, standard skewness and standard kurtosis were computed (Table 2).



Table 1: Normal and modified tissue images,  $d_f$ ,  $d_c$ 








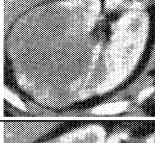




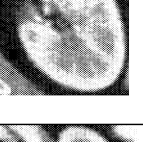
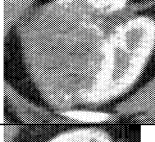



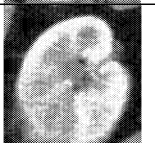
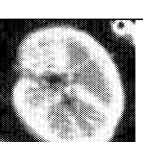
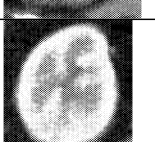
$d_f$	Normal tissue	Malign tissue	$d_c$
1.7			2.15
1.73			2.14
1.77			2.16
1.82			2.19
1.89			2.21
1.87			2.11
1.83			2.09
1.79			2.1
1.47			1.69
1.41			1.51

Table 2: Descriptive  $d_f$  statistical methods results

Descriptive methods	Normal tissue $d_f$	Modified tissue $d_f$
Average	1.73667	1.76875
Std. Deviation	0.0589522	0.0715853
Std. Skewness	0.769626	0.827251
Std. Kurtosis	-1.0833	0.0478851

95.0% confidence interval for mean	[1.711,1.761]	[1.738,1.798]
------------------------------------	---------------	---------------

Table 3: Comparison statistical methods results ( $d_f$ )

t Test	0.0968575>0.05
Kolmogorov- Smirnov Test	0.0684376>0.05

In order to compare the samples the t test and Kolmogorov-Smirnov test were performed. Both comparison tests show no significant difference between the two distributions at the 95.0% confidence level (Table 3).

These results yield that the trustworthiness level of the analysis made by calculating the box-counting method on the considered CT samples is low.

#### Statistical results for nonlinear time series method

The same procedures were applied for values obtained by means of nonlinear time series analysis. For each sample, the average, standard deviation, standard skewness and standard kurtosis were computed (Table 4).

In order to compare the samples the t test and Kolmogorov-Smirnov test were performed (Table 5). Both comparison tests show significant difference between the two distributions at the 95.0% confidence level.

Table 4: Descriptive  $d_c$  statistical methods results

Descriptive methods	Normal tissue $d_c$	Modified tissue $d_c$
Average	1.72988	1.97475
Std. Deviation	0.240782	0.242743
Std. Skewness	-2.27774	-2.35657
Std. Kurtosis	3.66811	1.26397
95.0% confidence interval for mean	[1.628,1.831]	[1.872,2.077]

Table 5: Comparison statistical methods results ( $d_c$ )

t Test	0.00101879 < 0.05
Kolmogorov - Smirnov Test	0.000567<0.05

The confidence level in this case is better then for the previously analyzed methodology.

We conclude that the box-counting method is using a certain threshold, this way losing some information on the tissue texture while nonlinear analysis is more precise and uses all the information in the images. We recommend the use of the second method for analyzing CT images.

We have also compared the results acquired when the CT was taken with contrast substances and without.


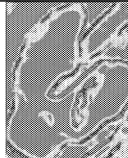

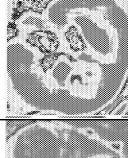
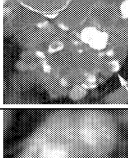
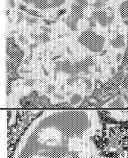

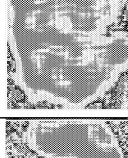


In the second case, the  $d_c$  values are smaller because of a series of features that are not so visible (blood vessels). The differences between the  $d_c$  of normal and modified tissue samples are smaller. So, we suggest that this methodology is better to be used with associated time series resulting from CT images taken with contrast substances.



## Benign affected tissue classification and inspection

The second step in the analysis was to determine the correlation dimension of the attractor for images containing kidneys with benign affections.

Table 5: Benign modified tissue images, their maps and associated  $d_c$  values

Affection	Image		$d_c$
Pyelonephros			1.36 (correspondent $d_c$ for healthy kidney -1.85)
Medullary sponge kidney			1.91(1.86)
Polychistic kidney			2.06 (1.9)
Kidney tuberculosis (renal TB)			2.3(1.92)
Trombosis			1.98(1.93)

The discrimination is obvious in the cases of pyelonephros (the resulted  $d_c$  values being smaller than in the case of normal tissue) and kidney tuberculosis (with  $d_c$  values larger than in the case of malign modified tissue). The  $d_c$  values for medullary sponge kidney tissue were generally a little bit larger than the ones for normal tissue. The  $d_c$  values for thrombosis affected kidney tissue were generally a little bit smaller than the ones for normal tissue. In the third column of Table 5 the kidney CT image map is presented. The kidney border and affection specific aspects like different types of tissue clusters and their delimitation can be seen clearer. Also, the different colors in the map identify different formations, specific to the affection. This method

proved more useful than the previous two in aiding the diagnostic in the case of benign affected tissue.

## CONCLUSIONS

The conclusions of the study on the selected set of CT images are: there are significant differences between the correlation dimension of the normal tissue and the correlation dimension of the modified tissue; significantly better results are obtained in the case of CT images taken when contrast substances are used; the enhancement method proved very helpful when the other two failed to provide good results. Future work aims at: enlarging the CT images data base; measuring, where it is possible, the percentage of the modified tissue in a kidney CT slice in order to provide information on what is causing the increase in  $d_c$  (percentage of affected tissue or  $d_c$  value of modified tissue); determining the position of tumors masses in an affected organ when considering horizontal slices and respectively reconstructed transversal slices in that organ .

## REFERENCES

- Bassingthwaight J.B., Liebovitch L.S., West B.J., 1994. *Fractal Physiology*. Oxford University Press.
- Cambel A.B., 1993. *Applied Chaos Theory*. Acad. Press.
- Dobrescu R., Vasilescu C., 2004. *Interdisciplinary Applications Of Fractal And Chaos Theory*. Academia Română, Bucuresti.
- Grassberger P., Procaccia I., 1983. "Characterization of strange attractors". In Phys. Rev. Lett. 50, 346-349.
- Hegger R, Kantz H., Schreiber T., 1999. "Practical implementation of nonlinear time series methods: The TISEAN package". In Chaos 9, pp. 413-435.
- Mattfeldt T., 2004. "Classification of binary spatial textures using stochastic geometry, nonlinear deterministic analysis and artificial neural networks". In Inst J. Pattern Recogn. Artif. Intelligence 17.
- Peitgen H-O., Jurgens H., Saupe H., 2000. *Chaos and Fractals – New Frontiers of Science*, Springer.
- Takens F., 1981. "Detecting strange attractors in turbulence". In Lectures Notes Math. 898, pp. 366-381.

## AUTHOR BIOGRAPHY

**ANDREEA UDREA** was born in Bucharest, Romania and went to the University "Politehnica" of Bucharest, Faculty of Automatic Control and Computers. She obtained her bachelor, master and PhD degrees in 2006, 2008 and respectively in 2011. At the present time she is a lecturer at the same university.



# **TELECOM SYSTEMS**



# BENCHMARK ANALYSIS FOR ADVANCED DISTRIBUTED DATA STORAGE FOR HETEROGENEOUS CLUSTERS

Catalin Negru, Florin Pop\*, Ciprian Dobre, Valentin Cristea

University POLITEHNICA of Bucharest, Faculty of Automatic Control and Computers, Department of Computer Science  
Spl. Independentei, 313, Bucharest 060042, Romania  
E-mails: {catalin.negru, florin.pop, ciprian.dobre, valentin.cristea}@cs.pub.ro

## KEYWORDS

Data Storage, Distributed Systems, Clusters, Benchmark.

## ABSTRACT

The necessity of a Large Scale Distributed Data Storage System offering scalability, reliability, performance, availability, affordability and manageability became a strong requirement for high-level application with multiple user interactions. This paper presents the benchmarking for performance of LUSTRE file system and highlights the results obtained from different test scenarios with IOzone and Intel IMB benchmarks, considering parallel I/O characteristics of Lustre file system. The paper also presents a set of best practices for data integrity security and accessibility and a few techniques for troubleshooting with LUSTRE. The results of the benchmark analysis were used to offer a perspective about the performance of NCIT-Cluster at University Politehnica of Bucharest in I/O and MPI jobs.

## INTRODUCTION

The emergence of clustered computers has created a multiplication of scientific, analytic and research data. Many applications such as seismic data processing, financial analysis, computational fluid dynamics, calculations to understand the fundamental nature of matter, including quantum chromo dynamics and condensed matter theory, created growing storage infrastructure challenge as traditional storage systems struggle to keep pace with speed and requirements of this kind of applications.

In this context, in many scientific applications, especially those that use large amount of data exists a gap between processor performance and I/O performance which led to I/O bottlenecks. Parallel file systems represent the solution which in most of the cases solves the bottleneck with I/O problems [1]. Numerous studies have shown that many scientific applications need to access a large number of small pieces of data from file. The I/O performance suffers considerably if applications access data by making many small I/O requests. To improve the parallel I/O performance, the small I/O requests are collected into fewer number of larger size requests. So, storage has become a very important part of clusters and distributed systems and is likely to become even more important as problem sizes grow [16, 17]. File systems

such as IBM's GPFS [2], SUN's open source Lustre File System [3] have proven to support concurrent file and file system access across thousands of files and data that are growing up reaching zeta scale.

Lustre represents a leading technology in class of parallel I/O technologies and open source standard for HPC and clusters. Lustre file system is currently used on nearly 1/3 of the world's Top100 fastest computers [4]. MPI-IO represents a parallel I/O interface that allows programs with many processes (like scientific applications) on many nodes to coordinate their I/O read and write and to obtain more efficiency [5].

IOzone is a file system benchmark tool. The benchmark generates and measures a variety of file operations. IOzone has been ported to many machines and runs under many operating systems. IOzone is useful for determining a broad file system analysis of a vendor's computer platform. The benchmark tests file I/O performance for several atomic, parallel and concurrent operations that highlight the performance of a parallel file system [7].

NCIT High Performance Computing Center from University Politehnica of Bucharest includes several research and teaching laboratories in the fields of High Performance Computing, Distributed Systems and Applications, E-Business and e-Government, Artificial Intelligence, Computer Networks. The Center's activity relies on a collaborative virtual environment using high-performance resources and computer-supported cooperative work tools. The solution is flexible, easily adaptable to different activities carried out by the Center, including project development, training, consultancy, technology transfer, etc. The mission of the Center is to promote advanced and interdisciplinary research, to develop a new paradigm for collaboration among computer scientists, computational scientists and researchers from a diversity of domains, to develop human resources by educational programs [8].

The paper is structured as follow: Section 2 presents the related work in the field of benchmark analysis for distributed data storage. Section 3 presents the proposed model for NCIT cluster and in Section 4 the experimental results. We present the conclusions and future work in Section 5.

---

\* Corresponding Author

## RELATED WORK

Large clustered computers provide low-cost compute cycles, and therefore have promoted the development of sophisticated parallel-programming algorithms based on the Message Passing Interface [6]. Chen et al. in [6] evaluated the I/O performance using the IOZONE benchmark on the iSCSI-based TerraGRID parallel filesystem. Their evaluations show that 10GbE, with or without protocol-offload, offered better throughput and latency than IB to socket-based applications. Although protocol-offload in both 10GbE and IB demonstrated significant improvement in I/O performance, large amount of CPU are still being consumed to handle the associated data-copies and interrupts. The emerging RDMA technologies hold promises to remove the remaining CPU overhead. We plan to continue our study to research the applications of RDMA in parallel I/O.

The benchmark could also be used for problem diagnosis in parallel file systems, problem referring to scalability and accessibility. Kasick et al. in [9] focus on automatically diagnosing different performance problems in parallel file systems by identifying, gathering and analyzing OS-level, black-box performance metrics on every node in the cluster. They developed a root-cause analysis procedure that further analyzes the affected metrics to pinpoint the faulty resource (storage or network), and demonstrate that this approach works commonly across stripe-based parallel file systems. Based on that, we tried to identify in this paper and in our approach the lateral effect caused by CPU cache and buffer cache.

Song et al. in [10] demonstrates that the stripe size is a vital performance parameter, but the optimal value for it is often application dependent. How to determine the optimal stripe size is a difficult research problem. Based on the observation that many applications have different data-access clusters in one file, with each cluster having a distinguished data access pattern, in [10] is proposed a segmented data layout scheme for parallel file systems. The basic idea behind the segmented approach is to divide a file logically into segments such that an optimal stripe size can be identified for each segment. We conduct out tests for benchmarks, considering parallel I/O characteristics of Lustre file system and different stripe size for data.

Another important sector that requires distributed data storage refers to server virtualization. Here, the challenge is on profiling physical resource utilization information of VMs when consolidated on a single server. In [11] Lu et al. formulate profiling as a source separation problem as studied in digital signal processing, and design a directed factor graph (DFG) to model the multivariate dependence relationships among different resources (CPU, memory, disk, network) across virtual and physical layers. The methodology outputs estimates of physical resource utilization on individual VMs and physical server aggregate resource utilization. The Xen-virtualization platform was used in order to evaluate the methodology for different consolidation scenarios with diverse applications including RUBiS, IOzone, SysBench, and Netperf.

## DATA STORAGE SOLUTION FOR CLUSTERS

In clusters, in general, data is stored on multiple virtual servers, generally hosted by third parties, rather than being hosted on dedicated servers. The center operators, in the background, virtualizes the resources according to the requirements of the customer and expose them as storage pools, which the customers can themselves use to store files or data objects. Physically, the resource may span across multiple servers. Based on cluster storage the Cloud storage began to offer a 'hot' new storage technology for different users with necessities. The fundamental challenge facing cloud storage is scalability. Here new multi-terabyte disk drives are the norm, but traditional RAID data protection technologies are lagging due to longer disk rebuild times. Per Bit addresses the challenge of scalable data protection with a new purpose-built, cloud storage solution. In a field as complex as enterprise storage in heterogeneous clusters, building testing mechanisms that accurately reflect real life and provide any real value to end-users is fantastically difficult. With such an incredibly wide range of enterprise storage workloads and products, it's very hard to build a benchmark that has any hope of resembling all of them

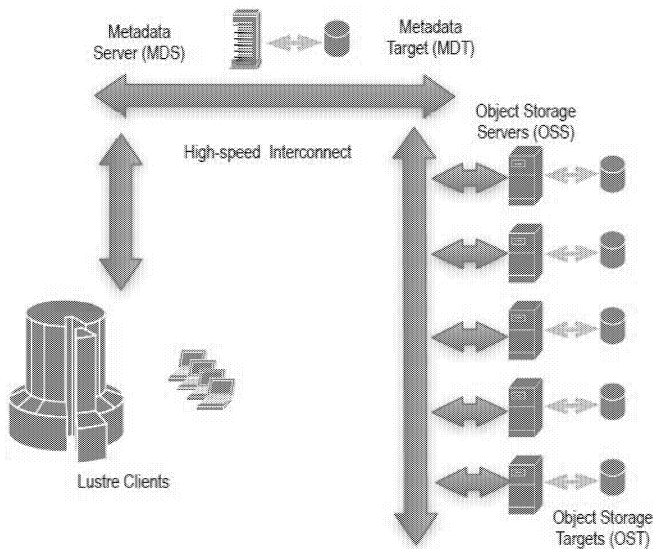
The important criteria for evaluating a data storage solution for clusters are:

- *Manageability*: the ability to manage a system with minimal resources;
- *Access method*: protocol through which cloud storage is exposed;
- *Performance*: performance as measured by bandwidth and latency;
- *Multi-tenancy*: support for multiple users (or tenants);
- *Scalability*: ability to scale to meet higher demands or load in a graceful manner;
- *Data availability*: measure of a system's uptime;
- *Control*: ability to control a system—in particular, to configure for cost, performance, or other characteristics;
- *Storage efficiency*: measure of how efficiently the raw storage is used;
- *Cost*: measure of the cost of the storage (commonly in dollars per gigabyte).

All of these aspects must be considered in concordance with all important levels in cluster storage architecture: network and storage infrastructure, storage management, metadata management, storage overlay and interface service.

Lustre is a storage architecture for clusters (see Figure 1). The central component of the Lustre architecture is the Lustre file system, which is supported on the Linux operating system. Lustre is a parallel file system and is designed to enable I/O performance. Mainly used in High Performance Computing environments, Lustre is also applicable to any enterprise storage environment where very high I/O bandwidth is required. Lustre is an object-based file system. It is composed of three components: Metadata servers (MDSs) object storage servers (OSSs), and clients. Figure 29 presents the Lustre architecture. Lustre uses block devices

for file data and metadata storages and each block device can be managed by only one Lustre service. The total data capacity of the Lustre file system is the sum of all individual OST capacities. Lustre client's access and concurrently use data through the standard POSIX I/O system calls [12].



**Figure 1. Architecture of a Lustre file systems [12]**

The main features of Lustre are: scalability, high-availability high-performance heterogeneous networking, security, access control list (ACL) with extended attributes, interoperability, object-based architecture, byte-granular file and fine-grained metadata locking, controlled striping, disaster recovery tool, internal monitoring and instrumentation interfaces.

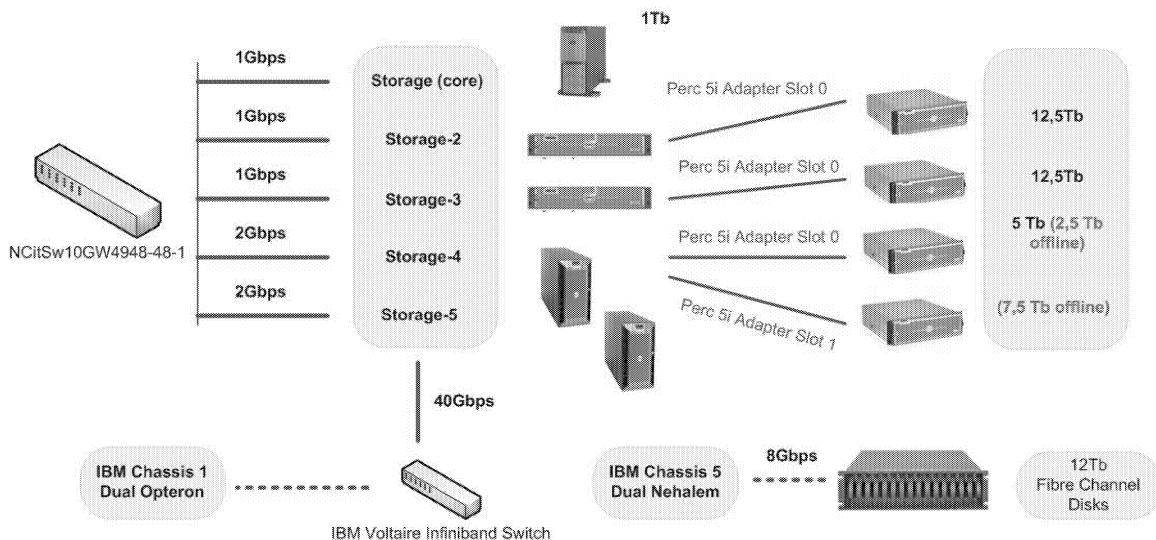
We analyze the Lustre file system in the context of NCIT cluster as a support for complex applications. The NCIT cluster has the following characteristics regarding data storage system: the storage system is composed of the following DELL solutions: 2 PowerEdge 2900 and 2 PowerEdge 2950 servers, and 4 PowerVault MD1000 Storage Arrays. There are four types of disk systems you can use local disks, NFS, LustreFS and FibreChannel disks. All home directories are NFS mounted. There are several

reasons behind this approach: many profiling tools cannot run over LustreFS because of its locking mechanism and second, if the cluster is shut down, the time to start the Lustre file system is much greater than starting NFS (see Figure 2).

For benchmarking we defined the following scenarios that are important for different case-studies:

- Write: measures the performance of writing a new file.
- Re-write: measures the performance of writing a file that already exists. When a file is written that already exist the work required is less as the metadata already exists.
- Read: measures the performance of reading an existing file.
- Re-Read: measures the performance of reading a file that was recently read.
- Random Read: measures the performance of reading a file with accesses being made to random locations within the file.
- Random Write: measures the performance of writing a file with accesses being made to random locations within the file.
- Random Mix: measures the performance of reading and writing a file with accesses being made to random locations within the file.
- Backwards Read: measures the performance of reading a file backwards.
- Record Rewrite: measures the performance of writing and re-writing a particular spot within a file.
- Fwrite: measures the performance of writing a file using the library function fwrite().
- Fread: measures the performance of reading a file using the library function fread().

The benchmark tests file I/O performance for the scenarios mention before using IOzone tool. We want to estimate the capacity of NCIT cluster in order to support different type of data storage operations, with different stripe size. The benchmark generates and measures a variety of file operations. IOzone has been ported to many machines and runs under many operating systems (we test on Linux OS).

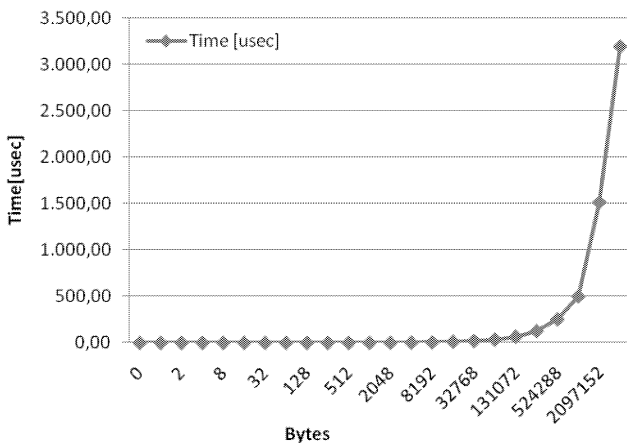


**Figure 2. NCIT Data Storage Architecture [13]**

## EXPERIMENTAL RESULTS

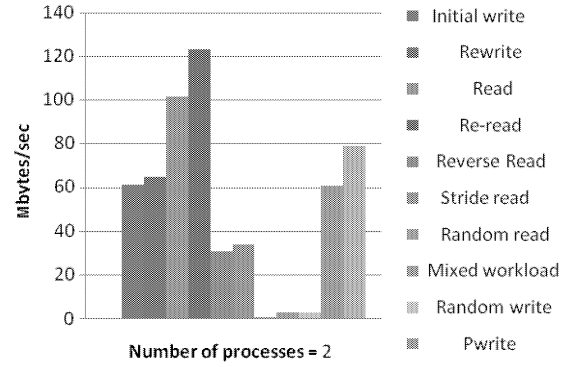
We conduct our test considering all mentioned scenarios in previous section using parallel I/O over Lustre FS. MPI-IO represents a parallel I/O interface that allows programs with many processes on many nodes to coordinate their I/O read and write and to obtain more efficiency [13]. One of the known issues of Lustre in MPI applications is represented by the not aligned I/O on stripe boundaries. One file might be distributed across two stripes which is representing a drawback in the performance of the application. Another problem is represented by large, contiguous writes, can cause significant contention at the network layer.

ROMIO implements the collective I/O operations using a technique termed two-phase I/O. Consider a collective write operation. In the first phase, the processes exchange their individual I/O requests to determine the global request. The processes then use inter-process communication to re-distribute the data to a set of aggregator processes. The data is redistributed such that each aggregator process has a large, contiguous chunk of data that can be written to the file system in a single operation. The parallelism comes from the aggregator processes performing their writes concurrently. This is successful because it is significantly more expensive to write to the file system than it is to perform inter-process communication [14].



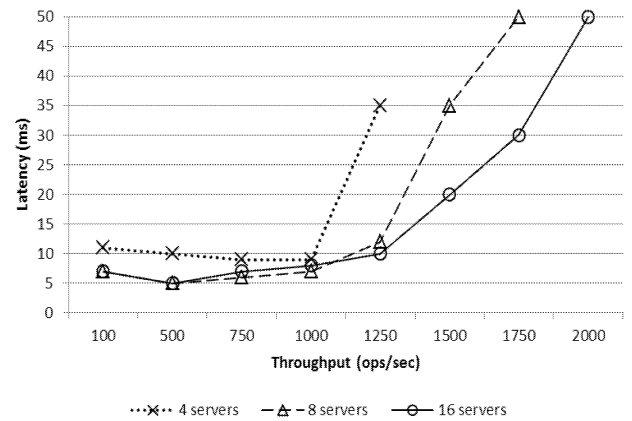
**Figure 3. Ping-Pong Benchmark between two processes (Parallel-I/O: MPI ROMIO over Lustre)**

Collective IO will apply read-modify-write to deal with non-contiguous data by default. However, it will introduce some overhead (IO operation and locking). In Figure 3 is presented a Ping-Pong benchmark which passes messages of different size between two processes which run on two machines on Quad queue on NCIT-Cluster at UPB. Can be observed that over 512KB transfer time rise exponential. So, the conclusion with this test shows that the Parallel-I/O paradigm offers performance for HPC collaborative application only for small messages. In Figure 4 is presented a IOzone test for a 256MB file in throughput mode with 5 active threads for Ping-Pong Benchmark between two processes. The conclusion with this test shows that the Read and Re-read operations are performant for this type of communication, so application that read in a high loop the same set of variables are the good candidate for parallel-I/O over Lustre.



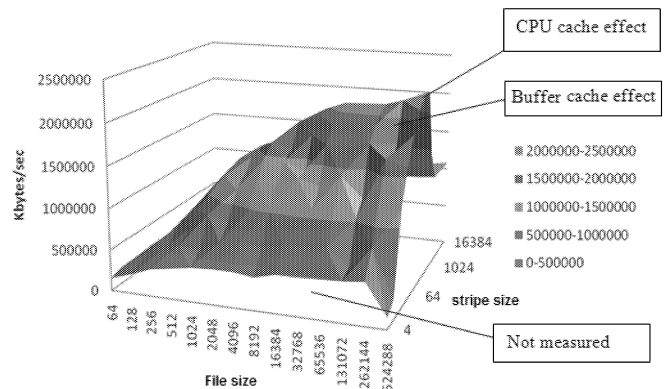
**Figure 4. Lustre throughput for Ping-Pong Benchmark**

Continuing the experiments, certain offsets have very high latencies. Considering this point, Lustre FS allocate its first indirect block. One can see from the data, the impact of this allocation is translated in latency for different operations (see Figure 5).



**Figure 5. Lustre latency for Ping-Pong Benchmark**

Considering the results presented for Read and Re-Read operations, Figure 6 presents a report regarding Read operation considering different file sizes and different stripe sizes. There are some lateral effects that influence the performance of this operation: first is the effect of buffer cache (maintaining the data stored in memory for a while) and the CPU cache effect, storing data for processing.



**Figure 6. Reader Test report for Ping-Pong Benchmark**



A sample of log file for our tests is:

```
Time Resolution = 0.000001 seconds.
Processor cache size set to 1024 Kbytes.
Processor cache line size set to 32 bytes.
File stride size set to 17 * record size.
Throughput test with 5 processes

Each process writes a 262144 Kbyte file in 4
Kbyte records

Children see throughput for 5 initial writers
    = 61570.22 KB/sec
Parent sees throughput for 5 initial writers
    = 37467.55 KB/sec
Min throughput per process
    = 9911.92 KB/sec
Max throughput per process
    = 15581.68 KB/sec
Average throughput per process
    = 12314.04 KB/sec
Min xfer = 167936.00 KB

Children see throughput for 5 rewriters
    = 65089.98 KB/sec
Parent sees throughput for 5 rewriters
    = 61649.19 KB/sec
Min throughput per process
    = 10390.88 KB/sec
Max throughput per process
    = 16787.00 KB/sec
Average throughput per process
    = 13018.00 KB/sec
Min xfer = 151552.00 KB
```

An adequate application that uses at the maximum level the performance of parallel storage in NCIT cluster is Air flow Simulator (Air (2011)), which is a solution that can be used for simulation and visualization of air flow and heat transfer in buildings using existing meshing tools such as SALOME and computational fluid dynamic engines such as Code-Saturne. The developed user-interface and post-processing procedures are also discussed. The paper provides an overview of existing technologies and protocols and shows how these technologies are used in the implementation of the proposed system [15].

## CONCLUSIONS

Cluster storage is an important piece of this puzzle called Cloud, and together with cloud computing represents cloud as technology destined for solving for example many

distributed applications. Worth saying that without a well optimized storage system much application that runs in cloud or a cluster can have a breakdown in performance.

This paper gives a perspective on performance on a storage system using IOzone tool, and special to characterize NCIT-CLUSTER and established the correct configuration parameters for different type of applications. I/O performance can suffer considerably if access data pattern is not the right one, especially in a parallel file system like Lustre. One important facility that a storage system based on Lustre file systems can give to the user is ability to set the stripe size and the number of stripes can be placed everywhere, because in this way the user can do better optimization of his application.

Regarding future work can be made a system that automatically makes profiling of the data model in applications that run on cluster or cloud and to suggest measures to improve performance.

## ACKNOWLEDGEMENTS

The research presented in this paper is supported by national project: "SORMSYS - Resource Management Optimization in Self-Organizing Large Scale Distributed Systems", Contract No. 5/28.07.2010, Project CNCSIS-PN-II-RU-PD ID: 201.

The work has been co-funded by the Sectorial Operational Program Human Resources Development 2007-2013 of the Romanian Ministry of Labor, Family and Social Protection through the Financial Agreement POSDRU/89/1.5/S/62557.

## REFERENCES

- [1] Huaiming Song, Yanlong Yin, Xian-He Sun, Rajeev Thakur, and Samuel Lang. 2011. Server-side I/O coordination for parallel file systems. In *Proceedings of 2011 International Conference for High Performance Computing, Networking, Storage and Analysis (SC '11)*. ACM, New York, NY, USA, Article 17, 11 pages.
- [2] Frank Schmuck and Roger Haskin. 2002. GPFS: a shared-disk file system for large computing clusters. In *Proceedings of the 1st USENIX conference on File and storage technologies (FAST'02)*. USENIX Association, Berkeley, CA, USA, 16-16.
- [3] Lustre file system, High Performance and Scalability, Web site: [www.lustre.org](http://www.lustre.org), Accessed on February 2012.
- [4] Niklas Edmundsson, Erik Elmroth, Bo Kagstrom, Markus Martensson, Mats Nylen, Ake Sandgren, and Mattias Wadenstein. 2004. Design and evaluation of a TOP100 Linux Super Cluster system: Research Articles. *Concurr. Comput. : Pract. Exper.* 16, 8 (July 2004), 735-750.
- [5] Jean-Pierre Prost, Richard Treumann, Richard Hedges, Bin Jia, and Alice Koniges. 2001. MPI-IO/GPFS, an optimized implementation of MPI-IO on top of GPFS. In *Proceedings of the 2001 ACM/IEEE conference on Supercomputing (CDROM) (Supercomputing '01)*. ACM, New York, NY, USA, 17-17.
- [6] H. Chen, J. Decker, and N. Bierbaum. 2006. Future networking for scalable I/O. In *Proceedings of the 24th IASTED*

- international conference on Parallel and distributed computing and networks(PDCN'06)*, T. Fahringer (Ed.). ACTA Press, Anaheim, CA, USA, 128-135.
- [7] IOzone Filesystem Benchmark, <http://www.iozone.org/> - web page of the project, Accessed on February 2012.
- [8] NCIT High Performance Computing Center Homepage, Web site: <http://cluster.grid.pub.ro/>, Accessed on February 2012.
- [9] Michael P. Kasick, Jiaqi Tan, Rajeev Gandhi, and Priya Narasimhan. 2010. Black-box problem diagnosis in parallel file systems. In *Proceedings of the 8th USENIX conference on File and storage technologies (FAST'10)*. USENIX Association, Berkeley, CA, USA, 4-4.
- [10] Huaiming Song, Yanlong Yin, Xian-He Sun, Rajeev Thakur, and Samuel Lang. 2011. A Segment-Level Adaptive Data Layout Scheme for Improved Load Balance in Parallel File Systems. In *Proceedings of the 2011 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID '11)*. IEEE Computer Society, Washington, DC, USA, 414-423.
- [11] Lei Lu, Hui Zhang, Guofei Jiang, Haifeng Chen, Kenji Yoshihira, and Evgenia Smirni. 2011. Untangling mixed information to calibrate resource utilization in virtual machines. In *Proceedings of the 8th ACM international conference on Autonomic computing (ICAC '11)*. ACM, New York, NY, USA, 151-160.
- [12] Understanding Lustre, Lustre 2.0 Operations Manual (821-2076-10), Chapter 1, ©2011, Oracle and/or its affiliates, [http://wiki.lustre.org/manual/LustreManual20\\_HTML/UnderstandingLustre.html](http://wiki.lustre.org/manual/LustreManual20_HTML/UnderstandingLustre.html), Accessed on February 2012.
- [13] Jean-Pierre Prost, Richard Treumann, Richard Hedges, Bin Jia, and Alice Koniges. 2001. MPI-IO/GPFS, an optimized implementation of MPI-IO on top of GPFS. In *Proceedings of the 2001 ACM/IEEE conference on Supercomputing (CDROM)* (Supercomputing '01). ACM, New York, NY, USA, 17-17.
- [14] Rajeev Thakur, William Gropp, and Ewing Lusk. 1999. Data Sieving and Collective I/O in ROMIO. In *Proceedings of the The 7th Symposium on the Frontiers of Massively Parallel Computation(FRONTIERS '99)*. IEEE Computer Society, Washington, DC, USA, 182-.
- [15] Alexandru Stroe, Emil Slusanschi, Ana Stroe, Simona Posea, Alexandru Herisanu, *Airflow Simulator Heat Transfer Computer Simulations of the NCIT-Cluster Datacenter*, The 18th International Conference on Control System and Computer Science, 2011, pp: 569-575
- [16] Devarshi Ghoshal, Richard Shane Canon, and Lavanya Ramakrishnan. 2011. I/O performance of virtualized cloud environments. In *Proceedings of the second international workshop on Data intensive computing in the clouds (DataCloud-SC '11)*. ACM, New York, NY, USA, 71-80.
- [17] Julian Borrill, Leonid Oliker, John Shalf, and Hongzhang Shan. 2007. Investigation of leading HPC I/O performance using a scientific-application derived benchmark. In *Proceedings of the 2007 ACM/IEEE conference on Supercomputing (SC '07)*. ACM, New York, NY, USA, , Article 10 , 12 pages.

# PROPOSAL OF SMOOTH CHANNEL SWITCHING MECHANISM FOR P2P STREAMING AND ITS APPLICATION

Naomi Terada

The University of  
Electro-Communications  
1-5-1 Chofugaoka, Chofu, Tokyo  
182-8585, Japan  
E-mail: naomi-te@is.naist.jp

Eiji Kominami \*

Atsuo Inomata  
Kazutoshi Fujikawa  
Nara Institute of Science and  
Technology  
8916-5 Takayama-cho, Ikoma, Nara  
630-0192, Japan  
E-mail: atsuo@is.naist.jp,  
fujikawa@itc.naist.jp

Eiji Kawai

National Institute of Information and  
Communications Technology  
1-8-1 Otemachi, Chiyoda-ku, Tokyo  
100-0004, Japan  
E-mail: eiji-ka@nict.go.jp

Hideki Sunahara

Keio University  
4-1-1 Hiyoshi Kohoku-ku Yokohama,  
Kanagawa, 223-8526, Japan  
E-mail: suna@wide.ad.jp

## KEYWORDS

Streaming, Peer-to-peer networks, Zapping

## ABSTRACT

In this paper, we present a smooth channel switching mechanism for enhancing the performance and reducing traffic of distributed peer-to-peer video streaming. This mechanism is designed for a system that uses a backup link and a *Predicted Link* to avoid congestion among nodes. Furthermore, it provides a *Preferred Keyword* procedure to reduce the channel switching time while switching from peer to peer. We present the implementation design and experimental results of this proposed mechanism and conclude that the *Predicted Link* is efficient in reducing channel switching time.

## 1. INTRODUCTION

Recently, live streaming has gained considerable attention with the improvement of network infrastructure and client PC performance. As one of many live streaming services, Ustream[11] is a website that consists of a network of diverse channels providing a platform for lifecasting and live video streaming of events online. Obviously, an IP-based streaming service has limitations of server and network capacity, and hence, a viewer client cannot receive all channels simultaneously as TV broadcasting can. Therefore, when a user changes the channel, he or she is forced to wait for a few seconds until the content data is retrieved. This waiting period is known as a zapping time, and it degrades the QoS of live streaming.

In addition to this zapping time, start-up delay and playback continuity are the main issues related to live streaming QoS. Different from server-client live streaming, P2P client

node is affected by the leaving behavior of peers. Therefore, previous studies have mainly focused on maintaining a distributed-tree [7] or managing multi-source stream[2].

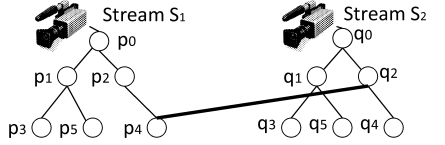
## 2. RELATED WORK

Several studies have reported the performance measurements of P2P streaming networks [8], [3], [5]; further, the results of the performance measurements of a multi-channel P2P streaming network has also been reported [12]. Another work has revealed that over three-quarters of all users switched between channels streaming similar genre of contents [4](e.g., news, sport, music). This indicates that the probability of a user switching to a channel with different content is not equal. A probabilistic switching algorithm has also been proposed [9]. We focused on users' preference while switching between streaming contents, assuming that each user has their own viewing pattern. We also considered the genre of the content as important in identifying the viewing pattern.

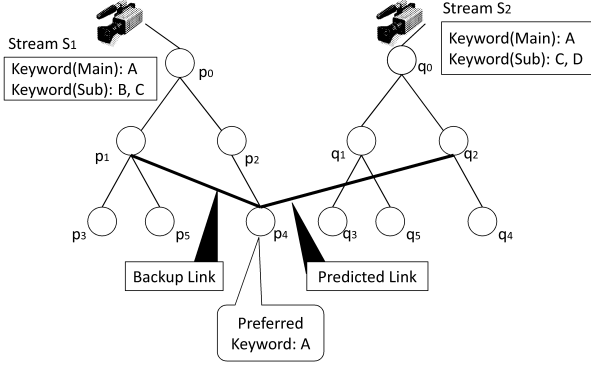
In this paper, we propose a mechanism to achieve the following: 1) predict the next probable stream source on the basis of users' preferences, and preload streaming data in advance to reduce zapping time; 2) improve playback continuity using backup links.

PeerCast[13] adopts an index server to manage multi-source streams. Figure 1 shows a tree-based P2P distribution system for multi-source streaming. A peer willing to join a *Stream S<sub>1</sub>* sends a query to an index server to find the IP address of a root peer  $p_0$ . Next, the peer joins the tree that originates from source  $S_1$ . Anysee[10] provides live media streaming to enlarge scale number of users. However, these systems do not focus on reducing waiting time.

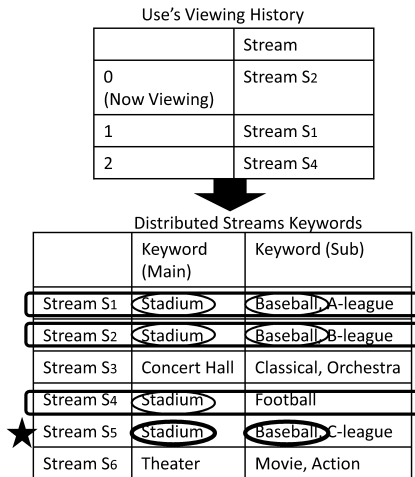
\* He is now working in Asahi Broadcasting Corporation.



**Figure 1.** Multi-Source Live Streaming



**Figure 2.** Backup Link and Predicted Link



**Figure 3.** An Example of Preferred Keyword Selection from User's Viewing List

### 3. PROPOSED SCHEME

We focused on the reduction of mean time to switch between multi-source streams. To minimize switching overhead, each peer should ideally have links to every stream ( $Streams S_1$  to  $S_n$ ); however, this approach is unrealistic because too many links generate an excessive amount of keep-alive messages, thus increasing network traffic. Our basic idea is to predict the next stream that is likely to be selected by considering a user's viewing history and to prefetch the streaming data for smooth switching between streams. We assume that prefetching streaming data can reduce zapping time considerably; this is because when a user switches to other content in an ordinary tree-based P2P system, a peer must send a few search requests to an index server and wait for a while. Further, at the beginning of the new connection, data buffering takes a few seconds. Basically, this peer join-

ing procedure is similar to that in Peercast; however, in our system, a joined peer attempts to link to other peers in order to prepare for link failed and channel switching. Therefore, some peers can be used to relay stream clips to other children peers. However, this solution is suitable for large-scale live streaming such as at a baseball stadium or a concert hall, where multiple cameras can be easily setup and maintained but reliability is still low.

#### 3.1 Backup Link

As shown in Figure 2, each content stream ( $Streams S_1$  and  $S_2$ ) has its own distribution tree.  $p_0$  is the root peer of  $Stream S_1$ , and  $q_0$  is the root peer of  $Stream S_2$ . In our proposed system, every peer is linked to another peer to receive stream data ( $p_4$  is linked to  $p_2$ ). Adding to this link, the peer tries to link another backup link ( $p_4$  is linked to  $p_1$ ) in case the original link fails.

#### 3.2 Predicted Link

Each stream has at least two keywords, as shown in Figure 2. A root peer sends its keywords to an index server when it begins streaming, and the index server stores those keywords with the root peer's IP address. A stream must have one main keyword to describe the location information of the live stream. We executed a preliminary observation to evaluate which keyword is a key factor for prediction of the next stream. This observation revealed that location information is this key factor, and additional information is described by sub keywords.

Figure 3 shows selection of the most frequently appearing keyword (*Preferred Keyword*). Some frequently appearing keywords are extracted from a user's viewing history. In this example, "Stadium" is defined as a *Preferred Keyword*. This means that any stream having "Stadium" as the main keyword is most likely to be viewed next.

We classified viewing history statuses into the following three cases.

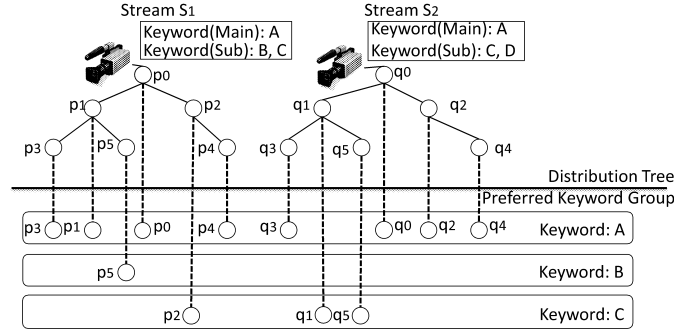
1. A peer has no users' viewing history
2. There is no corresponding keyword among users' viewing history
3. Some keywords are duplicated among users' viewing history

In the first and second case, the main keyword of a playback stream is assigned to a *Preferred Keyword*. In the third case, a duplicated main keyword is assigned to a *Preferred Keyword*. Figure 4 shows peer groups suiting preferences of users. Besides the distribution tree, peers are grouped according to a user's preference by using *Preferred Keyword*. For example,  $p_3$  attempts to establish a *Predicted Link* to  $Stream S_2$  because  $p_3$  belongs to *Preferred Keyword Group A* and  $Stream S_2$  also has keyword  $A$  as its main keyword.

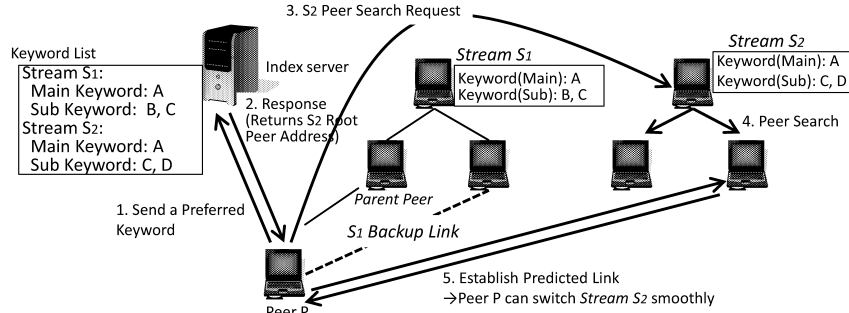
#### 3.3 Experimental Setup

Figure 5 shows a procedure for establishing *Predicted Link*.

1. Peer  $P$  sends a *Preferred Keyword* extracted from a user's viewing history (Peer  $P$ 's *Preferred Keyword* is "A")
2. The index server refers to the keyword list and returns the IP address of  $Stream S_2$ 's root peer



**Figure 4.** Example of Distribution Tree and Preferred Keyword Groups



**Figure 5.** Process for Establishing *Predicted Link*

3. *Peer P* sends a search request to *Stream S2*'s root peer
4. *Stream S2*'s root peer sends *Peer P*'s search requests to its child peers in order to find a peer that is ready to distribute to *Peer P*
5. *Stream S2*'s root peer returns a child peer's IP address to *Peer P*, and *Peer P* attempts to establish a *Predicted Link*

This procedure is run as a background process. *Peer P* uses the *Predicted Link* when a *Peer P* user switches to *Stream S2*. The index server maintains a root peer list, and once a peer establishes a *Predicted Link*, it periodically exchanges keep-alive messages. It should be noted that *peer P* continues forwarding *Stream S1* until it leaves the network. It is important to keep the distribution tree simple in order to prevent frequent restructuring of the tree. To run and test the designed system, we implemented a prototype system as a desktop application using Java Media Framework RTP API.

As shown in Table 1, we executed a set of experiments to evaluate the performance of our proposed scheme. Each server generates up to 100 peers, and the total number of peers on this P2P network is 1000.

**Table 1.** Video and Machines

Video Resolution	320 pixels × 240 pixels
Video Framerate	15 fps
Stream Bitrate	500 kbps
Servers	10
Peers	1000

### 3.4 Utilization of Predicted Links

We first examine the effectiveness of a *Predicted Link* with *Preferred Keyword*. In this experiment, we focused

on the usage frequency and efficiency of a *Predicted Link* when a user switches channels. The participants watched streams having zapping time, and the total number of channel switches was 194, as listed in Table 2.

The utilization of a *Predicted Link* using *Preferred Keywords* was 38.1%, as listed in Table 3. We also calculated the utilization of a *Predicted Link* that randomly links to other peers, unlike our proposed system, and we found that the utilization was only 9.8%. This shows that a *Predicted Link* with *Preferred Keyword* extracted from a user's viewing history is effective in determining the user's next action. In the simple tree-based P2P, the utilization of *Predicted Link* was 0% because it does not include a *Predicted Link*.

Our proposed system selects a *Preferred Keyword* from main keywords (high priority) and sub keywords (low priority); however, the experimental results show that a *Preferred Keyword* is selected from main keywords more often. As shown in table 4, the next switched stream is estimated more precisely by using only the main keyword.

**Table 2.** Experimental Conditions and Results

Number of Streams	6
Number of Keywords	2(Main) 7(Sub)
Participants	14
Number of Channel Switches	194

**Table 3.** Utilization of Predicted Links

Algorithm	Utilization of Predicted links(%)
Predicted Link	38.1
Link Random	9.8
Simple Tree-Based P2P	0

**Table 4.** Determination of Preferred Keywords

From main keyword only	42.2%
From main (priority) and sub keywords	38.1%
From main and sub keywords	15.4

### 3.5 Channel Switching Delay

We measured the channel switching delay. As seen in Figure 6, channel switching delay increases linearly with the number of peers in both simple tree-based p2p and our *Predicted Link* approach.

We show three patterns in our proposed algorithm:

#### 3.5.1 The Best Case

In the best case, users always used *Predicted Link*. This means the users switched streams on the basis of the *Preferred Keyword*, and therefore, switched between content in the same group.

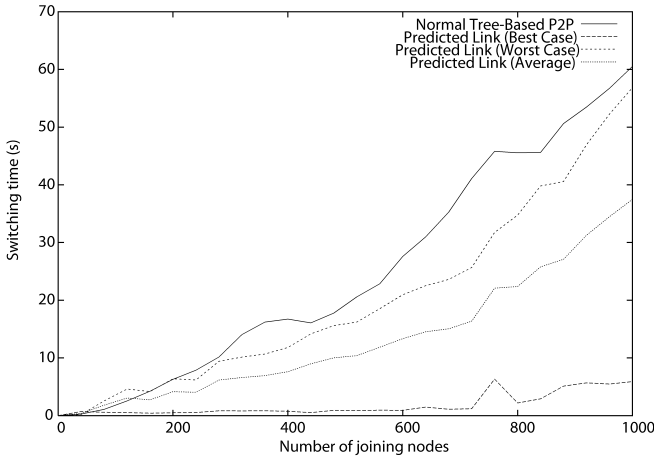
#### 3.5.2 The Worst Case

In this case, users did not use *Predicted Link*.

#### 3.5.3 Average

This scenario is based on the utilization of *Predicted Link* (Table 3); 38.1% of the channel switching was based on *Predicted Link* whereas the other 61.9% was not.

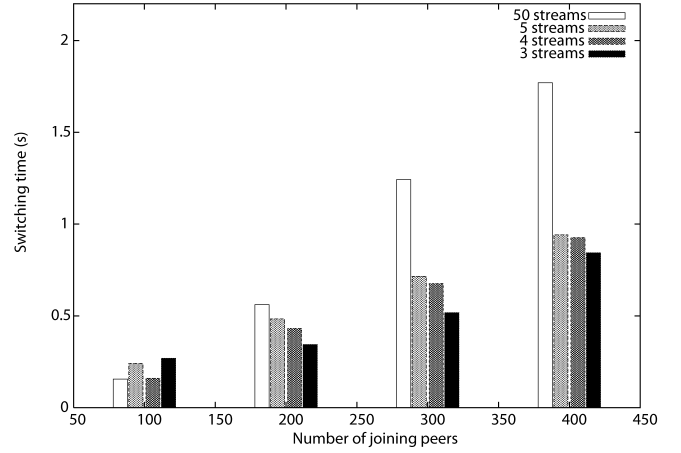
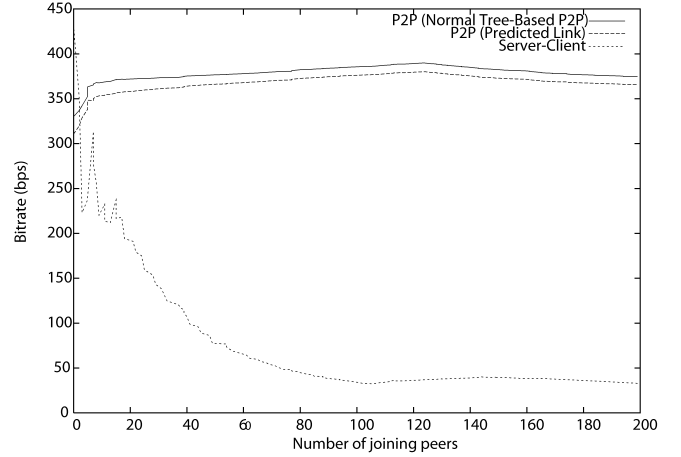
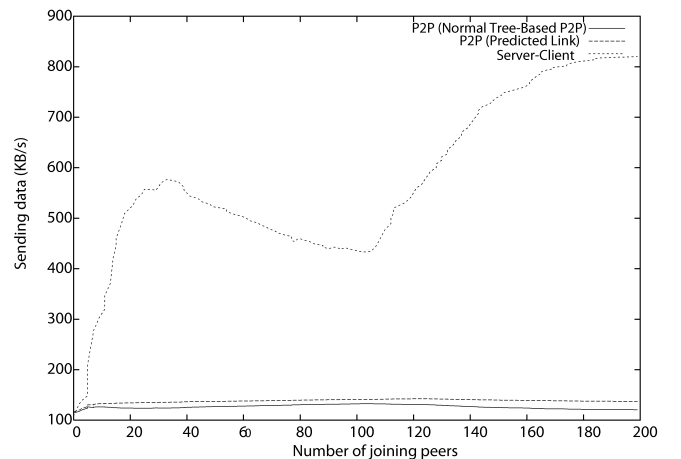
In a tree-based P2P system, as the number of peers joining the network increases, an excessive amount of search messages degrade the system performance[1]. In our proposed system, each peer has a list of peers in the same *Preferred Keyword* group, and *Predicted Link* is used as long as a user switches channels in the same group; this means that search messages are not exchanged.

**Figure 6.** Channel Switching Delay

### 3.6 Predicted Link Optimization

In section 3.2, we mentioned that a peer attempts to establish *Predicted Links* to streams having the same *Preferred Keyword*. As the number of streams in one group increases, an excessive amount *Predicted Links* are established, and hence, the network resources are strained. A survey has revealed that the channel switching delay should be limited to a maximum of 2 s [6], and other domestic research has shown that this delay should be limited to within 1 s. Figure

7 shows that the channel switching delay reaches this limit (1 second) when 5 streams are in one group. In our prototype system, each peer has a *Predicted Link* to every other node in the same group, and hence, the number of streams in one group should be less than 5.

**Figure 7.** Switching Time and Number of Peers in a Group**Figure 8.** Streaming Bitrate**Figure 9.** Streaming Data Traffic on a Root peer

### 3.7 Load of the Index Server

Figure 10 shows the query response time from the index server, and the query response time is constant. This shows

that the index server could deal with a load of a minimum of 1000 peers, without any difficulty.

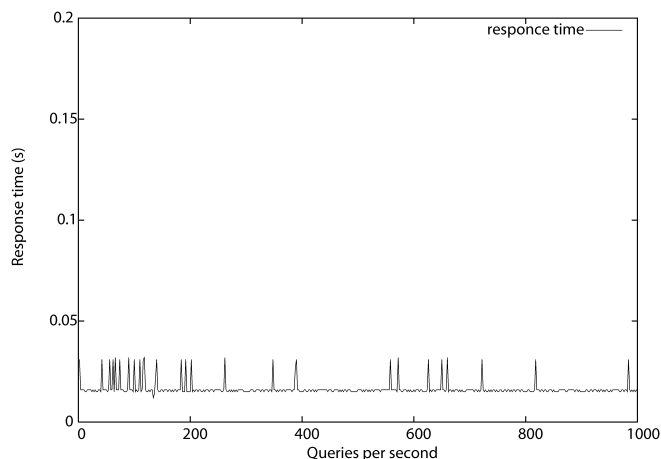


Figure 10. Query Response Time

### 3.8 Scalability

Presently, multi-bit rate streaming is widely adopted in most streaming applications. It adjusts streaming bitrate dynamically according to actual network throughput, and therefore, bit-rate degradation is observed under congested traffic conditions. For streaming of a high-quality movie, the server-client system shows a reduction of bit rate whereas the P2P distributed system and our proposed method maintains the bit rate, as shown in Figure 8.

Figure 9 shows streaming data traffic on a root peer. Compared to the server-client system, the P2P distributed system reduces network traffic dramatically. In the server-client system, a reduction in traffic was observed when the number of joining peers was around 100. We assumed that multi-bit rate streaming began to reduce video quality, and this decreased server-side traffic when the number of joining peers was around 100 s. Subsequently, traffic increased linearly with the number of joining peers.

## 4. CONCLUSION

In this paper, we presented a smooth channel switching mechanism for P2P streaming. It features 1) prediction of a probable next source and prefetching of streams to reduce zapping time and 2) improvement of playback continuity using backup links. We attempted to extract *Preferred Keyword* from users' viewing history and to group peers for establishing a *Predicted Link*.

Our experiments show that *Predicted Link* is effective when a user switches channels, and our proposed system reduces channel switching time for high-quality video even if the number of joining peers are increasing.

However, the performance of our system can be further improved. In the current system, *Preferred Keyword* is simply chosen from main or sub keywords of streams; however, our set of experiments shows that users switch channels according to the main keyword rather than sub keywords. In our future work, we can improve the method for creation of the keyword list and for selection of appropriate *Predicted Link*.

## REFERENCES

- [1] K. Aberer. Scalable data access in peer-to-peer systems using unbalanced search trees. In *In Proc. of Workshop on Distributed Data and Structures, WDAS 2002*, 2002.
- [2] V. Agarwal and R. Rejaie. Adaptive multi-source streaming in heterogeneous peer-to-peer networks. In *SPIE Conf on Multimedia Computing and Networking*, 2005.
- [3] E. Alessandria, M. Gallo, E. Leonardi, M. Mellia, and M. Meo. P2p-tv systems under adverse network conditions: a measurement study. In *Proceedings of the 28th Conference on Computer Communications, IEEE INFOCOM 2009*, pages 100–108, 2009.
- [4] M. Cha, P. Rodriguez, J. Crowcroft, S. Moon, and X. Amatriain. Watching television over an ip network. In *Proceedings of the 8th ACM SIGCOMM Conference on Internet Measurement, IMC '08*, pages 71–84, New York, NY, USA, 2008. ACM. ISBN 978-1-60558-334-1. URL <http://doi.acm.org/10.1145/1452520.1452529>.
- [5] D. Ciullo, M. Garcia, A. Horvath, E. Leonardi, M. Mellia, D. Rossi, M. Telek, and P. Veglia. Network awareness of p2p live streaming applications: A measurement study. *Multimedia, IEEE Transactions on*, 12(1):54–63, 2010. ISSN 1520-9210.
- [6] DSLForum. Triple-play services quality of experience(qoe) requirements. In *Technical Report, TR-126*, 2006.
- [7] M. S. Duc, D. A. Tran, K. A. Hua, and T. T. Do. Zigzag: An efficient peer-to-peer scheme for media streaming. In *In Proc. of IEEE Infocom*, 2003.
- [8] P. Gao, T. Liu, Y. Chen, X. Wu, Y. El-khatib, and E. Christopher. The measurement and modeling of a p2p streaming video service. In *Proceedings of the Second International Conference on Networks for Grid Applications (Grid-Nets2008)*, October 2008.
- [9] A. M. Kermarrec, E. Merrer, Y. Liu, and G. Simon. Surfing peer-to-peer iptv: Distributed channel switching. In *Proceedings of the 15th International Euro-Par Conference on Parallel Processing, Euro-Par '09*, pages 574–586, Berlin, Heidelberg, 2009. Springer-Verlag. ISBN 978-3-642-03868-6. URL [http://dx.doi.org/10.1007/978-3-642-03869-3\\_54](http://dx.doi.org/10.1007/978-3-642-03869-3_54).
- [10] X. Liao, H. Jin, Y. Liu, L. M. Ni, and D. Deng. Anysee: Peer-to-peer live streaming. In *INFOCOM*, 2006.
- [11] Ustream. <http://www.ustream.tv/>.
- [12] C. Wu, B. Li, and S. Zhao. Multi-channel live p2p streaming: Refocusing on servers. In *Proceedings of the 27th Conference on Computer Communications. IEEE INFOCOM 2008*, pages 1355–1363, April 2008.
- [13] J. Zhang, L. Liu, L. Ramaswamy, and C. Pu. Peercast: Churn-resilient end system multicast on heterogeneous overlay networks. *J. Network and Computer Applications*, 31(4):821–850, 2008.

# WIRELESS ROUTER AS A PHYSICAL ACCESS CONTROL SYSTEM (WRPACS)

Dragos Comaneci, Silvia Stegaru and Ciprian Dobre  
Department of Computer Science  
University POLITEHNICA of Bucharest  
Spl. Independentei, 313, Bucharest  
Romania

E-mails: [dragos@comaneci.ro](mailto:dragos@comaneci.ro), [silvia.stegaru@cti.pub.ro](mailto:silvia.stegaru@cti.pub.ro), [ciprian.dobre@cs.pub.ro](mailto:ciprian.dobre@cs.pub.ro)

## KEYWORDS

wireless router, access control, microcontroller, magnetic lock, smartphone

## ABSTRACT

Smartphones today integrate many sensors and provide large computing capacities. They enable the shift towards massive quantities of real-time information becoming access push rather than demand pull on a global case. CAPIM, a platform to support such a paradigm, integrates services to monitor and a context for adapting with the user's context using the sensors and capabilities of smartphones, together with online social data. It integrates context-aware services that are dynamically configurable and use the user's location, identity, preferences, profile, and relations with individuals, as well as capabilities of the mobile devices to manifest themselves in many different ways and re-invent themselves over and over again. In this paper we present the design and development details of the security and user identification components to support these services. We propose a secure platform for user authentication and session management, based on public key infrastructure (PKI) services. We analyze its strengths and weaknesses, and present as a case study the particular extension of the platform to support secure user access to restricted areas of a building. We also discuss an analysis of the implementation, cost assessments and problems that might arise, as a methodology to support the construction of mobile and context-oriented applications.

## 1. INTRODUCTION

As people realize that having more sensing and computing capabilities in every-day situations is attractive for many reasons, smartphones become commodity hardware.

Their success is the basis for a shift towards developing mobile applications that are capable to recognize and pro-actively react to user's environment.

Such context-aware mobile applications can help people better interact between themselves and with their surrounding environments. This is the basis for a paradigm where the context is actively used by applications designed to take smarter and automated decisions: mute the phone when user is in meeting, show relevant information for the user's current location, etc. CAPIM (Context-Aware Platform using Integrated Mobile services) (Dobre et al. 2011) is a solution designed to support the construction of context-aware applications. It integrates services designed to collect context data (location, user's interests and

characteristics, as well as the environmental data) and use it to provide a richer and simpler experience for the end user.

In the present work we provide an implementation of a fundamental part of CAPIM's design considerations for the management of user identity in context-aware applications. The user's identity is required by many context models. It can be used to infer preferences that are actively used in favor of the user, or it is used to provide personalized sets of services.

Today Public Key Infrastructures (PKI) solutions are generally accepted to support the management of identity. PKI provides a standardized and legally recognized service support (Carayannis and Turner 2006). Therefore it makes sense to use such services in providing electronic identity in context-aware integrated mobile services. PKI provides services such as confidentiality, integrity, authentication and non-repudiation (Ravi et al. 2005). By using the standards defined by PKI we can develop an approach to support the construction of rich context-aware applications that use the identity of the user as active context information. In particular, the security layer is used from the construction of social-aware mobile applications to intelligent housing, capable of actively recognizing the user entering the room for example. As such, in our current paper we shall focus on a mechanism for secure access to a physical area of a building built on top of CAPIM that leverages off the shelf hardware components (such as a wireless router) in order to provide the required services.

The rest of the paper is structured as follows. Section 2 presents similar projects already implemented to secure user access using a mobile handset. Section 3 shows an overview of the architecture of the system with a short description of all the main components and their role. Section 4 presents some implementation details of the core services present on the wireless router. Section 5 deals with test scenarios, possible system vulnerabilities and results as well as system deployment issues and costs. In Section 6 we conclude our discussion and present future work.

## 2. RELATED WORK

A similar notable project in the area of secure user access to restricted areas of a building with the use of a mobile handset has been developed at the Disco Lab at Rutgers University (Ravi et. al 2005; Iftode et. al 2004). Although the approach is different from our own (both in technology and system design), the goal is similar: to allow the use of a



mobile handset as an electronic key, or, more generally, and electronic ID in order to access distributed services. However, we provide a more generic platform that actually include context as part of the entire process. Our proposed platform provides security guarantees as to who is accessing the contextual services, where people are. It instruments using context-oriented policies the interactions between peoples and services. In particular, we present a case study for the use of the platform as a tool to create a simple instrument to mediate the access for the user inside an intelligent building, capable of recognizing the user.

### 3. ARCHITECTURE

The proposed system requires the interaction of many different components. These components can be summarized into two main parts : the Secure Service Communication Platform (SSCP) and the Secure Area Access Service (SAAS) that is built on top of SSCP.

#### 3.1. The Secure Service Communication Platform (SSCP)

The main components of SSCP are presented in Figure 1. On the mobile side two services are executed: the CAPIM Secure Communication Service, and the User Security Service. The CAPIM Secure Communication Service is responsible for session establishment, as well as for communication with other services that require user identification. The User Security Service implements the PKI operations for loading the user certificate, establishing of an SSL context for example, etc.

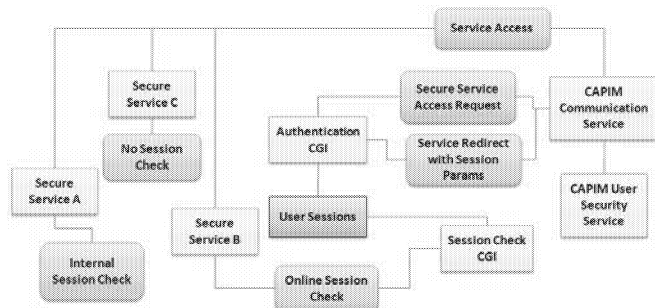


Figure 1: SSCP Main Components

On the server side of the platform there are main two components responsible for authentication and authorization. The authentication CGI (Common Gateway Interface) component is responsible for verifying the credential of the user, for creating the appropriate session and registering it in a local database. The session check CGI component, as its name suggests, is used by the other services as an interface to check validity and retrieve information related to the user's context (such as the user's rights as defined by the security policy).

For more fine-grained audit requirements, the sessions can be established per service. In this case the communication service on the client-side, upon authentication, also submits the name of the service that it requires access to. The authentication CGI verifies the name of the service in the local database, retrieves a certificate associated with that service, and uses the associated public key to encrypt a hash

of the session key. The services themselves are further responsible for specific objects and actions that the user can access within the service.

As illustrated in Figure 1, the services have three options for checking the user session, depending on the service requirements. The first option, used in the figure by service A, is an internal check of the session key. The session key is signed by the authentication service with its private key, so other services that have the certificate of the authentication service can use the public key stored within it to check the signature. This approach for verification is fast, but it involves processing on the service receiving the session key. Also, not much information about the user can be stored within the session key (which should be small, because it is transmitted with each request the user makes for a service). Therefore, this approach is suitable for services that only require a valid user and no other information (for example security rights).

The second option of verification, used by service B in Figure 1, is online session check. In this case the service receiving the session key from the user establishes a connection to the session check CGI. The session check CGI looks up the session in its' local database, retrieves the information associated with it (such as user details, user rights, etc.) and sends this information back to the requesting service. This approach involves minimal work on the service side but is also much slower since it requires communicating with the session check CGI. Another advantage is that the service can retrieve bundles of information associated with the user.

The third option (provided for consistency) is for services that do not require user identification. In this case the service simply ignores the session key.

#### 3.2. The Secure Area Access Service

Access to a secure area of a building has always been a constant security problem and a lot of specialized solutions have been developed to facilitate this service (Hwang and Baek 2007; Hsu et. al 2009; Park et. al 2009). Still, today they are either impractical for the user or lack the necessary security required for accessing sensitive areas. Also, the costs, both in equipment and training involved in implementing some of the solutions are prohibitive.

The approach proposed in CAPIM is feasible because many users today carry at least one smartphone. The idea is to have a key in the form of a digital certificate and associated private key stored on the mobile smartphone and, after authenticating through SSCP and getting a session key, use the obtained session key to send an access request for a certain area to the service.

To access the authentication service, the phone needs to have network connectivity with the server hosting the authentication CGI. This can be attained through different technologies, the most common being a local Wi-Fi network. Another option is for the phone to be connected to the mobile provider's data network and connect to the network where the authentication server resides through a secure tunnel such as VPN. For our purposes we shall consider a local Wi-Fi connection. Still, because the average Wi-Fi

communication range is tens of meters, a more proximity based solution is needed to determine that the user is in the presence of a door that protects access to a secure area. Hence, we can use Bluetooth for such a purpose.

Energy consumption also needs to be taken into consideration as our solution will have to employ different radio access technologies in order to attain its purpose. As such, we need to ensure that only one radio technology (3G/Wi-Fi/Bluetooth) needs to be active on the mobile device while performing the procedures described in the solution.

The proposed solution works as follow. In the beginning the users' mobile smartphone is connected to the local Wi-Fi network and authenticated through SSCP, thus having a valid session key. Using the location service the mobile handset determines that it is in the proximity of a door that leads to a restricted area, and automatically turns on the Bluetooth receiver on the phone and scans the area for devices. The mobile handset finds the device corresponding to the Bluetooth dongle of the door and proceeds to generating a random shared-key that will be used for the association between the two Bluetooth devices. The random shared-key is posted along with the MAC address of the mobile handset via Wi-Fi to the Secure Area Access Service (SAAS). The mobile handset then begins the Bluetooth association procedure with the dongle of the door. The device controlling the Bluetooth dongle of the door detects the MAC of the device trying to associate and queries the SAAS for the random shared-key generated by the mobile handset, retrieves it and uses it to carry out Bluetooth

association. After the association is complete the mobile handset sends a hello message and the door is opened. The association between the two devices is kept for a limited amount of time (for example 1-2 hours) so further access through the door are simple. A visual representation of this process is presented in Figure 2.

To ensure a higher level of security for extra-sensitive areas, the SAAS may require the user to prove its identity. This is done using a biometric service based on face recognition (Comaneci and Vlad 2011), but this can easily be adapted to alternate biometric inputs, such as voice or fingerprint. This type of verification is configurable for each area protected by SAAS.

Figure 2 also presents the components responsible for communication between the router and microcontroller board controlling the magnetic lock. The kernel module registers itself as a USB device driver on the router and exposes a simple char device interface that can be used by the Lock Service daemon in order to send open commands to the microcontroller that controls the actual magnetic lock.

The main components of the Secure Area Access Context Service are presented in Figure 3. Emphasis is given to the location of each component in the system. The Lock Service daemon resides on the router controlling access to one or more restricted areas of a building. The daemon is responsible for monitoring Bluetooth connection requests from different Bluetooth dongle receivers connected via USB to router and also servicing door open requests for the doors it controls.

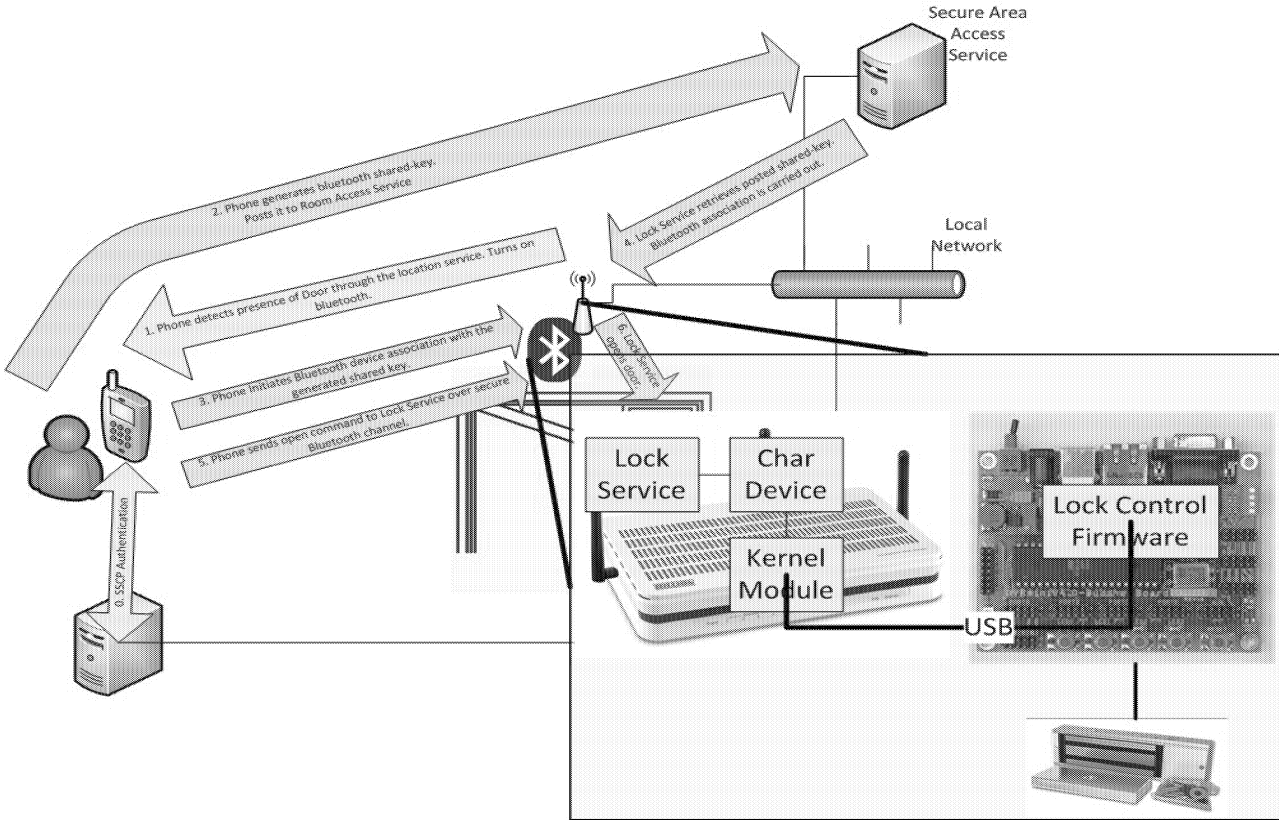


Fig 2: Schematic representation of the security process.

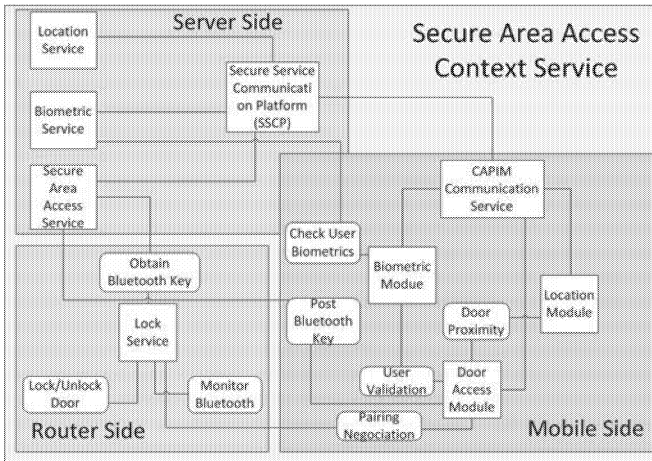


Figure 3: SAAS main components

On the server side there is the Room Access Service, which is a Bluetooth shared-key repository where the mobile handset posts the randomly generated shared-key for Bluetooth association, along with the MAC address of the handset, the Lock Service present on the router following up and retrieving the posted key. Also on the server side the Location Service offers information regarding the location of access points to restricted area, and the Biometric Service which checks user biometrics and can be used in case of highly restricted areas.

On the mobile side there is the Door Access Module, responsible for Bluetooth association, and the management of door access requests generated from door proximity alerts coming from the Location Module. Also, on the mobile side there is the Biometric Module, responsible for taking a photograph using the mobile handset integrated camera of the current user and sending it to the Biometric Service for verification.

From a user point of view, all of the processes described (with the exception of the biometric verification) should execute transparently in the background without any user intervention. The user interface should only provide status information in order for the user to be able to investigate any problems that might arise during the process. An example of the available user interface is provided in Figure 4.

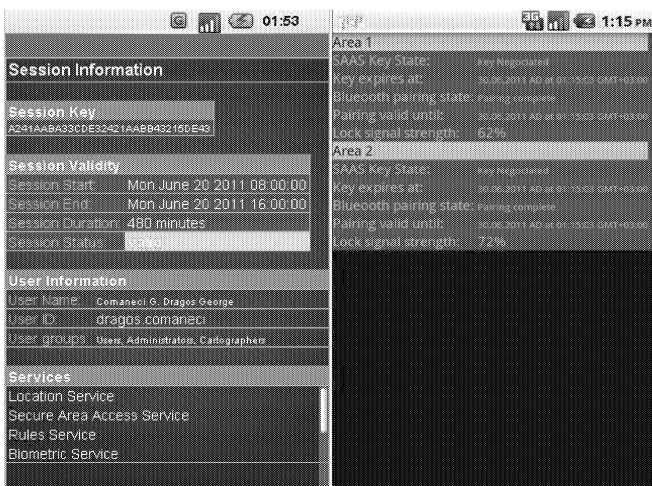


Figure 4: Mobile device information interface for SAAS and SSCP

## 4. IMPLEMENTATION

For the implementation and testing of the Lock Service an Asus 500gP V2 router with two USB ports was used. The firmware was replaced with the one provided by the open-source project DD-WRT [cyber09] in order to have root access to the device and install the Bluetooth and door controller modules, along with the Lock Service. The Lock Service was developed in C++ and cross compiled for the MIPS32 platform to work with the processor present on the router. The Lock Service also uses the BlueZ Bluetooth library for accessing the dongle connected to the router and OpenSSL for accessing the Room Access Service.

A kernel module was also developed for communicating with the microcontroller board. It exposes a char device interface that can be used to both inspect the current status of the microcontroller and send open commands to the magnetic lock. The kernel module relies on the usbcore driver module and was compiled for the Linux 2.4 kernel because DD-WRT for Asus 500gP V2 only supports a 2.4.

An example of the hardware configuration is presented in Figure 5. The Room Access Service was developed, as in the case of SSCP, in C++ using FastCGI for communicating with the hosting web server. It stores the shared keys in a database and uses unixODBC for database access so that any flavor of database can be configured with it.

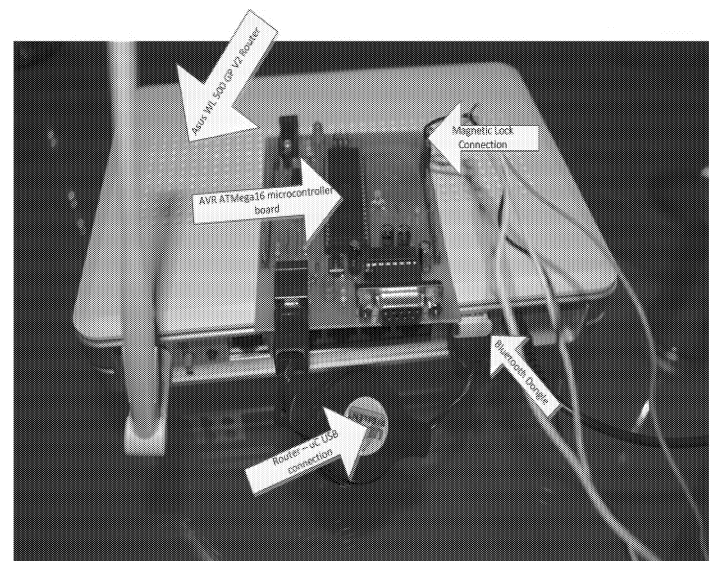


Figure 5: One possible hardware configuration

The Biometric Service was developed in Java as a distributed service that supports multiple dispatchers and workers and uses the EigenFace image matching algorithm (Zhang et. al 1997). A more detailed description of the Biometric Service can be found in (Comaneci and Vlad 2011). Details regarding the Location Service and Location Module, developed within the CAPIM project, are available in references (Militaru 2011; Greceanu 2011).

In order to communicate with the magnetic lock the router was connected to a custom board through USB (as seen in Figure 5). The microcontroller used, Atmel ATmega16, was first flashed with AVRUSBBootloader (an USB bootloader for Atmel AVR controllers) to make it easier to program

directly from the computer. The bootloader then loads our program at startup.

We have used the V-USB firmware for low-speed USB devices, modifying it to accept lock / unlock commands from the connected device, in our case the router. It then processes the command and acts accordingly, thus opening or closing the magnetic lock. First the V-USB microcontroller parameters were modified to work with our configuration. Secondly, we had to modify the driver signal interceptor so it would accept only the commands specified and ignore anything else received.

## 5. SCENARIOS AND RESULTS

Being a complex system, several test scenarios have been developed in order to assess the overall security and possible attack vectors. This section presents different scenarios suitable for our system, as well as performance and reliability tests.

### 5.1. Possible Security Attacks

Possible security breaches can stem from the technology in use as well as from the human element of the system, the mobile handset user. From a technology point of view, a possible attack can be expected in the form of an SSL man-in-the-middle attack. The man-in-the-middle attack (MITM), bucket-brigade attack, or sometimes Janus attack, is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, despite the fact that the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones.

A man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to the satisfaction of the other, thus making it an attack on mutual authentication. In order to prevent this type of attack, SSL authenticates the server using a mutually trusted certification authority. As such, it is recommended that an internal private highly secured certification authority be used in order to generate the user and server certificates used within the system. An attacker, in order to apply the MITM attack would first need to obtain a certificate and associated private key that can be used as a server certificate from that specific certification authority. To prevent even the case in which an attacker manages to obtain such a certificate, we can construct a trusted certificate store containing all the certificates belonging to the services within the system and check this store during the SSL context establishment. Of course, in this case, some sort of update mechanism needs to exist in order to modify the certificate store in case of expiration or revocation. The certificate store update may be correlated with the CAPIM application updates.

The Bluetooth pairing mechanism can also constitute another attack vector but this implies that the attacker be able to listen in on the Bluetooth communication between the mobile handset and the locking mechanism. Also, since the pairing keys have a limited validity time, the attacker

would need to intercept the pairing process once more in order to gain subsequent access to an area.

A denial of service attack (DOS) is also possible but can be easily prevented (at least on the server side components) through the use of the `mod_evasive` Apache DOS protection module.

Another possible attack would be for an attacker to be able to copy the user certificate and associated private key off the mobile handset and use as is. A completely secure solution to this problem can only exist if we can implement the equivalent of a PKI hardware token on the mobile handset. This can be done with the use of a specific component present on ARM processors dubbed TrustZone.

### 5.2. Solution Cost Assessment

The project was designed to be as cheap to implement as possible so, for the server components, existing computing hardware may be used. The only costs incurred are for the routers, Bluetooth dongles, magnetic locks and magnetic lock controllers. A two USB port WiFi router can be found at a medium price of 60 euros. A Bluetooth dongle compatible with BlueZ incurs a cost of 20 euros. The magnetic lock controller can be built out of a microcontroller board with an USB port and two relays that control the locking mechanism, the total component costs for it being around 20 euros. The most expensive component is the magnetic lock itself which, on average, has a cost of 100 euros. So, the total costs per room add up to 200 euros for all the required hardware components.

### 5.3. Deployment Issues

PKI being the base of the system, the most crucial component is, of course, the certification authority that will issue certificates for the users. It is recommended that the organization have its own internal CA for issuing certificates. Also, special protection measures must be taken in order to secure the CA private key. An LDAP server is also required for storing the user related information and certificates.

The next component on the list is a database system that will be used to store both the user sessions from the SSCP platform as well as data from the Location, Biometric and SAAS services. The databases and their location must be scaled accordingly to the number of users of the system and the number of protected areas present within the building. Also, since the Biometric service deals with large amounts of image data (a set of 16 images with different lighting conditions is required for each user in order for the algorithm to work correctly), it is recommended that a separate database server be used for this service.

A further requirement is an Apache web server for hosting the FastCGIs for SSCP and the SAAS service. Also, for redundancy and load balancing purposes, a greater number of web servers may be configured. For each secured area, a router will be required. The router will have to have at a minimum two USB ports (one for the Bluetooth dongle and another for the magnetic lock controller) for each door it controls (of course, an USB multiplexer can be added to commercial routers that do not meet this requirement). The

router will host The Lock service described earlier and special changes must be made to its firmware in order to be able to host the service. Also, from a hardware point of view, the router must have at least 8 MB of flash memory in order to host the new firmware and the additional modules required for the Lock service.

#### 5.4. Performance and reliability tests

The most crucial components of the system are the Authentication and Session Check CGI because, in the absence of these two components, any other service that requires user identification would fail. As such, these services must be evaluated for their response time as well as reliability.

Reliability was tested by simulating high request loads, 20 requests/second, on the SSCP Authentication and Session Check CGI as well as the SAAS Key CGI for more than an hour. As expected, the fastCGI module spawned accordingly the necessary number of instances and no failure was detected for those instances during the test.

A detailed breakdown of the medium time spent on an authentication request is presented in Figure 6. As can be deduced from the graph, the main time consumer is the LDAP check and information retrieval because of the multiple attributes stored by the LDAP directory schema for a single user. SSL context establishment was measured using the Apache log timestamps because the web server is in charge of this operation. For this test, the database, along with the OCSP responder and LDAP directory, was installed on a different physical machine from the Authentication CGI.

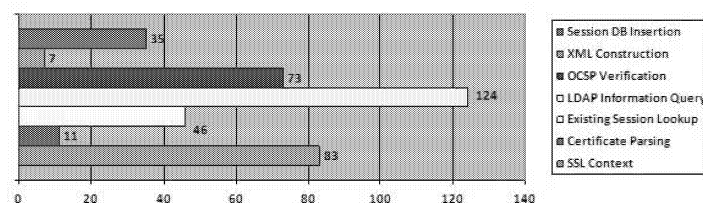


Figure 6: SSCP Authentication Request processing time breakdown

#### 6. FUTURE WORK

The proposed system has been designed in order to be able to easily integrate with as many existing access control systems as possible and also provide easy extension. One of the main directions we could follow to expand it is to integrate with RFID cards.

Any discussion of RFID on mobile phones is incomplete without also discussing Near Field Communications (NFC), which is an interface and protocol built on top of RFID and is targeted in particular at consumer electronic devices, providing them with a secure means of communicating without having to exert considerable effort in configuring the network. Future work includes customizing the NFP in order to integrate with our present solution, which would be much better suited, from a security point of view, than what is currently used, namely Bluetooth.

This is an ideal scenario for mobile phones as it would allow them to interact with other devices such as laptops while minimizing battery consumption.

In addition to this, new resources, besides sensitive areas, can be protected by our solution. An example of such a resource is a workstation. An authentication system can be developed and integrated with an already existing operating system. As such, when the user is in front of a computer from within the organization's network, he can use his smartphone in order to get credentials to log into the system, or, if a Bluetooth adapter is present on the workstation, log in automatically when the phone is in range.

#### 7. CONCLUSIONS

As smartphones become more and more popular due to the advances in technology, so do the needs for more portable and diverse applications increase. These powerful devices can now easily handle computational-intensive tasks such as image recognition, while letting you check your calls and your mail at the same time.

In this paper we have presented a generic platform to control the opening of a magnetic lock using identification through Public Key Infrastructures. One of the main advantages of this device is that, despite its low cost, it is generic and can also be integrated with other existing services. In addition to this, our approach integrates security measures including identification and localization of the users. Based on this platform we have presented our implementation, as well as several possible test scenarios.

#### ACKNOWLEDGEMENT

The research regarding the context-aware integrated mobile services is supported by national project: "TRANSYS - Models and Techniques for Traffic Optimizing in Urban Environments", Contract No. 4/28.07.2010, Project CNCIS-PN-II-RU-PD ID: 238. The work has been co-funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Romanian Ministry of Labour, Family and Social Protection through the Financial Agreement POSDRU/89/1.5/S/62557. All authors have equal contributions to the article.

CAPIM's official site and source code repository are available at <http://cipism.hpc.pub.ro/capim>.

#### REFERENCES

- S. Y. C. Hsu and W. Wu. 2009. "Constructing intelligent home-security system design with combining phone-net and bluetooth mechanism." In *Machine Learning and Cybernetics, International Conference*, volume 6(1), 3316–3323.
- E. Carayannis and E. Turner. 2006 "Innovation diffusion and technology acceptance: The case of PKI technology", volume 26(7). *Technovation*.
- D. Comaneci and B. Vlad. 2011. Face biometric distributed authentication service. Technical report, Faculty of Automatic Control and Computers, Computer Science Department, University Politehnica of Bucharest, 2011. Numeric Systems Architecture Course Project Description.

- C. Dobre, F. Manea, and V. Cristea. 2011. "CAPIM: A context-aware platform using integrated mobile services." In *Intelligent Computer Communication and Processing (ICCP)*, 2011 IEEE International Conference, 533–540.
- D. Greceanu. 2011. "Platform and services for context information aggregation and visualization." Technical report, University POLITEHNICA of Bucharest, Romania.
- I. Hwang and J. Baek. 2007. "Wireless access monitoring and Control System based on Digital Door Lock", volume 53(4). *Consumer Electronics, IEEE Transactions*.
- Y. Y. J. Zhang and M. Lades. 1997. "Face recognition: eigenface, elastic matching, and neural nets." In *Proceedings of the IEEE*, volume 85(9), 1423–1435.
- N. R. P. K. L. Iftode, C. Borcea and P. Zhou. 2004. "Smart phone: An embedded system for universal interactions." In *Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS 2004)*.
- I. Militaru. 2011. "Indoor localization service". Technical report, University POLITEHNICA of Bucharest, Romania
- N. D. N. Ravi, P. Stern and L. Iftode. 2005. "Accessing ubiquitous services using smart phones." In *Proceedings of the 3rd International Conference on Pervasive Computing and Communications*.
- P. S. Y. Park and J. Pyun. 2009. "Smart digital door lock for the home automation." In *TENCON 2009 - 2009 IEEE Region 10 Conference*, volume 1(1), 1–6.

## BIOGRAPHY

**DRAGOS COMANECI** finished his Bachelor studies within the University POLITEHNICA of Bucharest. His research interests include distributed mobile applications and security models and techniques. Currently he pursues his Master studies within the Distributed Systems track, with the University POLITEHNICA of Bucharest.

**SILVIA STEGARU** finished her Bachelor studies within the University POLITEHNICA of Bucharest. Her research interests include distributed mobile applications. Currently she pursues her Master studies with the University POLITEHNICA of Bucharest.

**CIPRIAN DOBRE**<sup>1</sup> PhD, is lecturer with the Computer Science and Engineering Department of the University POLITEHNICA of Bucharest. The main fields of expertise are Grid Computing, Monitoring and Control of Distributed Systems, Modeling and Simulation, Advanced Networking Architectures, Parallel and Distributed Algorithms. His research activities were awarded with the Innovations in Networking Award for Experimental Applications in 2008 by the Corporation for Education Network Initiatives (CENIC).

---

<sup>1</sup> Corresponding author

# Application of Vehicle Ad-hoc Networks in Traffic Control Systems

Benny M Nyambo<sup>1</sup>  
Goodbye Mavata<sup>2</sup>  
Gerrit K. Janssens<sup>3</sup>

<sup>1</sup>Computer Science Department, University of Zimbabwe, Harare, Zimbabwe  
Email: [nyambo@science.uz.ac.zw](mailto:nyambo@science.uz.ac.zw)

<sup>2</sup> Faculty of ICT Zimbabwe Open University, Harare, Zimbabwe  
Email: [gdmavata@gmail.com](mailto:gdmavata@gmail.com)

<sup>3</sup> Transportation Research Institute (IMOB), Hasselt University, Diepenbeek, Belgium  
Email: [gerrit.janssens@uhasselt.be](mailto:gerrit.janssens@uhasselt.be)

## KEYWORDS

Mobile ad hoc networks (MANET), Vehicular ad hoc networks (VANET), Intelligent Transportation Systems (ITS).

## ABSTRACT

Mobile ad hoc networks find use in a variety of areas which include rescue missions, battlefields and recently in inter-vehicular networks, generally known as Vehicular Ad Hoc Networks (VANETs). A lot of research has been done on the use of VANETs in traffic safety in road networks. This paper proposes a model for use of VANETs in an advanced traffic signal control system within a simulation environment. The idea is to use vehicular ad-hoc networking to reduce the average delay per person at road intersections, with the intent to reduce the average travelling time per person. The control system is designed with a generic and flexible logic that allows it to simulate a wide range of traffic signal control types and strategies. The strategies include mechanisms for deadlock and starvation avoidance at intersections. The control system is also designed as a distributed control system in which vehicles participate in a leader election process. This is a bid or a contest to gain or win the right of way for the vehicles for which the leader is in the same road segment which gets the green light. Specialized features of advanced control strategies are implemented within the control system framework which allows the implementation of transit signal priority and other specialized vehicles that might require prioritization within the simulation environment, allowing the simulation of both passive and active signal priority strategies. The capabilities of the control system are illustrated through a case study in which a simulation is done for a four way intersection and the results of the simulation studied with respect to the objectives of the prioritization strategies. An evaluation of the currently implemented system is performed.

## INTRODUCTION

A mobile ad hoc network (MANET) is a multi-hop wireless network temporarily and dynamically formed by a collection of mobile nodes without the use of any pre-existing network infrastructure or centralized administration. Applications such as disaster recovery, distributed collaborative computing and automated battlefields are typical examples of where ad hoc networks are deployed. Owing to its self-organization, rapid deployment and absence of any fixed infrastructure, ad hoc networks are gaining popularity as a significant and promising research domain.

The effects of node movement signal interference and power outages, however, make the available link state and network topology information inherently imprecise. On the other hand, heavy traffic, frequent link failure and network partition will incur transmission disruptions, causing data packets to be delayed and dropped. Dynamically changing topology and lack of network resource make the design of an adaptively distributed routing protocol challenging.

A Vehicular Ad-Hoc Network, or VANET, is a form of Mobile ad-hoc network (Nzouonta et al., 2008) formed on the fly between groups of cars connected by wireless links. It allows communication among vehicles in the close proximity and between vehicles and nearby fixed equipment, usually described as roadside equipment.

The main goal of VANETs is providing safety and comfort for passengers and other road users. To this end a special electronic device is placed inside each vehicle which will provide mobile ad-hoc network connectivity for the passengers. This network tends to operate without any infra-structure or legacy client and server communication. Each vehicle equipped with a VANET device is a node in the Ad-Hoc network and can receive and relay others messages through the wireless network. Collision warning, road sign alarms and in-place traffic view gives the driver



essential tools to decide the best path along the way. VANETs can also offer multimedia and Internet connectivity facilities for passengers, all provided within the wireless coverage of each car. Automatic payment for parking lots and toll collection are other examples of possibilities inside VANET.

Most concerns of interest to MANETs are of interest in VANETs, but the details are different. However, due to mobility constraints, driver behaviour, and high mobility, Inter-Vehicle Communication (IVC) networks exhibit characteristics that are significantly different from many generic MANETs [Blum et al., 2004]. Rather than moving at random, vehicles tend to move in an organized fashion. The interactions with roadside equipment can likewise be characterized fairly accurately. Finally, most vehicles are restricted in their range of motion, for example by being constrained to follow a paved highway. In VANET, nodes can work properly only if the participating vehicles cooperate with each other during communications. However, as a distributed network, individual vehicles might be non-cooperative for their own benefits (Zhou and Chunxiao, 2007).

Vehicular Networks are part of Intelligent Transportation Systems (ITS). Intelligent Transport Systems address the problems of road safety and congestion. Improving safety has long been a primary objective of many governments transport policies. Reducing congestion addresses many of these other objectives, such as the promotion of economic competitiveness. Congestion reduction also leads to environmental benefits such as improved air quality and reduced carbon dioxide emissions (UK Parliament, 2009).

Vehicles communicate with each other via Inter-Vehicle Communication (IVC) as well as with roadside base stations via Roadside-to-Vehicle Communication (RVC). The ultimate goal is that vehicular networks will contribute to safer and more efficient roads in the future by providing timely information to drivers and concerned authorities.

Other efforts include the construction of roundabouts, which in general have a favourable effect on traffic safety, at least for crashes causing injuries. The number of severe crashes appears to decrease after converting intersections into roundabouts (Daniels and Wets, 2005). However the cost of constructing a roundabout is quite high and the process also disrupt the smooth flow of traffic for some time. This can easily be avoided by implementing VANETs which can self-regulate at junctions with speed and efficiency.

Due to the human as well as financial suffering caused by road crashes, road safety is a relevant theme to study. The World Health Organization estimates that worldwide each year 1.3 million people are killed and between 20 and 50 million are injured in road crashes (Wilmots et al., 2009). This makes the issue on road safety important and its researchers' responsibility to help find solutions to this problem and to save lives.

In a large European state, a county road commission collects traffic data at major intersections, and then transmits the data via wireless broadband networks to enable real-time remote traffic signal control. In a major European capital, built-in roadway sensors detect traffic tie-ups due to accidents or weather, then immediately transmit the information to the centralized traffic

control centre via a high-speed wireless communications network. Sensors mounted on highway-bridge infrastructures communicate with Department of Transportation control facilities to identify conditions that could lead to structural failure. Through applications such as these and many others, Intelligent Transportation Systems are beginning to revolutionize traffic management and control all around the world (Motorola, 2008).

## RELATED WORK

Vehicular Traffic control at road crossings has always been a matter of concern for administrations. Several attempts have been made to design efficient automated systems to solve this problem. The primary tool of urban traffic control is signal control, which is applied in an urban network to facilitate the safety and efficiency of road transport in the network. Most present day systems use pre-determined timing circuits to operate traffic signals. Network control systems vary in their context from one urban area to another, and may include incident management, traffic signal management as well as motorway control functions [4]. However these systems are inefficient because they do not operate according to the current volume of traffic at the crossing.

Chattaraj et al. (2008) propose the idea of "Intelligent Traffic Control Systems using RFID". Their idea was to place two RFID readers (separated by some distance) in each direction of a road crossing and have a Central Computer System (CCS) to control them all. As a vehicle passes by a reader, it tracks the vehicle and retrieves its Electronic Product Code (EPC) data. The volume of traffic is not calculated simply by the number of vehicles but by a complex set of equations which take into account pre-defined factors (obtained by research) like:

- a) Type of vehicle (small vehicle like a scooter or a car, or a large vehicle like a bus or a truck)
- b) Priority assigned to the vehicle (each type of vehicle is assigned a specific priority based on its size, frequency of that vehicle at the crossing, time of the day, etc.)
- c) Priority assigned to the path of travel (essential when both the roads intersecting at the crossing are not of the same importance. e.g. national highway with an ordinary road)
- d) Time (time of the day, and day of the week).

So, the volume of traffic takes into account the priority assigned to each vehicle at the present time of the day and also the priority assigned to the two roads intersecting at the crossing. Once a vehicle has passed the crossing (i.e. it has gone out of the range of the readers), its data is moved from the dynamic database to the permanent database where it is stored along with its direction of travel (both arrival and departure directions) and time. Traffic signals are operated according to the current volume of traffic. This method is complex and can become expensive to implement if the road network has many intersections.

Sheng et al. (2006) design and build an experimental platform to conduct research on cooperative driving in intelligent transport systems. They develop a miniature vehicle that could operate as an automated vehicle. The platform allows experiments in single vehicle lane tracking and multiple vehicle collision avoidance. In



this system vehicles broadcast their intended paths, location and velocity.

In this paper a system is proposed which is based on vehicular ad hoc networks and does not require fixed infrastructure at each intersection. In addition, the system can also operate without traffic lights at the intersection. This system is expected to help with the hidden car problem or the blind spot problem since cars notify each other about their presence. The details of the proposed system are presented in Section 3.

## THE PROPOSED METHOD

We propose an algorithm to negotiate an intersection in the event of failure of traffic lights or when there are no traffic lights at all. This assumes that vehicles have the computational power to perform lightweight arithmetic operations such as aggregating values and simple integer comparisons. The strategy is distributed in nature with each individual vehicle at the leading node performing calculations in a leader election process. Embedded systems are incorporated into vehicles giving them the computational power they need to perform calculations. Thus even in the event that traffic lights fail or, alternatively if an intersection is uncontrolled, vehicles approaching this intersection have the capacity to handle or negotiate the intersection with efficiency that can supersede that of pre-timed logic control strategies.

Consequently, traffic lights and related infrastructure can actually be considered to be redundant. Moreover, the system that we propose has the advantage of being portable and may potentially result in future roads with no traffic lights; assuming that all future road vehicles have wireless communication devices. It may also be possible to eliminate all roadside infrastructures as future vehicles may have enough processing power housed on board.

In this work, we work on the assumption of a completely infrastructure-less system that minimizes waiting time at a road intersection, and controlling traffic lights to provide absolute priority for emergency vehicles, and relative priority for all other vehicles, based on sitting capacity. The idea is to use vehicular ad-hoc networking to reduce the average delay per person at road intersections, with the intent to reduce the average travelling time per person.

### 3.1 Algorithm

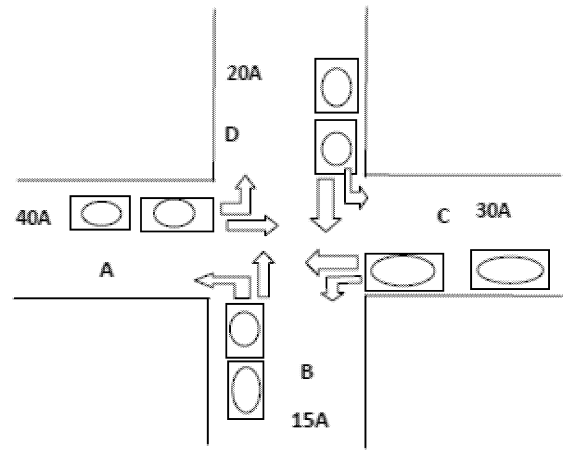
We propose a variation of a leader election algorithm. When vehicles approach an intersection they communicate their weighted values. Vehicles in the same node aggregate their weights together to contest in leader election process and the heavily weighted node wins.

For a node  $j$ , if  $x_i$  is the weight of the  $i^{th}$  vehicle then we can express the  $X_j$ , the aggregate weight of each node, as

$$X_j = \sum_{i=1}^n x_i = x_1 + x_2 + \dots + x_n \quad (1)$$

where  $n$  is the total number of vehicles in a node.

However starvation avoidance is considered to avoid bias and lope-sidedness by allowing little green time to the losing node. When a wing wins the leader election process, then it gets the green to move for a specific period, say 20 seconds. To avoid starvation of wings with less weight, the losing wings are given a green time smaller than the winner, say 15 seconds. This number can be varied depending on the number of vehicles in the losing node. If the number is too small, then the value can be made very small too, to reduce wasted time when no traffic is moving.



**Figure 1** Vehicles approaching an intersection from four different wings showing different weights depending on the amount and type of traffic in the wing.

To implement this algorithm we propose a means of allocating weights to vehicles. The vehicles are weighted according to carriage capacity. Thus a four-sitter carries a weight of 4 and an eighteen sitter bus will have 18 for a weight. The weighting of an ambulance or a presidential motorcade is more a ‘political’ issue than it is scientific, thus it remains in the better judgement of the authorities than it is a persuasion of a thoughtful calculation. In this research a large weight is used to symbolize an approaching special vehicle or person. A general approach to look at a vehicle or vehicles approaching an intersection as simple addition and subtraction of weights (in the case of vehicles leaving an intersection) is taken without consequences or deviation from the goal of the strategy. If, for example, a fire truck is weighted at 50, then 10 cars each with a carriage capacity of 5 resulting in an aggregated weight of 50 are considered equivalent. We may choose to say that if an ambulance approaches with a patient fighting for his last breathe then he gets absolute priority. This simply means giving it a weight extremely large that no other road segment can aggregate its node weight to surpass it. Thus without loss of generality, all vehicles are treated as node elements with a value they contribute to the total node weight of the segment to which they are part of.

The pseudo code of the algorithm can be written as:

- Aggregate weights in each node
- Compare weights between nodes
- Choose winning node and allocate it the green light  
winning node gets green light for  $N_1$  seconds  
losing nodes gets red light for same time
- After  $N_1$  seconds losing node gets green light for  $N_2$  seconds and the winning node gets the light red for the same time
- Run election again.

## THE SIMULATION SCENARIO

Here we present a simulation scenario of the system. Table 1 shows the weights in each of the four wings of the road. Wings which opposite each other are basically the same road and their weights are added. So in this case weights for wings A and C are added and so those of wings B and D. So in this case at 0 seconds wings B and D have weight total of 57 as compared to 47 for wings A and C. So wings B and D get the green light for 20 seconds and followed by a red light for 15 seconds. After 35 the leader election is computed again and wings B and D wins again and gets the green light for 20 seconds and a red for 15 seconds. However the third time wings A and C win the election and get the green light for 20 seconds followed by a red light for 15 seconds. This process repeats itself forever at every junction of the road network.

**Table 1:** A simulation scenario for a total of 105 seconds

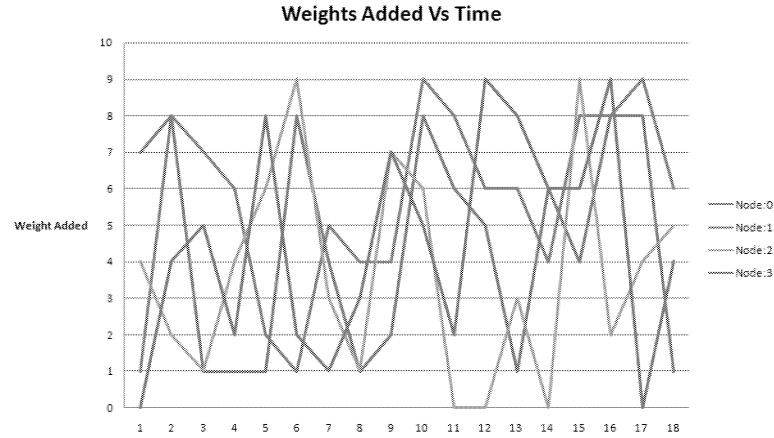
Time /seconds	Wing A	Wing B	Wing C	Wing D	Green
0	22	33	25	24	Wings B/D
35	30	27	30	36	Wings B/D
70	24	14	24	26	Wings A/C
105	36	25	27	31	Wings A/C

## THE SIMULATION RESULTS

In this section we present the results, and findings of the research experiments. The statistics that are used are drawn from the simulation results. Figure 2 show a sampled data set demonstrating the random nature in which nodes are added to an intersection. This simulates the random nature of arrival times at intersections. It eliminates any bias in the execution of the program. Different sets of data can be generated from different program executions but the output data is able to demonstrate the variation in the node weight that is added to a particular node.

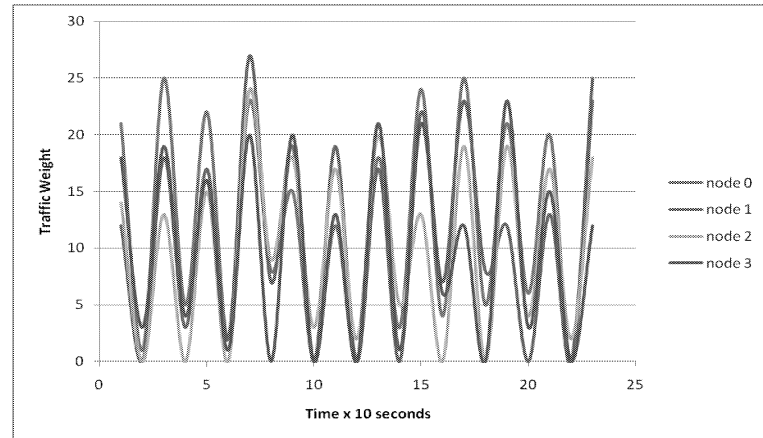
The weight of the nodes increases when more traffic is added to each node and the weight decreases when traffic leaves the junction (see figure 3). After the simulation was run for a fixed time period, a closer look at the average node weight for the

nodes show that the weights of the nodes tend to converge towards a mean value.



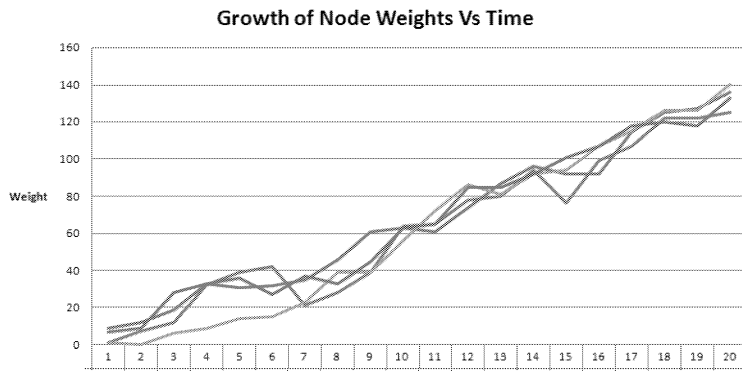
**Figure 2:** Weights added vs. Time

The results of the simulation show that as the simulation runs there is a general tendency of the algorithm to balance or consider fairly the weights of the nodes from all sides.



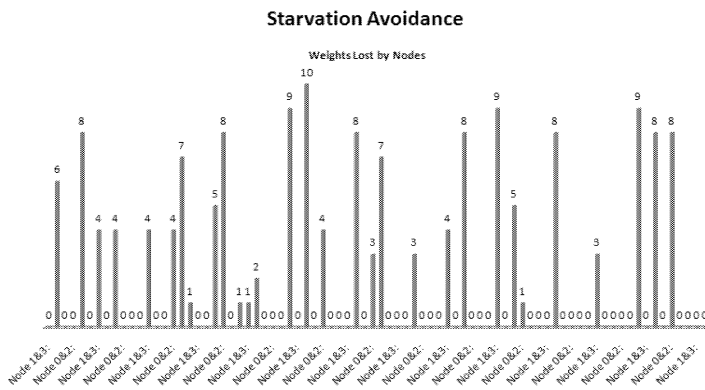
**Figure 3:** Node Weight growth vs. time

We realise that there should be a good compromise between the arrival rate and the departure rate at the junction. If the arrival rate becomes larger than the departure rate then the amount of traffic will almost linearly increase on all nodes (see figure 4). This will unfortunately defeat the sole aim of reducing the delay time per person. The departure rate should be made as big as possible and can also be augmented by other means as using dual carriages to increase the rate of flow of traffic.



**Figure 4:** Node Weight growth vs. time, when arrival rate is greater than departure rate

Figure 5 below reiterates the same thing this time giving a pictorial view as a bar graph of all the nodes and how starvation was avoided by a fair amount of traffic lost from each node.



**Figure 5:** Starvation avoidance graph.

We finally explain in Table 2, that despite the fact the nodes did not get equal number of green times, the algorithm was able to maintain a balance junction in terms of node weights. It simply means being denied a right of way is not negligence or favouritism but an ingenious way of handling an adaptive transit priority strategy. A snapshot of the output of the requests.csv output file is analyzed and given below.

Node	Share
0	29%
1	37%
2	16%
3	18%

**Table 2:** Shares of the nodes showing the green times

As can be seen from the pie chart Node 1 enjoyed the lion's share of the green time with 37% or the requests being granted as compared to Node 2 and 3 put together with 34%.

## CONCLUSIONS

This research outlines the presentation analysis and findings of using VANETs in self regulation at a four- way junction.

We have proposed an algorithm that can be used to negotiate traffic at an uncontrolled intersection. The algorithm works very well under normal conditions as well in heavy traffic. It also avoids starvation under heavy traffic when there is heavy traffic in one node and virtually no traffic in the other. However, there is need to reduce waiting time when the node, which is almost empty, clears. There is no need to wait for the stipulated time but to start travelling immediately in the heavy node.

We assume that if the algorithm works for a four way junction, then it should work for a three way junction. The system was able to resolve the problem of starvation by allowing time to all nodes to move traffic depending on their weights.

The algorithm we have just described works for a single junction. This will work perfectly in rural and remote areas where there are few roads. In a town there are many junctions and the behaviour of one junction will definitely affect the next one. There is a need for the algorithm to be expanded to include many junctions. We expect that since there will be close relationship between junctions, we will have to use the amount of traffic in a road and not at a single junction, to avoid traffic jams.

The proposed traffic regulation scheme fairs much better than the existing traffic light schemes currently used in most countries. The existing traffic light scheme does not take into account the amount of traffic in the respective wings of the junction. In this way there is always traffic congestion during pick hours caused by unbalanced junctions. In some countries they have road infrastructure that counts the number of cars that are approaching a junction and the traffic lights behaviour is governed by the traffic pattern. This also have a disadvantage of initial costs of setting up infrastructure. The reliability of this system will also depend on the working condition of the infrastructure. Our proposed scheme will not be affected by infrastructure breakdown so is expected to work all the time.

The concept and algorithm of traffic self regulation can also be applied in factories which use vehicles to transport materials from one section of the factory to the other. If the tracks of these vehicles cross, self regulation can bring efficiency in moving materials. The issue of priorities will be applied according to the operations of the factory. Many other ideas may arise from the concept of self regulation and it will bring efficiency and reduce costs in infrastructure setup.

## REFERENCES

- Blum J.J., A. Eskandarian, and L.J. Hoffman, Challenges of Intervehicle *Ad Hoc* Networks, IEEE Transactions on Intelligent Transportation, Vol. 5, no. 4, 2004.
- Chattaraj A., S. Chakrabarti, S. Bansal, S. Halder and A. Chandra .Intelligent Traffic Control System using RFID National Conference on Device, Intelligent System and Communication & Networking (AEC-DISC 2008) , 1-2 August, 2008.
- Daniels S., G. Wets, (2005). Traffic Safety Effects of Roundabouts: a review with emphasis on Bicyclist's Safety.

Proceedings of the 18th ICTCT-workshop. Helsinki, Finland, [www.ictct.org](http://www.ictct.org).

ETSC (European Transport Safety Council), Intelligent Transportation Systems and Road Safety (ISBN 90-76024-05-7), 1999 (<http://www.etsc.eu/oldsite/systems.pdf>)

Motorola Inc. Designing Intelligent Transportation Systems and Communications, White paper\_Motorola, Inc. 2008 ([http://wirelessnetworks-asia.motorola.com/markets/images/transportation/downloads/WiB/B/White\\_Paper/ITS\\_and\\_Comms.pdf](http://wirelessnetworks-asia.motorola.com/markets/images/transportation/downloads/WiB/B/White_Paper/ITS_and_Comms.pdf))

Nzouonta J., N. Rajgure, G. Wang, and C. Borcea . VANET Routing on City Roads using Real-Time Vehicular Traffic Information, IEEE Transactions on Vehicular Technology, vol. 58 no. 7, 2008

Sheng W., G.Y. Guo, Cooperative driving based on Inter-vehicle communications: Experimental Platform and algorithm. Proceedings, International conference on intelligent robots and systems, Beijing October, 2006.

UK Parliament, Intelligent Transport Systems, ([www.parliament.uk/parliamentary\\_offices/post/pubs2009.cfm](http://www.parliament.uk/parliamentary_offices/post/pubs2009.cfm)), Number 322, 2009.

Wilmots B., E. Hermans, T. Brijs, G. Wets. Analysing road safety indicator data across Europe: Describing, explaining and comparing. 4<sup>th</sup> IRTAD conference, Seoul, Korea, September 2009  
Yan L., M. Kihl, Y. Liu, L. He. The application of Inter-Vehicle Communication System to ITS, Geographical Information Science Research Conference (GISRUK 2007). NUI Galway, Ireland. April 2007.

Zhou W., C. Chunxiao, Cooperation Enhancement for Message Transmission in VANETs, Wireless Personal Communications, 43:141–156, 2007.

## BIOGRAPHY

**BENNY M. NYAMBO** obtained the Bachelor of Science Honours degree in Physics in 1999 and MSc in Applied Physics in 2002, both from the University of Zimbabwe, Harare, Zimbabwe. He is currently studying towards a PhD in Computer Science at the Hasselt University, Belgium. He has been a lecturer in Computer Science and the University of Zimbabwe since 2003. He has research interests in performance modelling of communication networks and in embedded systems.

**GERRIT K. JANSSENS** received degrees of M.Sc. in Engineering with Economy from the University of Antwerp (RUCA), Belgium, M.Sc. in Computer Science from the University of Ghent (RUG), Belgium, and Ph.D. from the Free University of Brussels (VUB), Belgium. After some years of work at General Motors Continental, Antwerp, he joined the University of Antwerp until the year 2000. Currently he is Professor of Operations Management and Logistics at Hasselt University (UHasselt) within the Faculty of Business Administration. His main research interests include the development and application of operations research models in production and distribution logistics.

# **SECURE TELECOM SYSTEMS**



# TOWARDS A SECURE DATA SHARING PEER-TO-PEER NETWORK BASED ON GEOMETRIC AND SEMANTIC DISTANCES

Ana-Delia Sâmbotin, Mugurel Ionuț Andreica  
Department of Computer Science  
Politehnica University of Bucharest  
Splaiul Independenței 313, sector 6, 060042, Bucharest  
Romania

E-mail: delia.sambotin@gmail.com, mugurel.andreica@cs.pub.ro

## KEYWORDS

P2P, virtual geometric coordinates, semantic distance, security, multicast, data sharing.

## ABSTRACT

In this paper we propose a new strategy that can be applied for creating a secure peer-to-peer topology in which the identity of the source node cannot be revealed. The main goal is to obtain a decentralized network distributed in space, where the users are allowed to share and exchange their music files. The proposed model uses different metrics for estimating the distance between nodes (like the round trip time and the semantic distance) and uses the smallest values in order to select a node's neighbors. For the identity protection, the system imposes the encryption of the traffic and that the communication is mediated by a node from the network, randomly chosen by each instance.

## INTRODUCTION

Peer-to-peer is a very popular technology which connects thousands of clients in a decentralized environment. They are used in a large number of situations, from the simple need to transfer a file, to more complex interactions like social networks or resource sharing. P2P is a popular technology especially used for file sharing because it allows the client applications to upload and download files over the network, without the need for some special server devices. This means that the peers from the network are both suppliers and consumers of resources, in contrast to the traditional client-server model where the suppliers are only the servers, and the clients are the consumers. There are also some disadvantages in peer-to-peer architectures. An important drawback is that P2P networks are typically less secure than a client-server network because security is handled by the individual computers, not by the network as a whole. The resources of the computers in the network can become overburdened as they have to support not only the workstation user, but also the requests from network users.

The main concepts behind the peer-to-peer networks are: sharing resources, decentralization and self organization. There are several types of peer to peer networks, based on the centralization degree of the overlay. In a fully decentralized network there is no intermediary device which keeps track of the peers position and activity. This type of network is very scalable because the failure of a peer does

not affect the entire network. The hybrid architecture consists of a central server which keeps the information about the users from the network as metadata. This kind of architecture can be classified in centralized indexing (the peers maintain active connections with the server) and decentralized (the server maintains connections with a set of peers, named supernodes). In this case we denote the server to be the component delegated with the role of supplying the basic information essential for a peer to connect the overlay. Due to the lack of a server device the peers must be able to organize themselves in order to obtain a stable network. There are different ways that the peers could connect with each other depending on which properties the topology wants to improve.

IP multicast provides a method of efficient many-to-many communication in contrast to the one-to-one model of IP unicast, in which data packets are sent from a single source to a single recipient. This concept is becoming increasingly important, both in the Internet and in private networks. The multicast technology enables the use of the following applications: video conferences, live broadcasting, web TV, web radio, video-on-demand, e-learning, whiteboard data exchange.

There are several ways to simulate a multicast network. The most intuitive and efficient one is to construct a network infrastructure, where the intermediary devices duplicate the received packets and send it to a group of users. This approach is not quite efficient due to the fact that the service providers must change the structure of the network and they must buy new equipments. These changes can be expensive and take a long period of time. Another way to simulate the multicast communication is to build an application layer multicast overlay; thus, the application is responsible with the multiplication of the received data and with forwarding it to other nodes. This solution is less expensive but it uses more of the client's resources.

In this paper we propose several methods in order to construct a secure data sharing peer-to-peer network with multicast capabilities. The work presented in this paper is a continuation of the one presented in (Sâmbotin and Andreica, 2011).

## RELATED WORK

In this section we present other approaches for some similar applications. We were interested in other similar approaches of building secure peer-to-peer networks and multicast

overlays.

### Peer-to-Peer Spatial Cloaking Algorithm

A location-based service (LBS) is an information service that needs to know the positioning of a user (mobile device) in order to provide some useful information, like where is the nearest bank. In (Chow et al., 2006) the authors propose a peer-to-peer spatial cloaking algorithm for mobile devices, which will help the users to protect their private information without seeking help from any centralized third party. A practical example could be when a mobile user looks after the nearest gas-station. For security reasons, the user will first find other peers to collaborate as a group and will cloak its exact location into a spatial region that covers the entire group. The next step assumes the random selection of one node within the group which will be delegated with the role of an agent. This means that the communication with the location-based database server will be mediated by the agent. Because the server processes the query based on the cloaked spatial region, it can only give a list of candidate answers that includes the actual answers and some false positives. After the agent receives the possible answers, it forwards it to the mobile user that requested it.

The described model can function in two modes: on-demand or proactive. The first one assumes that a mobile device will start this process when they need a information provided by the location-based service. In the second model, the users periodically search for different devices in order to form a group that will hide his location.

### CAN

In (Ratnasamy et al., 2001) the authors proposed a new strategy in which the network is composed of many individual nodes and in which the space is split between them. The CAN network resemble a hash table and the basic operations that can be performed in this model are: the insertion, lookup and deletion of (*key,value*) pairs. Each CAN node stores a chunk (called a zone) of the entire hash table. In addition, a node holds information about a small number of "adjacent" zones in the table. Requests (insert, lookup, or delete) for a particular key are routed by intermediate CAN nodes towards the CAN node whose zone contains that key. The CAN design is completely distributed (it requires no form of centralized control, coordination or configuration), scalable (nodes maintain only a small amount of control state that is independent of the number of nodes in the system), and fault-tolerant (nodes can route around failures).

The entire CAN space is divided amongst the nodes that coexist in the system. When a new node joins, the system must be allocated its own portion of the coordinate space. This is done by an existing node splitting its allocated zone in half, retaining half and handing the other half to the new node. A major problem that a peer encounters is finding the proper zone. In order to achieve its purpose the new node then randomly chooses a point *P* in the space and sends a *JOIN* request destined for point *P*. This message is sent through the network via any existing CAN node and by using the routing mechanism.

Under normal conditions each node sends periodic update messages to each one of its neighbors giving its zone

coordinates and a list of its neighbors and their zone coordinates. When a prolonged absence of an update message from a neighbor is noticed then it is interpreted as a failure. Once a node has decided that its neighbor has died it initiates the takeover mechanism and starts a takeover timer.

### Multicast Overlays over Peer-to-Peer Networks

As we can find in (Tan and Jarvis, 2007) there are different ways to build a multicast overlay depending on the properties that we want to improve. This paper describes and analyzes several ALM protocols which aim to construct a topology for multicast communication based on the most significant properties (application domain, group configuration, routing protocols). Also, the authors compare the IP multicast with the different ways of implementing a multicast network at the application layer, highlighting the advantages and disadvantages for each technology.

The concept of ALM (Application Layer Multicasting) concerns the implementation of multicasting functionality as an application service instead of a network service. This solution was considered due to the fact that one-to-many or many-to-many communication should use efficiently the network resources. A multicast network service implies that the local network must be equipped with routers that are capable of setting up and tearing down IP Multicast sessions as well as processing and routing IP Multicast packets. Therefore, instead of relying on the local internet providers to enable the multicast communication, we can assign the duty of creating a multicast overlay to the application layer. While IP Multicast is implemented by network equipment (routers) and avoids multiple copies of the same packet on the same link as well as possibly constructing optimal trees, ALM is implemented by the application and can lead to multiple copies of the same packet on the same link as well as typically building non-optimal trees.

ALM's disadvantages, such as longer delays and less efficient network usage compared to IP multicasting, are balanced by its advantages such as immediate deployability on the Internet, easier maintenance and update of the algorithm, and, last, but certainly not least, the ability to adapt to a specific application.

Some of the most popular ALM protocols that we will discuss are:

- ZIGZAG (Tran et al., 2004)
- NICE (Tran et al., 2004)
- OMNI (Banerjee et al., 2003)

ZIGZAG is a single source, degree-bounded application layer multicasting approach for media streaming. It arranges receivers into a hierarchy of clusters and builds a multicast tree on top of it. After applying the recursive rules of organizing the nodes into a multi-layer hierarchy of clusters, it will result that the nodes closer to the root will have large out-degrees and will run out of their bandwidth quickly. This effect might not be acceptable for bandwidth-intensive media streaming applications. This protocol provides a mechanism for maintaining a connected tree: when the parent node leaves the network without an announcement, the delegated node will help the children to reconnect immediately to the new parent. ZIGZAG periodically runs optimization algorithms to improve the quality of service.

NICE is an acronym which stands for the NICE Internet



Cooperative Environment. This scalable application layer multicast protocol uses a hierarchical clustering approach to support a larger number of receivers. NICE was designed to provide a topology for low bandwidth soft real-time data stream applications such as real-time stock quotes and updates and Internet radio. This approach detects inaccurate placement of hosts in clusters on different layers and gradually moves to a global optimal hierarchy. NICE allows nodes in a cluster to exchange periodic messages in order to maintain the appropriate peer relationships. In every cluster it will be a delegated node that will be responsible with maintaining the proper size of the structure and with identifying the departure of a peer in order to keep a connected tree.

OMNI stands for the Overlay Multicast Network Infrastructure and offers a multicast overlay for an efficient transfer of media streams. This method will generate a topology that consists of a set of devices called Multicast Service Nodes (MSN). These points are distributed in the network and provide efficient data distribution services to a set of peers. A client will be associated with a single MSN to receive multicast data service. The MSNs themselves run a distributed protocol to organize themselves into an overlay which forms the multicast data delivery backbone. The data delivery path from the MSN to its clients is independent of the data delivery path used in the overlay, and can be built using a network layer multicast or an application-layer multicast system.

### Traffic Analysis

Traffic analysis is the process of intercepting and examining messages in order to deduce information from patterns in communication. It can be performed even when the messages are encrypted and cannot be decrypted. Thus, for hiding the content of a message we can use encryption with public/private/symmetric keys, whereas traffic padding may be used to hide the traffic pattern.

In (Jiang et al., 2001) a strategy for improving the security in a wireless network is proposed. The authors developed a suitable cover mode with the objective of minimizing the energy consumption because usually, the peers from these types of networks are mobile devices with limited power supply. They also want to minimize the quantity of the dummy traffic because these information incurs an overhead. In order to prevent traffic analysis, the authors considered that it is important to hide not only the real traffic pattern, but also the changes in the real traffic pattern.

A cover mode is considered to be constructed so an intruder cannot determine the real operation mode of the network at any given time. The paper proposes several methods for building a cover mode, like: end-to-end and link. An end-to-end cover mode maintains a constant rate of traffic between each (source, destination) pair, independent of the actual operation mode while a link cover mode is obtained by achieving constant traffic rate on each link in the ad hoc network, independent of the actual operation mode. Unlike the end-to-end cover mode, link cover mode is implemented by inserting dummy packets on each link, so as to maintain a constant rate on that link.

The results that the authors obtained indicated that end-to-end cover mode generally performs worse than link cover mode, but in large networks, the two approaches yield similar

energy overheads.

### SYSTEM DESIGN

This section presents the application's purpose and its architecture. Furthermore we present a detailed description of each main component within the application and how these components are connected together. This section also presents each stage and the communication protocol used between the involved entities.

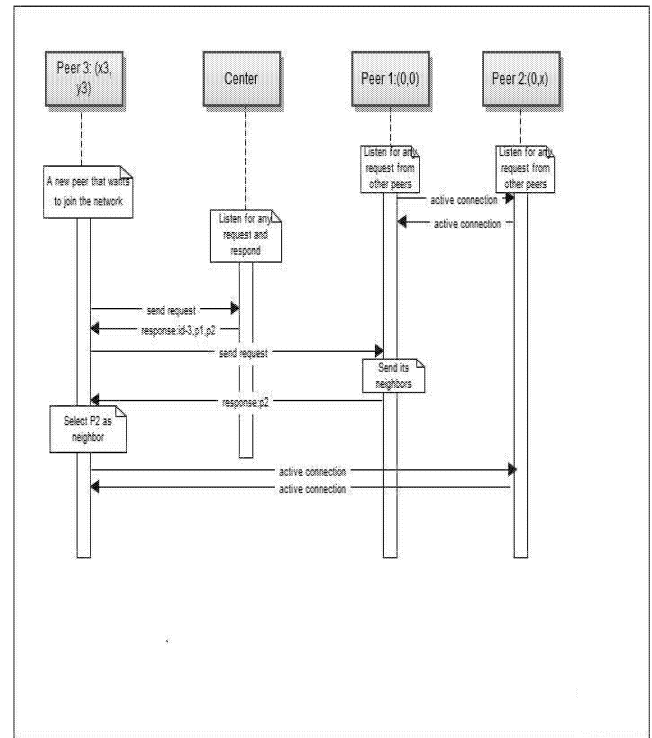


Figure 1: Multicast overlay construction steps.

### Application's Purpose

The main goal of our system is to create a new strategy for the constructions of a secure decentralized data sharing peer-to-peer overlay. This means that there isn't any entity which knows the entire network, but only fragments, and by fragments we understand the neighbors and the extended neighbors. Also, the system has the responsibility to protect the user's identity and to cover the traffic within the network. This model aims to enhance the security of the network where the identity of the source transfer cannot be identified. In order to achieve this, a new role of a mediator will be defined for a regular peer. Also, all the traffic within the system will be encrypted using symmetric keys.

This network must be completely decentralized in order to improve the stability issue (the failure of a node must affect a minimum number of peers). The final representation of the overlay should be as a tree structure, where the nodes have a reasonable number of neighbors; thus, the topology will not be considered to contain peers with the role of a server.

The application must allow a multicast communication over the peer-to-peer overlay. Thus, we want to construct an application layer multicast which will allow one-to-many communications. Each node should be able to send the same

message to any of its neighbors, regardless of the requesters, and to receive messages.

Another aim of this system is that its components should have a low level of dependency. Thus, the development of a new strategy should be easily integrated with the rest of the system.

### The Construction of the Overlay

In Fig. 1 we can identify the main stages a peer must go through in order to join the network.

Before starting the process of obtaining its coordinates, a peer must share a directory with music files, which is analyzed when the application starts. Thus, we are interested in extracting some additional information (like title, artist, album, genre) from these files and form a vector of tokens. Each token (an element from the vector) will have a weight value associated to it, which is computed based on metrics like term frequency and inverse document frequency. In other words, the weight assigned to a term using these metrics should be:

- highest when the term occurs many times within a small number of documents (thus lending high discriminating power to those documents);
- lower when the term occurs fewer times in a document, or occurs in many documents (thus offering a less pronounced relevance signal);
- lowest when the term occurs in virtually all documents.

The first step is to contact the bootstrap node in order to obtain the minimum amount of information needed for joining the network. It receives the data about the last three nodes that joined the system.

Furthermore the peer must contact each node in order to update the data associated with each peer. Mainly, we are interested in obtaining the coordinates of those nodes. Knowing the identity of its neighbors, the peer will ping each one of them and will compute the obtained RTT value. This value is combined with the semantic distance computed between the two nodes. The similarity (semantic distance) between two peers is computed using the cosine similarity that measures the cosine of the angle between the token vectors of the two peers. The result can take a value from 0 to 1, where 0 means that the two nodes have nothing in common, and 1 meaning that they have shared identically the files. We consider that the obtained value represents the distance between this two nodes (Skvortsov and Kostyuk, 2006).

$$\text{Sim}(A, B) = \cosine \theta = \frac{A \bullet B}{|A||B|} = \frac{x_1 \cdot x_2 + y_1 \cdot y_2}{(x_1^2 + y_1^2)^{1/2} (x_2^2 + y_2^2)^{1/2}}$$

Figure 2: Semantic distance formula.

Knowing some neighbors and the distance to them, the peer will try to compute its coordinates using the following assumptions and formulas. If the peer doesn't receive any data from the bootstrap node, this means that it can be considered to have the coordinates (0, 0). If the peer has only one neighbors with the coordinates  $(x_n, y_n)$  then it will choose the coordinates  $(x_n + dist, y_n)$ . If the node has 2 or more neighbors, then in order to obtain the coordinates of the point we will use the rules for computing distances proposed in (Sâmbotin et al., 2011).

### Security Module

In order to enhance the security we developed a different strategy adopted by the nodes from the system that will protect and disguise the identity of a node. The reason we need to do this is based on the issue of rights over the files that a user shares and it is undesirable that the application could provide a mechanism for tracing them.

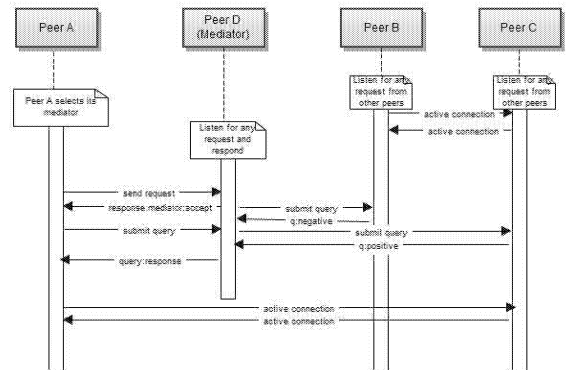


Figure 3: Transfer protocol

Fig. 3 presents the protocol used by the peers when they search for a file. First, we assume that each node shares some files in mp3 format and wants to search and find other songs. In order to retrieve the desired file, the user must submit a query through the network, and whenever a peer receives such a request and considers that it could respond affirmatively, it contacts the initiator. This approach is the most common one. Over this model we introduce the role of a mediator and some rules that will be described further.

Before submitting a query through the network, the peer randomly selects one of its neighbours that will be delegated with the communication between the initiator and the node that will respond affirmatively to the query. Thus, we can consider that the peer cloaks behind its neighbours and the diameter of the group that hides the initiator can increase.

The second step is to implement a mechanism that will protect the system from traffic analysis. For this, each node that sends a query will first establish a set of terms that will be inserted in the initial request. The tokens that are additionally inserted in the request are generated using a specific pattern. This means that they are formed from a randomly generated string that only contains symbolic characters that are appended at the beginning and at the ending of the file. Another used strategy will be that all nodes will periodically exchange messages (some will be dummy messages and others will have the purpose of maintaining the network and the connections between nodes), independent of the operation mode.

The message exchange assumes that all the traffic is encrypted using symmetric keys. When a mediator receives a list of tokens (some valid and others dummy), it will forward the request to its neighbours.

We must introduce some constraint for the role of a mediator peer. First, when a mediator is chosen by a node, it doesn't have the possibility to deny a request, but he must do everything it can in order to resolve a query. For security concerns, a node with this role will not try to resolve any of

the requests. The only action that it is allowed to do is to forward the received queries. The neighbours will try to resolve the query, and if neither of them will be able to respond affirmatively, then the mediator will become an initiator and will retain the node for which it has this role. This approach is used until a user gets a response or no one can provide the requested file. When a node will respond positively, the system will be able to transfer the data along the shortest path.

## Application Architecture

The system is made from the following main modules which interact with one another. Basically, each module represents a main functionality of the system. As we can see in Fig. 4, the main modules are:

- Network components
- Security module
- Listen thread
- Settle Neighbors thread
- GUI
- Input module
- Timeout thread

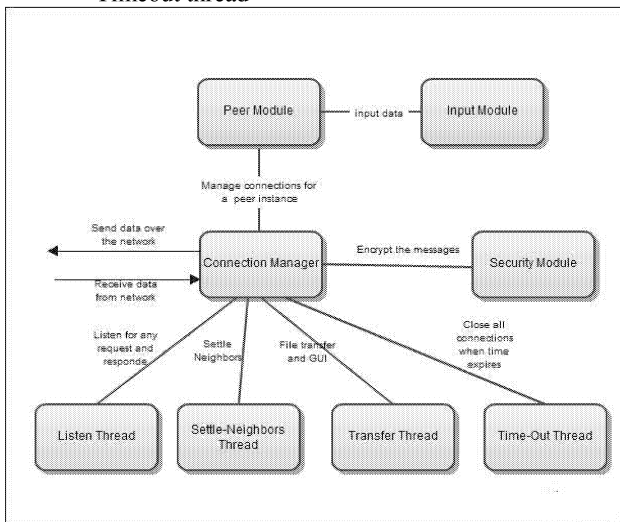


Figure 4: System architecture.

We have chosen this model because we wanted a loose coupling between the main parts. Thus, each component can be easily replaced with another component in the future.

## Module Description

The *network module* (connection manager in Fig. 4) is responsible for constructing the overlay that must provide the ability of finding the most appropriate peers for the file transfer. The final goal of the network module is to build a peer-to-peer overlay that can be represented as a tree structure and which will allow the multicast communication. This module is highly connected to the module responsible with the security within the system. That is because all the traffic is generated according to the strategy described in the previous section, i.e. encrypted using symmetric keys. One major aspect of the network is that it will be fully decentralized. This means that no peer will have a map with the entire overlay, but it will be aware only of the direct neighbors (with which it will keep an active connection) and

its extended neighbors (peers that are the neighbors' neighbors).

The network will be composed of a center node (or bootstrap node), which will not be a part of the network, but will have the responsibility to introduce other peers in the overlay by supplying information about other nodes, and at least one regular peer. In order to keep a consistent set of nodes, the central entity will be contacted before each valid departure of a peer from the network.

The input module is responsible for parsing and gathering the information from the configuration file which contains all the required data that a peer needs in order to start.

```
<config>
  <title>Global Parameters</title>
  <params>
    <ip>192.168.0.121</ip>
    <port>30001</port>
    <bandwidth>150</bandwidth>
    <ipBootstrap>192.168.0.6</ipBootstrap>
    <portBootstrap>30000</portBootstrap>
    <time>30</time>
  </params>
</config>
```

Figure 5: Sample configuration file.

As we can see in the figure above, a peer needs to know its ip, port, the address of the bootstrap node. The only parameter that must be changed is the ip parameter with the value.

The *Listen Thread module* is responsible with listening for any request from the network. These may come from another peer and have the following form: "action-info\_peer", where *info\_peer* is a representation of information regarding the requesting peer and *action* can be:

- *collect* – gather the updated coordinates of the neighbors
- *responseCollect* – the response of a peer with its coordinates
- *remove* – removes a neighbor from its list of neighbors
- *add* – add a new neighbor
- *extended* – ask for the neighbors
- *sendExtended* – send the list of neighbors

The *Graphical user interface (GUI)* is implemented as a different thread in order to organize the resources better. From the GUI window we can visualize some valuable information like which peers are the neighbors and the identity of the current peer.

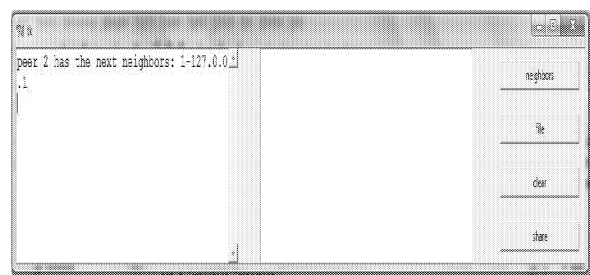


Figure 6: GUI.

The *Time out Thread* has the responsibility of stopping and exiting the program after a period defined by the user. The “time” tag from the xml configuration file is associated with this value.

The application is developed in Python and we only used one external module, Tkinter for the graphical interface. We have chosen Python because it is a powerful, pure object-oriented programming language with efficient data structures.

## EXPERIMENTAL EVALUATION

We simulated the construction of the network on one local machine for 50 to 300 peers. For the simulation phase we used a different module which uses the same formulas, strategy and metrics as the ones described in this paper.

In order to test our solution we first randomly generated the coordinates of a point and a number from 1 to 6 (the suffix of the shared folder). When a new peer joins and asks for the distance to its neighbours, it gets the geographical distance between one of these generated points and its neighbors. The value will be processed and combined with the similarity coefficient. We consider that we know the positioning of its neighbors.

We wanted to evaluate if the points will be distributed in the entire space or if they will gather in one area. In order to do so, we tested the system using different weights.

When the network considered only the geographical distances, the nodes were distributed through the entire space (see Fig. 7).

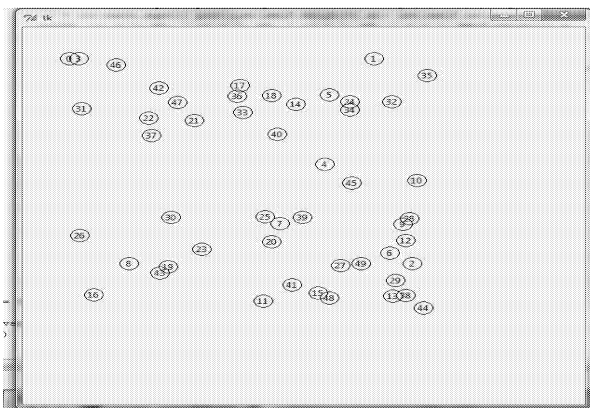


Figure 7: Points distribution (only geographical).

When we used only the semantic distance, the points gathered in one area, because the folders contained approximately the same files (see Fig. 8).



Figure 8: Points distribution (only semantic).

When we attributed an equal percent to each metric, the points formed a distributed group (see Fig. 9).

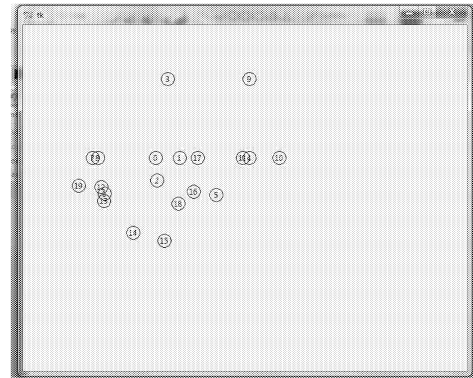


Figure 9: Points distribution (both metrics).

We also wanted to evaluate the security module in order to appreciate how the system will perform. Thus, we measured the time needed for the search operation with and without the mediator role.

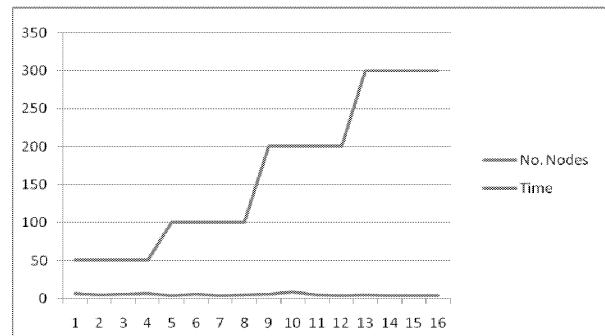


Figure 10: Results for the secure case: with mediator.

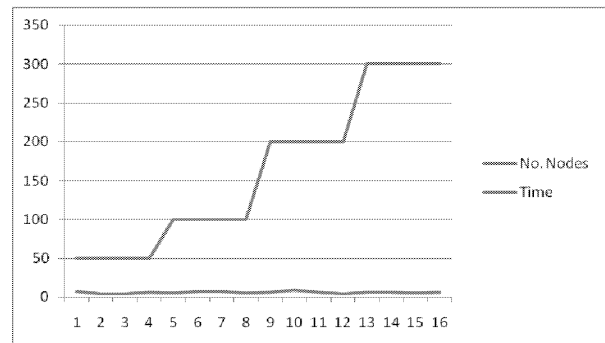


Figure 11: Results for the secure case: without mediator.

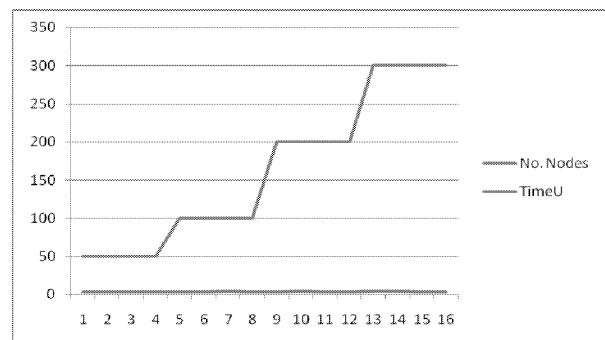


Figure 12: Results for the unsecure case.

As we can observe, the overhead is not induced by the new role of the mediator. We have been expected this because the neighbours are selected according to the smallest distance, which considers the similarity between two nodes. Thus, it is reasonable to affirm that in most cases, the searched file can be located in the proximity of a peer (one of the mediator's neighbors). The most expensive part is the generation of the keys and the exchanging of this entities among the nodes and the process of adding dummy data to the original request. The security module slows the response time of a node with approximately 35%.

We have also tested the main application. From these test cases we can declare that the communication through the network works properly.

## CONCLUSIONS AND FUTURE WORK

As we can observe from the previous section, we obtained a decentralized network which uses two distance metrics in the building phase: a geometric distance over virtual coordinates and a semantic distance. The neighbors of a peer are the closest nodes of that peer. The best scenario is to use both metrics: the structure of the network is more compact but not too congested.

The "cost paid" for a secure network when the content cannot be found is not very large and it is worth "paying". The process that takes longest is the key generation, but this will be performed only in the first phase.

As future work we want to test the application on several different machines. The security tests must consider the latency of the message exchange through the network. The result will be influenced by the quantity of the dummy data added to a request and by the additional number of messages that will be sent between a node and its mediator. Beside the network structure analysis, we are also interested to test the transfer speed of a file from a peer to another.

We also built the application in such a manner that we can easily add other metrics for the distance between two nodes. We want to consider the load of the network on a longer period of time when we compute the distance.

## ACKNOWLEDGEMENT

The work presented in this paper has been partially supported by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Romanian Ministry of Labour, Family and Social Protection through the Financial Agreement POSDRU/89/1.5/S/62557, and by CNCS-UEFISCDI under research grant PD\_240/2010 (contract no. 33/28.07.2010), PN II – RU program.

## REFERENCES

Banerjee, S.; C. Kommareddy; K. Kar; B. Bhattacharjee; and S. Khuller. 2003. "Construction of an Efficient Overlay Multicast Infrastructure for Real-time Applications". In *Proceedings of IEEE INFOCOM*, vol. 2, 1521-1531.

Chow C. Y.; M. F. Mokbel; and X. Liu. 2006. "A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location-based Service". In *Proceedings of the 14<sup>th</sup> Annual ACM International Symposium on Advances in Geographic Information Systems*, 171-178.

Jiang S.; N. H. Vaidya; and W. Zhao. 2001. "Power-Aware Traffic

Cover Mode to Prevent Traffic Analysis in Wireless Ad Hoc Networks". In *Proceedings of IEEE INFOCOM*.

Ratnasamy S.; P. Francis; M. Handley; R. Karp; and S. Shenker. 2001. "A Scalable Content-Addressable Network". In *Proceedings of the ACM SIGCOMM Conference*, 161-172.

Sâmbotin, A.-D.; M. I. Andreica; and E. Mocanu. 2011. "Strategies for Assigning Virtual Geometric Node Coordinates in Peer-to-Peer Overlays". In *Proceedings of the 6<sup>th</sup> International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC)*, 253-258.

Sâmbotin, A.-D.; and M. I. Andreica. 2011. "Towards a Peer-to-Peer Recommender System Based on Collaborative Filtering Techniques". In *Proceedings of the 18<sup>th</sup> International Conference on Control Systems and Computer Science (CSCS)*, vol. 2, 537-544.

Skvortsov, A. V.; and Y. L. Kostyuk. 2002. "Compression of Coordinates of Triangulation Nodes". In *Russian Physics Journal*, vol. 45 (5), 472-476.

Tan, G.; and S. A. Jarvis. 2007. "Improving the Fault Resilience of Overlay Multicast for Media Streaming". In *IEEE Transactions on Parallel and Distributed Systems*, vol. 18 (6), 721-734.

Tran, D. A.; K. A. Hua; and T. T. Do. 2004. "A Peer-to-Peer Architecture for Media Streaming". In *IEEE J. Sel. Areas Commun.*, vol. 22, no. 1, 121- 133.

# SECURITY COMMUNICATION LAYER FOR PUBLIC DISTRIBUTED REPORTING SERVICES

Decebal Popescu, Nirvana Popescu, Florin Pop\*, Vlad Ciobanu, Ciprian Dobre, Valentin Cristea

University POLITEHNICA of Bucharest, Faculty of Automatic Control and Computers, Department of Computer Science  
Spl. Independentei, 313, Bucharest 060042, Romania

E-mails: {decebal.popescu, nirvana.popescu, florin.pop, ciprian.dobre, valentin.cristea}@cs.pub.ro, vlad.ciobanu@cti.pub.ro

## KEYWORDS

Security, Distributed Electronic Services, Electronic Identity, Communication Protocol.

## ABSTRACT

The electronic management of user identities is a requirement for many modern applications. The user's identity defines its possible range of actions, and its management becomes critical in applications such as e-Banking, e-Payment, etc. Current solutions are based on methods that use certificate infrastructures, role and policy enforcement management, trust management using social networking, etc. We propose a solution for electronic management of identities that provides secure identification of a user using its electronic identity card (eID). The proposed nPA (the new German Identity card) Connector offers a trusted infrastructure for secure handling of electronic identities over the Internet. The nPA connector uses certificates obtained and guaranteed by a trusted Identity Provider. The user's personal data from the electronic Identity Card is transmitted from an original source service provider to subsequent destination service providers, all of which have previously signed a contract with the Identity Provider. The connector can be easily integrated within an application, providing a supplementary security layer for identity management. It can also be accessed remote as a Web service. In such cases the connector can be accessed by applications that can communicate with an Identity Provider from a trusted list of eID Service Providers. For that, the connector offers an interface for the application to query attributes from the electronic Identity card. The nPA connector can be considered a service provider between a user wielding a user agent (usually a web application accessed through a web browser) and an Identity Provider.

## INTRODUCTION

We live in an electronic world governed by necessity to move all citizen services in electronic distributed environments. In the context e-Services, the number of users that want to move from physical world into digital world grows exponential in last decade. The e-Services are easy to use, permanent and they have continuous access, direct communication, timely and consistent information. The e-Services are exposed to all kind of threads from the Internet,

so when it comes about their security or other challenges, it should receive a special attention. In a digital world, when it comes about e-Services, there are some main characteristics that are common to all of them. One of them is scalability, which indicates its ability to handle growing amounts of work in a graceful manner or its ability to be enlarged, so the distributed environments are required.

Security challenges are imposed at each step. Data encryption, password protection and account creation are other subjects discussed and applied during the development of the e-Service system. A large number of users characterize e-services and they must be able to respond to all their requests.

We propose a solution for electronic management of identities that provides secure identification of a user using its electronic identity card (eID). The proposed connector library represents a solution for the simple integration of the new German Identity card (nPA) into web applications by taking away the complexity of handling the communication with the Identity Server. The nPA connector provides the benefit of a service that offers the mechanism for sharing authentication data between trusted applications. The attributes that an application is allowed to query are specified within the contract signed with a trusted Identity Provider. The nPA Connector allows security systems and application to be developed and evolve independently. The main challenges with nPA are the integration in Enterprise Environments.

The paper is structured as follow: Section 2 presents the related work in the field of security communication and eID. Section 3 presents the proposed architecture and in Section 4 the implementation details are presents. We present the conclusions and future work in Section 5.

## RELATED WORK

Across Europe electronic identity (e-ID) card schemes are emerging. The motivation for their deployment varies from country to country, and hence also their ability to interoperate. National schemes for each country are defined by government agencies and application usage by non-government entities has been limited [1]. A very common situation is that for each service, users must remember the

---

\* Corresponding Author

associated name and password they are registered under. This method is prone to identity theft and its usability leaves much to be desired. The Trusted Platform Module (TPM) proposed in [2] is a microcontroller with cryptographic functions that is integrated into many computers. Using communication services like voice services, chat services and web 2.0 technologies (wikis, blogs, etc.) are a common part of everyday life in a personal or business context. These communication services typically authenticate participants. Identities identify the communication peer to users of the service or to the service itself. Calling line identification used in the Session Initiation Protocol (SIP) can be used for Voice over IP (VoIP) [3]. In [4] is dealing with the use of the Belgian electronic ID card to secure Presence notifications in the Session Initiation Protocol (SIP). More specifically, it addresses the secure authentication to a SIP registrar server thanks to the Belgian electronic ID card. The proposed solution consists in adding an Authenticated Identity Body (AIB) to the REGISTER requests issued by the user's agent, which simultaneously authenticates the user and protects the request header. The Italian Electronic Identity Card (EIC, for short) is a polycarbonate smart card equipped with a microchip (supporting cryptographic functions) and a laser band (featuring an embedded hologram). It contains personal (e.g. name, surname, date of birth, etc.) and biometric data (photo and fingerprint) of a citizen [5]. Currently, Republic of Turkey has introduced a new smart card based electronic identity card. By the help of this card, e-government projects of Turkey are expected to accelerate. Turkey is also prepared to use biometrics in citizen authentication. In this paper, we will shortly mention about physical and electronic properties of this card, use of biometrics, cryptographic details of the card, Electronic Authentication System and roll out of the card [6].

The new identity card ("Neuer Personalausweis", nPA) was introduced in Germany in 2010. It supports the Federal Government's eCard strategy. The nPA is part of the nationwide introduction of the use of smart cards in the federal administration. The eCard-API-Framework is a technical frame for implementing the eCard strategy and is specified in the technical guideline BSI TR-03112 of the Federal Office for Information Security (BSI) [7]. The basic goal is to expand the conventional use of the identity card to

the electronic world, thus enabling a secure and legally binding communication on the Internet [8].

## NPA CONNECTOR ARCHITECTURE

The main principle for using the nPA connector resides on the usage of certificates obtained from a trusted Identity Provider that specifies the data that an application is allowed to query from the identity card when interacting with the back-end user through the citizen's application.

The nPA Connector library represents a solution for the simple integration of nPA into web applications by taking away the complexity of handling the communication with the Identity Server.

The nPA Connector offers a trusted infrastructure for secure handling of electronic identities in the Internet for a variety of applications. The connector allows querying the attributes from the electronic Identity card providing also a useful tool for securely validating information about the citizens. The connector makes it easy for web applications to communicate with an Identity Provider from the eID Service Providers trusted list because it is mainly a mechanism for sharing authentication data between trusted applications (see Figure 1). The user's personal data from the electronic Identity Card is transmitted from an original source service provider to subsequent destination service providers, all of which have previously signed a contract with the Identity Provider, allowing them to query particular information about the user, and in agreement with the citizen's options for sharing their personal data.

At a deeper level, the nPA connector acts like a Service provider between a user wielding a user agent (usually a web application accessed through a web browser) and an Identity Provider. The user requests a web resource from the application which is in fact protected by the Service provider responsible for creating a secure context for querying sensitive data.

The service provider, who wishes to know the identity of the requesting user, and also personal information about the user, issued the authentication request to the Identity Provider through the user agent.

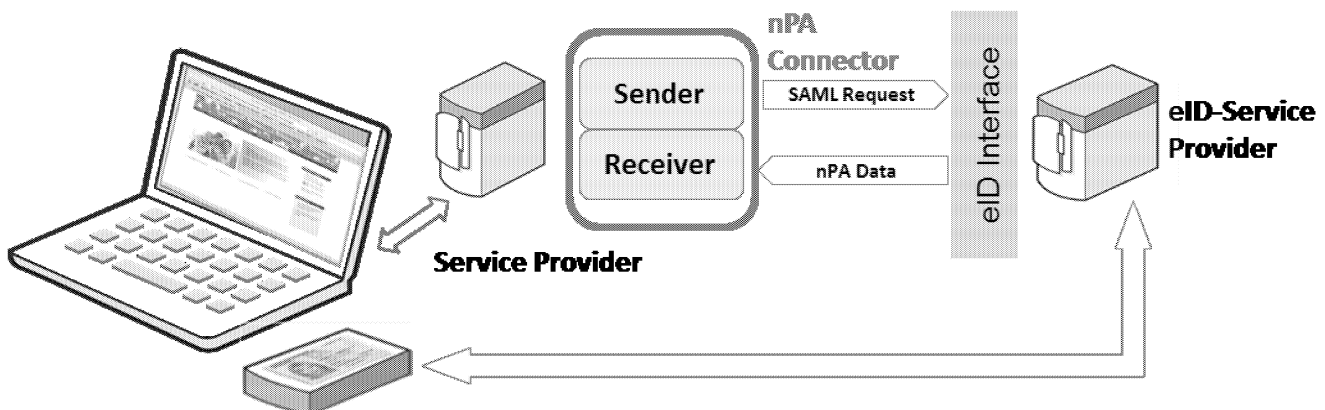


Figure 1. nPA Architecture and interactions

## IMPLEMENTATION DETAILS

This library allows security systems and application software to be developed and evolve independently, and also allows decoupling of the application software from the underlying security infrastructure. This is because SAML provides a set of interoperable standard interfaces. Standardizing the interfaces between systems allows for faster, cheaper, and more reliable integration. Furthermore, this library provides the possibility to configure custom extensions of the profiles of SAML usage, and the benefits that come from this customization open up more and different kinds of access management.

Following are some more concrete benefits of this connector brought by the usage of SAML protocol:

- *Platform neutrality.* Abstractization of the security framework away from platform architectures and particular vendor implementations. Making security more independent of application logic is an important tenet of Service-Oriented Architecture.
- *Improved online experience for end users.* It enables single sign-on by allowing users to authenticate at an identity provider and then access service providers without additional authentication by creating security contexts.
- *Reduced administrative costs for service providers.* The burden of maintaining account information burden is transferred to the identity provider.
- *Risk transference.* It pushes responsibility for proper management of identities to the identity provider, which is more often compatible with its business model than that of a service provider.

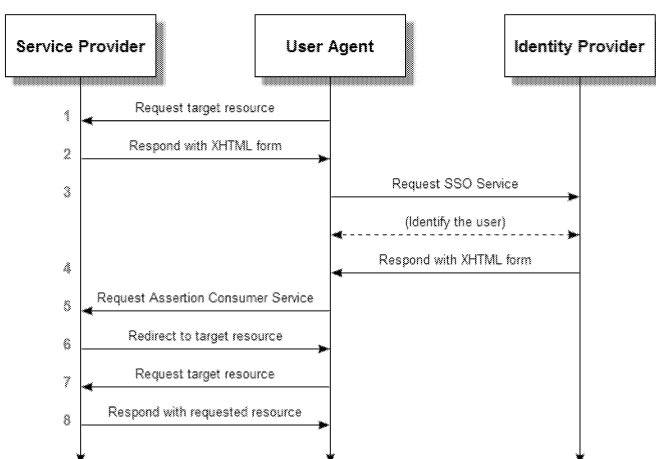


Figure 2. nPA protocol

The main functionality of the nPA connector library is based on the SAML 2.0 protocol [9]. SAML is a XML-based protocol whose functionality is defined by four basic concepts: assertions, protocols, bindings and profiles. Assertions are XML-based messages that are formed using

the rules of syntax and semantics defined in the SAML Core. These assertions are requested and transmitted using one of the specified protocols from one system entity to another.

The requested attributes and equivalent response attributes are defined in a custom schema, specified by the identity Provider server and imply custom made Marshallese and Un-Marshallese to build objects from and to XML files. There are two major types of configurations for profiles: profiles for requesting a number of specific attributes of the user for the Identity Provider; profiles for verifying the value of certain key attributes against a given value.

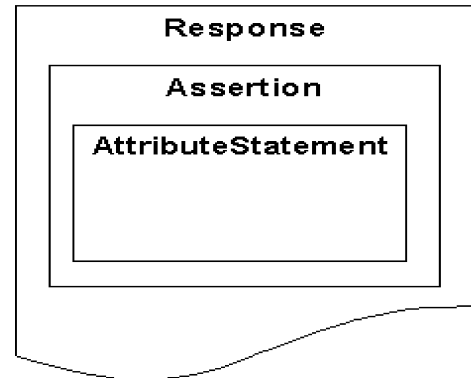


Figure 3. SAML message

The main functionality of the protocol provided by this library is illustrated in Figure 2, where the nPA connector (Service Provider) is responsible for creating a security context for the user agent. The nPA Connector uses the HTTPPost binding from SAML protocol to communicate with the user agent (see Figure 3).

The message flow of the protocol begins with a request of a secured resource at the Service Provider and follows these steps (presented in Figure 2):

### 1. Request a target resource at the SP

- For example <https://sp.example.com/myresource>
- The library performs a security check on behalf of the target resource : if a valid security context already exists skip steps 2 – 7

### 2. Respond with an XHTML form

```
<form method="post"
action="https://idp.example.org/SAML2/SSO/POST" ...>
  <input type="hidden" name="SAMLRequest"
value="request" />
  <input type="hidden" name="RelayState"
value="token" />
  ...
  <input type="submit" value="Submit" />
</form>
```

- The value of the SAMLRequest parameter is the base64 encoding of the actual <samlp:AuthnRequest> element



### 3. Request the SSO Service at the IdP

- The user agent issues a POST request to the SSO service at the identity provider

```
POST /SAML2/SSO/POST HTTP/1.1
Host: idp.example.org
Content-Type:
application/x-www-form-urlencoded
Content-Length: nnn
SAMLRequest=request&RelayState=token
```

### 4. Respond with an XHTML form

- The SSO service validates the request and responds with a document containing an XHTML form:

```
<form method="post"
action="https://sp.example.com/SAML2/SSO/POST" ...>

<input type="hidden" name="SAMLResponse"
value="response" />

<input type="hidden" name="RelayState"
value="token" />

...

<input type="submit" value="Submit" />
</form>
```

- The value of the SAMLResponse parameter is the base64 encoding of the actual <samlp:Response> element.

### 5. Request the Assertion Consumer Service at the SP

```
POST /SAML2/SSO/POST HTTP/1.1
Host: sp.example.com
Content-Type:
application/x-www-form-urlencoded
Content-Length: nnn
SAMLResponse=response&RelayState=token
```

### 6. Redirect to target resource

- The library creates a security context and redirects the user to the request resource

### 7. Request the target resource at the SP again

### 8. Respond with the requested resource

Since a security context exists, the service provider returns the resource to the user agent.

The requested attributes, are encrypted using a symmetric key and sent as a protocol message using the HTTP POST binding. The SSO service at the Identity provider validates the request and responds with a document containing the response. The value of the SAMLResponse parameter is the base64 encoding of a <samlp:Response> element, which

likewise is transmitted to the service provider via the browser.

The main issue with nPA is the security and support for authentication. Strong authentication continues being one of the most important security issues & goals and gains even more importance if services move to the cloud. Moreover, strong authentication is achieved best with a certificate on a smartcard. Considering this issue nPA-Smartcard provides three applications for official and commercial/private use: ePass(port), eID, eSign. The nPA uses the following Communication Protocols: Password Authenticated Connection Establishment (PACE) and Extended Access Control (EAC).

The nPA Connector stands for an extensible and configurable plugin for web based applications that wish to communicate with an Identity Provider with which they have previously signed an agreement and obtained a certificate that allows them to query certain sensitive information about the citizens. The configuration of the connector can easily be done by altering the configuration file (as seen in the examples in previous chapter).

For example, as use case, if a user has signed on and authenticated at a portal like <http://www.rentamovie-exampleportal.com> and wish to rent a movie, the website will only get access to the attributes specified within the contract of that website (for example the age of the end-user) with the Identity Provider, and in agreement with the user's preferences for displaying sensitive data (the user may not agree to share other information).

At a high level, the entry point in the library is represented by the eIDHandler which is an abstraction for handling both the request and the response messages as illustrated in Figure 4.

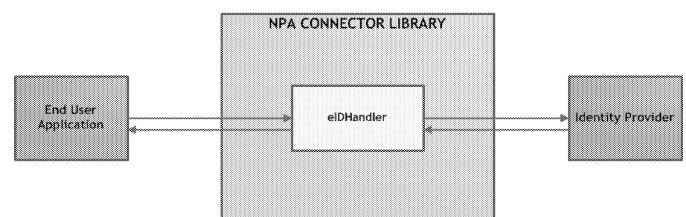


Figure 4. Entry point for nPA

The eIDHandler is actually an abstraction layer that offers methods like `handleRequest()`, `handleResponse()` and in fact uses dedicated handlers for request (eIDRequestHandler – responsible for creating custom extensions for the given profile), and response (eIDResponseHandler – responsible for reading the custom extensions from the response assertion received from the identity provider server). The core functionality of the SAML protocol is described and implemented in third party libraries and do not make the object of this document.

The message flow of the protocol begins with a request of a secured resource at the Service Provider and follows these steps: request a target resource at the SP, respond with an XHTML form, request the SSO Service at the IdP, respond

with an XHTML form, request the Assertion Consumer Service at the SP, redirect to target resource, request the target resource at the SP again, respond with the requested resource. The nPA library uses the Authentication Request

Protocol, as specified in SAML Core [9] to communicate with the Identity Provider. The overall flow of the authentication process through the library is shown in the Figure 5.

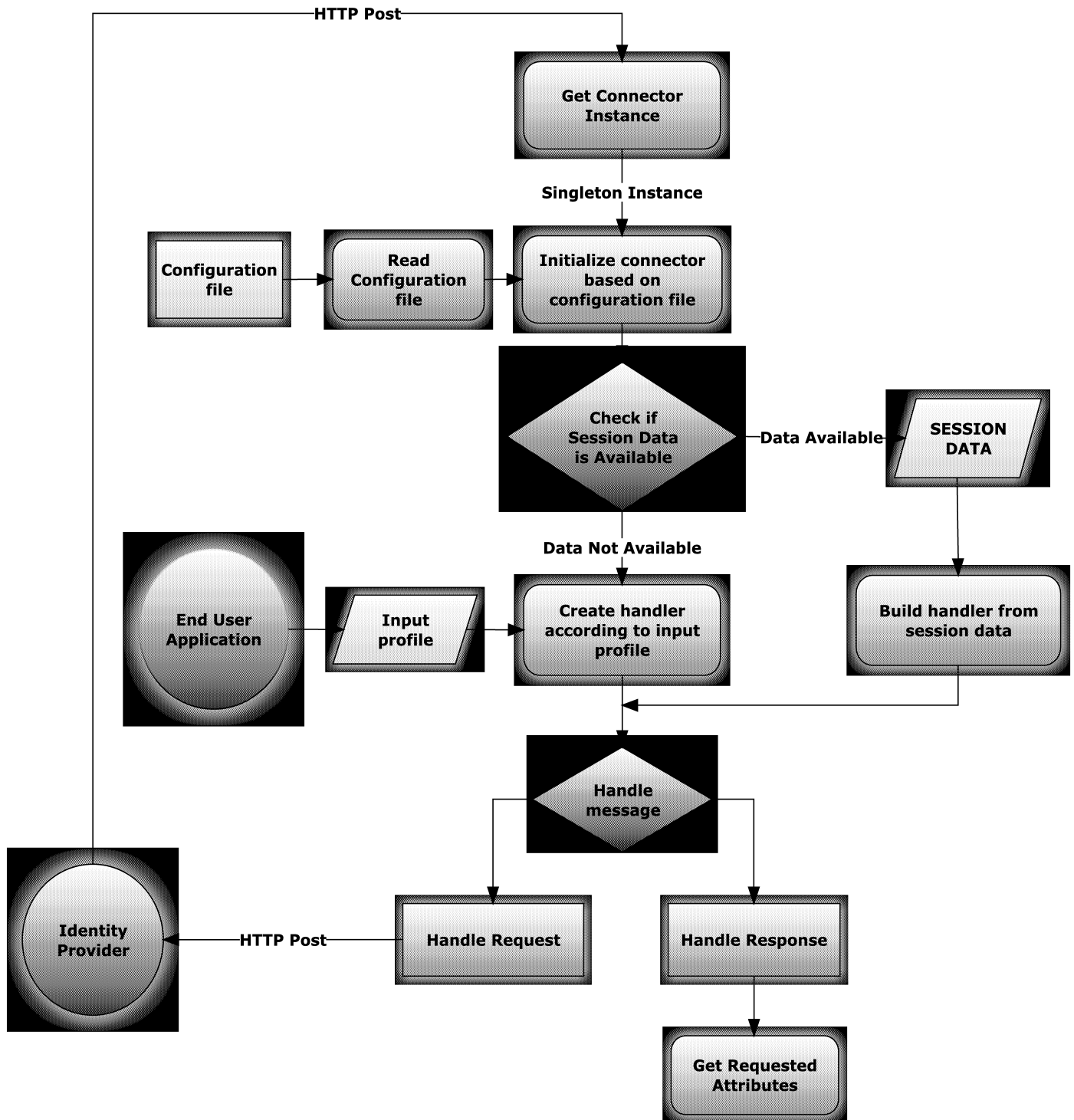


Figure 5. nPA authentication process

## CONCLUSIONS

We present in this paper the nPA connector architecture and implementation details. The nPA Connector consists in an application which allows a secure identification of a certain user using an electronic identity card (eID) over the Internet.

The nPA Connector is designed for PHP and JAVA implementation using the Apache Server and will be available under different OS, both Windows and Linux environments. The nPA Connector was tested on Windows 2008 and using IIS7. The solution uses the SAML library which has a MPL license.

The common requirements will be emphases as future work and will cover technical requirements for active directory and technical requirements for infrastructure, because presently, Active Directory integration of the nPA is not possible; observe the evolution of nPA enterprise integration (especially the evolution of eID services). On the other hand nPA enterprise integration for Active Directory logon is possible, because: complete PKI is run by the German government, PKI of German government promises to be highly reliable, and cost for smartcard logon with nPA will be far beyond cost of an own PKI with smartcard logon (not nPA).

## ACKNOWLEDGMENTS

The research presented in this paper is supported by national project: "SORMSYS - Resource Management Optimization in Self-Organizing Large Scale Distributes Systems", Contract No. 5/28.07.2010, Project CNCSIS-PN-II-RU-PD ID: 201. The work has been co-funded by the Sectorial Operational Program Human Resources Development 2007-2013 of the Romanian Ministry of Labor, Family and Social Protection through the Financial Agreement POSDRU/89/1.5/S/62557. The research presented in this paper was implemented in the international project called "PrO", developed by Centre for Advanced Studies on Electronic Services (e-CAESAR).

## REFERENCES

- Siddhartha Arora. 2008. National e-ID card schemes: A European overview. *Inf. Secur. Tech. Rep.* 13, 2 (May 2008), 46-53.
- Andreas Klenk, Holger Kinkelin, Christoph Eunicke, and Georg Carle. 2009. Preventing identity theft with electronic identity cards and the trusted platform module. In *Proceedings of the Second European Workshop on System Security (EUROSEC '09)*. ACM, New York, NY, USA, 44-51.
- Rainer Falk, Steffen Fries, and Hans Joachim Hof. 2010. Protecting Voice over IP Communication Using Electronic Identity Cards. In *Proceedings of the 2010 Third International Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies and Services (CENTRIC '10)*. IEEE Computer Society, Washington, DC, USA, 5-10.
- Sebastien Gamby, Laurent Schumacher, and Jean Ramaekers. 2007. Securisation of SIP Presence notifications thanks to the Belgian electronic identity card. In *Proceedings of the The 2007 International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST '07)*. IEEE Computer Society, Washington, DC, USA, 125-129.
- Franco Arcieri, Mario Ciclosi, Fabio Fioravanti, Enrico Nardelli, and Maurizio Talamo. 2004. The Italian electronic identity card: a short introduction. In *Proceedings of the 2004 annual national conference on Digital government research (dg.o '04)*. Digital Government Society of North America , Article No: 73.
- Mucahit Mutlugun and Oktay Adalier. 2009. Turkish national electronic identity card. In *Proc. of the 2nd int. conf. on Security of information and networks (SIN '09)*. ACM, New York, NY, USA, 14-18.
- BSI: *Advanced Security Mechanisms for Machine Readable Travel Documents*; Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI); Version 2.03. Technische Richtlinie TR-03110, 2010.
- Margraf, Marian: *Der elektronische Identitätsnachweis des zukünftigen Personalausweises*. SIT-SmartCard Workshop 2009, Darmstadt, 2009.
- Alessandro Armando, Roberto Carbone, Luca Compagna, Jorge Cuellar, and Llanos Tobarra. 2008. Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for Google Apps. In *Proceedings of the 6th ACM workshop on Formal methods in security engineering (FMSE '08)*. ACM, New York, NY, USA, 1-10.



# **AUTHOR LISTING**



## AUTHOR LISTING

Agape A. ....	18	Mansour H. ....	29
Agre G. ....	49	Mavata G. ....	85
Andreica M.I. ....	93		
Burceanu E. ....	39	Negru C. ....	67
		Nyambo B.M. ....	85
Ciminian A. ....	21	Oros R.-G. ....	14
Ciobanu V. ....	100		
Comaneci D. ....	78	Patrascu A. ....	5
Cotfas D. ....	14	Pilato G. ....	54
Cotfas P.A. ....	14	Pop F. ....	67/100
Cristea V. ....	5/39/67/100	Popescu D. ....	100
		Popescu N. ....	100
Dobre C. ....	5/21/39/67		
.....	78/100	Rizzo R. ....	54
Dochev D. ....	49		
		Sâmbotin A.-D. ....	93
Elayyan H. ....	29	Samoila C. ....	14
		Stegaru S. ....	78
Fujikawa K. ....	73	Steinmetz A. ....	35
		Sunahara H. ....	73
Hastik C. ....	35		
		Tanase M. ....	59
Infantino I. ....	54	Terada N. ....	73
Inomata A. ....	73		
		Udrea A. ....	59
Janssens G.K. ....	85	Ursutiu D. ....	14
Kawai E. ....	73	Vella F. ....	54
Kominami E. ....	73		
Leordeanu C. ....	5		