Biblioteka Informatyki
Szkół Wyższych

# Information Systems Architecture and Technology

## Network Architecture and Applications

**Library of Informatics of University Level Schools**

Series of editions under the auspices
**of the Ministry of Science and Higher Education**

The ISAT series is devoted to the publication of original research books in the areas of contemporary computer and management sciences. Its aim is to show research progress and efficiently disseminate current results in these fields in a commonly edited printed form. The topical scope of ISAT spans the wide spectrum of informatics and management systems problems from fundamental theoretical topics to the fresh and new coming issues and applications introducing future research and development challenges.

The Library is a sequel to the series of books including Multidisciplinary Digital Systems, Techniques and Methods of Distributed Data Processing, as well as Problems of Designing, Implementation and Exploitation of Data Bases from 1986 to 1990.

Wrocław University of Technology

# Information Systems Architecture and Technology

## *Network Architecture and Applications*

Editors
*Adam Grzech*
*Leszek Borzemski*
*Jerzy Świątek*
*Zofia Wilimowska*

Wrocław 2013

**Publication partly supported by**

Faculty of Computer Science and Management
Wrocław University of Technology

*Project editor*

Arkadiusz GÓRSKI

The book has been printed in the camera ready form

OFICYNA WYDAWNICZA POLITECHNIKI WROCŁAWSKIEJ
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław
http://www.oficwyd.pwr.wroc.pl;
e-mail: oficwyd@pwr.wroc.pl
zamawianie.ksiazek@pwr.wroc.pl

ISBN 978-83-7493-801-3

# CONTENTS

## PART 1. NETWORK PERFORMANCE ANALYSIS AND EVALUATION

## PART 2. TRAFFIC MANAGEMENT AND PROCESSING

## PART 3. WEB SYSTEMS DESIGN AND EVALUATION

# INTRODUCTION

The overall gain of contemporary proposed and deployed ICT (Information and Communication Technologies) applications is to explore and utilize new concepts, paradigms, methods, attempts and architectures to increase the effectiveness of business processes and to propose applications of high societal value through making use of reappraised distributed systems architectures, services and technologies in large-scale application context. New functionalities of information systems are supported by new concepts to provide network services.

The book addresses subjects dealing with various methodological, technological and applications aspects of distributed information and communication systems, i.e., technologies, organization, application and management involved in gain to increase efficiency, resources utilization, flexibility, functionalities and quality of services offered by contemporary information and computer systems.

Chapters, selected and presented in the book are devoted to discuss - on a very different level of generality - some selected communication technologies and address a number of issues important and representative both for available information and communication technologies as well as information system users requirements and applications. Submissions, delivered within distinguished chapters, are strongly connected with issues being important for contemporary information processing, communication and data communication system.

The book is divided into three parts, which include sixteen chapters. The parts have been completed arbitrary from chapters addressing some extensively researched and recounted in the world literature important and actual issues of distributed information systems. The proposed decomposition of accepted set of chapters into parts is to compose units presenting methods, algorithm and tools for distributed systems design and analysis, information systems requirement analysis, service oriented systems, web systems, traffic analysis as well as modeling, analysis and optimization of networks and distributed systems infrastructures enabling efficient delivery of information.

The first part - *NETWORK PERFORMANCE ANALYSIS AND EVALUATION* - contains chapters addressing various issues related to communication systems architectures and technologies, different aspects of requirement analysis, methods and algorithms for performance measures values estimation, influence of traffic classes and switching procedures on quality of service and methods allowing distributed systems overall analysis. The chapters present results of analytical and simulation studies.

The second part - *TRAFFIC MANAGEMENT AND TRAFFIC PROCESSING* – contains chapters where some selected problems strongly connected with various quality of service delivery strategies for networked systems and security of transferred data are considered.

The third part - *WEB SYSTEMS DESIGN AND EVALUATION* - contains chapters where some Web systems design and evaluation problems are .

## *PART I. NETWORK PERFORMANCE ANALYSIS AND EVALUATION*

The ***Chapter 1*** is devoted to evaluation of call control procedures available within Automatically Switched Optical Network (ASON) utilizing Generalized Multi-Protocol Label Switching (GMPLS) protocols named as ASON/GMPLS. The proposed evaluation of call control takes into account mean Call Set-up Time E(CallST) and mean Call Release Time E(CallRT) and is performed as dependent on offered traffic, request intensity and proportion of requests class.

***Chapter 2*** is devoted to present and discuss traffic model dedicated for design and analysis of the Next Generation Network (NGN), which is standardized for distribution of current and future multimedia services based on the IP Multimedia Subsystem (IMS). The proposed model is to evaluate mean Call Set-up Delay E(CSD) and Call Disengagement Delay E(CDD) in a single domain of IMS/NGN. Obtained analytical results are compared to results offered using other queuing approaches, i.e., M/G/1 systems and approximations of G/G/1 based on two or three moments of arrival distribution and two moments of service distribution.

The next ***Chapter 3*** gains is to present switch architecture and proper scheduling algorithms. These algorithms, i.e., SSMPS (Single Size Matching with Permanent Selection) and Maximal Size Matching with Permanent Selection (MSMPS) algorithms based on permanent connections between an inputs and an outputs were investigated using simulation for different distribution traffic. The analyzed algorithm were compared with different, known algorithms.

In the ***Chapter 4*** aim is to present a simulation model of a multiservice switching network with overflow traffic and simulation results of a Clos switching network carrying a mixture of different multi-service overflow traffic streams. The results of the simulation of the considered networks with overflow traffic are compared with the results of the simulation of a switching network with traffic streams generated by the infinite and finite number of traffic sources and Erlang and Engset traffic.

***Chapter 5*** aim is to present results of studies of routing quality and influence of self-similarity and Poisson traffic type on network performance for traffic class in Differential Services architecture. Presented simulation results are obtained for two network topologies and for two traffic classes: streaming and best-effort as a function of buffer lengths within streaming traffic class and for many proportions between these classes.

In the next ***Chapter 6*** Web system's performance predictions under given load and configuration is presented. Results retrieved from the proposed, adequate model are validated against three experiments outcomes. Proposed model successfully capture the performance characteristics of multitier web system including the cases of overload.

*PART II. TRAFFIC MANAGEMENT AND TRAFFIC PROCESSING*

***Chapter*** 7 aims are to review of the current state-of-the-art WMN (Wireless Mesh Networks) routing protocols and performance measures as well as to evaluate properties and to propose classification of WMN routing protocols.

The ***Chapter 8*** refers to anomaly detection in network traffic based on Self Organizing Map advantages. The proposed approach is to perform analysis of network data and find patterns that indicate occurrences of malicious activities. The basic property of the presented approach is an identification of suspicious network activity availability even if there is no knowledge of previous anomalies.

In ***Chapter 9*** the approach to some aspects of Multi-Level Security (MLS) systems verification on the base of Bell-LaPadula and Biba models is presented. The essence of the proposed approach to analyze properties of MLS security-design models and their instances is integration of various models and their evaluation and simulation.

The main purpose of the ***Chapter 10*** is to identify, analyze and classify distinctive sets of threats and vulnerabilities as well as some data protection opportunities related to innovative wireless transmission methods and technologies. The issues related to security, new threats and risks to data security in context of the technologies are discussed.

The ***Chapter 11*** is devoted to description of architecture that enables the virtualization management in the context of SOA (Service Oriented Architecture) and SLA (Service Level Agreement). The chapter includes the description of the SOA and virtualization themselves and the idea of quality-aware service request processing as well as service awareness on the low level of virtualization management that ensures quality during requests processing.

*PART III. WEB SYSTEMS DESIGN AND EVALUATION*

The ***Chapter 12*** gain is to present an attempt how service oriented architecture can evolve to event-driven-architecture, while preserving capabilities to communicate over World-Wide-Web. For this purpose new architectural style, protocol and developed API are presented.

The ***Chapter 13*** presents multi-agent system where geostatistical estimation methods (Simple Kriging and Ordinary Kriging) are applied to forecast network performance in a selected period of time.

In the ***Chapter 14*** is devoted to discuss results of the session-based analysis of data in online bookstore logs. In particular, it presents a comparison of buying and non-buying user sessions in terms of the session length, duration, and mean time per page. The findings show significant differences in characteristics of both kinds of sessions.

The ***Chapter 15*** gain is  to examine how selected graphical factors influence the efficiency of searching for a specific product in an electronic mock-up shop. The study investigates three various factors, each on two levels: two different types of search tasks (general and detailed) and types of digital presentation arrangements of the products.

In the last ***Chapter 16*** it is shown interrelations among persons' attitudes and graphical marketing information regarding various types of smartphone's packages designs.

# PART 1

# NETWORK PERFORMANCE ANALYSIS AND EVALUATION

*ASON, GMPLS, control performance,*
*connection control, call control, NGN*

Sylwester KACZMAREK*, Magdalena MŁYNARCZUK*

# CALL CONTROL EVALUATION IN ASON/GMPLS ARCHITECTURE

The Automatically Switched Optical Network (ASON) utilizing Generalized Multi–Protocol Label Switching (GMPLS) protocols named as ASON/GMPLS is one of the propositions of Next Generation Network. The basic assumption of ASON control plane is a separation of call control from connection control. The control plane is divided into call control and connection control components. Presented work regards the problem of call control evaluation in a single domain of ASON/GMPLS architecture. The authors present the evaluation of call control taking into consideration mean Call Set-up Time *E*(CallST) and mean Call Release Time *E*(CallRT). The evaluation is performed in conditions of offered traffic, request intensity. The analysis is performed with simulation method by using OMNeT++ discrete-event simulator for two structures of ASON/GMPLS architectures: Poland and Europe. Obtained results are compared with mean Connection Set-up Time *E*(CST) and mean Connection Release Time *E*(CRT).

## 1. INTRODUCTION

Strong demand for supplying high capacity applications with required quality of service and reliability leads to evaluation of typical IP networks with packet switching towards optical solutions which supports multiple types of switching including packet switching, Time-Division Multiplexing (TDM), wavelength and fiber switching.

One of the conception of architecture which has a chance to fulfill these requirements is the Automatically Switched Optical Network (ASON) [1,2] utilizing Generalized Multi-Protocol Label Switching (GMPLS) [3,4] protocols. The solution is known as ASON/GMPLS architecture.

* Department of Teleinformation Networks, Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, Gabriela Narutowicza 11/12 Street, 80-233 Gdańsk, Poland.

The ASON/GMPLS has ability to support high capacity services with guaranty of quality. According to standardization the architecture consists of three planes: the control plane, management plane and transport plane where the main role plays the control plane responsible for fast and efficient configuration of connections within a transport network to support both switched and soft permanent connections. In the process of connection establishment GMPLS protocols like RSVP-TE [5,6] for signaling and OSPF-TE for routing [7,8] are used.

The basic assumption of ASON control plane is a separation of call control from connection control. In the control plane recommendations regards components supplying call service functions and connection service functions. The call control is a signaling association between one or more user applications and the network to control the set-up, release, modification and maintenance of sets of connections. The connection control is performed by the protocol undertaking the set-up and release procedures associated with a connection and the maintenance of the state of the connection [2].

The ASON/GMPLS architecture is a conception of Next Generation Network which introduce the intelligence necessary to minimize the manual interactions required in service provisioning. The implementation of this architecture could be hard difficult since the control plane components are described in terms that place no restrictions regarding how call control functions and connection control functions are combined and provided. In the recommendations [1,2,3,5,7] the interactions among call and connection components and the information flow required for communication between components are defined via abstract interfaces.

For a time being introduction of the ASON/GMPLS architecture is concerned with performance evaluation in research society. Practical realizations of ASON/GMPLS architectures are performed in projects [9,10,11,12]. The performance evaluation for larger structures of networks requires simulation method.

In the work the authors present call control evaluation of ASON/GMPLS architecture based on results obtained in ASON/GMPLS simulation model in OMNet++ environment. The work is organized as follows. The control plane standardization in aspect of call control functions is presented in section 2. General information about ASON/GMPLS simulation for call control evaluation is described in section 3. The section 4 is devoted to presentation of results of the performed tests for call control investigation. Conclusions and outlook to future are presented in section 5.

## 2. CALL CONTROL IN ASON/GMPLS ARCHITECTURE

As it is mentioned in section 1 the recommendation [2] for ASON/GMPLS architecture separates the treatment of call components and connection control components in the control plane.

The call control components are Calling/Called Party Controller and Network Call Controller. The Calling/Called Party Controller (CCC) is responsible for generation of outgoing call requests, acceptance or rejection of incoming call requests, generation of call termination requests, processing of incoming call termination requests and call state management. The Network Call Controller (NCC) is instantiated at domain boundary where call parameters like user rights or access to network resource policy have to be examined.

The main connection control components are: Routing Controller, Connection Controller, Link Resource Manager, Termination and Adaptation Performer. The Routing Controller (RC) provides routing functions, the Link Resource Manager (LRM) in cooperation with the Termination and Adaptation Performer (TAP) maintains the network topology. The Connection Controller (CC) takes charge of coordination among the Link Resource Manager (LRM), Routing Controller (RC) and other connection controllers for the purpose of the control of connection set-ups, releases and the modification of connection parameters for existing connections. The interaction between call controller components is dependent upon both the type of call and the type of connection. The example of interaction between Calling/Called Party Controllers, Network Call Controller and Connection Controller for switched connection is presented in Fig. 1 [2].

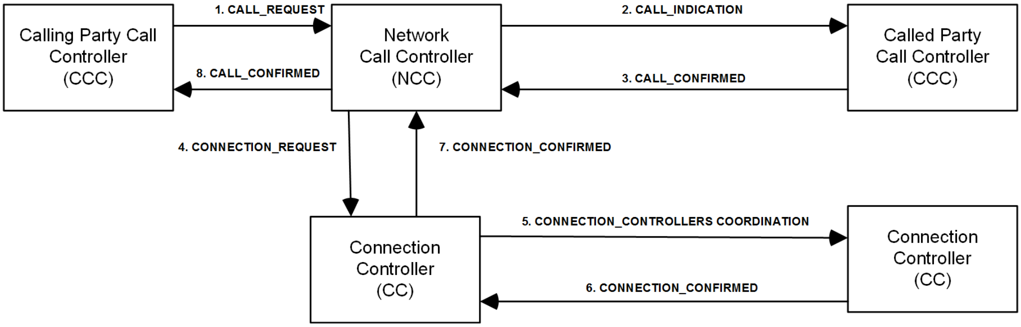

Calling Party Call Controller (CCC)
1. CALL_REQUEST
8. CALL_CONFIRMED
Network Call Controller (NCC)
2. CALL_INDICATION
3. CALL_CONFIRMED
Called Party Call Controller (CCC)
4. CONNECTION_REQUEST
7. CONNECTION_CONFIRMED
Connection Controller (CC)
5. CONNECTION_CONTROLLERS COORDINATION
6. CONNECTION_CONFIRMED
Connection Controller (CC)

Fig. 1. Called/calling party call controller interaction for switched connections

Detailed description of call and connection control components is beyond the scope of the work and can be found in [2].

## 3. ASON/GMPLS SIMULATION MODEL

The simulation model is created for a single domain of ASON/GMPLS architecture. The model is implemented in OMNeT++ simulator [13] and it is devoted to measure general parameters of control plane performance like: mean Call Set-up Time

*E*(CallST), mean Connection Set-up Time *E*(CST), mean Call Connection Release Time *E*(CallCRT) and mean Connection Release Time *E*(CRT) for different structures of telecommunications networks from SND network library [14].

The call control is represented by Calling/Called Party Controllers (CCC_1 and CCC_2), Network Call Controller (NCC) and IDS (additional block for call identifier assignment). Each transport element (emulated OXC) is represented as Control Element (CE) in the control plane. The structure of the CE include functionality of CC, LRM, RC, TAP. In the simulation two class of requests are provided: low priority and high priority. In the call control plane low and high requests are serve in the same way. In the transport plane we assume a pools of resources for high priority requests (protected pool) and common pool of resources for both low and high priority requests. The protected pool can be used by high priority requests only when the common pool is exhausted. The pool approach is detailed described in [15].

The Fig. 2 presents typical call set-up scenario and call release scenario for a single ASON/GMPLS domain consists of three nodes. In Fig. 2 measured times presented in the work are depicted.

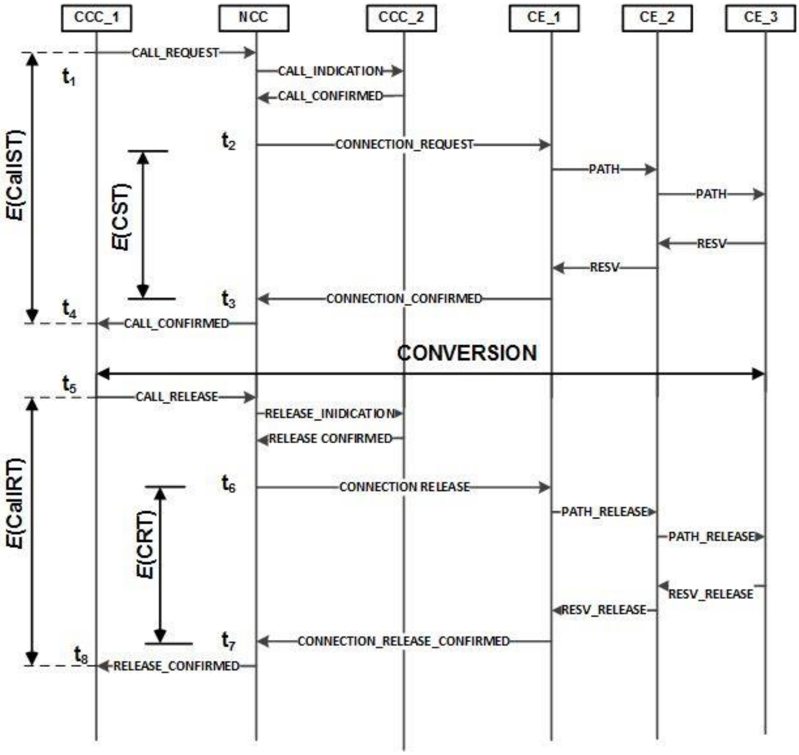


Fig. 2. The call set-up scenario and call release scenario

Due to limited space more detailed information about the network model and call scenarios are not provided and can be found in [16,17,18].

## 4. THE ASON/GMPLS CALL CONTROL RESULTS

The simulation model described in section 3 was used to evaluate call control in ASON/GMPLS architecture. The authors take into consideration mean Call Set-up Time *E*(CallST) and mean Call Release Time *E*(CallRT) which were calculated based on the simulation results (Fig. 2). The evaluation was performed in conditions of offered traffic, request intensity. Obtained results are compared with mean Connection Set-up Time *E*(CST) and mean Connection Release Time *E(*CRT). Additionally loss probabilities were investigated.

Because of limited number of practical implementations of ASON/GMPLS architecture we have no representative information concerned with traffic parameters of services. Due to this for comprehensive evaluation following assumptions were made:

-total simulation time: 3600s,
-warm-up period: 200s,
-15 measurements intervals,
-exponential distribution of call request,
-exponential distribution of connection release requests,
-20% of all generated requests are high priority,
-mean connection duration time: 2 min., 15 min., 30 min.,
-blocking probability of OXC: 0.001,
-signaling link capacity 10Mb/s,
-wavelength capacity: 1Gb/s
-capacity of single connection requests: 5Mb/s, 10Mb/s, 15Mb/s,
-the number of wavelengths per fiber: 40,
-20% of wavelengths are in the protected pool.

Although measurements in the simulation environments were performed at more intensities, due to limited space we demonstrate selected results important for call control evaluation. The simulation results estimated using *t*-Student distribution with confidence intervals equal 0.95 are presented in Fig. 3-9.

The Fig. 3 and Fig. 4 present mean Call Set-up times under condition of 2, 15 and 30 minutes connection duration. Presented results indicate that mean values of Call set-up Time *E*(CallST) and Call Release Time *E*(CallRT) significantly depend on request intensity assumed as sum of call requests and call release requests. The detailed process of call set-up scenario and call-release scenario is presented in [16].

Comparing results obtained in Fig. 3 and Fig. 4 we noticed that for the same connection duration the greater intensity is, the smaller the time of call set-up is. In Fig. 3 (requests intensity equals 65 requests per second) for Poland and Europe structures

*E*(CallST) is up to 18.6ms and 35.3ms respectively. In Fig 4 (322 requests per second) for Poland and Europe structures *E*(CallST) is up to 18.3ms and 35.1ms respectively.

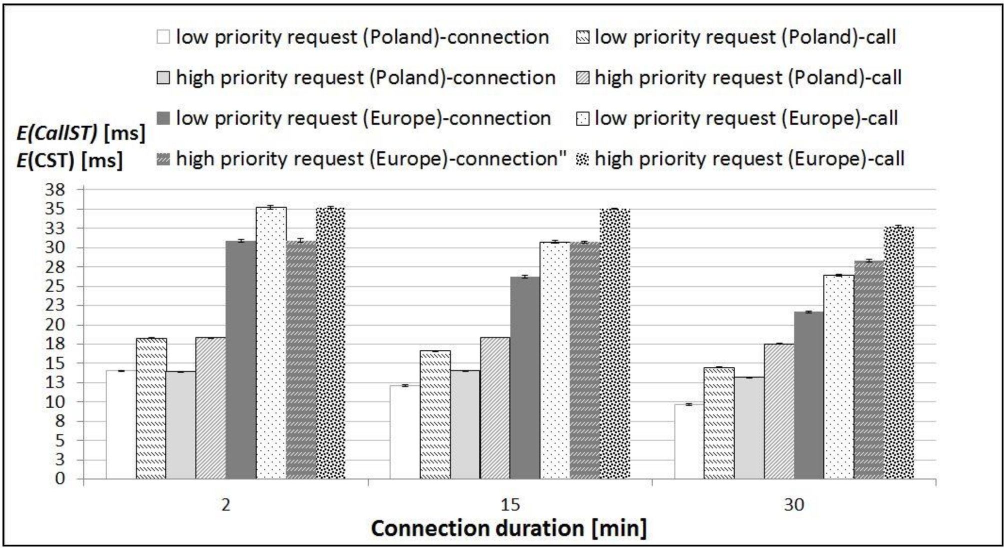


Fig. 3. Mean Call Set-up Time and Mean Connection Set-up Time for Poland and Europe structures for request intensity equals 65 requests per second

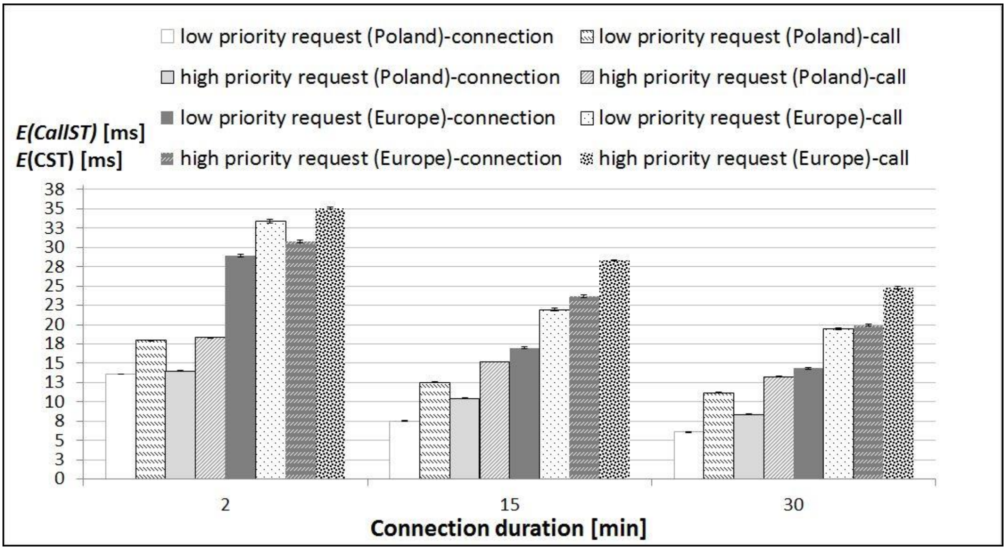


Fig. 4. Mean Call Set-up Time and Mean Connection Set-up Time for Poland and Europe structures for request intensity equals 322 requests per second

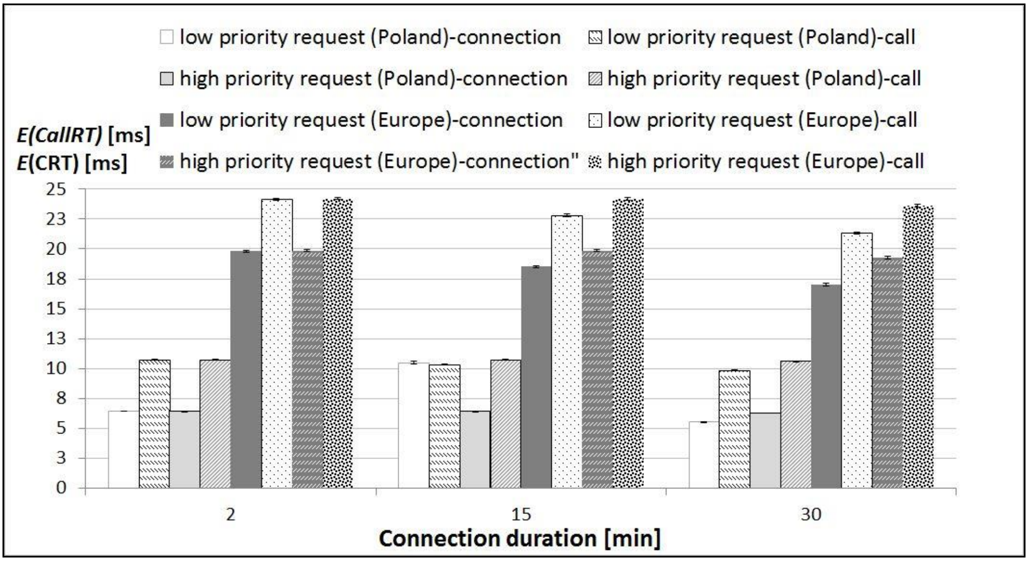


Fig. 5. Mean Call Release Time and Mean Connection Release Time for Poland and Europe structures for request intensity equals 65 requests per second

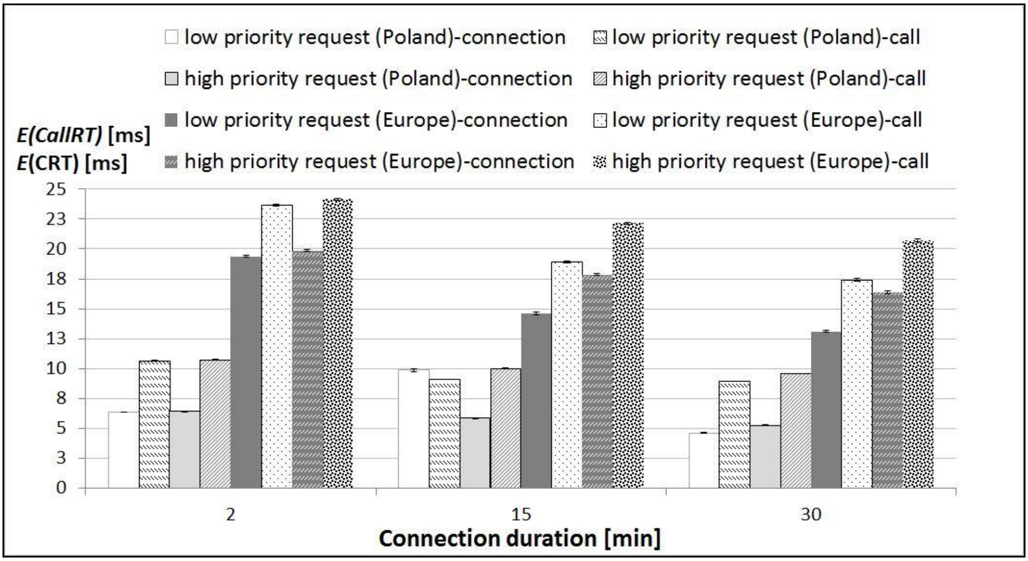


Fig. 6. Mean Call Release Time and Mean Connection Release Time for Poland and Europe structures for request intensity equals 322 requests per second

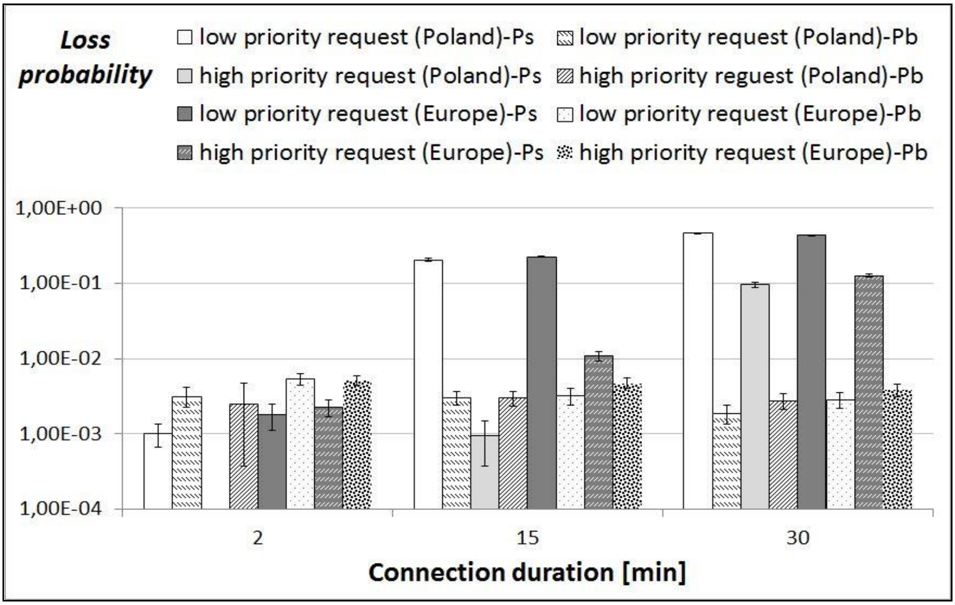


Fig. 7. Loss probability concerned with lack of optical resources (Ps) and blocking OXC probability (Pb) for request intensity equals 65 requests per second

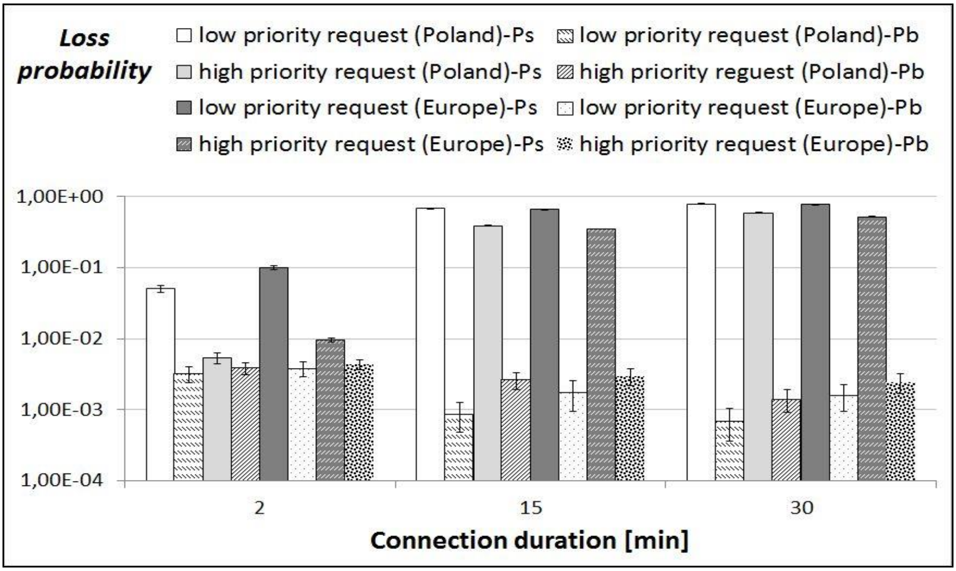


Fig. 8. Loss probability concerned with lack of optical resources (Ps) and blocking OXC probability (Pb) for request intensity equals 322 requests per second

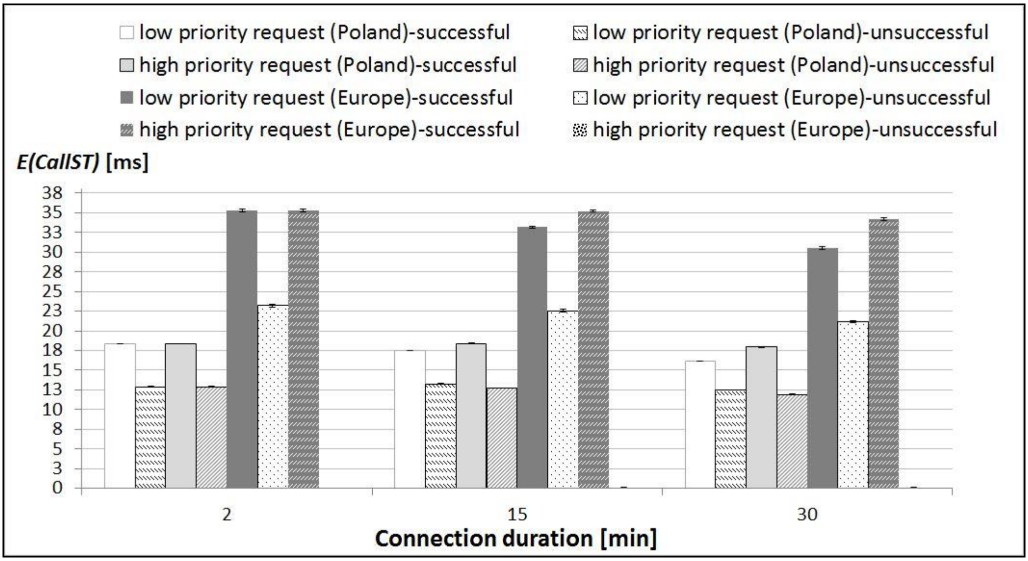


Fig. 9. Mean Call Set-up Time for successfully ended and unsuccessfully ended requests for Poland and Europe structures (request intensity equals 322 requests per second)

Detailed analysis presented in [16] shown that for greater intensities more connections are established to near nodes because of assumed no wavelength conversion in emulated OXCs.

Presented results indicate that values of *E*(CallST) for Poland structure are smaller than for Europe. The difference between E(CallST) is a result of different investigated structures. The Poland structure consists of 12 nodes, the Europe structure has 28 nodes. The bigger structure is, the longer lengths of established connections are. The longer connections are, the greater values of *E*(CallST) are.

The results presented in Fig. 3 and Fig. 4 indicate that high priority requests for greater offered traffic have higher *E*(CallST) than low priority requests. For explanation of this situation loss probabilities measurement were performed.

The Fig. 5 and Fig. 6 present mean Call Release times under condition of 2, 15 and 30 minutes connection duration. For Poland structure the mean values of Call Release Time *E*(CallRT) are smaller about 7ms in compare with *E*(CallST). For Europe structure the mean values of Call Release Time *E*(CallRT) are smaller about 11ms in compare with E(CallST). The difference between *E*(CallST) and *E*(CallRT) results from implemented release process presented in [16].

The Fig. 7 and Fig. 8 are presented for explanation of decrease tendency of *E*(CallST). The figures present loss probabilities for three values of connection duration in condition of two requests intensities values 65 requests per second and 322 requests per second respectively. The authors present loss probabilities (Ps) concerned with lack of free resources in a transport plane and blocking state of OXC

(Pb). The Fig. 7 indicate that for high priority request Ps loss probability is no greater than 0.1 but for low priority requests Ps loss probability is up to 0.4. The results indicate that the more offered traffic to the transport plane, the higher loss probabilities due to wavelength assignment assumption [19]. Additionally, the results shown that intensity equals 322 requests per second is too high to service quarantine. The Pb measurements (Fig. 7) convince that the higher offered traffic the shorter lengths of established connection. For intensity equals 65 requests per second the blocking probability on established connection is no higher than 0.0055 for Europe structure (Fig. 7) and no higher than 0.0032 for Poland structures. Obtained values of Pb convince that for intensity equals 322 requests per second more connections are established on shortest path. The blocking probabilities are no greater than 0.004 which convince about assumed no wavelength conversion in the transport plane and emulated OXC with blocking probability equal 0.001.

For reliable call control evaluation the authors investigate *E*(CallST) for successfully ended requests, finished with call confirmation and unsuccessfully ended requests, unfinished due to lack of optical resources or OXC blocking probability. The Fig. 9 present that *E*(CallST) for unsuccessfully ended high priority requests is equal up to 12ms for Poland structure and up to 35.3ms for Europe structure. The times concerned with unsuccessfully ended request decrease call control performance of ASON/GMPLS architecture.

Presented results indicate also that call service time corresponding with call set-up and defined as time difference between E(CallST)- E(CallST) is no longer than 4.7ms for Poland and Europe structures. The call service time corresponding with call release defined as time difference between E(CallRT)- E(CRT) is 4.3ms for Poland and Europe structures. Difference between call service times corresponding with call set-up and call release is concerned with different mechanism of release operation. The release of call is performed by Call identifier (CallID). Due to such approach the time of call release service is shorter.

## 5. CONCLUSIONS AND FUTURE WORK

The aim of the presented work was to evaluate call control in a single domain of ASON/GMPLS architecture. The evaluation was performed using simulation model which conforms to actual standards and research. The model makes it possible to determine mean values of Call Set-up Time *E*(CallST) and Call Release Time *E*(CallRT) for two structures of network: Poland and Europe. For more reliable evaluation the authors compared call times with connections times. Additionally, loss probabilities of generated requests were investigated.

Obtained results indicate that call control times corresponding with call service in call control plane have small impact on performance of ASON/GMPLS implemented architecture . The great impact on call control evaluation have connections times corresponding with connection control plane. For Poland and Europe structures mean value of call service time is not higher than 4.7ms, where total value of mean Call Setup $E$(CallST) is up to 35ms. Loss probabilities for low priority requests are greater than for high priority requests for the same intensities.

Presented results indicate that signaling link capacity was appropriate to serve requests with required quality of service. Presented call control functionality quarantines offering services with demand call of service. The model does not take into consideration request loss probabilities concerned with examination of user rights or access to network resource policy.

In the future work the authors are planning to perform evaluation of call control in multidomain ASON/GMPLS architecture, including limited queues for different class of requests.

## ACKNOWLEDGEMENTS

This research work was partially supported by the system project “InnoDoktorant–Scholarships for PhD students, Vth edition”, which is co-financed by the European Union in the frame of the European Social Fund.

## REFERENCES

[1] ITU-T Recommendation Y.2012, *Functional Requirements and architecture for next generation networks*, April 2010.

[2] ITU-T Recommendation G.8080/Y.1304, *Architecture for the Automatically Switched Optical Network (ASON)*, February 2012.

[3] MANNIE E., *Generalized Multi-Protocol Label Switching (GMPLS) Architecture*, IETF RFC 3945, October 2004.

[4] FARREL A., BRYSKIN I., *GMPLS, Architecture and applications*, Morgan Kaufmann Publisher, ISBN: 0-12088422-4, 2006.

[5] ITU-T Recommendation G.7713.2/Y.1704.2, *Distributed Call and Connection Management: Signalling mechanism using GMPLS RSVP-TE*, March 2003.

[6] OIF Guideline Document, Requirements for Generalized MPLS (GMPLS) Signaling Usage and Extensions for Automatically Switched Optical Network (ASON), IETF RFC 4139, July 2005.

[7] ITU-T Recommendation G.7715.1/Y.1706.1, *ASON routing architecture and requirements for link state protocols*, February 2004.

[8] KOMPELLA K., REKHTER Y., *OSPF Extensions in Support of Generalized Multi-Protocol Label Switch-ing (GMPLS)*, IETF RFC 4203, October 2005.

[9] CAVAZZONI C., BAROSCO V., et al., *The IP/MPLS Over ASON/GMPLS Test Bed of the IST Project LION*, Journal of Lightwave Technology, Vol. 21, November 2003, 2791-2803.

[10] MUNOZ R., et al., *Experimental demonstration of two new GMPLS lightpath setup protocols for soft-permanent connections over Metro-DWDM DPRing implemented on EMPIRICO ASON testbed*, Global Telecommunications Conference, GLOBECOM '04. IEEE, Vol. 3, 2004, 1798–1802.

[11] SPATH J., MAIER G., et al., *Mupbed: a pan-European prototype for multidomain research networks*, Photonics in Switching, 2006. PS '06. International Conference, 2006.

[12] KACZMAREK S., NARLOCH M., MŁYNARCZUK M., SAC M., *The realization of NGN architecture for ASON/GMPLS network*, Journal of Telecommunications and Information Technology, Nr 3, 2011, 47-56.

[13] OMNet++ Network Simulation Framework, www.omnetpp.org

[14] Network library, Zusse Institut Berlin, http://sndlib.zib.de/home.action

[15] SZYMAŃSKI A., LASOŃ A., RZĄSA J., JAJSZCZYK A., *Grade-of-Service-Based Routing in Optical Networks*, IEEE Communications Magazine, Vol. 45, No. 2, February 2007,82 – 87.

[16] KACZMAREK S., MŁYNARCZUK M., ZIEŃKO P., *Performance Evaluation of Control Plane Functions in ASON/GMPLS Architecture*, 17th Polish Teletraffic Symposium, Zakopane, 2012, 23-28.

[17] KACZMAREK S., MŁYNARCZUK M., ZIEŃKO P., Simulation model of ASON/GMPLS architecture, Conference Papers, ICT Young, 2013, 271-279.

[18] KACZMAREK S., MŁYNARCZUK M., ZIEŃKO P., *Influence analysis of selected parameters on the ASON/GMPLS control plane performance*, paper accepted in XXIX National Symposium on Telecommunications and Computer Telecommunications, 2013, 1-6.

[19] ZANG H., JUE J. MUKHERJEE B., *A Review of Routing and Wavelength Assignment Approaches for Wave-length-Routed Optical WDM Networks*, Optical Networks Magazine, January 2000, 47-60.

*IMS, NGN, call processing performance,
phase-type distributions, traffic model*

Sylwester KACZMAREK*, Maciej SAC*

# ANALYSIS OF IMS/NGN CALL PROCESSING PERFORMANCE USING PHASE-TYPE DISTRIBUTIONS

This work is a continuation of our research on the traffic model dedicated for design and analysis of the Next Generation Network (NGN), which is standardized for distribution of current and future multimedia services based on the IP Multimedia Subsystem (IMS). Our analytical and simulation models allow evaluation of mean Call Set-up Delay $E(CSD)$ as well as mean Call Disengagement Delay $E(CDD)$ in a single domain of IMS/NGN. Ensuring proper values of these call processing performance metrics, formerly known as Grade of Service (GoS) parameters, is very important for satisfaction of users and commercial success of IMS/NGN. In this work we investigate possibilities of improving conformity of the analytical and simulation model. For this reason we perform calculations using PH/PH/1 queuing systems, in which message inter-arrival and inter-departure times are described by phase-type distributions. The obtained analytical results are compared to our previous queuing approaches (M/G/1 systems and approximations of G/G/1 based on two or three moments of arrival distribution and two moments of service distribution) and also verified by a simulation model, which precisely implements the operation (algorithms) of all network elements. As a consequence, conclusions and necessary future work with the presented traffic model are provided.

## 1. INTRODUCTION

In this work we continue our investigations regarding the previously proposed simulation [1] as well as analytical [2] model of a single domain of the Next Generation Network (NGN) [3], which is a standardized proposition of a telecommunication network architecture delivering various multimedia services with guaranteed quality based on the IP Multimedia Subsystem (IMS) [4] (hence the names “IMS-based NGN” and “IMS/NGN” are commonly used). As key elements important for successful introduction of IMS/NGN are strict Quality of Service (QoS) guarantees for users,

* Department of Teleinformation Networks, Faculty of Electronics, Telecommunications and Informatics, Gdańsk University of Technology, 11/12 Gabriela Narutowicza Street, 80-233 Gdańsk, Poland.

proper design of the network is absolutely necessary. This is the aim of our models, which allow assessment of mean Call Set-up Delay $E(CSD)$ mean Call Disengagement Delay $E(CDD)$, a set of call processing performance metrics [5,6] prior called Grade of Service (GoS) parameters.

During our research we have already applied two queuing system solutions for the analytical model (M/G/1 [2] and approximations of G/G/1 based on two or three moments of arrival distribution and two moments of service distribution [7]), however, with both of them we have observed some discrepancies between calculations and simulations. Therefore, in this work we focus on further improving the conformity of theoretical and simulation results by investigating PH/PH/1 queuing systems with arrival and service distributions represented by phase-type distributions [8-12].

The rest of the text is organized as follows. Elementary details regarding the IMS/NGN network model, assumed call scenario as well as the proposed analytical and simulation traffic models are provided in section 2. Section 3 contains information about phase-type distributions, fitting this type of distributions to arrival and service distributions in IMS/NGN and analyzing PH/PH/1 queues. The results of the performed investigations are presented and discussed in section 4. The described research is summarized in section 5, which also includes the description of necessary future work.

## 2. TRAFFIC MODEL OF IMS/NGN

The analytical and simulation traffic models used in our investigations are based on the network model (Fig. 1) and call scenario (standard voice calls are assumed) [13-17], which are in details described in [2,18] (full description is not provided due to limited space). In our research we strongly base on the current standards and research for the ITU-T NGN architecture (the most advanced of all available NGN solutions [18,19]). The elements of the network model depicted in Fig. 1 perform the following roles in the assumed call scenario [2,13-18]:

- User Equipments (UEs): terminals that generate call set-up and disengagement requests as well as register themselves in the domain for user location purposes,
- P-CSCF (Proxy – Call Session Control Function): the server, which receives all messages from UEs and forwards them to the S-CSCF element,
- S-CSCF (Serving – Call Session Control Function): the main server handling all calls,
- RACF (Resource and Admission Control Functions): the unit representing the transport stratum, responsible for allocating resources for a new call and releasing resources associated with a disengaged call.

Communication in the network is performed using SIP protocol [20], except message exchange between P-CSCF and RACF, for which Diameter protocol [21] is used.

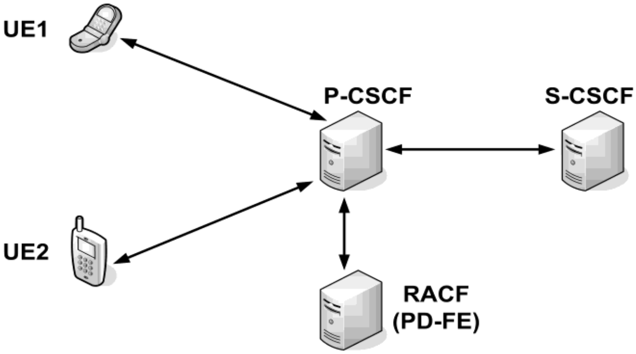


Fig. 1. Model of a single domain of IMS/NGN [2,13,14]

To aim of the traffic models used in our research is to evaluate mean Call Set-up Delay $E(CSD)$ and mean Call Disengagement Delay $E(CDD)$ [5,6]. Therefore, a set of input variables is used [1,2], the most important of which are [1,2]:

- $\lambda_{INV}$: the intensity of aggregated call set-up requests (SIP INVITE messages) generated by UE1 with exponential intervals,
- $T_{INV1}$ and $T_{INV2}$: the random variables describing times of processing SIP INVITE messages by P-CSCF and S-CSCF correspondingly,
- $a_k$ ($k = 1, 2, \ldots, 8$): the factors determining times of processing other SIP and Diameter messages by CSCF servers according to Tab. 1,
- $T_X$: the random variable describing time of processing messages by RACF,
- lengths and bandwidths of optical links, lengths of transmitted messages: values necessary to calculate communication times between network elements.

For simplification of calculations in the analytical model it is assumed that $T_{INV1}$, $T_{INV2}$ and $T_X$ input parameters are taken as constant values representing the maximum INVITE processing time by P-CSCF, the maximum INVITE processing time by S-CSCF, and the maximum message processing time by RACF respectively.

In the analytical model mean *CSD* and mean *CDD* are computed as a sum of mean values of the following component delays [2]:

- message waiting times in CSCF servers Central Processing Unit (CPU) queues, which store incoming messages when CSCF servers CPUs are busy,
- message processing times by CSCF servers CPUs and RACF (this unit does not contain a queue, it only responds with the delay defined by the $T_X$ input variable),
- message waiting times in communication queues (which precede each outgoing link and buffer messages when the link is currently busy),
- message transmission times (message lengths divided by links bandwidth),
- propagation times (5μs/km for optical links).

It is very important that, according to standards [5,6], message processing times in UEs representing many user terminals are not included in Call Set-up Delay and Call Disengagement Delay.

Table 1. Message processing times of CSCF servers

| Message | P-CSCF processing times | S-CSCF processing times |
|---|---|---|
| SIP INVITE | $T_{INV1}$ | $T_{INV2}$ |
| SIP 100 Trying | $T_{TR1} = a_1 \cdot T_{INV1}$ | $T_{TR2} = a_1 \cdot T_{INV2}$ |
| SIP 180 Ringing | $T_{RING1} = a_2 \cdot T_{INV1}$ | $T_{RING2} = a_2 \cdot T_{INV2}$ |
| SIP 200 OK (answer to INVITE) | $T_{OK1} = a_3 \cdot T_{INV1}$ | $T_{OK2} = a_3 \cdot T_{INV2}$ |
| SIP ACK | $T_{ACK1} = a_4 \cdot T_{INV1}$ | $T_{ACK2} = a_4 \cdot T_{INV2}$ |
| SIP BYE | $T_{BYE1} = a_5 \cdot T_{INV1}$ | $T_{BYE2} = a_5 \cdot T_{INV2}$ |
| SIP 200 OK (answer to BYE) | $T_{OKBYE1} = a_6 \cdot T_{INV1}$ | $T_{OKBYE2} = a_6 \cdot T_{INV2}$ |
| Diameter AAA | $T_{AAA1} = a_7 \cdot T_{INV1}$ | $T_{AAA2} = a_7 \cdot T_{INV2}$ |
| Diameter STA | $T_{STA1} = a_8 \cdot T_{INV1}$ | $T_{STA2} = a_8 \cdot T_{INV2}$ |

Comparing to the analytical model based on the analysis of theoretical queuing models, the simulator precisely implements the operation (algorithms) of all network elements as well as call set-up and disengagement scenarios. Therefore, the simulation model is much more accurate and can be regarded as a reference for evaluation of quality of the analytical results. Details regarding the implementation of the simulation model in the OMNeT++ framework [22] are out of scope of this work and can be found in [1,2].

## 3. APPLICATION OF PHASE-TYPE DISTRIBUTIONS FOR IMS/NGN

The motivation for investigating phase-type distributions [8-12] resulted from the discrepancies between call processing performance results (mean *CSD* and mean *CDD*) obtained using our analytical [2] and simulation [1] model of a single domain of IMS/NGN. Although were aware of the fact that intervals between messages at the inputs of IMS/NGN elements are generally not exponential, in our first approach [2] M/G/1 queuing systems were used to approximately describe the operation of CPU queues and communication queues in the analytical model. This solution was under many conditions acceptable but it provided poor confirmity of calculations and simulations under high load and also when IMS/NGN elements are connected using links with relatively low bandwidth. Commonly known approximations of G/G/1 systems based on two or three moments of arrival distribution and two moments of service distribution [7] used in the next step of our research did not improve the situation. This lead us to examination of PH/PH/1 queuing systems with arrival and service distributions described by phase-type distributions.

The term “phase-type distributions” refers to the set of probability distributions that result from a system of one or more inter-related Poisson processes occurring in sequence, or phases. Special cases of continuous phase-type distributions are [8-12,23]:

- degenerate distribution (point mass at zero or the empty phase-type distribution) - 0 phases,
- exponential distribution - 1 phase,
- Erlang distribution - 2 or more identical phases in sequence,
- deterministic distribution (or constant) - the limiting case of an Erlang distribution, as the number of phases becomes infinite, while the time in each state becomes zero,
- Coxian distribution - 2 or more phases in sequence with a probability of reaching the terminating state after each phase,
- Hyperexponential distribution (also called a mixture of exponential) - 2 or more non-identical parallel phases, each of which has its own probability of occurring,
- Hypoexponential distribution - 2 or more (not necessarily identical) phases in sequence, a generalization of an Erlang distribution (in which phases are identical).

A very important feature of the set of phase-type distributions is that it is dense in the field of all positive-valued distributions [8-12,23]. Therefore, phase-type distributions can represent or approximate (with any accuracy) any positive valued distribution. Several algorithms for fitting different subsets of phase-type distributions to experimental data with respect to specified number of first moments [8-12,23] or whole experimental histograms [12,24-26] have been proposed. Here we focus only on moment-based algorithms.

Results of our initial research on fitting phase-type distributions to message inter-avviral and inter-departure time distributions in a single domain of IMS/NGN are described in [27]. In this work we extended the set of moment-based fitting algorithms, applied them all to arrival as well as service distributions of all elements and obtained final results ($E(CSD)$ and $E(CDD)$) using PH/PH/1 queuing systems. The set of fitting algorithms investigated in this work include:

- APH1 [8,28] (“PH fit 1” from [27]) – fitting acyclic Erlang-Coxian phase-type distributions with respect to 3 moments of experimental data,
- APH2 [9,29] (“PH fit 2” from [27]) – fitting minimal order acyclic phase-type distributions with respect to 3 moments of experimental data,
- ME [10,11,29] (“PH fit 3” from [27]) – fitting matrix exponential (ME, [30]) distributions with respect to any number of moments of experimental data; in our research we consider two cases: 3÷4 moments (resultant distributions are the same for 3 and 4 moments) as well as 5 moments; the set of ME distributions is the superset of the set of phase-type distributions; when a fitted

distribution for particular input variables and network element is not a phase-type distribution, analysis of a queue with such a distribution can lead to undefined or unrepresentable value of mean waiting time (NaN – not a number) – in such case mean waiting time values obtained for the APH1 algorithm are used,

- PH1 [31,32] – an algorithm which fits several phase-type distributions of different order to a specified range of moments; phase-type distributions are chosen randomly and at the end the distribution which moments are the nearest the given ones is chosen; the algorithm produces different results every run and in many cases leads to very poor fitting; therefore, the results for this algorithm are not presented,
- PH2 – fitting order 2 (for 3 moments; [29,33]) or order 3 (for 5 moments [29,34]) canonical representation of phase-type distributions to experimental data; the algorithm works only when the given moments satisfy certain conditions; otherwise, for particular input variables and network elements distributions obtained for the APH1 algorithm are used.

In order to apply PH/PH/1 queuing systems in calculations, arrival and service distributions for each set of input variables and for all network elements have to be represented by phase-type distributions. For this reason up to five first moments of all arrival and service distributions are necessary. Since times of processing individual messages by network elements are known from the input variables (for links they are determined by message lengths and link bandwidths) and the set of messages handled by each element results from the assumed call scenario, we have a full description of all service distributions.

For arrival distributions the situation is more complicated as only message intensity is known from the call scenario and $\lambda_{INV}$ (message intensity is the inverse of mean interval between messages – the first moment). To obtain moments higher than the first, times of messages arriving at inputs of all CPU and communication queues were recorded using the simulation model [27,35] and further processed in the MATLAB [36] environment.

After fitting phase-type distributions to all arrival and service distributions, the next step is to calculate mean waiting time for all queues in the IMS/NGN domain. Analysis of PH/PH/1 queues can be done by solving quasi-birth-and-death (QBD) Markov chains using matrix-analytic mathods [37,38]. Several solvers have already been proposed, from which we tested two designed for the MATLAB environment [39,40]. Both of the tested solvers provide very similar results of mean waiting time. The first solver [39] is much slower but allows calculation of queue length distribution for PH/PH/1 queues, which is, however, unnecessary in our analytical model (further calculations are necessary to obtain mean waiting time). Therefore, in our work we used mainly the second solver [40], which computes mean waiting time fast and directly.

The results of our investigations are presented in the next section. Apart from fitting phase-type distributions to both arrival and service distributions of all elements (PH/PH/1 queuing models), we also assumed that either arrival or service distrubitions are exponential distributions (special cases of phase-type distributions), which resulted in M/PH/1 and PH/M/1 models correspondingly.

## 4. RESULTS

To compare the obtained results with our previous approaches to calculate $E(CSD)$ and $E(CDD)$) [2,7], we used the same data sets, which are presented in Tab. 2. Additionally, the same message lengths presented in Tab. 3 were assumed along with the identical values of the $a_k$ factors (Tab. 1): $a_1 = 0.2$, $a_2 = 0.2$, $a_3 = 0.6$, $a_4 = 0.3$, $a_5 = 0.6$, $a_6 = 0.3$, $a_7 = 0.6$, $a_8 = 0.6$.

Table 2. Input data sets

| Data set | $\lambda_{INV}$ [1/s] | $T_{INV1}$ [ms] | $T_{INV2}$ [ms] | $T_X$ [ms] | Links |
|---|---|---|---|---|---|
| 1a | 5÷250 | 0.5 | 0.5 | 3 | no links |
| 1b | 5÷250 | 0.5 | 0.5 | 3 | 300 km, 10 Mb/s |
| 1c | 5÷250 | 0.5 | 0.5 | 3 | 300 km, 100 Mb/s |

Table 3. Message lengths [41]

| Message | Length in bytes |
|---|---|
| SIP INVITE | 930 |
| SIP 100 Trying | 450 |
| SIP 180 Ringing | 450 |
| SIP 200 OK (answer to INVITE) | 990 |
| SIP ACK | 630 |
| SIP BYE | 510 |
| SIP 200 OK (answer to BYE) | 500 |
| Diameter messages | 750 |

As mentioned in the previous section, to fit phase-type distributions to arrival distributions and perform further calculations of mean waiting time, for each set of input variables and for all network elements second, third, fourth and fifth moment of message inter-arrival time had to be computed based on the simulation data. In our experiments simulations were performed using the following assumptions:

- warm-up period: 1500 s,
- 5 measurement periods,
- 0.95 confidence level,
- simulation is finished when confidence intervals for $E(CSD)$ and $E(CDD)$ do not exceed 5% of mean Call Set-up Delay and mean Call Disengagement Delay

or when total simulation time exceeds 10000 s; with such stop conditions at least 10000 message inter-arrival times were obtained during each simulation.

*E*(*CSD*) and *E*(*CDD*) values obtained for the previously described sets of parameters and assumptions are depicted in Fig. 2-4. Each of these figures includes four subfigures. The aim of each two subfigures at the top is to provide comparison of mean *CSD* results simulated and calculated using the analytical model for M/G/1 and different variants of PH/PH/1, PH/M/1 as well as M/PH/1 queuing systems. Subfigures at the bottom are analogical, but they concern mean *CDD*. In legends for all subfigures we listed types of the queuing systems followed by the algorithms for fitting phase-type distributions. The information in brackets represtents the numbers of moments fitted (more details is provided section 3).

Additionally to Fig. 2-4, we provide a mathematical way of evaluation of confirmity between calculations and simulations for all queuing approaches applied in the analytical model. For this reason the root-mean-square error (RMSE) is used, which is defined as follows:

$$\mathrm{RSME} = \sqrt{\underset{\lambda_{INV} \in \Lambda}{E}\left(Y_{\mathrm{simulation}} - Y_{\mathrm{analytical}}\right)^2} \tag{1}$$

where $Y$ is either $E(CSD)$ or $E(CDD)$ and $E()$ is the averaging operator over a particular set of call set-up request intensities $\lambda_{INV} \in \Lambda$. In this work the following sets of $\lambda_{INV}$ are considered to fully examine all queuing system solutions:

- "green" – IMS/NGN elements are low loaded and *E*(*CSD*), *E*(*CDD*) change very little with call set-up request intensity ($\lambda_{INV}$ = 20, 60, 100),
- "yellow" – IMS/NGN elements are quite highly loaded and *E*(*CSD*), *E*(*CDD*) start noticeably increasing with call set-up request intensity ($\lambda_{INV}$ = 130, 160, 190),
- "red" – IMS/NGN elements are overloaded and *E*(*CSD*), *E*(*CDD*) start going to infinity ($\lambda_{INV}$ = 205, 220, 225),
- "gr-yel" – the set including all call set-up request intensities from the "green" set and almost all call set-up request intensities from the yellow set ($\lambda_{INV}$ = 20, 60, 100, 130, 160),
- "all" – the set containing all call set-up request intensities from the "green", "yellow" and "red" sets ($\lambda_{INV}$ = 20, 60, 100, 130, 160, 190, 205, 220, 225).

All obtained RMSE values for the mentioned above $\lambda_{INV}$ sets are presented in Tab. 4-6. For all analyzed cases we marked two best (the smallest RMSE values, bold and underlined font) and two worst (the highest RMSE values, bold and italic font with gray background) results. When two queuing systems variants offer the same best or worst RMSE, the consecutive result is also marked on condition that it does not significantly differ from the previous ones.

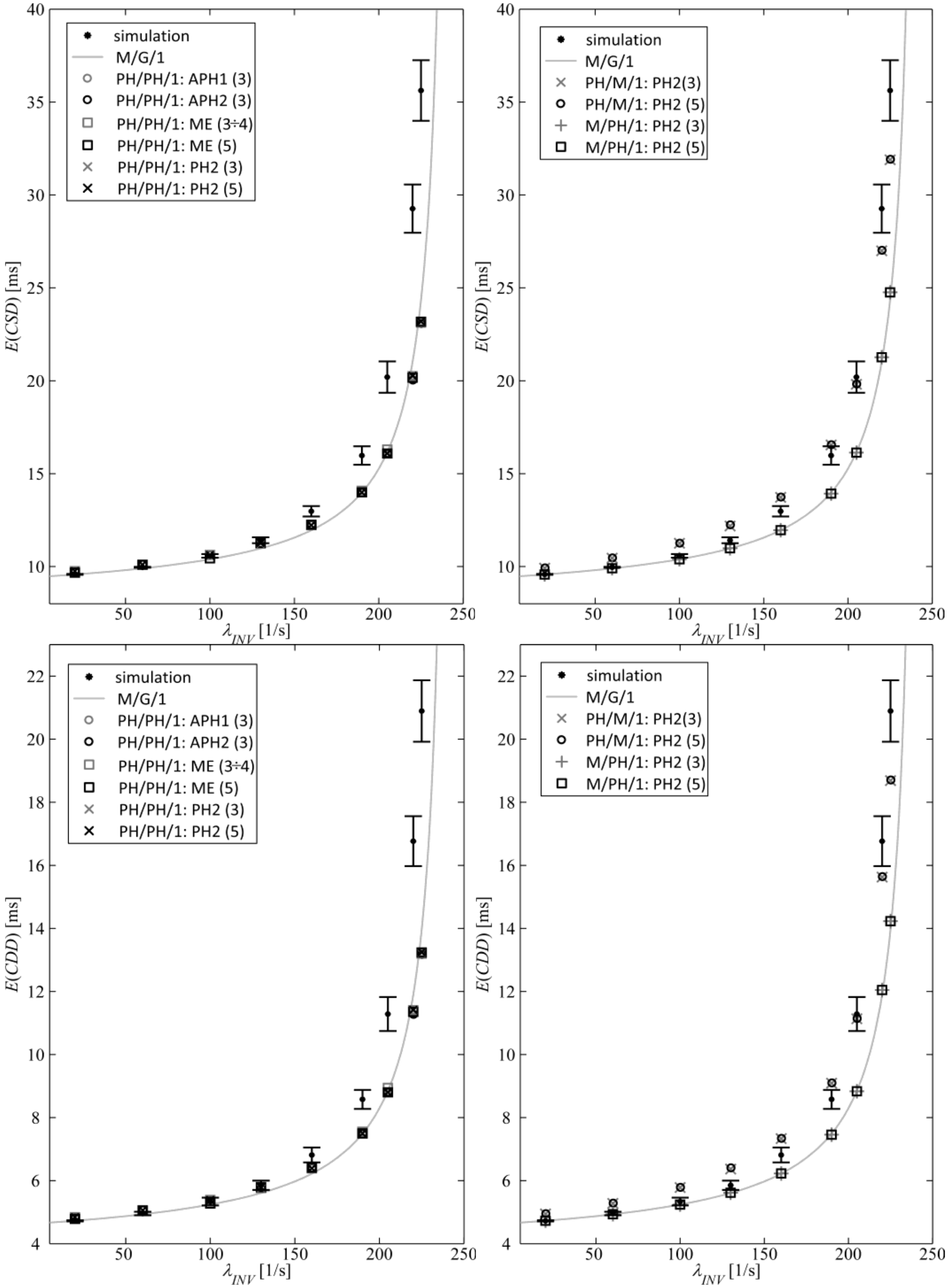


Fig. 2. Results for data set 1a

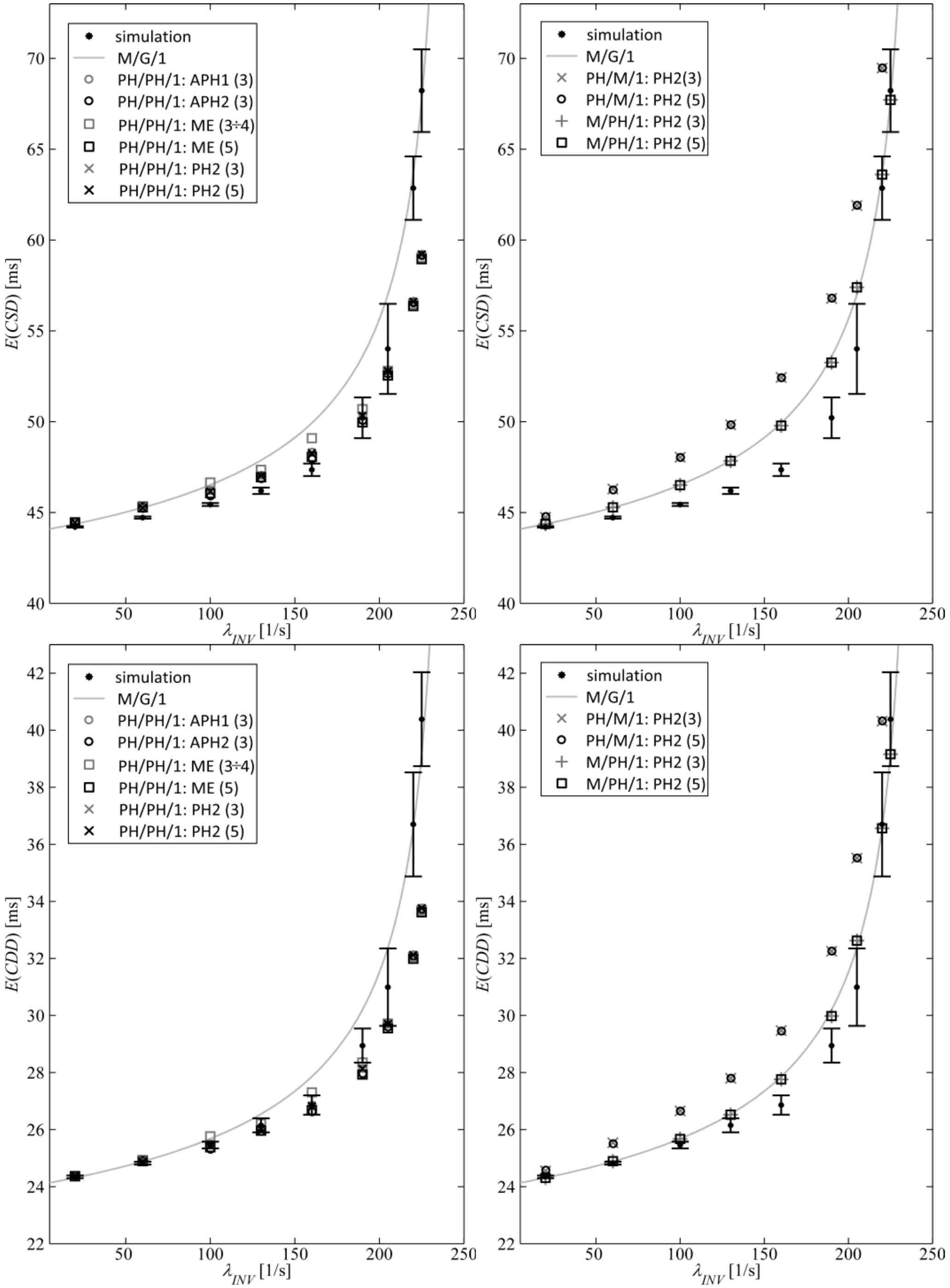


Fig. 3. Results for data set 1b

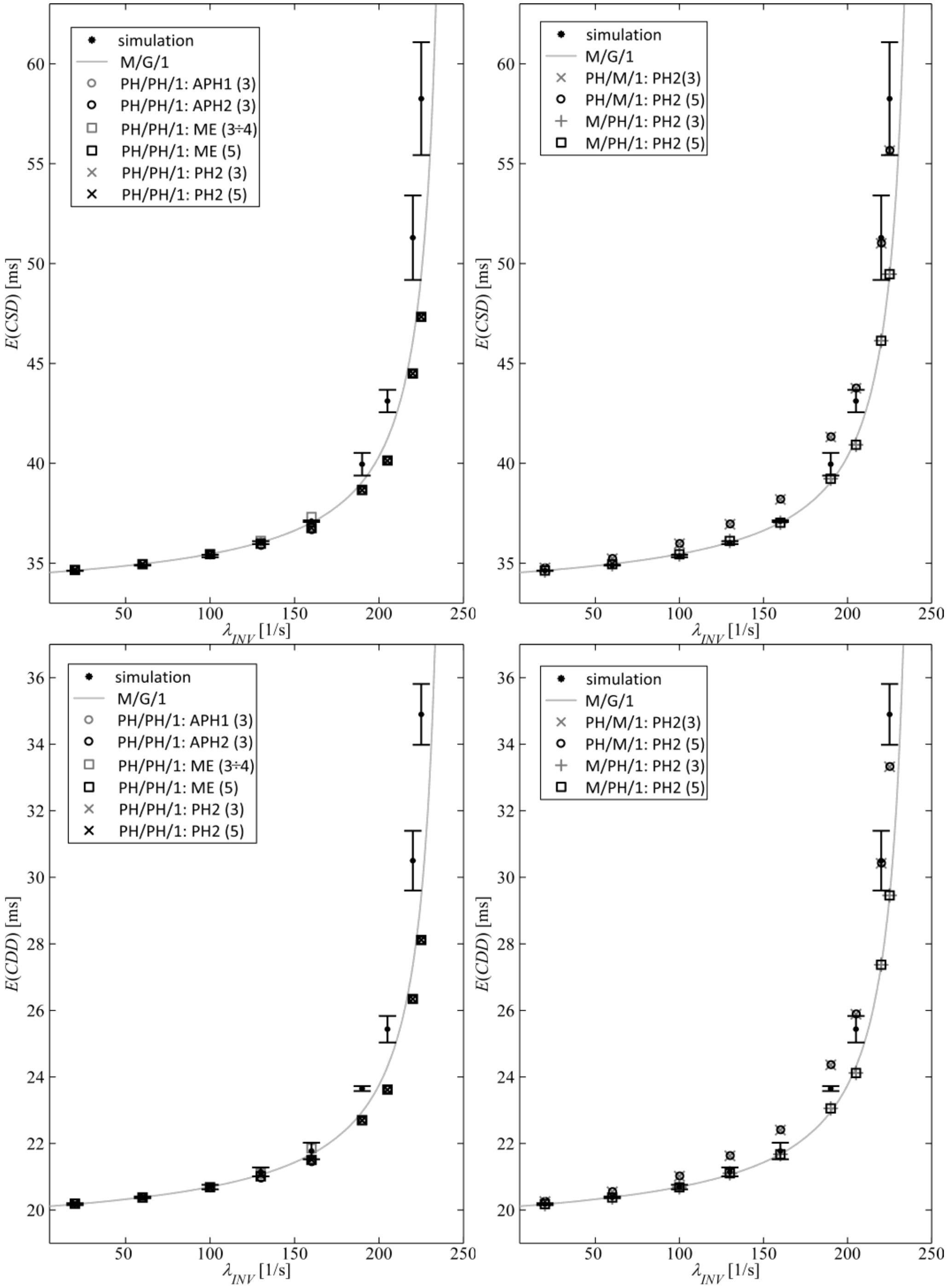


Fig. 4. Results for data set 1c

Table 4. RMSE for data set 1a

| | RMSE for *E*(*CSD*), [ms] | | | | | RMSE for *E*(*CDD*), [ms] | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | green | yellow | red | gr-yel | all | green | yellow | red | gr-yel | all |
| M/G/1 | **0.110** | ***1.317*** | 8.399 | 0.506 | 4.909 | **0.056** | ***0.728*** | 5.090 | 0.290 | 2.969 |
| PH/PH/1: APH1 (3) | 0.131 | 1.228 | 9.186 | 0.362 | 5.351 | 0.093 | 0.673 | 5.587 | 0.206 | 3.249 |
| PH/PH/1: APH2 (3) | 0.131 | 1.242 | ***9.315*** | 0.362 | ***5.426*** | 0.093 | 0.682 | ***5.667*** | 0.206 | ***3.296*** |
| PH/PH/1: ME (3÷4) | 0.131 | 1.181 | 9.176 | 0.362 | 5.342 | 0.093 | 0.642 | 5.580 | 0.206 | 3.243 |
| PH/PH/1: ME (5) | 0.121 | 1.220 | ***9.209*** | **0.343** | ***5.364*** | 0.077 | 0.668 | ***5.601*** | **0.192** | ***3.257*** |
| PH/PH/1: PH2 (3) | 0.131 | 1.228 | 9.186 | 0.362 | 5.351 | 0.093 | 0.673 | 5.586 | 0.206 | 3.249 |
| PH/PH/1: PH2 (5) | 0.131 | 1.226 | 9.173 | **0.357** | 5.344 | 0.092 | 0.672 | 5.578 | **0.204** | 3.244 |
| PH/M/1: PH2 (3) | ***0.522*** | **0.700** | **2.529** | ***0.627*** | **1.545** | ***0.341*** | **0.515** | **1.437** | ***0.420*** | **0.903** |
| PH/M/1: PH2 (5) | ***0.519*** | **0.719** | **2.519** | ***0.638*** | **1.542** | ***0.340*** | **0.526** | **1.431** | ***0.427*** | **0.902** |
| M/PH/1: PH2 (3) | **0.111** | ***1.343*** | 8.135 | 0.501 | 4.761 | **0.057** | ***0.743*** | 4.924 | 0.287 | 2.875 |
| M/PH/1: PH2 (5) | **0.111** | ***1.343*** | 8.135 | 0.501 | 4.761 | **0.057** | ***0.743*** | 4.924 | 0.287 | 2.875 |

Table 5. RMSE for data set 1b

| | RMSE for *E*(*CSD*), [ms] | | | | | RMSE for *E*(*CDD*), [ms] | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | green | yellow | red | gr-yel | all | green | yellow | red | gr-yel | all |
| M/G/1 | 0.705 | 2.637 | **1.805** | 1.477 | **1.889** | 0.133 | 0.954 | **1.059** | 0.489 | **0.826** |
| PH/PH/1: APH1 (3) | 0.567 | 0.736 | 6.375 | 0.718 | 3.719 | **0.060** | **0.474** | 4.711 | **0.071** | 2.734 |
| PH/PH/1: APH2 (3) | **0.405** | **0.515** | 6.443 | **0.502** | 3.739 | 0.094 | 0.606 | ***4.763*** | 0.167 | ***2.772*** |
| PH/PH/1: ME (3÷4) | 0.797 | 1.237 | 6.490 | 1.120 | 3.842 | 0.189 | **0.428** | 4.758 | 0.247 | 2.760 |
| PH/PH/1: ME (5) | **0.500** | **0.613** | ***6.591*** | **0.602** | 3.832 | 0.062 | 0.605 | ***4.834*** | 0.126 | ***2.813*** |
| PH/PH/1: PH2 (3) | 0.567 | 0.736 | 6.374 | 0.718 | 3.719 | **0.060** | **0.474** | 4.711 | **0.071** | 2.734 |
| PH/PH/1: PH2 (5) | 0.533 | 0.715 | 6.370 | 0.689 | 3.713 | **0.038** | 0.475 | 4.707 | **0.069** | 2.732 |
| PH/M/1: PH2 (3) | ***1.781*** | ***5.234*** | ***6.930*** | ***3.116*** | ***5.118*** | ***0.813*** | ***2.612*** | 3.778 | ***1.517*** | 2.693 |
| PH/M/1: PH2 (5) | ***1.751*** | ***5.222*** | ***6.930*** | ***3.093*** | ***5.110*** | ***0.793*** | ***2.599*** | 3.777 | ***1.500*** | 2.687 |
| M/PH/1: PH2 (3) | 0.703 | 2.438 | **2.025** | 1.420 | **1.874** | 0.130 | 0.822 | **1.181** | 0.448 | **0.834** |
| M/PH/1: PH2 (5) | 0.703 | 2.438 | **2.025** | 1.420 | **1.874** | 0.130 | 0.822 | **1.181** | 0.448 | **0.834** |

Based on Fig. 2-4 and Tab. 4-6 it can be observed that conformity of analytical and simulation results is dependent on many factors, including the variant of the queuing systems used in the calculations. Very important is also the offered load to CSCF servers CPUs (resulting from $\lambda_{INV}$ and the set of handled messages) as well as to communication queues (direct communication without links and communication queues – data set 1a; low link bandwidth, high load – data set 1b; high link bandwidth, low load – data set 1c).

Comparing the results for particular data sets (Fig. 2-4, Tab. 2) it can be noticed that relations between simulations and calculations are similar for *E*(*CSD*) and *E*(*CDD*). Nevertheless, mean *CSD* values are always higher than mean *CDD* because of more elements (and messages) taking part in call set-up comparing to call disengagement [1,2].

Table 6. RMSE for data set 1c

| | RMSE for *E*(*CSD*), [ms] | | | | | RMSE for *E*(*CDD*), [ms] | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | green | yellow | red | gr-yel | all | green | yellow | red | gr-yel | all |
| M/G/1 | 0.069 | **0.518** | 6.014 | **0.064** | 3.485 | **0.003** | **0.410** | 3.701 | 0.058 | 2.150 |
| PH/PH/1:<br>APH1 (3) | 0.067 | 0.783 | ***7.633*** | 0.161 | ***4.430*** | 0.012 | 0.579 | ***4.715*** | 0.125 | ***2.743*** |
| PH/PH/1:<br>APH2 (3) | **0.051** | 0.815 | ***7.648*** | 0.213 | ***4.441*** | 0.024 | 0.606 | ***4.724*** | 0.172 | ***2.750*** |
| PH/PH/1:<br>ME (3÷4) | 0.070 | 0.746 | 7.621 | 0.114 | 4.421 | 0.011 | 0.545 | 4.710 | **0.041** | 2.737 |
| PH/PH/1: ME (5) | 0.063 | 0.777 | 7.627 | 0.165 | 4.426 | 0.009 | 0.579 | 4.711 | 0.135 | 2.740 |
| PH/PH/1: PH2 (3) | 0.067 | 0.783 | 7.627 | 0.161 | 4.427 | 0.012 | 0.579 | 4.711 | 0.125 | 2.740 |
| PH/PH/1: PH2 (5) | 0.067 | 0.778 | 7.627 | 0.161 | 4.427 | 0.012 | 0.576 | 4.711 | 0.125 | 2.740 |
| PH/M/1: PH2 (3) | ***0.409*** | ***1.138*** | **1.556** | ***0.712*** | **1.138** | ***0.216*** | ***0.616*** | **0.947** | ***0.392*** | **0.664** |
| PH/M/1: PH2 (5) | ***0.409*** | ***1.137*** | **1.556** | ***0.712*** | **1.137** | ***0.216*** | ***0.615*** | **0.947** | ***0.392*** | **0.664** |
| M/PH/1: PH2 (3) | **0.058** | **0.426** | 6.018 | **0.070** | 3.484 | **0.005** | **0.350** | 3.703 | **0.049** | 2.147 |
| M/PH/1: PH2 (5) | **0.058** | **0.426** | 6.018 | **0.070** | 3.484 | **0.005** | **0.350** | 3.703 | **0.049** | 2.147 |

During our research we found out that using M/G/1 (based on two moments of service distribution) and M/PH/1 (where from three to five moments of service distribition can be fitted) queuing systems leads to very similar results (Fig. 2-4, Tab. 4-6). Moreover, based on the obtained results we cannot say that any of these queuing solutions is better than the other. These properties are fulfilled irrespectively of the algorithm used for fitting phase-type distributions to service distributions for M/PH/1 and the number of fitted moments. As the results for M/G/1 and M/PH/1 queuing systems are comparable but M/PH/1 system is more complicated in analysis (section 3), a better choice for IMS/NGN analytical traffic model is M/G/1.

In the case of PH/PH/1 and PH/M/1 queuing systems the algorithms used for fitting phase-type distributions in majority of situations also do not have a significant impact on the results (Fig. 2-4, Tab. 4-6). The only exception is the ME algorithm providing matrix exponential distributions, which only in a part of all cases are phase-type distributions. When a resultant distribution is not a phase-type distribution the obtained *E*(*CSD*) and *E*(*CDD*) values may differ from these for other queuing systems variants (section 3). Taking all these facts into account, in the next part of this work we do not distinguish particular algorithms for fitting phase-type distributions and consider the whole families of PH/PH/1 and PH/M/1 queuing systems.

When it is assumed that all network elements are directly connected to each other (without links – data set 1a, Tab. 2) and call set-up request intensity is low (the "green" $\lambda_{INV}$ set), the best results are provided by M/G/1 queuing systems (Fig. 2, Tab. 4). Only slightly worse are PH/PH/1 queuing systems, which, hovewer, are the most efficient when we take into account quite larger „gr-yel" set. For small $\lambda_{INV}$ values the worst queuing system is PH/M/1, which overestimates $E(CSD)$ and $E(CDD)$. This queuing solution is, however, the most effective for high (the "red" set) and the whole range (the "all" set) of call set-up request intensities. As a result, for data set 1a we propose to use PH/PH/1 queuing systems in the analytical model of IMS/NGN for the „gr-yel" set of call set-up request intensities and PH/M/1 queuing systems for other $\lambda_{INV}$ values. Such a combination of queuing solutions gives the results closest to simulations.

Comparing to data set 1a, a similar situation occurs for data set 1c (links with high bandwidth of 100 Mb/s). For the "green" and "yellow" sets the best queuing system solution is M/G/1, which is better than PH/PH/1 giving slightly worse results (Fig. 4, Tab. 6). Analogically to data set 1a, when considering the "red" and "all" sets we can achieve the smallest RMSE values using PH/M/1 queuing systems. Consequently, we propose to choose M/G/1 or PH/PH/1 queuing systems for the „gr-yel" set and PH/M/1 queuing systems for other $\lambda_{INV}$ values.

When IMS/NGN elements are connected using links with relatively low bandwidth (10 Mb/s, data set 1b) the best analytical results for low and medium call set-up request intensities (the "green" and "yellow" sets) are provided by PH/PH/1 systems (Fig. 3, Tab. 5). M/G/1 queues are only slightly worse than PH/PH/1 for the "green" set, however, for the "yellow" set they overestimate mean *CSD* and mean *CDD*. Nevertheless, when it comes to high $\lambda_{INV}$ values (the "red" set) and the whole set of $\lambda_{INV}$ (the "all" set) M/G/1 queuing solutions are the most advantageous. In the case of data set 1b PH/M/1 systems are not appropriate as they result in very high RMSE values. As a consequence, for the "green" and "yellow" sets PH/PH/1 queuing systems are advisable, while for the "red" set it is best to use M/G/1 queuing systems.

## 5. CONCLUSIONS AND FUTURE WORK

The described work is a continuation of our research on improving the conformity of analytical call processing performance results (mean Call Set-up Delay and mean Call Disengagement Delay) in a single domain of IMS/NGN with simulation results. For this reason different queuing solutions representing CSCF servers CPU queues as well as communication queues in the analytical model are tested. In the first part of our research we examined M/G/1 queuing systems and approximations of G/G/1 based on two or three moments of arrival distribution and two moments of service distribution [7]. In this work phase-type distributions are fitted to arrival and service distributions of all IMS/NGN elements based on from three to five moments and PH/PH/1, PH/M/1, M/PH/1 queuing systems are investigated.

The obtained results indicate that phase-type distributions applied in the analytical model of IMS/NGN can improve its conformity with simulations. From tested queuing systems with phase-type distributions the most useful are PH/PH/1 and PH/M/1, which for selected sets of call set-up request intensities offer results comparable or better than M/G/1 and always better than the above mentioned moment-based approximations of G/G/1 [7].

The performed research also allowed selection of the best queuing system for the analytical model of a single domain of IMS/NGN, which depends on links bandwidths and call set-up request intensity (divided during our investigations into several sets). For the “gr-yel” set PH/PH/1 queuing systems are always the best or only slightly worse than M/G/1 (irrespectively of links parameters), while for higher call set-up request intensities the situation is dependent on the parameters of links. When IMS/NGN elements are connected directly without links or using links with relatively high bandwidth, the closest to simulations for the “red” call set-up request intensity set are results provided by PH/M/1 queuing systems. On the other hand, when links with rather low bandwidth are used, the most efficient for the highest $\lambda_{INV}$ values are simple M/G/1 queues.

Although the obtained theoretical results are very close to simulations, we are going to continue our work on determining proper queuing models for CSCF servers CPUs and optical links. Our next aim is to investigate phase-type distributions fitted to the whole arrival and service distributions [12,24-26], not only to their several moments. Apart from that, we are planning to develop our traffic model in order to carry out research in a multi-domain IMS/NGN architecture, including also the elements specific for MPLS, Ethernet and FSA transport technologies [42-44].

## ACKNOWLEDGEMENTS

This research work was partially supported by the system project “InnoDoktorant – Scholarships for PhD students, V$^{th}$ edition” co-financed by the European Union in the frame of the European Social Fund.

## REFERENCES

[1] KACZMAREK S., KASZUBA M., SAC M., *Simulation model of IMS/NGN call processing performance*, Gdańsk University of Technology Faculty of ETI Annals, Vol. 20, 2012, 25-36.

[2] KACZMAREK S., SAC M., *Traffic Model for Evaluation of Call Processing Performance Parameters in IMS-based NGN*, In: Information Systems Architecture and Technology: Networks Design and Analysis, Grzech A., et al. (Eds.), Wrocław, Oficyna Wydawnicza Politechniki Wrocławskiej, 2012, 85-100.

[3] *General overview of NGN*, ITU-T Recommendation Y.2001, December 2004.

[4] *IP Multimedia Subsystem (IMS); Stage 2 (Release 11)*, 3GPP TS 23.228 v11.0.0, March 2011.

[5] *Call processing performance for voice service in hybrid IP networks*, ITU-T Recommendation Y.1530, November 2007.

[6] *SIP-based call processing performance*, ITU-T Recommendation Y.1531, November 2007.

[7] KACZMAREK S., SAC M., *Analysis of IMS/NGN call processing performance using G/G/1 queuing systems approximations*, accepted for publication in Telecommunication Review and Telecommunication News (Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne), 2013.

[8] OSOGAMI T., HARCHOL-BALTER M., *Closed form solutions for mapping general distributions to quasi-minimal PH distributions*, Performance Evaluation, Vol. 63, Iss. 6, 2006, 524-55.

[9] BOBBIO A., HORVATH A., TELEK M., *Matching three moments with minimal acyclic phase type distributions*, Stochastic models, Vol. 21, Iss. 2-3, 2005, 303-326.

[10] TELEK M., HORVATH G., *A minimal representation of Markov arrival processes and a moments matching method*, Performance Evaluation, Vol. 64, Iss. 9-12, 2007, 1153–1168.

[11] VAN DE LIEFVOORT A., *The moment problem for continuous distributions*, Technical report WP-CM-1990-02, University of Missouri, Kansas City, USA, 1990.

[12] ASMUSSEN S., NERMAN O., OLSSON M., *Fitting Phase-Type Distributions via the EM Algorithm*, Scandinavian Journal of Statistics, Vol. 23, No. 4, 1996, 419-441.

[13] *Functional requirements and architecture of next generation networks*, ITU-T Recommendation Y.2012, April 2010.

[14] *IMS for next generation networks*, ITU-T Recommendation Y.2021, September 2006.

[15] *Resource and admission control functions in next generation networks*, ITU-T Recommendation Y.2111, November 2008.

[16] *Resource control protocol no. 1, version 2 – Protocol at the Rs interface between service control entities and the policy decision physical entity*, ITU-T Recommendation Q.3301.1, June 2010.

[17] PIRHADI M., SAFAVI HEMAMI S. M., KHADEMZADEH A., *Resource and admission control architecture and QoS signaling scenarios in next generation networks*, World Applied Sciences Journal 7 (Special Issue of Computer & IT), 2009, 87-97.

[18] KACZMAREK S., SAC M., *Traffic engineering aspects in IMS-based NGN networks* (*Zagadnienia inżynierii ruchu w sieciach NGN bazujących na IMS*), In: Teleinformatics library, vol. 6. Internet 2011 (Biblioteka teleinformatyczna, t. 6. Internet 2011), Bem D. J, et al. (Eds.), Wrocław, Oficyna Wydawnicza Politechniki Wrocławskiej, 2012, 63-115 (in Polish).

[19] KACZMAREK S., SAC M., *Traffic modeling in IMS-based NGN networks*, Gdańsk University of Technology Faculty of ETI Annals, Vol. 1, No. 9, 2011, 457-464.

[20] ROSENBERG J., et al., *SIP: Session Initiation Protocol*, IETF RFC 3261, June 2002.

[21] CALHOUN P., et al., *Diameter Base Protocol*, IETF RFC 3588, September 2003.

[22] *OMNeT++ Network Simulation Framework*, www.omnetpp.org.

[23] CZACHÓRSKI T., *Queuing models in evaluation of effectiveness of computer networks and systems* (*Modele kolejkowe w ocenie efektywności sieci i systemów komputerowych*), Gliwice, Pracownia Komputerowa Jacka Skalmierskiego, 1999 (in Polish).

[24] THÜMMLER A., BUCHHOLZ P., TELEK M., *A Novel Approach for Phase-Type Fitting with the EM Algorithm*, IEEE Transactions on Dependable and Secure Computing, Iss. 3, 2006, 245–258.

[25] WANG J., LIU J., SHE. C., *Segment-based adaptive hyper-erlang model forlong-tailed network traffic approximation*, The Journal of Supercomputing, Vol. 45, Iss. 3, 2008, 296–312.

[26] HORVATH A., TELEK M., *PhFit: A General Phase-Type Fitting Tool.*, In: Proc. 12th International Conference on Computer Performance Evaluation, Modelling Techniques and Tools, TOOLS ’02, London, United Kingdom, 2002, 82–91.

[27] KACZMAREK S., SAC M., *Approximation of Message Inter-Arrival and Inter-Departure Time Distributions in IMS/NGN Architecture Using Phase-Type Distributions*, paper submitted to Journal of Telecommunications and Information Technology, 2013.

[28] *Moment Matching Algorithms*, www.cs.cmu.edu/~osogami/code/momentmatching/index.html.

[29] *BuTools Program Packages*, webspn.hit.bme.hu/~telek/tools/butools/butools.html.

[30] KUMARAN J., MITCHELL K., VAN DE LIEFVOORT A., *Characterization of the departure process from an ME/ME/1 queue*, RAIRO Operations Research, Vol. 38, 2004, 173–191.

[31] CASALE G., ZHANG E. Z., SMIRNI E., *KPC-Toolbox: Simple Yet Effective Trace Fitting Using Markovian Arrival Processes*, In: Proc. 5th International Conference on the Quantitative Evaluation of SysTems, QEST 2008, St. Malo, France, 2008, 83–92.

[32] *KPC Toolbox*, www.cs.wm.edu/MAPQN/kpctoolbox.html.

[33] TELEK M., HEINDL A., *Matching moments for acyclic discrete and continuous phase-type distributions of second order*, International Journal of Simulation Systems, Science & Technology, Vol. 3, No. 3-4, 2002, 47–57.

[34] HORVATH G., TELEK M., *On the canonical representation of phase type distributions*, Performance Evaluation, Vol. 66, No. 8, 2009, 396–409.

[35] KACZMAREK S., SAC M., *Message Inter-Arrival and Inter-Departure Time Distributions in IMS/NGN Architecture*, In: Proc. 17th Polish Teletraffic Symposium, PTS 2012, Zakopane, Poland, 2012, 37-43.

[36] *MATLAB - The Language of Technical Computing*, www.mathworks.com/products/matlab.

[37] PÉREZ J. F., VAN VELTHOVEN J., VAN HOUDT B., *Q-MAM: A Tool for Solving Infinite Queues using Matrix-Analytic Methods*, In: Proc. SMCTools 2008, Athens, Greece, 2008.

[38] GROSS D., SHORTLE J., THOMPSON J., HARRIS C., *Fundamentals of Queueing Theory*, 4th edition, Wiley, 2008.

[39] *PATS: Performance Analysis of Telecommunication Systems*, win.ua.ac.be/~vanhoudt/.

[40] *TELCOM 2825 Information Systems and Network Infrastructure Protection*, www.sis.pitt.edu/~dtipper/2130_notes.html.

[41] ABHAYAWARDHANA V. S., BABBAGE R., *A traffic model for the IP Multimedia Subsystem (IMS)*, In: Proc. IEEE 65th Vehicular Technology Conference, VTC2007-Spring, Dublin, Ireland, 2007.

[42] *Centralized RACF architecture for MPLS core networks*, ITU-T Recommendation Y.2175, November 2008.

[43] *Ethernet QoS control for next generation networks*, ITU-T Recommendation Y.2113, January 2009.

[44] *Requirements for the support of flow state aware transport technology in an NGN*, ITU-T Recommendation Y.2121, January 2008.

*switching fabric, scheduling algorithm,distribution traffic model*

Marcin DZIUBA*

# PERFORMANCE EVALUATION OF THE SSMPS AND MSMPS ALGORITHMS FOR VOQ SWITCHES UNDER DIFFERENT DISTRIBUTION TRAFFIC MODELS

In this paper performance evaluation of the Single Size Matching with Permanent Selection (SSMPS) [1] and Maximal Size Matching with Permanent Selection (MSMPS) algorithms [2] are presented. First and full description of the algorithms was discussed earlier in [1][2]. In this article, computer simulation results under non-uniformly, diagonally and lin-diagonally distributed traffic models are shown and discussed. Because the number of pages limit, the results were performed only for 16×16 and 32x32 switch sizes. Presented results for SSMPS and MSMPS algorithms are compared with other algorithms well known from the literature. It is shown that presented algorithms achieve similar performance results like another algorithms, but presented algorithms do not need any additional calculations. This fact cause that our algorithms can be easily implemented in hardware.

## 1. INTRODUCTION

Several well known architectures for packet switches are presented in the literatures [3]. These architectures provide fast configuration connection pattern between inputs and outputs and they are no-blocking during packet sending [3]. But not all packets can be send in one unit of time. In order to solve problem with directing packets to the same output (in the same time unit), a few types of packet buffers are proposed. Buffer module is one of the most important part of the switch architecture. According to the location of the buffers, they can be divided at three basic types: inputs buffers, output buffers and buffers which are placed inside switching fabric [4]. In the same time, three basic types of switching fabric can be presented: switching fabric

* Chair of Communication and Computer Networks, Poznan University of Technology, ul. Polanka 3, 60-965 Poznan, POLAND

with Input Queues (IQ), switching fabric with Output Queued (OQ)and switching fabric with different combinations of IQ and OQ.

As previously mentioned, switching fabric buffer module is very important module in switch architecture. In this article, switching fabric with VOQ (Virtual Output Queue) system [5][6] is presented. VOQ buffering system, in presented architecture are placed at the inputs of switching fabric. VOQ has been proposed to solve a HOL (Head of Line) effect [3]. In this kind of buffering system (VOQ), each switching fabric input has a separate queue for a packet directed to particular output of a switching fabric. Using switching fabric with VOQ, there is possibility to achieve 100% throughput. Using input buffers without VOQ, only 58,6% throughput can be provided. Another important aspect to achieve good results is scheduling algorithm. A scheduling algorithm is used to configure our switch and find the most optimal connections between inputs and outputs. Optimal means that in one time slot (basic time unit) we want to send the greatest number of packets. This kind of algorithm should provides low time delay, during packet sending and high efficiency. In this paper presented algorithms will be compared with another algorithms, well known from literature, by using computer simulations. Several algorithms were compared: iSLIP algorithm which is presented in [7], Parallel Iterative Matching (PIM) [5], Iterative Round-Robin Matching (iRRM) [8], Maximal Matching with Random Selection (MMRS) [9], [10], [11], Maximal Matching with Round-Robin Selection (MMRRS) [9], [10], [11], Random [12] and Permanent [12].

This paper is organized as follows. In first section switch architecture is described. Then algorithms are presented. In chapter 4, all simulation parameters are discussed. In section 5 simulation results are described. Finally some conclusions will be given.

## 2. SWITCH ARCHITECTURE

The switch architecture is presented in figure 1.

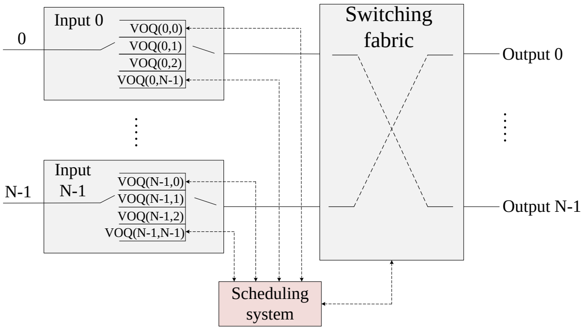


Fig. 1. 4×4 switch architecture

Figure 1 presents example of 4×4 switch architecture. It can be observed from figure 1, that discussed architecture consists of: input and output modules, switching fabric and scheduling system. Scheduling system will be discussed, in more details, in the next section. Presented switch architecture has four inputs and four outputs. As was mentioned above, switching fabric with input queuing system, where buffers are placed at the inputs, was used. Each input has separated queue which is divided into *N* independent VOQs. The total number of virtual queues depends of the number of inputs and outputs. Our switch architecture is symmetric, so total number of inputs is equal to the number of outputs. Base on this assumption, in general case total number of VOQs is equal to $2^N$. Each VOQ is denoted by VOQ (*i, j*), where *i* is number of input and *j* is number of output. It was assumed that $0 \leq i \leq N$-1 and $0 \leq j \leq N$-1. More details about switch architecture can be found in [1][2].

## 3. SCHEDULING ALGORITHMS

Presented algorithms based on permanent connections between inputs and outputs. Example of connection patterns in 4x4 switch, in each time slot are shown in figure 2.

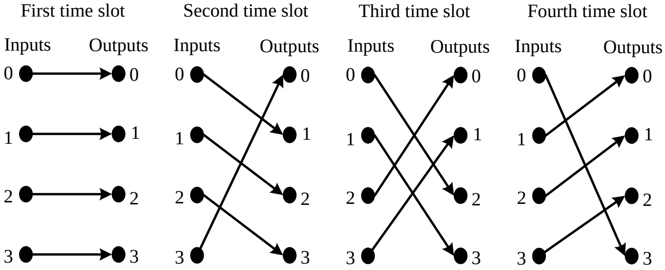
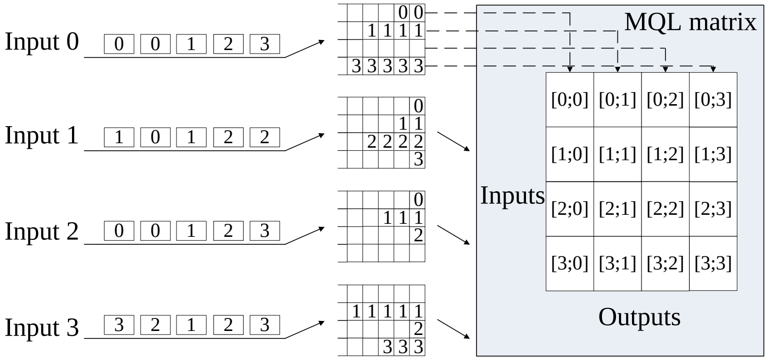


Fig. 2. Connection pattern in 4×4 switch [1]

Before the packet will be send through the switch, decision about input selection should be taken. It should be decided which packet from which input will be send. Selected packet will be send to the appropriate output in current time slot. In real hardware implementation, a few scheduling systems are used. These systems resolve problems related with establish connection between an input and an output. Three based scheduling mechanism: Random Selection, First in First Out (FIFO), Round-Robin selection were described in [3].

In this article, centralized scheduling mechanism was discussed. In presented solution, permanent connection pattern in each time slot is provided. This solution gives fair access to the all outputs. It means, that all outputs are treated equally and there is no prioritization for certain outputs. If we consider the implementation limits, centralized scheduling mechanism will has the advantage over traditional mechanisms. In

present communication nodes, where 10 Gb/s ports are used, one time slot is equal 50ns. Traditional scheduling mechanisms are based on three signals: demand, confirmation and acceptance. Sending these three signals takes more than 50ns. It means that one time slot is not enough for traditional scheduling mechanism. To solve this problem centralized scheduling mechanism is used. All current algorithm implementations based on small number of control signals between all modules in switch architecture. It provides fast configuration of switching fabric. Presented algorithms are based on centralized scheduling mechanism and permanent connection pattern. It provides fair access to the all outputs.
Discussed earlier, centralized scheduling mechanism, is responsible also for storing information about number of packets waiting in each virtual output queue. Based on this information Matrix of Queue Length (MQL) has been created. Matrix is the simplest way to store information about number of packets waiting in VOQs to be send through the switching fabric. Quick access to the information is also provided. For example, from figure 3, can be seen how the MQL matrix has been complemented.



| | | | |
|---|---|---|---|
| [0;0] | [0;1] | [0;2] | [0;3] |
| [1;0] | [1;1] | [1;2] | [1;3] |
| [2;0] | [2;1] | [2;2] | [2;3] |
| [3;0] | [3;1] | [3;2] | [3;3] |

Fig. 3. MQL matrix [1]

In each time slot all information in MQL matrix are updated. Matrix size is equivalent to the switch architecture. From figure 3 can be seen that presented matrix consists of four rows and four columns. It means that presented matrix storing information about packets waiting to be sent in 4×4 switch. This switch has four inputs divided into four VOQs (figure 1). One row in matrix is equivalent to the one switch’s input. Each item in the matrix has a unique identification. In the general case, each position can be marked as [*i*; *j*], where *i* is the input number and *j* is the output number. Each position in our MQL matrix, reflecting situation in each VOQ. For example, position [0;0] in matrix is adequate to the VOQ (0;0). More details about MQL matrix can be found in [1][2].

### 3.1. SSMPS ALGORITHM

As previously mentioned, algorithm SSMPS based on permanent connection pattern and information is stored in MQL matrix. Connections between inputs and outputs in switching fabric are classified into two groups. First of them is empty connections group which contains all connections where there is no packets to be send (0 in each positions in MQL matrix). Second group is non-empty connections group, where belong connections with packets to be sent through the switch. Main rule is, that algorithm try to avoid empty connections. When in connection pattern, in each time slot, is more than two empty connections, then algorithm all empty connections in this pattern replaced on the next available. This solution does not always lead to find better connection pattern. Advantage of this solution is, that our algorithm works fast and does not need any additional calculations. This kind of algorithm can be easily implemented is the hardware, for example in FPGA chip [13]. More details about SSMPS algorithm can be found in [1].

### 3.2. MSMPS ALGORITHM

MSMPS algorithm also based on permanent connection pattern and information stored in MQL matrix. This algorithm tries to find better connections eliminating empty connections from connection pattern in each time slot. Algorithm gives priority queues, where the highest number of packets are stored and waiting to be send through the switch. More details about this algorithm can be found in [2].

## 4. SIMULATION CONDITIONS

In this article performance results for SSMPS and MSMPS algorithms are presented. These algorithms were compared with another, well known from the literature, by using computer simulations. Packets are incoming at the inputs according to Bernoulli arrival model [3][14]. In this model, probability that packet will arrive at the input is equal to *p*, where *p* $\epsilon(0 < \mathrm{p} \leq 1)$. Only one packet can arrive at the input in each time slot. It was assumed also, that one packet may occupied only one time slot. Simulation results as a mean value of ten independent simulation runs are presented. Number of iterations in one simulation run is equal to 500.000, where the first 30.000 steps are reserved for obtaining convergence in the simulation environment. It was assumed also that discussed switching fabric is strict sense non-blocking. It means that there is always possible to establish connection between each suitable and idle input and suitable and idle output of the switching fabric [15]. In this paper, two the most important following parameters were compared:

1. Efficiency: this parameter is calculated according to equation 1. Numerator is the number of packets passed in n-*th* time slots through the switching fabric. Denominator is the number of packets which can be passed in n-*th* time slot through the switching fabric [1][2][15] .

$$q = \frac{\sum_n a_n}{\sum_n b_n} \tag{1}$$

where:
$q$ – efficiency,
$n$ - time slot number,
$a_n$- number of packets passed in *n* time slot through the switch,
$b_n$- number of packets which can be sent in *n* time slot through the switch.

2. Mean Time Delay (MTD): this parameter is calculated according to equation 2. Numerator is a sum of difference between time when a packet is transferred by the switch and the time when the packet has arrived to the buffer system. Denominator is a number of packets [1][2][15].

$$MTD = \frac{\sum_n (t_{out}(n) - t_{in}(n))}{k} \tag{2}$$

where:
$n$ - time slots number,
$t_{in}$ - time a packet arrive to the VOQ,
$t_{out}$ - time when the same packet is transferred by the switch,
$k$ - number of packets.

In this paper, three distributed traffic models were considered. Each of this model determines the probability that packet, which appeared at the input, will be directed to the suitable output.

### 4.1. DIAGONALLY DISTRIBUTED TRAFFIC

In this distribution traffic model, all packets (traffic) is concentrated into two diagonals of the traffic table. For example, input *i* has packets only directed to the output *j* and for output described by equation (($i$ + (*N*-1))mod *N*. The probability that packet will appeared at the suitable input *i* and will be transferred to the output *j* is equal to $p = \frac{1}{2}$. Rest of inputs have probability equal to $p = 0$. Traffic table and more details can be found in [14][16][17][18].

### 4.2. LIN-DIAGONALLY DISTRIBUTED TRAFFIC

Lin-diagonlly distributed traffic model based on diagonally distributed model. In this model, a load decrease linearly from one diagonal to the other [19]. Probability can be calculated according to equation 3,

$$p_d = p\,\frac{N-d}{N(N+1)/2} \tag{3}$$

with $d = 0$;   ; $N$ – 1, then $p_{ij} = p_d$ if $j = (i + d)\bmod N$
where:
$p_d$ – probability of packet arriving in lin-diagonally distributed traffic,
$p$ – probability of packet arriving in Bernoulli process,
$N$ – number of switch inputs/outputs,
$d$ – output number.

### 4.3. NON-UNIFORMLY DISTRIBUTED TRAFFIC

The last consider in this paper model, is non-uniformly distributed traffic model. The probability of the packet arriving at the input $i$, directed to the output $j$, in for 4×4 switch was presented in [15]. Some outputs have higher probability of being selected. This kind of probability can be marked as $p_{ij}$ and can be calculated according to equation 4 [20].

$$\boldsymbol{p_{ij}} = \begin{cases} \frac{1}{2}\ \boldsymbol{dla}\ \boldsymbol{i = j} \\ \boldsymbol{\frac{1}{2(N-1)}}\ \boldsymbol{dla}\ \boldsymbol{i \neq j} \end{cases}$$

$N$ – number of switch inputs/outputs.

## 5. SIMULATION RESULTS ANALYSIS

In this paper simulation results for 16×16 and 32×32 switches sizes were presented. The efficiency is plotted in figures 4 – 7 and the mean time delay (MTD) is plotted in figures 8 – 11.

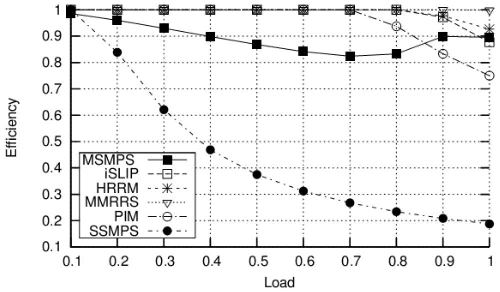


Fig. 4. The efficiency for Bernoulli arrivals with

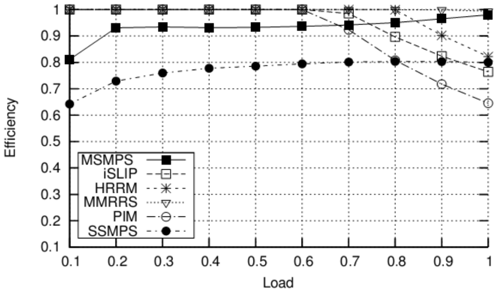


Fig. 5. The efficiency for Bernoulli arrivals with

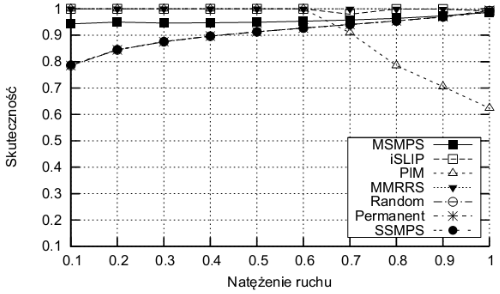


Fig. 6. The efficiency for Bernoulli arrivals with uniformly distributed traffic in 32×32 switches

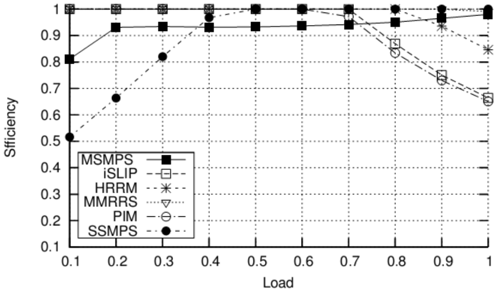


Fig. 7. The efficiency for Bernoulli arrivals with non-uniformly distributed traffic in 16×16 switches

From figures 4 – 7 can be observed that our algorithms achieved almost the same results (efficiency) like the rest of algorithms for the high load (above 80%). The worst results SSMPS and MSMPS algorithms achieve for diagonally distributed traffic (figure 4). The reason can be, that presented algorithms to much focused on provide equitable access for outputs instead of avoid empty connections. Above 60% load, efficiency for described algorithms increase and reached mean value about 0.9 with growing tendency for diagonally, uniformly and non-uniformly distributed models. Different phenomena can be observed in another compared algorithms.

From figures 8 – 11 can be seen that MSMPS algorithm achieve lower MTD, than the rest compared algorithms, for all distributed traffic models. Above 60% load, when some algorithm's MTD rapidly increase, MSMPS results are on the low level. It is mean that packets do not stay a long time in VOQ, before they will be send through the switch. The worst results achieved SSMPS. The reason why SSMPS algorithm achieved worse results is that this algorithm does not need any additional calculations. It works fast and is easy to implementation. This is strong point of SSMPS algorithm.

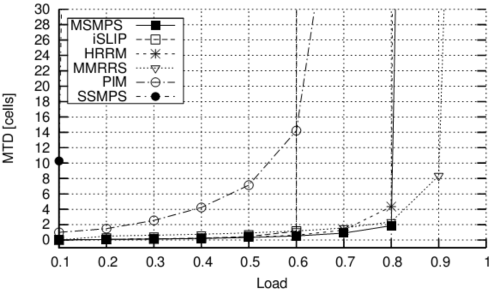


Fig. 8. The MTD for Bernoulli arrivals with di

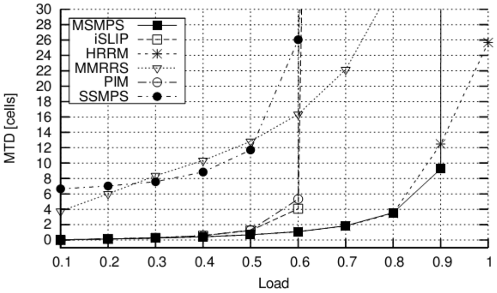


Fig. 9. The MTD for Bernoulli arrivals with lin-

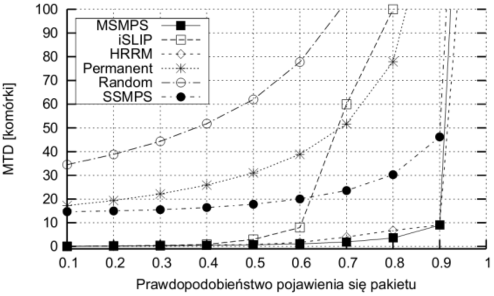


Fig. 10. The MTD for Bernoulli arrivals with uniformly distributed traffic in 32×32 switches

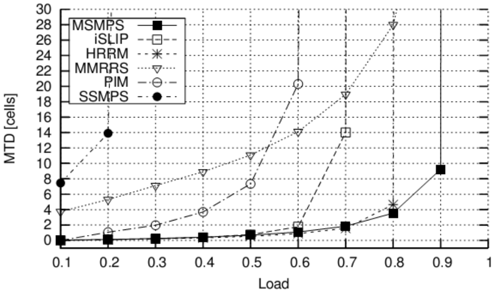


Fig. 11. The MTD for Bernoulli arrivals with non-uniformly distributed traffic in 16×16 switches

## 6. CONCLUSION AND FURTHER WORKS

In this paper, two algorithms were presented: SSMPS and MSMPS under different distribution traffic models. These algorithms can be used to configured switching fabric. Presented algorithms were compared with another algorithms, well known from the literature, by using computer simulations. Gathered results show that described algorithms achieved the same results like the rest of compared algorithms and for some cases, achieve better efficiency and lower MTD. In some cases SSMPS and MSMPS algorithms achieved worse results than the rest algorithms. The strong point is, that presented algorithms work very fast and do not need to do complicated calculations. For this reason SSMPS and MSMPS are easy to implementation and in an future works, can be try implement it in Field Programming Gate Array (FPGA) matrixes [13].

## REFERENCES

[1] DANILEWICZ G., DZIUBA M., *The New SSMPS Algorithm for VOQ Switches*, In: Information Systems Architecture and Technology. Networks Design and Analysis, seria Biblioteka Informatyki Szkół Wyższych, Oficyna Wydawnicza Politechniki Wrocławskiej, 2012, str. 171-180.

[2] DANILEWICZ G., DZIUBA M., *The New MSMPS Packet Scheduling Algorithm for VOQ Switches*, 8th IEEE, IET International Symposium on Communication Systems Networks and Digital Signal Processing (CSNDSP), Poznań, July 2012.

[3] CHAO JONATHAN H., LIU B., *High Performance Switches and Routers*, ISBN-13:978-0-470-05367-6, John Wiley and Sons, pp. 195-197, New Jersey, 2007.

[4] YOSHIGOE K., CHRISTENSEN K.J., *An evolution to crossbar switches with virtual ouptut queuing and buffered cross points*, IEEE Network, vol. 17, no. 5, 2003, pp. 48-56.

[5] ANDERSON T. and et al., *High-speed switch scheduling for local-areanetworks*, ACM Transactions on Computer Systems, vol. 11, no. 4, pp.319-352, November 1993.

[6] TAMIR Y. and FRAZIER G., *High performance multiqueue buffers for VLSI communication switches*, Proc. 15th Annu. Symp. Comput. Arch., pp.34 3-354, June 1988.

[7] McKEOWN N., *The iSLIP Scheduling Algorithm for Input-Queued Switches*, IEEE/ACM Trans. on Networking, vol. 7, pp. 188-200, April 1999.

[8] McKEOWN N., VARAIYA P., and WARLAND J., *Scheduling cells In an Input-Queued Switch*, IEE Electronics Letters, pp. 2174–2175, 1993.

[9] BARANOWSKA A., KABACIŃSKI W., *The New Packet Scheduling Algorithms for VOQ Switches* ICT 2004, LNCS 3124, pp. 711-716, 2004.

[10] BARANOWSKA A., KABACIŃSKI W., *MMRS and MMRRS Packet Scheduling Algorithms for VOQ Switches*, MMB PCTS 2004, pp. 359-368, September 2004.

[11] BARANOWSKA A., KABACIŃSKI W., *Evaluation of MMRS and MMRRS Packet Scheduling Algorithms for VOQ Switches under Bursty Packet Arrivals*, High Performance Switching and Routing (HPSR), pp. 327 -331, May 2005.

[12] DZIUBA M., *Comparison of Packet Scheduling Algorithms for VOQ Switches*, Poznańskie Warsztaty Telekomunikacyjne (PWT), Poznań, 2011.

[13] MAJEWSKI J., ZBYSIŃSKI P., *Układy FPGA w przykładach*, BN 978-8360233-23-8,BTC, Warszawa 2007.

[14] GIACCONE P., SHAH D., and PRABHAKAR S., *An Implementable Parallel Scheduler for Input-Queued Switches*, IEEE Micro, vol. 22, no. 1, pp.19-25, 2002.

[15] DANILEWICZ G., DZIUBA M., *Performance evaluation of the MSMPS algorithm under different distribution traffic*, 17-th Polish Teletraffic Symposium, (PTS 2012), Zakopane, December 2012.

[16] SHAH D., GIACCONE P., PRABHAKAR B., *Efficent Randomized Algorithms for Input-Queued Switch Scheduling*, Proc. of Hot-Interconnects IX, vol. 22, no. 1, pp. 10–18, January 2002.

[17] SHAH D., GIACCONE P., PRABHAKAR B., *Randomized Scheduling Algorithms for High-Aggregate Bandwidth Switches*, IEEE J. Select. Areas in Commun., vol. 21, no. 4, pp. 546–559, May 2003.

[18] JIANG Y., HAMDI M., *A Fully Desynchronized Round-Robin Matching Scheduler for a VOQ Packet Switch Architecture*, IEEE HPSR'01, pp. 407–411, May 2001.

[19] BIANCO A., GIACCONE P., LEONARDI E., NERI F., *A Framework for Differential Frame-Based Matching Algorithms in Input-Queued Switches*, IEEE Infocom, 2004.

[20] YOSHIGOE K., CHRISTENSEN K.J., *An evolution to crossbar switches with virtual output queuing and buffered cross points*, , IEEE Network, vol. 17, no. 5, pp. 48–56, September 2003

*multiservice switching networks, overflow traffic, blocking probability.*

Mariusz GŁĄBOWSKI*, Michał Dominik STASIAK*

# MULTI-SERVICE SWITCHING NETWORKS CARRYING OVERFLOW TRAFFIC STREAMS

The objective of this chapter is to propose a simulation model of a multiservice switching network carrying overflow traffic streams. As compared to Erlang-type traffic, overflow traffic is said to be degenerated and can be characterized by two parameters: the average value and the variance. The approach adopted in the present chapter assumes that the required values of these parameters will be determined on the basis of Pascal distribution. The chapter also presents and discusses the results of a study of some selected multiservice three-stage Clos networks to which overflow traffic with a different degree of degeneration is offered. The results of the study are then compared with the results of the simulations of switching networks with Erlang traffic.

## 1. INTRODUCTION

The overflow mechanism has been used in telecommunications systems since the 1950s. This mechanism is fairly simple. When all available resources of a given system are occupied (a link, cell, MPLS channel, etc.), calls are not lost but are redirected (overflow) to other, the so-called alternative, systems where connection paths can be set up (this traffic is generated only when the primary group is in blocking state). Initially, the overflow mechanism was used in traditional, hierarchical telecommunications networks. With time, along with the development of radio networks, in which optimization of limited radio resources became significantly more and more important, the traffic overflow mechanism was introduced to wireless networks, both second (i.e. GSM - Global System for Mobile Communications) and third generation (UMTS – Universal Mobile Telecommunication System), as well as to WiFi (Wireless Fidelity) networks and WiMAX (Worldwide Interoperability for Microwave Ac-

* Chair of Communication and Computer Networks, Poznan University of Technology, ul. Polanka 3, 60-965 Poznan, Poland

cess) networks [1,2]. The architectures of present-day packet networks, based on the DiffServ (Differentiated Services) and MPLS (Multi Protocol Label Switching) standards, also allow the traffic overflow mechanism to be effectively implemented [3,4]. As a result, switching devices in a network can be offered additional overflow traffic from other nodes in the network. Since the basic elements of nodes in communications networks are switching networks, degenerated overflow traffic will be then directly affecting the operating parameters of such systems. The present chapter deals with the analysis of the influence of overflow traffic upon the quality of service parameters (QoS) in multi-stage switching networks.

The chapter is structured as follows: Section 2 includes a short presentation of the most important properties of overflow traffic. Additionally, a simulation model of overflow traffic based on Pascal distribution is described. Section 3 discusses briefly the multiservice switching network and the adopted method for the simulation of switching networks with overflow traffic with a required degree of degeneration. Section 4 presents an analysis of the results of the study of multi-stage switching networks with overflow traffic and as a comparison also with Erlang traffic. This section also includes a presentation of the dependence between the total blocking probability of the switching network  and the peakedness coefficient of offered traffic. Section 5 sums up the results of the study presented in the chapter.

## 2. OVERFLOW TRAFFIC

Telecommunications networks employ a significant number of systems that take advantage of the traffic overflow mechanism. Hence, while modeling telecommunications and computer systems, an analysis of this type of traffic is very important. Unlike offered Erlang-type traffic [5], overflow traffic has non-Poisson character. Inasmuch as it is relatively easy to analyse and describe traffic with the Poisson traffic characteristics, the situation looks completely different with non-Poisson traffic, where its description is much more complex. Overflow traffic is non-Poisson traffic with peakedness [6,7]. The fact involves a situation wherein a non-periodic occurrence of time intervals with high traffic intensity that largely exceeds the capacity of available resources is regular. Because of the above, this traffic cannot be interpreted in the traditional, i.e. “Erlang”, way.

### 2.1. CHARACTERISTICS OF OVERFLOW TRAFFIC

Let us consider the diagram of traffic overflow shown in Fig. 1. Erlang type traffic with the intensity $A$ is offered to System 1 (Fig. 1) that has at its disposal the so-called primary resources with the capacity of $V$ allocation units (AU). The allocation unit is a general concept that defines the unit of capacity of a given system (channel, link, Basic Bandwidth Unit (BBU)) [8,9,10]. If primary resources are fully occupied, then a new call will be redirected (overflow) to System 2 that has the so-called secondary (alternative) resources with the capacity *V'*. The call stream offered to the secondary resources, as a result of the occupancy of the primary resources, degenerates and loses its Poisson character. Such traffic is characterized by a significant "peakedness", which in consequence leads to an increase in the blocking probability in System 2 (as compared to Erlang type traffic with the same average value).

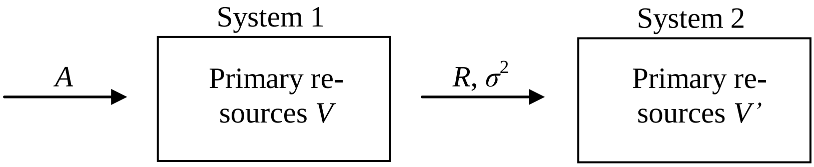


Fig. 1. Diagram of traffic overflow

Overflow traffic is most frequently characterized by two parameters, i.e. the average value *R* and the variance $\sigma^2$:

$$R = A\,E_V(A)\,, \tag{1}$$

$$\sigma^2 = R\left(\frac{A}{V+1-A+R}+1-R\right). \tag{2}$$

Formulas (1) and (2) that determine the parameters of overflow traffic are called Riordan formulas [7] and make the construction of analytical models that include dimensioning of alternative systems, both single-service [6,7,11] and multiservice [12,13], possible. The analysis of overflow systems often employs the value of variance ratio for the average value of overflow traffic. This parameter is said to indicate the degree of degeneration of overflow traffic and is called the peakedness coefficient or traffic degeneration coefficient [6]:

$$Z \;=\; \sigma^2 \,/\, R\,. \tag{3}$$

The peakedness coefficient for Erlang type traffic equals one (a variance equal to the average value), whereas in the case of overflow traffic its value is greater than one.

### 2.1. SIMULATION MODEL OF OVEWRFLOW TRAFFIC

In order to simulate an overflow call stream properly and accurately it is necessary to take into account the nature of the stream. This is possible through setting the value of the parameter $Z$ that determines the degree of degeneration of the stream with regard to the call stream of Poisson type. [14] proposes a model of the call stream, called the Pascal stream, that is characterized by a possibility of setting the required peakedness coefficient that is higher than one. It has been proved in traffic theory [5] that the properties of the Pascal stream are similar to the properties of an overflow call stream, and therefore the Pascal stream can be used to model overflow mechanisms.

In the Pascal model, the call stream can be described by two parameters: the number of traffic sources $S$ and the intensity of calls from one free source $\gamma$. The Pascal model, similarly to the Engset model, assumes that the number of traffic sources is finite though in the former model the intensity of the call stream increases with the increase in the occupancy of the system [5]:

$$\lambda(k) = (S+k)\,\gamma, \tag{4}$$

where $\lambda(k)$ is the intensity of the call stream with $k$ active traffic sources. The concept of the active traffic source involves a traffic source in the state of service, i.e. a traffic source that has generated the currently serviced call. The occupancy distribution in the Pascal model is described by Formula [14]:

$$p(k) = \binom{-S}{k}(-\beta)^k \Big/ \sum_{n=0}^{V}\binom{-S}{n}(-\beta)^n, \tag{5}$$

where $\beta$ is the average traffic offered to the system by one free source:

$$\beta = \gamma/\mu. \tag{6}$$

In Formula (6), the parameter $\mu$ is the intensity of the service stream of the source (the inverse of this parameter determines the average service time of the source). Distribution (5) makes it possible to determine all important characteristics of the Pascal model, e.g. the average traffic offered to the system can be determined by the following formula:

$$A = S\frac{\beta}{1-\beta}, \tag{7}$$

whereas the peakedness coefficient can be expressed by the following dependence:

$$Z = 1+\frac{A}{S}. \tag{8}$$

Formulas (6)-(8) enable us to construct a simulator of a Pascal-type call stream. With the set of required values of offered traffic *A*, peakedness coefficient *Z* and the intensity of the service stream $\mu$, it is possible to determine, on the basis of (8), the number of traffic sources *S*. Then, on the basis of (6) and (7), it is possible to determine the intensity of calls from one free source $\gamma$. The parameters $\gamma$ and $\mu$ themselves are enough to simulate a Pascal traffic source. Figure 2 shows a time diagram of active states of a Pascal traffic source.

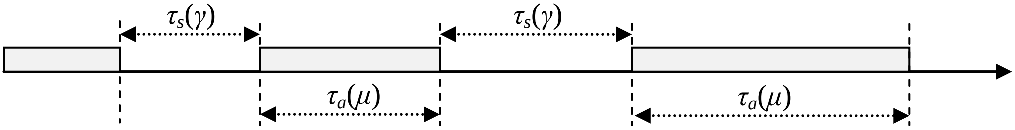


Fig. 2. Simulation of a Pascal-type traffic source

The values $\tau_a(\mu)$ define the activity time of the source determined by the random number generator with exponential distribution with the parameter $\mu$, whereas the values $\tau_s(\gamma)$ define the idle period of the source (silent period) (the time between the end of the activity period and the commencement of the next activity period), determined by the random number generator with exponential distribution with the parameter $\gamma$.

## 3. MULTISERVICE SWITCHING NETWORK

The objective of the simulation is a three-stage Clos switching network whose structure is presented in Fig. 3. The network is composed of *n* symmetrical switches in each stage, each with *n* inputs and *n* outputs. The assumption is that all links in the network: inputs, outputs and inter-stage links, have identical capacity equal to *f* AUs.

The output links are grouped into directions. Another assumption is that each *i*-th output link in each switch of the last stage creates the *i*-th direction.

### 3.1. BLOCKING IN SWITCHING NETWORK

Two types of blocking can be distinguished in the network: internal and external. The internal blocking occurs when a connection cannot be set up as a result of the lack of free connection paths, whereas the external blocking occurs when all output links in a given direction are occupied. The total blocking is then the sum of the internal and the external blocking. A switching network can operate in the following modes: the point-to-point selection and the point-to-group selection. In the point-to-point selection mode, the event of internal blocking occurs when setting up of a connection between a given link and a chosen output link in a given direction is not possible. In the point-to-group selection mode, the internal blocking occurs when a connection between a given input link and any free output link in a given direction cannot be set up. In the study, the point-to-group algorithm with random selection of outgoing links was assumed.

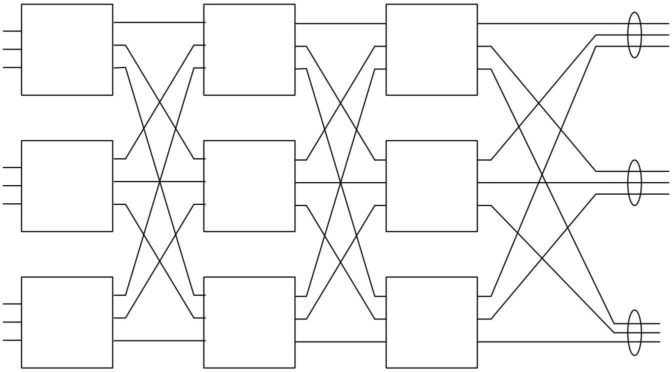


Fig. 3. Structure of the three-stage Clos network

The switching network is offered *m* traffic streams. Each call of class *i* demands $t_i$ AUs to set up a connection. The traffic streams involved can be of the Erlang, Engset or Pascal type with the required peakedness coefficient $Z_i$. The method for the simulation of Erlang and Engset traffic is described in [15]. In the case of the Pascal stream, after a determination of the parameters $\gamma_i$ and $\mu_i$, for class *i* calls, the operation of $S_i$ traffic sources, described in Section 2.1, is initiated. The admission of a new call for service (a transition from state *k*-1 of active sources to state *k* of active sources) is always followed by an initiation of two new sources, according to (4). A completion of a service, in turn, (a transition from state *k* of active sources to state *k*-1 of active sources) is followed by a disappearance of any two traffic sources inactive at the time of the transition.

### 3.2. A SIMPLIFIED DESCRIPTION OF THE SIMULATOR

The simulation experiments were carried out using a dedicated simulator (based on the event scheduling approach [16]) of the Clos network written in the C++ language. The simulator makes it possible to simulate any Clos network that services multiservice traffic. The simulator gives a possibility to service Erlang, Engset and Pascal traffic. Input data for each traffic class include: offered traffic and service intensity for the Erlang stream; offered traffic, the number of traffic sources and service intensity of calls for the Engset stream; offered traffic, the peakedness coefficient and service intensity of calls for the Pascal stream. In the case of overflow traffic (Pascal traffic), input parameters are calculated with the application of the dependencies presented in Section 2.1 to obtain the number of sources and the parameters appropriate for the generation of activity times and idle times of a source. It is also possible in the simulator to input proportions for the mixture of traffic of all types offered to the switching network. Two types of generators are used in the software simulator: one with a uniform distribution (multiplicative generator), and the other with the exponential distribution. In order to obtain acceptable accurateness of results, the simulator runs 10 simulation series. On the basis of the obtained results, with the *t*-Student distribution taken into account, a 99% confidence interval is established. The simulator operates according to the random algorithm of setting up connections – from among all existing connection paths (available and free for a given call), the algorithm randomly chooses a path that will be then used to set up a connection.

## 4. THE RESULTS OF THE SIMULATIONS OF NETWORKS WITH OVERFLOW TRAFFIC

The simulation study was carried out for a three-stage Clos network. The network under scrutiny was composed of symmetrical 4x4 switches. Each stage had 4 switches. The capacity of each of the links in the network was 30 AUs. Offered traffic was composed of 3 streams that demanded 6 AUs, 2 AUs and 1 AU, respectively. Traffic of each class was either Erlang, Engset or Pascal traffic with the required peakedness coefficient Z. The adoption was that traffic was offered in the following proportions: $A_1$: $A_2$: $A_3$ = 1:1:1. To set up connections in the network, the point-to-group was used. The simulation study was carried out with a dedicated digital simulator with the basic assumptions presented in Section 3. In the simulation experiments, a 99% confidence interval was established evaluated on the basis of the *t*-Student distribution for 10 series with at least 1,000,000 calls of each traffic class in each series. The results are presented in graphs relative to the average traffic offered per one allocation unit (AU) of the input link of a switching network.

Figure 4 shows the results for the traffic loss probability obtained in the simulation of the switching network that serviced three classes of traffic: Erlang ($t_1$=6 AUs), Engset ($t_3$=1 AU, $S$=544) and overflow traffic ($t_2$=2 AUs, $Z$=2), whereas Fig. 5 presents the results for the total traffic blocking probability for a network to which three Erlang traffic classes were offered in the first experiment ($t_1$=6 AUs, $t_2$=2 AUs, $t_3$=1 AU), and, as a comparison, three traffic classes in the second experiment, of which two were Erlang type ($t_1$=6 AUs and $t_3$=1 AU) and one was overflow traffic ($t_2$=2 AUs), i.e. was of Pascal type with the adopted peakedness coefficient $Z$=2. The presented results indicate that the traffic degeneration is an important factor in and has significant influence on the changes in the traffic characteristics of the network. The blocking probability of overflow traffic significantly increases along with the lack of changes in the blocking probability for Erlang type traffic.

Figure 6 shows the results of traffic loss effected during the network simulation in which all traffic classes were degenerated ($Z$=1.2 in the first experiment and $Z$= 1.5 in the second experiment). The presented results confirm that a change in the peakedness coefficient significantly influences the operation of the switching network. This phenomenon for the average traffic offered per one AU $a$=0.8 Erl is more precisely presented in Fig. 7 in which the percentage increase in the blocking probability of traffic (in relation to Erlang traffic streams) for each traffic class with respect to the degree of degeneration is shown.

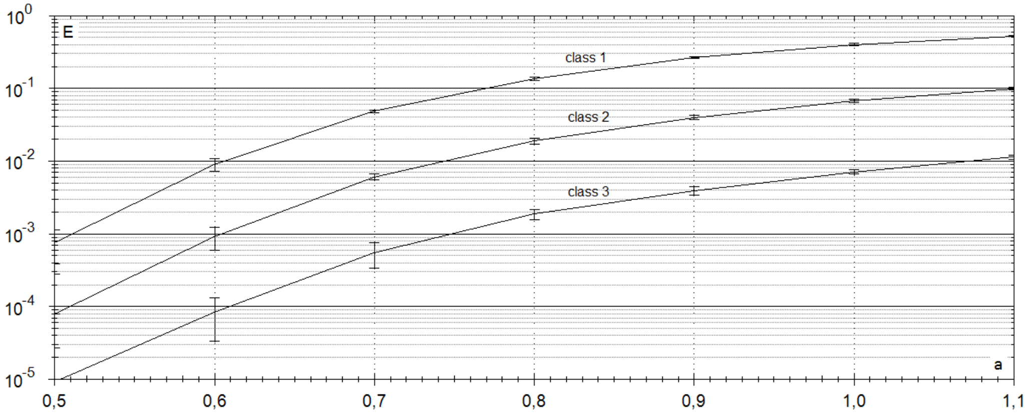


Fig. 4. Traffic blocking probability in the Clos network: class 1 – Erlang, class 2 – Pascal ($Z$=2), class 3 –Engset ($S$=544)

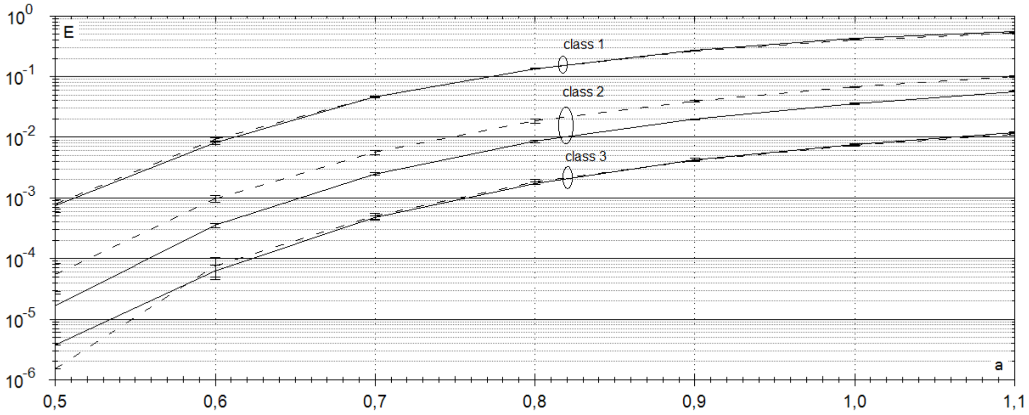


Fig. 5. Traffic blocking probability in the Clos network: —— class 1, class 2, class 3 –Erlang, - - - -class 1 –Erlang, class 2 –Pascal (*Z*=2), class 3 –Erlang

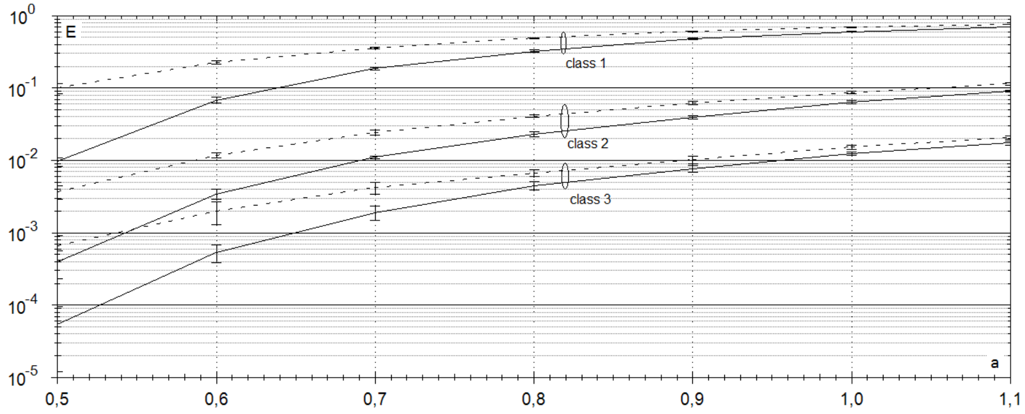


Fig. 6. Traffic blocking probability in the Clos network: —— class 1, class 2, class 3 –Pascal (*Z*=1.2), - - - - class 1, class 2, class 3 –Pascal (*Z*=1.5)

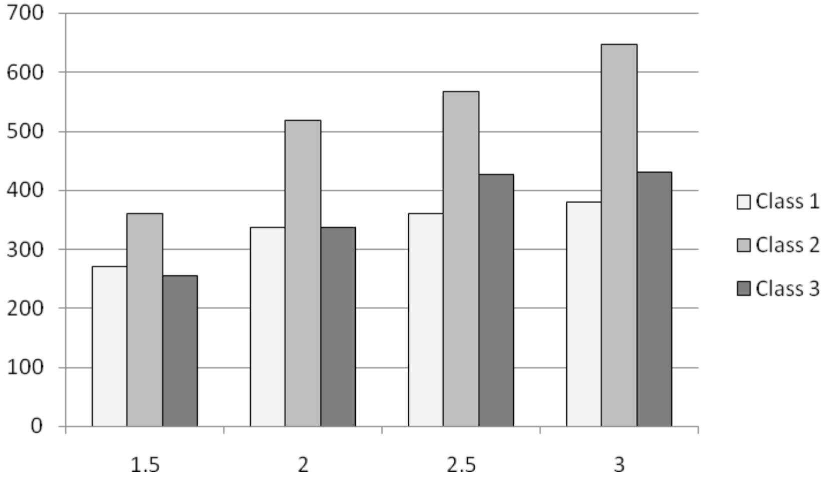


Fig. 7. Traffic blocking probability in the Clos network, ------ class 1, class 2, class 3 –Pascal (*Z*=1.2), - - - - class 1, class 2, class 3 –Pascal (*Z*=1.5)

## 5. CONCLUSION

This chapter proposes a simulation model of a multiservice switching network to which overflow traffic with a required degree of degeneration (peakedness coefficient) can be offered. The results obtained in the course of the simulation experiments indicate a significant influence of the degree of degeneration of traffic upon the characteristics of multiservice switching networks. This influence is significantly higher than the influence of degenerated traffic upon single-stage systems (single groups). This effect results from a complex, multi-stage structure of the switching network in which the phenomena of internal and external blocking occur. Summing up, the analysis of switching networks servicing overflow traffic cannot be validated unless the nature of such traffic is taken into consideration. Any exclusion of this fact may eventually lead to significant errors, far more larger than those that are characteristic for overflow systems based on single-stage systems.

## REFERENCES

[1] MACHOŃ P., WIECZORKOWSKA A., WOŹNIAK J., *Evaluation of IEEE 802.21 handover between IEEE 802.11 and UMTS networks*, Polish Journal of Environmental Studies, Vol. 16, No 4B 2007, 121–125.

[2] GŁĄBOWSKI M., *Modelowanie systemów multi-rate ze strumieniami zgłoszeń BPP*, Rozprawy Nr 433, Poznań, Wydawnictwo Politechniki Poznańskiej, 2009, 189.

[3] GŁĄBOWSKI M., KALISZAN A., *Convolution algorithm for overflow calculation in integrated services networks*, in: Proceedings of the 2011 17th Asia-Pacific Conference on Communication (APCC), IEEE, Kota Kinabalu, Malaysia, 2011, 428–433, doi:10.1109/APCC.2011.6152847.

[4] GŁĄBOWSKI M., HANCZEWSKI S., STASIAK M., *Erlang's ideal grading in DiffServ modelling*, in: Proceedings of IEEE Africon 2011, IEEE, Livingstone, Zambia, 2011, 1–6, doi:10.1109/AFRCON.2011.6072139.

[5] IVERSEN V., Editor., *Teletraffic Engineering Handbook*, ITU-D, Study Group 2, Question 16/2, Geneva, 2005.

[6] FREDERICKS A., *Congestion in blocking systems — a simple approximation technique*, Bell System Technical Journal, 1980, 59, 6, 805–827.

[7] WILKINSON R., *Theories of toll traffic engineering in the USA*, Bell System Technical Journal, 1956, 40, 421–514.

[8] ROBERTS J., Ed., *Performance Evaluation and Design of Multiservice Networks*, Final Report COST 224, Commission of the European Communities, Brussels, 1992.

[9] STASIAK M., GŁĄBOWSKI M., WIŚNIEWSKI A., ZWIERZYKOWSKI P., *Modeling and Dimensioning of Mobile Networks*, Wiley, 2011.

[10] VASSILAKIS V.G., MOSCHOLIOS I.D., LOGOTHETIS M.D., *Call-level performance modelling of elastic and adaptive service-classes with finite population*, IEICE Transactions on Communications, 2008, E91-B, 1, 151–163.

[11] BRETSCHNEIDER G., *Die Berechnung von Leitungsgruppen fur berfließenden Verkehr in Fernsprechwahlanlagen*, Nachrichtentechnische Zeitung (NTZ), 1956, 9, 533–540.

[12] GŁĄBOWSKI M., KUBASIK K., STASIAK M., *Modeling of systems with overflow multi-rate traffic, Telecommunication Systems, 2008,* 37, 1–3, 85–96, doi:10.1007/s11235-008-9070-8.

[13] HUANG Q., KO K.T., IVERSEN V.B., *An approximation method for multiservice loss performance in hierarchical networks*, in: Managing Traffic Performance in Converged Networks, 20th International Teletraffic Congress, ITC20 2007, Lecture Notes in Computer Science, vol. 4516, red. L. Mason, T. Drwiega, J. Yan, Springer, 2007, 901–912, doi:10.1007/978-3-540-72990-7 78.

[14] WALLSTROM B., *Congestion studies in telephone systems with overflow facilities*. Ericsson Technics, No. 3, 1966, 187-351.

[15] GŁĄBOWSKI M., KALISZAN A., *Simulator of full-availability group with bandwidth reservation and multi-rate Bernoulli-Poisson-Pascal traffic streams*, in: Proceedings of Eurocon 2007, Warszawa, 2007, s. 2271–2277, doi:10.1109/EURCON.2007.4400605.

[16] TYSZER, J., *Object-Oriented Computer Simulation of Discrete-Event Systems*, Kluwer Academic Publishers, 1999.

*self-similar traffic, routing, QoS, DiffServ, network performance*

Michał CZARKOWSKI*, Sylwester KACZMAREK*, Maciej WOLFF*

# TRAFFIC TYPE INFLUENCE ON QOS NETWORK PERFORMANCE OF STREAMING TRAFFIC CLASS

Feasibility study on QoS routing proved that the traffic type influence the network performance. The performance is defined here as a number of packets serviced by the network. In the paper additional element - buffers lengths used in service system was verified in terms of dependencies with routing performance. We present results obtained by simulation for many simulation scenarios. Analysis was done for two different network topologies and for two traffic types (Poisson and self-similar) and for two traffic classes (streaming and best-effort) as a function of buffer lengths within streaming traffic class and for many proportions between these traffic classes.  Analysis was done for two routing algorithms: OSPF and DUMBRA. To generate self-similar traffic multiplexed ON-OFF model was used. Relative measure was used for comparison of network performance for given traffic type. Received results in some cases were hard to comment and difficult to fit into regular pattern which points that the subject is complex and very complicated at the time. One of basic conclusion is that relative difference between these two networks structures and its performance depends on the buffer lengths in the service systems however with some exceptions.

## 1. INTRODUCTION

Modern packet networks should support services such as voice, video, etc. These services require from the network guarantee of proper quality for packets belonging to these services. The example solution for guarantee Quality of Services (QoS) is Differentiated Services (DiffServ) architecture with QoS routing. Within DiffServ three serviced traffic classes are distinguished: expedited forwarding (EF), assured forwarding (AF) and best-effort (BE). One of them, expedited forwarding, is a subject of this

* Department of Teleinformation Networks, Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, 11/12 Gabriela Narutowicza Street, 80-233 Gdańsk, Poland

study, this class will be called streaming traffic class. This class is used for services with the highest priority and QoS guarantees appropriate for data such as voice.  The best-effort is used for services with the lowest priority and no QoS guarantees.

Research in existing packet networks proved that in these networks traffic type has self-similarity characteristics [7]. Traffic from other domains in particular from domains without QoS generates self-similar traffic type to the domain with QoS. That is why DiffServ must also host self-similar traffic type with appropriate QoS.

This research was done for complex and existing network structures with many routers [13]. Previous researches in packet networks were focused to networks with single router [1][6][10] or simple network structures like several routers in a chain. Also many papers focused to routing performance deliver remarks and statements unfortunately not documented with solid simulation results. Authors of this paper wanted to keep realistic model and didn't decide to use analytic model with many simplifications due to problem complexity but decided to simulate real networks however with minor dependencies from network event simulation (couldn't use to high links bandwidth like 100Mbit/s or 1Gbit/s).

Simulation model used in this paper has been used also in previous research made by authors in the area of routing performance. OSPF performance was considered in [4] with focus to traffic type influence on efficiency of routing algorithm. During this research additional element (buffer length in service systems) has been qualified for further analysis. That was the reason why authors expanded the topic with additional simulations and analysis. In this paper we compare network performance for network with self-similar and Poisson offered traffic type as a function of buffer lengths within streaming traffic class.

The paper is split into several sections. The second section describes simulation model, including routing, service systems, traffic types and used measures. The third section contains a description of simulation scenarios including used proportions between traffic classes, network topology, etc. This section contains also results and analysis results of research.

The fourth section is summary and description of next research steps.

## 2. SIMULATION MODEL

A simulation model is based on model from work [3]. This model was implemented using discrete event network simulator called Omnet++ [12]. In this model full DiffServ network was implemented. In DiffServ architecture nodes are divided into edge and core nodes and deliver separated functions. Edge nodes mark traffic class of packets and accept or reject new traffic streams. Also core and edge routers send packets with defined politics like EF PHB, AF PHB or BE PHB.

In this model acceptance or rejection of the stream by the edge router depends on actual network load. Network measures QoS parameters such as loss ratio (IPLR, IP loss ratio), time delay (IPTD, IP time delay) and delay variance (IPDV, IP delay variance) for each path from an edge router (source) to an edge router (destination) in end to end relation. Edge routers check these parameters before adding the new stream to service. If these parameters satisfy the conditions defined by [11] the stream is added to service. In the next subsections the most important elements of the simulation model are described.

### 2.1. ROUTING

In the simulation model OSPF [8] and DUMBRA [3] routing algorithm is used. OSPF algorithm determines a single shortest path between source and destination router. For all traffic classes identical path between these two routers is used. In this implementation of OSPF routing inversion of link capacity metric is used.

DUMBRA algorithm determines four shortest paths between the source and the destination router. When source edge router adds new stream to services, it chooses also the best path from this four paths based on QoS parameters. Next, every four minutes path is chosen again based on current QoS parameters. This algorithm is described in detail in [3].

### 2.2. SERVICES SYSTEM

The networks locate two traffic classes: streaming (services as EF PHB) and best-effort (services as BE PHB). That is why each service systems consist of two buffers. The first buffer processes streaming traffic class and is serviced with higher priority. The second buffer processes best-effort traffic class and has lower priority. Length of the second buffer is constant and is equal to 50 packets. Length of the first buffer depends on simulation scenario and is specified in the simulation scenarios section.

### 2.3. OFFERED TRAFFIC TYPES

There are two offered traffic types used in simulation. The first traffic type is Poisson traffic, the second traffic type is self-similar traffic, which time intervals between events are dependent in long time scale. For modeling this traffic ON-OFF model is used. In this model many ON-OFF sources are multiplexed. Each of these sources has two states: ON and OFF. In ON state packets are generated with constant rate. Packets are not generated in OFF state. Duration of ON state is specified by Pareto distribution and duration of OFF state is specified by exponential distribution. Parameters of this model, such as number of multiplexed stream, average time of duration ON and

OFF state, etc. have been chosen so that get established level of self-similarity. Measure of this level is the Hurst ratio and is described in [9].

### 2.4. MEASURES

Result of the simulation is amount of packets within streaming class serviced by network. To compare results between network with Poisson traffic type and network with self-similar traffic type relative measure $\Delta A$ is defined by (1).

$$\Delta A = \frac{A_{SS} - A_P}{A_P} \qquad (1)$$

In formula (1) $\Delta A$ is relative measure, $A_P$ is amount of packets of streaming traffic class serviced by network with Poisson offered traffic type, $A_{SS}$ is amount of packet of streaming traffic class serviced by network with self-similarity offered traffic type. For any value in formula (1) all other simulation settings were unchanged.

## 3. RESULTS

### 3.1. SIMULATION SCENARIOS

Simulations were made for two network structures: New York and Norway. These are real network instances from SNDlib [13]. New York structure is network with 16 network nodes and 49 links. Density of this network is 3.06. Norway structure is network with 27 network nodes and 57 links. Density of this network is 1.89. These structures were used in simulations in order to show result for network with different density and size (figures 1 and 2). Grey routers in these figures are core routers, white routers are edge routers.

For any network structure simulations was made for 8 traffic class proportions. The proportions are in table 1. Any row in this table contains one proportion. For example, for first proportion: 5% of offered traffics are streaming traffic and 95% of offered traffics are best-effort traffic.

All above simulations were repeated for three sets of buffer lengths. These sets are presented in table 2. Numbers in this table represent buffer length for buffer assigned to streaming traffic class – higher priority and buffer assigned to best-effort traffic class – lower priority. For example, for first row: length of buffer for higher priority is equal $K_{ST}$=5 packets, length of buffer for lower priority is equal $K_{BE}$=50 packets.

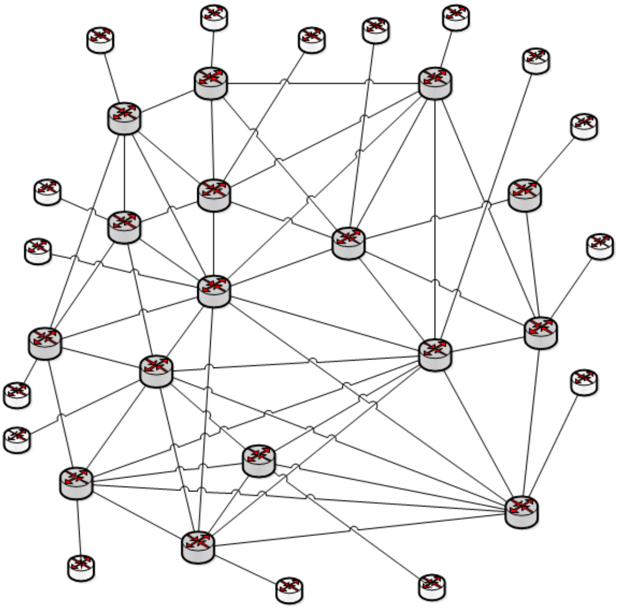


Fig. 1. New York structure

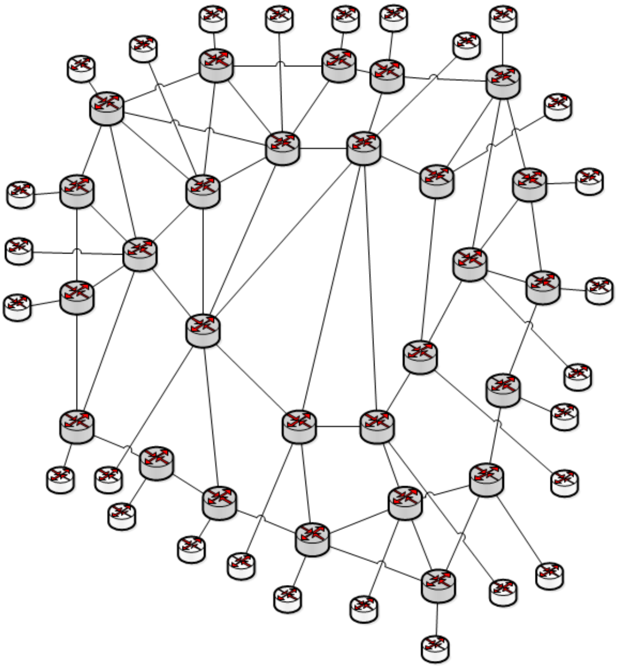


Fig. 2. Norway structure

Table 1. Traffic class proportions

| No. | Streaming traffic (ST) | Best-effort traffic (BE) |
|---|---|---|
| 1 | 0.05 | 0.95 |
| 2 | 0.1 | 0.9 |
| 3 | 0.15 | 0.85 |
| 4 | 0.2 | 0.8 |
| 5 | 0.25 | 0.75 |
| 6 | 0.3 | 0.7 |
| 7 | 0.35 | 0.65 |
| 8 | 0.4 | 0.6 |

Table 2. Buffer length

| No. | Higher priority | Lower priority |
|---|---|---|
| 1 | 5 | 50 |
| 2 | 8 | 50 |
| 3 | 10 | 50 |

All other simulation parameters are the same for all simulations. Packets length is equal 160B for streaming traffic class and 1500B for best-effort traffic class. Capacities of edge links are 20 Mbit/s, and capacities of core links are equal 3.5 Mbit/s. This value of capacities of core links is taken in order to reduce of simulation time, taking more real value for this parameter would extend the time needed for simulations and in consequently simulation for complex structures with many routers and links would be impossible. The Hurst ratio of self-similar traffic type is equal 0.9. This value of the Hurst ratio is based on [2], [5], [7]. Amount of all offered traffic have been chosen so as to packet was buffered in buffers.

Simulation time was 3600s. The simulations was made twelve times for each traffic proportion, each length buffer sets, each traffic type and each network structure and the average value was calculated. Result of the simulations is amount of packets services by network for streaming traffic class. All simulation results have been analyzed with applied statistical analysis including confidence intervals.

### 3.2. THE SIMULATION RESULTS

In figures 3 and 4 results in relative measures, which were described in section 2.4, for New York and Norway structures for OSPF routing are presented. In figures 5 and 6 results in relative measures $\Delta A$ for New York and Norway structures for DUMBRA routing are presented. In each figure shows relative measure for eight proportions of offered traffic class (tab.1.). For each proportion three bars are shown. First bar is for first set of queue length, second bar is for second set and third bar is for third set.

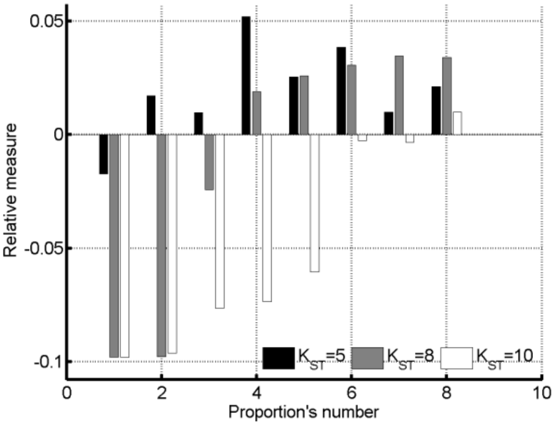


Fig. 3. Relative measure Δ*A* for New York structure and OSPF algorithm

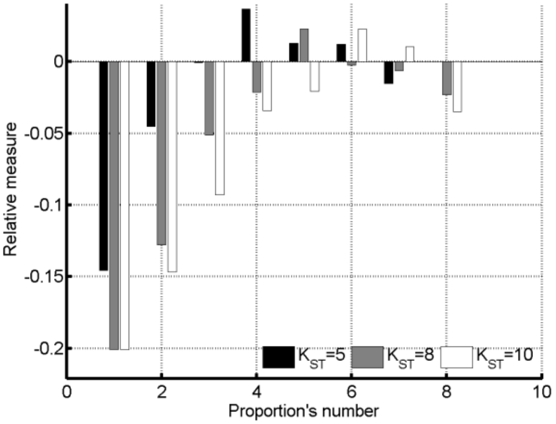


Fig. 4. Relative measure Δ*A* for Norway structure and OSPF algorithm

Conclusions for New York and Norway structures and OSPF algorithm:

– Higher dependence between type of offered traffic and relative measure for long buffer ($K_{ST}$=10 and $K_{ST}$=8) than for short buffer ($K_{ST}$=5).
– Greater performance for self-similar traffic type than Poisson traffic type for short buffer for many traffic proportions especially for high amount of streaming offered traffic.
– Depending on the level of streaming offered traffic class and relative measure and queue length: for positive relative measure, growing of relative

measure when growing offered traffic; for negative relative measure, decreasing of relative measure when growing offered traffic; growing and decreasing is higher for longer buffer and lower for small buffer.

These conclusions are right for all structures, but numerical, detailed results are different for different structures.

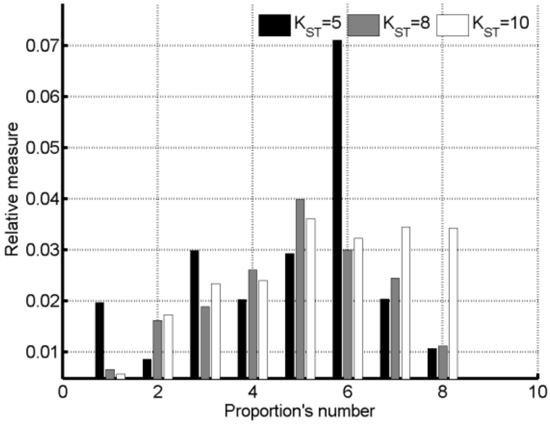


Fig. 5. Relative measure Δ$A$ for New York structure and DUMBRA algorithm

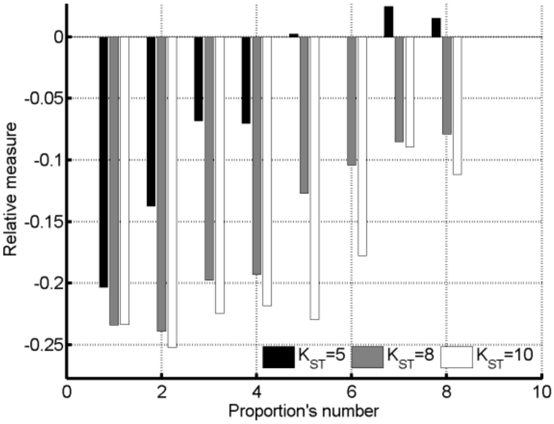


Fig. 6. Relative measure Δ$A$ for Norway structure and DUMBRA algorithm

Conclusions for DUMBRA algorithm are similar to conclusion for OSPF algorithm and additionally:

– For all traffic proportions and buffer length network has greater network performance for streaming traffic class for self-similar traffic type for New York structure and reversely for Norway structure.

Results of analysis all above conclusion are:

- Dependence on type of offered traffic for network with short buffer is smaller. In analytical models rather than self-similar traffic models for estimation traffic parameters like IPLR, IPTD and IPDV Poisson traffic models can be used.
- Network performance for streaming traffic class with self-similar traffic type is higher than for Poisson traffic type while using short buffers.

## 6. SUMMARY

The paper showed dependencies between buffers lengths and network performance for streaming traffic class with different traffic type. There are three important conclusions. Network performance for streaming traffic class does not depend on traffic type while using short buffers. Network performance for streaming traffic with self-similar traffic then for Poisson traffic is higher for large amount of offered traffic and small buffers length.

The research showed influence the length of buffer on network performance for network with self-similar traffic and network with Poisson traffic for different amount of offered traffic, different structures and different routing algorithm. This dependence is complex and difficult to clearly define.

Results of these researches confirmed the complex relationship between routing performance and buffers lengths which were presented in [10], but dependencies for complex structures are more complex and difficult to clearly identify.

Determining these dependences requires further researches and the simulations for other network structures and more numbers of network service classes.

## REFERENCES

[1] H. S. ACHARYA, S. R. DUTTA, R. BHOI, *The Impact of self-similarity Network traffic on quality of services (QoS) of Telecommunication Network*, International Journal of IT, Engineering and Applied Sciences Research (IJIEASR), Volume 2, No. 2, February 2013

[2] J. CANO, P. MANZONI, *On the use and calculation of the Hurst parameter with MPEG videos data traffic*, Proceedings of the 26th Euromicro Conference, vol.1, pp. 448–455, 2002

[3] M. CZARKOWSKI, S. KACZMAREK, *Simulation Model for Evaluation QoS Dynamic Ruting*, ISAT Conference 2009, Oficyna Wydawnicza Politechniki Wrocławskiej, pp. 255–264, 2009

[4] M. CZARKOWSKI, S. KACZMAREK, M. WOLFF, *Traffic Type Influence on Performance of OSPF QoS Routing*, Proceedings of 17th Polish Teletraffic Symposium, Zakopane 2012, pp. 29–35, 2012

[5] T. D. DANG, B. SONKOLY, S. MOLNAR, *Fractal analysis and modeling of VoIP traffic*, Telecommunications Network Strategy and Planning Symposium, 11th International, NETWORKS 2004, pp. 123–130, 2004

[6] Y. KOUCHERYAVY, J. HARJU, V. B. IVERSEN, *Multi-service IP Network QoS Parameters Estimation in Presence of Self-similar Traffic*, Proceedings of 6th International Conference, NEW2AN 2006, St. Petersburg, Russia, May 29–June 2, 2006.

[7] W. E. LELAND, M. S. TAQQU, W. WILLINGER, D. V. Wilson, *On the self-similar nature of Ethernet traffic (extended version)*, IEEE/ACM Trans. Netw., vol. 2, pp. 115, 1994

[8] J. T. MOY, *OSPF Anantomy of an Internet Routing Protocol*, Harlow, England: Adisson-Wesley, 2001

[9] O. I. SCHELUHIN, M. S. SMOLSKIY, A. V. OSIN, *Self-Similar Process in Telecommunication*, John Wiley & Sons, 2007

[10] X. TAN, Y. ZHUO, *Simulation Based Analysis of the Performance of Self similar Traffic*, Proceedings of 4th International Conference on Computer Science & Education, 2009

[11] ITU-T, Y-1541, *Network performance objectives for IP-based services*, February 2006

[12] OMNeT++, http://www.omnetpp.org/

[13] sndlib, http:/sndlib.zib.de/home.action

*queuing theory, analytic model, web application,
performance, multitier architecture*

Weronika STOCZEK*, Tomasz WALKOWIAK*

# AN ANALYTICAL MODEL FOR 3-TIER WEB SYSTEMS PERFORMANCE PREDICTIONS

Web system's performance predictions under given load and configuration is of great interest to all web service providers. In this paper there is presented an analytical model for these predictions. Basing on work presented in [8], queuing theory and multitier architecture analysis of modern applications, formulas defining the relation between the given input stream and average response time are defined in order to distinguish three types of requests. Results retrieved from the model are validated against experiments' outcomes. Proposed model successfully captures the performance characteristics of multitier web system including the cases of overload. However, as several simplifications are made, the performance metrics predicted from the model fit well to the experiment measurement only under defined conditions.

## 1. INTRODUCTION

As modern Web applications are complex systems with wide range of features and access to many external services, meeting performance expectations of nowadays user is a challenging task for Web systems providers. Simulations and modelling approaches [18] are eligible by system providers for planning the resource consumption of the application, and detecting the undesirable characteristics of the system.

In this paper focus is put on performance of web systems. One of the most important aspects of quality of service is application's performance seen from the user's perspective. If web application does not provide no or wrong responses for users' request, we assume that system is unavailable. This may be caused by a wide range of software bugs, hardware problems, malicious user activities or overload [18].

* Institute of Computer Engineering, Control and Robotics, Wroclaw University of Technology, ul. Janiszewskiego 11/17, 50-372 Wrocław, Poland

The main goal of the paper is the creation of the analytical model which will allow predicting the response time of the web system on given load. For this purpose the queuing networks [7] are used, where the queues represent different steps that request has to go through before is processed and the particular response is sent to the client side.

Solution that proposes mathematical formulas retrieved from queuing theory describes the relation between the load of the application and response time of application is presented in [8]. However, all of formulas defined by the author may be applied with assumption that the underlying stochastic process is ergodic, what means that the intensity of request stream in each node has to be smaller than intensity of request handling in that node. As a result of this assumption, this model does not describe the behaviour of the applications in cases of overload. As we can see in Fig. 4, the meaningful part of the real chart that stands for response time in case of overload is missing on chart derived from mentioned analytical model. Therefore, the main goal of this work is the improvement and extension of model from [8] with missing characteristics in cases of overload.

The paper is structured as follows. In the next chapter are presented related works and next assumptions to analysed systems are given, followed by the proposed analytical model. Section 4 is devoted to environment test and comparison of outcomes retrieved from the model with outcomes measured from real system. Finally, the work is summed up and the results are critically discussed.

## 2. BACKGROUND AND RELATED WORK

Providing good approach of Web server behaviours in simulation or analysis require understanding details of Web service's characteristic like: multitier architecture [13] or performance aspects [16].

Performance of web applications is popularly analysed and described in the literature by means of queuing theory. Modelling a simple single-tier application is often considered and well-studied problem [1,2,6,11,12,15]. Such solutions, however, are not adequate to the complexity of modern web applications based on the multi-layer architecture. In [10] and [14], authors point out the complexity of today's applications, however, as a simplification one PS queue representation is proposed. More complex models that capture the behaviours of a multi-layer architecture are presented in [5,8,13,17]. Analysis of the model in [13,17] is based on the Mean-Value Analysis (MVA) algorithm. Authors of [5] for evaluation of proposed solution have used tool PEPSY-QNS. Most relevant in relation to the goal of this work is solution proposed in [8] where mathematical formulas retrieved from queuing theory, defining the relation between system's performance and incoming stream of requests, are presented.

## 3. PROBLEM SOLUTION

### 3.1. ASSUMPTIONS OF THIS WORK

As this paper aims at retrieving formulas describing queuing networks, two types of them have to be distinguished [5]: networks with product and non-product form solutions. The analysis of networks with non-product form solutions is based on set of states that represent some particular conditions in the system. The main problem with these solutions is the state space explosion issue that leads to high computational complexity, so here the focus is put on product form models.

One can distinguish three types of product form networks: simple networks proposed by Jacksons[9] and further extended by Gordon and Newell (only with FIFO nodes) and much more complex and adequate to the defined problem, BCMP networks with of centres that may be one of four types (FIFO, PS, IS, LCFS-PR). BCMP networks [3,4] provide us also possibility of defining different classes of incoming customers, described with routing probabilities and service time distributions. It also has to be pointed out that closed multiclass queuing networks are much more difficult to analyse than open ones. Usually some efficient algorithms have to be applied in order to solve a closed complex network [3]. For mentioned reasons, the proposed model is going to be an open queuing BCMP network.

Important factor that has to be taken into account in modelling Web applications behaviours is Web server’s software architecture. Queues and server's algorithms used for ordering and rejecting the requests have to be analysed for creating the analytical model of complex web applications [15]. Web servers are processing many simultaneous tasks delivered in web requests, as only one of them can use resources and the others are obligated to wait for their turn. To avoid endless waiting, they are organised in queues. The general response time seen by the client consists of following components [15]: (1) time that request spends at the physical resource level (such as CPU and disk), (2) time that request spends waiting to use any of the physical resources, (3) time that request spends waiting in a queue for a process or thread to become available to handle the request (4) time consumed by network for distribution of requests.

In the proposed model, we assume the same architecture for all of the tiers. Proposed simplification in server’s software architecture is close to solutions used in real web and application servers. However, the differences in behaviour of database servers are not taken into account. Client's behaviours are also an important factor that should be analysed. Frequencies of some actions, proportions of the various tasks and most repeatedly used scenarios are defining the types and frequency of requests that are coming to the analysed system. In this model we distinguish three types of request, according to amount of tiers they involve in processing (Fig. 1). In this work the assumption is made that one request generates at most one database query and more complex processing scenarios, in which multiple tiers are involved multiple times are

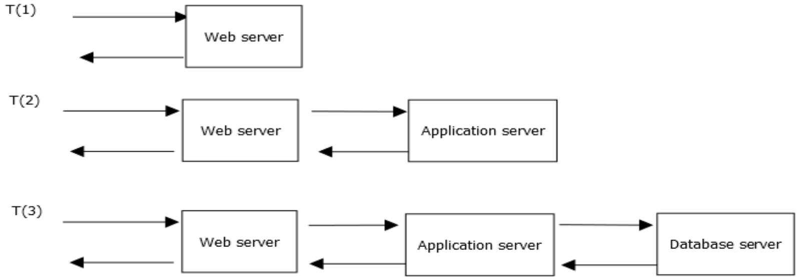


Fig. 1. Proposed queuing model for complex web system

not considered. The division of requests into three types is described with probability that the incoming request belongs to one of them. This parameter should be determined by analysis of the user's behaviours and characteristic of the particular system.

We also assume that the second and third type of requests that are reaching the application and database tiers on their route back are served with higher priority than new incoming requests. This is an generalisation as depending on the server implementation they are either directly reaching the process or thread for serving them or they are put into the preceding queue with high priority.

### 3.2. PROPOSED SOLUTION

Basing on queuing theory we can notice that in order to model the overload we always have to consider the amount of requests in the network and this will usually lead us to the high computational complexity. At this point we decided to propose two steps of calculations. In the first step, calculations that are independent on queuing theory which are modifying the input parameters of the model are made and in the second step this parameters are applied to the formulas retrieved from queuing model.

The queuing network model is presented in Fig 2. The links between stations reproduce the connections between resources of the real system. The model consists of a set of connected service points which stand for servers in multitier architecture. As a simplification the replication of the tiers is not considered. In result no dispatchers are

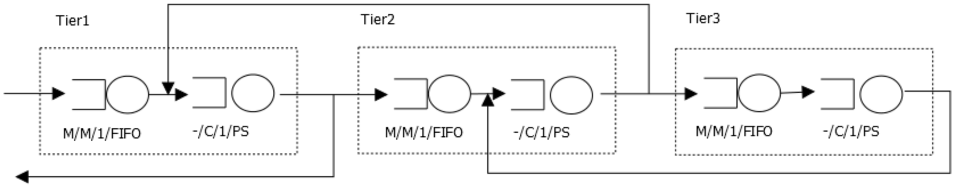


Fig. 2. Queuing network model of multitier web application

needed. However, to make model more adequate to the software architecture of servers each of them is composed of a two queues where jobs wait for a service. An M/M/1/FIFO node is used to represent the FIFO queue for requests waiting for an execution inside server that precedes the access to the circular buffer (-/C/1/PS queue) with access to the processor.

Analogically to model described in [8] three classes of requests where distinguished and described with distribution probabilities: $p_1$, $p_2$, $p_3$. However in this model, as described in subsection 3.1, the assumption is made that the requests of type 2 and 3 on the return route are served with higher priority. To model this property in the return routes the FIFO queues are skipped. The most significant factor that impacts the repose time of each tier is the amount of requests currently processed in the system. Incoming requests after reaching some point of overload are rejected. Therefore, the stream that reaches queues is equal to the real one only to some point of overload after which the queue is full and excessive incoming request are stored in preceding queue or are rejected by the system. Simplifying the behaviour in which the system is recovering for a while after rejecting excessive incoming requests, we can assume that stream that truly flows through the both of queues does not increase anymore after point, in which the load limit is reached. This property of the queues generally is described by following formula, where $\lambda_{\mathrm{exter}}$ is the incoming stream of requests and $\lambda_{\mathrm{overload}}$ is point of overload and $\lambda$ is stream that queue is actually capable to process:

$$\lambda = \begin{cases} \lambda_{\mathrm{exter}} & \text{for } \lambda_{\mathrm{exter}} < \lambda_{\mathrm{overload}} \\ \lambda_{\mathrm{overload}} & \text{for } \lambda_{\mathrm{exter}} \geq \lambda_{\mathrm{overload}} \end{cases}. \tag{1}$$

We assume that incoming stream of requests is a Poisson stream with constant parameter $\lambda_{\mathrm{exter}}$ . In this step of calculations five input parameters are required as presented in Table 1.

Table 1. Input model parameters

| | |
|---|---|
| $p_{1,}p_2, p_3$ | Probability that incoming request belongs to one of three types |
| $\lambda_{\mathrm{exter}}$ [Hz] | External stream of requests that is delivered to the application |
| $\mu_{\mathrm{iPS}}$ [Hz] | An intensity of processing time in PS queue for a tier number i |

One can distinguish two types of internal streams:

$\lambda_{\mathrm{i\ PS}}$ -stream that PS queue is capable to process in the tier number i, includes both newly arriving requests and requests in their routes back. This stream stops growing when the sum of both requests streams (returning and incoming) is bigger than intensity of processing in this queue. The relation between real stream of incoming request (external stream $\lambda_{\mathrm{exter}}$) that is an input parameter of this model and stream $\lambda_{\mathrm{i\ PS}}$ that can flow through the queue according to its processing capabilities and probability that it will reach this queue can be defined as follows:

$$\lambda_{1\ \mathrm{PS}} = \begin{cases} \lambda_{\mathrm{exter}} & \text{for } \lambda_{\mathrm{exter}} < \dfrac{\mu_{1\mathrm{PS}}}{\lambda_{\mathrm{exter}}\,(p_1 + 2p_2 + 2p_3)} \\ \left[\dfrac{\mu_{1\mathrm{PS}}}{\lambda_{\mathrm{exter}}\,(p_1 + 2p_2 + 2p_3)} - 1\right] & \text{for } \lambda_{\mathrm{exter}} \geq \dfrac{\mu_{1\mathrm{PS}}}{\lambda_{\mathrm{exter}}\,(p_1 + 2p_2 + 2p_3)} \end{cases} \tag{2}$$

$$\lambda_{2\ \mathrm{PS}} = \begin{cases} \lambda_{\mathrm{exter}} & \text{for } \lambda_{\mathrm{exter}} < \dfrac{\mu_{2\mathrm{PS}}}{\lambda_{\mathrm{exter}}\,(p_2 + 2p_3)} \\ \left[\dfrac{\mu_{1\mathrm{PS}}}{\lambda_{\mathrm{exter}}\,(p_2 + 2p_3)} - 1\right] & \text{for } \lambda_{\mathrm{exter}} \geq \dfrac{\mu_{2\mathrm{PS}}}{\lambda_{\mathrm{exter}}\,(p_2 + 2p_3)} \end{cases} \tag{3}$$

$$\lambda_{3\ \mathrm{PS}} = \begin{cases} \lambda_{\mathrm{exter}} & \text{for } \lambda_{\mathrm{exter}} < \dfrac{\mu_{3\mathrm{PS}}}{\lambda_{\mathrm{exter}}\,p_3} \\ \left[\dfrac{\mu_{1\mathrm{PS}}}{\lambda_{\mathrm{exter}}\,(p_3)} - 1\right] & \text{for } \lambda_{\mathrm{exter}} \geq \dfrac{\mu_{3\mathrm{PS}}}{\lambda_{\mathrm{exter}}\,p_3} \end{cases} \tag{4}$$

$\lambda_{\mathrm{i\ FIFO}}$ -stream that flows through the FIFO queues, include only newly arriving requests. FIFO queue is capable to process as many incoming requests as it is possible to forward to following PS queue. Having in mind that the requests in returning route are served with higher priority relation analogical to the previous case is defined as follows:

$$\lambda_{1\ \mathrm{FIFO}} = \begin{cases} \lambda_{\mathrm{exter}} & \text{for } \lambda_{\mathrm{exter}} < \dfrac{2\mu_{1\mathrm{PS}}}{(p_1 + 3p_2 + 3p_3)} \\ \dfrac{2\mu_{1\mathrm{PS}}}{(p_1 + 3p_2 + 3p_3)} - 0.1 & \text{for } \lambda_{\mathrm{exter}} \geq \dfrac{2\mu_{1\mathrm{PS}}}{(p_1 + 3p_2 + 3p_3)} \end{cases} \tag{5}$$

$$\lambda_{2\ \mathrm{FIFO}} = \begin{cases} \lambda_{\mathrm{exter}} & \text{for } \lambda_{\mathrm{exter}} < \dfrac{2\mu_{2\mathrm{PS}}}{(p_2 + 3p_3)} \\ \dfrac{2\mu_{2\mathrm{PS}}}{(p_2 + 3p_3)} - 0.1 & \text{for } \lambda_{\mathrm{exter}} \geq \dfrac{2\mu_{2\mathrm{PS}}}{(p_2 + 3p_3)} \end{cases} \tag{6}$$

$$\lambda_{3\ \mathrm{FIFO}} = \begin{cases} \lambda_{\mathrm{exter}} & \text{for } \lambda_{\mathrm{exter}} < \dfrac{2\mu_{3\mathrm{PS}}}{(p_3)} \\ \dfrac{2\mu_{3\mathrm{PS}}}{(p_3)} - 0.1 & \text{for } \lambda_{\mathrm{exter}} \geq \dfrac{2\mu_{3\mathrm{PS}}}{(p_3)} \end{cases} \tag{7}$$

With presented calculations we have estimated the processing capabilities of the queues. However we also have to take into account that requests rejected by the first tier will not be also delivered to the following tiers. What is more, some of the requests that are delivered further may be rejected by the second or third tier. Applying this observation to the model, we can say that internal stream that actually flows through the queues in model are as follows:

$$\lambda_{1\ \mathrm{inter\ FIFO}} = \lambda_{1\ \mathrm{FIFO}} \tag{8}$$

$$\lambda_{1\ \mathrm{intern\ PS}} = \min\{\lambda_{1\ \mathrm{PS}}, \lambda_{1\ \mathrm{FIFO}}\} \tag{9}$$

$$\lambda_{2\ \text{inter FIFO}} = \min\{\lambda_{2\ \text{FIFO}}, \lambda_{1\ \text{PS}}, \lambda_{1\ \text{FIFO}}\} \tag{10}$$

$$\lambda_{2\ \text{inter PS}} = \min\{\lambda_{2\ \text{PS}}, \lambda_{1\ \text{PS}}, \lambda_{2\ \text{FIFO}}, \lambda_{1\ \text{FIFO}}\} \tag{11}$$

$$\lambda_{3\ \text{inter FIFO}} = \min\{\lambda_{1\ \text{PS}}, \lambda_{2\ \text{PS}}, \lambda_{1\ \text{FIFO}}, \lambda_{2\ \text{FIFO}}, \lambda_{3\ \text{FIFO}}\} \tag{12}$$

$$\lambda_{3\ \text{inter FIFO}} = \min\{\lambda_{1\ \text{PS}}, \lambda_{2\ \text{PS}}, \lambda_{3\ \text{PS}}, \lambda_{1\ \text{FIFO}}, \lambda_{2\ \text{FIFO}}, \lambda_{3\ \text{FIFO}}\} \tag{13}$$

In next steps formulas derived from queuing models will be used. Presented formulas are analogical to [8], for three classes of requests T(1), T(2), T(3) defined in model, the average response time for each of the classes is defined.

As each tier consists of two nodes response time of the tier is described as a sum of response time of FIFO and PS node. The first component of the sum in formula (14) is standing for time spent in the FIFO queue the second one for time spent in PS queue. The stream that flows through the FIFO queue include only external incoming requests, stream for the PS queue includes doubled probabilities for types of requests that will visit this queue twice (also in returning route):

$$\mathrm{T}(1) = \frac{1}{\mu_{1\mathrm{F}} - \lambda_{1\ \text{inter FIFO}}(p_1 + p_2 + p_3)} + \frac{1}{\mu_{1\mathrm{PS}} - \lambda_{1\ \text{inter PS}}(p_1 + 2p_2 + 2p_3)} \tag{14}$$

For the second class of requests, the time spent in both web and application tier is summed up (15). As the requests are visiting the PS queue in web tier twice (back and forth) the time spend there is doubled.

$$\begin{aligned}\mathrm{T}(2) = {} & \frac{1}{\mu_{1\mathrm{F}} - \lambda_{1\ \text{inter FIFO}}(p_1 + p_2 + p_3)} + \frac{2}{\mu_{1\mathrm{PS}} - \lambda_{1\ \text{inter PS}}(p_1 + 2p_2 + 2p_3)} \\ & + \frac{1}{\mu_{2\mathrm{F}} - \lambda_{2\ \text{inter FIFO}}(p_2 + p_3)} + \frac{1}{\mu_{2\mathrm{PS}} - \lambda_{2\ \text{inter PS}}(p_2 + 2p_3)}\end{aligned} \tag{15}$$

Formula for the third type of requests is analogical to the previous two, but here time spent in PS queues of two first tiers is doubled and the time in third is added:

$$\begin{aligned}\mathrm{T}(3) = {} & \frac{1}{\mu_{1\mathrm{F}} - \lambda_{1\text{inter FIFO}}(p_1 + p_2 + p_3)} + \frac{2}{\mu_{1\mathrm{PS}} - \lambda_{1\text{inter PS}}(p_1 + 2p_2 + 2p_3)} \\ & + \frac{1}{\mu_{2\mathrm{F}} - \lambda_{2\ \text{inter FIFO}}(p_2 + p_3)} + \frac{2}{\mu_{2\mathrm{PS}} - \lambda_{2\ \text{inter PS}}(p_2 + 2p_3)} \\ & + \frac{1}{\mu_{3\mathrm{F}} - \lambda_{3\ \text{inter FIFO}}(p_3)} + \frac{1}{\mu_{3\mathrm{PS}} - \lambda_{3\ \text{inter PS}}(p_3)}\end{aligned} \tag{16}$$

The general average response time is defined by formula:

$$\mathrm{Avrg}_{\text{response time}} = p_1\mathrm{T}(1) + p_2\mathrm{T}(2) + p_3\mathrm{T}(3)\,. \tag{17}$$

## 4. EXPERIMENTS

Proposed analytical model was validated against measurements derived from experiment. For this purpose a simple test environment was prepared with a use of: two Apache servers configured to run with PHP and the backend database (MySQL) server. Three types of requests are generated as presented in Fig. 1.

To evaluate the proposed model, there were done a set of experiments with different processing intensities. The experiments are carried for following scenarios: equal processing capabilities in each tier (experiment 1), bottleneck in second tier (experiment 2), and bottleneck in first tier (experiment 3). Outcomes of experiments are compared with the characteristics retrieved from the model as presented in Fig 3.

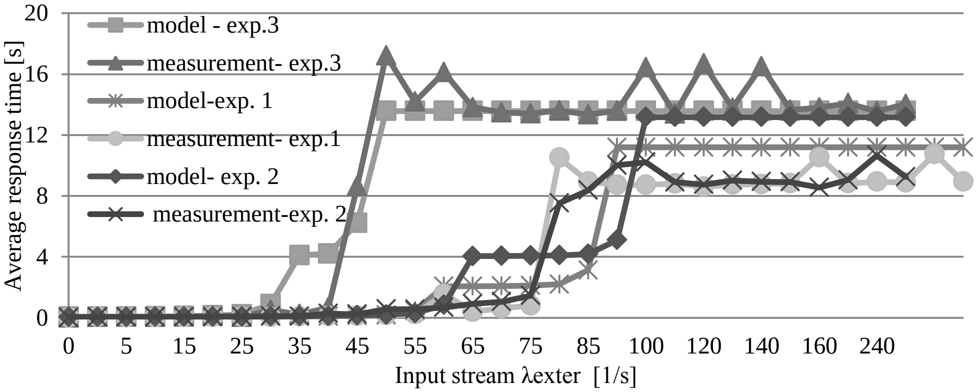


Fig. 3. Mean response time comparison output from measurement and model

## 5. CONCLUSIONS

The proposed analytical model extends the one presented in [8] by capturing the system behaviours in cases of overload and gives results close to behaviour of real 3-tier web system as presented in Fig. 4. It is achieved by describing the relation between amount of incoming requests incoming to the system and its performance including the behaviour after overload of the system. It is based on the observation that stream of requests that flows through the queues grows only to some point after which the excessive requests are rejected. Formulas 2-7 define the stream which queues are capable to process in relation to the incoming stream and probability that requests will reach given tier. Then in formulas 8 - 13 interaction between tiers is taken into account and final streams that flow through the queues are defined. These streams are applied to the formulas 14-16 retrieved from queuing network.

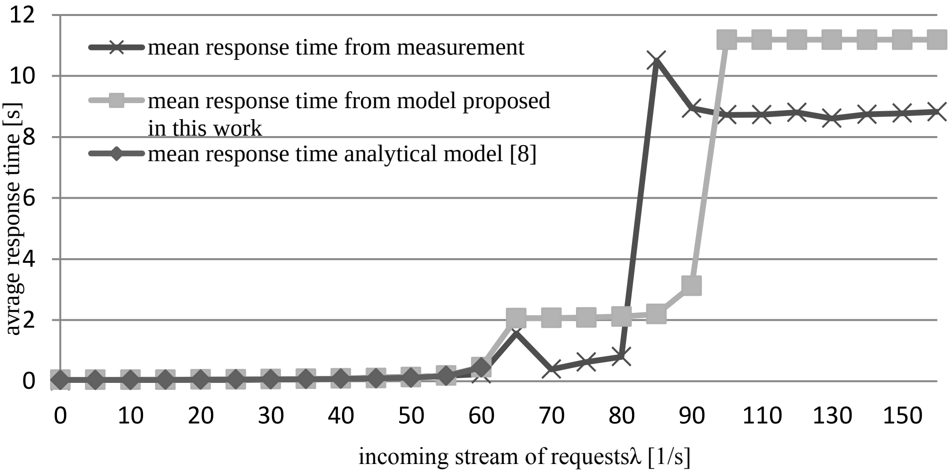


Fig. 4. Mean response time comparison for output form model presented in this work, model from [8] and measurement

Moreover, to make model more adequate to the software architecture of servers each of the tier is composed of a two queues where jobs wait for a service (Fig. 2).

Comparing presented solution to [13,17], it could be stated that the superiority of presented model is a good balance between the accuracy of the retrieved characteristic and the efficiency in model solution. With a really low computational complexity O(1), proposed model gives ability to carry on performance analysis under different model assumptions, avoiding the re-evaluation of the entire model. As the probabilities of requests distribution and service time in PS queues has to be measured, we can say that this model may be applied for an application with a given basic characteristic to check how it will act in case when service time in some tiers will change.

The weakest point of the proposed model is the estimation of overload points. The biggest impact on estimation of this parameter has inaccuracy in estimation the processing capabilities of PS queues. Another drawback is that it applies well in cases where bottleneck of the system is in the first tier or the processing time in all of them are similar. This problem may be solved by further modifications on input stream that will take into account interactions between the tiers in cases when next required in processing tier is full or behaviours such a waiting for the return of requests from following tiers. What is more, rejections of requests are considered in relation to the processing capabilities of the server for given stream of incoming requests per second. This considerations may be enriched with taking account also limit of clients on the server.

ACKNOWLEDGEMENT

The work was supported by the Polish National Science Centre under grant no. N N516 475940.

## REFERENCES

[1] ANDERSSON M., CAO J., NYBERG K., KIHL M., *Web Server Performance Modeling Using an M/G/l/K*PS Queue*, In: 10th International Conf. on Telecommunications, Vol. 2., 2003, 1501–1506.

[2] ANDERSSON M., CAO J., KIHL M., NYBERG C., *Performance Modeling of an Apache Web Server with Bursty Arrival Traffic*, In: Proceedings of the 4th International Conference on Internet Computing, Las Vegas, Nevada, 2003, 508–514.

[3] BALSAMO S., *Product Form Queueing Networks.* In: Performance Evaluation: Origins and Directions, Dept. of Math. And Computer Science University of Udine, Italy, 377–401.

[4] BALSAMO S., *Queueing Networks with Blocking: Analysis, Solution Algorithms and Properties,* In: LNCS, Vol. 5233, 2011, 233–257.

[5] BUCHMANN A., KOUNEV S., *Performance modeling and evaluation of large-sacle J2EE applicaitons,* In: Computer Measurement Group's International Conference, 2003, 273–283.

[6] DOYLE R. P., CHASE J. S., ASAD O. M, WEI J., VAHDAT A. M., *Model-Based Resource Provisioning in a Web Service Utility,* In: Proceedings of the 4th conference on USENIX Symposium on Internet Technologies and Systems, Vol. 4, 2003. 5–5.

[7] GRAHAM G. S., LAZOWSKA E. D., SEVCIK K. C.,ZAHORJAN J., *Quantitative System Performance, Computer System Analysis Using Queueing Network Models*, Prentice-Hall, 1984.

[8] IMIEŁOWSKI A., *Analytical Model of Multitiered Internet Applications with the Use of BCMP Queueing Networks*, In: Information Systems Architecture and Technology. Web Information Systems: Models, Concepts and Challenges, Vol. 39, 2008, 113–124.

[9] Jackson J., *Jobshop-Like Queuing Systems*, Management Science, Vol. 10, 1963, 131–142.

[10] KAMRA A., MISRA V., NAHUM E. M., *Yaksha: A Self-Tuning Controller for Managing the Performance of 3-Tiered Web sites*, In Proc. of the Twelfth IEEE International Workshop on Quality of Service, 2004, 47–56.

[11] KARLAPUD H., MARTIN J., *Web application performance prediction*. In: Proceedings of the IASTED International Conference on Communication and Computer Networks, 2006, 281–286.

[12] KIRTANE S., MARTIN J., *Application Performance Prediction in Autonomic Systems*. In: Proceedings of the 44th annual Southeast regional conference, 2006, 566–572.

[13] LIU X., HEO J., SHA L., *Modeling 3-Tiered Web Services,* In: Proceedings of the 13th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, 2006, 307–310.

[14] LIU X., HEO J., SHA L., *Adaptive Control of Multi-Tiered Web Application Using Queueing Predictor*. In: Network Operations and Management Symposium, 2006, 106–114.

[15] MENASCÉ D., *Web Server Software Architectures*, Internet Computing, Vol. 7, No. 6, 2003, 78–81.

[16] SLOTHOUBER L., *A Model of Web Server Performance*, In: Proceedings of the 5th International World Wide Web Conference, 1996.

[17] URGAONKAR B., PACIFICIY G., SHENOY P., SPREITZERY M., TANTAWI A., *An Analytical Model for Multi-tier Internet Services and Its Applications*, Performance Evaluation Review, Vol. 33, No. 1, 2005. 291–302.

[18] WALKOWIAK T., *Web server performance and availability model for simulation*, Journal of Polish Safety and Reliability Association, Vol. 3, No. 2, 2012, 189–196.

# PART 2

# TRAFFIC MANAGEMENT
AND PROCESSING

*Wireless Mesh Networks,*
*routing, WMN, metrics*

Piotr OWCZAREK*, Piotr ZWIERZYKOWSKI*

# ROUTING PROTOCOLS IN WIRELESS MESH NETWORKS - A COMPARISON AND CLASSIFICATION

Wireless Mesh Networks can give an answer for many open issues in the field of wireless networks. For WMN to be effective enough, it is required for a chosen routing protocol based on routing metrics that fits application needs to be used properly. Until now, many different routing protocols have been proposed. All of them have their own characteristics and there is no easy way to make any reliable comparison. The proposed paper presents a review of the current state-of-the-art WMN routing protocols and metrics. The paper also includes an evaluation of properties and proposed classification of WMN routing protocols.

## 1. INTRODUCTION

Wireless mesh networks, commonly known as MESH networks, have come a long way over the past years and their popularity is soaring. One of the main contributing factors for their growing popularity is the necessity to provide broadband access to the Internet. This is particularly evident in areas where no appropriate cabling infrastructure is provided, or where costs of building such an infrastructure would exceed potential resulting benefits.

A significant part of routing protocols in Wireless Mesh Networks (WMN) has been imported from Ad-Hoc networks (e.g. AODV and DSR protocols). These protocols are based on the simplest metrics, based on the number of hops in feasible paths, that are well-suited for the Ad-Hoc network, but are not particularly effective in MESH networks, because they do not take into account the quality of the link as well as the differences in technologies used in the networks in question. In the face of these differences and limitations, it is necessary to include in the consideration other routing metrics, specific to mesh networks, that would make any development of new

* Poznan University of Technology, Faculty of Electronics and Telecommunications, Chair of Communications and Computer Networks, Polanka 3, 61-131 Poznań

routing protocols, or a modification of existing protocols, possible. Such protocols must also satisfy a number of requirements, i.e. scalability, provision of routes without loops, speed of response to possible changes in the topology of the network, security, QoS issues and optimization of energy consumption.

The article is divided into four sections. Section 2 presents a description of the architecture of MESH network and the metrics used in routing protocols in MESH. Section 3 includes a presentation of those selected routing protocols that are then compared in the following section 3. Finally, Section 4 provides a summary of the results and the conclusions of the study.

## 2. WIRELESS MESH NETWORKS

### 2.1. INTRODUCTION

MESH networks guarantee the connectivity through a multihop wireless backbone formed by stationary routers and thus provide connectivity between mobile and stationary (landline) users and are frequently used to provide access to the Internet. Wireless Mesh Networks offer many advantages such as, for example, fast and easy extension of the system, self-configuration ability, self-healing aspect, elasticity, large territorial range, better and easier area coverage (as compared to IEEE 802.11 a/b/g/n), large throughput, reliability (a failure in a single point (node) is not followed by a failure in the whole of the network) and energy conservation. Regrettably, no standard has been worked out yet and hence available solutions are most frequently incompatible with one another.

Lack of appropriate routing protocols suitable for mesh networks is still an important problem. Since those metrics that are known from protocols for the Ad-Hoc network cannot be applied to mesh networks, any process of designing new protocols is substantially hindered. Therefore, a development of appropriate metrics has become an important stage in research studies aimed at working out new protocols.

### 2.2. METRICS USED IN WIRELESS MESH NETWORKS

The metrics that have been proposed for mesh networks can be divided as follows [2,3]:

- metrics related to the number of hops (Hop Count),
- metrics that determine the quality of a connection (Link Quality Metrics),
- metrics that are based on network load rate (Load-Dependant Metrics),
- Multi Channel Metrics.

The Hop Count Metrics is the oldest type of metric that has been used in the RIP protocol since the inception of the Internet. More attention should be given then to the remaining metrics. One can distinguish seven metrics based on the link quality [4]: Expected Transmission Count (ETX)[5], Minimum Loss (ML) [8], Expected Transmission Time (ETT) [5], Expected Link Performance (ELP) [5], Per-Hop Round Trip Time (RTT), Per-Hop Packet Pair Delay (PPD) and Expected Transmission on a Path (ETOP). Load-Dependent Metrics include: Distribution Based Expected Transmission Count (DBEXT) and Bottleneck Aware Routing Metric (BATD). The following multi-channel metrics stand out among other multi-channel metrics: Weighted Cumulative ETT (WCETT), Metric of Interference and Channel-switching (MIC) [6], Modified ETX (mETX) [11] , Effective Number of Transmissions (ENT) [11], iAWARE – [12] and Exclusive Expected Transmission Time (EETT) [13]. Table 1 shows the comparison of the selected characteristics of metrics used in the majority of routing protocols for wireless mesh networks. Results presented in the table were obtained by the authors from literature studies and the characteristics are given based on [3] and [7].

Table 1. A comparison of main routing metrics

| Name of Metric | Quality-aware | Data Rate | Packet Size | Intra-flow Interferences | Inter-flow Interferences | Medium Instability |
|---|---|---|---|---|---|---|
| Hop Count Metrics | | | | | | |
| Hop | ✗ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Link-Quality Metrics | | | | | | |
| ETX | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| ML | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| ETT | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ |
| ELP | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ |
| RTT | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| PPD | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ |
| ETOP | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| Load-Dependent Metrics | | | | | | |
| DBEXT | ✓ | ✗ | ✗ | ✓ | ✗ | ✓ |
| BATD | ✓ | ✓ | ✗ | ✓ | ✗ | ✗ |
| Multi-Channel Metrics | | | | | | |
| WCETT | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |
| MIC | ✓ | ✓ | ✓ | ✓ | ✓ | ✗ |
| mETX | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ |
| ENT | ✓ | ✓ | ✓ | ✗ | ✗ | ✓ |
| iAWARE | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| EETT | ✓ | ✓ | ✓ | ✓ | ✗ | ✗ |

## 2. ROUTING PROTOCOLS IN WIRELESS MESH NETWORKS

Routing protocols in wireless mesh networks can be divided into two categories: proactive and reactive [1]. Proactive protocols involve a situation where network nodes continuously maintain one, or a number, of routing tables that store routes to each of the nodes of a network and, at the same time, recurrently send them along the network to exchange and update information in neighboring nodes. Reactive protocols, in turn, receive information on the route to the destination (node) of a packet only at the moment when data transmission is to be effected (on demand). These protocols do not generate additional traffic in the network, but the time needed for data to be forwarded is prolonged by the time necessary to effect the exchange of information concerning the available route.

Another classification of the protocols that takes into account their particular features is proposed in [9]:

- Hop Count Based Routing – protocols based the on metrics of the hop-count type. Though these protocols do not in fact indicate the most effective connection paths, they are still in common use due to their low computational complexity.
- Link-Level QoS Routing – this group includes protocols that use the cumulative or the bottleneck value that defines the quality of the connection path (or section thereof).
- End-to-End QoS Routing – these protocols are based on the quality parameters, but in a global approach, i.e. for the end-to-end connection path.
- Reliability-Aware Routing – protocols based on the assumption of the availability of a number of simultaneous routes. In this group of protocols, depending of available implementation, packets are sent concurrently along a number of routes, or alternative routes are used only as an auxiliary solution.
- Stability-Aware Routing – protocols grouped in his category use a special architecture of the system to improve the stability of the operation of a network. These protocols prefer cable connection links in MESH networks or links in which no sections (segments) that are executed via mobile users are included.
- Scalable Routing – protocols for large networks where scalability is pivotal. The most typical representatives of this category are the hierarchical and the geographical routing.

The classification of routing protocols proposed by the authors is presented further on in the paper.

### 2.1 HOP COUNT BASED ROUTING PROTOCOLS

The group of the Hop Count Based Routing protocols includes:

- Light Client Management Routing Protocols (LCMR) **[9].** In this protocol, the destination routing path from the sender to the receiver between routers in the network is selected in the proactive way, whereas the path between clients and the routers of the network in the reactive way. In order to determine the best route, the hop-count metric is used. In this protocol, the functionality of routing is based exclusively on routers. To achieve that, routers service two routing tables: one for local clients of the network, the other for clients and remote routers. On the basis of the information they store, destination routing paths are selected. The instance of servicing two tables, however, is followed by a significant usage of resources.
- Orthogonal Rendezvous Routing Protocols (ORR) [19]. The operation of this protocol is based on the assumption that in the two-dimensional Euclidean space two orthogonal lines have at least two common points with a group of other orthogonal lines. In the process of finding a route, the source node sends a route discovery

packet in the orthogonal directions, while the destination node sends a route dissemination packet. The packets meet in a node called the rendezvous point. In this way, the end-to-end routing path is established in which the segment from the source to the rendezvous point is a reactive route, whereas the other part is a proactive route. This protocol requires a strict description of the directions towards the nodes of a network.

- HEAT Protocol [20]. The HEAT protocol uses distribution of temperature. The protocol adopts that each of the nodes of a network is a source of heat. The assumption is that gateways are the warmest, followed by nodes/clients that in the closest vicinity, and that the further from gateways, the temperature becomes lower and lower. Using the temperature distribution, the protocol always sends packets to a neighboring node that has the warmest temperature, thus reaching the destination.
- Dynamic Source Routing Algorithm (DSR) [23]. DSR is one of the most commonly used routing protocol in WMN networks and belongs to the group of unicast reactive protocols. The protocol uses source routing, which results in the knowledge of the whole of the destination routing path by any packet. The operation of the protocol occurs in the two consecutive stages: the route discovery phase and the route maintenance phase. The first, initiated by the source node, involves sending broadcast packets that include the destination address, the source address and a unique id to neighboring nodes. If the packet is received by a node that is not a destination node, this node adds its address to the header and then forwards the packet according to the same scheme. Thus, a packet that has reached its destination has in its header information on the end-to-end connection path. On the basis of information carried in the header, intermediate nodes collect information on routing paths. In the second phase, nodes supervise updated information on stored routes by generating error packets (RERR) forwarded towards the source node. When such a packet is received, a given router is removed from the database and further process proceeds in line with the phase one described earlier.
- Ad-Hoc On-Demand Distance Vector Routing Algorithm (AODV) [21]. The AODV protocol belongs to the most popular protocols because they employ simple mechanisms of the type “question - reply” to define routing paths. For this purpose, three types of packets are used: Route Request (RREQ), Route Reply (RREP) and Route Error (RERR). The source node sends RREQ packets when a necessity to send packets arises and then intermediate nodes, provided they know the route, send a RREQ packet further on towards the destination node, whereas when intermediate nodes do not know the route, they reply with a RERR packet. This process is then repeated until the packet reaches the destination node (the node sends then a RREP packet). In the case when the node receives RREQ packets from different routes, then the route along which the packet has reached the node as first is selected.

### 2.2. LINK LEVEL BASED ROUTING PROTOCOLS

Link-Level QoS Routing protocols include:

- Link Quality Source Routing Protocol (LQSR) [22]. A reactive routing protocol proposed by Microsoft Research Group that is based on the Dynamic Source Routing (DSR) algorithm. To improve the quality of the link, the LQSR protocol employs single link parameters instead of end-to-end path parameters. In the process of setting a connection path, the protocol describes individual links by the quality metric, and then sends back the information to the node that initiates the setting up of the path. Quality parameters may vary depending on the mobility of nodes and metrics used in the process, e.g. for stationary nodes they may include strictly quality parameters such as ETX, while for mobile nodes this can be a hop-count based parameter such as RTT and ETX. Though the protocol has many advantages, it is still necessary to develop more appropriate routing metrics that would take into account the specificity of the WMN network and the features of the LQSR protocol [9].
- Multi-Radio LQSR Routing Protocol (MR-LQSR) [22]. A protocol based on LQSR that takes into consideration the use of the multi-radio architecture in WMN networks. This is effected by the application of WCETT metrics that take into account both quality parameters of the link and the minimum number of hops. This protocol makes it possible to achieve the expected equilibrium (balance) between the delay and the throughput by selecting channels of best quality with a diversity of radio channels taken into account. The protocol also allows researchers to effectively compensate load among individual radio channels.
- ExOR Routing Protocol [23]. This protocol is based on broadcasts from the source to the receiver without setting up a direct routing path. Forwarding of packets is done in batches from the source node to selected intermediate nodes. Intermediate nodes themselves choose which one of them will be the node that will forward the packet in the next stage of transmission. This decision depends on the cost of the link based on the ETX metric. The ExOR protocol is based on broadcasts and therefore only the parameter related to the probability of reaching the goal by the packet is taken into consideration. The choice of nodes to be involved in particular stages of the process is, in turn, executed on the basis of the packet loss ratio (PLR) between the source node and the nodes involved. In the course of the process, many nodes can receive packets from the source node and hence it is necessary to select such nodes that can become nodes forwarding packets. It is in this group of nodes that a node with the highest priority is selected and it is just this node that will be responsible for packet (batch) forwarding (according to the procedure described above). The process is completed when 90 % of packets in each batch is received by the destination node, while the remaining 10 % of packets is resent again in line with the protocol based on the number of hops.

- AODV – Spanning Tree Protocol (AODV-ST) [22]. This protocol has been specially designed for WMN networks that use a multi-radio architecture and is based on the AODV protocol. The special feature of the AODV-ST is hybrid routing, which means that it employs AODV mechanisms for internetwork routing in WMNs and Spannig Tree (ST) between the network and edge routers. In short, AODV-ST makes advantage of proactive routing between nodes of the network and routers, and reactive routing with nodes of the internal WMN network. The AODV-ST protocol uses the ETT metric taking into account the expected time for a given packet traversing the link necessary to reach its destination.
- BABEL Routing Protocol [14]. BABEL is a proactive protocol based on the distance-vector routing protocol. During the process of selection of tracks, it takes advantage of some historical information available, including the error statistics for individual links. Within this process, links that have been used earlier and their quality satisfies the assumed criteria are favored in selection. The BABEL protocol performs simultaneously updating of the state of neighboring nodes (in the reactive way) and can make an exchange of routing information (e.g. following a failure of a link) effective.
- Better Approach To Mobile Ad Hoc (B.A.T.M.A.N.) [15]. A proactive protocol that shows a different approach to the selection of a connection path. Here, nodes find only the appropriate (adequate) link towards the source without taking into consideration the end-to-end route. Data are forwarded to the next node along the route, while the procedure is repeated according to the same assumption. The process is regarded to be completed when the destination node is reached. Each of nodes recurrently sends broadcasts to let the neighboring nodes about its existence. The neighboring nodes forward this information on until all the nodes in the network receive appropriate information on the other nodes in the network.

### 2.3. END-TO-END QOS ROUTING

End-to-End QoS Routing protocols include the following protocols:

- Quality Aware Routing Protocol [22]. This protocol makes it possible to maintain a given loss ratio along the end-to-end connection path through appropriate use of the ETX and ENT metrics. During the selection process of feasible connection routes, the number of retransmissions is checked and then this number is compared with the maximum admissible value in the protocols of the link layer. So long as the ENT value is higher than the admissible value, the link cost is deemed as infinitely high. At the same time, the ETX metric is also used to estimate the cost of individual links and, following that, links that do not satisfy the assumed parameters are eliminated from the connection route. The most important in this protocol is to determine boundary quality parameters related to packet loss along the end-to-end route.

- RingMesh Routing Protocol [9]. The protocol is based on the Token Ring protocol for wireless LAN networks. The protocol assumes that many concurrent rings are emerging to maintain a secure service of the WMN network with a large number of hops. Individual rings are implemented in the direction from the gateway to the rest of nodes, similarly as in the case of the Spaning Tree. Another assumption is that neighboring rings use different radio frequencies. The ring that spans the gateway is treated as the root ring, whereas other rings are the so-called child rings. Individual rings always include a common node called the pseudo gateway. Subsequent nodes of the network implement further rings created according to the procedure described above and to the transmission delay criterion opposite the source node.

## 3. COMPARISION OF ROUTING PROTOCOLS IN WMN

An unequivocal comparison of all the routing protocols presented in Section 2 is not possible due to their particular, individual-oriented features, as well as due to their different approach to the issue of routing determination methods (reactive and proactive protocols). Because of this, it is mainly comparisons of protocols representing the same group of protocols, or comparisons of protocols that are based on similar assumptions, that are to be found in the literature. Another approach to making a comparison of protocols involves their evaluation in view of objective features, i.e. delay, packet loss, overhead and throughput. Yet another approach involves a comparison of the protocols with regard to some defined features, for example, scalability, reliability of operation and traffic balancing.

In [9], Akyildiz presents a comparison of structural features of groups of protocols included in his study and discusses their main features that indicate potential areas of application of the protocols in relation to required parameters.

Table 2. Characteristic features of particular groups of routing protocols [9]

| Lp | Category of routing protocols | Features |
|---|---|---|
| 1 | Hop-count routing | Simple in routing metric; easy to be integrated with complicated schemes of routing path selection |
| 2 | Link-quality based routing | A certain metric for link quality is used to select routing path |
| 3 | Interference based routing | Interference or contention is directly considered in routing |
| 4 | Load-balanced routing | Congestion or network capacity is explicitly considered |
| 5 | Stability based routing | Stability has higher priority |
| 6 | End-toEnd QoS Routing | End-to-end QoS is ensured |

The authors of [16] and [17] attempt, in turn, to systematize the characteristic features for routing protocols and then to compare them element by element. Table 3 shows the comparison of the selected protocols, made by the authors, based on literature studies. Regrettably, it is not possible to make a viable comparison of all the presented protocols. However, it is worthwhile to mention here that the bulk of available comparative studies is based either on theoretical considerations or simulation models. In contrast, results obtained in real systems are not available and, in fact, it is such results only that would be comprehensive enough to render all features of any natural environment.

An interesting approach to the issue of the methodology employed in this kind of a comparison, as well as the resulting conclusions are presented in [18]. The authors present a description of the test environment, procedures employed in the study and conclusions related to a study of four routing protocols: AODV, OSLR, BABEL and B.A.T.M.A.N. The experiments conducted by the authors were aimed at providing essential data for a comparison of the above protocols and for a selection of the best protocol with regard to a given test scenario, which in the end clearly indicates an additional dimension of difficulties for researches in making comparisons of different protocols.

Table 3. Comparison of characteristic features of selected routing protocols

| Protocol | Type | Hello | Routing metrics | Loop free | Scalability | Reliability | Load balancing | Throughput | Congestion Control |
|---|---|---|---|---|---|---|---|---|---|
| DSR | reactive | No | shortest path | Yes | No | Yes | No | Decreases as mobility increases | No |
| AODV | Reactive | Yes | fastes & shortest path | Yes | No | Yes | No | Poor for more than 20 mobile nodes | No |
| LQSR | Reactive | Yes | Hop Mount, RTT, ETX | Yes | No | Yes | Yes | Yes | Yes |
| MR-LQSR | Reactive | Yes | Hop Mount, RTT, ETX | Yes | No | Yes | Yes | Yes | Yes |

## 4. CONCLUSIONS

This article presents an overview of a number of selected metrics used in routing protocols, as well as routing protocols for WMN networks. Additionally, a comparison of selected protocols on the basis of available sources in the literature is presented.

The authors introduce a division of metrics into categories with regard to particular features of the metrics. All metrics under consideration have been grouped within the following groups: Hop Count Metrics, Link–Quality Metrics, Load-Dependent Metrics and Multi-Channel Metrics.

In addition, the article includes another division of routing protocols grouped within the following categories; Hop Count Based Routing Protocols, Link Level Based Routing Protocols and End-To-End QoS Routing. It is worthwhile to notice that the above three categories are by no means exhaustive and, as a result, only some selected protocols are presented due to the complexity of this many-faceted problem. During the selection process of protocols, the popularity and common use of protocols were decisive in their inclusion.

The main authors' goal was to find features of all described protocols and their metrics which could be used in the objective comparison of the selected routing protocols and metrics. The presented article shows a comparison of described protocols on the basis of the literature of the subject and requires further simulation studies, which will constitute the next stage of the research.

## REFERENCES

[1] ROYER E.M., TOH C.K., *A review of current routing protocols for ad hoc mobile wireless networks,* Personal Communications, IEEE, 1999, 6.2: 46-55.

[2] ENTEZAMI F., POLITIS C., *Routing protocol metrics for wireless mesh networks*, Wireless World Research Forum, 2013.

[3] MOGAIBEL H.A., OTHMAN M., *Review of Routing Protocols and It's Metrics for Wireless Mesh Networks,* Conf. on Computer Science and Inf. Technology-Spring, 2009, 62-70.

[4] DE COUTO, Douglas S.J., et al. *A high-throughput path metric for multi-hop wireless routing*, Wireless Networks, 2005, vol. 11, no. 4, 419-434.

[5] DRAVES R., PADHYE J., ZILL B., *Routing in multi-radio, multi-hop wireless mesh networks,* Annual Int. Conf. on Mobile Computing and Networking, 2004, 114-128.

[6] YANG Y., WANG J., KRAVETS R., *Designing routing metrics for mesh networks*, IEEE Workshop on Wireless Mesh Networks, 2005.

[7] CAMPISTA M., Elias M., et al. *Routing metrics and protocols for wireless mesh networks*. Network, 2008, vol. 22, no.1, 6-12.

[8] PASSOS D., at al. *Minimum loss multiplicative routing metrics for wireless mesh networks*. Journal of Internet Services and Applications, 2011, vol. 1, no. 3, 201-214.

[9] AKYILDIZ I., WANG X., *Wireless mesh networks*. Wiley, 2009.

[10] ASHRAF U., ABDELLATIF S., SJUANOLE G., *An interference and link-quality aware routing metric for wireless mesh networks*, Vehicular Technology Conference (VTC-Fall), 2008, 1-5.

[11] KOKSAL C.E., BALAKRISHNAN H., *Quality-aware routing metrics for time-varying wireless mesh networks*. J. Selected Areas in Communications, 2006, vol. 24, no.11, 1984-1994.

[12] SUBRAMANIAN A.P., BUDDHIKOT M.M., MILLER S., *Interference aware routing in multi-radio wireless mesh networks.* In: 2nd Workshop on Wireless Mesh Networks, 2006, 55-63.

[13] JIANG W., et al. *Optimizing routing metrics for large-scale multi-radio mesh networks*, Int. Conf. on Wireless Communications, Networking and Mobile Computing, 2007, 1550-1553.

[14] CHROBOCZEK J., *The Babel routing protocol*, RFC 6126 (Experimental). Inter-net Engineering Task Force, Apr. 2011. URL: http://www.ietf.org/rfc/rfc6126.txt.

[15] http://www.open-mesh.org/projects/open-mesh/wiki

[16] RAO, S. Siva Nageswara; KRISHNA, YK Sundara; RAO, K. Nageswara, *A Survey: Routing Protocols for Wireless Mesh Networks*, IJRRWSN, 2011 vol. 1, no. 3.

[17] SRIKANTH V., JEEVAN A.C., AVINASH B., KIRAN T.S., BABU S.S., *A Review of Routing Protocols in Wireless Mesh Networks (WMN)*, Int. J. of Comp. Applications, vol. 1, no. 11, 2010.

[18] FRIGINAL J., et al. Towards *benchmarking routing protocols in wireless mesh networks*, Ad Hoc

Networks, 2011, vol. 9, no. 8, 1374-1388.

[19] CHENG, Bow-Nan; YUKSEL, Murat; KALYANARAMAN, Shivkumar. *Orthogonal rendezvous routing protocol for wireless mesh networks*, IEEE/ACM Transactions on Networking (ToN), 2009, 17(2), 542-555.

[20] BAUMANN, Rainer, et al. *HEAT: Scalable routing in wireless mesh networks using temperature fields,* World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium on a. IEEE, 2007, 1-9.

[21] PERKINS, Charles E.; ROYER, Elizabeth M. *Ad-hoc on-demand distance vector routing,* Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop on. IEEE, 1999, 90-100.

[22] CAMPISTA, Miguel Elias M., et al. *Routing metrics and protocols for wireless mesh networks,* Network, IEEE, 2008, 22(1), 6-12.

[23] JOHNSON, David B.; MALTZ, David A. *Dynamic source routing in ad hoc wireless networks,* Kluwer International Series in Engineering and Computer Science, 1996, 153-179.

[23] BISWAS, Sanjit; MORRIS, Robert. *ExOR: opportunistic multi-hop routing for wireless networks,* ACM SIGCOMM Computer Communication Review. ACM, 2005, 133-144.

*SOM, unsupervised learning, IDS,*
*network traffic, anomaly detection*

Łukasz BURDKA*, Katarzyna NIŻAŁOWSKA*,
Michał ADAMSKI*, Grzegorz KOŁACZEK*

# SOM-BASED SYSTEM FOR ANOMALY DETECTION IN NETWORK TRAFFIC

We present a system for anomaly detection in network traffic that takes advantage of a Self Organizing Map. The aim of the system is to perform analysis of network data and find patterns that indicate occurrences of malicious activities. There are many approaches to the problem of anomaly detection and although supervised learning or rule-based systems may be very accurate when trained properly, they lack usefulness when there is no classified training data for the network where such a system operates. Nature of computer networks vary and some anomalies may not yet be classified. Our method allows identification of suspicious network activity even if there is no knowledge of previous anomalies. In other words it is capable of working with unclassified data. In this project SOM is used to cluster traffic data and visualize it in a way that is convenient for human to analyze. A number of tools for manual analysis of clustered network traffic data is introduced. A set of methods for semi-automatic selecting regions containing probable network intrusions is proposed. The system provides a promising way of detecting large groups of similar anomalous activities as well as regions where rare but distinguishing anomalies may occur.

## 1. INTRODUCTION

### 1.1. MOTIVATION

Anomaly detection is an important issue in modern computer networks design. Continuous delivery of reliable and secure services over the network is the basis of functioning of many companies. Such services can suffer from various Internet at-

* Faculty of Computer Science and Management, Wrocław University of Technology, Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland, e-mail: lukasz.burdka@pwr.wroc.pl, katarzyna.nizalowska @student.pwr.wroc.pl, michal.adamski@student.pwr.wroc.pl, grzegorz.kolaczek@pwr.wroc.pl,

tacks. Among which network scans, worms and DDoS can be distinguished. Serious network disruptions can be detected or even prevented by a reactive Intrusion Detection System, built using our approach.

### 1.2. RELATED WORK

Different methods of coping with anomaly detection exist already. There are many systems suggested. However most of them are based on much more complicated structures and frequently require some level of supervision. In [1] hierarchical SOM based IDS is presented. In that paper, multi-layer SOM-based system is described. Such an idea has proven itself to be useful in other applications and authors tried to employ it to detect network intrusions. However, presented solution depends on data labels in the learning process. The structure of the system changes, depending on feedback indicating the current structure effectiveness. It is impossible to asses misclassification rate in unknown network traffic and thus it is not possible to use such a system in real-life application as the live data is unlabeled. We compare our solution with existing ones using Performance Metrics defined in [1].

Also [5] and [6] use Self Organizing Maps to solve the problem of anomaly detection. Both of those systems, however, utilize large structures of SOM hierarchies, making the application very complex.

In [4] an IDS similar to ours is presented. It uses only unlabeled data to detect intrusions, but authors utilize different clustering technique. Their system is based on Sub-Space Clustering and Multiple Evidence Accumulation. As we've shown in section 3.3 our method yields results at least as good as above approaches, still maintaining simple structure of the system.

### 1.3. OUR APPROACH

We present a novel approach for anomaly detection in network traffic. Our system is based on simple, one-layer SOM, with fully unsupervised learning process. As a result, it can be used to distinguish normal and abnormal traffic without any data labels. Additionally, it is highly adaptive and can be optimized to be either highly sensitive with a great *Detection Rate* or to ensure minimum *False Alarm Rate*.

We suggest two different approaches to construct a robust IDS, utilizing the approach we have described. Since our system is capable of finding anomalies in large data sets, it can be used to detect intrusions from past network logs, recorded over a certain amount of time. This ability can be used to label the data and use it as a training set for any classifier. It can also be utilized by our system itself to perform online analysis of any incoming traffic in real time.

## 2. SYSTEM DESCRIPTION

### 2.1. FRAMEWORK

The system takes advantage of a single-layer Self Organizing Map. Output is analyzed automatically in order to detect anomalous regions. The application not only presents the result of anomaly detection, but also provides a support for manual visual analysis of clustered data. The processing framework is as follows.

1. The dataset is chosen where each instance represent an entry from a network log.
2. Dataset is loaded to the application and attributes are selected.
3. Parameters are chosen and SOM is trained on the whole dataset.
4. Each instance is bound to the fittest neuron.
5. Instances bound to neurons that form suspicious clusters are marked as anomalies.
6. Instances bound to neurons that highly distinguish themselves from the rest are marked as anomalies.

Such an approach allows finding single anomalies as well as large groups of anomalous traffic. The output is presented on an interactive 2D image which allows verification of recognized anomalies and convenient analysis of patterns that occur in the dataset. Once the detection phase is completed a human can take advantage of developed analytical tools to examine patterns present in data.

### 2.2. METHODOLOGY

As a first step the SOM is trained in a standard manner. The set of instances *I* is processed by a matrix of neurons *N*. When the process ceases and all instances are bound to fittest neurons, prototypes of all neurons are calculated. For neuron *n*, its prototype $p_n$ is a vector, which coordinates are calculated as an arithmetical average of all instances bound to that neuron. The prototype is defined as follows

$$\rho_n = \sum_{k=1}^{|I_n|} i_k * \frac{1}{|I_n|} \tag{1}$$

Where $I_n$ is the set of instances bound to neuron *n*.

Based on the observation that the anomalous instances are highly more similar to each other than normal activities are, we utilize the Euclidean distance between prototypes as one of determinants, which regions should be marked as anomalies. The above statement is true for each class separately, since anomalies also differ between different classes. The distance between neurons $n_i$ and $n_j$ will later be referred to simply as a prototype distance and denoted by $d_{ij}$. The maximum distance for neuron $n_i$ will be denoted by $d\_max_i$.

The application visualizes the prototype distance for each neuron. Analysis of this visualization led to another important observation. Even if the prototype distance between neurons, representing one anomaly class, differ slightly, their distribution of prototype distances to all neurons in the map remains, in general, the same. This distribution, however, changes rapidly outside of the analyzed class. Therefore for each neuron $n_i$, a meta-prototype is calculated as a vector of a size equal to the total number of neurons. Each coordinate $j$ represents a neuron $n_j$ and has a value equal to the prototype distance between neurons $n_i$ and $n_j$. The meta-prototype of neuron $n_i$ will be denoted by $\pi_\mathrm{i}$ and defined as

$$\pi_i = (d_{i1}, d_{i2}, ..., d_{i|N|}) \tag{2}$$

The Euclidean distance between meta-prototypes of neurons $n_i$ and $n_j$ will later be referred to as the meta-distance and denoted by $\delta_{ij}$.

The maximum meta-distance for neuron $n_i$ will be denoted as $\delta\_max_i$. The meta-distance is the second determinant, used while deciding, which regions should be marked as anomalies. Since the meta-distance is also visualized, the process of finding anomalous clusters can be very efficiently performed by a human (see Fig. 2.). However, to enable automatic analysis of network data we propose a heuristic approach of finding anomalous regions of data placed in our SOM. To explain it, we introduce two additional concepts; region denoted as $R$ and meta-region denoted by $P$. Region and meta-region for neuron $n_i$ are defined by formulas

$$R_i = \{n_j : d_{ij} < d\_max_i * 0.1\} \tag{3}$$

and

$$P_i = \{n_j : \delta_{ij} < \delta\_max_i * 0.1\} \tag{4}$$

respectively.

This, however, applies only to neurons placed in the direct neighborhood of neuron $n_i$ or its neighbors, which also satisfy this criterion. This leads to creations of regions not only close to $n_i$, by means of distance and meta-distance, but also close spatially. For each neuron we can also designate the intersection of its region and meta-region and denote it by $\Lambda$. A union of the region and meta-region will be denoted by $L$. These properties of the neuron $n_i$ are defined as

$$\Lambda_i = R_{ni} \cap P_{n_i}, \tag{5}$$

$$\mathrm{L}_i = R_{n_i} \cup P_{n_i} \tag{6}$$

The neuron $n_i$ can form the anomalous cluster $\Xi$, only if the size of $\Lambda_i$ is larger than one. If so, the anomalous cluster is initially formed by the sum of $\Lambda_i$ and $\Lambda_j$ of each other neuron $n_j$ from $\Lambda_i$. Anomalous cluster $\Xi$ is subsequently extended by the addition of those neurons that exist in every $L$ of neurons already in $\Xi$. In other words, all neurons that are sure to be in $\Xi$ need to agree that the additional neuron fits in their anomalous cluster. For neuron $n_i$, its anomalous cluster is calculated, using the following two-step procedure

$$\Xi_i^1 = \Lambda_\mathrm{i} \cup \{\mathrm{n_j} : \mathrm{n_j} \in \Lambda_\mathrm{k}, \mathrm{n_k} \in \Lambda_i\}, \tag{7}$$

$$\Xi_i = \Xi_i^1 \cup \{\mathrm{n_j} : \forall_{\mathrm{n}_{\mathrm{k}\in\Xi_\mathrm{i}^1}} \mathrm{n_j} \in \mathrm{L_k}\}, \tag{8}$$

This way clusters grow from neurons that have their own regions and meta-regions. One neuron can belong only to one cluster and therefore those already clustered are not checked in further process. This approach leads to high precision in finding anomalies but needs to be extended by a method of finding single anomalies that do not form clusters. An observation has been made that these single anomalies are usually bound to neurons that are very far from other neurons. Especially by means of the meta-distance. Therefore we propose a following method of finding single anomalies: At first, we calculate the average sum of meta-distance of each neuron to all other neurons in SOM. Generally, the neurons that are above the average are considered suspicious. The sensitivity threshold is a value, set somewhere between the average and maximum sum of meta-distances. Depending on its choice, the system is biased to either detect more rare anomalies as a trade-off for higher false positive rate or to detect only large anomaly clusters and the strong outliers. The sensitivity threshold can be a value from range [0,1] and is denoted by σ. The neuron $n_i$ is considered a single anomaly if it satisfies the following condition

$$\Delta i > \Delta\_max - (\Delta\_max - \bar{\Delta}) * \sigma, \tag{9}$$

where $\Delta_i$ is sum of meta-distances from neuron $n_i$ to all other neurons, $\Delta\_max$ is maximum value of $\Delta$ from all SOM, and is an average value of all in SOM.

The relationship between sensitivity threshold and overall results is further explained in section 3.3. It should be chosen with respect to priorities of the particular use case of the system.

# 3. EVALUATION

## 3.1. EXPERIMENTAL SETUP

In our experimental work we use a 10% subset of KDD Cup 1999 Data set. The set consists of 494015 instances, described by 41 features and divided into 23 classes, including 22 attack types and one class, representing normal network activity. Full description of this data can be found in [2].

In order to properly evaluate results of experiments, we compare following quality measures; accuracy, precision and recall. Those measures are calculated from a confusion matrix obtained for two classes. First one, labeled ‘normal’, containing normal network activity and the second, named ‘anomaly’ containing all remaining classes and indicating anomalous activity.

To test quality of the system, we conducted a series of experiments. During the first experiment, we changed the size of the self organizing map to check, how the quality of anomaly detection is related to SOM dimensions. The second experiment was prepared to detect the impact of changing the sensitivity threshold on values of our quality measures. The last experiment tests, if the growth of epoch number implies the rise in the overall quality of anomaly detection.

## 3.2. EXAMPLE

Before presenting experimental results, we introduce the visualization example, comparing real classes of all instances and anomalies found by our system. As we can see in Fig. 1. on the left hand side, learned self organizing map is presented.

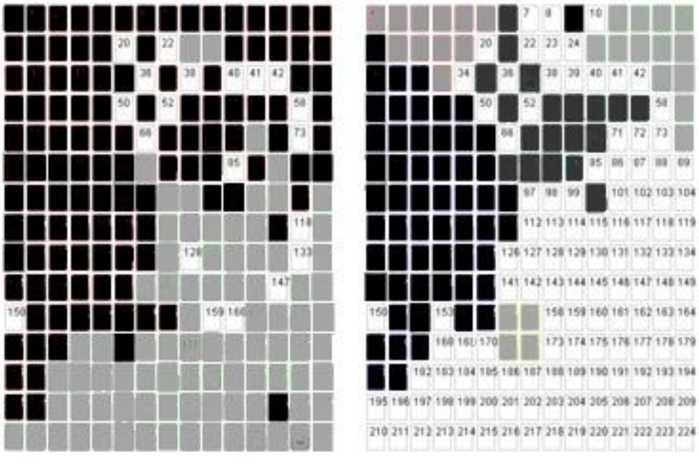


Fig. 1. Comparison of real classes distribution (left) and anomaly clusters, detected by our system (right)

Light grey (originally green) neurons contain instances of class ‘normal’ and black (originally red) neurons contain anomalous instances. Meanwhile on the right, we can see neurons, marked by our system as containing instances of anomalous network traffic.

Each shade of grey (originally different colors) in the right image represents one anomalous cluster and the single black neuron refers to a single anomaly. As we can see, the result is highly accurate. Anomaly division into different clusters coincides with the distribution of the different intrusion types.

Another image (Fig. 2.) is given to present a visual representation of meta-distance and its correlation with traffic activity type. The darker the color is, the smaller the meta-distance between given and selected neuron is.

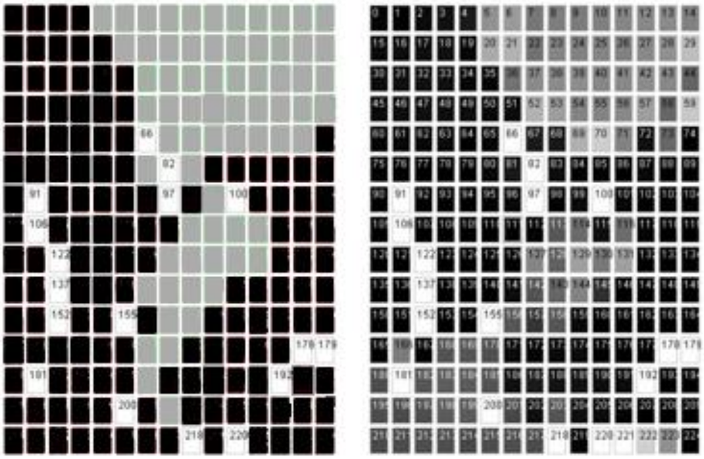


Fig. 2. Comparison of real classes distribution (left) and visual representation of meta-distance (right)

It is clearly visible that the meta-distance between neuron 111, containing anomalous traffic is much smaller to other anomalous neurons than to neurons, containing normal traffic.

Knowing this property, our program is also a convenient tool for manual analysis of traffic activity data.

### 3.2. EXPERIMENTAL RESULTS

Results of experiments, described in the previous section are presented in tables below.

Table 1. The impact of SOM dimensions on the quality of anomaly detection

| Map size | Precision | Accuracy | Recall |
|---|---|---|---|
| 10x10 | 98,185% | 97,027% | 98,113% |

| | | | |
|---|---|---|---|
| 15x15 | 96,553% | 95,511% | 97,905% |
| 20x20 | 96,528% | 95,727% | 98,211% |
| 25x25 | 94,910% | 94,450% | 98,365% |

The test was performed with varying SOM size and constant sensitivity (50%) and epoch number (50). As we can see, the size of the SOM does not influence the recall. However, using too large neural network can lead into decrease of accuracy and precision. This effect can be caused by the loss in meta-distance significance, when calculated for large networks, since its values are more uniform as the size of SOM increases.

Table 2. The result of sensitivity threshold changing

| Sensitivity | Precision | Accuracy | Recall |
|---|---|---|---|
| 0% | 100,000% | 90,844% | 88,598% |
| 15% | 99,995% | 97,667% | 97,100% |
| 25% | 98,463% | 96,918% | 97,687% |
| 50% | 96,553% | 95,511% | 97,905% |
| 90% | 96,389% | 94,969% | 97,384% |

Considering results of the previous test, this experiment was run with the SOM size 15x15 and number of epochs equal 50. Results presented in the Table 2 match our expectations. The lowest sensitivity implies highest precision but results in decrease of recall. However, when the sensitivity is high enough, recall stabilizes but precision continues dropping so overall accuracy starts to decrease from some point. Thus the best sensitivity value, maximizing all three indicators is 15%.

Table 3. Relation of number of epochs and detection quality

| Number of epochs | Precision | Accuracy | Recall |
|---|---|---|---|
| 10 | 99,384% | 97,727% | 97,775% |
| 20 | 98,122% | 96,259% | 97,202% |
| 30 | 99,999% | 98,454% | 98,076% |
| 40 | 99,986% | 98,169% | 97,734% |
| 50 | 99,995% | 97,667% | 97,100% |

The last experiment, which results are presented in Table 3 was held with 15x15 SOM and sensitivity threshold equal 15%. The aim was to examine the impact of epoch number on anomaly detection quality, represented by precision, accuracy and recall. As we can see, results of the experiments indicate that the number of epochs, contained in range of 10 to 50 does not have any meaningful relation with quality of anomaly detection.

### 3.3. RESULT DISCUSSION

To complete the evaluation, it must be said that during the tests, we noticed that vast majority of the false-positive classified instances were misclassified because at SOM learning phase, they have been placed in neurons also containing anomalies. Therefore it cannot be considered as totally wrong decision, since otherwise it would lead to decrease in the detection rate. Despite this issue, the results achieved by our system are fully satisfying. It can be proven by comparing our results to previous works, described in [4] and [1].

While our system can raise the detection rate up to 99.7%, keeping the false positive rate at 0.01%, when it is tuned properly, the system from [1] achieves 90.94% - 93.46% detection rate with FP rate in range of 2.19% - 3.99%. At the same time, the system from [4] was able to detect anomalies at the rate of 90% and FP rate below 3.5%. In average situations, when precise tuning up is impossible, our system manages to detect at least 97% of anomalies, keeping FP rate always below 3%.

It is also worth mentioning that our system is capable of tuning to either very high precision or the detection rate, depending on expectations and requirements of a specific case.

## 4. SUMMARY

### 4.1. CONCLUSION

IDS we presented is a novel system that have many advantages over other existing approaches. It takes advantage of sophisticated and accurate clustering technique and uses simple, but effective algorithm to discover network anomalies and intrusions. Our system uses only unlabeled data and thus can be utilized in real life applications. No assumptions about data distribution or traffic signature are made. The introduced heuristic approach was inspired by observations of nature of the network traffic, made using graphical tools, contained in our application.

System design makes it possible to detect any type of anomaly, even those yet unknown. IDS we proposed can be optimized to either be very sensitive, detecting almost all anomalies or to ensure no false positives detection. When parameters are tuned up, the performance on 10% KDD CUP 99 dataset is outstanding, detecting 99.7% of attacks with 0.01% false positive rate. However, the nature of SOM isn’t completely deterministic and therefore results may vary slightly.

### 4.2. FUTURE WORK

At the moment, the method of finding anomalies in previously gathered data is developed and the tool for data visualization and analysis is made. To allow its application as a part of a real intrusion detection system, a few work still needs to be done.

Primarily, there is a need to study a possibility of automatic selection of all parameters of the process and using our method in a semi-supervised IDS. Promising results of our system, used without any supervision suggest that that solution should be highly effective.

Another direction of research should be an analysis of ways for real-time data collection and passing it to our system.

To improve the effectiveness of our method, some more study need to be done for tuning up parameters, describing the SOM learning phase. This work would result in the decrease of the misclassification rate, caused by placing anomalous and normal instances in the same neurons.

## REFERENCES

[1] GUNES KAYACIK H., NUR ZINCIR-HEYWOOD A., HEYWOOD M. I., *A hierarchical SOM-based intrusion detection system,* In: Engineering Applications of Artificial Intelligence, Vol. 20 No. 4, June, 2007, 439-451.

[2] HETTICH S., BAY S. D., *The UCI KDD Archive.* , Irvine, CA: University of California, Department of Information and Computer Science. World Wide Web URL: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, 1999.

[3] ŻURADA J., BARSKI M., JĘDRUCH W., *Sztuczne sieci neuronowe,* Warszawa, Wydawnictwo Naukowe PWN 1996.

[4] CASAS P., MAZEL J., OWEZARSKI P., *Unsupervised network intrusion detection systems: Detecting the unknown without knowledge,* In: Computer Communications, Vol. 35 No. 7, April, 2012, 772-783.

[5] ZOLOTUKHIN M., HÄMÄLÄINEN T., JUVONEN A.. *Growing Hierarchical Self-Organizing Maps for Online Anomaly Detection by Using Network Logs*. Simulation, 2012, 2: 6.

[6] LICHODZIJEWSKI, P., A., *Network-Based Anomaly Detection Using Self-Organizing Maps*. IEEE Network, 1994, 8.5: 26-41.

*model-based verification & validation (MVV), multi-level security (MLS), specialized computer systems (SCS), security-design models, model-driven security*

Zbigniew ZIELIŃSKI*, Andrzej STASIAK*, Łukasz LASZKO*

# VERIFICATION OF SOME PROPERTIES OF MULTI-LEVEL SECURITY SYSTEM ON THE BASE OF MODEL SIMULATION

In the paper the approach to some aspects of multi-level security (MLS) systems verification on the base of Bell-LaPadula and Biba models is presented. The essence of the proposed approach to analyze properties of MLS security-design models and their instances is models integration and their evaluation and simulation. “Separability” problem of different security domains is considered and a method for its verification is proposed. The feasibility of the proposed approach by applying it to the example MLS project is demonstrated.

## 1. INTRODUCTION

Verification and validation methods deliver important analytical techniques for security assurance. Formal verification and validation methods may be used to increase dependability of software artifacts. The problem is especially important in construction of dependable multi-level security (MLS) systems.

Processing the data with different levels of sensitivity is particularly important for governmental, military or financial institutions. The problem of designing of dependable MLS systems has been extensively studied since the early 70s of the twentieth century [1–3]. Various multilevel security models (MLS) have been created to enforce confidentiality and integrity of data. Some of the more popular models are Bell-LaPadula (BLP) Model [1–2], Biba Model [3], Lipner’s Integrity Matrix Model and Clark-Wilson Model [4]. Lattice-based access control is one of the essential ingredients of computer security [5].

In a system development process, the security is usually considered as a non-functional requirement, but unlike other nonfunctional requirements, such as reliability

* Military University of Technology, ul. gen. Sylwestra Kaliskiego 2, 00-908 Warsaw, Poland

and performance, security has not been fully integrated within the development lifecycle and it is still mainly considered after the design of the system [6]. In the MLS systems security requirements introduce not only quality characteristics but also constraints under which the system must operate. Ignoring such constraints during the development process could lead to serious system vulnerabilities. The UML security models could be embedded in and simulated with the system architecture models, thus the security problems in MLS system can be detected early during the software design.

The basic idea of integrating system design models (expressed usually in UML) with security considerations was presented in [6-13]. In [7] a method of software design of MLS-type systems called MDmls has proposed. This method is based on MDD (Model Driven Development) approach [13]. The essence of the MDmls method is integration of the MLS security models with the system design models expressed in UML-based language [14-15].

One of the possible approach to the construction of a centralized (i.e., no distributed) computer system with multi-level security is to develop software in the virtualization technology [14-15] for the separation of in-dependent security domains. In this kind of systems "secure isolation" between the security domains of a shared resources of computer system is needed. Similar problems we could observe in the cloud infrastructure with multi-level security. One of the significant problems in the development of MLS systems is to prove of "separability". This problem lies at the interface of the hardware and software components. So, we extend the security-design models with the topology models [16] that allow binding of hardware and software components of the MLS system.

We see our contributions as follows. We proposed the way of integration of the MLS models with a topology model [16] that allow binding of hardware and software components of the MLS system. We show the feasibility of this approach by applying it to a non-trivial example: MLS security policy and security-design models verification of the Secure Workstation for Special Application (SWSA) Project with the use of IBM RSA tool.

The rest of the work is organized as follows. In Section 2 we describe our general approach to security modeling in MLS systems. In Section 3 we propose the way of hardware description with topologies model. In Section 4 we describe an example of MLS security models verification on the base of the model simulation. In Section 5 we draw conclusions.

## 2. GENERAL APPROACH TO SECURITY MODELING IN MLS SYSTEMS

In [15] we propose MlsML language, which in current implementation enables creating MLS lattice models, through which it is possible to investigate the effects of different policies using.

In the formal MLS model, the entities in an information system are divided into subjects and objects, all subjects and objects are labeled with a security level. The levels represent the relative sensitivity of the data and the clearance of the user on whose behalf the subjects are operating. For semantic reasons of model building the security level of subjects and objects will be distinguished.

Let $C = \{c_1, c_2 \ldots, c_L,\}$ denote the ordered set of clauses which represent sensitivity of data used in the MLS system, where $c_i \leq c_{i+1}$ for $1 \leq i < L$. Let $IC = \{\theta_1, \theta_2 \ldots, \theta_C,\}$ be the set of categories of information processed in the system.

For each subject $s \in S$ we assign a security level $SL(s)$ as a pair $< c_s, A_s >$ and for each of object $o \in O$ we assign a security level $SL(o)$ as a pair $< c_o, A_o >$, where $c_s$, $c_o \in C$ and $A_s, A_o \subseteq IC$. Security levels can be compared. It could be noticed that not all pairs of levels are comparable. This leads to the use of the concept of lattice of security levels.

A dominance relationship $dom(s, o)$ may be introduced between subject $s \in S$ with $SL(s) =< c_s, A_s >$ and object $o \in O$ with $SL(o) =< c_o, A_o >$, if $SL(s) \geq SL(o)$. It can be expressed as the formula:

$$dom(s, o) \Leftrightarrow (c_s \geq c_o) \wedge (A_o \subseteq A_s). \quad (1)$$

The BLP model is based around two main rules: the simple security property and the star property [1,2]. The simple security property (ss-property) states that a subject $s \in S$ can read an object $o \in O$ if the formula (1) is hold. The simple security property prevents subjects from reading more privileged data. The star property (*-property) states that a subject can write to an object, if subject is dominated by object.

Inspired by the work [12] we proposed our own language (meta)model MlsML and achieved formalization of restrictions for the specific BLP and Biba models [15]. Our proposal relates mainly to possible formalization of restrictions in the OCL language, towards the relationship between the users (subjects), facilities, privileges, performed actions and certain states of the system. Contrary to the work [9], which also proposes its own tool that implements proposed methodology, we have based our solution on a typical CASE environment that has appropriate support for the UML models validation process (actually DSL) in the "starting" defined OCL limitations and UML models (expanded by the semantic action language). Our approach has been validated in the IBM RSA tool with Simulation Toolkit and Extension for Deployment Planning (for hardware modeling).

The approach to properties analysis of MLS security-design models and their instances leads to the evaluation and simulation. The integration of security models with models of systems described in UML, and the topology model [16] enables the simulation, which allows to verify/test the security properties of the designed MLS system software or/and the security policy models at the stage of analysis and modeling.

A secure system can be defined as a system that supports a specified set of policies. In the MLS approach, we support multiple high level policies as BLP or Biba and policy of domains separation secure. The basic aspects of our security policies can be defined in terms of the following provisions: (1) data isolation; (2) a limited provision for access to other domain's information - only if it is in compliance with the BLP or/and Biba policy; (3) shared resources of the system must be cleansed between security domain context switches. Verification of separability of security domains is reduced to test conditions (1) and (3) taking account both the representation of software components and hardware for specific scenarios of use. Thus, to enable the examination of such conditions it is necessary to formulate a MLS system description at the component-level hardware and software architecture and its integration with the description of the behavior of the system.

In the article the method of MLS system description using domain-specific language extensions (DSL) was proposed.  For the description of software domain the MlsML profile [7,15] of the UML language was  used and for the description of hardware domain an extension of topology language from IBM [16] was proposed. This approach allowed to describe both hardware and software at the appropriate the level of detail for it to present the allocation of software components to specific hardware components. The integration of  hardware and software components models and the behavior of the system made it possible to perform simulation tests which allow you to confirm or exclude the domain separability property.

Let us consider the problem of testing the separability of security domains on the example of Secure Workstation for Special Applications[1] (SWSA) [14]. In SWSA Project the approach to the construction of a centralized computer system with multilevel security by developing software with the use of the virtualization technology was used, which allows  for the separation of independent security domains, called the Multiple Independent Levels of Security. SWSA system allow for the simultaneous launch of several specific instances of operating systems on one host (such as a workstation or server) designed to process data of different classification levels (eg, public or confidential).

We assume that the system under consideration consists of some types of resources from the ordered set $R = \{R_1, R_2, R_3, R_4, R_5\}$, where $R_1, R_2, R_3, R_4, R_5$ denotes accordingly processors' cores, memory  segments (banks), input/output channels, graphic cards and hard discs.

[1] Project No. OR00014011 supported by The Polish National Center for Research and Development

Let $Proc = \{1,..,n\}$ and $Mem = \{1,..,m\}$ denote, accordingly, the set of processors numbers and memory segments numbers in the system. Let each of processors consists of $r$ cores.

Matrix $B = [b_{ij}]_{n \times m}$ describes an access of processors to the memory segments in such way that $b[i,j] = 1$ iff $i - th$ processor has direct access to the memory with number $j$ and $b[i,j] = 0$ otherwise.

In the system we have the set of images of virtual machines treated as objects $VMI = \{vmi_1,..,vmi_k\}$. The function $SL: VM \rightarrow C \times 2^{IC}$ define security levels assigned to virtual machines i.e. each of $vmi_i \in VMI$ is assigned a pair $(c_i, A_i')$, where $A_i' \subseteq IC$. We assume that in the MLS system may be a set of concurrently running virtual machines $VM = \{vm_0, vm_1,..,vm_\kappa\}$, which of them constitutes a separate security domain with assigned $SL(vm_i)$; $vm_0$ is the home operating system with the virtual monitor manager (VMM) application.

Let Policy(x) [17] will be a function that returns the set of memory segments numbers from which information can flow into the specified segment x and Contents(x) determines the data values stores in the specified memory segment(s), and Current_Domain defines the relevant state of the current executing $\mathrm{vm_i}$.

On the base of results presented in the work [17] we can state that a MLS system is separation secure if the following holds:

```
For all vmᵢ ∈ VM, for any pair of states, s1 and s2, of the composite system
And for every memory segment, seg, of the virtual machine:
if
    Contents (Policy(seg)) in s1 = Contents (Policy(seg)) in s2
    Current_Partitions of seg in s1 = Current_Partitions of seg in s2 /\
    Contents seg in s1 = Contents seg in s2
then
    Contents seg in (top-step s1) = Contents seg in (top-step s2)
```

In order to ensure separability of security domains, VMM has to implement appropriate algorithm of hardware resources allocation. Further we limit our consideration only to the verification of the resource allocation algorithm.

A virtual machine $vm_i$ might request resources which will be represented by a vector $Req_i$, a value $Req_i[j] = l$ for $j \in \{1,..,|R|\}$ means that it is necessary to allocate for virtual machine $vm_i$ $l$ units of a resource type $R_j$.

A current core processors allocation we will describe by a matrix $CP = [cp_{ij}]_{n \times r}$ and $cp[i,j] = l$ in the case when core j of i-th physical processor was assigned to virtual machine with the number $l$ i.e. $(vm_l)$.

When s-th virtual machine is started, the procedure $Alloc(Req_s, i)$ of allocating cores of i-th physical processor is carried out if following conditions (2-3) of separation of virtual machines (MLS domains) are hold i.e.:

$$Run(vm_s) \underset{\phi}{\rightarrow} Alloc(Req_s, i)$$

$$\phi\text{: } (\exists i \in Proc\ |\{j\colon cp[i,j]=0\}| \geq Req_s[1]) \wedge \tag{2}$$
$$\wedge\ [\exists j \epsilon \{1,..,r\}\ cp[i,j]=l] \Rightarrow [\,SL(vm_l)=SL(vm_s)]$$

or

$$(\exists i \in Proc\ \ \forall j \in \{1,..,r\} :\ cp[i,j]=0) \wedge\ (Req_s[1] \leq r) \tag{3}$$

Similarly, conditions of separation due to memory allocation in physical memory segments might be formulated. However, it can be easily observed that if each of memory banks can be accessed directly only by one processor (by a channel) i.e. when $\forall j \in \{1,..,m\}\ \sum_{i=1}^{n} b[i,j]=1$ then constrains of domains separation due to memory allocation are equivalent to (1).

*Example 1.*

Let $R=\{Pcores, Mseg, Chan, Gcards, Hdisks\}$ and $Proc=\{1,2\}$, $r=4$, $Mem=\{1,2\}$. Assuming each processor have assigned one memory bank we obtain $B=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$. Let there will be three virtual machines $VM=\{vm_1, vm_2, vm_3\}$ and $\overline{Req_1}=[3,1,1,1,1]$, $\overline{Req_2}=[2,1,1,1,1]$, $\overline{Req_3}=[2,1,1,1,1]$. Further we consider the case when $SC(vm_1)=(confidential\,,\{\alpha,\beta,\gamma\})$, $SC(vm_2)=(confidential\,,\{\alpha,\gamma\})$, $SC(vm_3)=(restricted,\{\alpha,\gamma\})$. Initial allowable system resources $R$ are depicted by a vector $Z_0=[8,2,2,2,3]$. Thus if the first virtual machine $vm_2$ is started the procedure $Alloc(Req_2, i)$ for $i=1$ is executed and two cores of the processor number 1 are allocated for $vm_2$ and current core processors allocation will described by the matrix

$$\mathrm{CP}=\begin{bmatrix}2 & 2 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix}.$$

If the next started virtual machine will be $vm_3$ the condition (1) is not hold thus the procedure $Alloc(Req_3, i)$ for $i=2$ will be executed (because of condition (3)).

## 3. HARDWARE DESCRIPTION WITH TOPOLOGIES MODEL

Resources of SWSA which were used in the Example 1 (see chapter 2) have been described as elements of topology, suitable for modeling hardware. These elements have been defined as the palette (Fig. 1) – for specialized DSL language for topology models [16].

The proposed approach to analyze resources of SWSA as the elements of topology, together with their description, has been developed as a plugin, which is attached to IBM RSA environment. Switching this plugin on enables new palette with topology elements which are an important component of the constructed simulator. Complete set of available topology units of SWSA are presented in the Fig. 1.

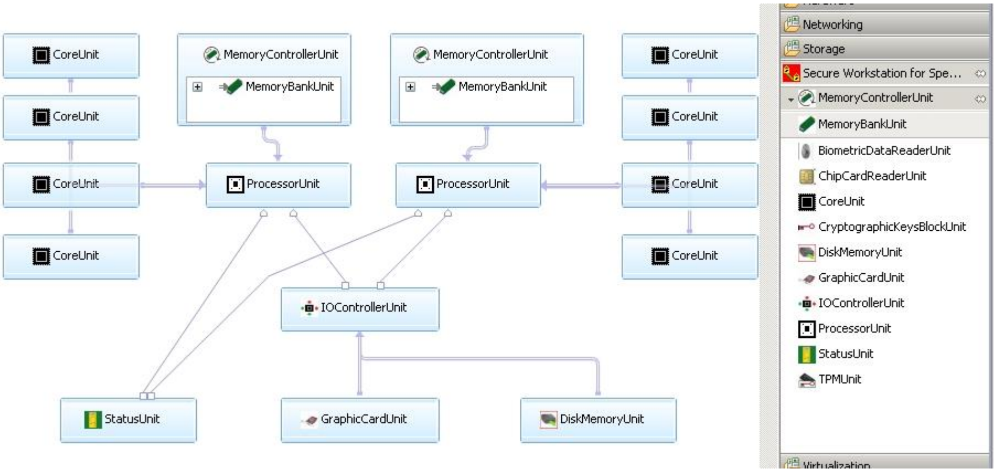


Fig. 1. Sketch topology model of SWSA and his topology palette

Allocation decisions, as referred to the Example 1, were mapped in the topology, by binding software components to hardware units: the VM2: one ProcessorUnit, two CoreUnit(s), one MemoryBankUnit, one GraphicCardUnit and one DiskMemoryUnit, and for other VMs in the same way according to defined resources requirements (Fig. 2b).

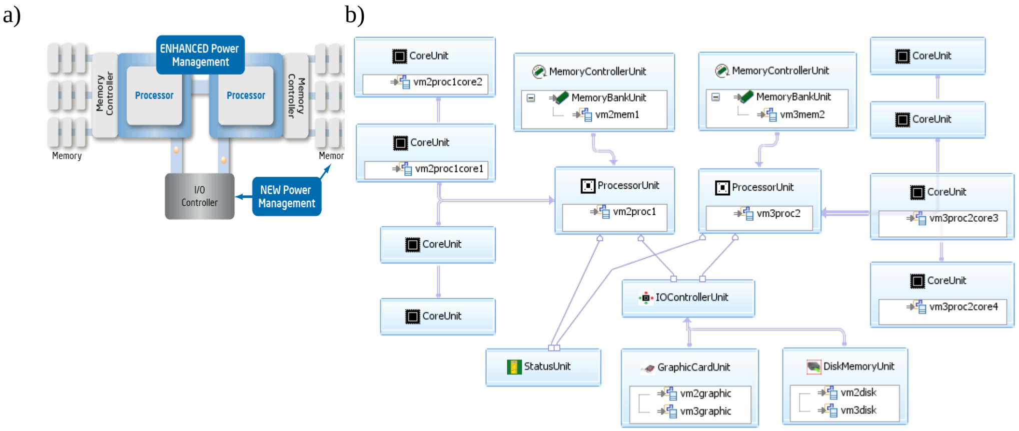


Fig. 2. Block diagram of the system based on the Xeon processor 5600 series (a) and its representation in the topology model (b)

The result of the hardware design is SWSA topology model, which can be examined for compatibility with the defined rules (e.g. At least one Core must be hosted on ProcessorUnit, Number of cores must be the power of 2, etc.).The allocation of resources given in the example is verified using simulation, as described in Chapter 4.

## 4 CASE STUDY: A SECURITY MODEL VERIFICATION AND SIMULATION

In the following part of work, we will present an example to illustrate the use of the proposed method for the construction of the MLS security policy used in the SWSA project.

The main difficulty of the proposed approach to the verification of compliance with the rules of the MLS by Virtual Machine Monitor (VMM) was the development of a simulator. The simulator should allow not only to verify the compliance security policy, but also should make it possible to validate the correctness of the design of VMM (i.e. separation of resources, see section (2)).

Simulator is based on the capabilities of IBM Rational Software Architect 8.5: Simulation Toolkit 8.5 [19-21] and Extension for Deployment Planning [16]. Both of these capabilities enabled the authors to make the MlsML language profile as well as the palette of topology elements for SWSA which create the *framework* of the simulator. Based on this framework a simulator that can examine algorithms of VMM monitor, can be built.

The construction process begins with creating hardware model of SWSA, which we present in the topology diagram. In such diagram not only units and relations are included, but also its correctness rules (checked online, live). The construction of simulator ends with the creation of software model (components of SWSA), and its binding with the topology model (hardware) - manually or using drag and drop method.

An example of using the simulator, as a reference to Example 1 is as follows: *Create an input to the simulation process* (as that defined in (2)); *Develop fragments of VMM behavior model* (which is the subject of the simulation); *Run simulation session*; *Select VMM scenario*; *Control the course of the simulation and collect its history* (Fig. 4); *Analyze the history of changes in status of resources, software components, and the state-word of the simulation* - SSS; *Develop report* (the output form simulation should clearly confirm of compliance with the security policies and separability (or lack thereof).

Let us to analyse the scenario which was shown in the Fig. 3. The process of running of the virtual machine on the base of the virtual machine image $vmi_j, j\epsilon\{1,2,...,$ K} with defined security context $sc(vmi_j)$, by the subject (user) $u_i$ with defined security level $sl_i$ we will describe as $u_i \xrightarrow{RUN} vmi_j$. The process running of the virtual machine (subject) will be generated on the basis of the image $vm_{j_k}$, and its current security level ($csl$) for a subject $vm_{j_k}$ will be defined as a pair $\langle clause,\ infCat\rangle$) from the following dependency:

$$csl := \langle min\left(Clause(sl(u_i)), Clause\left(sc(vmi_j)\right)\right),\ InfCat(sl(u_i)) \cap InfCat\left(sc(vmi_j)\right)\rangle \tag{4}$$

where $InfCat(e)$ is the set of information categories of the element $e \in U \cup VMI$.

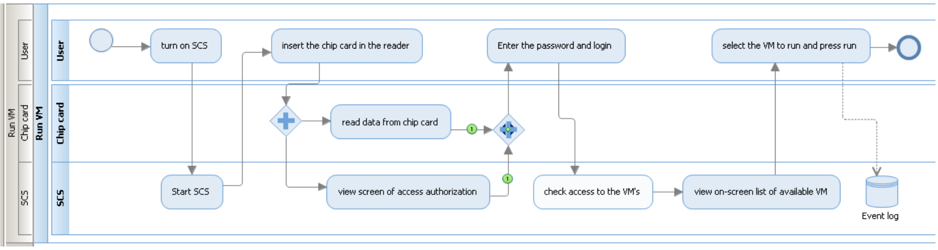
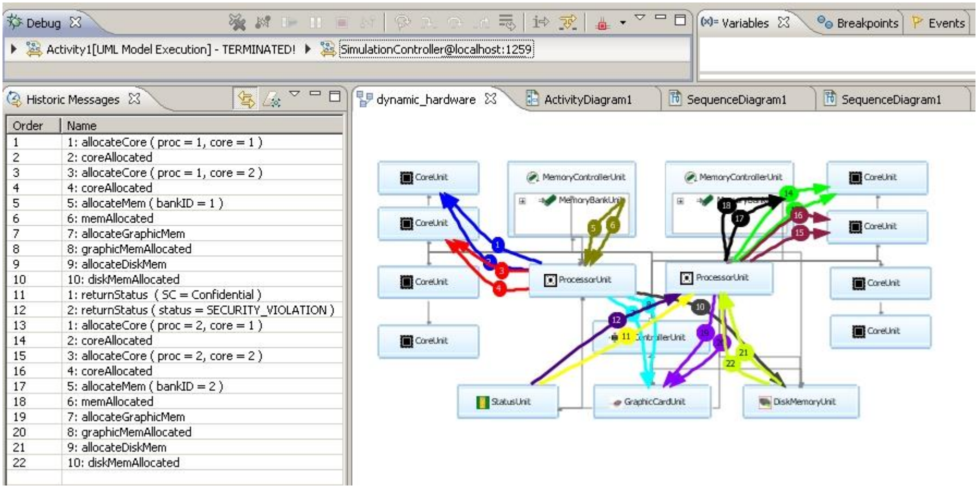

User
Chip card
Run VM
SCS
User
Run VM
Chip card
SCS
turn on SCS
insert the chip card in the reader
Enter the password and login
select the VM to run and press run
read data from chip card
Start SCS
view screen of access authorization
check access to the VM's
view on-screen list of available VM
Event log

Fig. 3 The business model of a process of virtual machine running in the SWSA system

For verification of the models behaviour we propose the use of the simulation mechanisms of UML models with the semantics action language as an extension. This is particularly important because the OCL language does not allow us to express constrains based on the states of models (there can be no changes in the characteristics of class instances (objects)). The diagram in Fig. 4 presents results of simulation of resources allocation as in the example 1. These results (i.e. historic messages between VMs[2]) confirm VMM's behaviour, which refuse to allocated requested resources to VM3 because of security violation (see step 12).



| Order | Name |
|---|---|
| 1 | 1: allocateCore ( proc = 1, core = 1 ) |
| 2 | 2: coreAllocated |
| 3 | 3: allocateCore ( proc = 1, core = 2 ) |
| 4 | 4: coreAllocated |
| 5 | 5: allocateMem ( bankID = 1 ) |
| 6 | 6: memAllocated |
| 7 | 7: allocateGraphicMem |
| 8 | 8: graphicMemAllocated |
| 9 | 9: allocateDiskMem |
| 10 | 10: diskMemAllocated |
| 11 | 1: returnStatus ( SC = Confidential ) |
| 12 | 2: returnStatus ( status = SECURITY_VIOLATION ) |
| 13 | 1: allocateCore ( proc = 2, core = 1 ) |
| 14 | 2: coreAllocated |
| 15 | 3: allocateCore ( proc = 2, core = 2 ) |
| 16 | 4: coreAllocated |
| 17 | 5: allocateMem ( bankID = 2 ) |
| 18 | 6: memAllocated |
| 19 | 7: allocateGraphicMem |
| 20 | 8: graphicMemAllocated |
| 21 | 9: allocateDiskMem |
| 22 | 10: diskMemAllocated |

Fig. 4 The states verification of the process of running virtual machines by the model simulation

[2] The environment used in the work enables you to collect the simulation results in the following forms: history of messages sent between objects, traces of messages passing control flow, history of console records. It should be noted that capabilities of this environment may be extended with the use of UAL language.

## 5 SUMMARY

We proposed and tested the complete environment based on the IBM RSA tool for MLS security policies verification, which can be easily used by security officers. The usefulness of this approach was confirmed in the completed SWSA project [22].

We demonstrated that the topology models may be successfully integrated with security-design MLS models for express and verification of the behaviour of developed MLS system components by means of simulation  in the deployment environment early i.e. in the modeling phase.

## REFERENCES

[1] BELL DE, LA PADULA LJ (1976) *Secure Computer System: Unified Exposition and Multics Interpretation*, ESD-TR-75-306, Bedford, MA: ESD/AFSC, Hanscom AFB. http://csrc.nist.gov/publications/history/bell76.pdf. Accessed 24 June 2012

[2] BELL DE (2005) *Looking Back at the Bell-La Padula Model* . Reston VA, 20191

[3] BIBA KJ (1975) *Integrity Consideration for Secure Computer System*, Report MTR-3153

[4] CLARK D, WILSON DR (1987) *A Comparison of Commercial and Military Computer Security Policies*. Proc. IEEE Symposium on Research in Security and Privacy, 1987,  184 –194

[5] SANDHU RS (1993) *Lattice-Based Access Control Models*, Computer, 9–19

[6] MOURATIDIS H, GIORGINI P, MANSON G (2005) *When security meets software engineering: a case of modeling secure information systems*, Information Systems 30 (2005), 609–629

[7] ZIELIŃSKI Z, STASIAK A, DĄBROWSKI W (2012) *A Model Driven Method for  Multilevel Security Systems Design*, Przegląd Elektrotechniczny (Electrical Review),  No. 2 (2012), 120–125

[8] BASIN D, CLAVEL M, DOSER J, LODDERSTED T (2006) *Model Driven Security: From UML Models to Access Control Infrastructures*, Vol. 15, No. 1 (2006), 39–91

[9] BASIN D, CLAVEL M, DOSER J, EGEA M (2009) *Automated analysis of security-design models. Information and Software Technology*, 51 (2009), 815–831

[10] AHN GJ., SHIN ME.: *Role-based authorization constraints specification using object constraint language*, in: WETICE'01: Proceedings of the 10th IEEE International Workshops on Enabling Technologies, IEEE Computer Society, Washington, DC, USA, 2001.

[11] SOHR K, AHN GJ, GOGOLLA M, MIGGE L (2005) *Specification and validation of authorization constraints using UML and OCL,* in: Proceedings of the 10th European Symposium on Research in Computer Security (ESORICS 2005), Lecture Notes in Computer Science, vol. 3679, Springer-Verlag, 2005.

[12] JÜRJENS J.: *UMLsec: extending UML for secure systems development*, in: J.-M. Jézéquel, H. Hussmann, S. Cook (Eds.), UML 2002 – The Unified Modeling Language, Lecture Notes in Computer Science, vol. 2460, Springer-Verlag, 2002.

[13] FRANKEL DS (2003) *Model Driven Architecture: Applying MDA to Enterprise Computing.* John Wiley & Sons

[14] ZIELIŃSKI Z, FURTAK J, CHUDZIKIEWICZ J, STASIAK A, BRUDKA M (2012) *Secured Workstation to Process the Data of Different Classification Levels*, Journal of Telecommunications and Information Technology, No. 3, 2012, 5–12

[15] STASIAK A, ZIELIŃSKI Z (2013) *An approach to automated verification of multi-level security system models* , in: New Results in Dependability and Computer Systems - Advances in Intelligent and Soft Computing (Series Ed.: Kacprzyk Janusz), Volume 224, Springer, 2013, 375–388

[16] NARINDER M (2008) *Anatomy of a topology model used in IBM Rational Software Architect Version 7.5*, Part 2: Advanced concepts, IBM, 2008

[17] ALVES-FOSS J, TAYLOR C, PAUL OMAN P (2004) *Multi-layered Approach to Security in High Assurance Systems*, Proceedings of the 37th Hawaii International Conference on System Sciences – 2004 IEEE

[18] KELLY S. TOLVANEN, J.-P.: "*Domain-Specific Modeling: Enabling Full Code Generation*", NJ: Wiley, 2008.

[19] MOHLIN M.: "*Model Simulation in Rational Software Architect: Simulating UML Models*", IBM, 2010.

[20] MOHLIN M.: "*Model Simulation in Rational Software Architect: Communicating Models*", IBM, 2010.

[21] ANDERS E., "*Model Simulation in Rational Software Architect: Activity Simulation*", IBM, 2010.

[22] KOZAKIEWICZ A, FELKNER A, ZIELIŃSKI Z, FURTAK J, BRUDKA M, MAŁOWIDZKI M. (2011) *Secure Workstation for Special Applications, Communications in Computer and Information Science*, Vol. 187, 2011, Springer, 174–181

*computer networks*
*data security, wireless transmission*

Tomasz BILSKI*

# DATA SECURITY IN EMERGING WIRELESS TRANSMISSION TECHNOLOGIES

Wireless transmission systems are continually developing. There are many improvements in the field. The development is gradual and sometimes revolutionary. The question is, if these new functions, new methods, new modes of wireless transmission may lead to new security threats and vulnerabilities? The paper is dedicated to some emerging wireless transmission innovations and security issues related to these innovations. Such technologies and transmission methods as: NFC (Near Field Communication), VLC (Visible Light Communication), Handover, Mesh networks, 4G and 5G cellular network, Mobile IPv6, beamforming, MIMO (Multiple Input Multiple Output), OFDMA (Orthogonal Frequency Division Multiple Access) are included into the research. The main purpose of the paper is to identify, analyse and classify distinctive sets of threats and vulnerabilities as well as some data protection opportunities related to innovative wireless transmission methods and technologies. Some of these emerging technologies may be used to improve security, while others create new threats and risks to data security. We will distinguish extraordinary sets of threats and vulnerabilities related to such factors as: energy consumption constraints in mobile devices, specific frequency band (e.g. EHF, visual), particular mode of transmission (e.g. MIMO, OFDMA), user mobility, interference and jamming.

## 1. INTRODUCTION

Due to their nature wireless transmission systems are essentially insecure. Bit error rate is much higher than in wired networks. It is relatively easy to snoop and to block transmission. Resources necessary to protect data (such as number of gates, processing power and energy) are constrained in mobile, wireless devices. General security requirements for wireless networks are common to IT systems: confidentiality,

* Institute of Control and Information Engineering, Poznań University of Technology, ul. Piotrowo 3a, 60-965 Poznań

integrity, availability, replay protection, access control, privacy, fairness and non-repudiation. Intentional as well as non-intentional threats should be evaluated. Such attacks as eavesdropping or jamming are relatively easy to execute in wireless environment. Furthermore, rising number of systems using the same unlicensed frequency bands increase interference and unavailability risk. A lot of security problems of common wireless systems should be solved today, nevertheless innovative wireless technologies emerge and new security problems crop up.

It is obvious that eavesdropping risk may be minimized by data encryption – upper layer protection and using cryptographic approaches. But in the case of mobile devices with low processing power and energy consumption constraints encryption/decryption overhead as well as key distribution and management issues may be prohibitive.

There are many emerging wireless transmission innovations. Such technologies and transmission methods as: NFC (Near Field Communication), VLC (Visible Light Communication), Handover, Mesh networks, 5G cellular network, Mobile IPv6, beamforming, MIMO (Multiple Input Multiple Output), OFDMA (Orthogonal Frequency Division Multiple Access), transmission in EHF (Extra High Frequency) are becoming popular. There are new security threats and vulnerabilities related to each of these innovations. Many research teams are working on them: looking for vulnerabilities and for new protection tools. Innovations mean new security problems but at the same time these new technologies may also be used as new solutions to old security problems. So, as an alternative to upper layer protection one may use physical layer[1] methods for data protection with such exemplary innovative technologies as beamforming, MIMO, OFDMA.

Another security issue is related to physical access to some devices. Access to subscriber’s device (smartphone, tablet) is usually easy for a malicious person independently of technology – there are millions of lost or stolen devices. But, in emerging technologies, like LTE, the higher density and diversity among base stations, access points and other wireless network devices, used to carry the traffic, lowers the barriers of physical access to the infrastructure. Decreasing cost of infrastructure devices should also be evaluated since it becomes very easy to build deceived infrastructure, for example by deploying small LTE cell for spoofing purposes.

[1] It must be noted that the use of physical layer for data protection originates from Shannon’s notion of perfect secrecy.

## 2. ENERGY CONSUMPTION CONSTRAINTS

In most up-to-date mobile devices energy is limited resource and on the other hand in modern devices there are many services with high level of energy consumption (e.g. Global Positioning System navigation and Bluetooth transmission). From the security point of view we have to analyse three general issues related to energy consumption constraints:

- extra level of energy usage related to data protection tools (encryption, decryption, key distribution, key management, authentication, authorization, accounting malware detection and prevention, firewall).
- common forms of attacks (e.g. port scanning), which use the energy resource of the attacked device in some way and in consequence gradually drain the batteries,
- dedicated attacks performed mainly to use the energy of the attacked device and in consequence to quickly, totally drain the batteries of mobile device (denial of service).

It was shown [3] that even simple, unsophisticated forms of attacks may increase the power consumption of mobile device. The experiments demonstrated that port scanning attacks or ping flooding attacks may sometimes double the power consumption of an exemplary Android based smartphone.

Dedicated “attacks against the mobile device energy” aim to activate device (e.g. via creating unsolicited network traffic, forcing erratic and CPU consuming behaviour, utilizing power consuming services like GPS navigation and Bluetooth) to produce rapid battery consumption. As a result, after a period of time, user is not able to use his device. The possibility of such attacks has been already demonstrated [2].

All data protection mechanisms utilize extra energy. For instance, using in a smartphone antivirus together with firewall means from 30% to 100% more energy usage in comparison to a smartphone without these security tools. For example, in a test performed with HTC Desire HD (Android 2.3.3) in normal operation mode and with disabled WiFi smartphone without security tools used 150 mW and the same smartphone running antivirus and firewall used 291 mW [3].

One of visible trends is based on offloading security tools. In the case of offloading some of the security mechanisms (like antivirus) execute on a server or in a cloud and remotely monitor mobile devices. The solution has some drawbacks. The energy related to processing in mobile devices is saved but at the same time additional energy is necessary for data transfer between mobile phone and security server. Furthermore, antivirus in server must be based on signature scanning method which may be easily defeated with encryption, polymorphism or other stealth techniques. Remote signature based scanning must be supplemented (especially in the case of rootkits) with host-based (and energy requiring) agents using behaviour-based virus detection methods.

This awareness, that the battery life is related to number of security mechanisms switched on, could cause the situation in which user turns off some services critical from the security point of view to save energy.

Authentication and authorization processes consume a lot of energy, especially in the case of mobile station which makes many disassociations and associations with many access points or base stations.

There are several research areas related to mentioned above problems:

- providing some models of relations between data security and energy consumption,
- implementing energy savings and power management methods,
- introducing features to enforce upper energy limits for security related processes,
- developing run-time mechanisms for scaling of security services to save energy,
- evaluating the standardisation of security standards and energy consumption in order to forecast battery life and to reduce the level of uncertainty for both users and developers,
- moving of some security mechanisms from mobile devices to the network infrastructure,
- creating security tools with reduced power consumption level.

A lot of theoretical and practical work had been done in order to design and implement some energy savings methods like adaptive power management algorithms in IEEE 802.11.

An attempt to provide an analytic model of relations between data security and energy consumption has been done by researchers from Worcester Polytechnic Institute [5]. They proposed 3-dimensional model of direct relationship between a given attack countermeasure and the level of security-reliability it can provide and relationship between the energy spent in carrying out a countermeasure and the energy level that is potentially lost if a given attack is successful. The model is a tool to compare the effectiveness of dissimilar attacks and their countermeasures even across multiple protocol layers. Some other important conclusion from the work is that there is no big difference between wireless protocols in terms of energy consumption per crypto operation. The energy consumption related to cryptography is dependent mainly on key length (independently on the selected algorithm).

## 3. MESH NETWORKS

Main security challenges related to wireless mesh networks are [1]:

- secure multi-hop routing,
- detection of corrupted nodes,
- denial of service attacks,
- fairness factor of the distribution of network resources.

An important factor is heterogeneity of the wireless links and devices in a mesh. It makes the protection of the communication between non-neighbouring nodes more complex since it may require the use of integrity and/or encryption on a higher protocol layer than the MAC (Medium Access Control) layer. Furthermore, different wireless technologies (IEEE 802.11, IEEE 802.16, …) used in a mesh networks may support different cryptographic algorithms with different security strength [7].

## 4. HANDOVER

Limited range of wireless transceivers (e.g. in IEEE 802.16 networks) is a problem for mobile users. If a user moves between access points or base stations of two systems handover procedure is necessary with some operations on MAC and also on IP layers (in the case user roams to a base station that is connected to another access router and another IP subnet). In the case of real-time services total handover interval is an important parameter. Mobile IPv6 is the standard to handle IP handovers between different subnets. The problem with this method is unacceptable latency (up to several seconds) to real-time applications. Several solutions to the problem had been provided. Generally, handover time may be optimized by predicting the pending handover and preparing it in advance, by eliminating unnecessary IP handovers (e.g. when user is roaming among base stations connected to the same access router) and by combining the mechanisms in the MAC layer with that of the IP layer [4].

The security problems linked to handover are related to security signaling. Security signalling during handover includes network access authentication and subsequent key management signalling for enabling link-layer ciphering. The process also needs time optimization. The delay introduced by different security handover mechanisms is quite significant, especially when all of them have to be processed one after another. Solutions proposed so far are based on EAP (Extensible Authentication Protocol) and Kerberos.

EAP is utilized by HOKEY (Handover Keying) working group[2] by IETF (Internet Engineering Task Force). HOKEY is based on fast re-authentication, handover key management and pre-authentication. EAP is extended in order to minimize message roundtrips. Keying material generated by a previous EAP session is utilized during re-authentication and client (in order to pre-authenticate) runs EAP for a candidate target authenticator from actual serving access network. Kerberos is used by Ohba et al. [11] for secure key distribution. In the proposed method the mobile node obtains master session keys without communicating with a set of authenticators before handover. Signalling related to key distribution is based on re-keying. The process is separated

[2] http://www.ietf.org/html.charters/hokey-charter.html

from EAP re-authentication and AAA (Authentication, Authorization and Accounting) signalling similar to initial network access authentication.

## 5. BEAMFORMING AND MIMO

Beamforming and MIMO antenna systems are widely adopted in modern computer networks and mobile phone systems. Beamforming solves some problems with interferences and power constraints. But the advantages are not limited to the interferences.

Theoretical foundations of wireless security were presented many years ago, e.g. [6]. Secrecy capacity has been defined as the difference between the capacity of the legitimate link and the link between the transmitter and the eavesdropper – in other words it is related to SNR (signal to noise) difference between the legitimate receiver and the eavesdropper. In MIMO and beamforming systems the difference may be increased by transmit antenna selection or by transmitting jamming signal in the direction of the illegitimate eavesdropper.

It was shown that beamforming may be used to improve SNR difference between the legitimate receiver and the illegitimate receiver and to minimize eavesdropping risk. There are several works on beamforming usage in order to minimize eavesdropping risk. Some proposed solutions assume that the location of the eavesdropper is known, others assume the location and channels of the eavesdropper are random and unknown, e.g. [13].

Mukherjee and Swindlehurst [10] have shown robust algorithms that minimize the transmit power required for the desired receiver to achieve appropriate signal to interference plus noise ratio (SINR) of the wireless data stream. Minimizing this power the transmitter may maximize the power available to broadcast an artificial jamming signal (noise) that disrupts the ability of the eavesdropper to recover the desired signal and data. The jamming signal will not obstruct desired receiver since the signal is designed to be orthogonal to the information signal when it reaches the desired legitimate receiver.

Common beamforming system uses antenna array integrated with a single node. Cooperative beamforming is used in randomly distributed nodes in a network cluster – antenna array is created with a use of antennas from many nodes. The idea has been proposed by Ochiai et al. [12]. The main purpose of the technique is to transmit data on long distances in energy-efficient way. However, cooperative beamforming may also be used for security enhancement. Wang et al. [14] presented cooperative beamforming and jamming scheme, where a part of intermediate nodes adopt distributed beamforming while others jam the eavesdropper, simultaneously. The method is based on particular secrecy strategy and takes into account the individual power constraints of each node.

Another solution to eavesdropping problem has been proposed by Yang et al. [16]. The method is based on transmit antenna selection (TAS) at the transmitter. One of many MIMO antennas of transmitter is selected in such a way that maximizes the post-processed signal to noise ratio (SNR) at the legitimate receiver without increasing SNR at the illegitimate receiver. The antenna is selected with a use of some feedback from the legitimate receiver.

## 5. COOPERATIVE RELAYING

Cooperative relaying is also widely investigated. Cooperative relaying means employing an extra relay (another user of wireless network) to assist the transmission between a source and a destination in the case of problems with the direct link range.

The security problem here is that the relay may be trusted or untrusted. The relay may be a legitimate user or may act like a legitimate user who helps to counter external eavesdroppers and increase the security of the networks. In the case of untrusted relay, the relay node acts both as an eavesdropper and a helper, i.e., the eavesdropper is co-located with the relay node. An example of the research in the area of cooperative relaying security is a study of the joint source and relay beamforming designs in MIMO two-way untrusted relay systems for enhancing physical layer security [9].

## 6. OFDMA

Orthogonal frequency division multiple access (OFDMA) has recently evolved as a leading technology. The technology is used in mobile cell phone 4G networks (Long-Term Evolution) as well as in computer networks (e.g. in IEEE 802.16 standard). Some suggestions how to use ODFMA to protect data has been already provided. For example, Wang et al. [15] recommends to improve downlink security with a use of specific power and subcarrier allocation at base stations.

## 7. VLC

Visible Light Communication is a small distance communication system based on light emitting diodes (LED) and photodetectors. For example, lamp fitted with LED streams data embedded in its beam to the photodetector, which converts tiny changes in light amplitude into bit stream. An important feature is the spectrum, which is unlicensed and less crowded than unlicensed radio bands. Furthermore, it may be used even underwater where RF bands are strongly absorbed.

The security issues are related to interferences from other sources of light (e.g. the Sun) and to spoofing. Risk related to sniffing is relatively low since communication distance is short and illegitimate data receiving devices are observable – line of sight between data source and data receiver is necessary in order to transmit bits.

VLC system may be used as an supplementary, out-of-band communication channel for authentication purposes. In the case the radio channel is used for data transmission the same channel is not always good solution to authentication problem. So, an out-of-band channel is necessary. Some different out-of-band channels have been proposed: relative location measured via ultrasound, visual markers photographed with camera smartphones. An advantage of mentioned above methods is they are verifiable by human. An exemplary protocol for creating an out-of-band channel for authentication with visible laser light has been proposed in [8]. The authors assume the laser transmission is not confidential. An attacker is able to either violate the confidentiality of data transmitted by VLC or to violate its authenticity. Proposed protocol, based on off the shelf components (so relatively cheap), establishes a secret, authenticated shared key between the personal trusted device and a remote device.

## 8. LTE

In the past, voice-dominated, closed cell phone networks have been built on proprietary interfaces and protocols (e.g. SS7 signalling protocol) so mobile networks have been relatively difficult to penetrate, and have provided less incentive for malicious attacks than IP networks. RAN (Radio Access Network) and backhaul had complex deployment configurations, specific to operator, location and equipment vendor. Attacks on them required sophisticated preparation and on-site access.

Today, contemporary mobile networks are primarily data networks with more open architecture and protocols (e.g. Diameter open signalling protocol). New threats emerge here like signalling flood (such number of signaling messages is sent by clients that servers may not immediately process them), which may be caused either by malicious activity directed at the mobile network, or accidentally as an indirect effect of upgrades[3].

Smartphones, applications running in smartphones, exponential growth of traffic and especially introduction of 4th cell phone generation LTE based on IP stack of protocols are the general factors decreasing level of security in cell phone networks.

[3] In January 2012, NTT DoCoMo in Japan experienced a signalling flood that disrupted network access, caused by a VoIP OTT application running on Android phones
[http://www.reuters.com/article/2012/01/27/us-docomo-idUSTRE80Q1YU20120127]

Small cells, femtocells and Wi-Fi hotspots integrated with cellular networks make attacks on mobile networks easier to plan and to carry out. Furthermore, some changes in data encryption scheme leave the IP traffic in the part of the backhaul infrastructure unprotected.

LTE security is generally based on GSM and UMTS security. On the other hand LTE uses different cryptographic algorithms with longer keys (128 or 256 bits). Key hierarchy is extended.

It must be observed that modern attack on a mobile device may have impact on: the cell phone subscriber, corporate network of the subscriber, the mobile core network and Internet.

## 9. CONCLUSION

In general, innovations in IT (not only in wireless transmission) are often made without previous solutions to security problems. New functionality almost always means new threats and new vulnerabilities.

Incorporating IP protocol in mobile phone networks (in LTE generation) means introducing all security threats and vulnerabilities of Internet to cell phone networks.

In each innovative wireless technology we have to seek opportunities for improving data protection and simultaneously be aware of all new threats and vulnerabilities introduced by the technology.

There are many data protection methods related to different layers of protocol stack. Data encryption is popular security control integrated with upper layers (network layer, transport layer, application layer). In the case of mobile devices with low processing power and energy consumption constraints encryption/decryption overhead as well as key distribution and management issues may be prohibitive. So, security controls located at the physical layer are becoming necessary. By the way, it must be noted that there are currently efforts within IETF to integrate independent security mechanisms working in different layers.

Commonly used security controls such as EAP or Kerberos may be used in wireless systems but they should be revised and modified in order to adjust them to security features of wireless communication environment.

Security level related to malware may be increased by preemptive approaches. The security of mobile applications should be verified and certified before the applications are deployed. The device should be configured in such a way that only trusted applications are downloaded.

Techniques such as MIMO, beamforming, OFDMA are widely adopted in modern wireless communication systems. In such systems eavesdropping risk may be minimized with a use of such methods as dedicated subcarrier allocation in OFDMA, transmit antenna selection and jamming the illegitimate receiver.

New technologies such as VLC solve some security problems and may be used as an additional out-of-band communication channel for security purposes in wireless systems.

## REFERENCES

[1] BEN SALEM N, HUBAUX J.P., *Securing Wireless Mesh Networks*, Wireless Communications, IEEE, Vol. 13, Issue 2, 2006, pp. 50–55.

[2] BICKFORD J.E., *Rootkits on Smart Phones: Attacks, Implications and Energy-Aware Defense Techniques*, Graduate School—New Brunswick Rutgers, The State University of New Jersey, 2012.

[3] CAVIGLIONE L., MERLO A., *The energy impact of security mechanisms in modern mobile devices, Network Security*, February2012, http://www.ai-lab.it/merlo/publications/NS-2012.pdf.

[4] CHUNG-KUO C., CHIN-TSER H., *Fast and Secure Mobility for IEEE 802.16e Broadband Wireless Networks*, 2007 International Conference on Parallel Processing Workshops (ICPPW 2007).

[5] COLON OSORIO F.C., AGU E., MCKAY K., *Tradeoffs Between Energy and Security in Wireless Networks,* Worcester Polytechnic Institute, 2005. Retrieved from: http://digitalcommons.wpi.edu/computerscience-pubs/67

[6] CSISZAR I., KORNER J., *Broadcast channels with confidential messages*. Information Theory, IEEE Transactions on, vol. 24(3), 1978, pp. 339–348.

[7] EGNERS A., MEYER U., *Wireless Mesh Network Security: State of Affairs,* 5th IEEE Conference on Local Computer Networks (LCN), Denver (USA), October 2010.

[8] MAYRHOFER R., WELCH M., *A Human-Verifiable Authentication Protocol Using Visible Laser Light,* Second International Conference on Availability, Reliability and Security (ARES'07), 2007.

[9] MO J., TAO M., LIU Y., XIA B., MA X., *Secure Beamforming for MIMO Two-Way Transmission with an Untrusted Relay,* 2013 IEEE Wireless Communications and Networking Technology WCNC, p. 3279–3284.

[10] MUKHERJEE A., SWINDLEHURST A. L., *Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI*, IEEE Transactions on Signal Processing, Vol. 59, No. 1, January 2011, pp. 351–361.

[11] OHBA Y., DAS S., ASHUTOSH D., *Kerberized Handover Keying: A Media-Independent Handover Key Management Architecture*, MobiArch'07, August 27–31, 2007, Kyoto, Japan.

[12] OCHIAI H., MITRAN P., POOR H.V., TAROKH V., *Collaborative beamforming for distributed wireless ad hoc sensor networks*, IEEE Trans. Signal Process., vol. 53, no. 11, Nov. 2005, pp. 4110–4124.

[13] ROMERO-ZURITA N., GHOGHO M., MCLERNON D., *Physical Layer Security of MIMO Frequency Selective Channels by Beamforming and Noise Generation*, 19th European Signal Processing Conference (EUSIPCO 2011), pp. 829–833.

[14] WANG H., LUO M., XIA X., YIN Q., *Joint Cooperative Beamforming and Jamming to Secure AF Relay Systems With Individual Power Constraint and No Eavesdropper's CSI,* IEEE Signal Processing Letters, Vol. 20, No. 1, January 2013, pp. 39–42.

[15] WANG X., TAO M., MO J., XU Y., *Physical-Layer Security in OFDMA-based Broadband Wireless Networks,* 2011 IEEE International Conference on Communications (ICC), pp. 1–5.

[16] YANG N., LEP YEOH P., ELKASHLAN M., SCHOBER R., COLLINGS I.B., *Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels*, IEEE Transactions on Communications, Vol. 61, No. 1, January 2013, pp. 144–154.

*Service Oriented Architecture, Service Level Agreement,
virtual resources management*

Jan KWIATKOWSKI*, Mariusz FRAŚ*, Grzegorz PAPKALA*

# SLA-AWARE MANAGEMENT OF VIRTUALIZATION FOR SOA

Managing the virtualized computational resources in scope of applications based on SOA paradigm is a complex problem that has number of different solutions. The ideal one shall combine the flexibility with the possibility of reaching the business goals. This leads to the idea of combining the management of resources directly with the Service Level Agreements (SLA), which has to be fulfilled. The chapter is devoted to description of the modified PlaTel-R architecture that enables the virtualization management in the context of SOA and SLA. Such an approach can bring the resource utilization closer to the business aims. The chapter includes the description of the SOA and virtualization themselves and the idea of quality-aware service request processing by PlaTel-R. Those are followed by parts presenting the new extensions of the system, namely service awareness on the low level of virtualization management that ensures quality during requests processing.

## 1. INTRODUCTION

Service Oriented Architecture has been a buzz word few years ago. Since then it matured and has been evolved to cloud. Nonetheless SOA is a concept that has a strong grounding. On the other hand many areas of SOA solutions still needs further research and development. Especially service quality offered by SOA-based systems is still a challenge. Among the quality attributes defined for a SOA systems [8], three of them directly relate to non-functional parameters of services and perception of the quality of service for the end user: availability, usability, and performance of service delivery. Particularly for the last one is very difficult to fulfill sufficient values of non-functional parameters. The quality issues of SOA-based systems are investigated, inter alia, at the service abstraction layer [1]. Often used solutions at this layer to guarantee proper quality of service delivery are redundancy of services (e.g. CDN solutions) and service requests distribution [5, 2].

* Wrocław University of Technology, 50-370 Wrocław, Wybrzeże Wyspiańskiego 27

The management of non-functional demands in the context of SOA is challenging task, especially at run-time. It requires proper means and architectural solutions at service execution environment. Cooperation between service provider and service consumer in the context of service level agreement (SLA) should supported and automated by the service delivery system as far as possible. Proposed architectural models of management SLA aim to achieve run-time adaptability [10]. The other challenging task is to proper management of execution environment resources to support as well service guaranties as proper resource utilization. Great opportunity to suitable and effective accomplishment of both tasks is SLA support combined with well-defined virtualization.

Although virtualization is already being used as a common and proven way to decrease the overall hardware needs and costs, still the hardware utilization is around 15-20% and storage utilization does not go above 60%. Mission critical services are used as before due to the easier maintenance, controlling and monitoring. Reduced budgets and “do more with less” attitude make it much more complicated for the real applications since the costs of implementation are higher than maintenance ones.

The chapter describes modified architecture of PlaTel-R that enables the virtualization management in the context of SOA and SLA. The chapter is organized as follows. Section 2 introduces PlaTel-R application [4] and presents its extensions to virtual resources aware service delivery system. In the section 3 the functionalities of new PlaTel-R modules as well as some implementation details are presented. Finally, section 4 outlines the work and discusses the further works.

## 2. THE ARCHITECTURE OF PLATEL-R

### 2.1 DESIGN OVERVIEW

PlaTel is a platform designed to support the execution, composition and monitoring of network services based on Service Oriented Architecture paradigm [4]. Among other applications building up the system PlaTel-R is dedicated to managing of execution of the services on the available resources and handle client’s requests taking into account non-functional service parameters. To increase resource utilization it exploits the capabilities offered by virtualization [6]. The real services are hidden from client point of view. The system advertises virtual services in accordance with SOA paradigm, and handles client’s request for services. The client deals with virtual service that can be executed on different machines as service instances. Apart from effective resource utilization the main function of PlaTel-R is quality-aware distribution of service requests to service instances.

PlaTel-R has modular structure where each of the modules is a service itself and is independent from the other services. Furthermore the system can work on different numbers of nodes requiring only minimal amount of extra services to be installed on top i.e. XEN (a software that allow multiple operating systems to execute on the same computer hardware concurrently), *libvirt* (a library for managing platform virtualization), and *Munin* (specialized application which is capable of gathering the data using countless scripts and metrics).

The modules of PlaTel-R compose two independent parts of the system. The Controller, Service Monitor and Estimator/Predictor modules (Fig. 1) constitute the service virtualization part that acts as a broker for service requests and can be located as a Broker far away of the rest of the system, being able to take into account data transfer issues [7]. The VRM Manager, VRM Database, VRM Facade, VRM Matchmaker, VRM Virtualization, and VRM Monitor constitute the resource virtualization part (VRM stands for Virtual Resource Management).

The Controller module is responsible for QoS-aware distribution of clients requests to proper service instances. The decisions are based on service execution monitoring by Service Monitor and AI-based prediction of values of service parameters performed by Estimator/Predictor module [3, 7].

The modules of VRM communicate with each other using XML-RPC protocol. This solution has been chosen due to its simplicity and support offered by particularly any popular programming language. The modules run as standalone services listening on specific ports. The only module offering SOAP access in VRM is VRM Facade module. It interprets massages sent in requests, dynamically inserts there extensions necessary to support various system functionalities and is used as a gateway to VRM. For simplicity this module is not included in figure 1, however some its functionality represents Service Monitor since it cooperates with VRM Facade very close in the area of service execution monitoring.

From the point of view of system control the most important modules are VRM Manager which is responsible for controlling the work of all VRM modules, and VRM Database which is dedicated to provide one spot for persistent data storage across the whole VRM. It is based on PostgreSQL relational database and Django web framework. The module provides consistent API that makes all the other modules independent on the data model changes.

The VRM Matchmaker module is used to match existing set of available hardware and software resources with the incoming request. The module is based on HTCondor and the ClassAd Language. Unlike in Condor the matching is done regardless of used parameters, what is great for potential system growth and usage of parameters that have not been thought of while creation of parameters ontology. VRM Virtualization module is responsible for launching and conducting operations on virtual machines, and offers common interface to access to different virtualization systems. The state of the environment is a dynamic issue that requires decent monitoring to give the overview. The VRM Monitor module provides the “on demand” monitoring of available computational resources and running service instances.

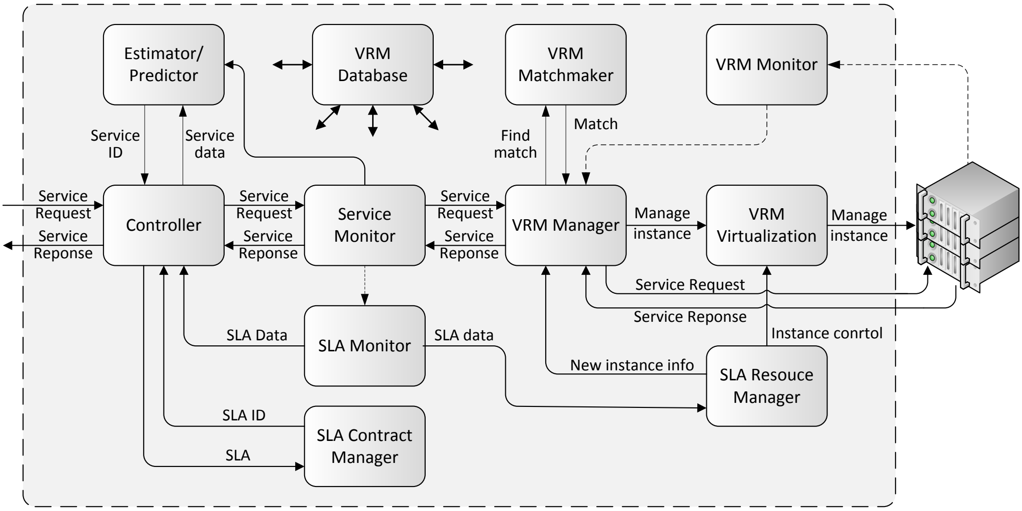


Fig. 1. Extended PlaTel-R architecture

### 2.2. THE EXTENTIONS OF PLATEL-R

The proposed modification of PlaTel-R architecture consists in extension it by SLA functionalities that can be used to describe expected service behavior in terms of measurable metrics and support automatism of system work in this area. Based on it the system can adapt and react to actual needs and conditions in order to maximize customer satisfaction and minimize overall cost of service delivery. The general architecture of PlaTel-R including the new modules is presented in figure 1.

The new modules supporting SLA capabilities are:

- **SLA Contract Manager -** it is responsible for management of the predefined SLA templates and contracted SLAs. Furthermore, the manager is responsible for marking the SOAP messages according to the client's contract.
- **SLA Monitor -** it extends capabilities of already existing VRM Monitor module. The main task of the SLA Monitor is detection of violation of SLA contract and then passing this information to the SLA Resource Manager.
- **SLA Resource Manager** – it is responsible for management of the resources according to the contracted SLAs. This basically means to provide the resources according to the signed SLA and adjust them depending on the demand changes while operation.

PlaTel-R is already enabled to modify the SOAP messages on the fly. Extra information can be added there while sending the response to notify the client about actual resource usage by the service instance that was responsible for perform the request. The exchanged information during communication with the service, and various metrics related with service execution are defined in the WSDL file.

Due to realized extensions, the data model used by VRM Database has to be extended in a way that will enable the storage of hierarchic structure of metrics described in the SLA. The set of basic metrics should be fixed and based on VRM Monitor supported ones. VRM Monitor gives access to resource usage of the servers and service instances running on them. The other metrics can be related to requests to certain service. The above is controlled by VRM Facade and Service Monitor.

The data model and SLA creation capabilities are independent on the domain in which the service operates. The characteristics and metrics can be chosen arbitrary according to the needs of particular application.

The data model that supports SLA has to fulfill the following requirements:

1. Allow the storage of arbitrary complex metrics which are basically structured into the tree.
2. Allow mapping of the SLA parameters to services and operations.
3. Allow mapping of the metrics (for particular service) to resources.

Metrics and parameters included in the SLA templates and stored in the database must have the same meaning between signing parties. To ensure this some extra mechanisms could be used such as e.g. ontologies. The new database contains the following data supporting new functionalities [9]:

- **Customer -** contains the information about the service clients, specifically their authentication data,
- **Agreement -** contains the information about active SLAs,
- **Metric -** the list of resource metrics available in PlaTel-R,
- **Parameter** - contains the parameters composed from single metrics or other parameters,
- **Objective -** contains the actual value of parameter accepted by the client,
- **Agreement Template -** contains the list of predefined set of service metrics to be guaranteed under the contract based on the te~~a~~mplate.

## 3. SLA MODULES FUNCIONALITIES

The basic functionalities which involve SLA-aware service requests processing are (see Fig. 2):

- contracting SLA concerning service quality,
- request identification in terms of SLA requirements,
- request distribution such that SLA would be satisfied,
- monitoring of SLA fulfillment,
- SLA event driven virtual resource management.

The above functionalities are supported by three new modules that integrate with previous service requests processing.

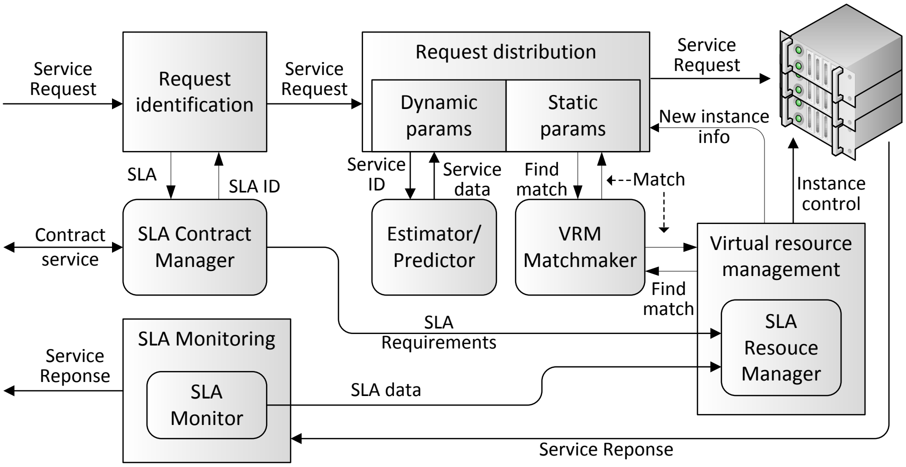


Fig. 2. SLA-aware client request processing

The SLA-aware client request processing concerns establishing SLA contracts with clients, and handling client's requests for given service. Some more details of these processes are described in the next three subsections. The main steps of the service request handling scenario are the following (Fig. 2):

1. Service request identification (classification). This operation is based on previous client registration in the system and registered SLA contracts.
2. Request distribution – it addresses client request to proper service instance taking into account SLA requirements. This can be performed in two independent phases by one or two system modules: Broker controller and/or VRM Manager. These phases apply to the following cases:
   a. Handling fuzzy SLA requirements. As the fuzzy SLA parameters are considered parameters which values can be evaluated only with some accuracy. An example of such parameters is service response time.
      One of the proposed solution is fuzzy-neural controller located in Broker (described e.g. in [3]). On the basis of current values of execution environment parameters the service request is directed to the service instance (or the set of service instances) which predicted response time guarantee fulfillment of SLA parameters. This phase can be also accomplished using various procedures in the VRM Manager.
   b. Handling strict SLA requirements. As the strict SLA parameters are considered parameters which values can be precisely controlled by the system. An example of such parameters are guaranteed amount of RAM or processor usage.
      At this phase the service instance selection is further clarified. The control of service instance to guarantee strict SLA parameters is performed using online monitoring of virtual resources, so it can be accomplished only in VRM Manager (with use of VRM Matchmaker).

3. Virtual resource management. This operation includes tuning of allocated to service instance resources as well as new service instance creation. The resource management is driven by events signaled by SLA Monitor which tracks fulfillment of SLA parameters (more details are given in sections 3.2 and 3.3).

### 3.1. SLA CONTRACT MANAGER

SLA Contract Manager has two tasks to perform. It is responsible for advertising the agreement templates to the clients and for identification (classification) of incoming request according to the signed contracts.

Client identification is based on the SOAP extension for authentication. First, the client has to be registered in the PlaTel-R to be able to use hosted services. Two SOAP authentication methods are used: basic (using plain text name/password headers to send the credentials) and digest (using the MD5 hashed password and challenge/response protocol to enable secure authentication).

In the current implementation the contract negotiation process consist in acceptance of one of the offered templates. Offerings are checked against free resources. Each template is built from the set of parameters where the value of such parameter can be described using an operator (one of: ==, <, >, <=, >=, IN, BETWEEN) and expected value.

In more complex scenario the negotiation process should be supported when offered values of parameters for given set of service instances are not sufficient. The SLA Contract Manager must know some characteristics of the service and be able to calculate conditions to assure the given service parameters (e.g. the number of serviced client requests per instance). Assuming that is possible to find necessary resource quantity and decide about contract acceptance. As the result of this procedure the SLA Contract Manager triggers SLA Resource Manager and tuning of allocated resources (e.g. RAM) to service instance or the new service instance is created.

Resource requirements analysis is the task of the SLA Resource Manager. It is assumed that the resources are limited in each of the virtual servers, therefore supplying with resources for each template has to be performed in the following way:

- each parameter in the template is analyzed against its real resource usage (this is done by the SLA Resource Manager),
- maximal value is taken and checked against free resources in the servers,
- the server that has minimal amount of resources sufficient to ensure requirements is marked so that the resource won't be taken by another negotiation process run in the same time,
- when the negotiation finishes with success the service resources are properly secured (by starting new service instance or by extending resources of existing one).

### 3.2. SLA MONITOR

Monitoring activities are performed in several ways. VRM Monitor is able to query the nodes (real or virtual) on demand, gathering all the information that is required. The module also performs continuous monitoring of selected resource usage. This is implemented as a CRON (Time Based Job Scheduler) scripts running on the servers. Such an approach has advantage of simplicity, but lacks of any management capabilities on top of them, and makes it unsuitable for distributed environment that is built from large number of nodes. The monitoring is also performed by the VRM Facade module and Service monitor module that log the information about incoming requests (time, duration, client, etc.).

SLA monitoring has to perform its tasks based on the historical data that is gathered currently by CRON scripts and modules themselves. Main task of SLA monitoring is SLA violation detection. The SLA violation should lead to some reaction of the system. Not each and every such an event should immediately cause the change. In many cases the violation can be just a single event that should be recognized, but without any further actions. The action can depend on the SLA itself.

The two cases are to be considered:

- **SLA was violated -** this is the simplest and most obvious condition. It requires only to register the event or force the system to react always to every violation.
- **SLA violation exceeds threshold -** the number of violation are tracked and the actions are fired when the threshold is exceeded.

  The threshold can be expressed quantitatively or relatively. In the first case the number of violations executes system reaction. In the second case the number of violations is compared to the number of requests in the some defined interval. Based on that the violation ratio is calculated.

Detection of the violation is the first step. The second one is to identify where it occurred exactly, and the last is to react accordingly. Finding the cause of violation means to find the service or the service instance is the source of problems. Let say that we found that response time of certain service is exceeding the threshold. That means either that there is not enough instances running or that one of the instances is causing some problems. Thus, the violation has to be addressed accordingly. To find the tentative service instance the violation ratio has to be computed for all running instances. The notification of the violation is directed to the SLA Resource Manager (Fig. 2) which is responsible for the suitable reaction.

### 3.3. SLA RESOURCE MANAGER

SLA Resource Manager performs the crucial part of virtualization for SOA. It is expected to balance two contradictory requirements: the minimization of resource usage so that the overall costs of service delivery is minimal and maintenance of the

SLA fulfillment. Those two requirements basically are performed using the following main activities: delivery of the service instance while new agreement is signed, adjusting resource utilization based on the notifications from SLA Monitoring.

SLA Resource Manager can be notified that certain service or instance is underperforming violating the SLA. In such case a manager should diagnose the reason and apply proper solution. The reason of violation can be either some service instances are poorly supplied with resources to perform the operations within certain SLA requirements or the whole service is poorly supplied. In the first case the solution is to provide more resources to the service instances, the latter case can be simple solved by creation of another service instance.

The decision about new resource allocation can be taken in two ways. First, when the value of some fuzzy parameter is signaled to be exceeded by SLA Monitor just the new service instance is executed and distribution modules are informed about it (so they can distribute requests to more executive entities). Second, for each service instance strict parameters are monitored in proper time slots. When the given threshold is exceeded or one of them the proper activity is performed. The increase of needed resource (e.g. RAM or processor power) can be calculated using average usage of such resource by one request or on the basis of strictly indicated resource requirement in the SLA.

While notifications from SLA Monitor would only handle the scenario when some requests are not performed according to the QoS defined in the SLA, the case when the service instances are over-supplied with resources is not serviced. SLA Resource Manager is responsible himself to perform continuous checks of the running service instances against signed SLAs and shrink assigned resources when it is possible. The processing is reverse to the process of increasing resource usage. Checking of the service instances has to be performed when values of strict parameters are not specified in the SLA for that service instances. In all of the other cases the manager should check the resource usage and if the value is to small e.g. less than 50% (in some time period) act appropriately. The service instances with the lowest load should be marked for shutdown (no further requests are passed to them) and eventually when no more requests are being processed shutdown.

## 4. CONCLUSIONS

The purpose of this chapter was to present the virtualization management in the context of SOA and SLA. The development of the proposed solutions has been undertaken for PlaTel-R project which is a prototype for virtualization management aimed to support Service Oriented Architecture.

The new PlaTel-R architecture provides useful mechanisms to tie requirements of request processing with low level virtual resource management. It permits to control and properly react on SLA events in order to keep service processing such client requirements have been satisfied. Meanwhile it also permits to keep resource usage as low as possible. The presented solution is based on rules that have to be defined by the user. The next step should employ more sophisticated methods of resource utilization. Especially, more advanced methods that estimate necessary service instance resource supply are welcome.

Nonetheless the proposition has been a next step toward presented ultimate goal which is QoS-aware virtual resource management, and has brought the PlaTel-R closer to be a self-aware system.

**Acknowledgements** The research presented in this paper has been partially supported by the European Union within the European Regional Development Fund program no. POIG.01.03.01-00-008/08.

## REFERENCES

[1] BRAWN P. C., *Implementing SOA*, Pearson Education, 2008.

[2] FRAŚ M., *The architecture of complex service requests broker*, Information Systems Architecture and Technology: Networks and Networks Services, A. Grzech (eds), Wroclaw University of Technology Publishing House, Wrocław, 2010, pp. 369-379.

[3] FRAS M., ZATWARNICKA A., ZATWARNICKI K., *Fuzzy-neural controller in service request distribution broker for SOA-based systems*. In Proc. of Int. Conf. Computer Networks 2010, Kwiecien A., Gaj P., Stera P. (eds), Springer, Berlin, Heidelberg, 2010.

[4] GRZECH A. & others, *Smart Work Workbench: integrated tool for IT services planning, management, execution and evaluation*, Computational collective intelligence: technologies and applications, P. Jędrzejowicz, & others (eds.), Berlin; Heidelberg, Springer, 2011. pp. 557-571.

[5] KUNZ M., SCHMIETENDORF A., DUMKE R., WILLE C., *Towards a Service-Oriented Measurement Infrastructure*, In Proc. of the 3rd Software Measurement European Forum (Smef 2006), Rome, Italy, May 2006, pp. 197-207.

[6] KWIATKOWSKI J., FRAS M., *Request distribution toolkit for virtual resources allocation*, Parallel processing and applied mathematics: 9th International Conference, PPAM 2011, Torun, Poland, September 11-14, 2011, revised selected papers, Roman Wyrzykowski & others (eds.), Berlin; Heidelberg, Springer, 201,. pp. 327-336.

[7] KWIATKOWSKI J., FRAS M., *Quality aware virtual service delivery system*, 17th Polish Teletraffic Symposium 2012, Zakopane, 6-7 December 2012, eds. Tadeusz Czachórski, Mateusz Nowak, Gliwice, IITiS PAN, Pracownia Komputerowa Jacka Skalmierskiego, 2012, pp. 115-121.

[8] O’BRIEN L., MERSON P., BASS L., *Quality Attributes for Service-Oriented Architectures*, Proc. of the Int. Workshop on Systems Development in SOA Environments, IEEE Computer Society, Washington DC, 2007.

[9] PAPKALA G., *Management of virtualization in Service Oriented Architecture*, Wroclaw University of Technology, Faculty of Computer Science and Management, Master Thesis, 2013.

[10] RAIBULET C., MASSARELLI M., *Managing Non-functional Aspects in SOA through SLA*, Proc. of 19th International Workshop on Database and Expert Systems Application, DEXA 2008, Turin, Italy, 2008.

# PART 3

# WEB SYSTEMS DESIGN
AND EVALUATION

*WEDA, SOA, EDA, Websockets, MEP, duplex, architecture, CEP*

Jitka HÜBNEROVÁ*

# WEDA – NEW ARCHITECTURAL STYLE FOR WORLD-WIDE-WEB ARCHITECTURE

In this paper we will describe, how service oriented architecture can evolve to event-driven-architecture, while preserving capabilities to communicate over World-Wide-Web. For this purpose we will introduce new "WEDA" architectural style, protocol and developed API, which can be established easily into existing web services stack, so millions of web services can be extended, but not forced to be completely rewritten. Second impact of the new architectural style is better performance for web services and benefit of possibility to extend communication to duplex level with client contract without needing the client to publish a public endpoint over the Internet.

## 1. INTRODUCTION

A web service [1] is a software system designed to support inter-operable machine-to-machine interaction over a network. At the time of writing, (SOAP, REST, plain old XML) web services are widely used technique which standardizes many aspects of distributed processing and communication over the World-Wide-Web. Behind the wall, there stays event-driven architectural style (EDA) [2], which had many of forms by the years and now it is often discussing together with SOA and how these two can interact. As complexity of protocols grows, there is still less chance that some even good protocol becomes widely popular. The world of application integration over the public Internet is very conservative, and it is logical output of number of interested sides, which have to communicate with each other. From this assumption we come out to the concept of WEDA, which will be introduced in this paper. This post is designed to enable us to do (a very) comprehensive picture of the whole architectural style (its conceptual and technical infrastructure). Any chapter won't go into the depth. Deeper understanding we keep to the other posts and work.

* NTI FM TUL, Hálkova 6, 461 17 Liberec 1, Czech Republic

## 2. WEDA ARCHITECTURAL STYLE

WEDA is hybrid architectural style derived from other network-based styles, such as SOA web services (message, service or resource oriented model [3]), SOA 2.0 and HTML5 web-sockets which provides uniform connector interface to the clients by using existing widely used standards, and allowing server implementers to extend their web services (SOAP 1.2, REST, POX) with new type of endpoints and binding. And yes, service providers can keep their HTTP endpoints to legacy clients and provide it together with new endpoints to those clients, which are supporting HTML5 web-socket transport binding mechanism of WEDA. When implemented, we can design real-time web services using well known standards and we can extend existing ones to better performing experience. We can write truly asynchronous web-services, so web server or orchestrated services can work on long running transactions without affecting the user experience and resources. We will get World-Wide-Web based messaging and workflow orchestration ESB platform [4].

Weda architectural style is defined by architectural ontology entities constrained in their relationships in order to achieve a desired set of architectural properties. It was chosen because unlike component-based approach it has ability to model dynamic behaviors. However formal description isn't goal of this paper.

Table 1. WEDA major architectural ontology entities

| Ontology entity | Details | Example |
|---|---|---|
| Infrastructure | Service provider, Origin server, server host process | Apache httpd, IIS, web infrastructure |
| Management | Service host, Weda gateway, set of endpoints and channels traversable through firewalls and reverse proxies. | WEDA transport binding, Weda client and server API, websocket connection, session manager, weda channel, Event processor with Esper engine |
| Service | Object representing a set of operations for the client, IO data, message exchange patterns, temporarily available thru the set of endpoints to a service. In Weda there are infrastructure specific services for eventing. | SOAP 1.2 Calculator service, SOAP1.2 Weda statement, ws-eventing services, REST service, OGC SOS service |
| Data | Service contract and callback contracts, Weda messages | WSDL 2.0, Weda subprotocol, SOAP encoding, XML, MTOM |
| Service consumer | Proxy stub | Application client, user agent , event source or event sink |
| Process | Discovery, Choreography | Uddi |

Figure 1 gives a high-level process view of WEDA infrastructure and management.

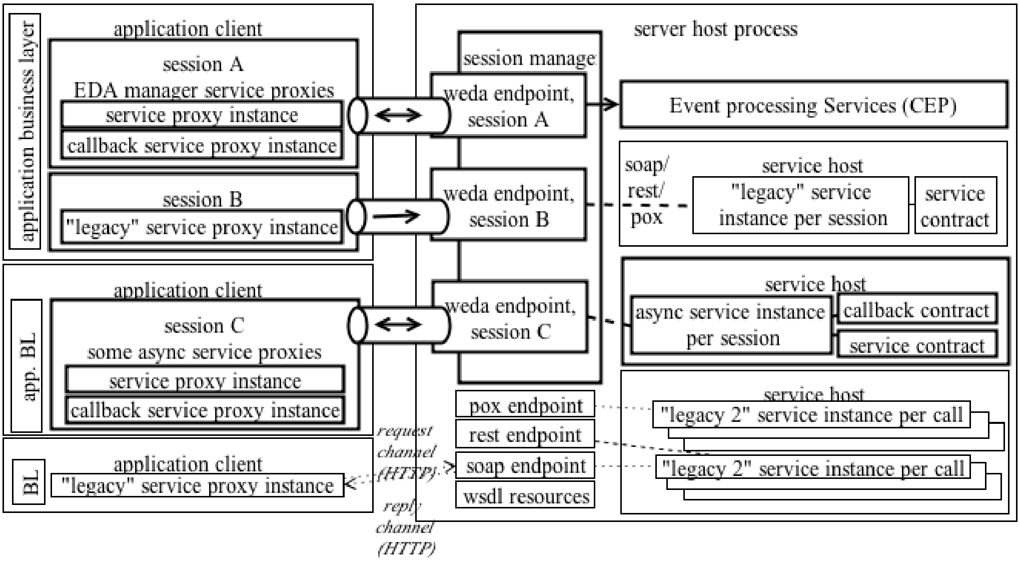


Fig. 1. High-level process view of WEDA infrastructure and management

Schema indicates number of application clients connecting to server host process as usual in client-server style. Server host process runs in standard web server, such as Apache, IIS or it can be console app as well. Figure 1 shows how we can combine existing standards with new parts of stack, allowing the vendors to reuse their code. At the top part of the schema new parts of infrastructure are highlighted by a wider line. Entities of Weda channel stack mentioned in the paper are:

- Weda gateway with session channel manager and endpoint manager components
- Weda channels and Weda subprotocol
- Weda endpoints – addressing, binding, contract and its description

Other topics taking apart:

- Service enhancements – asynchronicity and pipelining, complex event processing
- Implementation, experimental systems, benchmarking

At the bottom of Figure 1 we have a very standard web service host, which is run-time environment that creates and controls web-service's context and instance lifetime and makes it active. Inside service host there is one "legacy" service, instantiated per call. This allows using the service instance by HTTP channel, because state is not maintained between the calls giving us a stateless web service. Stateless web services should have light-weight initialization code (or none at all) that can be called from a single threaded model. Now we will get closer to the highlighted parts.

# 3. WEDA CHANNEL STACK

## 3.1. OVERVIEW

The main purpose of the work is to ensure interoperability between the implementations of different Web services/Weda vendors. The main audience will be the people, who wish to extend a Web services stack with an implementation of Weda. This will enable them to write a Weda implementation that will interoperate with other independent Weda implementations. Channel stack is a layered communication stack with one or more channels that process messages. At the bottom of the stack is a transport channel that is responsible for adoption to the underlying transport. Weda architecture builds upon the duplex web socket connection. We know, that is unusually ambitious in going from very low level (data on the wire) to very high level (application semantics), in a single leap but we need such wideness to make things begin to function. When implemented, it should provide an easy-to-reference API for use in web or desktop applications and should be easily pluggable into the existing stack.

## 3.2.WEDA GATEWAY

Weda gateway (Fig.2) is required component in the architecture style. The defining features are message orientation, queuing, routing.

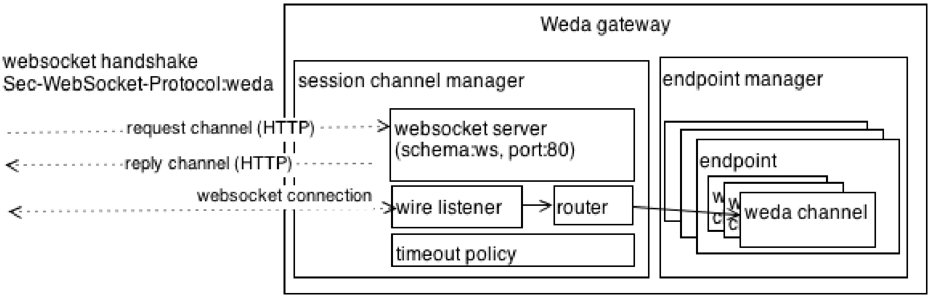


Fig. 2. WEDA gateway

Weda gateway MUST be bootstrapped at the application start and its main responsibility is to configure and run Websocket server, so the frames become accessible by the implementation of Websocket API called here as “wire listener” component and transformed into messages. Wire listener MUST deal with the websocket framing issues. Websocket frame is described by [5] section 5.2. Web socket differs from TCP in that it enables a stream of messages instead of a stream of bytes. Web socket fragmenting mechanism has consequences to providing API, which pull messages into application layer. Our future work will present on how implementation should aware of how to act with fragmented frames because we won’t mention the details here. HTTP servers can share their default HTTP and HTTPS ports (80 and 443) with a Weda gateway. Statefull firewalls only verify that a packet correlates to an existing, unclosed, connection. HTML 5 WebSocket doesn’t require port forwarding. Connections continue to be established from the client, but the client and server swap roles once the connection is established. Web sockets also punch through proxies by using the same CONNECT model that HTTPS uses today. Since firewalls typically simply enforce the rules for inbound traffic rejection and outbound traffic routing, there usually are no specific Web Socket traffic-related firewall concerns.

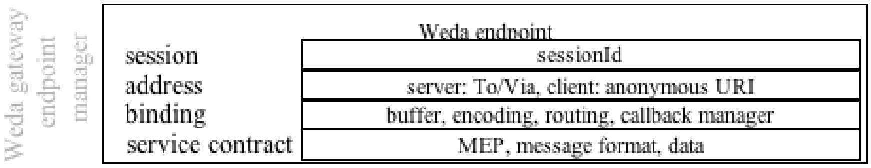
Gateway component called “Endpoint manager” manages resource-based logical endpoints. Weda gateway MUST take care about registering of all configured endpoints, creation of channels and making them listening for incoming messages from the “router” component. When connection aborts for some reason, endpoint manager MUST unregister an endpoint from the gateway. Implementations of Weda Gateway MUST be capable of finalizing a websocket handshake with the subprotocol agreement (Sec-WebSocket-Protocol:weda, underlaying protocol) according to [5].

Weda gateway session channel manager MUST initialize Weda channel (details are not mentioned here). It also SHOULD allow configure session wsdl extension on portType element (useSession = true) and session policies such as idle and session timeouts. This provides the capability to periodically enforce new policies on active user connections and ensures that any system changes to user properties are enforced on existing sessions.

### 3.3.WEDA ENDPOINTS

All communication with a service occurs through its source endpoints. Basically a service exposes endpoints which client consumes. As explained in the previous section, Weda gateway manages endpoints and focuses on mapping the incoming messages to an endpoint. In Weda the endpoint (figure 3) is defined as tuple

```
Weda endpoint = <session, address, binding, service contract>.
```


Weda gateway endpoint manager

|  | Weda endpoint |
|---|---|
| session | sessionId |
| address | server: To/Via, client: anonymous URI |
| binding | buffer, encoding, routing, callback manager |
| service contract | MEP, message format, data |

Fig.3 . schema of WEDA endpoint

An endpoint address uniquely identifies the endpoint for a service. Addresses answer the question “where” to find service by URI and desired behavior, such as message exchange pattern. Weda endpoint addressing consists of logical (To) address and physical (Via) address as on Figure 4. It is fully compatible with WS-Addressing model [6] so upper stack can make use of addresses definitions. Weda specification defines a “To” URI scheme, using the ABNF syntax defined in RFC 5234 [7], and terminology and ABNF productions defined by the specification RFC 3986 [8] as

*weda-URI = "weda:" "//" service endpoint*

service = < a collection of related endpoints>
endpoint = <port, defined in [9], Section 2.13>
and Via URI according to the rules in the Websocket Protocol section 3 [5].

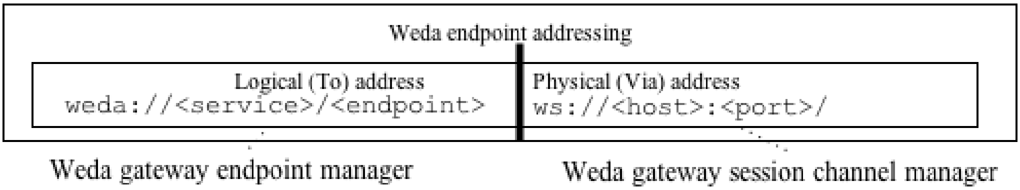

Weda endpoint addressing
Logical (To) address
weda://<service>/<endpoint>
Physical (Via) address
ws://<host>:<port>/
Weda gateway endpoint manager
Weda gateway session channel manager

Fig.4. WEDA endpoint addressing

Client cannot be reached by a meaningful global URI, when implementing a duplex service (chapter 4). Client-side endpoint cannot have a stable, resolvable URI. Endpoint reference address to which the response is to be sent by asynchronous interactions MUST be defined as absolute anonymous logical endpoint address *http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous* with reference id set by Session channel manager. To do so, a web service MUST conform to WedaDuplex WSDL policy assertion. This policy is identified by the URI *http://nti.tul.cz/policy/wedaduplex.* A Web service endpoint with a WedaDuplex policy assertion MUST send any messages intended for the client to the anonymous URI endpoint reference and MUST NOT define other address in the ReplyTo Header.

Endpoint binding specifies transports and protocols and answers the question “how” to find and reach a service. This binding is identified by the URI *http://nti.tul.cz/binding/weda* and described by WSDL 2.0 [9] binding extension. Every Weda endpoint MUST implement an FIFO Input queue buffer onto which incoming messages are placed to await processing by the encoder. Receive window for flow control mechanism is extended from the spare room in the buffer and counted by subtracting a whole input queue buffer size and filled buffer size as

$$RcvWindow = RcvBuffer - ReadMessages \qquad (1)$$

Sender MUST limit data to *RcvWindow*. *RcvWindow* is part of responses. *RcvWindow* should be manageable parameter. We can find right *RcvWindow* by running benchmarks over the system with *RcvWindows* turned off.

Weda transport binding provide listener and factory that is capable of appropriate channel opening and closing and message exchange pattern support. Channel is responsible for preparing and delivering messages in a consistent way. Weda channel is duplex session-aware state machine patterned after some of the fundamental message exchange patterns (duplex, datagram, request-reply) with rules for binding.

Table 2. Digest of rules for binding the MEPs

| No. | Rule description |
|---|---|
| R01 | Weda channels MUST support sessions which implies that all messages on that channel are correlated with each other. |
| R02 | The Weda binding extension MUST be used defining WSDL 2.0 XML representation of Interface Operation Component [9 section 2.4.2]. |
| R03 | Duplex MEP is native MEP for Weda. Since SOAP and REST doesn't support this MEP, Weda channel MUST be capable of transforming messages to the webservices layer MEP (request-reply for standard webservices, datagram for callback duplex services). |
| R04 | Request-reply MEP isn't supported natively by Weda, but the channel's state machine MUST be capable of transforming duplex messages into this MEP since service contract MAY define use of it. Weda session duplex channel must receive or send weda messages only in opened state and must be capable of doing session-durable duplex correlation. Messaging format MUST uniquely identify message in time and space. For SOAP and POX message format, WS-Addressing headers MUST be used and wsa:MessageID MUST be present in the request and wsa:RelatesTo MUST be present in the reply. If wsa:ReplyTo is present in the request, the property MUST equal to anonymous URI. SOAP Request-Response message pattern [10 section 6.2] MUST be defined in the declaration. For REST message format, resource URI MUST present messageId parameter. |
| R05 | Datagram MEP isn't supported natively by Weda, but the channel's state machine MUST be capable of transforming duplex messages into this MEP as defined in the state machine model since service contract MAY define use of it. There MUST NOT be any additional rules such as in HTTP binding empty responses with 202: Accepted header. For SOAP and POX message format, WS-Addressing headers MAY be used and wsa:To MAY be present. SOAP Response message pattern [10 sec. 6.3] MUST be defined in the declaration. Other top level messaging layer can be used, for example to achieve message reliability [11]. |

Endpoint contract answers the question "what" will be transmitted. It specifies message format (how data are serialized by Weda subprotocol and SOAP/REST/XML encodings) and data contract (what data are to be serialized is purposefully left to service implementers with use of existing standards). For defining Weda description, we only will use concrete definitions (binding and service) of WSDL2.0, not abstract ones (types and interface). If user has their formal agreement on interfaces described by the WADL schema, he still can use our WSDL2.0 concrete definitions while preserving the data contract definitions on WADL. When Duplex MEP is used (weda asynchronous services), it MUST be represented as two one-way operation elements - one with input and one with output and when Datagram MEP is used it should provide only the input operation element. Informal definition of Weda subprotocol defines wire messages with applying session channel, flow control and serialization management. We won't describe it here in this paper.

## 4. SERVICE AND SERVICE-CONSUMER ENHANCEMENTS

Weda architecture style can have a large impact on how new services are built. Session service instance has some advantages that old call-living instances didn't have. For example downstream business and data tier could be cached per session (for example ORM model which is expensive to create and forget) and application client can interact with the service from multithreaded environment.

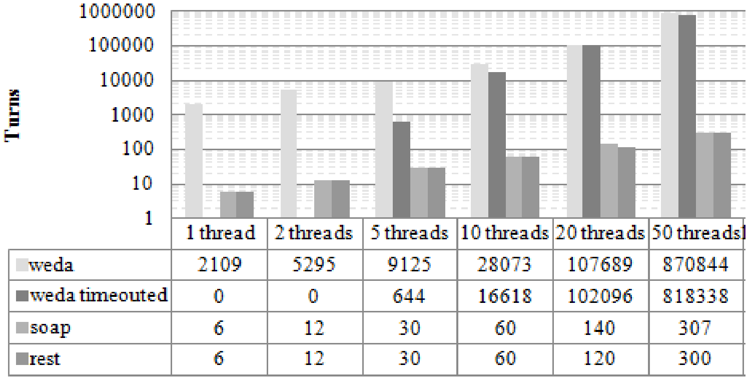
In general, any application participating in a web service interaction is playing a role in a distributed application. As such, it will benefit if it's designed to run asynchronously from other components in the distributed system. Unfortunately while application can be written asynchronously at the moment, the underlying mechanism which could bring asynchronicity to the web services isn't used now. The question is whether it's the web service that's asynchronous, or our access to it. Most likely the services are synchronous, but we are accessing it asynchronously even in modern application. It is because HTTP transport request-reply message exchange pattern doesn't allow us to make real asynchronicity, because callback cannot be invoked. And because of that, service implementers don't develop their web services contracts as duplex. With Weda we can define a duplex service contract. Client must implement client-specific contract called callback contract, which will allow the server to invoke a reply by datagram operation after it finishes time-consuming calculation.

Pipelining in Weda architecture style can lead to bigger bandwidth usage compared with the traditional content delivery technique. Because Websockets can send and receive at any time, are directly controlled by the programmer, and are not subject to proxy interference, the pipelining ability is safe and should not be disabled as with HTTP [12]. There is right reason to disable HTTP pipelining. But none for Weda.

In Weda architecture style we have offered a set of components which can provide practical event-based behavior of theoretically known concept of SOA 2.0. We are calling it Weda event processor cumulatively. This component is OPTIONAL and client and server don't need to implement it. Description of whole eventing system in Weda we left on other paper. In short - complex event processing engine linked on WEDA endpoint and duplex services are encapsulated into the Weda event processor component. Subcomponent called Weda dispatcher allowing us using existing WS-eventing [13] standards on subscription service. Statement service does administration of topics, defined here as EPL rules (by domain experts). Notification service makes use of duplex callback contract definition of Weda.

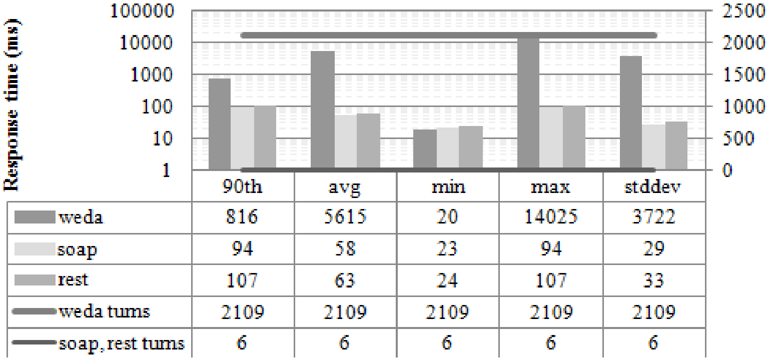
## 5. IMPLEMENTATION, EXPERIMENTAL SYSTEMS AND BENCHMARKING

We implemented Weda architectural style into Weda API. On this API we built two experimental systems. On server side resides OGC Sensor Observation Service [14] with LittleBear spatial database and OGC Sensor Alert Service and Weda eventing processor. At the client side two client applications were made. Web application is public GIS Viewer system which presents SOS service's data graphically upon public WMS layers while those data loaded over Weda. SOS is standard service integrated to the new architecture without changes in contracts and business logic. Desktop client application was extended to load testing tool (none existed) allowing us to do real benchmarks of Weda against REST and SOAP over HTTP SOS service. At the end of this paper we are presenting excerpts of results of Weda performance attributes in comparison to REST and SOAP over HTTP.  We prepared a request-reply operation of OGC Sensor observation service GetCapabilities. We ran request for constant three minutes period. The results on Figure 5 show big increase of number of processed requests. Test ran with disabled flow control mechanism so we can view time outing (responses after more than 30s) limits of architecture. With flow control on and right message window configured, the difference of processed messages still is interestingly big. Response time for 1 client is although slightly worse, since server is processing much more concurrent requests in parallel. Still we talk about 90th percentile with RTT less than 816ms while processing 2019 requests in 3minutes.



| | 1 thread | 2 threads | 5 threads | 10 threads | 20 threads | 50 threads |
|---|---|---|---|---|---|---|
| weda | 2109 | 5295 | 9125 | 28073 | 107689 | 870844 |
| weda timeouted | 0 | 0 | 644 | 16618 | 102096 | 818338 |
| soap | 6 | 12 | 30 | 60 | 140 | 307 |
| rest | 6 | 12 | 30 | 60 | 120 | 300 |

Fig.5. WEDA turns per threadcount with *RcvWindow* Off (burst strategy 5ms, delay 30s, duration 3min)



| | 90th | avg | min | max | stddev |
|---|---|---|---|---|---|
| weda | 816 | 5615 | 20 | 14025 | 3722 |
| soap | 94 | 58 | 23 | 94 | 29 |
| rest | 107 | 63 | 24 | 107 | 33 |
| weda turns | 2109 | 2109 | 2109 | 2109 | 2109 |
| soap, rest turns | 6 | 6 | 6 | 6 | 6 |

Fig.6. Response times for 1 thread (burst strategy 5ms, delay 30s, duration min) and turns

## 6. CONCLUSION AND FUTURE WORK

We presented an overview of Weda architectural style, new possible service enhancements and excerpts of benchmark results measured on developed experimental systems that use implementation of Weda API. Results appear to be very promising as well as new capabilities leading to World Wide Web based ESB platform. In future posts we will focus on deeper descriptions of outlined components and formal description and verification of architectural style.

## ACKNOWLEDGEMENT

This work was supported by the Ministry of Education of the Czech Republic within the SGS project no. 78001/115 on the Technical University of Liberec.

## REFERENCES

[1] Web Services Glossary - http://www.w3.org/TR/2004/NOTE-ws-gloss-20040211/, 2013-24-18

[2] Hugh TAYLOR, Angela YOCHEM, Les PHILLIPS, and Frank MARTINEZ. 2009. *Event-Driven Architecture: How SOA Enables the Real-Time Enterprise (1st ed.)*. Addison-Wesley Professional.

[3] Web Services Architecture - http://www.w3.org/TR/ws-arch/, 2013-01-12

[4] CHAPPELL, David A.: Enterprise service bus - theory in practice. : O'Reilly, 2004. - ISBN 978-0-596-00675-4

[5] The WebSocket Protocol RFC6455 - http://tools.ietf.org/html/rfc6455, 2013-06-28

[6] Web Services Addressing - http://www.w3.org/Submission/ws-addressing/, 2013-06-01

[7] Augmented BNF for Syntax Specifications: ABNF – http://tools.ietf.org/html/rfc5234, 2013-01-18

[8] Uniform Resource Identifier (URI) – http://www.ietf.org/rfc/rfc3986.txt, 2013-06-04

[9] Web Services Description Language Version 2.0 – http://www.w3.org/TR/wsdl20/ - 2013-06-17

[10] SOAP Version 1.2 Part 2 - http://www.w3.org/TR/2007/REC-soap12-part2-20070427/, 2013-05-14

[11] Web Services Reliable Messaging - http://docs.oasis-open.org/ws-rx/wsrm/200702, 2012-12-05
[12] Hypertext Transfer Protocol -- HTTP/1.1 Pipelining - http://tools.ietf.org/html/rfc2616#section-8.1.2.2, 2013-05-18
[13] Web Services Eventing - http://www.w3.org/Submission/WS-Eventing/, 2013-06-18
[14] OGC® Sensor Observation Service - http://www.opengeospatial.org/standards/sos, 2013-06-28

*Web server performance, spatio-temporal prediction,*
*geostatistical estimation methods, kriging*

Anna KAMIŃSKA-CHUCHMAŁA*, Tomasz SALWA

# SPATIAL WEB SERVER PERFORMANCE PREDICTION WITH USING GSLIB

In recent years, we can see a huge growth in communication networks. The Internet has become widely available, not only at home, school or office, but almost everywhere using mobile technology. Many users of smartphones can connect to the Internet. Nowadays more and more people use network, not only to browsing Web pages, but also to use multimedia. Is coming new era – Internet of Things. As one can see, research on network performance and its prediction, is nowadays an important aspect of Web development.

This paper proposes to use of geostatistical estimation methods: Simple Kriging and Ordinary Kriging to prediction network performance in a selected period of time. The data used to estimation where derived from MWING (Multi-agent Web pING) developed by the Distributed Computer Systems Division at Wroclaw University of Technology. In this paper authors consider two agents installed in Gdańsk and Las Vegas, which was being connected to the mostly European servers.

First of all, preliminary data analyses were made. In the next step, 3D predictions were performed with using open source library GSLIB. Finally, the estimation results of Simple Kriging and Ordinary Kriging were compared with each other. The conclusions ending the paper.

## 1. INTRODUCTION

Due to the need to work on improvement of the Web performance, the research of prediction Web server loads is required. Moreover, possibility of new quality of prediction is also very important. By the time, in Web performance prediction were using in 2D methods (for example neural networks and time series [6] or genetic algorithm [9]) given only temporal information about considered Web server. In this paper spatio-temporal (3D) methods were applied. They belong to geostatistical estimation

* Institute of Informatics, Wroclaw University of Technology, 50-370 Wrocław, Wybrzeże Wyspiańskiego 27, Poland

methods, which results give information not only about how predicted performance of Web server was changed in time (temporal), but also how performance of Web in whole considered area (space) looks like.

In the following section two estimation methods from geostatistics: Ordinary and Simple Kriging were described. After that, next section is focused on analysis of database and discussion of the experiment, from which data was obtained. In subsequent section was given in detail models of predictions and their results, additionally these two methods of predictions are compared to each other. The last section summarized all conducted research with indication of the main goal of predictions.

## 2. KRIGING ESTIMATION METHODS

Kriging method was invented by engineer Daniel G. Krige in 1950 [7]. Kriging is a geostatistical estimation method, where in order to creating predictions linear combinations of research variables are used. Estimation is conducted by weight of mean. Analysis of variables *Z* (for example observation of performance) are allocated to weights *w* (kriging of weights), what caused minimization of estimation variance (called kriging variance), which is calculated as a function of assumed model of variogram e.g. localization of server between them and relative to point or block which is estimated. Kriging method is using to obtain “local estimation”, because respect only the data from the nearest neighborhood [8].

The fundamental of kriging technique are Simple Kriging (SK) and Ordinary Kriging (OK), which are described below.

### 2.1. SIMPLE KRIGING (SK)

Simple Kriging is based on knowing local mean *s* of research variable *Z(x)* (e.g. download file times from given server). In this method local means have values close to global mean (e.g. mean of download file times from all research servers). To local mean *s* weight *w* is assigned. Simple Kriging estimator is given by the formula:
where:

$$Z^*(x) = s + \sum_{i=1}^{N} w_i(Z(x_i) - s), \tag{1}$$

$Z(x_i)$- a random variable at each of the N locations constructed the data locations $x_i$;
$s$- mean;
$w_i$- weight of residua $(Z(x_i) - s)$.

Estimation error is formulated as difference between predicted and real measurement values of download time:

$$Z^*(x_0) - Z(x_0), \tag{2}$$

$$E[Z^*(x_0) - Z(x_0)] = 0. \tag{3}$$

When estimate error is equal 0, then it means that estimator is unbiased.

### 2.2. ORDINARY KRIGING (OK)

In Ordinary Kriging methods the local means $s$ are unknown [5] and their values do not have to be close to global mean (in our case to mean performance of Web servers). Mean estimate is conducted only for servers in local neighborhood. Ordinary Kriging could be calculated for estimate values at given point, localization (for considered server) and is so called Ordinary Point Kriging or for some given area (block) and called Ordinary Block Kriging. Weighted mean of performance is formulated as:

$$Z^*(x) = \sum_{i=1}^{N} w_i Z(x_i), \tag{4}$$

where:

$Z(x_i)$- value of research variable;
$w_i$- weight coefficient.

Important element in this method is proper selection of krigings coefficient (weights) $w_i$, so that the sum is equal unity:

$$\sum_{i=1}^{N} w_i = 1. \tag{5}$$

## 3. DATABASE ANALYSIS

The database for this research, were collected during active measurements made by the Internet measurement infrastructure called MWING (Multi-agent Web pING) system [2], [3]. The data was collected by MWING agents located in two places: Gdansk and Las Vegas (see figure 1). Web performance was measured by total downloading time of rfc1945.txt file, which size was equal 138 kB. This experiment relay on Web transactions with using HTTP protocol.

The database contains the information about a server's geographical location which the agent targeted, the web performance variable which is the total downloading time of rfc1945.txt file, and the timestamp of taking a measurement. The data were measured in the two intervals: between 7th and 28th of February 2009 for agent in Gdansk and between 1st and 31th of May 2009 for agent in Las Vegas and they were taken every day at the same time: at 06:00 a.m., 12:00 p.m., and 6:00 p.m.

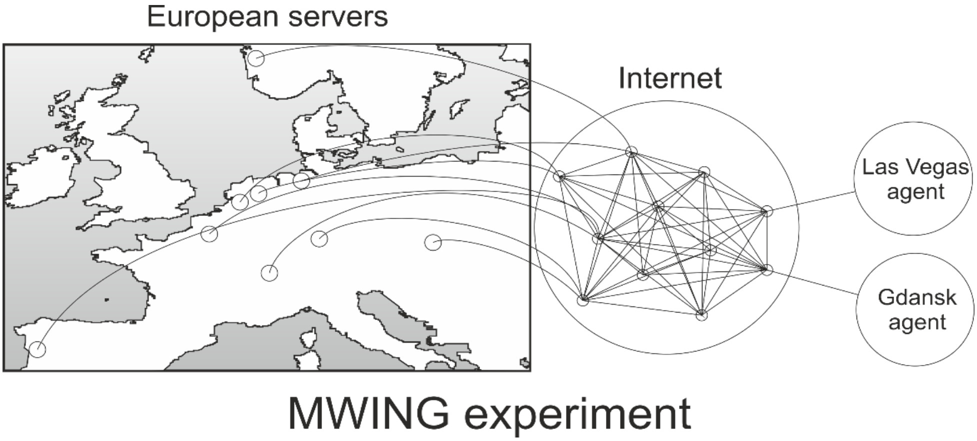


Fig. 1. Internet measurement infrastructure system – MWING

Basic statistics from database obtained from agent located in Gdansk are presented in table 1. This statistics indicate (especially variability coefficient and kurtosis) the high variability of Web server performance. The largest fluctuation had a measurement of download time of file for 06 a.m. The difference was between 0.11s to 29.06s. However mean value was equal 0.6s and standard deviation 1.59s. It means that the most of downloads was done quickly and indicated high values of download time appeared occasionally as unpredictable peaks.

Table 1. Fundamental statistics of total download file – database from Gdansk

| | Minimum value [s] | Mean value [s] | Maximum value [s] | Standard deviation [s] | Variability coefficient [%] | Skewness | Kurtosis |
|---|---|---|---|---|---|---|---|
| 06 a.m. | 0.11 | 0.60 | 29.06 | 1.59 | 266.01 | 15.41 | 266.01 |
| 12 p.m. | 0.12 | 0.62 | 12.15 | 1.08 | 173.66 | 7.28 | 61.95 |
| 06 p.m. | 0.12 | 0.60 | 7.93 | 0.77 | 128.92 | 5.01 | 32.03 |

Additionally skewness coefficient for whole considered research hours was equal more than 3, thus the data should be transform to logarithmic values, because of significant asymmetry. It is important from point of view of further predictions, because in geostatistical methods the data should be close to symmetric distribution.

In figures 2 and 3 exemplary histograms for 06 a.m. with the data before and after logarithmic calculation are presented. The histogram in figure 2 with original data is characterized big ride side asymmetry of distribution. This explain the fact that the skewness coefficient is such high and equals more 15 for 06 a.m.

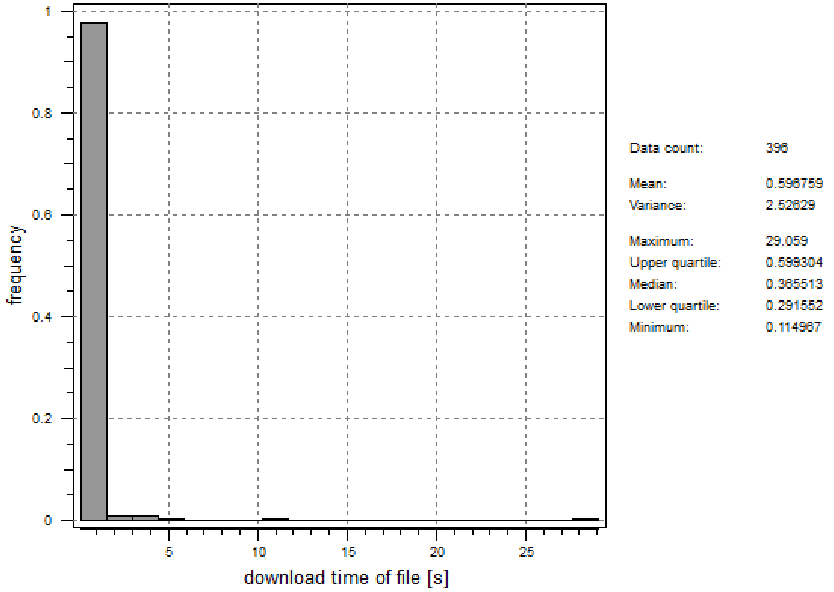


Fig. 2. Histogram of total download time for 06 a.m. (data obtained from agent in Gdansk)

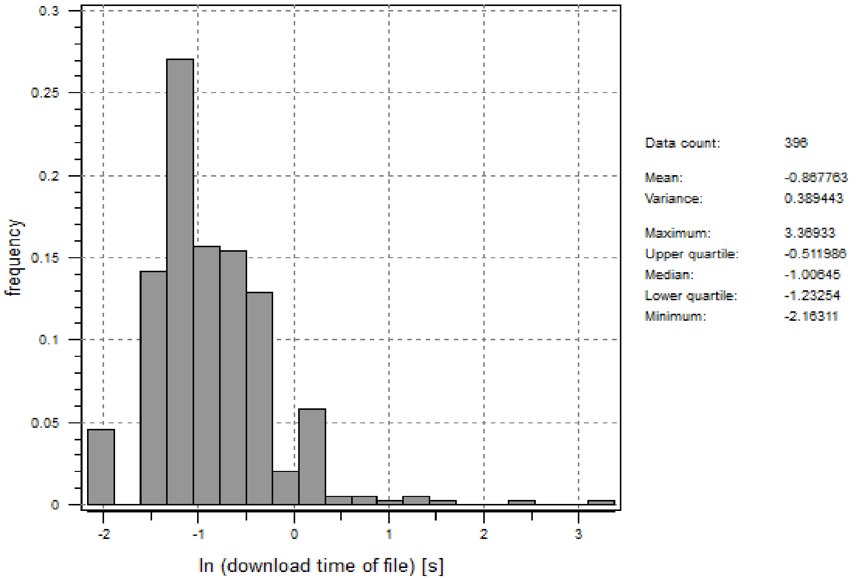


Fig. 3. Histogram of total download time after logarithmic calculation for 06 a.m. (data obtained from agent in Gdansk)

In table 2 statistical parameters for data from agent in Las Vegas are presented. It is observed that minimum value of download time is increasing in comparison to minimum values from agent in Gdansk. This behaviour could be caused by longer distance between agent in Las Vegas in America and servers in Europe than agent in Gdansk in Europe and servers in Europe. Moreover mean value is higher too, in interval between 2.5s to 2.7s. In this data also appeared unpredictable peaks even equals 32s for 06 p.m., but they are only sporadic cases. Skewness coefficient is less than 3 only for 12 p.m., thus merely this data will be original without logarithmic calculation for further predictions.

Table 2. Fundamental statistics total download file – database from Las Vegas

| | Minimum value [s] | Mean value [s] | Maximum value [s] | Standard deviation [s] | Variability coefficient [%] | Skewness | Kurtosis |
|---|---|---|---|---|---|---|---|
| 06 a.m. | 0.28 | 2.49 | 21.71 | 3.04 | 121.74 | 3.51 | 12.92 |
| 12 p.m. | 0.29 | 2.70 | 16.44 | 3.15 | 116.94 | 2.83 | 7.90 |
| 06 p.m. | 0.29 | 2.65 | 31.87 | 3.25 | 122.76 | 3.74 | 19.40 |

Following step in conducted research is the calculation of directional variograms along time axis necessary for geostatistical prediction methods. As example, in figure 4 variogram function is approximated by theoretical spherical model for 06 a.m. from agent in Gdansk. Both for histogram and variogram graphical calculation Stanford Geostatistical Software Modeling (SGeMS) was used [1].

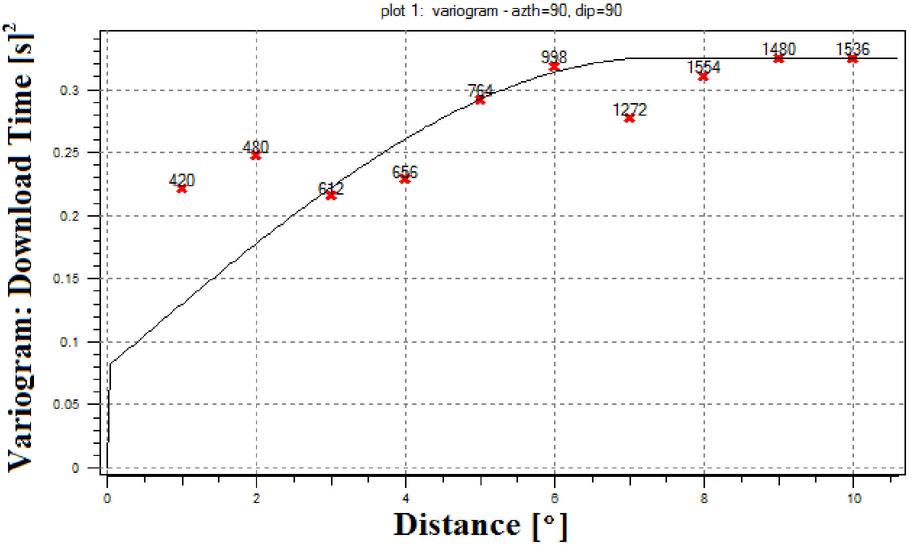


Fig. 4. Directional variogram for 06 p.m. from agent in Gdańsk approximated with spherical function

## SPATIAL WEB SERVER PERFORMANCE PREDICTION RESULTS

For computing spatial Web server performance prediction with geostatistical estimation methods: SK and OK Geostatistical Software Library (GSLIB) was used (especially KT3D program). It is an open source collection of geostatistical programs developed at Stanford University [10].

Prediction length for data from agent in Gdansk was calculated for 4 days long, between 1st to 4th March 2009. Data obtained from agent in Las Vegas was using to compute with one week horizon length i.e. 1st to 7th June 2009.

In table 3 and 4 statistical results, the best which could obtained from predictions models, are presented. Analyzing global statistics in table 3 from agent in Gdansk it is visible that similar results for both kriging methods: SK and OK were obtained. Minimum predicted value of download time for 06 p.m. equals 0.15s in case of OK and 0.17s for SK, which is a difference of only 0.02s. Discrepancy between minimum and maximum download of time and variability coefficient for both methods are the smallest for 12 p.m. Moreover variance and standard deviation are the largest for 06 p.m. Average percentage error of prediction *ex post* is the highest for 06 a.m. due to meaningful variability of data also approved by the high skewness coefficient (more than 15). For other hours error of prediction was close to 20% for both methods, what mean good prediction accuracy.

Table 3. Global statistics for predicted total download file – database from Gdansk

| Simple Kriging - SK | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Minimum value [s] | Mean value [s] | Maximum value [s] | Standard deviation [s] | Variability coefficient [%] | Variance $[s]^2$ | Average error of prediction [%] |
| 06 a.m. | 0.26 | 0.48 | 1.19 | 0.21 | 44.50 | 0.05 | 33.52 |
| 12 p.m. | 0.23 | 0.48 | 1.03 | 0.20 | 40.89 | 0.04 | 23.18 |
| 06 p.m. | 0.17 | 0.44 | 1.28 | 0.24 | 55.99 | 0.06 | 20.19 |
| Ordinary Kriging - OK | | | | | | | |
| 06 a.m. | 0.26 | 0.49 | 1.23 | 0.22 | 46.11 | 0.05 | 33.50 |
| 12 p.m. | 0.22 | 0.49 | 1.05 | 0.21 | 42.63 | 0.04 | 22.75 |
| 06 p.m. | 0.15 | 0.44 | 1.29 | 0.25 | 58.00 | 0.06 | 19.48 |

In table 4 predicted download time for OK and SK methods from agent in Las Vegas are presented. The best accuracy of prediction (only little above 20%) for both methods was for 06 a.m. The main reason of this situation is fact that dispersion through the data here and also variability coefficient are the smallest. The maximum values (above 7s) is the highest for 06 p.m. for both methods. Interesting phenomenon occur for 12 p.m., namely error is the biggest, because only these data are original and no logarithmized. This is due to the fact that skewness coefficient was equal less than 3 (2.83s), but it is already sufficient value meaning on dispersion of data.

Table 4. Global statistics predicted total download file – database from Las Vegas

| Simple Kriging - SK | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Minimum value [s] | Mean value [s] | Maximum value [s] | Standard deviation [s] | Variability coefficient [%] | Variance $[s]^2$ | Average error of prediction [%] |
| 06 a.m. | 0.32 | 1.45 | 1.91 | 0.44 | 30.28 | 0.19 | 20.64 |
| 12 p.m. | 0.37 | 2.26 | 6.62 | 1.43 | 63.49 | 2.05 | 45.28 |
| 06 p.m. | 0.34 | 2.15 | 7.33 | 1.72 | 80.29 | 2.97 | 29.40 |
| Ordinary Kriging - OK | | | | | | | |
| 06 a.m. | 0.32 | 1.45 | 1.91 | 0.44 | 30.30 | 0.19 | 20.62 |
| 12 p.m. | 0.36 | 2.25 | 6.62 | 1.44 | 64.12 | 2.07 | 44.48 |
| 06 p.m. | 0.34 | 2.20 | 7.51 | 1.82 | 82.63 | 3.31 | 30.59 |

Spatial prediction of Web server performance with using geostatistical estimation methods OK and SK give us information not only about performance in considered servers, but also information about performance about whole considered area. In figure 5 raster map is presented. Figure 5 show Web performance in 1st March 2009 from point of view agent in Gdansk for 06 p.m.

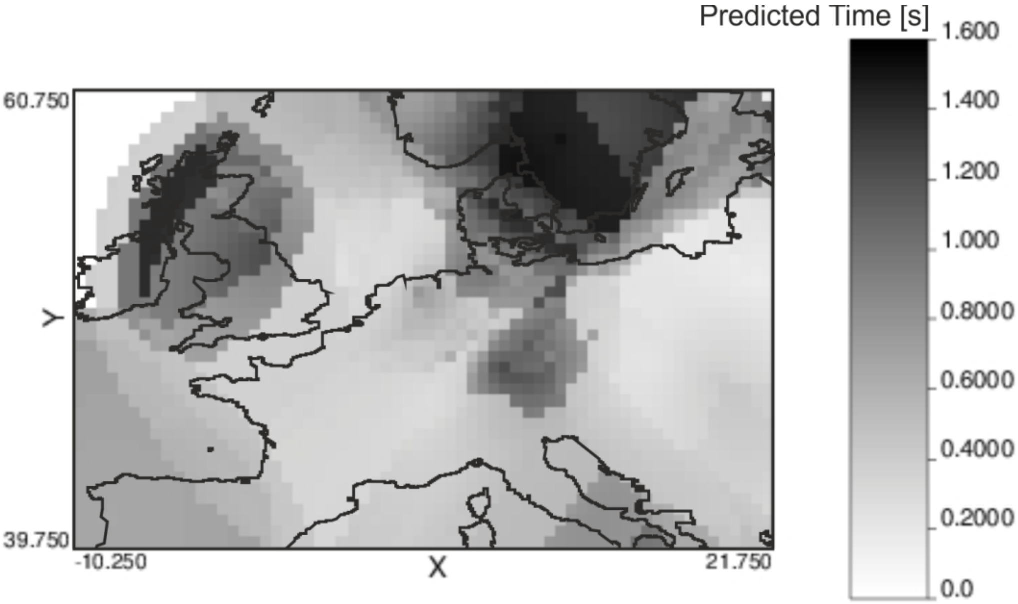


Fig. 5. Predicted download time in Europe from agent in Gdansk for 06 p.m. in 1st March 2009

For better analyzing Web server performance is considered exemplary Web server in Budapest from the point of view agent in Las Vegas. In figure 6 total downloads of file from server in Budapest (Hungary) during May 2009 are presented. Length of time during download file for whole month is very differential and fluctuated between 2s to 10s. As could be seen, there is no easily recognizable pattern of the behavior of this server in the course of considered month. Thus, prediction of performance such variable Web server with good accuracy is very difficult.

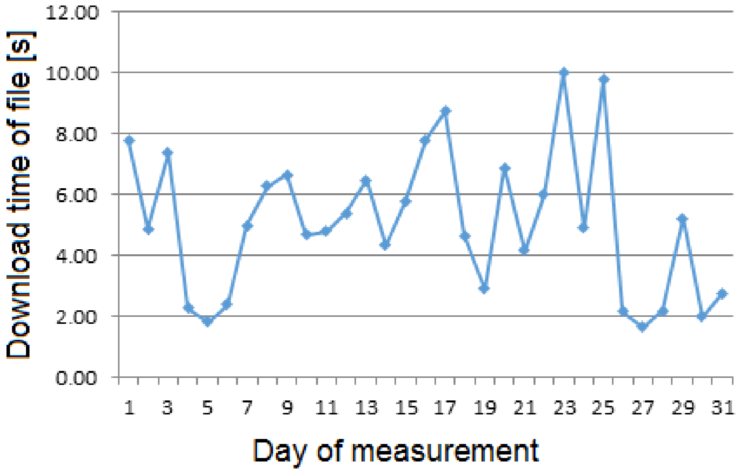


Fig. 6. Download time of file in Budapest server from agent in Las Vegas in May 2009

In table 5 comparison of predicted and real download time file from considered server in Budapest are presented. Predicted values are compute with using SK method for one week advance. The data are obtained from agent located in Las Vegas.

Table 5. Comparison of predicted (with using SK) and real total download file from server in Budapest, Hungary between 1st and 7th June 2009– database from agent located in Las Vegas

| | Real download time for 06 a.m. [s] | Predicted download time for 06 a.m. [s] | Real download time for 12 p.m. [s] | Predicted download time for 12 p.m. [s] | Real download time for 06 p.m. [s] | Predicted download time for 06 p.m. [s] |
|---|---|---|---|---|---|---|
| 01.06 | 1.4312 | 1.6119 | 7.4489 | 3.3740 | 5.7879 | 7.3292 |
| 02.06 | 1.8244 | 1.6092 | 9.1395 | 3.1551 | 6.8980 | 7.1564 |
| 03.06 | 4.3649 | 1.6036 | 5.3916 | 3.0597 | 9.4279 | 6.9878 |
| 04.06 | 1.6144 | 1.6111 | 4.8424 | 2.9553 | 7.4339 | 6.8233 |
| 05.06 | 3.4350 | 1.6121 | 3.0850 | 2.8080 | 7.9734 | 6.6628 |
| 06.06 | 1.8271 | 1.6004 | 3.4467 | 2.8478 | 9.2409 | 6.3530 |
| 07.06 | 1.6399 | 1.5981 | 6.2987 | 2.9720 | 10.9074 | 6.2102 |

Very interesting phenomena could be seen in this results in table 5, - for original database (not logarithmized) for 12 p.m. error *ex post* is the highest and equal more than 40% and also difference between minimum and maximum values is significant. The shortest times of download are for 06 a.m. with error equal 22.7%. However, the best accuracy of prediction in this cases is for 06 p.m. and error of prediction is equal 22%.

## 5. CONCLUSIONS

Spatio-temporal geostatistical methods: SK and OK were used to prediction Web server performance in this paper. Results of prediction process were described and accuracy of prediction was discussed. Authors concluded, that estimation methods SK and OK could be useful for analysing and predicted Web server performance. These estimation methods and also simulation methods from group of geostatistical methods give new possibility of spatial prediction in this field. Authors compared methods from group of geostatistical methods in [4].

As further research it will be valuable to perform new active experiment with agents in new localizations, prepare new models and work regarding better accuracy of prediction.

## REFERENCES

[1] BOHLING G., *SGeMS Tutorial*, Idaho, 2007.

[2] BORZEMSKI L., *The experimental design for data mining to discover web performance issues in a Wide Area Network*, Cybernetics and Systems: An International Journal 41, 2010, 31-45.

[3] BORZEMSKI L., CIHCOCKI L., KLIBER M., *Architecture of Multiagent Internet Measurement System MWING Release 2,* In: Hakansson, A., Nguyen, N.T., Hartung, R.L., Howlett, R.J., Jain, L.C. (eds.) KES-AMSTA 2009. LNCS, vol. 5559, Springer, Heidelberg 2009, 410–419.

[4] BORZEMSKI L., KAMIŃSKA-CHUCHMAŁA A., *Web performance forecasting with kriging method*, Contemporary Challenges and Solutions in Applied Artificial Intelligence Studies in Computational Intelligence, Springer, Vol. 489, 2013, 149-154.

[5] CHILES J., DELFINGER P., *Geostatistics: Modeling Spatial Uncertainty*, 2nd edition, Wiley, 2012.

[6] CORTEZ P., RIO M., ROCHA M., SOUSA P., *Multi-scale Internet Traffic forecasting using neural networks and time series methods*, Expert Systems, Vol. 29, Issue 2, May 2012, 143-155.

[7] HENGL T., *A Practical Guide to Geostatistical Mapping of Environmental Variables*, European Communities, 2007.

[8] WACKERNAGEL H., *Multivariate Geostatistics: an Introduction with Applications*, Springer, Berlin 2003.

[9] WANG C., ZHANG X., YAN H., ZHENG L., *An Internet Traffic Forecasting Model Adopting Radical Based on Function Neural Network Optimized by Genetic Algorithm*, First International Workshop on Knowledge Discovery and Data Mining, 2008, WKDD 2008, 367-370.

[10] http://www.gslib.com/

*Web traffic analysis, log file analysis, user session, Web server, Web store, online store, e-commerce, electronic commerce, B2C, Business-to-Consumer*

Grażyna SUCHACKA*

# STATISTICAL ANALYSIS OF BUYING AND NON-BUYING USER SESSIONS IN A WEB STORE

The analysis of Web server log files has been the main way to discover Web server workload characteristics and Web user behavioral patterns. It is especially useful in online retail environments as the additional knowledge of customer behavior may be used to boost the Web site conversion rate and thus, to increase the revenue from e-business. The paper discusses results of the session-based analysis of data obtained from online bookstore logs. In particular, it presents a comparison of buying and non-buying user sessions in terms of the session length, duration, and mean time per page. The findings show significant differences in characteristics of both kinds of sessions.

## 1. INTRODUCTION

Capabilities of capturing knowledge on Web users' behavior have gained a huge interest in recent years. Along with the popularization of offline and online analytical applications, the Web analytics became available for everybody. Especially online retailers can hugely benefit from analytical tools. The analysis of e-customers' behavior and identification of factors characterizing buyers vs. non-buyers allow online retailers to optimize the Web site structure, to personalize the Web service, to apply efficient product recommendation strategies, and to support marketing decisions.

In the scientific literature, the issue of valuation and prioritization of user sessions in online stores has gained much attention (e.g., in [1, 2, 3, 4, 6, 7, 8]). In fact, e-customers exhibit differentiated navigational patterns on a Web store site, corresponding to their differentiated needs, expectations, and goals. Most of users remain only visitors browsing products available in a store, reading information on them, comparing prices, etc. Only a very small fraction of all visitors are buyers finalizing a pur-

* Opole University, Institute of Mathematics and Informatics, ul. Oleska 48, 45-052 Opole, Poland.

chase transaction and that is why characterization of their sessions is so important. The main way to discover knowledge on e-customers has been the analysis of historical data recorded in Web server access logs, especially by using data mining methods.

In our data set, only 0.6% of all user sessions (excluding robot-generated and administrative sessions) ended with a purchase. One may expect that the users conducting these sessions spent more time on the site and opened more Web pages than other users. The goal of this paper is characterization of sessions ended with a purchase vs. sessions without the purchase in terms of the number of visited pages, the duration of a user-site interaction, and the mean time per page. To the best of our knowledge, no such comparative analysis has been conducted so far. It is a part of a wider study aimed at the identification of factors characterizing more valuable user sessions and working out a method for predicting the probability of making a purchase online.

## 2. STATISTICAL ANALYSIS OF USER SESSIONS

The analysis was based on access log files obtained from a Polish online bookstore (the store name is not given in the paper due to a non-disclosure agreement). Data was collected for a period of one month, in December 2011. A dedicated C++ computer program was used to read, preprocess, clean, and analyze the data.

First, data describing HTTP requests was read from log files and preprocessed. Then, data was cleaned – since our goal was a click-stream analysis, data corresponding to hits for embedded objects (such as graphical and video files), as well as page requests generated by robots and connected with administrative tasks, was eliminated from the initial data set.

Afterwards, based on HTTP request records, user sessions were identified. A *user session* means a sequence of page requests issued by a given user during the visit in the Web store. Each individual user was identified based on two data fields describing each HTTP request: a client IP address and a client browser information. Consecutive user sessions were reconstructed based on requests' arrival times, assuming a minimum 30-minute interval between two subsequent sessions of a given user.

Using a graphical method [5], outlier sessions were identified and excluded from the data set. Eventually, the analyzed data encompassed 16 077 user sessions. Based on these sessions, we investigated some statistics regarding the aggregate behavior of users visiting the Web store. First, we glance at all user sessions and then analyze the "non-accidental" sessions, dividing them into two separable groups: buying sessions (i.e., sessions ended with a purchase confirmation) and non-buying sessions.

### 2.1. PRELIMINARY DATA ANALYSIS

A very important aspect of a user session analysis in a Web store is the *session length* which is the number of pages requested by the user during the session. One can infer that the more pages a user visits during the session, the more interested in the site content the user is. Session length statistics for all 16 077 sessions are presented in the second column of Table 1. The mean number of pages per session is equal to 3.7 – this is a rather pessimistic result for a Web store site, given that making a purchase by a user requires making many actions on the site, i.e., visiting many pages: selecting products, adding them to the shopping cart, user registration or logging on, and realization of a multiple-step checkout process (however, this result does not diverge from results reported for other Web sites).

Table 1. Session length statistics (in number of pages)

| **Statistics** | **All sesssions** | **"Non-accidental" sessions** |
|---|---|---|
| Mean | 3.7 | 8.3 |
| Median | 1 | 4 |
| Mode | 1 | 2 |
| Standard deviation | 9.4 | 14.8 |
| Minimum | 1 | 2 |
| Maximum | 193 | 193 |

Comparison of the mean with other statistics for all sessions indicates that the distribution of the session length is strongly right-skewed. The median is lower than the mean and it is equal to 1, which means that more than half of the visitors ended their sessions just after entering the site. In fact, 9 036 sessions, i.e., about 56%, contained only one page. The median and the mode are equal to the minimum and the maximum is quite high.

Such results suggest that most of visitors entered the Web store "by accident", probably following a search engine link or clicking on a banner add located on a Web page referring to the Web store. This may be an indication that ads were placed on inappropriate pages or ad contents does not correspond to the store site well.

Taking into consideration the "accidental" character of many user sessions, we decided to exclude such sessions from further analyses and to analyze only sessions which contain more than one page and last longer that one second (they are called *"non-accidental" sessions* throughout the paper). There were 5 481 such sessions. The session length statistics for "non-accidental" sessions are presented in the third column of Table 1. One can observe that results are more optimistic in this case, and especially the mean, the median, and the mode are higher.

In the next subsection we explore characteristics of two kinds of "non-accidental" sessions:

- *buying sessions* (i.e., sessions in which users made a purchase confirmation action), in the number of 5 381, and
- *non-buying sessions*, in the number of 100.

We attempt to find differences between these two kinds of sessions. In particular, we want to identify factors characterizing buying sessions, i.e., such session characteristics which increase the probability of making a purchase in the Web store.

### 2.2. COMPARISON OF BUYING AND NON-BUYING SESSIONS

The first session attribute analyzed in the context of a purchase confirmation action on the site is the *session length*. Results presented in Table 2 show significant differences in numbers of pages visited by users depending on the kind of session. For buying sessions the mean, the median, the mode, and the minimum are one order of magnitude higher than for non-buying ones. The minimum buying session's length is equal to 12, although at least half buyers visited as many as 52 pages in their sessions.

Table 2. Session length statistics for non-buying and buying sessions (in number of pages)

| **Statistics** | **Non-buying sessions** | **Buying sessions** |
|---|---|---|
| Mean | 7.3 | 65.7 |
| Median | 4 | 52 |
| Mode | 2 | 34 |
| Standard deviation | 11.7 | 41.3 |
| Minimum | 2 | 12 |
| Maximum | 193 | 183 |

Fig. 1-left shows a histogram of session lengths for non-buying sessions. The histogram illustrates a strong right-skew of session length distribution. It is confirmed in Fig. 2-left, presenting a cumulative distribution of non-buying sessions lengths. 56 % of non-buying sessions contain less than five pages and 90% contain less than 16 pages. Longer sessions are rare; in particular, only 2% of non-buying sessions contain more than 40 pages.

For buying sessions, the distribution of session lengths is not so strongly right-skewed and does not include such a long tail as for non-buying sessions (Fig. 1right). The mean (65.7) is not much higher than the median (52). Most of sessions contain from 23 to 45 pages; however, the standard deviation (41.3) is much higher than for non-buying sessions (11.7).

A cumulative distribution of session lengths in Fig. 2-right confirms that 50% of buying sessions contain more than 52 pages and 10% contain more than 136 pages.

Such results are not surprising and confirm the intuition that users who open more pages during their visits in a Web store are more interested in making a purchase.

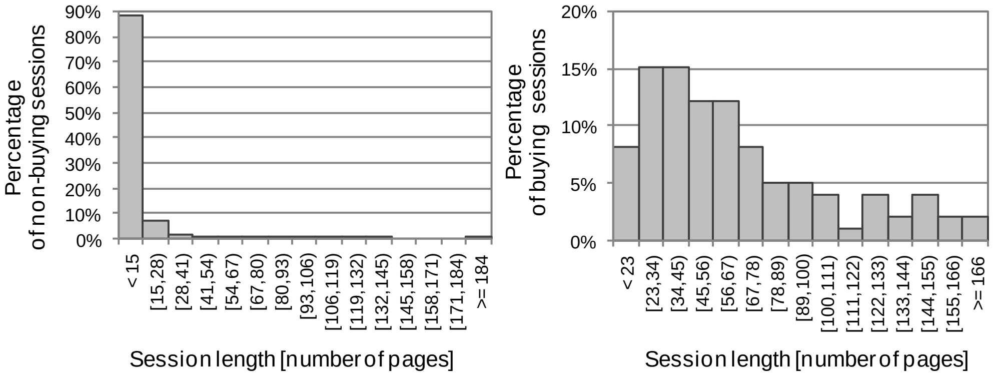


Fig. 1. Histogram of session lengths: (left) for non-buying sessions, (right) for buying sessions

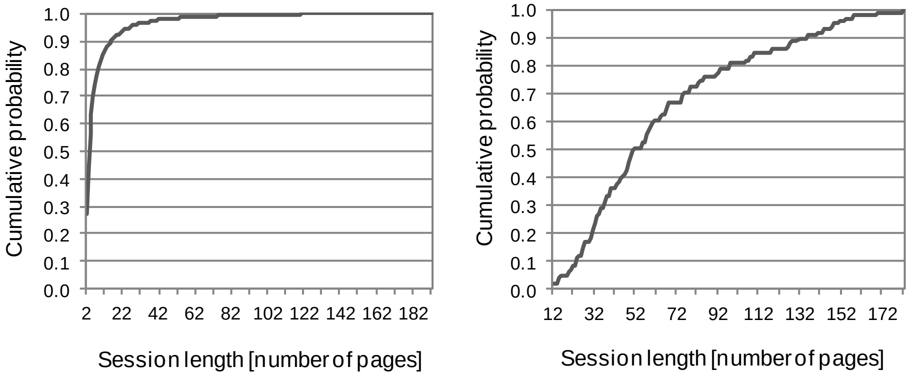


Fig. 2. Cumulative distribution of session lengths: (left) for non-buying sessions, (right) for buying sessions

The second important aspect of user session analysis in a Web store is the time spent by users in the store, i.e., the *session duration*. It is measured as the time interval (in seconds) between arrival times of the last and the first pages requested in the session by a user. The session duration is shorter than the actual time of the user-site interaction, in fact, because the time a user browses the last page in the session is unknown at the server side (for the same reason this attribute cannot be determined for sessions containing only one page, which had been excluded from the analysis as "accidental" sessions).

Table 3 presents session duration statistics for both kinds of "non-accidental" sessions. For non-buying sessions the mean is equal to 6 minutes, which may seem a good result until we look at the median, which is only 2 minutes. The corresponding statistics for buying sessions are much higher. In particular, one can notice that at least 2 minutes were needed to complete a purchase transaction. Buying sessions' durations are more differentiated which is reflected by a higher standard deviation value.

Table 3. Session duration statistics for non-buying and buying sessions

| **Statistics** | **Non-buying sessions** | **Buying sessions** |
|---|---|---|
| Mean | 6 min | 28 min |
| Median | 2 min | 22 min |
| Mode | 2 s | 6 min |
| Standard deviation | 10 min | 21 min |
| Minimum | 2 s | 2 min |
| Maximum | 106 min | 114 min |

Intuitively, bigger session lengths should correspond to longer session durations. The longer the session lasts, the bigger a chance of recognizing the store offer, finding interesting products, adding them to the shopping cart, and the purchase confirmation is. In fact, there is a positive association between the session length and the session duration, and the shapes of distribution and cumulative distribution of session durations (Fig. 3 and Fig. 4) are similar to these of session lengths (cf. Fig. 1 and Fig. 2).

Fig. 3-left presents the histogram of session durations for non-buying sessions. Likewise in the case of the session lengths, the session duration distribution is strongly right-skewed. The cumulative distribution in Fig. 4-left confirms that most of non-buyers spend little time in the Web store – more than 80% of non-buying sessions last below 10 minutes. Buying sessions usually last much longer and their durations are not so differentiated (Fig. 3-right). 93% of buyers spend less than an hour in the store before making a purchase and one-third of buyers take it less than 16 minutes (Fig. 4-right). Very long-lasting buying sessions are rare: the last 7 from among all 15 classes of the histogram of session durations (Fig. 3-right) contained only 0, 1, or 2 sessions.

The third important aspect of user session characterization is the *mean time per page*, computed based on the session length and the session duration for "non-accidental" sessions. This value represents the average time (in seconds) the user browsed a single page in the session. Unlike the session duration, which does not include the last page visited in session, the mean time per page is not underrepresented as it is computed for all visited pages except one.

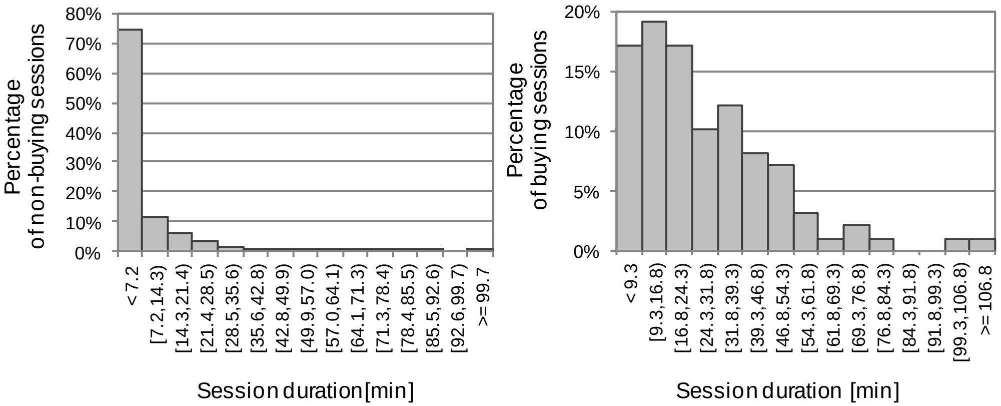


Fig. 3. Histogram of session durations: (left) for non-buying sessions, (right) for buying sessions

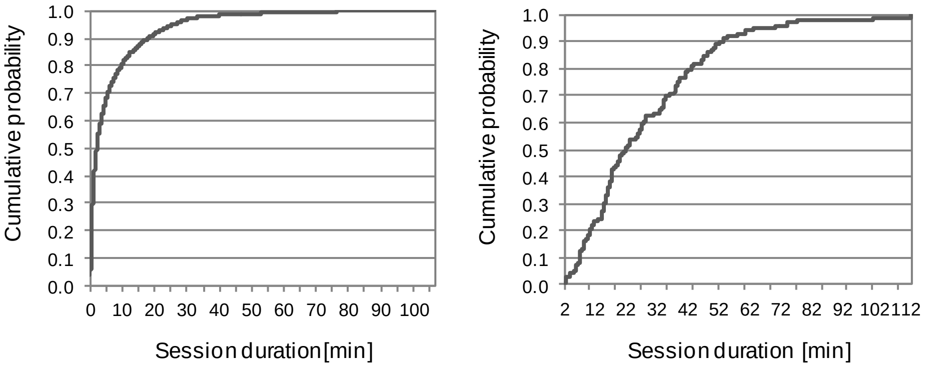


Fig. 4. Cumulative distribution of session durations: (left) for non-buying sessions, (right) for buying sessions

Users may exhibit different usage patterns on the site and may spend different times browsing different kinds of pages. For example, new visitors will probably want to become acquainted with the store profile and look very briefly at the store offer – in this case the mean time per page will be rather short. Other visitors, who are more acquainted with the store assortment and have more or less defined goal of e-shopping, may visit less pages and spent more time on them, reading detailed information on available products and conditions of purchase and delivery – in this case the mean time per page will be longer.

Mean time per page statistics, presented in Table 4, indicate significant differences between non-buying and buying sessions. A user who remains only a visitor, browses a single Web page for 106.6 seconds, i.e., almost two minutes, on average. It is fairly long – however, one may observe that the median of the corresponding mean time per page is only under half minute. Mean times per page for non-buyers are very differentiated – the standard deviation is as much as 3.7 minutes. The minimum, equal to 0.15 second, seems to be too short for a human visitor – it suggests that not all robot-generated sessions had been identified and eliminated from the data set.

Table 4. Mean time per page statistics for non-buying and buying sessions

| **Statistics** | **Non-buying sessions** | **Buying sessions** |
|---|---|---|
| Mean | 106.6 s | 26.7 s |
| Median | 27.5 s | 24.9 s |
| Mode | 2 s | - |
| Standard deviation | 224 s | 13.3 s |
| Minimum | 0.15 s | 5 s |
| Maximum | 29.9 min | 1.4 min |

Distribution in Fig. 5-left and cumulative distribution in Fig. 6-left confirm that most non-buyers spend a great deal of time on browsing pages: 30% percent of them spend more than one minute on a single page. Buyers usually browse pages faster (let us notice that times in Fig. 5-left and 6-left are given in minutes and times in Fig. 5-right and Fig. 6-right – in seconds). Mean times per page for non-buying sessions are very differentiated – their standard deviation value is almost 17 times higher than for buying sessions. This indicates that may be a few different subgroup of similar visitors, which may be worth a more detailed insight.

The findings also suggest that some non-buyers make intensive browsing/searching actions but do not decide to finalize the transaction during the same visit. On the other hand, at least some buyers seem to be acquainted with goods available in the store and efficiently navigate to the checkout (a few of them even had added some items to the shopping cart during the previous visit in the store, in fact). This brings up the need to analyze sessions of returning visitors (especially buyers) in a longer time perspective.

For buying sessions, the histogram of mean times per page (Fig. 5-right) has a slightly different shape than the histogram of session durations (cf. Fig. 3-right) – above all, it is less skewed and more symmetric. Its first class, containing the sessions characterized by the mean time per page below 10 seconds, is much less numerous – its numerousness is only one third of that for the first class of the session duration histogram. This shows that there is not a simple dependence between the session length (i.e., the number of visited pages) and the session duration. That is why buying sessions should be analyzed more precisely in order to distinguish various classes of customers, characterized by various navigation profiles.

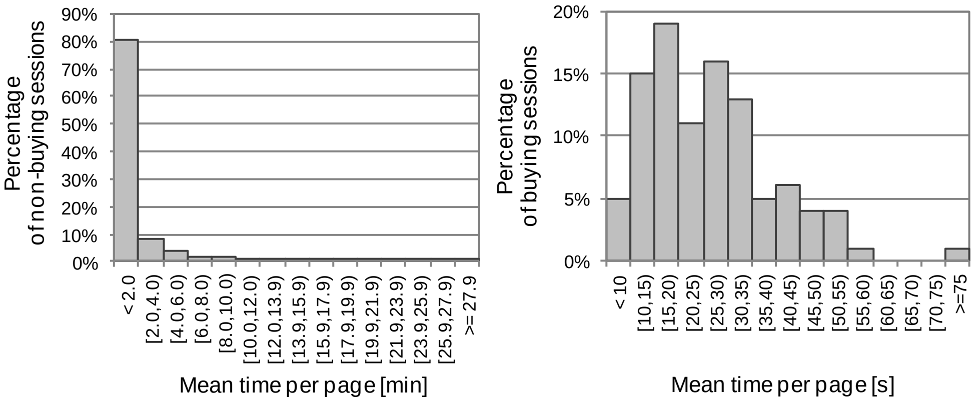


Fig. 5. Histogram of mean times per page: (left) for non-buying sessions, (right) for buying sessions

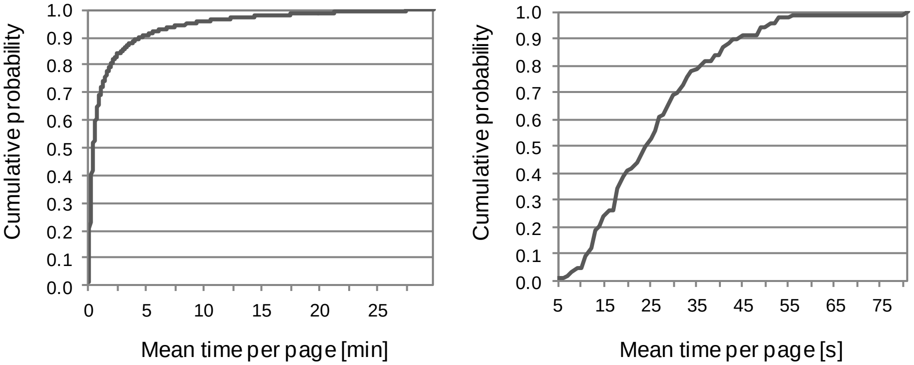


Fig. 6. Cumulative distribution of mean times per page: (left) for non-buying sessions, (right) for buying sessions

## 3. CONCLUDING REMARKS

The session-based analysis presented in the paper has shown that the prevailing majority of sessions on the online bookstore Web site last very short and include very few pages. In fact, more than half of all user sessions are “accidental” sessions, including only one page and/or lasting no longer than one second. The analysis of “non-accidental” sessions, divided into buying and non-buying sessions, show significant differences between these two groups in terms of the session length, the session duration, and the mean time per page.

Most of non-buyers spend relatively little time in the store, visiting a dozen or so pages, and browse a single page for a relatively long time. Buyers usually spend much more time in the store visiting several dozen pages and navigate much faster through the site. Distributions of the session lengths, the session durations, and the mean times per page have different shapes for both kinds of sessions – essentially for non-buyers they are strongly right-skewed and heavy-tailed.

Our research provides an important contribution to the identification of factors characterizing more valuable user sessions in online retail environments. Combined with other factors (e.g., visited session states [7]), the findings may be applied in a method for predicting the probability of making a purchase online. This knowledge may be also used to transform more non-buying users into buying ones.

Our future work will concern the analysis of other aspects of user sessions and customer behavior online, e.g., in the context of returning visitors (especially buyers) in a longer time perspective. Usually buying users do not purchase goods during their first visit in an online Web store but after visiting the store without buying anything they visit competitive Web stores, and sometimes come back to the given store just to buy. Another interesting aspect of future work would be the analysis of buying behavior depending on the type of the Internet access, i.e., stationary and mobile devices.

One has to remember that depending on the e-business branch, the size and character (global or local) of the online store, season of the year, and other factors, user sessions may have different characteristics, and it is difficult to generalize our results to other online stores. Therefore, the natural continuation of our work will be the session-based analysis done for other data sets.

## REFERENCES

[1] ATAULLAH A., *MyQoS: a profit oriented framework for exploiting customer behavior in online e-commerce environments*, Lecture Notes in Computer Science, Vol. 4831, 2007, 533–542.

[2] BORZEMSKI L., SUCHACKA G., *Business-oriented admission control and request scheduling for e-commerce websites*, Cybernetics and Systems, Vol. 41, No. 8, Taylor & Francis, 2010, 592–609.

[3] CHEN Y.-L., KUO M.-H., WU S.-Y., TANG K., *Discovering recency, frequency, and monetary (RFM) sequential patterns from customers' purchasing data*, Electronic Commerce Research and Applications, Vol. 8, No. 5, October 2009, 241–251.

[4] GUITART J., CARRERA D., BELTRAN V., et al., *Designing an overload control strategy for secure e-commerce applications*, Computer Networks, Vol. 51, Issue 15, October 2007, 4492–4510.

[5] LAROSE D. T., *Discovering knowledge in data. An introduction to data mining*, New Jersey, Wiley-Interscience, 2005, pp. 34–35.

[6] SONG Q., SHEPPERD M., *Mining Web browsing patterns for e-commerce*, Computers in Industry, Vol. 57, 2006, 622–630.

[7] SUCHACKA G., CHODAK G., *Practical aspects of log file analysis for e-commerce*, Communications in Computer and Information Science, Vol. 370, Springer, Berlin Heidelberg, 2013, 562–572.

[8] WANG Q., MAKAROFF D.J., EDWARDS H.K., *Characterizing customer groups for an e-commerce website*, In: Proc. of EC'04, New York, NY, USA, ACM Press, 2004, 218–227.

*electronic shops design, digital signage,*
*usability factors, information processing*

Rafal MICHALSKI*, Jerzy GROBELNY*, Maciej KRAKOWIAK*

# THE INFLUENCE OF E-SHOP GRAPHICAL PROPERTIES ON THE PRODUCT INFORMATION SEARCH

The general goal of this study was to examine how selected graphical factors influence the efficiency of searching for a specific product in an electronic mock-up shop. The study investigates three various factors, each on two levels: two different types of search tasks (general and detailed) and types of digital presentation arrangements of the products, namely: grid-based and list-based, and two locations of the main menu: left and right hand sides of the computer screen.

In the experiments, the subjects were asked to perform the tasks as fast and accurately as possible in the fully working, and separate instances of the electronic shops prepared according to the described factors.

The obtained results descriptive statistics were provided and analyzed and a standard analysis of variance was used to test whether the independent variables significantly influenced the mean search times.

* Faculty of Computer Science and Management, Wroclaw University of Technology, Poland.

*human-computer interaction, package design, digital signage*
*usability factors, subjective evaluation, information processing*

Jerzy GROBELNY*, Rafał MICHALSKI*, Joanna BŁAŻEJEWSKA*

# THE ROLE OF THE PACKAGE DESIGN FACTORS IN A DIGITAL SIGNAGE BASED MARKETING

The main objective of this paper was the analysis of persons' attitudes towards graphical marketing information regarding various types of package designs. In this research, various graphical variants of smartphone's packages were experimentally examined by sixty students of Wroclaw University of Technology. The packages were electronically presented to the subjects on the computer screen. A binary pairwise procedure was employed to assess the examinees' attitudes towards the prepared versions of the package designs. They differed in the location of the product within the package, colors used, and the graphical properties of the applied text format.

* Faculty of Computer Science and Management, Wroclaw University of Technology, Wybrzeze Wyspianskiego 27, 50-370 Wrocław, Poland.

## BIBLIOTEKA INFORMATYKI SZKÓŁ WYŻSZYCH

*Information Systems Architecture and Technology. Advances in Web-Age Information Systems*, pod redakcją Leszka BORZEMSKIEGO, Adama GRZECHA, Jerzego ŚWIĄTKA, Zofii WILIMOWSKIEJ, Wrocław 2009

*Information Systems Architecture and Technology. Service Oriented Distributed Systems: Concepts and Infrastructure*, pod redakcją Adama GRZECHA, Leszka BORZEMSKIEGO, Jerzego ŚWIĄTKA, Zofii WILIMOWSKIEJ, Wrocław 2009

*Information Systems Architecture and Technology. Systems Analysis in Decision Aided Problems*, pod redakcją Jerzego ŚWIĄTKA, Leszka BORZEMSKIEGO, Adama GRZECHA, Zofii WILIMOWSKIEJ, Wrocław 2009

*Information Systems Architecture and Technology. IT Technologies in Knowledge Oriented Management Process*, pod redakcją Zofii WILIMOWSKIEJ, Leszka BORZEMSKIEGO, Adama GRZECHA, Jerzego ŚWIĄTKA, Wrocław 2009

*Information Systems Architecture and Technology. New Developments in Web-Age Information Systems*, pod redakcją Leszka BORZEMSKIEGO, Adama GRZECHA, Jerzego ŚWIĄTKA, Zofii WILIMOWSKIEJ, Wrocław 2010

*Information Systems Architecture and Technology. Networks and Networks Services'*, pod redakcją Adama GRZECHA, Leszka BORZEMSKIEGO, Jerzego ŚWIĄTKA, Zofii WILIMOWSKIEJ, Wrocław 2010

*Information Systems Architecture and Technology. System Analysis Approach to the Design, Control and Decision Support*, pod redakcją Jerzego ŚWIĄTKA, Leszka BORZEMSKIEGO, Adama GRZECHA, Zofii WILIMOWSKIEJ, Wrocław 2010

*Information Systems Architecture and Technology. IT TModels in Management Process*, pod redakcją Zofii WILIMOWSKIEJ, Leszka BORZEMSKIEGO, Adama GRZECHA, Jerzego ŚWIĄTKA, Wrocław 2010

*Information Systems Architecture and Technology. Web Information Systems Engineering, Knowledge Discovery and Hybrid Computing,* pod redakcją Leszka BORZEMSKIEGO, Adama GRZECHA, Jerzego ŚWIĄTKA, Zofii WILIMOWSKIEJ, Wrocław 2011

*Information Systems Architecture and Technology. Service Oriented Networked Systems*, pod redakcją Adama GRZECHA, Leszka BORZEMSKIEGO, Jerzego ŚWIĄTKA, Zofii WILIMOWSKIEJ, Wrocław 2011

*Information Systems Architecture and Technology. System Analysis Approach to the Design, Control and Decision Support*, pod redakcją Jerzego ŚWIĄTKA, Leszka BORZEMSKIEGO, Adama GRZECHA, Zofii WILIMOWSKIEJ, Wrocław 2011

*Information Systems Architecture and Technology. Information as the Intangible Assets and Company Value Source*, pod redakcją Zofii WILIMOWSKIEJ, Leszka BORZEMSKIEGO, Adama GRZECHA, Jerzego ŚWIĄTKA, Wrocław 2011

*Information Systems Architecture and Technology. Web Engineering and High-Performance Computing on Complex Environments,* pod redakcją Leszka BORZEMSKIEGO, Adama GRZECHA, Jerzego ŚWIĄTKA, Zofii WILIMOWSKIEJ, Wrocław 2012

*Information Systems Architecture and Technology. Networks Design and Analysis*, pod redakcją Adama GRZECHA, Leszka BORZEMSKIEGO, Jerzego ŚWIĄTKA, Zofii WILIMOWSKIEJ, Wrocław 2012

*Information Systems Architecture and Technology. System Analysis Approach to the Design, Control and Decision Support* pod redakcją Jerzego ŚWIĄTKA, Leszka BORZEMSKIEGO, Adama GRZECHA, Zofii WILIMOWSKIEJ, Wrocław 2012

*Information Systems Architecture and Technology. The Use of IT Models for Organization Management*, pod redakcją Zofii WILIMOWSKIEJ, Leszka BORZEMSKIEGO, Adama GRZECHA, Jerzego ŚWIĄTKA, Wrocław 2012

Wydawnictwa Politechniki Wrocławskiej
są do nabycia w księgarni
plac Grunwaldzki 13, 50-377 Wrocław
budynek D-1 PWr., tel. 71 320 29 35
Prowadzimy sprzedaż wysyłkową
zamawianie.ksiazek@pwr.wroc.pl

ISBN 978-83-7493-801-3