Workshop Knowledge in Telecommunication Technologies and Optics 2012

Workshop KTTO 2012 November 14-16, 2012
Malenovice, Czech Republic

Workshop proceedings
Editors: Miroslav VOZNAK and Martin VACULIK
This workshop is supported by the project No CZ.1.07/2.2.00/28.0062, Joint activities of BUT and TUO while creating the content of accredited technical courses in ICT.

Preface

The KTTO 2012 Conference was held in Malenovice, Czech Republic from November 14th to 16th, 2012. The conference was divided into one plenary session with invited lectures, four conference sessions and three workshop sessions. The accepted papers for conference sessions were published in a special issue of journal AEEE (Advances in Electrical and Electronic Engineering) which is covered by Elsevier and all papers are indexed in scientific citation database SciVerse SCOPUS. The workshop KTTO 2012 was an important event accompanying the main conference programme.

The event contributed to networking of researchers and sharing their recent results in field of Telecommunications. I would like to thank all lecturers, authors of the submitted papers in conference, workshop and their reviewers. I would also like to thank my colleagues from organizing committee who actively participated in the preparations and made the success of the event possible. Last but not least, I would also like to thank our partners and sponsors.

Miroslav Voznak
On behalf of
Scientific and Programme Committee
KTTO 2012
# Workshop on Knowledge in Telecommunication Technologies and Optics 2012

## Table of Contents

<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improvement of E-model MOS estimation</td>
<td>1</td>
</tr>
<tr>
<td>Michal Halas, Adrian Kovac</td>
<td></td>
</tr>
<tr>
<td>Open IMS Core implementation for testing of NGN networks</td>
<td>6</td>
</tr>
<tr>
<td>Filip Rezac, Jan Rozhon</td>
<td></td>
</tr>
<tr>
<td>Relation between Computational Power and Time Scale for Breaking Authentication in SIP Protocol</td>
<td>9</td>
</tr>
<tr>
<td>Miroslav Voznak, Jan Rozhon, Filip Rezac</td>
<td></td>
</tr>
<tr>
<td>Impact of SRTP protocol on VoIP call quality</td>
<td>13</td>
</tr>
<tr>
<td>Michal Halás, Lubos Javorcek, Adrian Kovac</td>
<td></td>
</tr>
<tr>
<td>Using BESIP, UCI and NETCONF as SBC</td>
<td>16</td>
</tr>
<tr>
<td>Lukas Macura</td>
<td></td>
</tr>
<tr>
<td>Contact Center Models</td>
<td>19</td>
</tr>
<tr>
<td>Erik Chromy, Tibor Misuth</td>
<td></td>
</tr>
<tr>
<td>Anomaly-based Intrusion Detection in IP Networks</td>
<td>24</td>
</tr>
<tr>
<td>Pavel Nevlud, Lukas Kapicak, Jaroslav Zdralék</td>
<td></td>
</tr>
<tr>
<td>Application of Erlang Formulas in Contact Center Environment</td>
<td>27</td>
</tr>
<tr>
<td>Erik Chromy, Tibor Misuth</td>
<td></td>
</tr>
<tr>
<td>Simulation of 16-QAM and 64-QAM Demodulator into MATLAB/Simulink with Xilinx Toolkit</td>
<td>31</td>
</tr>
<tr>
<td>Miroslav Bures, Jaroslav Zdralék</td>
<td></td>
</tr>
<tr>
<td>Advantages of Audio Signal Separation to Tonal and Noise Parts for LP modeling</td>
<td>34</td>
</tr>
<tr>
<td>Ondrej Raso, Miroslav Balik, Zdenek Martinasek</td>
<td></td>
</tr>
<tr>
<td>Admission Control Methods and Quality of Service</td>
<td>36</td>
</tr>
<tr>
<td>Erik Chromy, Matus Weber, Tomas Behul</td>
<td></td>
</tr>
<tr>
<td>Development of the Course Radio-Communication Engineering</td>
<td>41</td>
</tr>
<tr>
<td>Marek Dvorský, Martin Tomis</td>
<td></td>
</tr>
</tbody>
</table>
Innovation of Laboratory Exercises in Subject "Data Networks" ........................................43
Pavel Bezpalec

Inovace laboratorních cvičení předmětu Kódy a bezpečnost ........................................45
Tomáš Vaněk

Modelování datové komunikace po silnoproudém vedení – podstata a dosavadní
modely .................................................................47
Petr Mlynek, Martin Koutněk, Jiří Misurec

Analýza hlavních komponent (PCA) .................................................................49
Jan Skapa
IMPROVEMENT OF E-MODEL MOS ESTIMATION

Michal Halas
Department of Telecommunications
Faculty of Electrical Engineering and Information Technology, Slovak University of Technology, Slovak republic
michal.halas@stuba.sk

Adrian Kováč
Department of Telecommunications
Faculty of Electrical Engineering and Information Technology, Slovak University of Technology, Slovak republic
kovac@ktel.elf.stuba.sk

Abstract. In the article we propose a method of improving ITU-T E-model MOS estimate of VoIP call quality. The improvement consists of including the effects of network jitter as measured and distributed in RTCP packets; jitter buffer size at receiver and codec packetization settings as input parameters of E-Model. Our method uses Pareto/D/1/k system for modeling general VoIP input traffic stream interarrival times and jitter buffer behavior resulting in additional packet loss. Consequently we propose the inclusion of jitter buffer size, codec packetization and network jitter into E-Model by means of substitution of existing Ppl (packet loss) parameter for Pplef (effective packet loss) in computationally effective manner suitable for real-time MOS estimate without the need of capturing large packet traces from the network and performing estimation of Hurst parameter or using other means of traffic statistics description in advance.

Keywords- E-model, MOS, packet loss, jitter, jitter buffer, network traffic, call quality

1. INTRODUCTION

The Internet, VoIP and in general IP traffic is known to possess the property of being self-similar, long-range dependent or in other words “bursty”.

The behavior of a “bursty” traffic differs from ideal stochastic model of absolutely independent packets when trying to assess or describe the traffic interarrival times via standard well-known distributions. This property translates into the failure of general queuing models, such as M/M/1/k, which counts on Exponential and Poisson characteristics of input stream and service time, to describe the situation of incoming VoIP stream at buffer on receiver’s side.

In our article we analyze and improve original E-Model designed to give real-time estimate of VoIP call quality in MOS scale based solely on network performance parameters and codec type. We work with the 04/2009 version of E-model, which still after numerous updates, does not incorporate the effects of jitter. While the performance of the E-Model estimate is satisfactory under good network conditions, the E-Model MOS estimate becomes too optimistic under slightly and moderately impaired network conditions as shown in our previous work [1], [2] and [3].

Our measurements and simulation showed that the performance and estimate accuracy of E-Model deteriorates unacceptably beyond network jitter (calculated by RFC 1889) over 20 ms for all tested codecs including G.711 with and without PLC, G.723.1 ACELP and MP-MLQ, G.726 and G.729. Fig. 1 shows an example of E-Model MOS inaccuracy of VoIP network connection in following manner:

• “MOS E-Model” – represents MOS as estimated via software on receiving side by reading network performance from RTCP protocol not accounting for the effects of local jitter buffer.

• “MOS measured” – represents MOS estimated by measuring software – IX-Chariot – based of the net voice input packet stream entering the decoder behind buffer;

• “MOS modified E-Model” shows estimate performed via software using E-Model [4] incorporating the effects of jitter and buffer size based on actual codec configuration and data about network performance from RTCP without physically observing or interfering with packet stream behind jitter buffer.

As we can observe, the actual discrepancy of E-Model estimate, being around 1.00 MOS scale under 40 ms jitter is unacceptable for all purposes. These network conditions are not unreal and are common on WiFi and mobile connections.

![Figure 1. Comparison of MOS estimates for G.729 codec at 40 ms RFC jitter and 40 ms buffer size, 0 % packet loss under varying network delay](image-url)
II. BRIEF E-MODEL DESCRIPTION

Mean opinion score (MOS) is a measure based on subjective user satisfaction with overall listening and conversational quality on five grade scale from 5 (best) to 1 (worst). MOS can be estimated by subjective methods based on physical testing or by objective methods relying on and working solely with real-time measured network performance parameters (delay, packet loss) which unfortunately does not include jitter and jitter buffer size.

E-model defined by ITU-T G.107 [4] is widely accepted objective method used for estimation of VoIP call quality. E-model uses a set of selected input parameters to calculate intermediate variable – R factor, which is finally converted to MOS value. Input parameters contribute to final estimate of quality in additive manner as expressed in (1).

\[ R = R_0 - I_s - I_d - I_{e-eff} + A \]  

Where

- \( R_0 \) represents the basic SNR, circuit and room noise;
- \( I_s \) represents all impairments related to voice recording;
- \( I_d \) covers degradations caused by delay of audio signal;
- \( I_{e-eff} \) impairment factor presents all degradations caused by packet network transmission path, including end-to-end delay, packet loss and codec PLC masking capabilities;
- \( A \) is an advantage factor of particular technology;

We focus at \( I_{e-eff} \) parameter, which is calculated as (2):

\[ I_{e-eff} = I_e + (95 - I_s) \cdot \frac{P_{pl}}{P_{pt}+P_{pl}} \]  

Where \( I_e \) represents impairment factor given by codec compression and voice reproduction capabilities, \( Bpl \) is codec robustness characterizing codec’s immunity to random losses.

The values are given for 8kHz sample rate codecs in ITU-T G.133 appendix [6]. \( P_{pl} \) parameter represents measured network packet loss in %.

In this paper we propose a substitution of \( P_{pl} \) parameter for \( P_{del} \) further described in section IV of the paper.

III. JITTER, DELAY AND BUFFER EFFECTS ON MOS

A. Model Implementation Presumptions

- The variance of input packet stream can be considered constant for the short time-scale we operate on as induced from the results from [9 and 15]. The Hurst parameter value from short-term point of view in order of seconds is constant and can be put equal to \( H=1 \).

B. Network Delay Description and Statistics

Voice packets are generated at sending device – IP phone – as a homogenous flow with constant transmit intervals depending mostly on packetization interval set in the codec. VoIP packets that traversed transport network have their regular spacing disrupted irregularly. Internet traffic arrival times and delay can be successfully statistically modeled by long-tailed Generalized Pareto distribution (GPD) [8, 9, 10, 12, 14]. We use GPD to further describe VoIP input packet stream. Delay distribution of received packets is in fig. 2.

Real-time change of network parameters causes variations in network delay. Differences between packet arrivals are not constant and arrival times oscillate between minimal delay \( T_{a-min} \) and infinite delay, which is effectively a lost packet. Mean value of the process exists and is interpreted as an End-To-End delay \( T_a \) (one of the input parameters for E-model).

Real packet path usually consists of a mixture of different networks with different devices and technologies. Each device adds a degree of uncertainty in packet delivery time. Overall delay statistics is a sum of all partial statistics at each device.

Pareto distribution is well suited to describe delay, which has lower bound, no upper bound and finite mean value. Probability density function of Pareto (PDF) is given by eq. (3) and cumulative distribution function (CDF) by eq. (4).

\[ f(x, \mu, \sigma) = \frac{1}{\sigma} \left( 1 + \frac{x - \mu}{\sigma} \right)^{-\frac{1}{\xi}} \]  

\[ F(x, \mu, \sigma) = \frac{1}{\sigma} \left( 1 + \frac{x - \mu}{\sigma} \right)^{-\frac{1}{\xi}} \]  

Where \( \sigma = \text{std. deviation} \), \( \xi = \text{shape parameter} \), \( \mu = \text{location parameter} \) (minimal value of random variable with Pareto distribution). \( \mu \) is an offset of Pareto distribution from
zero on time axis and represents minimal delay $T_{min}$ (Fig. 2). The shape parameter must meet condition $\xi < 0$ and to get valid results from eq. (3) and (4) $\mu \leq x \leq \mu - \sigma/\xi$.

### C. Jitter and Jitter Buffer Model

Jitter $J$ [ms], as defined in RFC 1889 for RTP / RTCP protocol, is a floating average of differences between packet arrival times (or “Timestamps”) between consecutively received packets. $J$ is calculated as given by eq. (5). Each inter-packet difference is given by eq. (6). $R$ denotes timestamps of packet reception, $S$ of packet transmission and indices $i,j$ are consecutive packet numbers. Jitter value is one of the QoS parameters in RTCP protocol.

\[
J = J + ((D_{(i,j)} - J) / 16 \text{ [ms]} \quad (5)
\]

\[
D_{(i,j)} = (R_j - R_i) - (S_j - S_i) \text{ [ms]} \quad (6)
\]

Loss due to a jitter buffer is caused by its limited size. When packets arrive too early or too late to the input queue, there is no place to store them and drop occurs. This situation is shown in Fig. 3 with jitter buffer as Pareto/D/1/K system.

![Image of Voip input buffer function as Pareto/D/1/K system](image)

As has previously been shown in our previous work [1, 2, 3] and several studies in the field of Internet and IP traffic [8, 9, 10, 12, 14] the distribution of packet arrival and interarrival times is long-tailed with long-range dependency (LRD).

As analysed and proposed in our previous work [2] the packet loss of fixed receiving jitter buffer with packet reordering capability can be calculated as given by eq. (7).

\[
P_{\text{loss,wr}}(x, \xi, \mu, \sigma) = \int_{\xi}^{\infty} \frac{1}{\sigma} \left(1 + \frac{x - \mu}{\sigma}\right)^{-\frac{1}{\xi}} \, dx \quad (7)
\]

\[
= 1 - \int_{\xi}^{\infty} \text{PDFdx} \quad (7)
\]

where $x = T_{buff} = \text{actual size of jitter buffer in [ms]}$, $\xi = \text{Pareto shape parameter (needs to be fitted)}$, $\mu = \text{mean value of network delay (measured)}$ and $\sigma = \text{scale parameter representing observed network jitter}$. A further study is needed to find optimal relationship between $\sigma$ scale parameter and actual value of jitter $J$ and substitution into equations.

Loss probability on buffer (7) can be simplified to eq. (8):

\[
P_{\text{loss,wr}}(x, \xi, \mu, \sigma) = \left(1 + \frac{x - \mu}{\sigma}\right)^{-\frac{1}{\xi}} \quad (8)
\]

When considering jitter buffer without reordering, we need to calculate probability with which the packet will arrive in different than expected time-slot as opposed to probability of packet entirely missing the buffer in buffer with reordering capability. Probability of packet loss is given by eq. (9).

\[
P_{\text{loss,wr}}(x, \xi, \mu, \sigma) = \int_{\xi}^{\infty} \frac{1}{\sigma} \left(1 + \frac{x - \mu}{\sigma}\right)^{-\frac{1}{\xi}} \, dx \quad (9)
\]

\[
= 1 - \int_{\xi}^{\infty} \text{PDFdx} \quad (9)
\]

Based on local time invariance and presumptions in section A, supported by the results in [2, 3], we consider distribution functions of interarrival times of two consecutive packets to be in the ratio of 1:1 hence eq. (9) can be rewritten to (10).

\[
P_{\text{loss,wr}}(x, \xi, \mu, \sigma) = \left[1 + \frac{x - \mu}{\sigma}\right]^{-\frac{1}{\xi}} \quad (10)
\]

IV. PROPOSED E-MODEL MODIFICATION TO IMPAIRMENT FACTOR

Based on simulation results and measurements we have determined optimal shape parameter $\xi = -0.1$ with relative MSE of MOS of only 12.0%. We add two parameters to E-model through eq. (11) which incorporates jitter buffer size $x$ [ms] and network jitter $\sigma$ [ms].

\[
P_{\text{jitter}} = \frac{(1 - (1 + \frac{x - \mu}{\sigma})^{-\frac{1}{\xi}})^2}{2} \quad (11)
\]

After substitution of parameters $\xi = -0.1$ and $\mu = 0$ we get equation for jitter buffer packet loss as eq. (11):

\[
P_{\text{jitter}} = \frac{\left(1 - \frac{-0.1 x^2}{\sigma}\right)}{2} \quad (11)
\]

Further we express effective packet loss $P_{ppl}$ incorporating network and jitter buffer packet loss. $P_{ppl}$ from eq. (13) substitutes $P_{pl}$ in eq. (2) which leads to eq. (14):

\[
P_{ppl} = P_{pl} + P_{jitter} - P_{pl}.P_{jitter} \quad (12)
\]

\[
P_{ppl} - P_{pl} + \left(1 + \frac{-0.1 x^2}{\sigma}\right) - P_{pl}.\left(1 + \frac{-0.1 x^2}{\sigma}\right) \quad (13)
\]

\[
Ie_{eff} = Ie_{有效} = (95 - Ie) . P_{ppl} e - Bpl \quad (14)
\]

Eq. (14) is the final proposed equation for equipment impairment factor calculation in E-model including jitter buffer loss and buffer size through effective packet loss $P_{ppl}$. 

![Image of a network diagram](image)
Iterative distribution fitting was performed using various distributions to find best fit parameters. These parameters and distributions were put under Kolmogorov-Smirnov and Chi-Squared tests to find best descriptive statistics of Pareto-distributed stream time differences with applied jitter. Results of finding best descriptive statistics with optimal iteratively found parameter set with error of 10e-5 are sorted in tab. 1.

### Table I. Best fit parameters of tested distributions

<table>
<thead>
<tr>
<th>Distribution</th>
<th>Best fit distribution parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generalized Pareto (GPD)</td>
<td>$k=0.19328 \alpha=0.0224 \mu=-0.00306$</td>
</tr>
<tr>
<td>Generalized Extreme</td>
<td>$k=0.36239 \alpha=0.01384 \mu=0.00909$</td>
</tr>
<tr>
<td>Weibull</td>
<td>$\alpha=0.39981 \beta=0.01718$</td>
</tr>
<tr>
<td>Gen. Gamma</td>
<td>$k=0.98444 \alpha=0.40502 \beta=0.05293$</td>
</tr>
<tr>
<td>Log-Pearson 3</td>
<td>$\alpha=6.081 \beta=1.175 \gamma=1.641$</td>
</tr>
<tr>
<td>Laplace</td>
<td>$\lambda=39.109 \mu=0.0247$</td>
</tr>
<tr>
<td>Weibull (3P)</td>
<td>$\alpha=0.4745 \beta=0.01408 \gamma=1.3003E-5$</td>
</tr>
<tr>
<td>Gamma</td>
<td>$\alpha=0.46676 \beta=0.05293$</td>
</tr>
<tr>
<td>Logistic</td>
<td>$\sigma=0.01994 \mu=0.0247$</td>
</tr>
<tr>
<td>Lognormal</td>
<td>$\sigma=2.8971 \mu=-5.504$</td>
</tr>
</tbody>
</table>

Statistical tests showed as a proof of concept, that GPD Pareto distribution is also the most suitable one for describing interarrival times of general long-tailed LAN/WAN packet streams impaired by random jitter with equal distribution. This shows also Pareto distribution to be the best compromise between calculation complexity (compared to fractal modelling methods) and statistical significance for modelling also jitter buffer loss behaviour under variable jitter.

To explain best fit parameters of GPD from tab. 1:

- $\sigma$ in all equations corresponds to optimised $\sigma$ in tab. 1. Proposed relation between $\sigma$ and actual jitter $J$ substituted can be expressed in ratio $J/\sigma \in <1;2>$. For actual imposed 40 ms network jitter the optimized parameter was $\sigma=0.0224$ $(s) = 22.4$ ms what would yield $J/\sigma$ ratio = 22/14 $\in <1;2>$. Actual parameter substitution ratio needs further testing.

- $\xi$ = shape parameter - corresponds to optimised $k$ in tab. 5. Actual shape parameter for our model was chosen to be $\xi=[-k]$ rounded to one tenth in order to maintain exponent in all equations of integer value for computational effectiveness.

- $\mu$ = location parameter - corresponds to $\mu=\mu=0.00306$ in tab. 1. It was chosen as $\mu=0$ with negligible effect.

## VI. Conclusion

Proposed change in equipment impairment factor calculation leads to improved MOS estimate of E-model when network jitter is present. Proposed method is useful for MOS prediction under real network conditions with jitter. Discovered dependence of buffer packet loss at different jitter strengths for different buffer sizes is illustrated in fig. 4.

### Acknowledgment

This work is a part of research activities conducted at Slovak University of Technology Bratislava, Faculty of Elec-trical Engineering and Information Technology, Department of Telecommunications, within the scope of the projects “Analysis of the impact of traffic parameters on voice quality in IMS networks”, supported by the STU University grant programme “Grant programme to support young researchers”.

The support was also provided by the Center of Excellence for SMART Technologies, Systems and Services II., ITMS 26240120029, co-funded by the ERDF.

### References


COMMUNICATIONS, Issue 11, Volume 10, pp. 341-350, November 2011, ISSN: 1109-2742.


[7] Chromy, E., Misuth, T., Kavacky, M.: Erlang C Formula and Its Use In the Call Centers. In: Journal AEEE - Information and Communication Technologies and Services, Volume 9, Number 1, pp. 7-13, March 2011, ISSN 1804-3119


Open IMS Core implementation for testing of NGN networks

Filip Rezac
Department of Telecommunications
VSB – Technical University of Ostrava
Ostrava, Czech Republic
filip.rezac@vsb.cz

Jan Rozhon
Department of Telecommunications
VSB – Technical University of Ostrava
Ostrava, Czech Republic
jan.rozhon@vsb.cz

Abstract — This paper deals with the implementation of the Open IMS Core in the test IMS network at the Department of Telecommunications in Ostrava. This issue was solved under the OPVK project - Joint activities of VUT and TUO while creating the content of accredited technical courses in ICT. Task was to innovate a laboratory exercises in Switching Systems course. The article describes the architecture of the technology and how to create and test Open IMS Core.

Keywords - CSCF; Diameter; FHoSS; IMSU; Open IMS Core; SIP

I. INTRODUCTION

The objective of the third generation networks (3G), among which include the IMS, is to unite the two most successful models in communications: cellular networks and the Internet (each model works on a different principle). IP (Internet Protocol) Multimedia Subsystem (IMS) is a key element in the 3G architecture that allows users, especially mobile subscribers to use all services provided by the Internet (website, e-mail, watching a movie or videoconference). Standard IMS has several objectives, notably the unification of data and multimedia to packets (eg voice and video), because current systems for voice, work on the principle of switching circuits. Furthermore, it provides safety increase and connection control improvement, providing the operators ability to create accounts with the services of subscriber’s choice or a simple and cost-effective scalability [1].

Open IMS Core has been created within the project of Frenhifers Institute - FOKUS in Berlin, as an open-source solution of an essential elements of the IMS / NGN architecture. It is a professional environment for testing the IMS network. Most manufacturers and operators, fixed or mobile, using it for testing their services, debugging and verification of properties of services which they offer. Open IMS Core is a popular tool for its flexibility and performance [2].

II. OPEN IMS ARCHITECTURE

Open IMS Core consists of two main parts. The first is FHoSS (The FOKUS Home Subscriber Server), which simulates the user's home server HSS. While the second part, named Ser_ims (Servers IMS) includes code for all three simulations of CSCF servers. The basic elements of the Open IMS are shown in Figure 1.

The Open IMS SIP proxy must follow all traffic with the least possible delay, to ensure the minimum total time for the connection setup. Features that ensure it, are contained in the CSCF (P-CSCF, I-CSCF, S-CSCF). One part of the CSCF registration services that maintain routes to users, their preferences and data. Used to determine the position of the participant, setting its own services and to protect IMS core from potential attacks. These types of registration services are part of the core network and allows for all the correct destination address for routing messages. Finally, it must be able to IMS core in certain cases, such as the forced termination of a call or B2B (Back to Back) calls and act as a signaling process as a terminal device. Given that the correct CSCF functionality relies on information about specific services, user profiles and user defined search function CSCF in the Open IMS Core HSS implemented [3]. Communication in IMS uses mainly two protocols, SIP protocol that is used to build, maintain and end the connection and Diameter protocol [4], which is used for authentication, authorization, and accounting. For the actual data transfer IP protocol is used.

![Figure 1. Basic Elements of the Open IMS Core.](image-url)
III. OPEN IMS CORE ENVIRONMENT

Open IMS environment image was created using VMware Workstation virtualization 7th, under the operating system Ubuntu 10th 04 LTS - Lucid Lynx. On the website dedicated to the development environment of Open IMS Core, the instructions to install the environment are presented [2, 5].

Prior to installation, the simulation environment must meet a set of the following software requirements:

- A set of compilers GCC version 3 or 4
- Tools make, ant, bison and flex.
- JDK (Java Development Kit) version 1.5 and higher.
- MySQL database system or another.
- Libraries libxml2 (greater than version 2.6) and libmysql.

To make use of IPsec and TLS security, you must have installed IPsec tools and openssl. After fulfilling the above pre-installation requirements have been downloaded source code CSCF SIP servers and databases FHoSS. First was created OpenIMSCore main directory, where they were also created two folders and ser-ims FHoSS. In these two directories are downloaded source code CSCF servers and databases.

To start CSCF servers, you must open the files pcescf.sh, icscf.sh, scscf.sh. These components should be run concurrently. Subsequently, using the file startup.sh starts FHoSS component. Then enters into the Web browser address http://localhost:8080/. This will start the graphical interface shown in Figure 2 for environment configuration Open IMS Core.

A. Creating a New User

To create a new user in the IMS network, it is necessary to create a record in a database stored in the HSS. Creating this record consists of three consecutive steps. The first is to create a user account IMSUM (IMS subscription), which sets the user name and a set of properties. The next step is to create a private identity IMPI, which is in the form name @ domain setup password. The final step in creating a record of the user in FHoSS is setting its public identity Imps, which is set in the format sip: name @ domain. These items are set in Figure 3 below.

B. Registration Process

To register a user to IMS network, clients can use Monster UTC IMS Openica Lite [6]. Communication options to the user can be in the form of text messages, call or video call. Figure 4 shows the tool Wireshark reports REGISTER, 401 and 200 UNAUTHORIZED OK to register the user to the IMS network.

Before the registration process, the client must learn about SIP servers, namely P-CSCF. The client sends a REGISTER message P-CSCF server that wrote the report server forwards the I-CSCF. Since the I-CSCF does not have information whether a user is assigned S-CSCF server, sends a request via the protocol Diameter HSS database. Once the I-CSCF detects addresses previously assigned S-CSCF, the server forwards the REGISTER message. In the event that this is the first register as a user to the network and it still has not been previously assigned S-CSCF server, the message sent in the UAA list of features S-CSCF server and I-CSCF according to them, decides which S-CSCF server assigns the user. After receiving the REGISTER message server S-CSCF sends a request to the database HSS. It is because of user authentication, and also due to store information on the allocation of SIP URI S-CSCF to
the user. S-CSCF server authenticates the user and generates a 401-Unauthorized, which is forwarded to the I-CSCF and P-CSCF back to the client. When the client receives this message, it generates a new REGISTER message. With this news it is treated the same as the first REGISTER message, it means that it is forwarded to the P-CSCF server, then the message is forwarded to the I-CSCF. I-CSCF server once again requests information about the assigned S-CSCF. In this case, the database HSS sends back a previously saved SIP URI of the assigned S-CSCF server that is forwarded to the REGISTER message. This report is compared with the authentication vectors. If authentication is successful, the S-CSCF sends a report that informs the HSS database that the user is registered to the network. Server S-CSCF receives a message in which the user profile. This profile is a list of all public identities that are assigned to registered private identity. S-CSCF server then sends a 200 OK message, indicating that the REGISTER request was successful. Message 200 OK is again forwarded via I-CSCF and P-CSCF back to the user.

C. Communications

Communication in IMS network between two clients is shown in Figure 5 The analysis is performed using a packet analyzer Wireshark.

A user initiates the transmission of a message and sends an INVITE P-CSCF server, the message server sends the S-CSCF. Both servers are located in the home network.

![Figure 5. Communications Between Two IMS Clients.](image_url)

V. CONCLUSION

The basic output of the project was to modernize and supplement the qualitative level of education in the Switching Networks subject in labs so that with the advent of new technologies maintain the timeliness and value of education. The project offered students the opportunity of experiencing and practical testing of modern information systems, a new generation of NGN, namely the Open IMS system. Also allow students to further develop and preview the implementation of communications solutions for the current and future telecommunications world.

ACKNOWLEDGEMENT

This work has been supported by the grants: OPVK No CZ.1.07/2.2.00/28.0062, Joint activities of VUT and TUO while creating the content of accredited technical courses in ICT.

REFERENCES

Relation between Computational Power and Time Scale for Breaking Authentication in SIP Protocol

Miroslav Voznak, Jan Rozhon and Filip Rezac
Department of Telecommunications
VSB-Technical University of Ostrava
Czech Republic
voznak@ieee.org, jan.rozhon@gmail.com, filip.rezac@vsb.cz

Abstract—The security of modern communications lies on the series of algorithms, which can be split into two groups – hash functions and ciphers. While the former is mainly used for authentication and integrity checks the main purpose of the latter is to encrypt the communication so that only rightful recipient can access the content of the message. Both groups have long history and both are being improved all the time. However, due to the standardization and the slower implementation of newly proposed standards these algorithms are often used even when their weaknesses are discovered. The typical example is the MD5 Message-Digest algorithm. This paper presents examples of the possible passwords and the time needed to break them to fill in the gap in the common knowledge about how long it takes to break an MD5 hash function.

Keywords-component; MD5; hash function; SIP; CUDA

I. INTRODUCTION

Voice over IP incorporates several authentication algorithms that can be viewed as a potential security risk. Typical example is MD5 digest access authentication, which is commonly used in communications based on Session Initiation Protocol. Since the technology of parallel computing has undergone a huge leap since the SIP standardization, it can now pose a huge threat to this kind of authentication and SIP communication in general. The MD5 hash function is widely used in various implementations of web services and applications, VoIP communication and others although it is well known that the procedures for “cracking” this tool exist and are very efficient. The main reason for this is the fact that although the original plain text input or the appropriate text string that would produce the same hash (collision) can be obtained by well-known procedures, the time to obtain them is usually very long, or at least long enough not to cause any security risk.

As we are going to describe in the following text, the technology evolved faster than the area of securing the digital communications. In this paper we are going to present several measurements illustrating the actual amount of time necessary to crack the MD5 hash function of password with typical length and characters that are com-monly used. Moreover, we are going to present the time consideration regarding the “cracking” of digest access authentication, which is the most common method for user authentication in SIP. To steal user passwords we are going to use open-source tools Hashcat and cudaSIPcracker, which can utilize the CUDA cores in the graphic cards and thusly make the brute force attacks very efficient.

II. STATE OF THE ART

In this section, we are going to describe the basics of MD5 and its implementation in digest access authentication as well as some basics of CUDA technology to provide the user with necessary background information for complete understanding of the topic.

A. MD5

The MD5 Message-Digest Algorithm is widely used cryptographic hash function producing the 16-byte long hash values from input of an arbitrary length. It was de-signed in 1991 and is used in modern communications for data integrity checks and authentication mechanisms used to conceal the plaintext passwords and prevent its transmission over insecure networks.

![Figure 1. Schematic operation of MD5 hash function according to [1].](image)
Since its design several flaws of MD5 have been discovered allowing for creation of collisions (different inputs produce same output) or even breaking the cipher, which is why this hash function is not recommended for SSL certificates or digital signatures and should be replaced by other and more secure hash functions.

Despite this recommendation, MD5 still can be seen in production environments even in situations where the possible attack can cause significant damage. The example of this is the SIP communication, where the MD5 is used for authentication and if the attacker is able to capture network traffic, he can relatively easily steal the user account. The illustration of this attack and the security considerations will be present-ed later.

The MD5 algorithm splits the input into 512 bit chunks on which the given mathematical operations are performed. If the data cannot be divided, the input is zero-pad-ded and the 64-bit information about the original length is appended. Each chunk is then processed in 4 rounds as it is outlined on the Fig. 1 [1,2].

B. Digest Access Authentication

The Digest Access Authentication Scheme is widely used to prevent the plaintext passwords to be transmitted over the insecure network. In SIP we can encounter a digest authentication based on the MD5 algorithm. Basically, we can state that the client transmits the MD5 hash calculated from its credentials and the message headers. In greater detail we can distinguish three stages of calculation:

- $H(A1) = \text{MD5}(\text{username:realm:password})$,
- $H(A2) = \text{MD5}(\text{method:sip_uri})$,
- $\text{Response} = \text{MD5}[H(A1):\text{nonce}:H(A2)]$.

All the parameters required for the response calculation are transmitted over network insecurely. To be more precise, the required information can be obtained by examination of SIP headers in the authentication request. Method and sip_uri can be obtained from the request line of the SIP header. For example the following request line:

```
REGISTER sip:localhost SIP/2.0
```

results in method equal to "REGISTER" and sip_uri equal to "sip:localhost". All the other parameters for the response calculation can be found in authentication header, which may look as follows:

```
Digest username="100", realm="asterisk", \nnonce="16f24eb8", uri="sip:localhost", \nresponse="729cf3487af16529195ea7867ee3d883", \nalgorithm=MD5
```

From this it is obvious that if the attacker manages to capture the SIP message containing this content, he could try to gain knowledge about the original client password.

C. CUDA

CUDA is the abbreviation for the Nvidia’s Compute Unified Device Architecture, which allows for running high level programs written for instance in C/C++ on a graphic card. The graphic cards are designed to contain so called stream processors (or CUDA units), the main purpose of which is a calculation of graphical information. However, since 2006 and the Nvidia chip G80 these processors can be used for general calculations such as weather modeling, molecular dynamics modeling and so on. The main advantage of using graphic card (GPU) over processor (CPU) is the number of stream processors, which is very high even for mainstream GPUs and which allows for massive parallelization.

Whereas the CPU can offer 4 to 8 cores capable of handling complex operations using the modern instruction sets such as SSE, the GPU offers simple cores in high quantities. The basic difference between CPU and GPU is depicted on the Fig. 2 [3,4].

![Figure 2. Comparison of simplified CPU and GPU architectures][3]

There are several tools that use the power of CUDA architecture or its AMD counterpart STREAM to maximize their computational power. In our case, we are going to use Hashcat and CudASIPcracker.

III. EXPERIMENT

To find out how quickly the attacker can steal the password from the communication we have prepared a testing platform with massive computational power. The corner-stone of this platform are two dual-core GPUs nVidia GTX590, which provide 1024 stream processors (CUDA cores) working at 607 MHz. The theoretical computational power according to the manufacturer reaches 2.5 TFLOPS. The other important data about the measuring platform summarizes following list:

- CPU Intel 3930K @ 3.2GHz (6 cores),
- 16 GB DDR3 RAM @ 1600 MHz,
- OS Windows 7 SP1 x64.

From the given we can state that the platform is the current high-end. On this platform two MD5 cracking tools were installed. First, the Hashcat in its CUDA variant. Second, the CUDA SIP Cracker.

A. CudaHashcat

Hashcat [5] is an open-source software tool for breaking the hash functions in vast variety of implementations ranging
from MD5 and salted MD5 to such special implementations such as Joomla hash, or even DES.

In our case we focused on using hashcat to break the MD5 hash values of password of reasonable length and character set. We used two assumptions: first, the password to be remembered can contain only numbers, lower and upper case letters, not special characters. Second, the password length was determined to 8 characters because of the compromise between password efficiency and the easiness to remember it. Of course longer or shorter passwords can be used; however the former need more time to be cracked, while the latter can be broken in matter of minutes, which is very insecure. The special character can be used for passwords as well; however it is not likely because of the need to configure the telephones. In general, same approach can be used even for passwords with special characters.

To generate passwords we used strong password generator to generate three passwords of a length 8 and from the given characters. This way we created three groups of passwords – from lowercase characters, from lower and uppercase characters and from the lower and uppercase letters and digits. These three groups of passwords were then exposed to attack using hashcat, which resulted in the data contained in the Tab. 1.

<table>
<thead>
<tr>
<th>Plain Password</th>
<th>Time to Crack [s]</th>
<th>Theoret. Max. [s]</th>
</tr>
</thead>
<tbody>
<tr>
<td>nrlcwelm</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>ryvbbwlo</td>
<td>7</td>
<td>35</td>
</tr>
<tr>
<td>skxznwpwv</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>vCczDrrU</td>
<td>4920</td>
<td></td>
</tr>
<tr>
<td>YbmfeCFp</td>
<td>7320</td>
<td>8500</td>
</tr>
<tr>
<td>QiecRWsd</td>
<td>1935</td>
<td></td>
</tr>
<tr>
<td>CDoXEGcr</td>
<td>3599</td>
<td></td>
</tr>
<tr>
<td>ATszJRL2</td>
<td>5280</td>
<td>34700</td>
</tr>
<tr>
<td>fAD9cBy9</td>
<td>5580</td>
<td></td>
</tr>
</tbody>
</table>

It is clear that breaking the relatively secure password encoded by the MD5 hash is the question of hours due to the usage of high performance GPU computing. The maximal computational power of the measuring platform was estimated to 6 300 M/s, which can give us the theoretical maximum for each group of password using the following equation (1) and (2).

\[ T_{\text{max}} = \frac{N}{v} \]  
\[ N = N_{\text{char}}^l \]  

In (1) the \( N \) specifies the total number of possible passwords of the given length and character set and \( v \) is the computational speed of the platform. \( N_{\text{char}} \) is the number of characters in the given character set and \( l \) is the password length. Although the character set between second and third group increased by 10 numbers to 62 total characters, the three given hashes from the third group had similar breaking times as the hashes from the group 2. To complete the picture it is necessary to say, that the first hash with only lowercase characters as the character set took 9 138 seconds to be cracked using the CPU. From this it is obvious that for calculations such as hash computation the graphic cards are superior to CPUs.

### B. CudaSIPcracker

The Hashcat provided us the means to calculate the plaintext password from the given hash values. It is one of the best tools for this, but it did not give us the needed password from the SIP communication. For this purpose, the CUDA SIP Cracker comes to the scene.

This tool can calculate the password from the strings contained in the SIP header as stated in the section 2. However it is not well optimized and in our environment it allowed only one GPU core to be utilized. Therefore the Hashcat was chosen as the main tool for this paper. Still the calculation of the last given hash took almost 7 days, which is of course a high value, however still easily reachable.

### IV. Conclusion

This paper did not try to come up with the breath-taking new technology; it was rather focused on bringing some enlightenment to VoIP community. In present days many people know about the computational capacity of the massively parallel applications using the CUDA, STREAM or OpenCL technology, but quite few know what the relation between this computational power and the time scale for cracking the passwords is. By this paper we wanted to show that even seemingly strong password can be broken in matter of hours using commonly available software, not mentioning the speed and efficiency of some proprietary solutions. The speeds reached in our experiment could still be increased using AMD graphic cards, which seem to tend to a better performance in this type of calculations. With this in mind the standard digest access authentication in SIP should always be enhanced by other security precautions like SIPS, IPSec, or other when communicating over the insecure network.

### Acknowledgment

This work has been supported by the project OPVK No. CZ.1.07/2.2.00/28.00 62, Joint activities of BUT and TUO while creating the content of accredited technical courses in ICT.

### References


IMPACT OF SRTP PROTOCOL ON VOIP CALL QUALITY

Michal Halas, Lubos Javorcek, Adrian Kováč
Department of Telecommunications
Faculty of Electrical Engineering and Information Technology, Slovak University of Technology, Slovak republic
michal.halas@stuba.sk, javorcek@gmail.com, kovac@ktl.elf.stuba.sk

Abstract. The article describes the impact of VoIP communications security using SRTP protocol on the voice quality. SRTP as one of the protocols ensuring the protection of multimedia transmission significantly contribute to increased security in VoIP networks, its usage affects the quality of voice communications. The paper describes how to setup SRTP protocol support for Asterisk. The impact of security on voice quality is experimental verified for G.711 and GSM codecs. For measurements, we investigated the effect of increasing level of packet loss (1, 3 and 5%) of the final voice quality at the way of unencrypted and encrypted transmission.

Keywords- SRTP, VoIP, MOS, packet loss, network traffic, call quality

I. INTRODUCTION

VoIP communication as a kind of specific data transfer might be a target of security attacks. With the increasing usage of this technology is also becoming increasingly topical issue of security. The paper deals with problems of security of VoIP communications using the SRTP protocol and security impact on the quality of voice communication.

Firstly it is described how to configure support for SRTP protocol in Asterisk, which is one of the most popular open source PABX. This PABX is part of experimental laboratory, which is examined the impact of security on the quality of voice communication for selected codecs and also the impact of several levels of packet loss rate on voice quality.

II. SRTP SUPPORT IN ASTERISK

Asterisk was installed as a standalone service on a server running Linux Ubuntu 10.11. Therefore standard installation is not described, attention will be devoted to configuration of support SRTP and TLS protocols.

First of all it should be added necessary libraries to the system to ensure the functioning of the TLS and SRTP, it is done by the libraries libssl-dev and srtp-1.4.2.tgz (http://srtp.sourceforge.net/download.html). After the successful installation, it is needed to compile and install Asterisk from source packages, to provide integration support for both protocols. In our case it was a version of Asterisk 1.8.7.1.

SRTP is after the installation immediately usable, but support for TLS requires the creation of appropriate certificates that will be placed in the folder /etc/asterisk/keys, which need to be manually created.

Subsequently, to generate the certificate we will use the script ast_tls_cert, which is part of Asterisk installation source files.

To create a server certificate in our case we used the command

```
./ast_tls_cert -C 192.168.1.2 -O ,,UT FEI STU“\n-d /etc/asterisk/keys
```

To create a client certificate command

```
./ast_tls_cert –m client -c /etc/asterisk/keys/ca.crt \n-k /etc/asterisk/keys/ca.key -C 192.168.1.3 \n-O ,,UT FEI STU“ -d /etc/asterisk/keys -o user1
```

Finally we must enable support for SRTP and TLS and configure asterisk in itself, particularly in the sip.conf file. It is necessary to add the following entry to the section [general].

```
[general]
tlsenable = yes
tlsbindaddr = 0.0.0.0
tlscafile = /etc/asterisk/keys/asterisk.pem
tlsconf = /etc/asterisk/keys/asterisk.pem
tlscafile = /etc/asterisk/keys/asterisk.pem
```

As the client application we used BLINK, which needs to have appropriate generated certificates, specifically files /etc/asterisk/keys/asterisk.pem in the configuration it is needed to change SRTP Encryption option from “optional” to “mandatory”.

transport = tls
and enable encryption using SRTP
encryption = yes

As the client application we used BLINK, which needs to have appropriate generated certificates, specifically files /etc/asterisk/keys/asterisk.pem and /etc/asterisk/keys/user1.pem. In the configuration it is needed to change SRTP Encryption option from “optional” to “mandatory”.

transport = tls
With these settings, the client is able to connect using a secure connection TLS and SRTP as key exchange mechanism is used SDES.

III. MEASUREMENTS AND RESULTS

To experimentally measure the impact of security on the call quality was created following experimental network consisting of 3 computers, its topology is shown in Figure 1.

![Figure 1. Topology of experimental laboratory](image)

On the PC1 it was installed client software BLINK version 0.2.7, which was used to generate a number of encrypted and unencrypted calls. On the host there was also installed a measurement program OmniPeek Network Analyzer which analyses voice quality using non-intrusively method based on RTCP protocol messages. This software provides Predictive MOS (PMOS) value and R-Factor value of all running calls.

PC2 using software WANem emulates transmission lines of specific parameters, we used it to setup specific levels of packets loss.

PC3 act as a server with Asterisk, the phone extension 202 of which were directed test call was set up to automatically replayed the selected voice file to make the call without any user intervention. The corresponding part of configuration in the file extensions.conf is

```
exten => 202,1,Answer()
same => n,Playback(twisted2)
same => n,Hangup()
```

In measurements we investigated the effect of SRTP protocol usage to increasing transmission bandwidth of calls and claims affect the quality of communication when there is packet loss on the transmission line.

For each measurement were created 10 simultaneous phone calls, each lasting 2 minutes and measurements were repeated 3 times in a row and the results were statistically processed. We studied these parameters for G711 and GSM codecs with disabled VAD mechanism.

Encrypted SRTP calls necessarily leads to increase in transmission bandwidth as it presented in the figure 2.

Measurements showed that for 10 calls with G.711 codec is needed without encryption 1.747 Mbps, with encryption 1.829 Mbps which is an increase of approximately 4.7%.

The GSM codec for unencrypted stream is needed 0.732 Mbps, with encryption 0.8117 Mbps what constitutes an increase of more than 10.9%.

This fact is very important especially in the dimensioning of the transmission paths and QoS methods, as in the case of poorly designed transmission parameters may increase of the transmission capacity, cause increased loss and delay which results in reduced quality of voice communication.

Subsequently the measurements examine the effects of varying levels of packet loss rate on the quality of communication with and without security encryption. Specifically, the set of loss rates were 0%, 1%, 3% and 5%.

The obtained results are presented in table 1 and charts figure 3 and 4.

<table>
<thead>
<tr>
<th>TABLE I. MOS VALUE FOR SELECTED CODECS AND LEVEL OF PACKET LOSS.</th>
<th>0%</th>
<th>1%</th>
<th>3%</th>
<th>5%</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711 RTP</td>
<td>4.170</td>
<td>3.953</td>
<td>3.400</td>
<td>2.960</td>
</tr>
<tr>
<td>G.711 SRTP</td>
<td>4.170</td>
<td>3.952</td>
<td>3.396</td>
<td>2.922</td>
</tr>
<tr>
<td>GSM RTP</td>
<td>3.520</td>
<td>3.418</td>
<td>3.149</td>
<td>2.917</td>
</tr>
<tr>
<td>GSM SRTP</td>
<td>3.520</td>
<td>3.403</td>
<td>3.165</td>
<td>2.925</td>
</tr>
</tbody>
</table>
IV. CONCLUSION

Measurements showed that the implementation of SRTP security protocol for transmission of VoIP calls minimal affects the quality of voice communication. For any amount of loss level it was only minimal impairment in MOS value, observed changes are on the edge of measurability.

However in real deployment of encryption transfer, need to be expected an increase of required bandwidth for the transmission of encrypted flows. In the case of GSM codec is an increase at almost 11%. In case of large quantities of calls and inadequately dimensioned transmission line, or incorrectly configured queuing method, it can lead to in-creasing the delay and loss rates, which will degrade the quality of voice communications.

Considering the fact that VoIP is increasingly used, also increases the intensity of security attacks. It is therefore appropriate to secure the transfer using SRTP protocol, because it has only a minimal effect in changing the quality of communication it is a convenient way to reliably ensure the security of communications.

ACKNOWLEDGMENT

This work is a part of research activities conducted at Slovak University of Technology Bratislava, Faculty of Electrical Engineering and Information Technology, Department of Telecommunications, within the scope of the projects “Analysis of the impact of traffic parameters on voice quality in IMS networks”, supported by the STU University grant programme “Grant programme to support young researchers”.

The support was also provided by the Center of Excellence for SMART Technologies, Systems and Services II., ITMS 26240120029, co-funded by the ERDF.

REFERENCES


Abstract—Goal of this workshop is to show possibilities of BESIP[4] PBX in organisation as Session Border Controller (SBC). After two years of development, we are focusing to release stable version of BESIP, which is able to run on almost any hardware, from virtual appliance to SOHO router. SBC configured in BESIP[4] is one result of project. The aim of the BESIP[4] project is the development and implementation of an embedded SIP communication server based in open-source solutions for small branch offices. BESIP[4] provides advanced management services based on the ideas described above, is modular, each element consists of several applications. The core of the BESIP distribution is based on OpenWrt, the basic SIP services such as call routing and endpoint registrations are ensured by Kamailio[8], the advanced and supplementary services have been nested in Asterisk[9]. We tweaked the yuma - YANG-based Unified Modular Automation toolkit for the NETCONF protocol and customized it for our needs, BESIP is manageable by any NETCONF client.

I. INTRODUCTION

The aim of the BESIP project is the development and implementation of embedded SIP communication server with an easy integration into the computer network based on open-source solutions. The solution will serve to provide SIP IP telephony infrastructure for small branch offices, and offers several advanced management services and support for SIP communication server itself. This project is supported by CESNET organization (http://www.ces.net). During our work, we try to focus on security and reliability by default. This paper deals with preparation and tests of BESIP as SBC for small or medium organisation.

II. REQUIREMENTS

Typical organization needs some basic tasks to be served by SBC. There are SBCs on the market which are able to do this and many other jobs. BESIP cannot be concurrence for other commercial systems with hardware acceleration. But it can be option for smaller organizations with limited budget. Our work was focused primarily to this users. It can vary from organization to organization, but main goals of SBC are:

A. Topology hiding

It is crucial to hide internal infrastructure to rest of the world. Nobody should know informations about internal IP addresses or gateways.

B. NAT traversal

Many organizations needs to allow user to use they phones even if they are behind NAT. This can be done either directly in internal PBX or on SBC.

C. Registration from outside

To allow external users to either redirect registration to internal PBX or to register to SBC and forward calls to internal system.

D. Security

To check SIP messages against basic security incidents and make internal system safe.

E. Routing

Sometimes it is needed to route requests from internal system to more external systems and this functionality can be achieved by SBC too. Many SIP providers require only one IP of gateway for peering and they do not allow traffic from another IP addresses. Evenmore, if external routing database is needed (like ENUM), it is good to lookup for it inside SBC. There are several possibilities to route traffic from internal network to outside. Depending on scenario, SBC routing takes care of it.

1) Redirect server: Internal system routes all traffic to SBC, which will try to find best free of charge way to destination (like ENUM or known free gateways). If destination route and gateway is known, it will reply with 3XX message, specifying right gateway which should be used. Internal system has to understand 3XX redirect message.

2) Not acceptable: There is another option in routing which will send 4XX reply “Not acceptable” if gateway is not found. At this scenario, internal system routes all traffic to SBC which will try to find best free of charge gateway. If gateway is found,
SBC will route request there. If not, 4XX “Not acceptable” is returned. Internal system has to be configured for fallback. So if primary way (SBC) fails, it will route request by another path (paid gateway). This scenario is very good if it is complex to setup internal system routes.

3) SIP routing types: SIP protocol was developed as domain-based. This implicates that domain part is used for routing to right gateway and user part of request is used to find specific user. This is right scenario and works well. Gateway lookup is most often served by DNS NAPTR and SRV records. But in telephone world, this scenario is little bit complicated, if user part is not username but telephone number. If so, routing is more complex, because telephone numbers has to be directed to different gateways based on prefix. BESIP SBC can do both routing types. First, domain part is checked. After it, user part is taken into account. If it is telephone number, it is parsed and checked again known prefixes. In modern systems, telephone number should be only alias of user@domain because global routing will be focused to Internet type as other protocols do (email, jabber, ...). Instead of searching phone number, it is easier to remember user uri and call directly to uri which is similar or same as email.

4) Number Normalisation: Number normalisation is used when there are more kind of number types. For example, is it possible to call number XXXX to achieve local users, or to call +XXXXXXX... to achieve external users. Normalisation is optional and can be switched off but it is good idea to normalise all numbers before doing any prefix lookups. When normalised, numbers are in international E.164 format but without + sign.

III. Technology

BESIP core is kamailio. It is powerful SIP proxy with all advantages and disadvantages. Advantage is that it is highly configurable, stable compact and extendable software. It is relatively easy to interconnect it with LDAP, SQL, DNS or other lookup databases and route SIP request according to result. Disadvantage is that it is complex to hide internal topology because entire call is one SIP dialog. In opposite of this, if Asterisk is used ad SBC, call is divided into two independent call legs and informations will not flow to other side. Both scenarios are possible, but at this stage of development, only kamailio SBC is supported. In many situations, SIP routing is based on external databases like ENUM, DNS, SQL or LDAP. Our system is able to query all of this databases to route request.

A. LDAP

Lightweight Directory Access Protocol is widely used for authentication purposes in campus networks. It is common place to authenticate users or get structured data. In our setup, we are able to communicate with LDAP and do:

1) Authentication: It is possible to authenticate INVITE and REGISTER requests via LDAP. Special attribute with cleartext password is used for it. It is not possible to call BIND function of LDAP and use user password because SIP needs to make hashes from it to work.

2) Attribute-Value Pairs: During authentication, it is possible to get specific data from LDAP based on username (AVP). This can be rpid, email or call privileges now, but in future, it can be extended to more attributes. This is good for specific requirements of the user. For example, specific redirection, privileges or routing.

3) Number to name aliases: If request user part is telephone number, it is possible to search in LDAP database, if it belongs to some user. If so, call is forked and forwarded to user@domain. In most cases, this will search user in location database if he is registered.

4) Name to number alias: If request user part is not number, it is possible to search in LDAP database and find corresponding telephone number. Call is forked and forwarded to that number.

B. MediaProxy

For NAT traversal and topology hiding, MediaProxy is used. MediaProxy can act as proxy only for private IP addresses or it can be configured that any request going from/to local network can be translated into SBC address. This prevents outside world from communicating with internal systems but it will not hide internal Ips, they are still inside SIP headers.

C. Topoh

This is main kamailio module for topology hiding. It will replace all local ips by virtual ones and add hashes to them. So there is no information about any internal device in SIP request. Disadvantage is, that request can be very long after adding hashes. It is often that it is longer than 1500 bytes and there can be problem with UDP fragmentation. It is good to use TCP transport when using this module.

D. UCI

Unified Configuration Interface (UCI) is OpenWrt technology used for abstraction layer between software configurations and user. All fully-working OpenWrt packages which needs some configuration should use this abstraction layer. We created kamailio UCI init script, which translates UCI configuration into kamailio config. This will make configuration of BESIP much more easier because user does not have to know kamailio syntax.

IV. Conclusion

BESIP[4] is able to act as SBC for small and medium organisations. Even if we are still working on stable version, it is possible to use it now. Advantage of BESIP[4] is, that it is not Linux distribution with all packages, libraries and files but it is distributed as image. Image can be used for Vmware, KVM or other virtualisation technology or it can be embedded into specialized device. Today, x86 targets are used for virtualisation and MIPS targets are used to flash into some SOHO routers like ASUS WL-500gp or TPLink 1043ND. Even more, any OpenWrt user can use BESIP[4] packages
without flashing his device because we provide standard
OpenWrt feeds for BESIP packages.

REFERENCES

[1] Voznak, M., Macura, L., Slachta, J., Modular SIP Server on embedded
Platform, In Recent Researches on Communications and Computers, Part
of CSCC’12 , Kos, July 14-17, 2012, pp. 260-265, ISBN 978-1-61804-
109-8

SIP Server Solution, In Proc. 35th International Conference on Telecom-
munication and Signal Processing, Prague, July 3-4, 2012, pp. 263-266,
ISBN 978-14673-1116-8 (will be indexed in ISI, SCOPUS and IEEE-
Xplore)

Communication Systems, In Proc. International Conference on Telecom-
munication Systems, Modeling and Analysis (ICTSM2012), Prague, May


[5] Voznak, M., Rezac, F. Threats to Voice over IP Communications Systems,
WSEAS TRANSACTIONS on COMMUNICATIONS, Issue 11, Volume
9, pp. 1348-1358, September 2010, ISSN: 1109-2742. SCImago=0,039
(SCOPUS, ACM)

Solution for IP Telephony - BESIP. The 13th International Conference
on Research in Telecommunication Technologies, pp. 119-121, September


Contact Center Models

Erik Chromy, Tibor Misuth
Institute of Telecommunications, Faculty of Electrical Engineering and Information Technology
Slovak University of Technology Bratislava
Bratislava, Slovakia
chromy@ut.fei.stuba.sk, misuth@ut.fei.stuba.sk

Abstract—Contact center is complex communication system which arises as upgrade of private branch exchange and offers integrated system for communication with customers whether by telephone call, e-mail or even by text chat with contact center agent. It is very difficult to describe such complex system by mathematical models, therefore in the next we will see under term contact center only the system for processing of telephone calls. The paper deals with models that we can use for calculation of important traffic parameters of contact center.

Keywords—Contact center; Erlang B formula; Erlang C formula; M/M/m/∞; M/M/m/K

I. INTRODUCTION

Today there almost isn’t a company or institution that could exist without any form of outer contact. On the contrary the accessibility of simple, fast and convenient form of connection with their clients or business partners grows day by day.

Contact center is one of many other ways how the institution is able to provide for all its communication requirements towards clients and partners. Central part of any contact center and its basic logic is realized by Automatic Call Distribution (ACD) functionality. ACD is responsible for correct and efficient routing of all types of requests (phone calls, emails, etc.) since they arrive to the contact center until they are served.

ACD belongs to the basic software features, that is needed to the contact center realization. Agents assigned to the individual service groups (Fig. 1) process the same type of incoming calls. ACD classifies and routes incoming calls according to programmed rules – e.g. according to the called number, arrival time of call, length of the waiting queue, etc.

Then the calls are routed to the agent service groups (sales department, technical department, customer service, etc.). Through the ACD the calls can be routed to the next free, or to the longest free agent of the particular service group. The result is the uniform distribution of working load on all agents of the service group or processing the major of phone calls by one of the best agents.

Contact centers are built in order to effective resources utilization (whether technical or human). Thereat, we have also to think about the situation that there is no free agent with appropriate skills for the customer. Therefore, there must be waiting queues in contact center.

II. TRAFFIC PARAMETERS IN CONTACT CENTER

Each component of ACD system can be more or less precisely converted to a mathematical model [1], [2]. Since the ACD systems usually handle large amount of requests per time unit, the vast majority of these models is based on statistic principles. The accuracy of results depends mostly on correct model selection. Moreover precise description of input argument and variable dependencies can significantly influence them as well.

A. Input traffic model

Arriving calls (or other requests) rate per time unit can be considered as random variable. Contact center’s goal is to provide its services to wide range of customers so that we can assume the requests population to be unlimited. Once the population is unlimited we can pronounce the ACD system to be a queuing system with unlimited request population [3], [4].

Each request towards contact center originates randomly and independently from all other requests. From mathematic point of view are events (calls) independent if for any arbitrary set of requests \( A_1, A_2, \ldots, A_n \) and arrival probabilities in selected time interval \( P(A_1), P(A_2), \ldots, P(A_n) \) is true [5].
\[ P(\bigcap_{i=1}^{n} A_i) = \prod_{i=1}^{n} P(A_i) \] (1)

So the arrival probability of \( n \) requests during the same time interval equals to product of individual request arrival probabilities for this interval.

The calls per time unit rate can be simplified to acquire only integer values and the random variable is discrete. Any random variable can be described by probability density function. In case of discrete random variable \( X \) with values \( x \) it’s defined by the formula:

\[ f(x) = P(X = x). \] (2)

Obviously the \( \sum_{x \in H} f(x) = 1 \), where \( H \) is the set of all values the random variable \( X \) can acquire.

Next important random variable’s characteristics are the mean and variance. Let random variable \( X \) has values \( x_1, ..., x_n \) with corresponding probabilities \( p_1, ..., p_n \). Then mean is defined as

\[ E(X) = \sum_{i=1}^{n} x_i p_i \] (3)

**Poisson distribution** [4], [5] is most usually used to model arriving requests to a queuing network. Following formula define probability that \( k \) requests arrive during time interval \( T \) for which average arrival rate \( \lambda \) is defined

\[ p_k = f(k) = P(X = k) = \frac{\lambda^k e^{-\lambda}}{k!} \] (4)

Next, mean and variance for Poisson distribution are:

\[ E(X) = \lambda \] (5)

\[ D(X) = \lambda \] (6)

The interarrival time is very important variable as well. Since the arrival rate is random variable the interarrival time must be random variable as well. Based on independence of each request the interarrival time for Poisson traffic flow is exponentially distributed continuous random variable with mean equals to \( 1/\lambda \) [6]. The probability density of this random variable is defined by following formula \( (t \) represents the interarrival time) [4], [5]:

\[ f(t) = \lambda e^{-\lambda t} \] (7)

The random variable with Poisson distribution is the most frequently used instance to model input traffic.

**B. Service group model**

Service group consists of one or more agents with similar skills and knowledge and optionally a queue. Therefore each service group is dedicated to serve requests of specific types corresponding to knowledge of its agents.

From the queuing theory point of view an agent is the server where the requests are processed. In case there are more requests at the same time present, the later coming requests have to wait in the queue.

Danish mathematician A. K. Erlang is very closely connected to the origin of queuing theory [3]. The paper concerning application of statistics in telephone service was published by him in 1909. This document initialized further research of queuing theory. Later together with Markov chains theory his ideas helped to define and describe more complicated queuing models.

In 1953 D. G. Kendall introduced dedicated queuing system categorizing scheme. It is based on combination of letters and numbers in pattern [3, 4] (A/B/X/Y), where \( A \) represents the interarrival time distribution, \( B \) defines the handling time distribution, \( X \) denotes the server count and \( Y \) defines the maximum system capacity. Comparison of theory with real systems showed the best distribution to describe the interarrival time is exponential distribution noted as \( M \). That’s why our research is based on M/M/X/Y models.

Both Erlang and M/M/X/Y models are based on the same assumption and following requirements must be met [7]:

- Number of source (requests population) is much more greater than the server count,
- The requests are generated randomly and independently of each other,
- Calls arrive individually and can be assigned to any agent in corresponding service group (full accessibility),
- The average request count per time unit from all sources is constant,
- The handling time is random variable with exponential distribution,
- Queuing discipline is FIFO.

Several metrics exists to evaluate the contact center service. Among the most important parameters appertain [3, 4, 7, 8, 9]:

- Average waiting time – defines the average waiting time the request spends in the queue before it is assigned to the agent (usually named as \( W \)),
- Average queue length – denotes the average number of requests present in the queue at any moment (usually named as \( Q \)).
• Average number of requests in the system – this parameter informs about Access lines utilization (usually named as $K$),

• Average time spent in the system – shows the average time the request spends in system from entrance to the queue until it is served and exits the system (usually named as $T$),

• Agent utilization – informs about percentage of time used by agents to handle the requests,

• AHT (Average Handling Time) – denotes the average time the agent is occupied by handling one request including the time spent for „paper-work“ before and after the handling,

• GoS (Grade of Service) – any denotes the percentage of requests served (assigned to agent) before defined threshold AWT (Acceptable Waiting Time),

• Call loss probability – probability the request is not served at all due to some reason (insufficient capacity of lines, maximum waiting time exceeded, etc.),

• Queuing probability – probability the request entering the system is not assigned to a free agent immediately but has to wait in the queue.

The first two metrics are the most frequently used to monitor the control center service level. They are capable of describe almost all situations that can occur in contact center quite well.

C. Erlang B formula - model $M/M/m/m$

Erlang B formula is the very basic formula which does not contain the queue. Incoming calls are assigned to a free agent directly if there is any, otherwise they are considered lost and the caller receives busy signal [7]. An analogy to this behavior is usage of all trunks that interconnects contact center to PSTN (Public Switched Telephone Network) or any other communication network. Once there is no more available lines, the requests cannot be put through to the contact center and is blocked (rejected). This implies the Erlang B formula is widely used to dimension the trunk capacity between contact center and communication networks. Nowadays VoIP technology is more and more important, but the basic capacity problem is only slightly modified to available data throughput of the connection. Thus Erlang B formula can be used in this case as well.

The Erlang formula operates with 3 basic variables:

• $A$ – the offered traffic in Erlangs,

• $N$ – number of lines / trunks (requested simultaneous connections),

• $P_B$ – call loss probability.

The original form of the equation allows us to find the call loss probability if $A$ and $N$ values are known:

$$P_B(N, A) = \frac{A^N}{N!} \sum_{i=0}^{N} \frac{A^n}{i!}$$

(8)

If we know the rate of calls per time unit $\lambda$ and the average number of served requests per the same time unit $\mu$ (so the average handling time is $1/\mu$) then the traffic load can be easily evaluated as [10]

$$A = \frac{\lambda}{\mu}$$

(9)

If we substitute $A$ in equation (8) we receive following:

$$P_B(N, \lambda, \mu) = \frac{\left(\frac{\lambda}{\mu}\right)^N}{N!} \sum_{i=0}^{N} \left[\left(\frac{\lambda}{\mu}\right)^i \frac{1}{i!}\right]$$

(10)

that is the same formula as obtain from $M/M/m/m$ queuing system [3], [4]. We have just analytically showed the two mentioned formulas are in fact identical in terms of usage (9) for offered load computation.

A slight modification can be added to the original Erlang B formula to obtain so called extended Erlang B formula [11]. This formula considers some of the lost calls are retried immediately.

D. Erlang C formula - model $M/M/m/\infty$

The immediate loss of incoming call if there is no free agent available (Erlang B formula principle) is probably not the best approach how to handle requests in contact center. However the second Erlang formula, the Erlang C formula, eliminates this disadvantage. In this case the system contains the queue, where the incoming requests can wait until an agent is available. The maximum queue length is unlimited so however this model is better to use, it still has some limitations. The algorithm is very simple. FIFO queuing discipline is used, so when any agent becomes available, the first request from the queue is immediately assigned to him / her. If the queue is empty, the agent remains in available state and waits for the next incoming call, which will be assigned to him / her without queuing.

Erlang C formula [7] is originally defined as function of two variables: the number of agents $N$ and the traffic load $A$. Using this values it calculates the probability $P_c (11)$, that the arriving request is not assigned to agent immediately but has to wait in the queue.
The comparison of both Erlang equation (8) and (11) shows that they define the probability the system is not capable of immediate request processing. The only difference is the way, how the nonresponded calls are handled.

At this point we can use the equation (9) once again. Moreover we define the variable $\rho$, that presents the utilization of 1 agent as [3, 4, 11]:

$$\rho = \frac{\lambda}{N\mu}$$  \hspace{1cm} (12)

By combining equations (9), (12) and (11) we obtain following

$$P_C(N, A) = \frac{A^N N}{N!(N-A)} \sum_{i=0}^{N-1} \frac{A^i}{i!} + \frac{A^N N}{N!(N-A)}$$  \hspace{1cm} (13)

$$P_C(N, A) = \frac{(\frac{\lambda}{\mu})^N N!}{N!N-(\frac{\lambda}{\mu})^N} = \frac{(N\rho)^N}{N!(1-\rho)} \sum_{i=0}^{N-1} \frac{(N\rho)^i}{i!} + \frac{(N\rho)^N}{N!(1-\rho)}$$

If we start from M/M/m/$\infty$ queuing model we can derive identical equation that will define probability $m$ or more requests are present in the queuing system so the new coming request will be inserted to the queue [3, 4, 11]. This simply means Markovian M/M/m/$\infty$ and Erlang C formulas are identical and this relationship can be easily proved analytically.

Since the Erlang C considers the queue, there are some more parameters and variables which can be measured and more or less influenced by model inputs. From the callers point of view the most important value is the waiting time or time the request spends in the queue before reception by an agent. This value is random variable described by probability density function [9]

$$F_W(\tau) = \begin{cases} 1 - P_C & \tau = 0 \\ 1 - P_C \cdot e^{-\mu(N-A)\tau} & \tau > 0 \end{cases}$$  \hspace{1cm} (14)

Based on this formula we can calculate the average waiting time (or average speed of answer ASA) $W$

$$W = \frac{P_C}{\mu(N-A)}$$  \hspace{1cm} (15)

and using Little’s theorem [9] and (9) equation we obtain the average number in the queue $Q$

$$Q = \frac{\lambda W}{\mu(N-A)} P_C = \frac{A}{(N-A) P_C}$$  \hspace{1cm} (16)

The general definition of probability density function of any statistical distribution and its properties [5] gives us an opportunity to derive GoS parameter value from (14) equation once the acceptable waiting time (AWT) value is known [3, 10]

$$GoS = 1 - P_C \cdot e^{-\mu(N-A)AWT}$$  \hspace{1cm} (17)

Following equation is valid for the average number of requests in queuing system [9]

$$K = N\rho + \frac{\rho}{1-\rho} P_C = A + \frac{A}{(N-A) P_C}$$  \hspace{1cm} (18)

Again, the Little’s theorem allows us to get the average time $T$ the request will spend in the system

$$T = K \frac{A}{\lambda} = \frac{A+Q}{\lambda} = \frac{1}{\mu} + W = \frac{1}{\mu} + \frac{P_C}{\mu(N-A)}$$  \hspace{1cm} (19)

Erlang C represents the basic formula for contact center simulation and parameters estimation. The most important limitation is the unlimited queue length. Nowadays it is not a computer memory related problem however no real call would be satisfied by extremely long waiting time. Majority of long waiting calls would be interrupted before served, but the Erlang C formula does not take it into account. So the real results and model’s results would not correspond and the simulation would be useless.

E. Mmodel M/M/m/K

The contact center modeled by Markov M/M/m/K model is stable in every traffic load, because in the case of full occupancy each other call is blocked. The parameter $\rho$ is therefore used for determination of traffic load per server, or per agent

$$\rho = \frac{\lambda}{m\mu} = \frac{A}{m}$$  \hspace{1cm} (20)

Probability that the system is empty (there is not any query) is given by:

$$P_0 = \sum_{i=0}^{m-1} \frac{m^i}{i!} \rho^i + \frac{m^m}{m!} \rho^m \frac{1 - \rho^{K-m+1}}{1 - \rho}$$, for $\rho \neq 1$  \hspace{1cm} (21)
\[ P_0 = \left[ \sum_{i=0}^{m} \frac{m^i}{i!} + \frac{m^m}{m!} (K - m + 1) \right]^{-1}, \text{ for } \rho = 1 \] (22)

Probability that in the system there are just \( n \) queries is given by:

\[ P(n) = \frac{1}{n!} \left( \frac{\lambda}{\mu} \right)^n P_0 = \frac{m^n}{n!} \rho^n P_0, \quad n = 0, 1, \ldots, m \] (23)

\[ P(n) = \left( \frac{\lambda}{m \mu} \right)^{n-m} P_m = \frac{m^n}{m!} \rho^m P_0, \quad n = m, m+1, \ldots, K \] (24)

where \( P_m \) is probability that just \( m \) queries are in the system.

In the case that just \( K \) queries are in the system each other incoming call is blocked. Probability \( P(K) \) specifies the probability of call blocking \( P_B \), and from equation (22) we have:

\[ P_B = \frac{m^n}{m!} \rho^K P_0 \] (25)

III. CONCLUSION

The objective of this paper is to show some of the approaches towards contact center parameter estimation. Probably the most widely used are simple Erlang B and C formulas and different Markovian models (M/M/m, M/M/\infty and M/M/m/K). The strongest advantage of Erlang formulas is their simplicity and ability to describe the most important operation situations of contact centers. However due to their limitations some special cases must be described by more complicated Markovian models.

The main advantage of Markov model is the wide spectrum of important traffic parameters of Contact Center calculations:

- Probability that calling customer will have to wait in the waiting queue for free agent,
- Probability of empty system,
- Mean number of requests in the whole system,
- Mean time that the request spend in the system,
- Mean time that the request spend in the waiting queue,
- Mean number of requests waiting in the queue.

In case of very complicated contact centers all mathematical models would be extremely complicated. In such cases it is a lot easier to use simulation software and experimentally test various values of parameters against expected results.

ACKNOWLEDGMENT

This work is a part of research activities conducted at Slovak University of Technology Bratislava, Faculty of Electrical Engineering and Information Technology, Institute of Telecommunications, within the scope of the projects „Grant programme to support young researchers of STU - Modeling of Traffic in NGN Networks“ and „Support of Center of Excellence for SMART Technologies, Systems and Services II, ITMS 26240120029, co-funded by the ERDF“.

REFERENCES

ANOMALY-BASED INTRUSION DETECTION IN IP NETWORKS

Pavel Nevlud, Lukas Kapicak, Jaroslav Zdralék
Department of Telecommunications, FEECS
VSB-TU Ostrava
Ostrava, Czech Republic
pavel.nevlud@vsb.cz

Abstract — The paper describes anomaly-based intrusion detection system for IP networks. As source of data are used pcap file with unreal data to avoid some ethical issues. As intrusion detection engine was used Snort and Suricata with own rules. For testing attacks was used powerful interactive packet manipulation program Scapy.

Keywords- Anomaly-based detection, attack, open-source, threats.

I. INTRODUCTION

The Intrusion Detection System is a process of monitoring the events in a computer system or network and analyzing them for signs of possible incidents. Which are violations or imminent threats of violation of computer security polices, acceptable use polices, or standard security practices [1].

An intrusion detection system gathers and analyzes information from various networks or systems to identify possible security issues. An intrusion prevention system is the process of performing intrusion detection and attempting to stop detected incidents. The detected incidents can be stopped with reset of TCP session or with drop some packets. IDS typically records information related to observed events, notifies security administrator with important observed events, and produces reports.

There are two main types of intrusion detection systems. The first type is signature-based and it relies on pattern-matching techniques. The patterns contain a database of signature of known attacks and IDS tries to match these signatures with analyzed data.

The second type of IDS is anomaly-based and it relies on build statistical model describing the normal network traffic. Any significant deviations compare to the model is considered as an attack. Anomaly-based IDSs have the advantage to detect zero-day attacks. New attacks can be detected as soon as they occur. This requires a training phase and careful settings of the detection threshold [2].

II. ANOMALY-BASED NETWORK IDS TECHNIQUES

Anomaly-based IDS build statistical model of the legitimate traffic during the training phase. We suppose attack-free network behavior. In the second phase, called detection phase, is traffic compared to the model. It is used distance function. When the distance measured exceeded a given threshold, the traffic is considered as a anomalous, and it may be marked as an attack.

![Basic architecture of anomaly-based intrusion detection system](image)

The major benefit of anomaly-based detection methods is that detection of attacks or stolen accounts is very simple. They can be also very effective in detecting previously unknown threats. The initial profile is generated over a period of time. Profiles for anomaly-based detection can be either static or dynamic. As additional events are observed, dynamic profile is adjusted constantly.

According to the type of processing related to the behavioral model of the target system, anomaly-based detection techniques can be classified into three main categories. The first type is statistical-based, second is knowledge-based and last is machine learning-based anomaly detection system.

In the statistical-based case, the behavior of the system is represented from a random viewpoint. On the other hand, knowledge-based IDS try to capture the claimed behavior from available system data as protocol specification, network traffic instances, etc. Finally, machine-learning IDS schemes are based on the establishment of an explicit or implicit model that allows the pattern analyzed to be categorized [3], [4].

A. Statistical-based Intrusion Detection System

In statistical-based system, the network traffic activity is captured and a profile representing its stochastic behavior is
Two datasets of network traffic are considered during the anomaly detection process. One corresponding to the currently observed profile over time and second is for the previously trained statistical profile. As the network events occur, the current profile is determined and an anomaly score estimated by comparison of the two behaviors. The score normally indicates the degree of irregularity for a specific event. The intrusion detection system will flag the occurrence of an anomaly when the score surpasses a certain threshold.

The earliest statistical approaches corresponded to univariate models, which modeled the parameters as independent Gaussian random variables. Later, multivariate models that consider the correlations between two or more metrics were proposed. These are useful because experimental data have shown that a better level of discrimination can be obtained from combinations of related measures rather than individually. Other studies have considered time series models. They use an interval timer, together with an event counter or resource measure, and take into account the other and the inter-arrival times of the observations as well as their values [5].

B. Knowledge-based Intrusion Detection System

One of the most widely used knowledge-based intrusion system is expert systems. Expert systems are intended to classify the audit data according to a set of rules, involving three steps. First, different attributes and classes are identified from the training data. Second, a set of classification rules, parameters or procedures are deduced. Third, the audit data are classified accordingly.

More restrictive in some senses are specification-based anomaly system, for which the desired model is manually constructed by a human expert. If the specifications are complete enough, the model will be able to detect illegitimate behavioral patterns. Specification could be developed by using finite state machine methodology. Sequence of states and transitions among them seems appropriate for modeling network protocols.

C. Machine Learning-based Intrusion Detection System

Machine learning methods are based on establishing an explicit or implicit model that enables the patterns analyzed to be categorized. A singular characteristic of these methods is the need for labeled data to train the behavioral model, a procedure that places severe demands on resources.

A Bayesian network is a model that encodes probabilistic relationships among variables of interest. This method is generally used for intrusion detection in combination with statistical schemes. This include the capability of encoding interdependencies between variables and predicting events, as well as the ability to incorporate both prior knowledge and data.

A neural networks can be adopted in the field of anomaly intrusion detection, because of their flexibility and adaptability to environmental changes. This detection approach has been employed to create user profiles to predict the next command from sequence of previous ones, to identify the intrusive behavior of traffic patterns.

A genetic algorithm are categorized as global search heuristics, and are particular class of evolutionary algorithms. GA use techniques inspired by evolutionary biology such as inheritance, mutation, selection and recombination. Thus, genetic algorithms capable of deriving classification rules and/or selecting appropriate features or optimal parameters for the detection process.

III. IMPLEMENTATION SNORT AND SURICATA AS INTRUSION DETECTION SYSTEM

For testing purpose was used Snort engine an Suricata engine with own rules. Both engine was installed on the server with Ubuntu server 10.04 distribution.

A. Snort IDS

As intrusion detection system has been chosen the Snort project. The Snort is open-source project developed by the Sourcefire. The Snort is the one of the most widely deployed IDS/IPS technology worldwide [6].

Network Intrusion Detection System allows to capture network traffic and compares this traffic with predefined pattern to analyze attacks. When attack appears the alert message could be displayed on the screen of Syslog server or it could be saved for the future analyzes.

First, traffic is acquired from the network via libpcap. Packets are passing through a series decoder routines that first fill out the packet structure for link level protocols. Then there are decoded parameters such as TCP and UDP ports.

Packets are sent through pre-registered set of preprocessors. Each preprocessor checks if every packet is what it should be. At this stage can be used anomaly-based features some modules.

After that packets are sent to the detection engine. The detection engine checks each packet against the various options listed in the Snort configuration files. Every keyword option is a plugin. This feature allows to be easily extended.

The default logging and alerting mechanisms are logged and encoded in ASCII format and it is used full alerts. The full alert mechanism displays the alert message in addition to the full packet headers. The alerts could be sent to the Syslog server.

The main configuration of the Snort is divided in the sixth section. The first section is used for settings of variables in network. There are defined some network parameters such as available networks, ports, ip addresses of servers:

```
var HOME_NET 10.0.0.0/24
var EXTERNAL_NET any
var HTTP_port 80
```

The second section is used for configure path in dynamic loaded libraries:
The third section is used for configure preprocessors. For example preprocessor module flow is used for tracking flow that is important for portscan. Preprocessor stream is used for stateful inspection or stream reassembly used for Snort.

The forth section defines configuration output plugins. For example output plugin tcpdump is applied for log packets in binary tcpdump format.

```
output log_tcpdump: tcpdump.log
```

The fifth section is used for add any runtime configuration directives. Some command line options may be specified in this section.

```
config interface: eth0
```

The sixth section analyze customize rule sets. In this section is set path for specific rules. These rules may be updated directly from the internet or may be created by administrator.

```
include $RULE_PATH/myrules.rules
include $Rule_path/attack.rules
```

### B. Suricata IDS engine

The Suricata engine is an open-source next generation intrusion detection and prevention system. It was developed by the Open Information Security Foundation [7].

One of the main features is automatic protocol detection. The engine can support keywords such as HTTP, FTP, TLS and SMB. This is going to malware detection and control.

The HTTP library is an HTTP normalizer and parser. This integrates and provides very advanced processing of HTTP streams for Suricata. The Suricata engine and the HTTP library are available under the GPLv2.

A Suricata engine use security oriented HTTP parser with HTTP library. There is support for special keywords such as http_body, http_raw_uri, http_header, etc. This library also supports compressed flows that could be decoded by gzip.

Flowint module allows storage and mathematical operations using variables. It operates with the addition of mathematical capabilities and the fact that an integer can be stored and manipulated.

It could be used the same rules for Suricata and for Snort, or we can create own rules. It can be used a new keyword for example:

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"HTTP GET method"; content:"GET"; sid:10000006;)
```

### IV. EXPERIMENTAL RESULTS FROM TESTING

For testing IDS exists a lot of commercial and open source tools. We tested a lot of open source tools. One of the best solution for penetration testing and security auditing is BackTrack linux distribution. This distribution can be used as live DVD or live USB. For our testing was used BackTrack 5 R3 release.

When we started attack, Snort IDS generated alert. Information contains this alert is saved in the file /var/log/snort/alert or it can be displayed on the screen.

```
TESTING NMAP
** [122:1:0] (portscan) TCP Portscan 
[Priority: 3]
```

```
11/16-11:28:58.849822 10.0.0.2 -> 100.0.0.10
PROTO:255 TTL:0 TOS:0x0 ID:0 IpLen:20 DgmLen:152
```

To generate some alert, Suricata detect HTTP GET method and show alert message on the screen.

```
TESTING SCAPY
```

```
To generate some alert, Suricata detect HTTP GET method and show alert message on the screen.
```

V. CONCLUSION

This paper presented our experiences with intrusion detection system. It was tested two IDS system. The first one was Snort project with own rules and with some modules to support anomaly-based method. The second one was Suricata engine with own rules to test some application protocols, such as HTTP. Suricata is better that support multicore hardware.

As penetration test was used distribution BackTrack with a lot of testing tools. The most used penetration tool was scapy that allow create any type of packet with support PHP scripting.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 218086 - project INDECT.

REFERENCES


Application of Erlang Formulas in Contact Center Environment

Erik Chromy, Tibor Misuth
Institute of Telecommunications, Faculty of Electrical Engineering and Information Technology
Slovak University of Technology Bratislava
Bratislava, Slovakia
chromy@ut.ifei.stuba.sk, misuth@ut.ifei.stuba.sk

Abstract—This paper deals with simulation of important parameters of the Call Center using the Erlang B and Erlang C formulas. Erlang B formula is basic mathematical model used for estimation of necessary access links capacity in contact centers. Erlang C formula is defined as a function of the number of agents N and the load A. On the basis of their values it is possible to determine the probability $P_B$, that the incoming call will not be served immediately, but it will have to wait in the waiting queue. Simulations satisfy the assumption of Markov models.

Keywords—contact center; QoS, Erlang B Formula, Erlang C formula

I. INTRODUCTION

Call Center is dynamical, technical system (hardware, software and human sources) designed for effective connecting people with the requirements for service with operator or with systems able to satisfy their requirements. The core of the Call Center is Automatic Call Distribution (ACD).

Each of the components of the ACD can be described with some precision by means of mathematical tools and causalities. Since the ACD systems process a large number of incoming requests, the majority of models is based on the principles of mathematical statistics. The right choice of a statistical model is able to ensure the sufficient accuracy of the results. It is essential to describe the dependency of input variables and parameters that can greatly affect the accuracy of the results. The modeling of Call Center parameters is possible through Markov models, but also through Erlang formulas.

This paper deals with simulation of important QoS [1], [2], [3], [4], [5] parameters of the Call Center and is organized in two main sections. Section 2 analyzes Erlang B formula and represents results obtained by simulations and Section 3 analyzes Erlang C formula and represents results obtained by simulations.

II. APPLICATION OF ERLANG B FORMULA IN CONTACT CENTER ENVIRONMENT

Erlang B formula is basic mathematical model used for estimation of necessary access links capacity in contact centers. Furthermore, it enables modeling of the extreme and not usual case of contact center implementation without waiting queue. Incomming calls are either assigned to a free agent or are blocked and not served in case of no free agent is available. The most important output parameter of the model is the probability of call blocking $P_B$. To avoid problems and accuracy issues when computing results for large contact centers (many agents, therefore division of two large numbers), all calculations are done using slightly modified algorithm [6].

$$P_B(N,A) = \frac{1}{1 + \sum_{k=1}^{N-1} \frac{N-k}{A}}$$

where $N$ is number of agents and $A$ is traffic load.

For a system without waiting queue it is also important to determine the mean number of requests in the system $K$ (i.e. mean number of occupied agents and links) and utilization of agents $\eta$ [7], [8], [9]:

$$K = A(1 - P_B)$$

$$\eta = \frac{K}{N} = \frac{A(1 - P_B)}{N}$$

A. Erlang B formula simulations

The whole process of simulation for Erlang B model is shown in the following Fig. 1.

B. Erlang B formula simulation results

The parameters of simulated model are:
- Incomming calls rate $\lambda = 667$ per hour,
- Mean call service time $1/\mu = 150$ seconds,
- Number of agents $N = 1.45$,
- Simulation time $T_{sim} = 30$ hours,
- time step of simulation $= 1$ second.
The trends of important simulation outputs in dependence on number of agents are shown on Fig. 2.

From value approx. $N = 25$ agent continual decreasing of agents utilization occurs. Mean number of requests $K$ is changing to the constant value near 28. It is exactly the value of load $A$ in Erlangs, for which the contact center is exposed by given input parameters.

III. APPLICATION OF ERLANG C FORMULA IN CONTACT CENTER ENVIRONMENT

Erlang C formula [10] works in the basic form with 3 input parameters: the number of agents $N$, the load $A$ and the probability $P_c$ (that the incoming call will not be served immediately, but it will have to wait in the waiting queue). Value of load $A$ (generated by incoming calls) is divided into 2 components: $\lambda$ and $1/\mu$. Erlang C formula thus works with 4 values, while 3 of them act as input parameters and the last parameter is the output parameter. By adding of the waiting queue we can obtain a set of new parameters that can be calculated and then compared with the simulation results:

- Average number of requests in the waiting queue $Q$

$$Q = \frac{\lambda W}{\mu(N - A)}$$

(4)

- Average number of requests in the call center $K$

$$K = N\eta + \frac{\eta}{1 - \eta} P_c = A + \frac{A}{(N - A)} P_c = A + Q,$$

(5)

- Average waiting time in the waiting queue $W$

$$W = \frac{P_c}{\mu(N - A)},$$

(6)

- Average time spent in the call center $T$

$$T = K = A + Q = 1 + W = \frac{1}{\mu} + \frac{P_c}{\mu(N - A)},$$

(7)

- Value of GoS (Grade of Service) for AWT (Acceptable Waiting Time) [7], [11] = 20 s

$$GoS = 1 - P_c \cdot e^{-\mu(N - A)AWT},$$

(8)
• Average utilization of agents \( \eta \)

\[
\eta = 1 - \frac{\sum_{k=0}^{N-1} \frac{N-k}{n \cdot k!} A^k}{\sum_{i=0}^{N-1} \frac{A^i}{i!} + \frac{A^N N}{N!(N-A)}}.
\]  

(9)

Probability of insertion into waiting queue \( P_C \) can be entered in three different variants

• Direct entry of value \( P_C \),

• Entry of average waiting time \( W \),

• Entry of GoS.

When using a \( P_C \) as input variable, this variable is considered to the upper limit.

A. Erlang C formula simulation results

The whole process of simulation for Erlang C model is shown in the following Fig. 3.

B. Erlang C formula simulation results

The parameters of simulated model are:

• Incoming calls rate \( \lambda = 667 \) per hour,

• Mean call service time \( 1/\mu = 150 \) seconds,

• Simulation time of the call center work is 30 hours with 1 second step (run to steady state is 1 hour).

The calls that can not be processed immediately are placed into the waiting queue (according to Erlang C formula). For the system stability it is necessary to satisfy the condition \( A < N \). Therefore the calculations and simulations are realized for the number of agents in the range of 28 to 37. In this range are the most notable changes observed in output parameters.

From the caller point of view, the most important parameters are the average waiting time in the waiting queue \( W \) and parameter GoS (this case is evaluated for \( AWT=20 \) seconds). The caller expects the lowest value of \( W \) and also the value GoS, which is close to 100%. From the call center point of view, the most important parameters are the number of agents \( N \) and their utilization \( \eta \), because these two variables significantly affect the financial demands of service. The aim of the operator is to minimize the number of agents and to maximize their utilization. The aim of the analysis is therefore to find such a minimum number of agents \( N \), when the operation parameters are yet on the sufficient level. As suitable we can consider the GoS parameter on level 80% and the average waiting time about 10 seconds.

The Fig. 4 shows the characteristic curve of the important call center simulation results according to Erlang C model assumptions in relation with the number of agents \( N \). The characteristic curve of the average waiting time has a very strong exponential character and thus a slight increase of the number of agent (about 1 to 2 agents) can bring a significant improvement of this parameter. A similar, even though less aggressive, is the characteristic curve of the probability \( P_C \).
GoS parameter also exponentially converges to the level 100% and we can see that a small change in the number of agents can bring significant improvement. The characteristic curve of agents load \( \eta \) is in the displayed range almost linear.

According to the above mentioned requirements on the provided quality of service by the call center is in this case possible to consider 32 agents as sufficient. By adding two agents it is possible to shorten the average waiting time by half and to increase the value of GoS parameter at 10% on very decent level (90%). The utilization of agents does not decrease below 80% and therefore it does not create unnecessarily long pauses, when the agents were redundant.

IV. CONCLUSION

The paper deals with the possibility of application of Erlang B and Erlang C formulas in contact center environment. Through the simulation it is possible to monitor important QoS parameters.

Disadvantage of Erlang B formula is absence of waiting queue. Therefore, the better alternative is usage of the Erlang C formula.

Based on calculations and simulations it can be stated, that in term of simplicity and accuracy of obtained results Erlang C formula is applicable for call center simulations. However, its shortness is the possibility of calculations only for one service group, and also the need to define for all agents the same service time.

For the purpose of further study it would be interesting to expand the simulations by more independent service groups at the same time and the random distribution of call between them according to defined probabilities. Another interesting possibility could be different average service time for individual agents. Finally there is possibility to simulate the impact of unequal performance of agents on the results of the whole call center.

ACKNOWLEDGMENT

This work is a part of research activities conducted at Slovak University of Technology Bratislava, Faculty of Electrical Engineering and Information Technology, Institute of Telecommunications, within the scope of the projects „Grant programme to support young researchers of STU - Modeling of Traffic in NGN Networks” and „Support of Center of Excellence for SMART Technologies, Systems and Services II., ITMS 26240120029, co-funded by the ERDF”.

REFERENCES


Simulation of 16-QAM and 64-QAM Demodulator into MATLAB/Simulink with Xilinx Toolkit

Miroslav Bureš, Jaroslav Zdrálek
Department of Telecommunications
VSB – Technical University of Ostrava
17. listopadu 15, 708 33 Ostrava, Czech Republic
miroslav.bures@vsb.cz, jaroslav.zdralek@vsb.cz

Abstract—This paper deals with the simulation and implementation 16-QAM and 64-QAM demodulator using the software tools "System Generator for DSP" from Xilinx and MATLAB-Simulink [1]. Simulation results were verified by the programmable elements in Field-programmable Gate Arrays (FPGAs)

Index Terms—16-QAM, 64-QAM, modulation, demodulation, Xilinx, OFDM, FPGA

I. INTRODUCTION

Nowadays, new-digital technologies bring a significant increase in the quality of transmission-information systems. This is particularly the truth in connection with Digital Video (DVB) and Audio (DAB, DRM) Broadcasting systems. All these systems use a digital modulation technique called Orthogonal Frequency Division Multiplexing (OFDM).

System OFDM uses a principle of frequency divided transmission channel. This division is made by hundreds of sub-carrier frequencies, which are further modulated by a multi-level modulation such as Quadrature Phase Shift Keying (QPSK) or M-Quadrature Amplitude Modulation (M-QAM). Thus the modulated signal is highly resistant to Inter-Symbol Interference (ISI) and Inter-Carrier Interferences (ICI), which are often caused by multi-path spread signal and the Doppler Effect.

On the receiving side, it is necessary to ensure a coherent demodulation. The main parameter, on which depends an overall Bit Error Rate (BER), is the precision of synchronization.

II. DIGITAL RADIO DRM

Digital Radio Mondiale (DRM) is a universal, worldwide open standard of digital radio, which was designed for low (LF), medium (MF) and High (HF) frequency bands. Currently available specification of DRM+ is designed to work at Very High Frequency (VHF) band [2].

A. DRM Specification

1) Source Coding: For source coding of input audio streams three basic codecs are used in DRM. Differences between codecs are mainly the quality of sound and bit rate. DRM uses a combination of Advanced Audio Coding (AAC), Code Excited Linear Prediction (CELP) and Harmonic Vector Excitation Coding (HVXC). AAC Codec provides the highest audio quality compared to CELP and HVXC, which reaches a lower quality and lower bit rate. AAC codec is used for standard audio coding. CELP and HVXC are used especially for encoding a spoken word. To increase the efficiency Spectral Band Replication (SBR) may be used [2].

2) Transmission Modes: A distorted receiving signal is caused in the radio channel by disturbing noise. The digital system DRM is equipped with mechanisms that ensure errorless signal decoding in order to overcome this signal distortion. Choosing an optimal combination of modulation type and coding rate is the goal how to ensure a signal reception in the maximal possible quality. These combinations are called Transmission Modes (Modes of robustness).

DRM system distinguishes four basic transmission modes. These schemes can have a large transfer rate and little robustness or, conversely, the lowest bit rate, but great robustness. A basic overview of transmission modes with the specific features of the OFDM signal is defined in Table I.

Parameter $T_s$ specifies the duration of the OFDM symbol, $T_g$ is duration of a Guard Interval (GI) and $T_u$ is the duration of useful (data) part of the OFDM symbol, i.e. without GI. $\Delta f$ is the distance between two sub-carriers waves and is given.
by following equation 1:

$$\Delta f = \frac{1}{T_u} \quad [Hz]$$  \hspace{1cm} (1)$$

where $T_u$ is the duration of the useful OFDM symbol part.

A broadcast signal is organized into Super Frames blocks. One Super Frame consists of three normal frames. Each frame contains $N_s$ OFDM symbols with symbol duration $T_f$. OFDM symbol contains data or synchronization information for the demodulation and decoding. The frame thus consists of the data, pilot and control signals.

<table>
<thead>
<tr>
<th>TABLE II: Partition of QAM symbols on di-bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>I,Q component</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>$a_0a_1a_2$</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>-1</td>
</tr>
<tr>
<td>-3</td>
</tr>
<tr>
<td>-5</td>
</tr>
<tr>
<td>-7</td>
</tr>
</tbody>
</table>

For the purpose of OFDM demodulation are substantial pilot signals that carry information about the frequency, time and frames synchronization. The receiver based on the knowledge of pilot signals is capable of carrying out equalization transmission channel and coherent demodulation. Pilot signals are evenly distributed across time and frequency domains [2].

III. THEORETICAL DESIGN OF OFDM DEMODULATOR IN THE DRM SYSTEM

Internal structure of DRM receiver can be divided into several basic logical blocks which include OFDM demodulator. The other units are the radio-frequency circuits, frame decoder, audio and data flow decoders. A simple block diagram can be seen in Fig. 1.

A block of M-QAM demodulator was chosen for the subsequent implementation. Furthermore, the functionality of this block was verified by simulations and then their implementation into FPGA.

IV. IMPLEMENTATION OF M-QAM DEMODULATOR IN THE ENVIRONMENT OF SYSTEM GENERATOR FOR DSP

A. M-QAM Modulation

Quadrature Amplitude Modulation is a multi-level modulation where the modulation signal affects the amplitude and phase of a carrier wave. This basic principle provides high spectral efficiency.

The modulation states of M-QAM modulation are composed of multiple n-bits groups which describe modulation symbols, where $M = 2^n$. Placement all the symbols then forms the constellation diagram. These symbols are then transmitted in the form of signal elements whose duration equals to a symbol’s period $T_s$.

M-QAM modulation is usually carried out by quadrature modulators also known as vector’s (IQ) modulator. A function of a quadrature modulator is based on the fact that any signal of constant $\omega_c$ angular frequency and arbitrary time variable phase $\Phi_c(t)$ and any time variable amplitude $U_c(t)$ is expressed in a usual form:

$$u(t) = U_c(t) \sin [\omega_c t + \Phi_c(t)]$$  \hspace{1cm} (2)$$

The same signal is also possible to compose of two components with the same frequency and with a constant mutual phase shift of 90 degrees (known as Quadrature Component) and the amplitude $I(t)$, $Q(t)$, i.e.

$$u(t) = I(t) \sin (\omega_c t) + Q(t) \cos (\omega_c t)$$  \hspace{1cm} (3)$$

M-QAM signals can be demodulated using a quadrature demodulator, whose function is essentially inverse function to the modulator [3].

B. Realization of 16-QAM and 64-QAM Demodulator

The diagrams in Fig. 2, 3 implements a 16-QAM and 64-QAM demodulator shown in Table II. The entire circuit implements demodulation on the principle of finding the minimal Euclidean distance of each sample in an ideal constellation diagram. The principle consists in assigning position and its subsequent transfer to the group di-bit using encoder. Subsequently di-bits I and Q components are composed into a serial data output in meaning of a demodulated data [4].

Fig. 4 shows the block of simulation involvement. Randomly generated input vector is mapped by QAM modulator and then transmitted over the Additive White Gaussian Noise.
Fig. 4: Simulation diagram of M-QAM demodulator

(AWGN) channel with variable value of the Signal to Noise Ratio (SNR).

Demodulated signal is then compared with the broadcast signal and the calculated value of BER.

V. IMPLEMENTATION OF SELECTED BLOCKS

After simulation and functionality verification was generated VHSIC Hardware Description Language (VHDL) code for both units and then synthesized and implemented into Xilinx ISE development environment. For implementation was chosen chip from product line Spartan3E.

After synthesis and subsequent mapping of the hardware structure (this is known as the Place&Route) found the overall use of the circuit. Figure 5 shows the core of the circuit with the placement and interconnection of the internal structures.

(a) 16-QAM

(b) 64-QAM

Fig. 5: Layout of blocks on a chip

VI. CONCLUSION

The aim of this article is to determine the suitability of software “System Generator for DSP design” and implementation of OFDM demodulator blocks. System Design using MATLAB-Simulink and then generating the VHDL code is very efficient. The advantage is especially high efficiency of the proposal in terms of total time spent implementing and debugging the resulting application. Another significant advantage is verification of the circuit design by simulation using standard components. Using this kind of implementation brings advanced development of hardware receivers of digital radio into common practice. The new development will provide a massive series production and the price reduction, which is currently now very high.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Community’s Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 218086 - project INDECT.

REFERENCES


Advantages of Audio Signal Separation to Tonal and Noise Parts for LP modeling

Ondrej Raso
Department of Telecommunications
Brno University of Technology, FEEC
Brno, Czech Republic
raso@feec.vutbr.cz

Miroslav Balik, Zdenek Martinasek
Department of Telecommunications
Brno University of Technology, FEEC
Brno, Czech Republic
balik@feec.vutbr.cz, martinasek@feec.vutbr.cz

Abstract—In this article, advantages of audio signal separation to tonal and noise parts for linear predictive modeling is shortly described. These advantages lay in the possibility to modulated separately each parts instead of modeling the whole signal.

Keywords: Audio Signals; Digital Signal Processing; Digital Filters; Linear Prediction Model; Frame theory

I. INTRODUCTION

Linear prediction modeling is used in a wide area of applications. For example: speech coding, model based spectral analysis, signal restoration, video coding, interpolation, etc. [2].

Linear prediction can in a certain conditions describe model based power spectrum estimation of analyzed signal. The advantage of the model based, or sometimes called parametric methods, spectrum estimation is the fact that it should reach better resolution than the standard non parametric power spectrum estimations like periodogram, modified periodogram or Blackman - Tukey method etc. The better resolution of parametric methods is related with inherent extrapolation of autocorrelation function [3]. A disadvantage of the parametric method is the frequency resolution decrease with the increasing level of wideband noise [3].

The model based approach of power spectral estimation is often used in objective method for speech quality assessment, for example: Itakura and Itakura – Saito measures [4], Musical signal distortion [4], Spectral distances (linear, nonlinear, log – spectral), cepstral distance, log-area ratio distance [5] etc.

But usage of the linear predicton in objective method for quality assessment in general audio, mainly music or singing, signal is not common. For example, the standard Perceptual Evaluation of Audio Quality (PEAQ) [6] incorporates 7 models: Disturbance Index [7], Noise-to-Masked-Ratio [8], Objective Audio Signal Evaluation [9] and others [6]. None of these incorporated models do not use any form of linear prediction. This happens for several reasons.

One of these reasons is the fact that power density spectra of musical signals are more different than power density spectra of speech signals. Musical instruments reach higher dynamic, they have greater frequency range and they are more non stationary than speech signal [10]. The signal with length of 10 ms is usually considered as stationary signal in the case of speech signal, but this does not apply to musical signals [11].

Next, a model of creation of musical signal like in the case of speech signal cannot be conclusively described. There is usually only one acoustic source (in a case of one speaker) and they are speech organs of human. These human speech organs should be modeled by an input signal and a modulating filter. The input signal is the excitation signal from the lungs and vocal cords. And the modulating filter is trying to modulated the excitation signal as it modulates system of the oral cavity vocal tract.

The situation is considerably more complicated for musical signal. The music has usually more than one acoustic source and these acoustic sources are from different musical instruments or singing. Hence, the musical signal cannot be modeled in the similar way like speech signals.

But even if the musical signal cannot be modeled in this way, we can estimate its spectrum like any other signal by parametric methods. The problem arises when we have to determine the order of this LP model. Too low order cannot describe the rapid changes in the spectrum and too high order follows a stochastic nature of the analyzed signal, the spectrum is so much variable. Hence, we have to choose “optimal” order in some sense. For speech signal we can estimate the order from the model of creation of speech signal, but for musical signal we have to estimate it by some other way.

One way how the optimal LP order could be experimentally determined was published in [13][14]. This article will topically follow mentioned publications and it focuses on the experimental determination of LP order for so called “tonal” and “noise” part of musical signal. [The differences between LP order of the tonal and noise part will by statistically analyzed. It will be examined if the differences in LP orders are statically significant. We believe that the differences are statistically significant and the tonal parts will reach higher values of LP orders than the values of LP orders of noise parts.]

Recently, a transformation based on frame theory
which can separated tonal part from analyzed signal was introduced. Namely constant-Q nonstationary Gabor transform (CQ-NSQT) [15] which is based on nonstationary Gabor transform (NSQT) and constant Q-transform (CQT).

Furthermore, there is module Deconstruct from audio software iZotope RX™ 2 [1] for separation audio signal to the tonal and noise part.

The separation to tonal and noise part is very useful for audio LP modeling. The both part can be modeled separately or only the noise part could be modeled and it can be done in an easier way. It will be shown in this article that the LP orders reach higher value for tonal signal part than for case of noise signal part.

II. SEPARATION TO TONAL AND NOISE PARTS

The Deconstruct module from audio software iZotope RX™ 2 [1] will be used for the separation to the tonal and the noise parts. Tested signals will be divided into 3 groups and these groups will be called as original signal group, tonal part and noise part. An example of the separation is shown in spectrograms in Figures 1 and 2. Firstly, the spectrogram of Mozart original record signal is shown and in the second figure the spectrogram of the tonal part of Mozart record signal is shown. In the spectrogram of tonal part, clear harmonic structures can be seen by a comparison of spectrogram of original signal.

Fig. 1: Spectrogram of Mozart original record signal.

Fig. 2: Spectrogram of the tonal part of Mozart record signal.

III. CONCLUSION

In this article, advantages of audio signal separation to tonal and noise parts for linear predictive modeling were shortly described.

ACKNOWLEDGMENT

This research was supported by the grant OP VK No. CZ.1.07/2.2.00/28.0062, Joint activities of BUT and TUO while creating the content of accredited technical courses in ICT.

REFERENCES

Admission Control Methods and Quality of Service

Erik Chromy, Matus Weber and Tomas Behul
Institute of Telecommunications, Faculty of Electrical Engineering and Information Technology
Slovak University of Technology Bratislava
Bratislava, Slovakia

Abstract—Today great attention is dedicated to Quality of Service in IP network. This paper deals with problematic of Admission Control methods and Quality of Service. Admission Control methods are divided into two main groups - parameter based and measurement based Admission Control methods. Admission Control algorithms are analyzed and also simulated in NS-2 environment. Simulation results compare bandwidth, loss rate and link load of individual algorithms for VoIP, constant bitrate video and FTP services.

Keywords-quality of service; admission control method; PBAC; MBAC

I. INTRODUCTION

Many network control mechanisms exist nowadays. These mechanisms prevent network traffic congestion, provide network resources to services and also ensure adequate QoS for users. Admission control methods used in simulations are analyzed further in this article. Functionality of methods was verified and compared through simulations done in network simulator NS-2. For algorithm comparison and observation of service relations, were realized 4 scenarios.

In each scenario were tested and compared algorithms Admission Control Tangent at Origin (ACTO), Hoeffding Bounds (HB), Predicted Sum (PS) and Parameter Based Admission Control (PBAC) method. Our goal was to compare individual algorithm for given type of service (VoIP, FTP and CBR video) and to find out which one is suitable.

II. ADMISSION CONTROL MECHANISMS

Main idea of Admission Control (AC) methods leans on the fact that request for connection won’t be accepted until QoS is ensured. Method, which controls admission, has to respect existing connections in the network and has to ensure requested QoS that these connections had in previous time.

AC mechanisms prevent network congestion. Main QoS [1], [2], [3], [4], [5], [6] condition for AC methods is to ensure needed bandwidth, so that new flow can be connected through network.

A. Parameter based admission control

Parameter Based Admission Control (PBAC) method is used mainly in ATM (Asynchronous Transfer Mode) networks and in other packet networks. When user requests connection establishment, this AC method performs the functions based on desired traffic parameters (peak cell rate, sustainable cell rate and burstiness). But great memory consumption is needed for storing of traffic parameters and state of every connection settings in every network node. If this method is used in large IP networks, this gives rise to substantial restrictions on the scalability, because the amount of status information and operational parameters increases with the number of connections [7], [8].

PBAC estimates needed bandwidth based on Gauss distribution. Equation (1) defines estimation method of needed bandwidth [9]:

\[ C = m + a'\sigma, \]

where:

\[ a' = \sqrt{\frac{-2\ln(\varepsilon)}{\ln(2\pi)}}, \]

and:

\[ C \text{ is bandwidth [kbit/s], } m \text{ is average value of bandwidth [kbit/s], } \sigma \text{ is standard variation of bandwidth [kbit/s] and } \varepsilon \text{ is upper limit of probability of overload [%].} \]

B. Measurement based admission control

MBAC algorithms are based on measurement of delay, jitter, loss and network load. New flow is accepted under this condition [10]:

\[ n + b \leq a, \]

where:

\[ a \text{ is total available bandwidth [kbit/s], } b \text{ is load during last measured interval [kbit/s] and } n \text{ is bandwidth requested by new reservation [kbit/s].} \]

MBAC methods are realized through MBAC algorithms.

1) Hoeffding bound (HB)

New flow is accepted if sum of peak bandwidth of new flow and measured bandwidth is smaller than link load. Bandwidth is calculated by equation:
Flow α is accepted under condition:
\[ \hat{C}_H + p^\alpha \leq \mu , \]
where:
\[ \nu \] is measured bandwidth of incoming flow [kbit/s], \( p^\alpha \) is peak bandwidth of flow α [kbit/s], \( \mu \) is link bandwidth [kbit/s], \( p_i \) is peak bandwidth from \( N \) sources [kbit/s] and \( \varepsilon \) is probability of packet loss [%].

Advantage of this method is the prediction of incoming flow bandwidth from average bandwidth of incoming flow.

2) Admission control tangent at origin (ACTO)
Algorithm accepts new flow under following condition [10]:
\[ e^{\beta^p} \hat{\nu} \leq \mu . \]
where:
\[ p \] is peak bandwidth of flow [kbit/s], \( s \) is space parameter of Chernoff’s limitation (0<\( s <1 \)), \( \hat{\nu} \) is estimation of actual load and \( \mu \) is bandwidth [kbit/s].

Advantage of this method leans on increasing of link load and lowering packet loss. This method does not need to know number of sources in network.

3) Predicted sum (PS)
Algorithm samples traffic load in certain intervals. After each sample a prediction of next period traffic load is stated by on-line traffic predictor. This prediction of next sample period is then used for determination of flow acceptance. PS accepts new flow based on condition [11]:
\[ x(n+1) + r_a \leq \eta C , \]
where:
\[ x(n+1) \] is predicted traffic load of next sample period \( n+1 \) [kbit/s], \( r_a \) is peak bandwidth (or bandwidth of tokens [kbit/s], \( C \) is bandwidth [kbit/s] and \( \eta \) is link load parameter [%].

Advantage of this method leans on stability of this method under network conditions, it also enables exact network load control and setting of QoS.

III. SIMULATIONS

For simulations were designed a simulation model (Fig. 1). The goal was to compare efficiency and to find out most effective method. AC algorithm efficiency was evaluated based on actual link load, packet loss and accuracy of link bandwidth allocation. Simulations were realized in network simulator NS-2. Simulation model is a simple topology interconnected with 5 Mbit/s bandwidth link. Topology is an example of access network, where traffic aggregation occurs. In node 0 were monitored changes and this point was overloaded. Parameters at node 0 output were monitored: bandwidth, packet loss and link load. At node 0 individual algorithms were applied. Simulation took 3000 seconds. Through sequence aggregation of traffic, transient effects occur. After 1500 seconds each method starts to process the data.

For simulations were used three data flows. First flow was VoIP traffic. For VoIP traffic were used exponential on/off source. Second flow was constant bitrate video (CBR), running on UDP protocol. Last one was standard FTP traffic. For FTP we used Pareto’s on/off source. List of used parameters is concluded in Tab. I [12].

<table>
<thead>
<tr>
<th>source type</th>
<th>protocol</th>
<th>bit rate [kbit/s]</th>
<th>packet size [bit]</th>
<th>flow length [packets]</th>
<th>on/off [ms]</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP Exp</td>
<td>UDP</td>
<td>64</td>
<td>1000</td>
<td>160</td>
<td>312.5/325</td>
</tr>
<tr>
<td>video - CBR</td>
<td>UDP</td>
<td>2000</td>
<td>12000</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>FTP - Pareto</td>
<td>TCP</td>
<td>1000</td>
<td>12000</td>
<td>160</td>
<td>500/1000</td>
</tr>
</tbody>
</table>

In individual scenarios were tested and compared algorithms: ACTO, HB, PS and PBAC for assigned services (Tab. II). Algorithms were compared based on prediction of bandwidth, packet loss and link load.

<table>
<thead>
<tr>
<th>scenario</th>
<th>service</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VoIP</td>
</tr>
<tr>
<td>2</td>
<td>Video</td>
</tr>
<tr>
<td>3</td>
<td>FTP</td>
</tr>
</tbody>
</table>
A. Scenario 1

In scenario 1, algorithms were tested with VoIP traffic. Results of bandwidth prediction are shown on Fig. 2.

Figure 2. Simulation of AC algorithms with VoIP service

From the graphs we can see that the best bandwidth prediction made ACTO algorithm. Differences between predicted bandwidth and actual allocated bandwidth are minimal. ACTO algorithm can predict traffic load more accurately and carefully monitors system state. HB algorithm acted more conservatively, predicted smaller bandwidth and didn’t follow exact traffic fluctuations. PS algorithm was more effective and reached better results than HB algorithm. PBAC algorithm showed still the same allocated bandwidth, so this algorithm has low flexibility. The reason why this occurs could be the fact, that this algorithm does not change parameters for AC during transfer. Results for Scenario 1 are listed in Tab. III, packet loss and link load with VoIP service are shown.

TABLE III. PACKET LOSS AND LINK LOAD WITH VOIP

<table>
<thead>
<tr>
<th>algorithm</th>
<th>packet loss [%]</th>
<th>link load [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTO</td>
<td>0</td>
<td>90.98</td>
</tr>
<tr>
<td>HB</td>
<td>2.88E-04</td>
<td>87.26</td>
</tr>
<tr>
<td>PS</td>
<td>0</td>
<td>89.73</td>
</tr>
<tr>
<td>PBAC</td>
<td>2.59E-04</td>
<td>70.34</td>
</tr>
</tbody>
</table>

These results reveal that ACTO, HB and PS algorithms allow high network load with low packet loss. Because of the same level of allocated capacity and low flexibility of PBAC method, link load dropped down to 70.34 %. Best for VoIP traffic seems to be ACTO algorithm.

B. Scenario 2

In scenario 2, algorithms were tested with Video (CBR) service. Fig. 3 shows results for bandwidth allocation of selected algorithms.

Figure 3. Simulation of AC algorithms with video service

From the graphs it’s evident that all 4 algorithms provided almost the same bandwidth prediction with video service. Differences were minimal. Simulation has almost no fluctuations, because we used CBR video (no exponential nor Paret’s on/off source). In Tab. IV, packet loss and link load are shown.

TABLE IV. PACKET LOSS AND LINK LOAD WITH CBR VIDEO SERVICE

<table>
<thead>
<tr>
<th>algorithm</th>
<th>packet loss [%]</th>
<th>link load [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTO</td>
<td>0</td>
<td>41.47</td>
</tr>
<tr>
<td>HB</td>
<td>0</td>
<td>41.36</td>
</tr>
<tr>
<td>PS</td>
<td>0</td>
<td>41.81</td>
</tr>
<tr>
<td>PBAC</td>
<td>0</td>
<td>41.97</td>
</tr>
</tbody>
</table>

Simulations showed that ACTO, HB, PS and PBAC algorithms provide similar link load and zero loss with CBR video. The video source generated only 2 Mbit/s and link capacity was 5 Mbit/s, so at node 0 the loss was zero. Best link load had PBAC algorithm. PBAC does not change parameters and has low flexibility (level of allocated bandwidth is still the same), thus it suits best for traffic with constant bit rate.

C. Scenario 3

In scenario 3, algorithms were tested only with FTP traffic. In Fig. 4 results for bandwidth allocation are shown.

Figure 4. Simulation of AC algorithms with FTP service

We can see that HB algorithm provided conservative prediction (it predicted smaller bandwidth and did not follow fluctuations exactly), its prediction was better than other algorithms. Upper limit of allocated bandwidth on PS method was higher than with other methods. ACTO and PBAC
methods allocated lower bandwidth than actual bandwidth was. This effect can lead to packet delay. In Tab. V, loss and link load is listed.

<table>
<thead>
<tr>
<th>algorithm</th>
<th>packet loss [%]</th>
<th>link load [%]</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACTO</td>
<td>9.38E-05</td>
<td>77.02</td>
</tr>
<tr>
<td>HB</td>
<td>1.13E-04</td>
<td>92.67</td>
</tr>
<tr>
<td>PS</td>
<td>1.00E-04</td>
<td>81.11</td>
</tr>
<tr>
<td>PBAC</td>
<td>8.25E-05</td>
<td>68.48</td>
</tr>
</tbody>
</table>

Lower limit of prediction in case of ACTO and PBAC leads to unacceptance of new flow request. Results shows that for FTP service HB algorithm is suitable.

**D. Scenario 4**

Scenario 4 analyzes bandwidth allocation with combined traffic: VoIP, video and FTP together. Fig. 5 shows results for bandwidth prediction. Again, we explored accuracy of bandwidth allocation, loss and link load.

![Figure 5](image_url) Simulations of AC algorithms with VoIP, video and FTP services

Best prediction of bandwidth provided ACTO method. Differences between predicted bandwidth and actual allocated bandwidth are minimal. ACTO algorithm responds very quickly on actual fluctuations during data transfer. Compared to the first three scenarios, when bandwidth was allocated only to one service, we can see minor change in transfer speed, because traffic is more bursted. All three services compete for network resources. Upper limit of allocated bandwidth was higher than actual bandwidth with PS and HB methods. PBAC method reached 4.3 Mbit/s bandwidth. Results for Scenario 4 are listed in Tab. VI.

Prioritization of VoIP service, that had highest priority, lead to suppression of video and FTP flow. Results show that for this scenario, ACTO is suitable method (considering all three monitored parameters). Comparable good results provided also PS algorithm, but it predicted higher level of bandwidth allocation, and that would mean ineffective usage of network resources.

**IV. COMPARISON OF AC METHODS**

Considering all three examined parameters: accuracy of bandwidth allocation, packet loss and link load, for each scenario, one best suitable method was chosen (Tab. VII).

<table>
<thead>
<tr>
<th>scenario</th>
<th>service</th>
<th>algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>VoIP</td>
<td>ACTO</td>
</tr>
<tr>
<td>2</td>
<td>video (CBR)</td>
<td>PBAC</td>
</tr>
<tr>
<td>3</td>
<td>FTP</td>
<td>HB</td>
</tr>
<tr>
<td>4</td>
<td>VoIP, video, FTP</td>
<td>ACTO</td>
</tr>
</tbody>
</table>

**V. CONCLUSION**

Today great attention is dedicated to Quality of Service in IP network. This paper includes analysis and simulations of the following AC algorithms: ACTO, HB, PS and PBAC with VoIP, video (CBR) and FTP services. Simulations were realized for 4 scenarios (different combinations of services) in NS-2 environment. Our goal was to compare individual algorithms by achieved parameter levels: link load, packet loss and allocation of bandwidth. Accuracy of bandwidth prediction (allocation) leant on differences between needed bandwidth and predicted bandwidth.

Based on the simulation results we can say follows:

- for the network with VoIP traffic is the most suitable MBAC algorithm ACTP,
- for the network with video CBR traffic is the most suitable PBAC method,
- for the network with FTP traffic is the most suitable MBAC algorithm HB,
- for the network with combined traffic VoIP, video CBR and FTP is most suitable MBAC algorithm ACTO.

**ACKNOWLEDGMENT**

This work is a part of research activities conducted at Slovak University of Technology Bratislava, Faculty of Electrical Engineering and Information Technology, Institute of Telecommunications, within the scope of the projects „Grant programme to support young researchers of STU - Modeling of
Traffic in NGN Networks” and „Support of Center of Excellence for SMART Technologies, Systems and Services II., ITMS 26240120029, co-funded by the ERDF.

REFERENCES


Development of the Course
Radio-Communication Engineering

Marek Dvorsky, Martin Tomis
Department of Telecommunications
VSB Technical University of Ostrava
Ostrava, Czech Republic
marek.dvorsky@vsb.cz

Abstract—The project aims to create a new teaching support of the course “Radio-Communication Engineering”, that is an optional subject of the bachelor study program Information and Communication Technology, Mobile Technology, Telecommunication Engineering and Computational Mathematics. The second aim of the project is the creation of new laboratory guides.

Keywords- Radio-Communication Engineering; laboratory; measurement; guide.

I. INTRODUCTION

There is currently no support for teaching the new subject Radio-Communication Engineering (RCE). The newly created course RCE promotes and expands student’s overview in elective courses Radio Cellular Networks (RCN) and Radio Networks (RN). The Department of Telecommunications (DoT) currently offer the subject in Radio Networks in the third year of undergraduate study and the subject of Radio Cellular Networks in the first year of graduate studies. Practical teaching of this subject runs in a Radio Network Laboratory (RNL), which has a capacity of 10 students.

II. MAIN AIMS

The main aim of the project is to create new teaching materials with regard to new trends in radio communications. It was created five new laboratory measurements, as well as new processing contents of 14 exercises. It was also created 14 new teaching lectures that are available to students in electronic form (PDF) via e-learning system Moodle. [2]

III. METHODS OF SOLUTION

To ensure new laboratory exercises it was necessary to purchase some new equipment. It was bought equipment for measuring various parameters of the radio receivers (wild-band receiver WINRADIO [4], power meter, antenna analyzers, various types of antennas, interference analyzer software, etc.). After buying the equipment it was developed five new instructions for laboratory exercises. It was also created a new e-learning course in system Moodle.

IV. SPECIFIC OUTPUTS

A. Teaching materials

The main aim of the project is to create new teaching materials regarding to new trends in radio communications. RCE course contents:

- Introduction to radio communications.
- Basic concepts, variables used in radio communication, spectrum allocation.
- Radio waves in free space, the main types of radio waves, radio waves propagation.
- The base scheme of radio communication, signal processing.
- Source encoding, codec, radio channel.
- Analog modulation.
- Digital modulation.
- Antennas I - principles, basic characteristics.
- Antennas II - basic types, properties and construction.
- Antennas III - special types, antennae, EH antenna, magnetic antenna.
- OK2KQM HAM VSB.
- Radiolocation systems, radar, principles.
- Digital radio and television broadcasting.
- Receivers - basic block diagrams, software radio.
- There was no extra spending from grand budget to create theoretical part of the project.

B. 5 new laboratory measurements

- Measurement of coaxial cable parameters. There were purchased some samples of coaxial cables, Grid Dip Metter (GDO) and a power-probe to realize this measurement. The GDO and power-probe were bought from different financial source (Fig.1).
- Measurement of receiver noise factor. There were purchased a short-wave receiver and True-RMS voltmeter to realize this measurement (Fig. 2).

- Input antenna impedance. There were purchased some short-wave antennas and antennas analyzer AA520 to realize this measurement. [3]

- Directional characteristics of unknown antenna. There were purchased a short-wave receiver and True-RMS voltmeter to realize this measurement.

- WiFi Spectrum. There was purchased a WiFi analyzer WIFI-PILOT to realize this measurement (Fig. 3).

Figure 1. I. measurement working-place

Figure 2. II. Measurement working-place

Figure 3. V. Measurement working-place

V. CONCLUSION

There were developed five new laboratory measurements and fourteen theoretical lessons of the new course Radio-Communication Engineering. This helps to bring a maximum efficiency and autonomy of teaching each of the students. Acquisition of RNL Laboratory Equipment in RCE is also usable for courses Cellular Radio Networks and Telecommunications Networks.

ACKNOWLEDGEMENT

This project was funded by OP VK ‘Joint activities of VUT and TUO while creating the content of accredited technical courses in ICT’ CZ.1.07/2.2.00/28.0062 [1]

REFERENCES


Innovation of Laboratory Exercises in Subject "Data Networks"

Pavel Bezpalec
Department of Telecommunication Engineering, Czech Technical University in Prague, Faculty of Electrical Engineering
Technicka 2, 166 27 Praha 6, Czech Republic
Email: bezpalec@fel.cvut.cz

Abstract—This paper informs about project of innovation educational process in subject "Data Networks" in practical laboratory exercises as well as in theoretical lectures. For a graduate in our profession it is important to gain not only theoretical foundation through education, but also an adequate practical proficiency.

Keywords—teaching; laboratory exercise; testing; analysis

I. INTRODUCTION

Subject A2B32DAT – Data Networks is a required course taught in the third semester of bachelor study program CME (Communication, Multimedia and Electronics) in field of communication technique at the Czech Technical University in Prague.

The course introduces students to the basics of communication in a variety of data networks. The aim of the course is to provide a more comprehensive view of communication protocol for specific types most commonly used data networks according to the RM-layer OSI model. The course also allows students to look into ways of communicating with TCP/IP in the Internet, including the possibility of a practical realization of the data network in laboratory conditions using real equipment.

The project is primarily targeted to upgrading laboratory equipment to follow the modern technical trends in the field of network infrastructure and to innovating practically oriented laboratory tasks.

II. INNOVATION OF PRACTICAL COURSES

Main work has been done in innovation of practical laboratory exercises. Hereafter there is refreshed practical courses syllabus that contains and five totally rebuild practical tasks.

| Task 1 | Realization and testing of structure cabling system |
| Task 2 | PoE switch – configuration, measuring, testing |
| Task 3 | Large data network – routing within AS |
| Task 4 | Small data network – connection to Internet via ADSL router |
| Task 5 | E-mail – configuration and protocol analysis |

A. Innovation of theoretical workshops and individual work

The number of theoretical workshops has been reduced to two and consist of segment of theory and segment of simulation presentation. Simulation should enrich educational process with demonstration of behavior theoretically known methods and principles.

Simulations are mainly in a manner of

- basic principles of communications in data network
- IPv4 and IPv6 packet and message formatting
- call flow and message interchange in network behaviour
- mechanism of power initiation used by PoE
- principles and procedures for e-mail transport
- principles of DNS searching

All simulations are done by multimedia presentation.

Next, new individual work has been added. Within this individual work students design, develop, realize and test real speech enabled IVR (Interactive Voice Response) system based on VoiceXML integrated development tool created by RDC (Research and Development Centre) at CTU in Prague in conjunction with our department. For realization students use Speech IVR system technology with IBM Voice Enabler software for speech recognition and synthesis running on strong server farm.

B. Innovation of practical tasks

All input study materials for practical tasks have been innovated and transformed into Internet—ready form and then published to server that belongs to our department (www.comtel.cz → Předměty → A2B32DAT → Materiály pro výuku) and therefore are anytime easily accessible not only by our students.

Innovation of Task 1 – material and tools to successful task realization (cables, connectors …) has been bought, repaired and/or re-measured.
Innovation of Task 2 – new Power-over-Ethernet devices has been bought, namely PoE switch, IP telephone, WiFi Access point and small PoE camera for each laboratory group.

Innovation of Task 4 – new laboratory ADSL DSLAM as well as 5 ADSL router modules have been bought. Now VoIP terminal endpoints supporting H.323 signaling and software for detailed and educational analysis of signaling messages exchange has been bought.

New server with storage farm has been bought, on that all supporting servers for practical Task 5 (i.e. SMTP server, POP server, DNS server …) has been migrated as virtual servers running in virtualized behaviour. This new server with storage farm is physically located in special room outside of student’s laboratory.

III. INNOVATION OF THEORETICAL LECTURES

The revised basic of telco knowledge that has been deeply studied has extended a spectrum of lectures. Mainly English written literature has been translated into new lecture base that is in form of MS PowerPoint presentation. This chosen format is able to show new concepts with animated explanation. This is more didactical. An electronic form of these new lectures has been exported to pdf format and then placed on Internet (www.comtel.cz → Předměty → A2B32DAT → Materiály pro výuku) from where are easily accessible by students.

IV. CONCLUSION

Main goals of subject innovation are:

- New knowledge implementation.
- New simulation implementation in theoretical workshops.
- New server with storage farm supporting laboratory tasks as well as students projects.
- Workplace innovation for practical tasks.
- Practical tasks optimization and material, tools and device complementation.
- New study material creation for theoretical parts of course.
- All study material is now in electronic form of presentation.
- Motivation of students to study modern telco technologies.

V. ACKNOWLEDGEMENT

This research has been supported by FRVS grants No FRV 27/2012/F1a.
Inovace laboratorních cvičení předmětu
Kódy a bezpečnost

Tomáš Vaněk
Katedra telekomunikační techniky
České Vysoké Učení Technické v Praze
Praha, Česká Republika
tomas.vanek@fel.cvut.cz

Abstract— Projekt "Inovace laboratorních cvičení předmětu Kódy a bezpečnost" se zabývá modernizací a zefektivnění výuky stejnojmenného předmětu. Cílem projektu je inovace přednášek a doplnění a rozšíření laboratorní části cvičení. Inovace předmětu je zaměřena převážně na modernizaci stávajících a vytvoření nových praktických laboratorních úloh, tak aby lépe pokrývaly současné trendy v oblasti informační bezpečnosti. Hlavními cíli řešení je zvýšení efektivity studia formou zvýšení počtu laboratorních úloh, inovace přednášek o aktuální tématu z oblasti informační bezpečnosti a zlepšení podmínek pro online testování znalostí studentů.

Keywords-výuka, inovace, bezpečnost, protokol, cvičení, přednášky, kryptologie

I. ÚVOD

Předmět Kódy a bezpečnost je povinným předmětem programu STM (Softwarové technologie a management) bakalářského studijního programu elektrotechnické fakulty ČVUT v Praze. Předmět vznikl transformací X36BEZ předcházející formy studia. Základním cílem předmětu "Kódy a bezpečnost" je seznámit studenty s problematikou informační bezpečnosti. Jde o velmi důležitou dynamicky se rozvíjející oblast informačních technologií, jejíž význam se neustále narůstá. Inovace předmětu bude sledovat aktuální metody a systémy ochrany dat a snažit se je vysvětlit pomocí moderních učebních postupů. Hlavním nedostatkem cvičení je malé množství praktických laboratorních úloh, kde by se studenti mohli seznámit s praktickými aspecty bezpečnosti v oblasti informační bezpečnosti.

II. CÍLE ŘEŠENÍ

Cílem řešeného projektu je odstranit výše zmíněné nedostatky současného stavu, kdy obsah předmětu v některých částech neodpovídá moderním trendům v oblasti informační bezpečnosti. Globálním cílem je zatrativnění výuky a celkové modernizace předmětu. Jednotlivými dílčími cíly jsou:

- modernizace stávajících přednášek a jejich doplnění o aktuální tématu z oblasti informační a komunikační bezpečnosti
- zatrativnění přednášek pro studenty díky novým témátum a výukovým animacím
- zatrativnění cvičení pro studenty díky novým laboratorním úlohám
- vytvoření dvou nových laboratorních úloh.

Pro úlohy budou vytvořeny nově výukové materiály.

III. INOVACE PŘEDNÁŠEK

V Tabulce 1 a 2 jsou původní osnovy přednášek a cvičení předmětu Kódy a bezpečnost. Z osnovy jsou vidět hlavní nedostatky stávajícího řešení, kdy v přednáškách jsou zcela nejrůznější kryptografické protokoly jako IPsec, SSL/TLS, problematika zabezpečení hovorů v mobilních sítích elektronický podpis apod. V oblasti přednášek je možné vypustit partie týkající se modulární aritmetiky, protože ty jsou nyní probírány v samostatném předmětu Matematika pro informatiky (kód A7B01MCS).

<table>
<thead>
<tr>
<th>Tyden</th>
<th>Nápisy přednášek</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Úvod do kryptologie, historický přehled. Základy modulární aritmetiky,</td>
</tr>
<tr>
<td>2.</td>
<td>Základy teorie čísel, matematické základy kryptografie, substituční šifry</td>
</tr>
<tr>
<td>3.</td>
<td>Blokové, transpoziční a exponenciální šifry, zřízení společného klíče</td>
</tr>
<tr>
<td>4.</td>
<td>Teorie informace, teorie složitosti algoritmů</td>
</tr>
<tr>
<td>5.</td>
<td>Hašovací funkcí, MD5, SHA-x, HMAC</td>
</tr>
<tr>
<td>6.</td>
<td>Testy prvočíselnosti, proudové šifry, RC4</td>
</tr>
<tr>
<td>7.</td>
<td>Blokové šifry, DES, 3DES, AES, operační mody</td>
</tr>
<tr>
<td>8.</td>
<td>Asymetrická kryptografie 1</td>
</tr>
<tr>
<td>9.</td>
<td>Asymetrická kryptografie 2</td>
</tr>
<tr>
<td>10.</td>
<td>Sdílení tajemství</td>
</tr>
<tr>
<td>11.</td>
<td>Seznámení s kvantovou kryptologií</td>
</tr>
<tr>
<td>12.</td>
<td>Seznámení s kryptoanalýzou</td>
</tr>
<tr>
<td>13.</td>
<td>Kryptografie elliptických křivek</td>
</tr>
</tbody>
</table>
Změny v osnovách přednášek a cvičení jsou vyznačeny tučně. Navrhované změny budou zavedeny do výuky v letním semestru akademického školního roku 2011/12.

Tabulka 2 – Osnova inovovaných přednášek

<table>
<thead>
<tr>
<th>Týden</th>
<th>Náplň přednášky</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Úvod do kryptologie, historický přehled</td>
</tr>
<tr>
<td>2.</td>
<td>Základy teorie čísel, matematické základy kryptografie, substituční šifry</td>
</tr>
<tr>
<td>3.</td>
<td>Blokové, transpoziční a exponenciální šifry, zřízení společného klíče</td>
</tr>
<tr>
<td>4.</td>
<td>Teorie informace, teorie složitosti algoritmů</td>
</tr>
<tr>
<td>5.</td>
<td>Hašovací funkce, MD5, SHA-x, HMAC</td>
</tr>
<tr>
<td>6.</td>
<td>Testy prvočíselnosti, proudové šifry, RC4</td>
</tr>
<tr>
<td>7.</td>
<td>Blokové šifry, DES, 3DES, AES, operační módy</td>
</tr>
<tr>
<td>8.</td>
<td>Asymetrická kryptografie 1</td>
</tr>
<tr>
<td>9.</td>
<td>Asymetrická kryptografie 2</td>
</tr>
<tr>
<td>10.</td>
<td>Kryptografické protokoly – IPsec, SSL/TLS, SSH, SCP</td>
</tr>
<tr>
<td>11.</td>
<td>Zabezpečení bezdrátových a mobilních sítí (GSM, UMTS, WiFi, WiMAX)</td>
</tr>
<tr>
<td>12.</td>
<td>Zabezpečení protokolů pro přenos hlasu v datových sítích (SIP, H.323, IAX)</td>
</tr>
<tr>
<td>13.</td>
<td>Zabezpečení e-mailové komunikace (PGP, S-MIME), elektronický podpis</td>
</tr>
</tbody>
</table>

IV. INOVACE CVIČENÍ

Cvičení jsou organizována formou seminářů a laboratorních úloh. Vzhledem k rozsahu předmětu se cvičení konají jednou za 2 týdny. Laboratorní úlohy demonstrují různé technologie a aspekty informační bezpečnosti.

V. KONKRETNÍ VÝSTUPY

Konkrétními výstupy rešení projektu je vytvoření dvou nových laboratorních cvičení, inovace dvou stávajících přednášek a vytvoření materiálů na přednášky a laboratorní cvičení včetně elektronických testů pro online testování znalostí studentů.

VI. ZÁVĚR

V rámci inovace předmětu Kódy a bezpečnost byly inovovány dvě přednášky tak, aby lepši pokrývaly oblast informační bezpečnosti a v rámci cvičení byly vytvořeny dvě nové laboratorní úlohy a inovována jedna stávající. Pro přednášky i pro laboratorní úlohy byly vytvořeny nové výukové materiály v elektronické formě dostupné na školním LMS systému Moodle.

Tabulka 3 – Stávající osnova cvičení

<table>
<thead>
<tr>
<th>Týden</th>
<th>Náplň přednášky</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Úvodní cvičení. Seznámení s obsahem předmětu a náplní cvičení. BOZP</td>
</tr>
<tr>
<td>2.</td>
<td>Google Hacking</td>
</tr>
<tr>
<td>3.</td>
<td>Kryptoanalýza I</td>
</tr>
<tr>
<td>4.</td>
<td>Kryptoanalýza II</td>
</tr>
<tr>
<td>5.</td>
<td>Kryptoanalýza III</td>
</tr>
<tr>
<td>6.</td>
<td>Úvod do laboratorních úloh</td>
</tr>
<tr>
<td>7.</td>
<td>Laboratorní úloha – Útoky v lokálních sítích na spojové vrstvě RM OSI</td>
</tr>
<tr>
<td>8.</td>
<td>Semestrální project</td>
</tr>
<tr>
<td>9.</td>
<td>Laboratorní úloha – IPsec VPN</td>
</tr>
<tr>
<td>10.</td>
<td>Semestrální project</td>
</tr>
<tr>
<td>11.</td>
<td>Laboratorní úloha – SSL VPN</td>
</tr>
<tr>
<td>12.</td>
<td>Semestrální project</td>
</tr>
<tr>
<td>13.</td>
<td>Zápočtový test</td>
</tr>
<tr>
<td>14.</td>
<td>Zápočet</td>
</tr>
</tbody>
</table>

Tabulka 4 – Osnova inovovaných cvičení

<table>
<thead>
<tr>
<th>Týden</th>
<th>Náplň přednášky</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Úvodní cvičení. Seznámení s obsahem předmětu a náplní cvičení. BOZP</td>
</tr>
<tr>
<td>2.</td>
<td>Google Hacking</td>
</tr>
<tr>
<td>3.</td>
<td>Kryptoanalýza I</td>
</tr>
<tr>
<td>4.</td>
<td>Kryptoanalýza II</td>
</tr>
<tr>
<td>5.</td>
<td>Kryptoanalýza III</td>
</tr>
<tr>
<td>6.</td>
<td>Úvod do laboratorních úloh</td>
</tr>
<tr>
<td>7.</td>
<td>Laboratorní úloha – Útoky v lokálních sítích na spojové vrstvě RM OSI</td>
</tr>
<tr>
<td>8.</td>
<td>Semestrální project</td>
</tr>
<tr>
<td>9.</td>
<td>Laboratorní úloha – Srovnání VPN technologií</td>
</tr>
<tr>
<td>10.</td>
<td>Semestrální project</td>
</tr>
<tr>
<td>11.</td>
<td>Laboratorní úloha – Detekce a prevence šifrových útoků ve smíšeném prostředí IPv4/IPv6</td>
</tr>
<tr>
<td>12.</td>
<td>Semestrální project</td>
</tr>
<tr>
<td>13.</td>
<td>Zápočtový test</td>
</tr>
<tr>
<td>14.</td>
<td>Zápočet</td>
</tr>
</tbody>
</table>

PODĚKOVÁNÍ

Tento projekt byl financován Ministerstvem školství České republiky, Fondem rozvoje vysokých škol č. 28/2012/F1a.
Abstract—Nejlepší cestou pro implementaci nových telekomunikačních technologií je vybudování nové infrastruktury, ale více než polovina všech nákladů v telekomunikační infrastrukturě je právě potřebná pro vybudování nových telekomunikačních sítí. Toto vybudování s sebou přináší otázku, zda nevyužít infrastrukturu stávající, jejíž využití je atraktivním řešením z hlediska finančních nákladů. Jednou z těchto infrastruktur je silnoproudé vedení a s ním spojená datová komunikace po silnoproudém vedení (Power Line Communication).

Klíčová slova - datová komunikace po silnoproudém vedení, modelování

I. ÚVOD

Technologie přenosu dat po silnoproudých vedeních, Power Line Communication (PLC), není novinkou. Historie této technologie, například podle publikace [1], je datována do počátku 20. století. V roce 1950 byla navržena jedna z prvních PLC technologií, známá jako hromadné dálkové ovládání (HDO) a poté nasazena na distribuční sít středního a nízkého napětí [2].

Tento příspěvek je zaměřena na rozbor PLC komunikace a stanovení podstaty modelování datové komunikace po silnoproudém vedení.

II. PODSTATA MODELOVÁNÍ PLC

Silnoproudé vedení není uzpůsobeno pro datovou komunikaci kvůli své frekvenční a časové proměnnosti. Dále silnoproudé vedení představuje z hlediska PLC velmi zaručené přenosové medium, především díky šumu na pozadí a impulznímu rušení [5]. Z těchto důvodů se velmi obtížně modeluje [3], [4].


V poslední době se v publikacích [15], [16] a [14] začíná uvažovat s hybridním přístupem, který kombinuje dohromady různé způsoby modelování tak, aby výsledný model byl co nejvhodnější pro specifickou oblast využití.

III. MODELOVÁNÍ PLC

Pro vytvoření celého komunikačního systému PLC komunikace je nutné, kromě modelů vedení, modelovat zdroje rušení a také vytvořit model komunikačního systému představující vysílač a příjímač komunikace. Pro účely modelování lze tedy PLC komunikační systém rozdělit na dílčí části:

- PLC komunikační model,
- Model silnoproudých vedení,
  - Prostředí s vícecestným šířením signálu,
  - Dvojbrané popsané kaskádními parametry,
- Model zdrojů rušení.

Složením těchto jednotlivých modelů vznikne model PLC komunikačního systému. Na základě simulací tohoto celého modelu s různými modely vedení bude možné provést analýzu konkrétní silnoproudé sítě s přesným získáním z hlediska možnosti nasazení různých kombinací PLC technologií, modulací, kódování atd., aby bylo dosaženo co nejlepších parametrů datového přenosu v uvedených systémech.

Pro simulaci PLC komunikace je stěžejní částí simulace vedení. Existují dva hlavní přístupy pro modelování silnoproudých vedení [13]. První modeluje silnoproudé vedení jako prostředí s vícecestným šířením signálu. Parametry takového vedení jsou získány z topologie distribučních sítí nebo na základě měření. Druhá možnost modelování silnoproudých vedení je pomocí dílčích bloků – dvojbranových, popsaných kaskádními parametry, které charakterizují závislost vstupních a výstupních napětí a proudů pomocí dvojbranových.

A. Prostředí s vícecestným šířením signálu

Silnoproudé vedení může být považováno za vícecestný kanál, jelikož vícecestné šíření je způsobeno impulzně nepřezpůsobenými odbočkami vedení.

Silnoproudé vedení vykazuje značné nehomogenity, které se projevují odrazy, vícecestným šířením a tedy většinou nejlepších parametrů vedení.
Na Obr. 1 je zobrazen model reprezentující vícecestně silnoproudé vedení. Přenašený signál prochází k přijímači přes $N$ různých cest. Každá cesta $i$ je definována určitým zpožděním $\tau_i$ a faktorem útlumu $C_i$.

B. Kaskádní parametry vedení jako dvojbranu

Silnoproudé vedení je často složeno z několika různorodých úseků, proto je vhodné jej modelovat pomocí dvojbrojů a specifikovat pomocí kaskádních parametrů. Kaskádní tvar rovnice pro popis dvojbranu vychází z obecného dvojbranu, viz Obr. 2. Parametry vedení jsou soustředěny pouze do jednoho bodu a napětí a proud jsou v jednom čase stejné ve všech místech vedení. Přípomoc uvedených dvojbrojů lze nahradit jak celé vedení, tak i jenom určitý úsek vedení. Pro modelování dalších vlastností či připojených zařízení je možné články zapojovat kaskádě za sebou a získat tak celý úsek silnoproudého řetězce, např. od transformátoru až po model zátěže.

![Obr. 1. Modelování silnoproudého vedení vícecestným šířením](image1)

![Obr. 2. Dvojbran pro určení kaskádních parametrů vedení](image2)

IV. ZÁVĚR

Příspěvek poskytuje přehled dosavadní publikované literatury z oblasti modelování silnoproudých vedení.

Byly nastíněny dvě metody modelování silnoproudého vedení, první jako prostředí s vícecestným šířením a druhá pomocí kaskádně zapojených elementárních dvojbrojů. Sestavené modely silnoproudých vedení umožní provést výzkum v oblasti různých topologií distribuční sítě a připojených komponent a umožní studium jejich vlivu na datovou komunikaci.

![Obr. 3. A Deterministic Frequency Domain Model](image3)
Analýza hlavních komponent (PCA)

Jan Skapa
Department of Telecommunications
Faculty of Electrical Engineering and Computer Science
VŠB-Technical University of Ostrava 17. listopadu 15/2172, 708 33 Ostrava-Poruba, Czech Republic
Email: jan.skapa@vsb.cz

Abstract—Tento článek popisuje použití analýzy hlavních komponent (PCA – Principal Component Analysis) jako nástroje pro redukci dimenze statistického problému. Pokud jsou data silně korelovaná (tedy existuje lineární závislost mezi jednotlivými proměnnými), je možné použít PCA k rozlišení těch komponent, které řešený problém vysvětluji významně od těch, které k vysvětlení jemu přispívají pouze nepatrně.

I. INTRODUCTION

Metoda analýzy hlavních komponent (PCA – Principal Component Analysis) je používána ke snížení dimenze problému. Z hlediska statistiky můžeme na jednotlivé vektory pohlížet jako na díly proměnná. PCA nahrazuje původní soubor pozorovaných (vzájemně korelovaných) znaků souborem nových (hypotetických), vzájemně nekorelovaných znaků tak, že první nová osa (první hlavní komponenta, PC1, první nový znak) je vedena ve směru největší variability mezi objekty, druhá osa (druhá hlavní komponenta, PC2, druhý nový znak) je vedena ve směru největší variability, který je kolmý na směr první komponenty, atd. Dohláží tedy k natočení ortogonálního pravděpodobnostního prostoru tak, aby hlavní komponenty, odpovídající sestupně setříděné variabilitě odpovídaly rozložení okolo jednotlivých os.

II. MATHEMATICKÝ APARÁT

A. Střední hodnota

Střední hodnota \( \bar{x} \) vektoru \( x \) o délce \( M \) vzorků je dána vztahem

\[
\bar{x} = \frac{1}{n} \sum_{k=1}^{M} x[k].
\]  

(1)

B. Kovariance

Kovariance (vzájemná variance) \( \text{cov}(x_1, x_2) \) vektorů \( x_1 \) a \( x_2 \) o délce \( M \) vzorků je dána vztahem

\[
\text{cov}(x_1, x_2) = \frac{1}{n} \sum_{k=1}^{M} (x_1[k] - \bar{x}_1)(x_2[k] - \bar{x}_2).
\]  

(2)

C. Variance

Variance (disperze) \( \text{var}(x) \) vektoru \( x \) o délce \( M_1 \) vzorků (prvky na hlavní diagonále kovarianční matice) je dána vztahem

\[
\text{var}(x) = \frac{1}{n} \sum_{k=1}^{M_1} (x[k] - \bar{x})^2.
\]  

(4)

D. Směrodatná odchylka

Směrodatná odchylka \( \text{std}(x) \) (standard deviation) souvisí s variances vektoru vztahem

\[
\text{std}(x) = \sqrt{\text{var}(x)}.
\]  

(5)

E. Korelace, korelační koeficient

Korelace je definována pro reálné posloupnosti \( x_1 \) délky \( M_1 \) vzorků a \( x_2 \) délky \( M_2 \) vzorků jako posloupnost \( r_{x_1,x_2} \) délky \( 2 \cdot \max(M_1, M_2) - 1 \) vzorků

\[
r_{x_1,x_2}[k] = \begin{cases} 
\frac{1}{L} \sum_{n=0}^{L-1-k} x_1[n]x_2[n+k], & k \geq 0 \\
\frac{1}{L} \sum_{n=0}^{L-1+k} x_1[n-k]x_2[n], & k < 0
\end{cases}
\]  

(6)

kde \( k \in \langle -\max(M_1, M_2) - 1, \max(M_1, M_2) - 1 \rangle \), \( L = \max(M_1, M_2) \). Korelací obvykle posuzujeme pomocí tzv. korelačních koeficientů.

Normovaná korelace (viz [2]) je normozměnou verzí vzájemné korelace. Jeho hodnoty leží v intervalu \( \langle -1, 1 \rangle \). Hodnota 1 odpovídá maximální korelací (překrytí signálů), hodnota −1 odpovídá signálu v protifází.

\[
r_{n_{x_1,x_2}}[k] = \frac{r_{x_1,x_2}[k]}{\sqrt{r_{x_1,x_1}[k] r_{x_2,x_2}[k]}}
\]  

(7)

Silná korelace mezi signály znamená, že informaci, obsaženou v prvním signálu \( x_1 \), signál \( x_2 \) rozšíří jen o malé množství další informace.

Pearsonův korelační koeficient je dán vztahem Jeho hodnota udává míru lineární závislosti.

Vzhledem k tomu, že výše uvedené vzorce mohou být nějaké specifického prostředí, nebo máte v plánované aplikaci další specifické požadavky, doporučuji si tyto formulace srovnat s vaším vytvořením či případně se poradit s vědníkem, abyste se jistě přesvědčili o pravdivosti a průběžnosti jejich aplikace v rámci vašeho projektu.
\[
\text{covmt} = \begin{bmatrix}
\text{cov}(x_1, x_1) & \text{cov}(x_1, x_2) & \ldots & \text{cov}(x_1, x_N) \\
\text{cov}(x_2, x_1) & \text{cov}(x_2, x_2) & \ldots & \text{cov}(x_2, x_N) \\
\vdots & \vdots & \ddots & \vdots \\
\text{cov}(x_N, x_1) & \text{cov}(x_N, x_2) & \ldots & \text{cov}(x_N, x_N)
\end{bmatrix}.
\]

(3)

\[
\rho_{x_1, x_2}[k] = \frac{\text{cov}(x_1, x_2)}{\sqrt{\text{var}(x_1) \text{var}(x_1)}} = \frac{\sum_{k=1}^{N} (x_1[k] - \bar{x}_1)(x_2[k] - \bar{x}_2)}{\sqrt{\sum_{k=1}^{N} (x_1[k] - \bar{x}_1)^2} \sqrt{\sum_{k=1}^{N} (x_2[k] - \bar{x}_2)^2}}.
\]

(8)

F. Vlastní čísla, vlastní vektory matice

Vlastní čísla \( \lambda \) a vlastní vektory \( u \) matice \( A \) jsou řešením rovnice

\[
A \cdot u = \lambda \cdot u.
\]

Tu lze přepsat do tvaru

\[
(A - \lambda I)u = 0.
\]

Tato soustava má netrivíální řešení v tom případě, kdy je determinant matice soustavy roven nule, tedy

\[
det(A - \lambda I) = 0.
\]

Věta 1: Je-li \( A \) je reálná symetrická matice řádu \( N \), potom jsou všechny kořeny rovnice (11) reálné, tedy všechna vlastní čísla jsou reálná.

Věta 2: Dva vlastní vektory odpovídající různým vlastním čísům matice \( A \) jsou navzájem ortogonální.

Věta 3: Ke každé symetrické matrice \( A \) existuje ortonormální matice \( R \) taková, že \( R^TAR = B \) je diagonální matice, kde prvky \( b_{ij} \) na hlavní diagonále matice \( B \) jsou všechna vlastní čísla \( \lambda_i \) matice \( A \) (počítána i s jejich násobností) a sloupcové vektory matice \( R \) jsou jednotkové vzájemně ortogonální vlastní vektory matice \( A \) přislušející vlastním čísům \( \lambda_i \).

Důkazy předchozích vět lze nalézt např. v [1], [4].

III. POSTUP TVORBY HLAVNÍCH KOMPONENT.

Metoda úspěšně redukuje dimenzi problému, jestliže mezi původními proměnnými je silně vzájemná korelace. Metoda je založena na analýze vlastních čísel a vlastních vektorů symetrických kovariančních matice. Postup tvorby hlavních komponent vysvětlím na příkladu.

Příklad 1: Nalezněme hlavní komponente pro soubor dat, daný proměnnými \( x_1, x_2 \). Obrázek 1 zobrazuje data proložená regresní přímkou \( y = 0.9259x \), jejíž koeficienty byly nalezeny metodou minimalizace součtu čtverců odchylek.

Tabulka I zobrazuje hodnoty proměnných \( x_1, x_2 \), centrovány hodnoty a standardizované hodnoty. Někdy se používá také standardizování centrovanych hodnot. Potom \( \bar{x} = 0 \) a \( \text{stč}(x) = 1 \).

Dále budeme pracovat s centroványmi proměnnými.

Nyní vypočteme hodnoty Pearsonova korelačního koeficientu, který udává míru lineární závislosti mezi proměnnými. Z chyby regrese je patrné, že míra lineární závislosti je vysoká. Při srovnání součtu čtverců odchylek regresní křivky a skutečných hodnot dostaneme při použití polynomu 1. a 2. stupně téměř shodné výsledky, výrazně lepší hodnoty regrese dává až polynom 3. řádu. Z hodnot blízkých 1 je patrné, že vzájemná korelace je vysoká, tudíž je vysoká také míra lineární závislosti mezi proměnnými \( x_1 \) a \( x_2 \). To souhlasí s očekáváním, položeným na základě analýzy chyby regrese.

Dalším krokem je vypočet vlastních čísel a vlastních vektorů kovarianční matice. Vlastní vektory odpovídají směrovým kosinům os pootočených ve směru nejvyšší variance původních proměnných. Velikost vlastních čísel určuje, kolik z celkové variance všech hlavních komponent ta která hlavní komponenta vysvětluje. Seřadíme tudíž vlastní čísla i

\[ x_{1s} = x_{1c} / \text{std}(x_{1c}) \]

\[ x_{2s} = x_{2c} / \text{std}(x_{2c}) \]

\[ y = 0.9259x \]
**Table I**

<table>
<thead>
<tr>
<th>Původní hodnoty</th>
<th>Centrované hodnoty</th>
<th>Standardizované hodnoty</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_1$</td>
<td>$x_2$</td>
<td>$(x_1 - \bar{x}_1)$</td>
</tr>
<tr>
<td>2.5</td>
<td>2.4</td>
<td>0.69</td>
</tr>
<tr>
<td>0.5</td>
<td>0.3</td>
<td>-1.31</td>
</tr>
<tr>
<td>2.2</td>
<td>3.9</td>
<td>0.39</td>
</tr>
<tr>
<td>1.0</td>
<td>2.2</td>
<td>0.09</td>
</tr>
<tr>
<td>3.1</td>
<td>3.0</td>
<td>1.29</td>
</tr>
<tr>
<td>2.3</td>
<td>2.7</td>
<td>0.49</td>
</tr>
<tr>
<td>2</td>
<td>1.6</td>
<td>0.19</td>
</tr>
<tr>
<td>1</td>
<td>1.6</td>
<td>-0.81</td>
</tr>
<tr>
<td>1.5</td>
<td>1.0</td>
<td>-0.31</td>
</tr>
<tr>
<td>1.1</td>
<td>0.9</td>
<td>-0.71</td>
</tr>
</tbody>
</table>

**Figure 2.** Standardizovaná data $x_1$ a $x_2$, centrovaná a standardizovaná data.

**Table III**

<table>
<thead>
<tr>
<th>Vlastní čísla</th>
<th>Vlastní vektory</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>B</td>
<td>1</td>
</tr>
<tr>
<td>0.7071</td>
<td>0.7071</td>
<td>0</td>
</tr>
<tr>
<td>0.7071</td>
<td>0.7071</td>
<td>0</td>
</tr>
</tbody>
</table>

**Figure 3.** Hlavní komponenty $PC_1$ a $PC_2$.

**Table IV**

<table>
<thead>
<tr>
<th>$n$</th>
<th>$m$</th>
<th>$\text{cov}(x_1, x_1)$</th>
<th>$\text{cov}(x_1, x_2)$</th>
<th>$\text{cov}(x_2, x_1)$</th>
<th>$\text{cov}(x_2, x_2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1.0000</td>
<td>0.0000</td>
<td>0.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0.0000</td>
<td>1.0000</td>
<td>0.0000</td>
<td>1.0000</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0.0000</td>
<td>1.0000</td>
<td>0.0000</td>
<td>1.0000</td>
</tr>
</tbody>
</table>

Hlavní komponenty pak odpovídají součinu matici zadaných vstupních (centrovaných) dat s jednotlivými vlastními vektory.

Vlastní vektory sestupně podle velikosti vlastních čísel. Pak při redukci dimenze volíme jen tolik hlavních komponent, kolik procent celkové variance jimi chceme popsat. V našem případě, pokud chceme popsat více než 95% celkové variance (hladina významnosti $\alpha = 0.05$), stačí vzít v úvahu pouze první hlavní komponentu.

**Figure 2.** Standardizovaná data $x_1$ a $x_2$ proložená regresní přímou s osami postočenými ve směru nejsvětší variance.

Z hodnot nulové korelace hlavních komponent je zřejmé, že nově vytvořené komponenty již nejsou navzájem lineárně.
závislé.

IV. CONCLUSION

V článku byla podrobně rozebrána metoda analýzy hlavních komponent a její využití k redukcii dimenze či vytvoření proměnných, které nejsou na sobě vzájemně závislé (jsou nekorelované).

ACKNOWLEDGMENT

Tento příspěvek vznikl za podpory projektu Společné aktivity VUT a VŠB-TUO při vytváření obsahu a náplně odborných akreditovaných kurzů ICT, č. projektu: CZ.1.07/2.2.00/28.0062.

REFERENCES