

International Journal of Advances in Telecommunications Electrotechnics, Signals and Systems

a publication of the International Science and Engineering Society



**Vol. 5, No. 1
2016**

ISSN: 1805-5443

www.ijates.org

I J
A T
E S²

International Journal of Advances in Telecommunications Electrotechnics, Signals and Systems

a publication of the International Science and Engineering Society

Vol. 5, No. 1, 2016

ISSN: 1805-5443

Editor-in-Chief

Jaroslav Koton, Brno University of Technology, Czech Republic

Co-Editors

Ondrej Krajsa, Brno University of Technology, Czech Republic

Norbert Herencsar, Brno University of Technology, Czech Republic

Editorial Board

Oguzhan Cicekoglu, Bogazici University, Turkey

Sergey Ryvkin, Trapeznikov Institute of Control Sciences Russian Academy of Sciences,
Russian Federation

Hongyi Li, Bohai University, China

Emilia Daniela Bordencea, TU Cluj-Napoca, Romania

Albert Abilov, Izhevsk State Technical University, Russian Federation

Joze Guna, University of Ljubljana, Slovenia

Jaroslav Koton, Brno University of Technology, Czech Republic

Ondrej Krajsa, Brno University of Technology, Czech Republic

Danilo Pelusi, University of Teramo, Italy

Aims and Scope

The International Journal of Advances in Telecommunications, Electronics, Signals and Systems (IJATES²) is an all-electronic international scientific journal with the aim to bring the most recent and unpublished research and development results in the area of electronics to the scientific and technical societies, and is supported by the ISES (International Science and Engineering Society, o.s.). The journal's scope covers all the aspects of telecommunication, signal processing, theory and design of circuits and systems for electronics.

The IJATES² is ready to publish experimental and theoretical full papers and letters submitted by prospective authors. Paper submitted for publication must be written in English and must follow a prescribed format. All papers are subjected to a critical peer-review prior to publication.

The IJATES² is an open access journal which means that all content is freely available without charge to the user or his/her institution. Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the articles in this journal without asking prior permission from the publisher or the author. This journal provides immediate open access to its content on the principle that making research freely available to the public supports a greater global exchange of knowledge.

www.ijates.org

Copyright © 2012-2016, by ISES, o.s.

All the copyright of the present journal belongs to the International Science and Engineering Society, o.s.

CONTENTS

Vol. 5, No. 1, 2015

ISSN: 1805-5443

A No-Reference Image Quality Metric with Application in Low-Dose Human Lung CT Image Processing <i>Gergő Bognár</i>	1
Objective Empirical Mode Decomposition metric <i>Dawid Laszuk, Oswaldo Jose Cadenas, Sławomir Jarosław Nasuto</i>	8
Electronic Elections Based on Group Signatures <i>Lukas Malina, Jan Smrz, Jan Hajny</i>	15
Evaluation of Responses in MTL Model Excited from Multiple Stochastic Sources <i>Lubomir Brancik, Edita Kolarova</i>	22
Benchmarking Further Single Board Computers for Building a Mini Supercomputer for Simulation of Telecommunication Systems <i>Gábor Lencse, Sándor Répás</i>	29
Efficient Routing and Spectrum Allocation Considering QoT in Elastic Optical Network <i>Bingbing Li, Young-Chon Kim</i>	37
Wideband Analog Transmission System Based on the External Intensity Electro-Optic Modulator <i>Jiri Svarny</i>	44
Investigating the Performance of the MPT Multipath Communication Library in IPv4 and IPv6 <i>Béla Almási, Szabolcs Szilágyi</i>	53

A No-Reference Image Quality Metric with Application in Low-Dose Human Lung CT Image Processing

Gergő Bognár

Abstract—In this paper a no-reference image quality metric designed for human lung CT scans is presented. The metric can be used for several purposes, including the evaluation of visual quality of CT scans or controlling enhancement processes. The developed method is based on a modified SKFCM image segmentation algorithm combined with the SSIM metric. A lung phantom was constructed for validation purposes. Tests were performed both with synthetic images, using the lung phantom with added noise, and with real CT images. The presented methods include simulations, quantitative studies and subjective evaluation. Experimental results show that the metric values reliably follow the visual image quality of CT.

Keywords—CT, fuzzy C-means, image quality metrics, low-dose, lung phantom, noise modeling

I. INTRODUCTION

ONE of the motivations behind the construction of the is to provide a tool for objective evaluation of the quality of low-dose CT scans. As it is known, dose reduction lowers the radiation exposure risks, but at the same time decreases the image quality. Therefore a quality measurement method can be relevant and useful, in this respect.

In X-ray computed tomography, the attenuation of the X-ray photon beam of the human body follows the Beer–Lambert law:

$$I = I_0 \exp\left(-\int_L \mu\right), \quad (1)$$

where I_0 is the source intensity of the beam, I is the observed intensity, recorded by the CT scanner sensors, L represents the beam path and μ is the linear attenuation coefficient function of the body parts. The recorded sinogram can be considered as a sampling of the Radon transform of μ . The reconstruction of μ can be received by means of the so-called filtered backprojection method. For details we refer the reader to [3]. We note that μ depends on photon energy, therefore normalized HU (*Hounsfield Unit*) values are commonly used. Quantum noise and electric noise are present in the recording process, and quantization noise arise during the reconstruction due to discretization.

There are several existing methods for image quality measurement, based on various approaches (see e.g. [6]). The mainstream full-reference metrics are SSIM (*structural similarity index*) [12] and VIF (*visual information fidelity*) [10].

G. Bognár is with the Department of Numerical Analysis, Faculty of Informatics, Eötvös L. University, Budapest, 1117 Hungary e-mail: bognargergo@caesar.elte.hu.

Manuscript received November 15, 2015; revised January 15, 2016.

Unfortunately, they cannot be applied directly in case of CT scans, because in general no high quality reference scans exist. We remark that the SSIM metric has already been applied [7] to compare low-dose reconstructions and original CT scans, where the latter serve as reference images. The existing no-reference metrics are relative in the sense that while they may follow the decrease of the quality of the same image, the metric values are incomparable for different images. The proposed metric, presented in the following section is based on the SSIM metric and on a modified version of the SKFCM (*spatially constrained kernelized fuzzy C-means*) image segmentation algorithm [13]. Besides the SSIM we also studied the CNR (*contrast-to-noise*) and SNR (*signal-to-noise*) metrics [2], which are often used in medical image processing. It turned out that SSIM performs better. For instance, CNR and SNR are very sensitive to the selection of the regions. On the other hand SSIM is normalized, i.e. the metric values are always within the interval $[-1, 1]$.

The outline of this article is as follows. In Section II the quality measurement method is described. Section III contains an analytical study of the metric with the constructed lung phantom and noise model. In Section IV the results on real low-dose and normal lung CT images are presented.

II. METRIC CONSTRUCTION

The metric construction consist of three main steps: preprocessing, segmentation and quality measurement.

We start with a preprocessing step, since experiments performed on real low-dose CT images show that the segmentation technique detailed below is more effective if a preliminary background removal and gamma correction is applied. Here background refers to the region outside the body. For background removal Gaussian and median filtering, thresholding and region fill turned out to be appropriate. Gamma correction was applied to regions with intensity below -700 HU. Fig. 2 (a) shows the result of this step for test image Fig. 1 (a).

We continue with the segmentation part. Human lung CT images, using HU values as pixel intensities, have similar structures and histograms (see Fig. 1). This happens because different human bodies have similar tissue combinations. The proposed segmentation method assigns pixels to tissue clusters according to intensities, spatial distribution and tissue properties.

The SKFCM algorithm was used as starting model. SKFCM is a derivation of the conventional FCM (*fuzzy C-means*) algo-

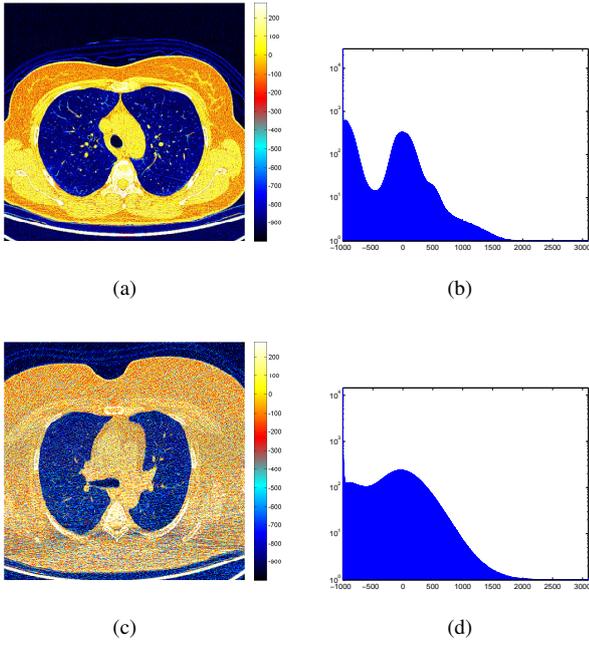


Fig. 1: Low-dose CT images with their histograms, using fake colors.

rithm, replacing the original Euclidean distance with a kernel-induced distance, and adding a spatial penalty to the objective function. SKFCM was originally developed for noisy medical images in order to create homogeneous regions. The SKFCM objective function for segmenting a pixelset $x = (x_k)_{k=1}^N$ into C clusters is:

$$J_m = \sum_{i=1}^C \sum_{k=1}^N u_{ik}^m (1 - K(x_k, v_i) + P_{m,i,k}), \quad (2)$$

where $v = (v_i)_{i=1}^C$ are the cluster prototypes, $U = (u_{ik})_{i=1,k=1}^{C,N} \in [0, 1]^{C \times N}$ stands for the partition membership matrix, satisfying:

$$\forall k : \sum_{i=1}^C u_{ik} = 1, \quad \forall i : 0 < \sum_{k=1}^N u_{ik} < N, \quad (3)$$

K is a Gaussian RBF with standard deviance σ , and $m > 1$ determines the level of cluster fuzziness. $P_{m,i,k}$ represents the spatial penalty term in the neighborhood N_k of pixel x_k , within cluster v_i :

$$P_{m,i,k} = \frac{\alpha}{|N_k|} \sum_{r \in N_k} (1 - u_{ir})^m, \quad (4)$$

where the parameter $\alpha \in (0, 1)$ controls the penalty effect. Then SKFCM can be considered as an optimization problem, i.e. minimization of J_m under the constraints for U .

The standard SKFCM cannot be applied directly in case of lung CT scans, because it generates the same homogeneity level in all of the clusters. In case of lung CT scans, the segmentation goal is to create homogeneous fat, muscle and internal organ regions, with a detailed lung region. The structure of the lung tissue must be preserved since it is diagnostically relevant. In order to achieve this goal, the spatial penalty

TABLE I: Cluster prototypes

Material	Prototype (HU)
Air	-1000
Lung	-600
Fat	-100
Muscle, internal organs	100
Bone	500

term $P_{m,i,k}$ in the objective function had to be modified. One of the problems with the original penalty term was the constant window size. In the modified version, we specified different window sizes for different clusters. In addition to that a weighted summation is used inside the windows, allowing different homogeneity levels in the clusters. Then the modified spatial penalty is:

$$P_{m,i,k} = \alpha \sum_{r \in N_{ik}} w_{ir} (1 - u_{ir})^m, \quad (5)$$

where N_{ik} stands for the neighborhood of pixel x_k within cluster v_i , and w_{ik} are the weighted coefficients satisfying:

$$\forall i : \sum_{r \in N_{ik}} w_{ik} = 1, \quad x_k \notin N_{ik}. \quad (6)$$

Another important modification was the use of fixed cluster prototypes. In the original SKFCM the number of clusters is fixed, but the cluster prototypes are allowed to change during the iterative optimization. In case of lung CT scans, fixed cluster prototypes give a reliable and comparable segmentation result. Table I contains the selected clusters and prototypes.

Similarly to the standard SKFCM the objective function J_m can be minimized by the following iteration scheme. Initialize U with:

$$u_{ik}^{(0)} = \frac{(1 - K(x_k, v_i))^{-1/(m-1)}}{\sum_{j=1}^C (1 - K(x_k, v_j))^{-1/(m-1)}}, \quad (7)$$

and in each iteration step update U with:

$$u_{ik}^{(t+1)} = \frac{(1 - K(x_k, v_i) + P_{m,i,k}^{(t)})^{-1/(m-1)}}{\sum_{j=1}^C (1 - K(x_k, v_j) + P_{m,j,k}^{(t)})^{-1/(m-1)}}. \quad (8)$$

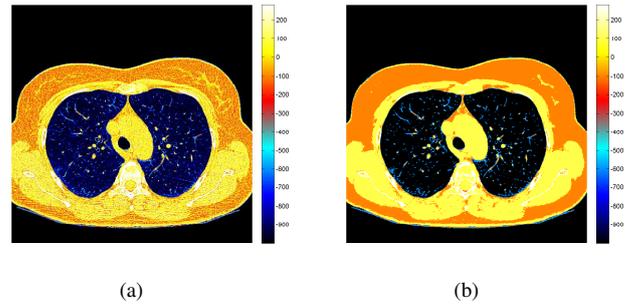


Fig. 2: The result of preprocessing and segmentation.

As a consequence of noise, overfitting may happen. In order to avoid it, early stopping is necessary. The iteration stops, when one of the following criteria are met.

- The iteration reaches $t_{max} = 10$ steps,
- $E^{(t)} = \|U^{(t)} - U^{(t-1)}\|_{\infty}$ error satisfies $E^{(t)} < \varepsilon$,
- $E^{(t)} > \beta E^{(t-1)}$, where $\beta \in (0, 1)$ is a fixed constant.

The last criterion prevents overfitting. Namely, if the decrease of $E^{(t)}$ is under a desirable speed, the iteration stops.

The parameters were optimized by means of tests performed on real CT images. The result is as follows: $m = 2$, $\alpha = 0.3$, $\beta = 0.75$, $t_{max} = 10$. The dimension of the window N_{ik} is 3×3 in case of air and lung clusters, and the weights are generated from the Gaussian filter with standard deviance 0.5. For other clusters the window size is 9×9 , and the weights come from the Gaussian filter with standard deviance 1.5. Experimental results show, that the iteration works better if the standard deviance of Gaussian RBF K is proportional to the image noise level. Noise level was roughly estimated by using wavelet transform and calculating the standard deviation of the detail component, which mostly contains noise. The result of segmentation applied to test image Fig. 1 (a) is shown on Fig. 2 (b).

In the final step, we employ the full-reference SSIM metric to the result of segmentation and the starting preprocessed image. Here the result of segmentation serves as reference image. The metric value lies within the interval $[-1, 1]$, where higher value means better quality. The performed tests using both synthetic and real CT images show that it complies with the visual quality of the CT scans.

III. PHANTOM STUDY

We constructed a lung phantom for testing and validating the developed metric. This phantom serves as an analytical and schematic model of the lung. We used the lung phantom and noise model to generate synthetic images with different noise levels. They served as test cases for the segmentation and quality measurement method.

During the construction of the lung phantom we followed the principles of the Shepp–Logan head phantom [11], which is the most popular analytical phantom. The tissues are represented by means of elliptical regions, therefore the Radon transform of the phantom can be calculated directly [9], and the synthetic sinogram can be obtained in an analytical form. The lung phantom, as shown on Fig. 3, consists of 6 big and 200 small ellipses. Big ellipses represent fat, muscle and bone

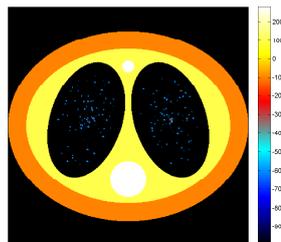


Fig. 3: Lung phantom.

tissues, small ones the lung tissue. Small ellipses have random sizes, placed randomly inside the lung area, 100-100 on each side. Prototypes of Table I shows the ellipse intensities. The exact phantom specification is given in Appendix A.

We used the noise model for digital sensors given in [4]. It includes both quantum noise and electric noise. This model can be applied to CT scanner sensors, as well. The model describes the electric noise as a signal-independent Gaussian random variable with expected value 0 and fixed variance, and the quantum noise as a signal-dependent Poissonian random variable. Approximating the Poisson distribution with Gaussian distribution, the noise model is:

$$I_{noise} = I + \eta(I), \quad \eta(I) \sim \mathcal{N}(0, aI + b), \quad (9)$$

where I is as in (1), I_{noise} stands for the detected, noisy intensity. The positive parameters a and b control the effect of the quantum and electric noise, respectively. Similar equation, with modified a and b parameters, can be given for the quotient of the source and the observed intensities:

$$\frac{I_{noise}}{I_0} = \frac{I}{I_0} + \eta\left(\frac{I}{I_0}\right), \quad \eta\left(\frac{I}{I_0}\right) \sim \mathcal{N}\left(0, a\frac{I}{I_0} + b\right), \quad (10)$$

where I_0 stand for the source intensity.

CT screening process was simulated by using the lung phantom and the noise model above. The simulation parameters were chosen to imitate the settings of the real CT scans. Namely, photon beam energy is set to 57 KeV, with the corresponding value $\mu_{H_2O} \approx 0.2 \text{ cm}^{-1}$ (see [5]). The output resolution is 512×512 pixels, pixel distance is chosen to 0.06 cm. Simulation starts with generating a synthetic sinogram by sampling the analytical Radon transform of the lung phantom. Generated noise can be added after converting the sinogram to intensity quotients. Then, reversing this method

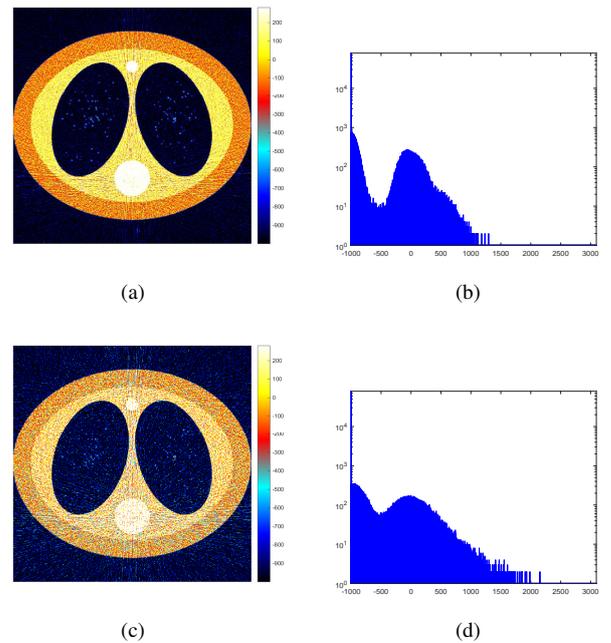


Fig. 4: Synthetic lung phantom scans with different noise levels.

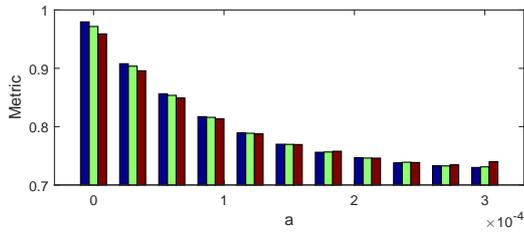


Fig. 5: Dependence of the metric values on parameter a with three fixed values of parameter b : $5 \cdot 10^{-8}$ (blue), 10^{-7} (green) and $2 \cdot 10^{-7}$ (red).

a noisy phantom scan can be reconstructed. In the following examples filtered backprojection with Ram-Lak filter was used as reconstruction algorithm. With given direction L and Radon transform $P(L)$ the intensity quotient is:

$$\frac{I}{I_0} = \exp(-0.2 \cdot 0.06 \cdot P(L)). \quad (11)$$

Adding noise to I/I_0 , with I_{noise}/I_0 the noisy $P_{noise}(L)$ Radon transform will be:

$$P_{noise}(L) = -\frac{1}{0.2 \cdot 0.06} \cdot \ln\left(\frac{I_{noise}}{I_0}\right). \quad (12)$$

Fig. 4 contains two synthetic lung phantom reconstructions with their histograms. The images are generated with parameters $b = 10^{-7}$, $a = 6 \cdot 10^{-5}$ and $a = 3 \cdot 10^{-4}$, respectively. The synthetic and the real CT images have similar visual appearance and histogram structure (compare Fig. 4 to Fig. 1). The noise appears a similar way, similar artifacts can be observed (e.g. beam hardening). This shows that the lung phantom can be used as a schematic model for a two-dimensional slice of a human lung CT scan.

We can deduce from the experimental results on synthetic scans that the segmentation process preserves the structure of the images and the metric value reliably follows the image quality. In Fig. 5 a quantitative study of the metric and the lung phantom is demonstrated, with different a and b parameter values. The diagram shows the dependence of the metric values on parameter a with three fixed values of parameter b . Blue bars belong to $b = 5 \cdot 10^{-8}$, green bars to $b = 10^{-7}$, red bars to $b = 2 \cdot 10^{-7}$. Each value is calculated as an average of 20 measurements. We can conclude that with fixed level of electric noise, the metric values follow the change of quantum noise level.

IV. REAL CT TESTS

Experimental results on real CT scans show that the proposed segmentation preserves the structure of the images, and the given metric value is a reliable characterization of image quality. We compared multiple datasets, compared the metric to existing methods, performed quantitative study based on the patient size and made comparison to subjective evaluations.

A. Datasets

This study is primarily based on 20 low-dose lung CT scans from Pozitron-Diagnostics Health Centre, Budapest, Hungary.

These scans were recorded with Siemens Somatom scanner using the same settings, namely photon beam energy is 57 KeV, tube current is 30 mAs with 130 kVp. Each scan consist of 231 to 298 slices, the resolution of a slice is 512×512 , the pixel distance is between 0.0576 and 0.0744. Beside that, test were performed on two additional datasets: 50 low-dose lung scans from public database ELCAP [8], and 20 normal-dose lung scans from public database LIDC-IDRI [1].

Considering the scans of Pozitron-Diagnostics Health Centre, the metric values lie between 0.61676 and 0.85809. Fig. 14 gives a comparison of metric values with 8 images from the dataset. Tests on the scans from database ELCAP give similar results. Namely, metric values are between 0.65505 and 0.85857. The similarity of the results is reasonable, because the two low-dose dataset contain visually similar CT images. Segmentation gives a better result on normal-dose scans from database LIDC-IDRI, comparing to low-dose scans. In this case metric values lie in a higher range, between 0.82946 and 0.93688, as expected.

B. Comparison to CNR and SNR

We compared the CNR and SNR metrics to the proposed metric. Here we remark that to calculate these metrics a nearly homogeneous background and body region need to be selected. Both metrics are very sensitive the way we select that regions. We used a semi-automatic region selection based on the segmentation but a per-image supervision was required. Fig. 6 shows the selected ROI for a low-dose test image. There is a strong relation between the metric values and the CNR and SNR values, the Pearson linear correlation coefficient is 0.86 in both cases. Fig. 7 shows the CNR values against the metric values.

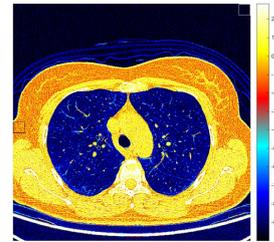


Fig. 6: ROI used to calculate CNR and SNR, white rectangle for background, black rectangle for body ROI.

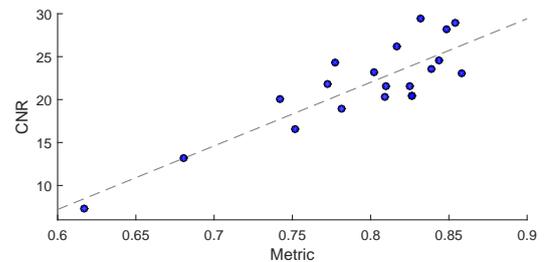


Fig. 7: Correlation between the metric values and the CNR values.

C. Quantitative study of the metric values

According to the properties of the CT screening, the patient size affects the quality of the scan. During the scans of larger patients the radiation dose is usually increased (i.e. by increasing the tube current or lowering the kVp) to maintain image quality. With fixed tube current and kVp, we can expect worse image quality in case of larger patients. As discussed before, the scans from Pozitron-Diagnostics Health Centre have the same recording parameters, except the pixel distance and the number of slices. These parameters are set individually for each patient, according to the size of their bodies. Consequently, in case of these CT scans, an image quality metric should correlate with the patient size. The test results show that the largest patients have the lowest metric values (see Fig. 14). We studied this effect regarding to real and synthetic images, as well.

Before a CT scan, the weight of the patient is measured, this parameter is stored in the file headers. The weight can be considered as a rough characterization of the patient size. We compared the metric values to the weight parameters, the Pearson linear correlation coefficient of 0.62 indicates a relation between these two properties. We note that heavy but tall patients may have small thoracic region. A better description should consider other properties as well, for instance the height of the patients, but this parameter is not available. To give a better characterization of the patient size, we measured the body area on the selected slices. Using the segmentation, we counted the pixels, which, according to their intensities, belong to muscles, fat, internal organs or bones. Then we scaled this area with the pixel distances. The Pearson linear correlation coefficient between the measured area and the metric values is -0.88 , which indicates a strong relation. Fig. 8 presents this relation, the metric values against the measured body area.

We simulated different patient sizes with the lung phantom. At fixed level of noise, namely with noise parameter $a = 6 \cdot 10^{-5}$ and $b = 10^{-8}$, we performed two simulations. First we enlarged the phantom with fixed pixel distance, then with the original phantom we generated synthetic images with different pixel distances. We remark that the two simulations are similar, the main difference is that in the first case the phantom is cropped to the viewing area (see Fig. 9), while in the second case, the viewing area is enlarged and the whole phantom is visible (see Fig. 10). The generated synthetic images are still similar to the real CT scans, and with larger phantom or bigger pixel distance we can observe higher level of noise, as

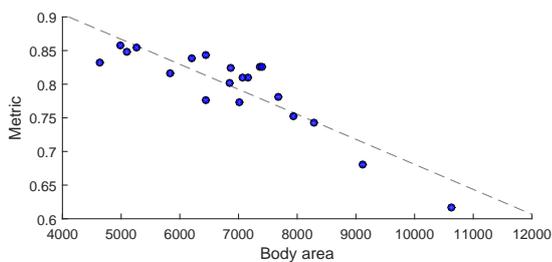


Fig. 8: Correlation between the metric values and the measured body area.

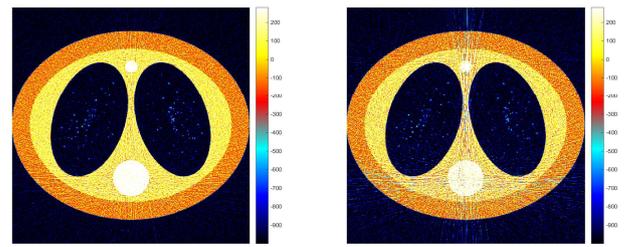


Fig. 9: Phantoms with pixel distance 0.055 cm and 0.07 cm.

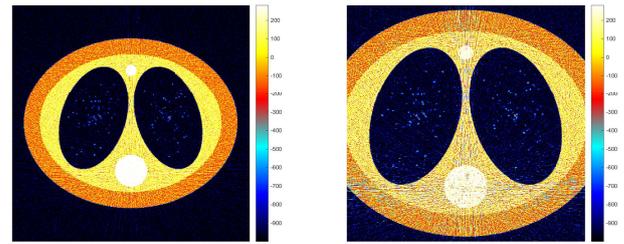


Fig. 10: Enlarged phantoms, with size multiplier 0.9 and 1.2.

expected. The metric values follow the size, the Pearson linear correlation coefficients are nearly -1 in both cases. Fig. 11 and Fig. 12 show the metric values against pixel distances and size, respectively. Each value is calculated as an average of 20 measurements.

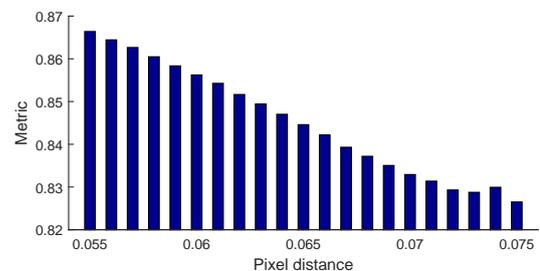


Fig. 11: Dependence of the metric values on the pixel distances.

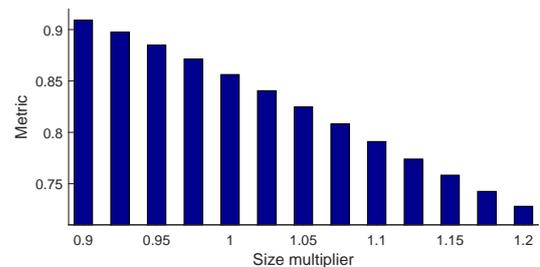


Fig. 12: Dependence of the metric values on the size multipliers.

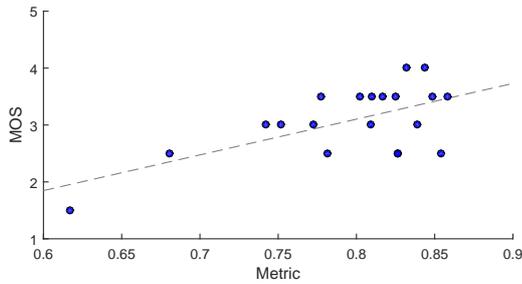


Fig. 13: Correlation between the metric values and the subjective MOS.

We can conclude that the proposed metric handles the quality degradation caused by the patient size well.

D. Subjective quality evaluation

To interpret and discuss the measurement results, we transformed the metric values into 1 to 5 scores. As mentioned before, the SSIM values are always between -1 and 1 , in practical cases between 0 and 1 . In our case the metric values are above 0.6 for real CT images and above 0.7 for synthetic images. Considering this, we transformed the $[0.6, 1)$ interval into 1 to 5 integer scores. In case of low-dose images the lowest metric values is therefore 1, the highest is 4, the most of the images get score 3. In case of normal-dose images, the lowest score is 3, the highest is 5, the most of the images get score 4.

Finally we provide comparison to subjective quality scores. Two radiologist medical doctors associated with Pozitron-Diagnostics Health Centre evaluated the 20 low-dose scans the institute provided. They assigned scores between 1 and 4, where 1 means the worst, 4 the best quality. We compared the MOS (*mean opinion score*) of the two evaluations to the metric values. The Pearson linear correlation coefficient between the MOS and the metric values is 0.62 which indicates a relation between them. Fig. 13 shows the MOS against the metric values. Since the Pearson linear correlation coefficient between the two different subjective evaluations is also 0.62 , we can conclude that, taking the uncertainties into consideration, the proposed metric values describe the quality well according to the subjective evaluations. We note that more reliable results can be given with further evaluations including more scans and more radiologist test subjects.

V. CONCLUSION

In this paper a no-reference image quality metric for human lung CT scans is presented. The metric construction is based on segmentation, modifying and adjusting the SKFCM algorithm. The modified objective function of SKFCM made it possible to applying this method to lung CT images. Quality measurement was performed with SSIM, comparing the result of the segmentation with the preprocessed original image. The metric was tested and validated with a constructed lung phantom and real CT scans. Synthetic images were created using the lung phantom and noise model, and real, low-dose

and normal lung CT scans were examined. We performed simulations, quantitative studies and subjective evaluation as well. Experimental results in each cases show that the proposed metric is a good estimation of image quality.

The results presented in this paper are preliminary and further clinical evaluation is required.

The possible applications of the metric include measuring and comparing image enhancement methods, optimizing the parameters of the CT process or the settings of the CT scanners. For instance, tube current and voltage may be optimized based on the metric, achieving low radiation dose yet good image quality, even in real time during the CT recording.

The method was developed especially for low-dose lung CT scans, regarding the attributes of this images. However, if the parameters of segmentation is adjusted properly, it seems possible to use the metric with other type of CT images or even with other type of medical images. This utilization needs further research.

APPENDIX A LUNG PHANTOM SPECIFICATION

X	Y	Major axis	Minor axis	Theta	HU level
0	0	1.0	0.8	0°	-100
0	0	0.85	0.65	0°	200
-0.35	0.05	0.3	0.5	-18°	-1100
0.35	0.05	0.3	0.5	18°	-1100
0	-0.45	0.15	0.15	0°	400
0	0.5	0.05	0.05	0°	400
...	0°	400

The table above contains the exact specification of the lung phantom: center coordinates (X and Y), axes, rotation angles (Theta) and intensity levels in HU. The last row stands for the 100-100 small ellipses inside of the third and fourth big ellipses. These small ellipses are placed randomly, and have random axes between $1/512$ and $4/512$.

ACKNOWLEDGEMENTS

The author would like to thank to medical doctors, especially Zs. Lengyel MD, associated with Pozitron-Diagnostics Health Centre for their contribution, and Prof. S. Fridli for helpful feedback.

The author acknowledges the U.S. National Cancer Institute and the Foundation for the National Institutes of Health, and their critical role in the creation of the free publicly available LIDC/IDRI Database used in this study. The author acknowledges the Computer Vision and Image Analysis Group of Cornell University and the International Early Lung Action Program, and their work by creating the ELCAP Public Lung Image Database, also used in this study.

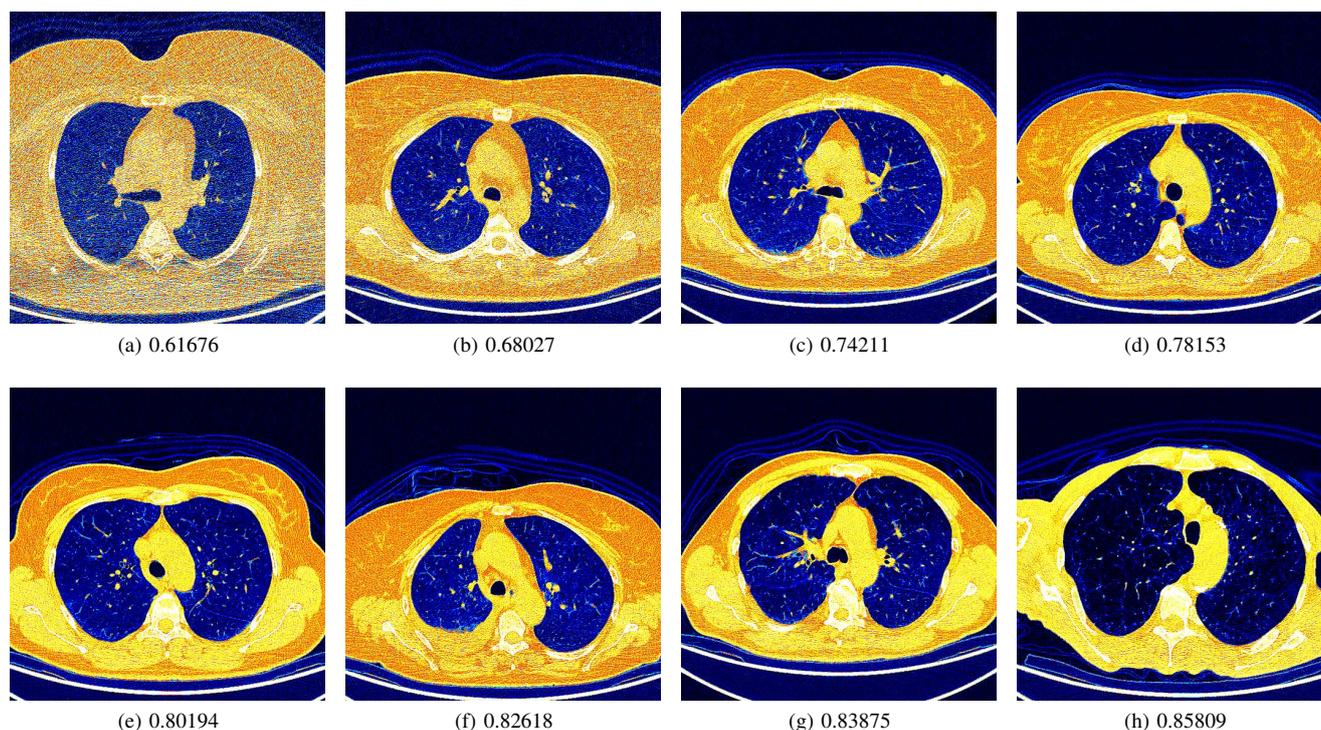


Fig. 14: Low-dose CT scans with different quality and the metric values. (Pozitron-Diagnostics Health Centre)

REFERENCES

- [1] S. G. Armato III, G. McLennan, L. Bidaut, M. F. McNitt-Gray, C. R. Meyer, A. P. Reeves, B. Zhao, D. R. Aberle, C. I. Henschke, E. A. Hoffman, E. A. Kazerooni, H. MacMahon, E. J. R. van Beek, D. Yankelevitz, et al., "The Lung Image Database Consortium (LIDC) and Image Database Resource Initiative (IDRI): A completed reference database of lung nodules on CT scans," *Medical Physics*, vol. 38, no. 2, pp. 915–931, Feb. 2011.
- [2] J. T. Bushberg, J. A. Seibert, E. M. Leidholdt Jr., J. M. Boone, *The Essential Physics of Medical Imaging*, 2nd ed. Philadelphia, PA: Lippincott Williams & Wilkins, 2002, pp. 255–292.
- [3] S. R. Deans, *The Radon transform and some of its application*. New York: John Wiley & Sons, 1983, pp. 11–16.
- [4] A. Foi, M. Trimeche, V. Katkovnik, K. Egiazarian, "Practical Poissonian-Gaussian noise modeling and fitting for single-image raw-data," *IEEE Transactions on Image Processing*, vol. 17, no. 10, pp. 1737–1754, Oct. 2008.
- [5] J. H. Hubbel, S. M. Seltzer. (2004, July). Tables of X-Ray Mass Attenuation Coefficients and Mass Energy-Absorption Coefficients (version 1.4). Gaithersburg, MD: National Institute of Standards and Technology [Online]. Available: <http://physics.nist.gov/xaamdi>
- [6] W. Lin., C.-C. J. Kuo, "Perceptual visual quality metrics: A survey," *J. Vis. Commun. Image R.*, vol. 22, no. 4, pp. 297–312, May 2011.
- [7] L. Pfister, Y. Bresler, "Tomographic reconstruction with adaptive sparsifying transforms," in *2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Florence, 2014, pp. 6914–6918.
- [8] ELCAP Public Lung Image Database. (2003, December) [Online] Available: <http://www.via.cornell.edu/databases/lungdb.html>
- [9] F. Schipp, "Radon transform," unpublished.
- [10] H. R. Sheikh, A. C. Bovik, "Image information and visual quality," *IEEE Transactions on Image Processing*, vol. 15, no. 2, pp. 430–444, Feb. 2006.
- [11] L. A. Shepp, B. F. Logan, "The Fourier reconstruction of a head section," *IEEE Transactions on Nuclear Science*, vol. 21, no. 3, pp. 21–43, Jun. 1974.
- [12] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
- [13] D.-Q. Zhang, S.-C. Chen, "A novel kernelized fuzzy C-means algorithm with application in medical image segmentation," *Artificial Intelligence in Medicine*, vol. 32, no. 1, pp. 37–50, Sep. 2004.



Gergő Bognár received his BSc and MSc degree (with honors) in Computer Science from Eötvös L. University, Budapest, Hungary in 2012 and 2014, respectively. Currently he is a PhD research student in the Department of Numerical Analysis, Faculty of Informatics, Eötvös L. University. His research interests include image reconstruction, analysis, segmentation and quality measurement, with special emphasis on tomographic images.

Objective Empirical Mode Decomposition metric

Dawid Laszuk, Oswaldo Cadenas, Sławomir J Nasuto

Abstract—Empirical Mode Decomposition (EMD) is a data-driven technique for extraction of oscillatory components from data. Although it has been introduced over 15 years ago, its mathematical foundations are still missing which also implies lack of objective metrics for decomposed set evaluation. Currently, the most common technique for assessing results of EMD is their visual inspection, which is very subjective. This article provides objective measures for validating EMD output, which are derived from the original definition of oscillatory components. Three proposed metrics refer to component's idealised characteristics, i.e. its significant instantaneous frequency and the ability to extract amplitude- and frequency-modulated parts. Possible application of these metrics is presented on two examples.

Keywords—Empirical Mode Decomposition, Hilbert-Huang Transform, Hilbert Transform, Intrinsic Mode Function, Metric, Signal Decomposition.

I. INTRODUCTION

Empirical mode decomposition (EMD) has been proposed recently by Huang et al. [1]. Over past 15 years the method has gained worldwide recognition as a data-driven method for extraction of physically meaningful oscillatory components [2]–[4].

In the original paper on EMD [1] authors noted that small perturbations to the input signal results in different outputs. This is highly undesired effect, but unfortunately due to the heuristic nature of the EMD it is impossible to determine which set of intrinsic mode functions (IMFs) — the output of the EMD — is better. There were many attempts to improve the algorithm, for example ensemble empirical mode decomposition [5]. It assumes that adding small fluctuations to the input signal results in slight perturbation of the output around true decomposition. Thus, creating large ensemble of signals with added small noise will exhaust all possible perturbations and result in large ensemble of decompositions with the mean value being the true set. However, evaluations of this approach indicate that obtained results most of the time do not resemble oscillations and the problem of method being empirical remains. Other attempts to improve EMD, e.g. [6]–[8], have similar issues; there is no mathematical framework and all manipulations are driven mainly with intuition. Nevertheless, researchers usually can make, and do, assessments of method's performance based on their knowledge and experience. Few authors ([1], [9], [10]) have made attempts to formulate rules based on which sets of IMFs should be chosen. All of them, however, are based on the assumption that IMFs belong to Hilbert's L^2 function space, which is not necessarily true. As stated in [1] obtained orthogonality (in Hilbert sense) is purely by coincidence and should not be expected from the method.

Manuscript received November 16, 2015, revised January 13, 2016.

The authors are with the School of Systems Engineering, University of Reading, Reading, RG6 6AY, UK (e-mail: d.laszuk@pgr.reading.ac.uk).

The most popular validation method is based on a visual inspection of the results [9], [11], [12]. This introduces the artefact of subjective opinion into the process. Conclusions from their research cannot be generalized, since they have looked at different, often single, features of output. In this article objective methods for validating the decomposed sets are introduced. The proposals are based on the features that IMF are expected to possess. Each variant focuses on a different characteristics of the data.

The rest of the paper is organized as follows. Section II introduces empirical mode decomposition. Section III describes proposed validating methods. Section IV describes two conducted numerical experiments with conclusions in section V.

II. EMPIRICAL MODE DECOMPOSITION

Empirical mode decomposition (EMD) is a data-driven method for time-frequency analysis. It decomposes data into components called intrinsic mode functions (IMFs). The algorithm encapsulating performing EMD on signal $S(t)$ is as follows:

- 1) Assign trend as a difference between input signal and sum of extracted components, i.e. $r_0(t) := S(t) - \sum_{j=1}^n c_j(t)$. If it is a first iteration, than $r_0(t) := S(t)$.
- 2) Identify all local extrema (both minima and maxima) in time series $r_i(t)$, that is whenever the derivative is $dr_i(t)/dt = 0$.
- 3) If the number of extrema is less or equal 2 then $r_i(t)$ is considered as a trend — a low frequency modulation — and the algorithm stops.
- 4) Calculate top (e_{max}) and bottom (e_{min}) envelopes by interpolating respectively local maxima and local minima with natural cubic splines.
- 5) Calculate the instantaneous mean of both envelopes $m(t) = \frac{1}{2}(e_{max}(t) + e_{min}(t))$.
- 6) Subtract the mean from the input time series $h_i(t) = r_i(t) - m_i(t)$. This step is called sifting, because it removes trend from fast varying component.
- 7) If $h_i(t)$ fulfills the stopping criteria, then it is considered to be an IMF (component $c_n(t) := h_i(t)$) and start again from step 1 with updated set of components. Otherwise, assigned residue as $r_{i+1}(t) := h_i(t)$ and repeat from step 2.

As a result, EMD decomposes signal $S(t)$ into a set of N oscillatory $c_j(t)$ components (IMFs) and a trend $r(t)$ function. Procedure to perform EMD is not uniquely defined. It depends on interpolation technique used for spanning envelopes, definition of extrema, stopping criteria, etc. Different combinations of those settings can produce different outputs even for the same input data. This leads to an obvious question: which set of settings does produce the most significant results?

In the original article on the EMD [1], it was suggested to apply the Hilbert transform (HT) to the obtained set of IMFs. The HT converts a real-valued signal $S(t)$ into an analytic form $A(t)$, which then can be decomposed into amplitude and phase modulation parts [13]. Mathematically, it can be presented as

$$A(t) = a(t) \cos(\phi(t)), \quad (1)$$

where functions $a(t)$ and $\phi(t)$ are amplitude and phase, respectively. Taking derivative of phase over time ($\dot{\phi}$) allows to extract component's instantaneous frequency. With this terms average frequency can be defined as

$$\dot{\Phi} = \frac{1}{T} \int_0^T \dot{\phi}(t) dt, \quad (2)$$

where T is the length of time over which the signal is observed. A combination of EMD and HT on all components is called Hilbert-Huang transformation.

III. PROPOSED VALIDATION METHODS

The main reason for method proposed in this paper is to avoid the use of subjective judgment in evaluation of EMD performance. This is achieved by relying on the intrinsic features reportedly possessed by the IMFs, or on those that would help in the future analysis [1]. The main considered characteristics are: 1) decrease of average frequency with increase of IMFs index, 2) distinct instantaneous frequency for each IMF and 3) disjoint Fourier spectra support for IMF's amplitude and phase.

In this section, IMFs are represented in polar form, i.e. time series of the j^{th} indexed IMF are assumed to have amplitude, a , and phase, ϕ , modulations ($\text{IMF}_j(t) = a_j(t) \cos(\phi_j(t))$). Although, all proposed metrics are designed for continuous functions, in most cases, change to the discrete domain is a straightforward operation. Such processing requires exchanging integration operator over time period T into sum over all data points P .

A. Validation method I

This metric is based on the empirical evidence for the decrease of average instantaneous frequency, simply referred to as the average frequency, with the increase of IMF's index number. Although the order with which the IMF components are constructed in general corresponds to the decreasing IMF average frequencies, there are instances when the instantaneous frequencies cross over between the components. Since it has been claimed that each IMF has a significant instantaneous frequency [1], such behaviour is unwelcome and hence it is penalised by this metric. Penalties are introduced when instantaneous frequency of an IMF with lower number (high average frequency) is smaller than instantaneous frequency of any IMF with higher number. The penalty value is proportional to the length of the crossing over effect, i.e.

$$m_j^I = \sum_{k=j+1}^N \int_{\phi_k > \phi_j} \frac{dt}{T} \quad (3)$$

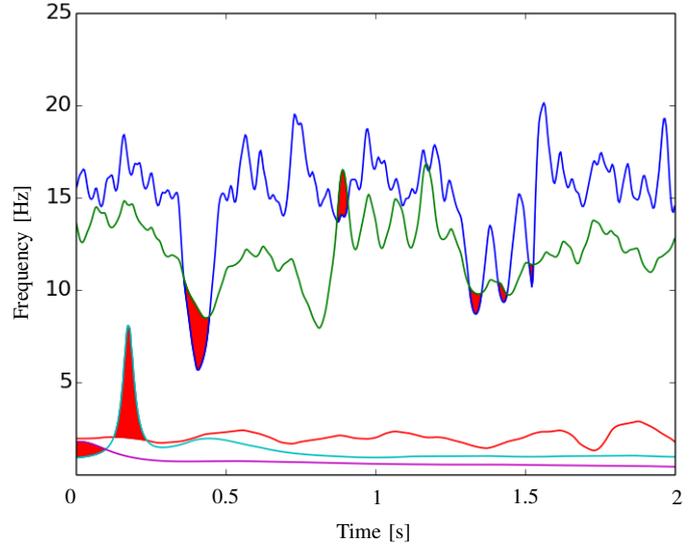


Fig. 1. Plot of instantaneous frequency for each IMF as a function of time. Coloured regions indicates where the frequency crossing over occurs. Metric M_I penalises based on the length of those regions.

where k, j are IMFs' indices. Formula (3) compares functions of instantaneous frequencies of two IMFs and returns the total duration, over which the IMF with higher index has lower frequency. The crossing over effect has been presented in Figure 1. It shows instantaneous frequency of each IMF as a function of time. Coloured regions indicate where the crossing over occurred. Summing over all pairs of IMFs allows us to assess results for particular EMD. Metric value for the whole set is given as

$$M_I = \sum_{j=1}^N m_j^I, \quad M_I \in \left[0, \frac{N(N-1)}{2}\right], \quad (4)$$

According to this measure, the best IMF set is the one, for which $M_I = 0$, i.e. there are no crossing-over parts in instantaneous frequency domain. The worst case, $M_I = N(N-1)/2$, is when the order of all IMFs is reversed, i.e. when the first IMF is under all others and the last IMF is above all others. However, this theoretical upper limit is very unlikely and the corresponding IMF set could be still considered upon index reversal.

B. Validation method II

Another validating measure is based on the Bedrosian theorem [14]. It refers to the necessary conditions for the signal's amplitude, $a(t)$, and phase, $\phi(t)$, to be exactly recoverable using Hilbert transformation. For signal $s(t) = a(t) \cos(\phi(t))$ these conditions require that the support of amplitude and phase's Fourier spectra are not overlapping. In other words, if the amplitude function, $f(t) = a(t)$, and the phase function, $g(t) = \cos(\phi(t))$, then

$$\langle \mathcal{F}(f), \mathcal{F}(g) \rangle = 0, \quad (5)$$

where \mathcal{F} represents the Fourier transform and $\langle h(t), l(t) \rangle = \int h^*(t)l(t)dt$ is the dot product. Here it is assumed, that all functions belong to L^2 normed space.

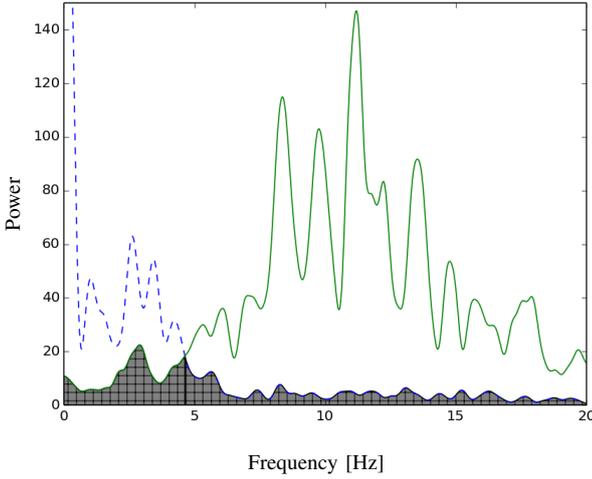


Fig. 2. Example of comparing Fourier spectrum of the amplitude with the spectrum of phase. Gray-striped area indicates where two functions overlap.

Let $F_j^a = |\mathcal{F}(a_j(t))|$ and $F_j^\phi = |\mathcal{F}(\cos(\phi_j(t)))|$ be absolute values of Fourier transforms of a_j and $\cos(\phi_j)$, respectively, for j IMF. Their normalised measure of overlapping spectra is given as

$$m_j^{\text{II}} = \frac{\langle F_j^a, F_j^\phi \rangle}{\sqrt{\|F_j^a\| \|F_j^\phi\|}}, \quad (6)$$

where $\|h\| = \langle h, h \rangle$ is a norm of a function h . Assumptions of Bedrosian's theorem are completely fulfilled when spectra are not overlapping, thus minimum value of m_j^{II} is zero. This allows for different definitions of a metric for the whole IMF set, depending on application of EMD. First proposition is based on a biggest value of overlap m_j in considered decomposition, i.e.

$$M_{\text{II}} = \max_j \{m_j^{\text{II}}\}, \quad M_{\text{II}} \in [0, 1], \quad (7)$$

and the second refers to the cumulative overlap within the decomposed set, i.e.

$$M_{\text{III}} = \sum_{j=1}^N m_j^{\text{II}}, \quad M_{\text{III}} \in [0, N], \quad (8)$$

where in both cases N is the number of extracted IMFs. Zero for both metrics implies no overlap between amplitude's and phase's spectra in any of IMFs.

Visual interpretation of the validation measure (6) is presented in Figure 2. It shows example Fourier spectra of slowly changing amplitude (dashed line) and higher frequency phase (solid line). Gray-striped region indicates overlapping area of both spectra. Proposed value is a measure of ratio of the overlapping area to the total area under both functions.

Since metric M_{III} is a sum over all IMFs, it also contains the one which maximizes value m_j^{II} (Eq. (6)). This means that M_{III} for each decomposition has to be at least equal or higher than M_{II} .

C. Application of the validation measures

Each of the presented metrics highlights different properties of the decomposition. Computing all three values is equivalent to finding a point $M = (M_I, M_{\text{II}}, M_{\text{III}})$ in a 3-dimensional space, where each dimension relates to the specific metric. The best decomposition corresponds to the minimum over all the metrics, i.e. $M = (0, 0, 0)$, and the worst decomposition to $M = (\frac{N(N-1)}{2}, 1, N)$. For any other point one has to decide on the importance, or weight, for each of the proposed metrics, on the basis of the problem being considered. Although the distance in the M -space is not strictly defined, it can be any L^p norm, thus we suggest using the weighted Manhattan metric, i.e.

$$\|M\| = w_1 M_I + w_2 M_{\text{II}} + w_3 M_{\text{III}}, \quad (9)$$

where w_i are respective weights. Their values should reflect the relative importance of features one is concentrated on.

IV. EXPERIMENT

Measures proposed in section III quantify characteristics of well behaved IMFs. The smaller those metrics are, the better the IMF decomposition set represents the desired properties of the EMD-based decomposition.

One could also extend the EMD method into an optimization problem for any parameter, where cost is defined by M_i measures. In the following examples, optimization was performed to choose the best value of a parameter `FIXE_H` for an input signal. The parameter `FIXE_H` indicates when to stop sifting procedure; it refers to the number of consecutive iterations of sifting for which the residue fulfils definition of an IMF. EMD was performed for each value of the parameter and the decomposition which minimized its value was chosen as the best.

For illustration two experiments were conducted. First one is performed on synthetic signal constructed of four sinusoidal components and the second on filtered Gaussian noise. All signals utilized in the following experiments, were generated with a single floating point precision. As it was shown in [15], in most cases this does not influence quality of the decomposition, but can increase the performance. Boundary effect introduced by using Hilbert transform was removed by symmetrically truncating the signal to 80% of the original, i.e. removing initial and final 10% of samples. Additionally, the signal was smoothed by adding mean of each sample's neighbours.

A. Experiment 1

First experiment was conducted on a synthetic signal composed of harmonic components. The test signal was generated according to the following formula

$$S_1(t) = \sum_{j=1}^5 A_j \sin(2\pi f_j t + \phi_j) + \mathcal{N}(0, 0.1), \quad (10)$$

where values for the amplitude (A_j), the frequency (f_j) and the phase shift (ϕ_j) are included in Table I. The values of these parameters were selected at random, with constraints

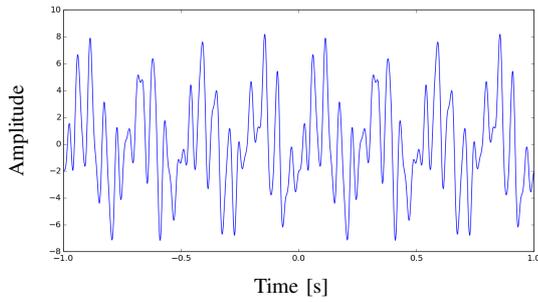


Fig. 3. Test signal $S_1(t)$ used in experiment with synthetic data, generated according to Eq. (10).

that amplitude had to be an integer smaller than 5 and that minimum distance between frequencies was 4. Moreover, in equation (10) the symbol $\mathcal{N}(\mu, \sigma)$ denotes noise in the form of the normal distribution with a mean μ and a variance σ^2 . The graphical representation of the signal can be seen in Fig. 3.

The experiment was conducted as follows:

- 1) Generate test signal $S_1(t)$.
- 2) Set value range of the parameter – FIXE_H spanning from 0 to 20.
- 3) For each value FIXE_H, decompose the signal with EMD and calculate all metrics (M_I , M_{II} and M_{III}).
- 4) The best decomposition set is the one with the smallest sum of all metrics $M = M_I + M_{II} + M_{III}$ (all weights equal).

TABLE I
PARAMETERS FOR AMPLITUDE (A_j), FREQUENCY (f_j) AND PHASE SHIFT (ϕ_j) OF EQUATION 10.

j	A_j	f_j	ϕ_j
1	1	35	2.0
2	1	25	4.0
3	3	19	0.0
4	2	15	3.4
5	3	4	5.7

The signal was decomposed 20 times with the EMD under different stopping criteria conditions, i.e. FIXE_H ranged from 1 to 20. All validating metrics, computed for each decomposition, are presented in the Table II. Decomposition sets are assessed based on a sum total of all metric values for a parameter. The best set is the one with the smallest sum; likewise the worst set is one with the largest value.

For the provided signal, the best decomposition was obtained with the parameter FIXE_H = 17. The figure 4 shows all components. Likewise, the worst decomposition set is obtained for FIXE_H = 1 (Fig. 5). Although these results appear similar, especially when comparing the first IMFs of both decompositions, there are few differences between obtained sets. Main difference is in the number of produced components. The set with higher value of metric M has one additional IMF. It might not be obvious at which stage it was added, but there seems to be more components with low number of extrema. Moreover, the difference is also clear when analysing position and amplitude of extrema. Comparing second and third IMFs one can see that in the best decomposition

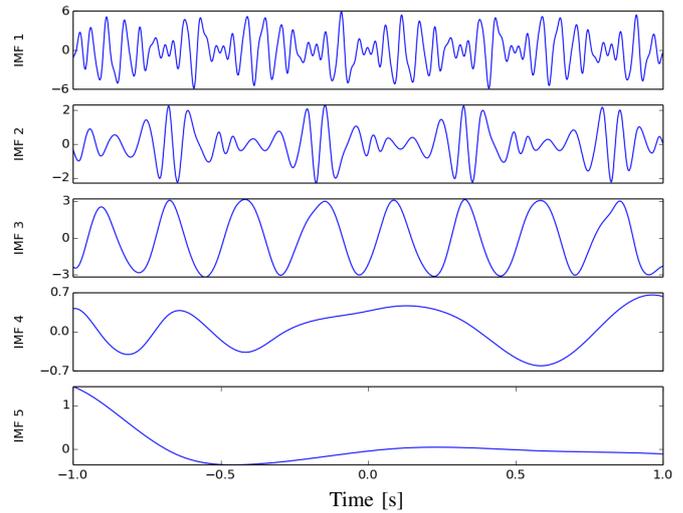


Fig. 4. The best EMD decomposition set, i.e. producing the smallest metric M value, for given range of FIXE_H parameters. Decomposition obtained from signal $S_1(t)$.

position of local extrema are relatively evenly spaced. The same observation holds for the amplitude of extrema — there is a clear stable modulation in the amplitude. In contrast, the worst decomposition has less visible structure, even though it also contains an apparent repeating pattern.

TABLE II
METRIC VALUES OBTAINED BY PERFORMING THE EMD ON $S_1(t)$ WITH VARYING VALUE OF FIXE_H PARAMETER.

FIXE_H	M_I	M_{II}	M_{III}	$M_I + M_{II} + M_{III}$
1	1.17	0.63	0.87	2.66
2	1.13	0.57	0.77	2.47
3	1.33	0.48	0.53	2.27
4	1.17	0.61	0.88	2.65
5	0.91	0.22	0.51	1.64
6	0.92	0.22	0.51	1.65
7	0.93	0.22	0.50	1.64
8	1.15	0.35	0.69	2.19
9	1.12	0.32	0.66	2.10
10	1.12	0.35	0.72	2.19
11	1.18	0.30	0.54	2.02
12	1.20	0.29	0.54	2.03
13	0.98	0.14	0.31	1.44
14	0.98	0.16	0.32	1.45
15	0.96	0.16	0.31	1.43
16	0.97	0.16	0.32	1.45
17	0.96	0.16	0.30	1.42
18	1.44	0.48	0.64	2.56
19	1.45	0.36	0.50	2.32
20	1.56	0.27	0.45	2.24

B. Experiment 2

For this experiment signal was generated using Gaussian noise with mean value 0 and standard deviation 1

$$S_2(t) = \mathcal{N}(0, 1). \quad (11)$$

As it has been suggested in [10], in order to obtain meaningful decomposition it is necessary to have ratio of signal's sampling frequency, f_s , to the highest Fourier frequency, f_f , of at least 10 ($f_s/f_f \geq 10$). This means that when sampling with

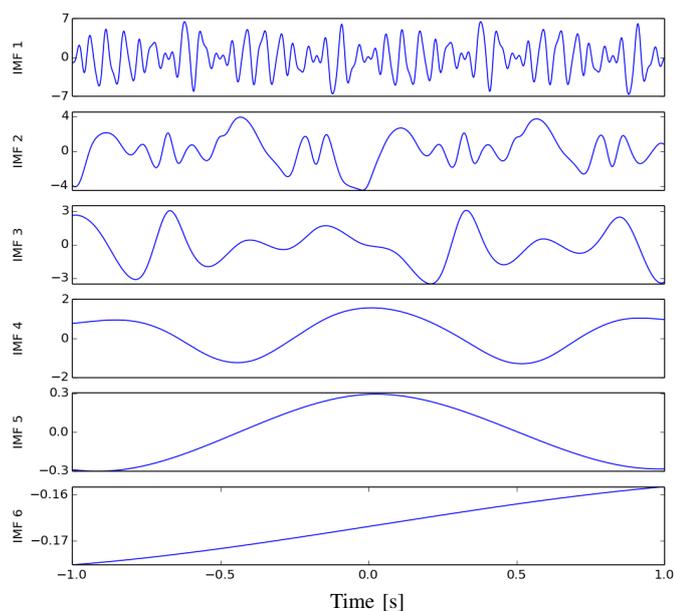


Fig. 5. The worst EMD decomposition set, i.e. producing the biggest metric M value, for given range of FIXE_H parameters. Decomposition obtained from signal $S_1(t)$.

frequency 500 Hz, signal has to be low-pass filtered with the cut off frequency of 50 Hz. For the experiment, we used the zero-phase Butterworth low-pass filter of order 4. The resulting signal is visualised in Figure 6.

The experiment was conducted similarly to the Experiment I, with the difference in weights used to calculate the metric. The exact steps of execution were:

- 1) Generate the test signal, $S_2(t)$.
- 2) Set the value range of the parameter – FIXE_H spanning from 1 to 20.
- 3) For each value FIXE_H , decompose the signal with the EMD and calculate all metrics (M_I , M_{II} and M_{III}).
- 4) The best decomposition set is the one with the smallest sum of all metrics $M = 2 \cdot M_I + M_{II} + 0.5 \cdot M_{III}$.

Such a choice of weights puts more emphasis on selecting IMFs with more mutually separate instantaneous frequencies. It also increases significance of the component with the most overlapping amplitude and phase Fourier spectra; the sum of all measuring values (Eq. (6)) has lower priority. Overall, the metric, M , is meant to select a decomposition with the most distinct frequencies. This effect should be visible when analysing location of extrema, as they should be spaced more evenly.

All calculated values of metrics are presented in the Table III. The last column contains a weighted sum of all other metrics for each value of the parameter FIXE_H . The smallest and the largest values are obtained for FIXE_H equal to 2 and 12, respectively. The best decomposition can be seen in the Figure 7, whereas the worst in the Figure 8. Comparing the two decompositions one can see the difference in the number of IMFs — two more in the worst EMD set. In this case, two first IMFs seem to be similar, or at least without any obvious differences. Analysing position and value of the

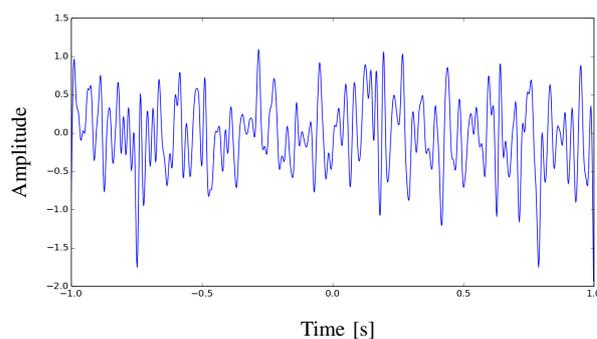


Fig. 6. Test signal $S_2(t)$ used in experiment with filtered Gaussian noise generated.

third component's extrema, one can see that there are more extrema for $\text{FIXE_H} = 12$. Additionally, IMF 6 from the worst decomposition does not seem to have any close counterpart in the best decomposition. Its small amplitude suggests that the component might be hidden within amplitude modulation of any other IMF.

TABLE III
METRIC VALUES OBTAINED BY PERFORMING THE EMD ON $S_2(t)$ WITH VARYING VALUE OF FIXE_H PARAMETER.

FIXE_H	M_I	M_{II}	M_{III}	$2M_I + M_{II} + 0.5M_{III}$
1	1.64	0.60	0.84	4.30
2	1.62	0.59	0.70	4.18
3	1.78	0.58	0.85	4.56
4	2.17	0.56	0.67	5.23
5	2.27	0.53	0.82	5.48
6	2.17	0.45	0.69	5.14
7	2.25	0.47	0.79	5.37
8	2.07	0.57	0.89	5.15
9	2.21	0.53	1.04	5.47
10	2.20	0.55	0.86	5.38
11	2.25	0.55	0.87	5.48
12	2.58	0.60	1.04	6.28
13	2.56	0.60	1.00	6.22
14	2.17	0.51	0.74	5.22
15	2.54	0.61	0.81	6.09
16	2.51	0.60	0.80	6.02
17	2.52	0.60	0.80	6.04
18	2.51	0.60	0.78	6.01
19	2.52	0.60	0.78	6.03
20	2.59	0.58	0.99	6.26

V. CONCLUSION

In the recent years, EMD has been proven very useful in many areas of science and engineering. Unfortunately, due to its flexibility and a lack of mathematical framework, this technique has been misused. Metrics proposed in this paper refer to idealized characteristics of EMD — either suggested, or intended while creating the method. In contrast to the most validation methods discussed in the literature, the ones proposed in this paper are objective, independent from user's subjective judgment of the decomposition. Since EMD creates a set of oscillatory components, the properties on which these metrics were based are related to their frequencies. Validation of the whole IMF decomposition set is performed either on the basis of significant and mutually separate instantaneous

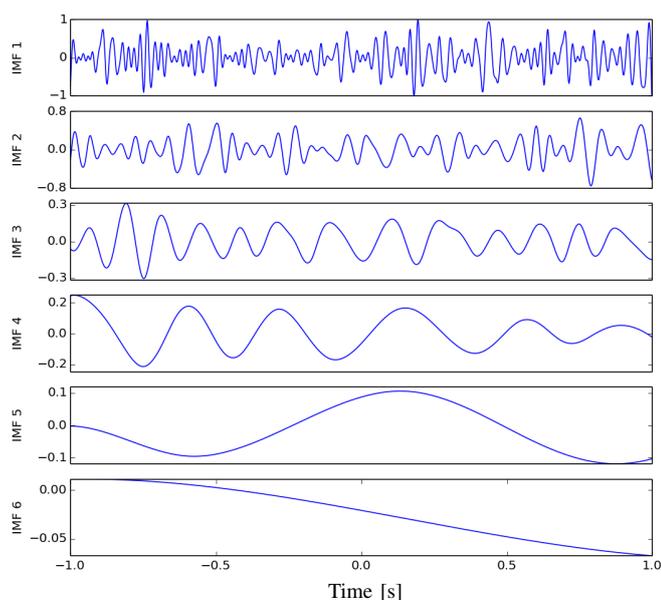


Fig. 7. The best EMD decomposition set, i.e. producing the smallest metric M value, for given range of FIXE_H parameters. Decomposition obtained from signal $S_2(t)$.

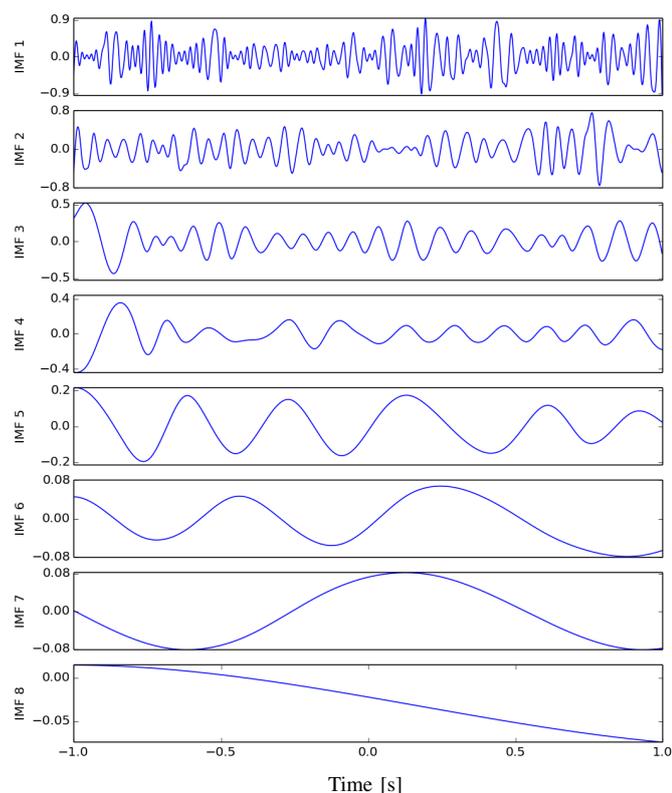


Fig. 8. The worst EMD decomposition set, i.e. producing the biggest metric M value, for given range of FIXE_H parameters. Decomposition obtained from signal $S_2(t)$.

frequencies, or on the attempt to fulfill, or be closer to, the Bedrosian conditions.

An analysis of examples presented in the section IV seems to support the usefulness of the proposed metrics. Although the behaviour of the decomposition can be changed by adjusting weights w_i of the desired feature (Eq. (9)), it should still provide good results. The best decomposition always produces less IMFs, which suggests having more compact information representation of the original signal. Moreover, visual inspection confirms that the best decompositions have better structured (evenly spaced locations of extrema) than the worst ones.

Nevertheless, despite the foregoing discussion, until there is a mathematical foundation of the EMD, it is impossible to create a single metric, which would capture all required features. Proposed measures should be considered as an assistance for an inexperienced user, providing him with additional arguments for used parameters choices.

REFERENCES

- [1] N. E. Huang, Z. Shen, S. R. Long, M. C. Wu, H. H. Shih, Q. Zheng, N.-C. Yen, C. C. Tung, and H. H. Liu, "The empirical mode decomposition and the Hilbert spectrum for nonlinear and non-stationary time series analysis," 1998.
- [2] N. E. Huang and Z. Wu, "A review on Hilbert-Huang transform: Method and its applications to geophysical studies," 2008.
- [3] T. M. Rutkowski, D. P. Mandic, A. Cichocki, and A. W. Przybyszewski, "EMD approach to multichannel EEG data — the amplitude and phase components clustering analysis," 2010.
- [4] D. Mandic, N. Rehman, Z. Wu, and N. Huang, "Empirical Mode Decomposition-Based Time-Frequency Analysis of Multivariate Signals: The Power of Adaptive Data Analysis," *Signal Processing Magazine, IEEE*, vol. 30, no. 6, pp. 74–86, Nov 2013.
- [5] Z. Wu and N. E. Huang, "Ensemble Empirical Mode Decomposition: a Noise-assisted Data Analysis Method," *Advances in Adaptive Data Analysis*, vol. 1, no. 1, pp. 1–41, Jan 2009. [Online]. Available: <http://www.worldscientific.com/doi/abs/10.1142/S1793536909000047>
- [6] S. Meignen and V. Perrier, "A New Formulation for Empirical Mode Decomposition Based on Constrained Optimization," *IEEE Signal Processing Letters*, vol. 14, no. 12, pp. 932–935, Dec 2007.
- [7] C. Huang, L. Yang, and Y. Wang, "Convergence of a Convolution-Filtering-Based Algorithm for Empirical Mode Decomposition," *Advances in Adaptive Data Analysis*, vol. 01, no. 04, pp. 561–571, Oct 2009.
- [8] B. Matei and S. Meignen, "A new optimization based approach to the empirical mode decomposition," *Annals of the University of Bucharest*, vol. 1, no. 4, pp. 129–139, 2014.
- [9] S. Riemenschneider, B. Liu, Y. Xu, and N. E. Huang, "B-spline based empirical mode decomposition," 2005.
- [10] N. Stevenson, M. Mesbah, and B. Boashash, "A sampling limit for the empirical mode decomposition," in *ISSPA 2005: The 8th International Symposium on Signal Processing and its Applications, Vols 1 and 2, Proceedings*, vol. 2. IEEE, 2005, pp. 647–650.
- [11] S. Qin and Y. Zhong, "A new envelope algorithm of HilbertHuang Transform," *Mechanical Systems and Signal Processing*, vol. 20, no. 8, pp. 1941–1952, 2006. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0888327005000993>
- [12] R. Rato, M. Ortigueira, and A. Batista, "On the HHT, its problems, and some solutions," *Mechanical Systems and Signal Processing*, vol. 22, no. 6, pp. 1374–1394, 2008, special Issue: Mechatronics. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0888327007002701>
- [13] L. Cohen, *Time-frequency Analysis*, 1995.
- [14] E. Bedrosian, "A product theorem for Hilbert transforms," *Proceedings of the IEEE*, vol. 51, no. 5, pp. 868–869, May 1963.
- [15] D. Laszuk, O. Cadenas, and S. J. Nasuto, "EMD performance comparison: Single vs Double floating points," *International Journal of Signal Processing Systems*, vol. 4, no. 4, pp. 349–353, 2016.



Dawid Laszuk has received his MSc in Physics (Biomedical specialty) from the University of Warsaw. His thesis concentrated on creating interface and data analysis methods for hybrid brain computer interfacing. He is currently engaged in research to achieve his PhD in Electronic Engineering; this work involves empirical mode decomposition implemented on a graphical processing unit for the analysis of neurological signals (primarily EEG). His research interests also include augmentation and integration of organic and electrical components.



Oswaldo Cadenas received a PhD in Computer science from the University of Reading in 2002 where he has remained as lecturer. Dr Cadenas works on parallel formulation of algorithms and its implementation as parallel hardware architectures.



Sławomir J Nasuto has received an MSc in Mathematics from the University of Marie Curie-Skłodowska in Lublin, Poland in 1993 and a PhD in Cybernetics from University of Reading in 1999. He has been a member of academic staff in School of Systems Engineering at Reading since 2000. His research interests span computational neuroscience and neuroanatomy, analysis of signals generated by the nervous system including EEG, single neuron and multivariate spike trains or EMG and their applications for Brain Computer Interfaces and Animats (robots controlled by neural cultures). He also has research interests in Stochastic Diffusion Search, an algorithm belonging to a family of Swarm Intelligence methods and he has been involved in applications of such techniques in aerospace problems.

Electronic Elections Based on Group Signatures

Lukas Malina, Jan Smrz, Jan Hajny

Abstract—This work deals with electronic elections and voting systems. The paper presents a secure electronic voting solution for small and medium groups of voters. The proposed solution is based on modern cryptographic schemes such as ElGamal encryption and a group signature scheme that keeps user privacy, ballot authenticity and confidentiality. The solution offers a user revocation that can be accomplished only by the cooperation of two system entities. The solution is experimentally implemented and tested and the performance results are measured. The results demonstrate that the solution is practical and can be run on various devices such as PCs, laptops, smartphones, etc.

Keywords—Cryptography, electronic election, group signature, privacy, security, voting.

I. INTRODUCTION

Electronic election and voting systems that run via Internet become more and more popular in many nations, e.g., the United States, the UK, Switzerland, Estonia etc. [1]. Many companies and organizations start to use Internet voting to privately elect board members and officers. Internet voting systems which are based on information and communication technologies, e.g. web access via Internet, can significantly speed up the counting of electronic ballots and can provide the remote access for voters in abroad, persons with disabilities etc. Electronic voting systems have to usually provide many phases, e.g. setup, distributing, voting, collecting and ballots counting. These systems have to be secured as well as possible to minimize the possibility of cyber attacks, frauds or privacy leaks. In addition, there are online voting systems which offer the digital interaction between government and citizens as a part of the electronic government (E-government). For example in Estonia [2], the citizens can vote in public elections via Internet. On the other hand, these systems have to keep the privacy for civilians and must be trustworthy for public.

Nowadays e-voting systems have to guarantee the privacy of the votes, preserve the correctness of the results and have to be organized in a trustworthy way. In this paper, we deal with secure and privacy-preserving electronic voting systems which use strong cryptographic primitives. We focus solely on the cryptographic concept that allows voters and election observers to verify that ballots are correctly recorded, tallied and declared. We propose a novel solution that is based on the combination of ElGamal encryption and group signatures. The solution keeps voters in anonymity due to their election pseudonyms and group signatures. This work extends our previous work [3] by the experimental implementation of the

Authors are with Department of Telecommunications, Brno University of Technology, Brno, Czech Republic, e-mail: malina@feec.vutbr.cz and xsmrzj00@stud.feec.vutbr.cz and hajny@feec.vutbr.cz

Manuscript received November 19, 2015, revised January 14, 2016. Research described in this paper was financed by the National Sustainability Program under grant LO1401. For the research, infrastructure of the SIX Center was used.

proposed solution and by measuring the performance results. The experimental implementation helps to verify the practical use of the solution on current devices and PCs.

This paper is organized as follows: Firstly, Section II presents the related work. Then, we introduce our proposal of a secure digital voting solution which is suitable for the Internet environment in Section III. In Section IV, we present the security analysis of the solution and we evaluate the performance of our solution. In Section V, the implementation of the solution and experimental results are described. The last section (VI) concludes our work.

II. STATE OF THE ART

The first electronic voting scheme was proposed by David Chaum [4] in 1981. Since then many e-voting schemes have been proposed, e.g. e-voting schemes with publicly verifiable secret sharing [5], [6], [7], e-voting based on mix of cryptosystems (ElGamal encryption, threshold public-key cryptosystem, proofs of knowledge) [8], e-voting based on homomorphism encryption [9] or Pailliar's crypto system [10] and e-voting schemes based on the discrete logarithm problem with secret sharing [11] or on secret sharing techniques with a secure multi-party computation [12]. Nevertheless, only several schemes have been tested in practice. The paper [2] describes e-voting experience from Estonian local elections in 2005. The e-voting system uses special ID cards which replace ordinary identity card. These cards are equipped with electronic microchips, which hold personal information about cardholders, two digital certificates and private keys protected by a PIN number. One certificate is used for authentication and the second one is used for digital signature. These cards can be used also by different organizations for different services. A digital double-envelope approach is used to ensure the security and anonymity of voters. The paper [13] describes e-voting experience from Switzerland. In 2004 and 2005, five e-voting pilot trials were studied in order to grapple all security risks, technical risks and possible attacks.

Chaum *et al.* [14] present a practical voter-verifiable election scheme which allows voters to verify the success of their votes. This verification ensures that their digital ballots are included in the poll. Digital ballots are encrypted twice into onion envelopes. The verification of digital ballots is provided by a public bulletin board where voters check that their encrypted ballot receipts appear correctly. Nevertheless, this system has a few disadvantages. For example, if the authority (knowing the associations of all onions) is compromised then it could jeopardize the secrecy of the votes. Another issue is the possibility of double voting, and the new unwished ballot can replace the old ballot. In 2008, the paper [15] presents an e-voting scheme that uses code voting and linkable group signatures. The proposal

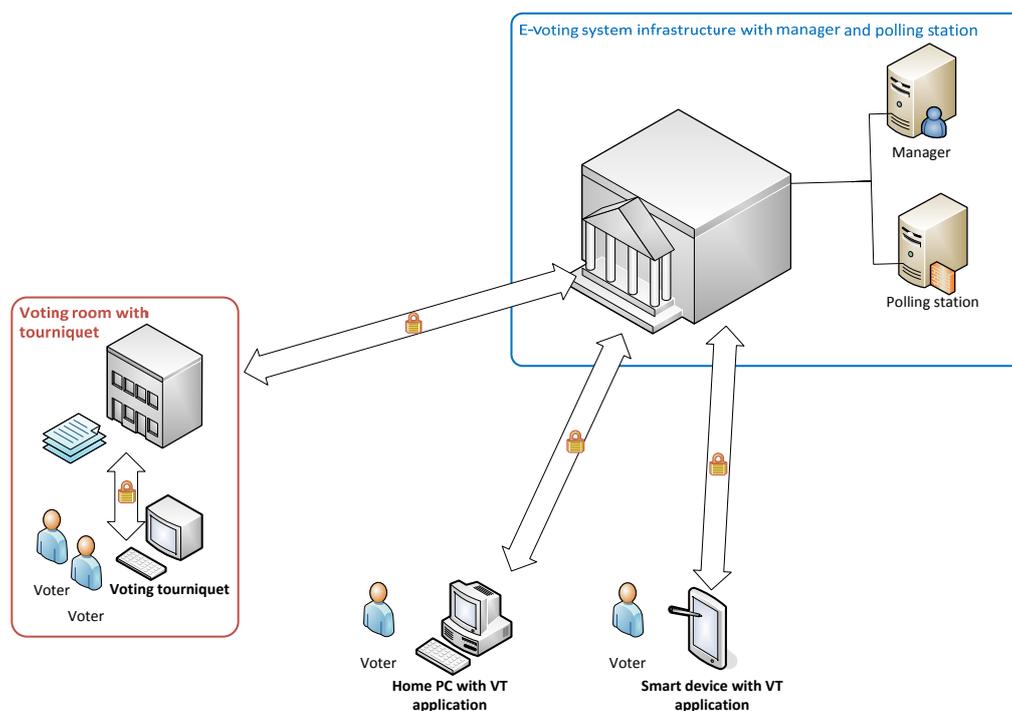


Fig. 1. System model of our e-voting solution.

uses a group signature scheme with two authorities: issuer and opener. Nevertheless, the proposed scheme uses the group signature scheme which requires a secure storage to store a private key on voter's PC. Kremer *et al.* [16] present an election verifiability property in electronic voting protocols. The election verifiability is based on boolean conditions and allows to identify which parts of an e-voting system need to be trusted. Their approach can be applied to systems using blind signatures, homomorphic encryption and mixnets. The paper [17] presents a commitment consistent encryption (CCE) that enables to build the universally verifiable voting schemes with a perfectly private audit trail and practical complexity. CCE is a public key encryption scheme that derives a commitment on the encrypted message and the private key is used to open the commitment. This approach enables to keep the privacy of votes perfectly. The paper [11] presents a practical and secure anonymous Internet voting protocol. The solution is based on a modified ElGamal blind signature scheme and a secret sharing cryptosystem.

In this paper, we propose a solution which is based on the combination of group signatures and probabilistic ElGamal encryption to keep voter in anonymity during the voting and tallying phases. Only the cooperation of a cryptographic manager and an election authority can reveal the user identity and revoke this user from the e-voting system. Further, the proposed solution is implemented to get the performance results.

III. OUR SOLUTION OF PRIVACY-PRESERVING E-VOTING

In this section, we present our solution of a secure and privacy-preserving electronic voting system based on modern cryptographic schemes. Firstly, we describe a system model

which is used in our solution. Then, we introduce cryptographic primitives used in our solution and present the phases of our e-voting solution.

A. System Model

The system model of our solution is depicted in Fig. 1. The proposed solution consists of four system entities (manager, polling station, voting tourniquet and voters) that can be described as follows:

- **Voter (V)** - a person who is able to vote after joining the e-voting system.
- **Manager (M)** - is an entity which manages, sets and generates all system keys and system cryptography parameters. The manager adds/removes all voters into the e-voting system. Before voting, the manager adds all applicants (voters), who are entitled to vote, into a database. The manager generates cryptographic parameters and keys. The manager as the main authority in the system securely keeps all personal information of applicants (full name, address and identification number). The manager can disclose the personal data of revoked voters only in certain election events which require to prevent misusing the system.
- **Polling Station (PS)** - is an entity which organizes elections, generates ballots with the names of the candidates and starts the electoral period. The polling station sends ballots with candidates to the voters after their requests. PS receives and stores the encrypted ballots into a ballot box (database). After the end of the voting period, PS calculates voting results. PS may request the revocation of malicious ballots by sending these data to the manager.

- **Voting Tourniquet (VT)** - is an application which enables voters to interact with the manager and the polling room in the e-voting. VT can be run on users' PC, smartphones or terminals in the voting rooms.

B. Cryptography Used

In our solution the cryptography is based on a group signature scheme, the ElGamal encryption, a secure hash function and the TLS (Transport Layer Security) protocol. The TLS protocol establishes the secure channels between entities in our system model. The ElGamal encryption scheme is used for hiding the content of ballots and for keeping the user privacy. We choose this asymmetric key encryption scheme because it is probabilistic (a single message can be encrypted to many possible ciphertexts). This property is needed for maintaining the user privacy and unlinkability. Further, the non-repudiation, integrity and authentication of ballots have to be provided. Classic signature schemes, e.g., RSA, ECDSA, DSA, provide these properties but do not offer privacy and unlinkability. Hence, we employ Group Signature (GS) schemes because these schemes provide the non-repudiation, integrity and authenticity of signed ballots and keep user privacy and unlinkability. In our scheme, we use the group signature scheme described in [18] which is suitable also for smart phone devices. Nevertheless, we can use other group signature schemes, e.g., [19], [20].

C. Phases of Our Solution

Our solution consists of seven phases: System Setup, User registration, Election Setup, Voter Join, Voting, Tallying and Voter Revocation.

1) *System Setup*: In this phase, all cryptographic parameters are generated. Between Polling Station (PS) and Manager (M) is established a secure connection via TLS. PS generates a public ElGamal encryption key (PS_{pubkey}) and a private ElGamal decryption key ($PS_{privkey}$) for secure communication.

2) *User Registration*: Every new user (voter) has to make a registration. The user has to fill in his personal information and provide these data to manager (M). M verifies the voter's personal data, for example, by scanned ID card. Then, M securely stores the personal data into his database and generates authentication credentials V_{ac} (e.g. a login, an authentication code, a password, a certificate) for every member of the system (voter). After the successful registration, the user of the voting system, voter (V), securely obtains his/her authentication credentials V_{ac} and can download a voting tourniquet application. The voter registration phase is depicted in Figure 2.

3) *Election Setup*: In the Election Setup phase, Polling Station (PS) which organizes elections creates election data (ballots, election start and stop dates, the list of candidates, the number and area of voters, ...). After the creation of election data, PS sends to M the message Start of Election, which contains election data designed for M. M generates group signature scheme parameters such as one public group key ($pubgkey$), n group member private keys for voters

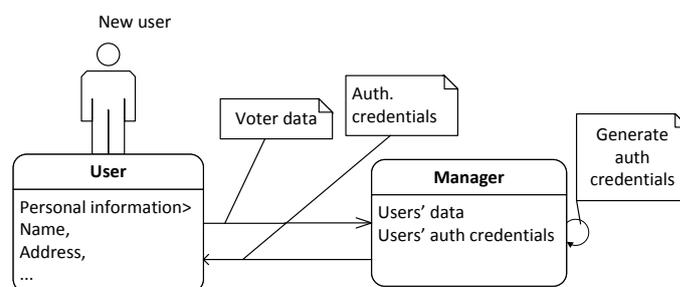


Fig. 2. User Registration phase.

($V_{privgkey}$) where n denotes the number of voters. Further, M generates revocation key ($revgkey$) for this election. M generates voters' election pseudonyms Voter IDs. M sends the list of Voter IDs to PS. PS generates an election encryption public key (EE_{pubkey}), an election encryption private key ($EE_{privkey}$). To secure election encryption it is needed some probabilistic encryption scheme, such as ElGamal. Finally, PS randomly chooses a secret election key ($elsec$). The election setup phase is shown in Figure 3.

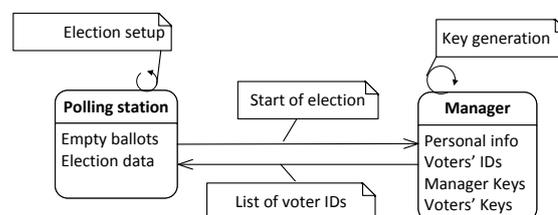


Fig. 3. Election Setup phase.

4) *Voter Join*: Voting Tourniquets (VT), which are involved into the election, establish secure connections with manager (M) via TLS. Firstly, voters have to login into the VT terminal/application and connect with M by using his/her authentication credentials V_{ac} . Voters are authenticated by the manager only if they provide valid authentication credentials V_{ac} . The authentication process should permit only few attempts for one voter's login and after the unsuccessful authentication the algorithm holds and the voter's login is blacklisted. After the successful authentication to the manager, V obtains the Voter ID which is needed for the election via different communication channel (secure email communication, encrypted SMS). V also securely gets the group signature private key ($V_{privgkey}$) and group signature parameters (e.g. $pubgkey$), for the voting phase. These data are securely sent by an encrypted connection via TLS that uses authentication credentials V_{ac} to establish the encryption key.

Later, voters use their voters' ID to download ballots from PS. VT sends the encrypted Voter ID to PS by using the public ElGamal encryption key of PS (PS_{pubkey}). PS can decrypt this message by the private ElGamal decryption key ($PS_{privkey}$). The voter who provides the valid voter ID obtains only one empty ballot (bal) that contains the list of candidates. V also obtains an election token (tok) which is unique and is derived from the Voter ID and the secret election key of PS ($elsec$) by a secure hash function h . Finally, V gets

the election encryption public key ($EEpubkey$) from PS. If V does not provide a valid voter ID to PS then PS stops this phase and does not send any ballot, token and public key to the voter. Figure 4 depicts the Voter Join phase with ballots withdrawing.

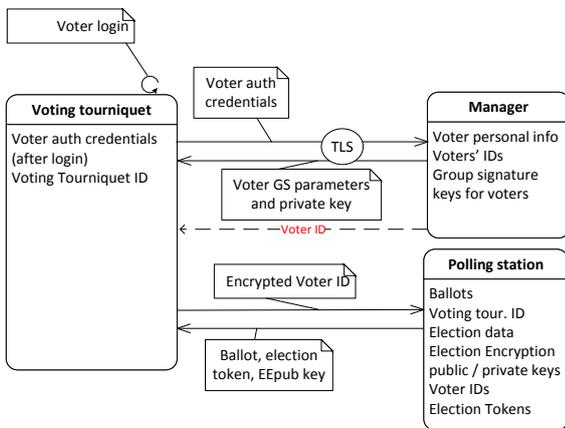


Fig. 4. Voter Join phase

5) *Voting*: During the voting phase, voters access into Polling Station (PS) which simulates a polling room via the Voting Tourniquet (VT) application. Voters use their group signature private keys $V_{privgkey}$ to sign the filled ballots ($fbal$) and election tokens (tok). Every voter computes the group signature of the ballot and the election token and encrypts this signature, the ballot and the election token by the election encryption public key ($EEpubkey$). This encrypted message $enc_{EEpubkey}(sig_{V_{privgkey}}(fbal||tok)||fbal||tok)$ is sent to PS. The voting phase is shown in Figure 5.

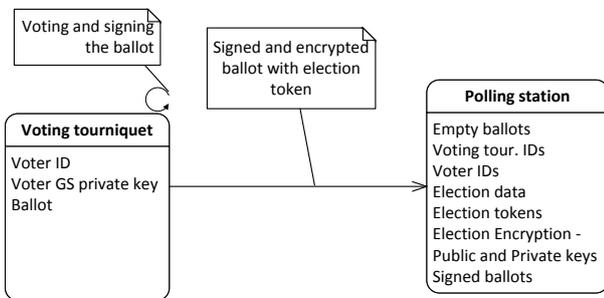


Fig. 5. Voting phase.

6) *Tallying*: In the tallying phase, the voting phase is stopped. Firstly, PS sends the election stop message to M. After that, M stops providing the group signature private keys to voters who miss the election event. Firstly, PS decrypts the message $enc_{EEpubkey}(sig_{V_{privgkey}}(fbal||tok)||fbal||tok)$ by the private key $EEprivkey$. PS checks via election tokens tok if there are no duplicates (e.g. by checking their receiving time stamp). All newer ballots connected with the election tokens which have been already used are discarded. Then, PS uses the group public key $pubgkey$ to check the signatures $sig_{V_{privgkey}}(fbal + tok)$. Some group signatures enable to employ a batch verification which provides the verification of n signatures in one period. Only a voter with a valid group

private key $V_{privgkey}$ is able to sign a message correctly. All ballots with a wrong signature are dropped and not counted by PS. PS counts valid ballots in the final result. The tallying phase is shown in Figure 6.

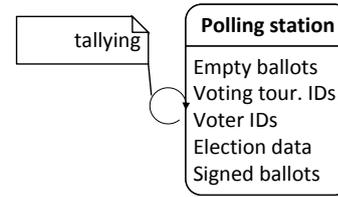


Fig. 6. Tallying phase.

7) *Voter Revocation*: If malicious voters break the rules of the election than the e-voting system is able to revoke this voter. The voter can be revoked by adding his/her election token to a black list. To disclose a voter identity, PS can send Voter ID to M, which is able to find the user real ID in a database. The manager with PS can revoke the voter for the next election events. Moreover, M is able to determine the user ID from the group signature by the manager revocation key ($revgkey$). Nevertheless, PS must send to M a suspicious signed ballot (e.g. a corrupt ballot). M uses it for identifying the malicious Voter. The voter revocation phase is depicted in Figure 7.

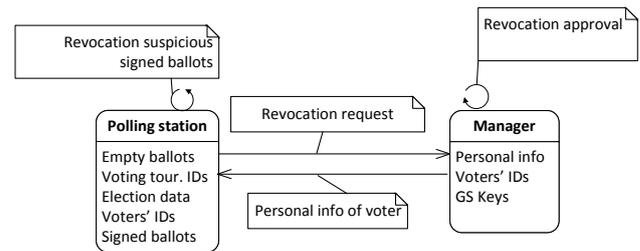


Fig. 7. Voter Revocation phase.

IV. SECURITY ANALYSIS AND EVALUATION OF OUR SOLUTION

In this section, we outline the security analysis and the performance evaluation of our solution.

A. Security Analysis

We focus on these main security requirements which are typical for e-voting systems:

- **Ballot correctness and integrity** - Only ballots connected with an election token which are correctly signed are valid. An attacker (A) who wants to modify the ballot has to recompute the group signature of the ballot and election token. The attacker must use a valid group member private key and an election token or a Voter ID. Nevertheless, the voter keeps these parameters in secret. All invalid signed ballots are discarded.
- **Election non-repudiation** - A voter who signs a filled ballot and election token by his/her valid group member private key is not able to deny this action later.

- **Duplicates elimination** - The valid signature of ballots and election tokens are stored in PS voting into a ballot-box database which contains ballots and election tokens. If a signature with the election token which has been already used is sent to PS than PS discards this newer signed ballot and the election token.
- **Ballot non-multiplicity** - The designed e-voting system generates same number ballots as the number of potential voters. The manager of the e-voting system generates and releases only one Voter ID per one voter. The Voter ID is sent to the voter by different communication channel, e.g. via encrypted SMS. The voter needs this Voter ID to obtain an election token from PS and also needs the valid group member private key. Only one valid signed ballot with the one valid election token is counted in the final result.
- **Election privacy** - Only the manager knows voter's identities. In the voting phase, voters send the group signatures that are signed behalf of the group of voters. The group signature contains election token which is connected to the Voter ID. Only PS and the voter is able to connect the election token and Voter ID. The filled ballot and the election token are encrypted by the encryption ElGamal public key. Only PS can decrypt the ballot and the election token. PS is able to detect the Voter ID from the election token, but PS is not able to determine voter identity. On the other hand, the manager is able to detect who signed the filled ballot by the revocation key and determine the voter's group signature private key which leads to the voter's identity. Nevertheless, M is not able to decrypt the encrypted and signed ballots with election tokens that are sent during the voting phase. M and other voters without the valid ElGamal decryption private key of the Polling Station are not able to decrypt signed ballots and election tokens. Then, M is not able to revoke the signed ballot without cooperation with PS. Only the cooperation of PS and M can reveal the real identity of the voter.

B. Performance Evaluation

Table I shows the cryptographic primitives used in our solution in the main phases such as Voter Join, Voting and Tallying. Voting takes one ElGamal encryption (EncEG) and one group signature signing (SigGS). Tallying takes n ElGamal decryptions (DecEG) and n verifications of the group signature (VerGS), where n is a number of signed messages. Generally, ElGamal encryption requires two exponentiations and EG decryption requires one exponentiation. Nevertheless, the number of exponentiations depends on the total length of the message m where m has to be split and converted into elements $m_i \in G$ of order q . The length of the message m depends on the size of the group signature, e.g. 2636 bits if the GS scheme [18] is used (ca. 1500 bits with the BBS04 GS scheme [19]), the size of the election token, e.g. 256 bits if SHA-256 hash is used, and the size of the ballot, e.g. 256 bits if the election has 256 candidates.

The performance of group signatures depends on the scheme which is used. For example, the signing in the GS scheme [18]

TABLE I
CRYPTOGRAPHIC PRIMITIVES USED IN OUR E-VOTING SOLUTION

Phase	VT	M	PS
Voter Join with M	TLS	TLS	-
Voter Join with PS	EncEG	-	DecEG + hash
Voting	EncEG + SigGS	-	-
Tallying	-	-	n (DecEG + VerGS)

takes 0 pairing operation (3 pairings can be precomputed) and 9 exponentiations and the verification takes 5 pairings and 10 exponentiations. Nevertheless, this GS scheme [18] supports a batch verification which reduces the pairing operations from $5 * n$ to 2.

The batch verification verifies many signatures in one process. The batch verification reduces the number of bilinear pairing operations e from $n * k$ to l , where n is the number of signatures, k is the number of bilinear pairing operations during an individual message verification, and l is the number of bilinear pairing operations during the batch verification. Equation (1) describes pairing operations in the batch, where $f_i \in G_1, h_i \in G_2, c_i \in Z_q^*$ are parameters (e.g. elements mapped in groups and the finale field of integers' modulo q) for each i signature from the total number of signatures n , and, A is a constant value which is known by a verifier and does not depend on the concrete parameters of signatures.

$$e\left(\prod_{i=1}^n f_i^{c_i}, h_i\right) = A \quad (1)$$

If all signatures are valid, then the batch verification is valid. If one signature is invalid, then the batch verification is invalid and the computational complexity of the batch verification, which is linear in case of presence n valid signatures, degrades to logarithmic. The batch must be split to two batches that are verified again separately. This procedure is performed until all invalid signatures are detected.

V. IMPLEMENTATION AND EXPERIMENTAL RESULTS

This section describes the implementation of the proposed solution and presents the performance results of main solution phases.

A. Implementation of Our E-voting Solution

The proposed solution is implemented by the JAVA programming language (JDK 1.8). The solution runs in Java Runtime Environment 8 and consists of three projects that represent system entities: Manager, Voting tourniquet and Polling station. The graphical user interfaces for Manager, Voting tourniquet, Polling station and Ballot are depicted in Fig. 8. The Manager application can add and revoke voters. The Polling Station application sets, starts and ends election events. The Voting tourniquet application enables to choose election candidates and create ballots. The Ballot form contains the ballot ID, token, time of election, and if the ballot is signed and verified correctly.

The standard cryptographic schemes and key builders are implemented by methods specified in `javax.crypto.*`, `java.security.*`. The advanced cryptographic schemes (e.g.

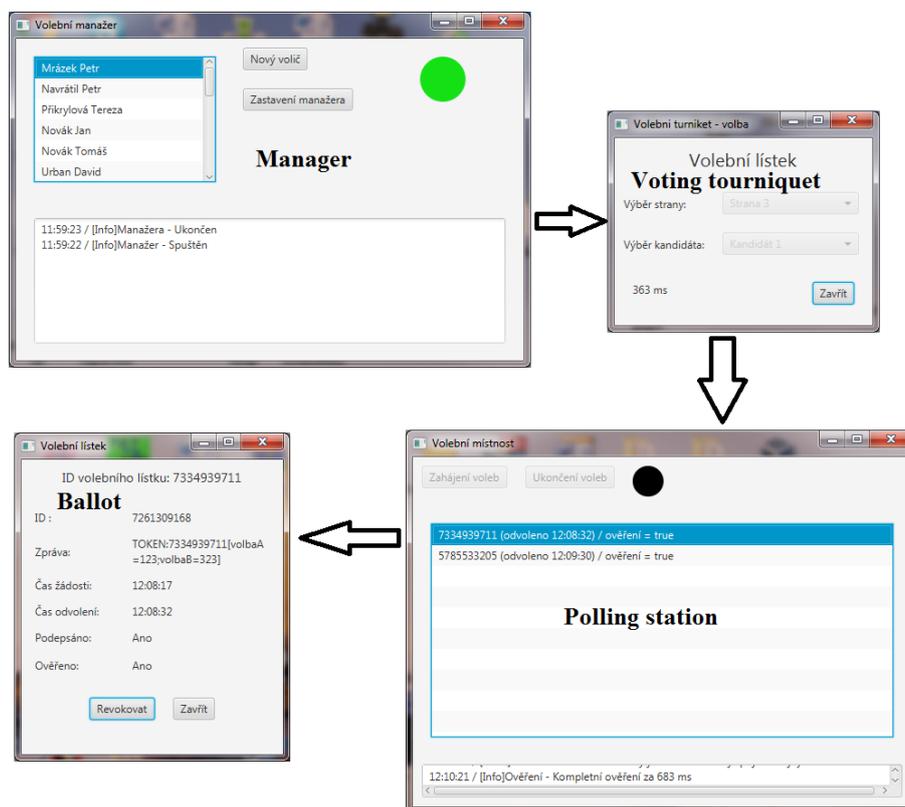


Fig. 8. Graphical user interfaces of entities during election event.

the BBS group signature scheme) are implemented by using external libraries, i.e. the bouncy castle library (available on www.bouncycastle.org) and the Java Pairing Based Cryptography (jPBC) Library (available on <http://gas.dia.unisa.it/projects/jpbc/index.html>). The implementation of the BBS scheme uses the MNT curves type D with the embedding degree $k = 6$, the 175-bit order of curves and the pre-generated parameters `d840347-175-161.param`.

B. Performance Results

We focus on main phases that are Election setup, Voting and Tallying because these parts employ the group signature scheme (BBS). The BBS scheme represents the most time and memory expensive cryptographic method that is used in our solution. The voting phase takes about 380 ms per one ballot on PC (Intel(R) Core(TM) i5-4210U CPU @ 1.7 GHz 2,4 GHz, 8 GB RAM, Windows 8.1 Pro) where the most time consuming part is the BBS group signature signing phase. The results of the BBS scheme, which is implemented and measured on smartphones in the paper [21], show that current smartphones need several seconds to generate the BBS signature. In an election event, the voter can use a smartphone to sign, encrypt and send the ballot but these devices takes several seconds only for computing one group signature.

The tallying phase is performed on the Polling Station that is simulated by PC (Intel(R) Core(TM) i5-4210U CPU @ 1.7 GHz 2,4 GHz, 8 GB RAM, Windows 8.1 Pro). The most time

consuming part of this phase is the verification phase of the BBS group signatures. The BBS verification phase takes about 430 ms without any optimization tricks.

Figure 9 shows the performance of group member key generation for n voters and the tallying phase for n ballots. The results demonstrate that the proposed solution is practical for small (up to hundreds members) and medium (up to several thousands members) groups of voters because the tallying of 10 ballots takes about 2.6 s and the tallying of 1000 ballots takes about 4 minutes which is reasonable time in practice during an election event. We assume that servers for counting and verifying ballots can be more powerful than used PC in order to improve the performance of the tallying phase. Moreover, the verification process of group signatures can be optimized by several tricks, e.g. precomputation, batch verification, that are studied in [21], [22] and [23].

During the Election Setup phase, group member keys used by voters have to be generated in a practical time. The results show that the key generation takes about 1.5 s for 10 voters and about 38.4 s for 1000 voters.

VI. CONCLUSION

In this paper, we present the electronic voting solution which provides secure elections and keeps the user privacy. Our solution is based on group signature schemes that ensures non-repudiation, integrity and authenticity and ElGamal encryption ensures the confidentiality of the ballots. The performance of voting and tallying phases depends mainly on the group signature scheme. The implementation of the proposed

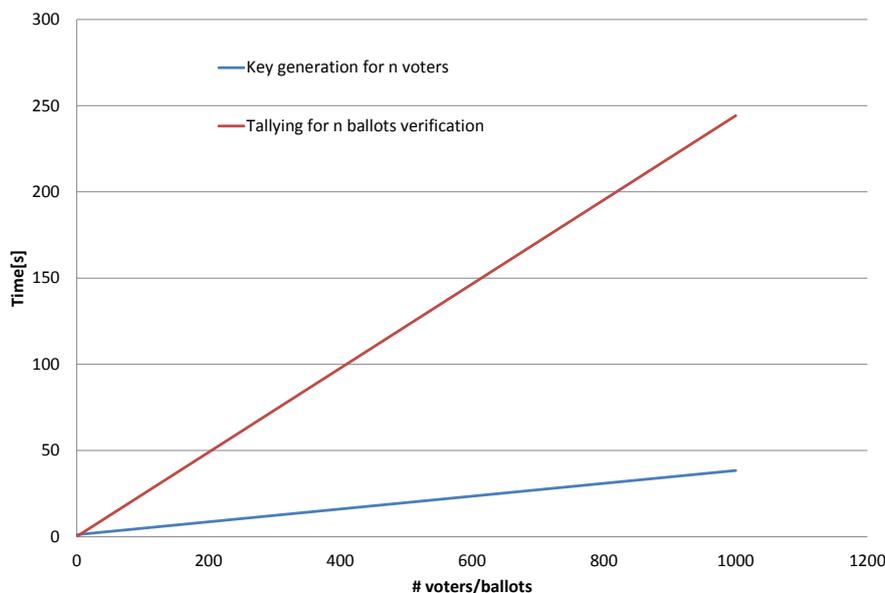


Fig. 9. Performance of group member key generation and the tallying phase.

solution with the BBS group signature scheme demonstrates that the performance results are practical on current PCs if the number of voters and ballots are from hundreds to thousands. Nevertheless, the proposed e-voting solution can use a different group signature scheme that can be more efficient than the BBS scheme. Verifying the signed ballots can be optimized by employing the group signature scheme that supports the batch verification. These optimization tricks can improve the performance of the tallying phase that runs in the polling station.

REFERENCES

- [1] J. Budurushi and M. Volkamer, "Feasibility analysis of various electronic voting systems for complex elections," in *Conference for E-Democracy and Open Government*, 2014, p. 141.
- [2] Ü. Madise and T. Martens, "E-voting in estonia 2005. the first practice of country-wide binding internet voting in the world," *Electronic Voting*, vol. 86, 2006.
- [3] L. Malina, J. Smrz, J. Hajny, and K. Vrba, "Secure electronic voting based on group signatures," in *Telecommunications and Signal Processing (TSP), 2015 38th International Conference on*. IEEE, 2015, pp. 6–10.
- [4] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, vol. 24, no. 2, pp. 84–90, 1981.
- [5] B. Schoenmakers, "A simple publicly verifiable secret sharing scheme and its application to electronic voting," in *Advances in Cryptology-CRYPTO99*. Springer, 1999, pp. 148–164.
- [6] B. L. K. Kim, "Receipt-free electronic voting through collaboration of voter and honest verifier," 2000.
- [7] C. A. Neff, "A verifiable secret shuffle and its application to e-voting," in *Proceedings of the 8th ACM conference on Computer and Communications Security*. ACM, 2001, pp. 116–125.
- [8] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, ser. WPES '05. New York, NY, USA: ACM, 2005, pp. 61–70. [Online]. Available: <http://doi.acm.org/10.1145/1102199.1102213>
- [9] M. Hirt and K. Sako, "Efficient receipt-free voting based on homomorphic encryption," in *Advances in CryptologyEUROCRYPT 2000*. Springer, 2000, pp. 539–556.
- [10] I. Damgård, M. Jurik, and J. B. Nielsen, "A generalization of pailliers public-key system with applications to electronic voting," *International Journal of Information Security*, vol. 9, no. 6, pp. 371–385, 2010.
- [11] C.-L. Chen, Y.-Y. Chen, J.-K. Jan, and C.-C. Chen, "A secure anonymous e-voting system based on discrete logarithm problem," *Appl. Math*, vol. 8, no. 5, pp. 2571–2578, 2014.
- [12] D. G. Nair, V. P. Binu, and G. Santhosh Kumar, "An improved e-voting scheme using secret sharing based secure multi-party computation," 2014.
- [13] N. Braun and D. Brändli, "Swiss e-voting pilot projects: Evaluation, situation analysis and how to proceed," *Electronic Voting*, vol. 86, pp. 27–36, 2006.
- [14] D. Chaum, P. Y. Ryan, and S. Schneider, *A practical voter-verifiable election scheme*. Springer, 2005.
- [15] J. Helbach, J. Schwenk, and S. Schäge, "Code voting with linkable group signatures," in *Electronic Voting*, 2008, pp. 209–208.
- [16] S. Kremer, M. Ryan, and B. Smyth, *Election verifiability in electronic voting protocols*. Springer, 2010.
- [17] E. Cuvelier, O. Pereira, and T. Peters, "Election verifiability or ballot privacy: Do we need to choose?" in *Computer Security-ESORICS 2013*. Springer, 2013, pp. 481–498.
- [18] L. Malina, A. Vives-Guasch, J. Castellà-Roca, A. Viejo, and J. Hajny, "Efficient group signatures for privacy-preserving vehicular networks," *Telecommunication Systems*, pp. 1–19, 2014.
- [19] D. Boneh, X. Boyen, and H. Shacham, "Short group signatures," in *Advances in Cryptology-CRYPTO 2004*. Springer, 2004, pp. 41–55.
- [20] L. Malina and J. Hajny, "Efficient security solution for privacy-preserving cloud services," in *Telecommunications and Signal Processing (TSP), 2013 36th International Conference on*. IEEE, 2013, pp. 23–27.
- [21] L. Malina, J. Hajny, and V. Zeman, "Usability of pairing-based cryptography on smartphones," in *Telecommunications and Signal Processing (TSP), 2015 38th International Conference on*. IEEE, 2015, pp. 617–621.
- [22] A. L. Ferrara, M. Green, S. Hohenberger, and M. Ø. Pedersen, "Practical short signature batch verification," in *Topics in Cryptology-CT-RSA 2009*. Springer, 2009, pp. 309–324.
- [23] L. Malina, J. Hajny, and V. Zeman, "Trade-off between signature aggregation and batch verification," in *Telecommunications and Signal Processing (TSP), 2013 36th International Conference on*. IEEE, 2013, pp. 57–61.

Evaluation of Responses in MTL Model Excited from Multiple Stochastic Sources

Lubomír Brančík, and Edita Kolářová

Abstract—The paper presents a technique for simulation of stochastic responses and their statistical characteristics in multiconductor transmission lines (MTL). The method follows a theory of stochastic differential equations (SDE) and relevant numerical techniques for their solution. The MTL's model, formed via generalized Π sections in cascade, is designed to cover various situations at stochastic and/or deterministic excitations. In this way both the noisy pulses driving MTL's terminal ports and effects of possible unwanted disturbances along the MTL's wires are allowed to be simulated. First the state-variable method is applied to derive a deterministic description, then voltage stochastic variations are incorporated to define the vector linear SDE. To obtain the characteristics of stochastic responses, firstly the set of trajectories is statistically processed, while a weak stochastic backward Euler scheme, consistent with the Itô stochastic calculus, is applied. Finally, a method of direct calculation of variances, based on the solution of relevant Lyapunov-like differential equations, is used with advantage. All the simulations were performed in the Matlab language environment.

Keywords—Multiconductor transmission line, state variable, stochastic differential equation, stochastic source.

I. INTRODUCTION

The techniques based on stochastic differential equations (SDE) find their place in many fields of engineering where stochastic influences are relevant to be considered [1]–[3]. In the electrical engineering SDE approach has been used in many various fields, see at least [4]–[6]. An interesting application is to simulate stochastic responses in systems with distributed parameters like e.g. transmission lines (TL), often used in high-speed electronic systems [7]–[9]. Both internal structural noises and possible external disturbances can be covered. In former papers the SDE approach was applied for TL systems in which the external drivings were only possible from TLs' terminating ports [10]–[12]. In [13] a possibility to consider multiple external random sources is proposed, however, only for the single TLs. In this paper an extension of this approach is done towards MTL's model as shown in Fig. 1, where the excitations are allowed in any node. Such a model can be used to simulate effects of unwanted random disturbances along the MTL wires, for

example [14]. To formulate a basic SDE system description a state-variable method is applied on the MTL's generalized RLCG-based model, and generalized Thévenin equivalents are utilized to join the sources to respective nodes [15]. In Fig. 1, non-deterministic voltage vectors are marked by asterisks, but various combinations are allowed. A task is to find the statistical characteristics of the stochastic responses: the expectation and the standard deviation. Hence a weak stochastic backward Euler scheme is used for the numerical solution of the SDEs, which utilizes two-point distributed random variables as initial stochastic processes [2], [3]. In addition to [14], direct calculation of variances of stochastic responses is performed, utilizing Lyapunov-like differential and algebraic matrix equations [16], [17]. All methods were programmed in the Matlab language environment.

II. DETERMINISTIC MODEL FORMULATION

We will consider MTL, nonuniform in general, defined by its length l and per-unit-length (p.u.l.) matrices $\mathbf{L}_0(x)$, $\mathbf{C}_0(x)$, $\mathbf{R}_0(x)$ and $\mathbf{G}_0(x)$ of the order $n \times n$, with n as a number of active conductors. In the MTL m -sectional lumped-parameter model in Fig. 1, the voltage vectors \mathbf{v}_k , $k = 1, \dots, m+1$, and the current vectors \mathbf{i}_k , $k = 1, \dots, m$, are the $n \times 1$ vectors of the state variables in view. The model lumped parameters are set by matrices $\mathbf{L}_k = \mathbf{L}_0(x_k + \Delta x/2)\Delta x$, $\mathbf{C}_k = \mathbf{C}_0(x_k)\Delta x$, $\mathbf{R}_k = \mathbf{R}_0(x_k + \Delta x/2)\Delta x$ and $\mathbf{G}_k = \mathbf{G}_0(x_k)\Delta x$, with $\Delta x = l/m$ [10]. The border shunt elements, \mathbf{C}_1 , \mathbf{G}_1 , and \mathbf{C}_{m+1} , \mathbf{G}_{m+1} , are taken half-size to ensure the model to be a cascade connection of generalized Π networks of the same type. The current vectors of external sources are determined by $\mathbf{i}_{ik} = \mathbf{G}_{ik}(\mathbf{v}_{ik} - \mathbf{v}_k)$, where the internal Thévenin matrices are supposed as regular, i.e. $\mathbf{G}_{ik} = \mathbf{R}_{ik}^{-1}$ exists.

A state-variable description of the MTL model in Fig. 1, first with all the parameters deterministic (excitation voltage vectors \mathbf{v}_{ik}^* replaced by \mathbf{v}_{ik}) can be written as

$$\mathbf{M} \frac{d\mathbf{x}(t)}{dt} = -(\mathbf{H} + \mathbf{P})\mathbf{x}(t) + \mathbf{P}\mathbf{u}(t) \quad (1)$$

with terms as follows. The vector of state variables

$$\mathbf{x}(t) = \begin{bmatrix} \mathbf{v}_C(t) \\ \mathbf{i}_L(t) \end{bmatrix} \quad (2)$$

contains $n(2m+1)$ elements grouped to $n \times 1$ column vectors, namely $\mathbf{v}_C(t)$ holds $m+1$ vectors of state voltages and $\mathbf{i}_L(t)$ holds m vectors of state currents. The matrix

$$\mathbf{M} = \text{diag}(\mathbf{C}, \mathbf{L}) \quad (3)$$

holds the block diagonal matrices $\mathbf{C} = \text{diag}(\mathbf{C}_1, \mathbf{C}_2, \dots, \mathbf{C}_{m+1})$, $\mathbf{L} = \text{diag}(\mathbf{L}_1, \mathbf{L}_2, \dots, \mathbf{L}_m)$, and zero matrices $\mathbf{0}$. The matrix

Manuscript received November 22, 2015, revised January 23, 2016. This work was supported by Czech Science Foundation under grant 15-18288S "Research of Signal Integrity at High-Speed Interconnects". For research, infrastructure of the SIX Center was used.

L. Brančík is with the Department of Radio Electronics, Brno University of Technology, Technická 12, 616 00 Brno, Czech Republic (phone: +420 541146563; fax: +420 541146596; e-mail: brancik@feec.vutbr.cz).

E. Kolářová is with the Department of Mathematics, Brno University of Technology, Technická 8, 616 00 Brno, Czech Republic (e-mail: kolara@feec.vutbr.cz).

doi: 10.11601/ijates.v5i1.145

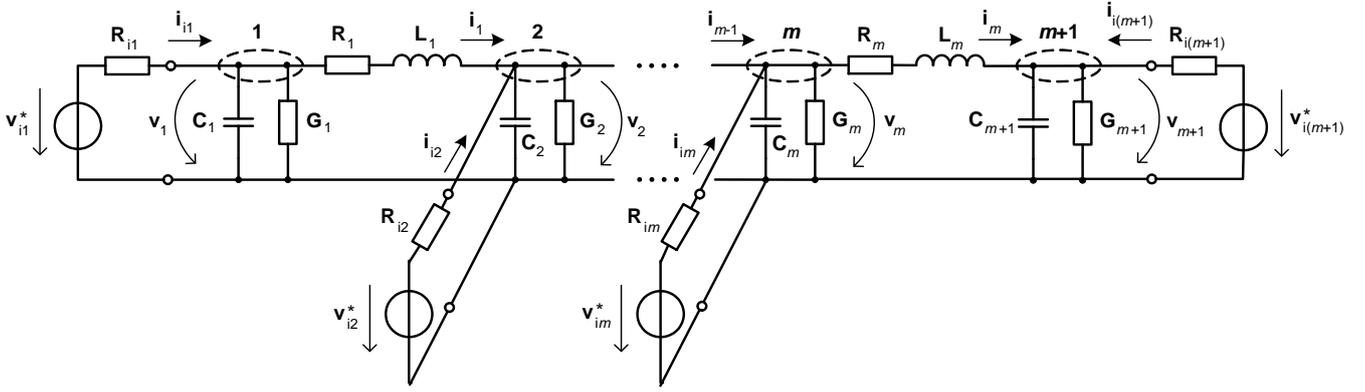


Fig. 1. Schematic representation of MTL model excited from stochastic sources.

$$\mathbf{H} = \begin{bmatrix} \mathbf{G} & \mathbf{E} \\ -\mathbf{E}^T & \mathbf{R} \end{bmatrix} \quad (4)$$

is similarly created by the matrices $\mathbf{G} = \text{diag}(\mathbf{G}_1, \mathbf{G}_2, \dots, \mathbf{G}_{m+1})$, $\mathbf{R} = \text{diag}(\mathbf{R}_1, \mathbf{R}_2, \dots, \mathbf{R}_m)$, and a block matrix \mathbf{E} containing the identity matrices $\pm \mathbf{I}$ and zero matrices $\mathbf{0}$, see [10] for details. The matrix

$$\mathbf{P} = \begin{bmatrix} \mathbf{Y}_I & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{bmatrix} \quad (5)$$

depends on external circuits and contains the block diagonal submatrix $\mathbf{Y}_I = \text{diag}(\mathbf{G}_{i1}, \mathbf{G}_{i2}, \dots, \mathbf{G}_{i(m+1)})$. The drive vector

$$\mathbf{u}(t) = \begin{bmatrix} \mathbf{v}_1(t) \\ \mathbf{0} \end{bmatrix} \quad (6)$$

contains the subvector $\mathbf{v}_1(t) = [\mathbf{v}_{i1}^T(t), \mathbf{v}_{i2}^T(t), \dots, \mathbf{v}_{i(m+1)}^T(t)]^T$. If we introduce denotations

$$\mathbf{A} = -\mathbf{M}^{-1}(\mathbf{H} + \mathbf{P}), \quad \mathbf{B} = \mathbf{M}^{-1}\mathbf{P} \quad (7)$$

then (1) can be written

$$\frac{d\mathbf{x}(t)}{dt} = \mathbf{A}\mathbf{x}(t) + \mathbf{B}\mathbf{u}(t) \quad (8)$$

with a formal solution

$$\mathbf{x}(t) = e^{\mathbf{A}t} \mathbf{x}(0) + \int_0^t e^{\mathbf{A}(t-\tau)} \mathbf{B}\mathbf{u}(\tau) d\tau \quad (9)$$

if $t = 0$ is chosen as a beginning of the time interval of interest.

III. MODEL WITH STOCHASTIC EXCITATIONS

In this section the Itô stochastic calculus [1] is applied to get responses to the input sources influenced by stochastic processes. Instead of $\mathbf{v}_{ik}(t)$, used in the deterministic solution above, stochastic versions of the voltage vectors are used as

$$\mathbf{v}_{ik}^*(t) = \mathbf{v}_{ik}(t) + \boldsymbol{\alpha}_k \boldsymbol{\xi}_k(t) \quad (10)$$

$k = 1, 2, \dots, m+1$, where $\boldsymbol{\xi}_k(t) = [\zeta_{k1}(t), \zeta_{k2}(t), \dots, \zeta_{kn}(t)]^T$ are noise vectors whose elements $\zeta_{kl}(t)$ represent white noise processes (related to the l -th wire of the MTL, and the k -th section of its model), and $\boldsymbol{\alpha}_k = \text{diag}(\alpha_{k1}, \alpha_{k2}, \dots, \alpha_{kn})$ are constant matrices whose elements α_{kl} express intensities of respective noises. Then, taking into account (6) and (10), (8) can be rewritten as

$$\frac{d\mathbf{x}(t)}{dt} = \mathbf{A}\mathbf{x}(t) + \mathbf{B}(\mathbf{u}(t) + \delta\mathbf{u}(t)) \quad (11)$$

where

$$\delta\mathbf{u}(t) = \begin{bmatrix} \delta\mathbf{v}_1(t) \\ \mathbf{0} \end{bmatrix} = \begin{bmatrix} \boldsymbol{\alpha}\boldsymbol{\xi}(t) \\ \mathbf{0} \end{bmatrix} \quad (12)$$

with a noise intensity matrix $\boldsymbol{\alpha} = \text{diag}(\boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \dots, \boldsymbol{\alpha}_{m+1})$, and a stochastic processes vector $\boldsymbol{\xi}(t) = [\xi_1^T(t), \xi_2^T(t), \dots, \xi_{m+1}^T(t)]^T$.

A method of converting the differential equation (11) on its stochastic version lies in multiplying it by dt , and replacing all the products $\zeta_{kl}(t)dt$ by $dW_{kl}(t)$, with $W_{kl}(t)$ designating Wiener processes [1]. By this the vector linear SDE with additive noises is formulated

$$d\mathbf{X}(t) = (\mathbf{A}\mathbf{X}(t) + \mathbf{B}\mathbf{u}(t))dt + d\mathbf{b}_W(t) \quad (13)$$

where $d\mathbf{b}_W(t)$ arises from (11) and (12), namely

$$\begin{aligned} d\mathbf{b}_W(t) &= \mathbf{B} \begin{bmatrix} \boldsymbol{\alpha} d\mathbf{W}(t) \\ \mathbf{0} \end{bmatrix} = \mathbf{B} \sum_{k=1}^{m+1} \sum_{l=1}^n \begin{bmatrix} \boldsymbol{\alpha}^{(p)} \\ \mathbf{0} \end{bmatrix} dW_{kl}(t) = \\ &= \sum_{k=1}^{m+1} \sum_{l=1}^n \mathbf{b}^{(p)} dW_{kl}(t) \end{aligned} \quad (14)$$

with $\boldsymbol{\alpha}^{(p)}$ denoting the p -th column of the noise intensity matrix $\boldsymbol{\alpha}$, while $p = n(k-1) + l$, and $d\mathbf{W}(t)$ containing differentials of Wiener processes.

It is common to mark stochastic solutions by capital letters to distinguish them from deterministic ones, like $\mathbf{X}(t)$ vs. $\mathbf{x}(t)$ in (13) and (8), respectively. Considering a multidimensional Itô formula and marking in (14), the SDE (13) has a solution

$$\begin{aligned} \mathbf{X}(t) &= e^{\mathbf{A}t} \mathbf{X}(0) + \int_0^t e^{\mathbf{A}(t-\tau)} \mathbf{B}\mathbf{u}(\tau) d\tau + \\ &+ \sum_{k=1}^{m+1} \sum_{l=1}^n \int_0^t e^{\mathbf{A}(t-\tau)} \mathbf{b}^{(p)} dW_{kl}(\tau) \end{aligned} \quad (15)$$

with $\mathbf{b}^{(p)}$ defined in (14), while $p = n(k-1) + l$. The right terms in (15) are called Itô integrals. The solution $\mathbf{X}(t)$ is a random process and for its expectation we have for $t > 0$

$$E[\mathbf{X}(t)] = e^{\mathbf{A}t} E[\mathbf{X}(0)] + \int_0^t e^{\mathbf{A}(t-\tau)} \mathbf{B}\mathbf{u}(\tau) d\tau \quad (16)$$

as expectations of the Itô integrals are zero. It is evident that for a constant initial value $\mathbf{X}(0)$ the expectation of a stochastic solution agrees with the deterministic solution (9).

IV. APPLICATION OF NUMERICAL METHODS

A. Stochastic Backward Differentiation Formulae

When considering a numerical technique from the theory of ordinary differential equations (ODE) some care is needed as according to the definition of the Itô integral a stochastic integral must always be evaluated at lower endpoint of the discretization interval. To solve SDEs we can utilize the stochastic backward Euler scheme [2], consistent with the Itô stochastic calculus, and sufficiently stable for higher-order circuits represented by the MTL's model.

Let us consider the solution $\mathbf{X}(t)$ on the interval $t_0 \leq t \leq T$, with respect to an equidistant discretization $t_r = t_0 + rh$, where $h = (T - t_0)/N = t_{r+1} - t_r$, $r = 0, \dots, N-1$, and with the discretization of the Wiener processes $\Delta W_{kl}^{(r)} = W_{kl}(t_{r+1}) - W_{kl}(t_r) = \int_{t_r}^{t_{r+1}} dW_{kl}(\tau)$. To use a stochastic numerical scheme, random increments of the Wiener processes should be generated as the independent Gaussian random variables, while $E[\Delta W_{kl}^{(r)}] = 0$ and $E[(\Delta W_{kl}^{(r)})^2] = h$. Subsequently, the stochastic backward Euler scheme for solving (13) can be written as

$$\begin{aligned} \mathbf{X}^{(r+1)} &= (\mathbf{I} - \mathbf{A}h)^{-1} (\mathbf{X}^{(r)} + \mathbf{B}\mathbf{u}^{(r+1)}h + \Delta \mathbf{b}_w^{(r)}) = \\ &= (\mathbf{I} - \mathbf{A}h)^{-1} \left(\mathbf{X}^{(r)} + \mathbf{B}\mathbf{u}^{(r+1)}h + \sum_{k=1}^{m+1} \sum_{l=1}^n \mathbf{b}^{(p)} \Delta W_{kl}^{(r)} \right) \end{aligned} \quad (17)$$

where $p = n(k-1) + l$. The solution (17) is one with a strong convergence, and it is useful when the individual stochastic trajectories are important. Our problem does not require good pathwise approximations but only the approximations of the expectations $\mu_{kl} = E[X_{kl}]$ and the standard deviations $\sigma_{kl} = \sqrt{E[(X_{kl} - \mu_{kl})^2]}$ of the SDE solutions. Therefore, we can apply a weak version of (17), where the increments of the Wiener processes $\Delta W_{kl}^{(r)}$ are replaced by simpler, two-point distributed random variables $\Delta \widehat{W}_{kl}^{(r)}$, while the probability $P(\Delta \widehat{W}_{kl}^{(r)} = \pm \sqrt{h}) = 1/2$. The numerical efficiency of the weak scheme is generally better than of the strong one [2], [3].

B. Estimates of Statistical Characteristics

For the vector linear SDE with additive noises, like (13), a resultant stochastic process $\mathbf{X}(t)$ has the multivariate normal distribution [2], [3]. We are not going to study any correlations, so we can use the usual procedure to determine confidence intervals for individual items $X_{kl}(t)$, based on the Student's t -distribution [2], [18]. Taking into account a sole item of interest, and marking $X_{kl}^{(r)} = X_{kl}(t_r)$, as in (17), the sample mean and sample standard deviation are respectively determined via all J realizations by the formulae [19]

$$\bar{X}_{kl}^{(r)} = \frac{1}{J} \sum_{j=1}^J X_{kl,j}^{(r)} \quad (18)$$

$$s_{kl}^{(r)} = \sqrt{\frac{1}{J-1} \sum_{j=1}^J (X_{kl,j}^{(r)} - \bar{X}_{kl}^{(r)})^2} \quad (19)$$

for $r = 0, \dots, N-1$ to cover whole time interval. Then, based on a Student's t -distribution with $J-1$ degrees of freedom, a two-sided $100(1-\alpha)\%$ confidence interval (related to individual trajectories) is determined as

$$\left(\bar{X}_{kl}^{(r)} - t_{1-\alpha/2, J-1} s_{kl}^{(r)}, \bar{X}_{kl}^{(r)} + t_{1-\alpha/2, J-1} s_{kl}^{(r)} \right) \quad (20)$$

In case we need confidence interval for sample mean it can be got from (20) by replacing $s_{kl}^{(r)}$ with $s_{kl}^{(r)}/\sqrt{J}$.

C. Expectation and Variance Direct Computations

As was mentioned above, when considering in (16) constant initial conditions $\mathbf{X}(0)$, the expectation $\boldsymbol{\mu}(t) = E[\mathbf{X}(t)]$ of the stochastic responses $\mathbf{X}(t)$ follows respective deterministic solution (9), namely

$$\frac{d\boldsymbol{\mu}(t)}{dt} = \mathbf{A}\boldsymbol{\mu}(t) + \mathbf{B}\mathbf{u}(t) \quad (21)$$

To enable forming confidence intervals the variances of stochastic processes are needed. As is known, the variances $D_k(t) = \sigma_k^2(t) = \text{var}(X_k(t))$, $k = 1, \dots, n(2m+1)$, with $\sigma_k(t)$ as the standard deviation, are diagonal elements of the covariance matrix $\boldsymbol{\Sigma}(t) = \text{cov}(\mathbf{X}(t))$ of respective random vector $\mathbf{X}(t) = [X_1(t), \dots, X_{n(2m+1)}(t)]^T$. It is valid [19]

$$\begin{aligned} \boldsymbol{\Sigma}(t) &= E \left[(\mathbf{X}(t) - \boldsymbol{\mu}(t)) (\mathbf{X}(t) - \boldsymbol{\mu}(t))^T \right] = \\ &= E \left[\mathbf{X}(t) \mathbf{X}(t)^T \right] - \boldsymbol{\mu}(t) \boldsymbol{\mu}(t)^T \end{aligned} \quad (22)$$

If we now designate $\mathbf{Q}(t) = E[\mathbf{X}(t) \mathbf{X}(t)^T]$, then taking into account (13) and (14), and following the theory in [3], $\mathbf{Q}(t)$ satisfies the Lyapunov-like matrix ODE

$$\begin{aligned} \frac{d\mathbf{Q}(t)}{dt} &= \mathbf{A}\mathbf{Q}(t) + \mathbf{Q}(t)\mathbf{A}^T + \mathbf{B}\mathbf{u}(t)\boldsymbol{\mu}(t)^T + \\ &+ \boldsymbol{\mu}(t)(\mathbf{B}\mathbf{u}(t))^T + \sum_{k=1}^{m+1} \sum_{l=1}^n \mathbf{b}^{(p)} \mathbf{b}^{(p)T} \end{aligned} \quad (23)$$

with $p = n(k-1) + l$, and the expectation $\boldsymbol{\mu}(t)$ in (21). To solve (21), a backward Euler scheme is used, with a time step h , as

$$\boldsymbol{\mu}^{(r+1)} = (\mathbf{I} - \mathbf{A}h)^{-1} \cdot (\boldsymbol{\mu}^{(r)} + \mathbf{B}\mathbf{u}^{(r+1)}h) \quad (24)$$

To solve (23), the same numerical scheme leads to the Lyapunov-like matrix equation [20]

$$\begin{aligned} (\mathbf{I} - \mathbf{A}h)\mathbf{Q}^{(r+1)} - \mathbf{Q}^{(r+1)}\mathbf{A}^T h &= \mathbf{Q}^{(r)} + \\ + \left(\mathbf{B}\mathbf{u}^{(r+1)}\boldsymbol{\mu}^{(r+1)T} + \boldsymbol{\mu}^{(r+1)}(\mathbf{B}\mathbf{u}^{(r+1)})^T + \sum_{k=1}^{m+1} \sum_{l=1}^n \mathbf{b}^{(p)} \mathbf{b}^{(p)T} \right) h \end{aligned} \quad (25)$$

where $\boldsymbol{\mu}^{(r+1)}$ is given by (24), with the same step h , and being resolved for $\mathbf{Q}^{(r+1)}$, e.g. by using an alternating-direction-implicit (ADI) iteration [17]. Then, designating $\mathbf{V} = \mathbf{I} - \mathbf{A}h$, $\mathbf{W} = -\mathbf{A}^T h$, and $\mathbf{F}^{(r+1)}$ as the right side of (25), we solve in each time step, $r = 0, 1, \dots$, a matrix equation

$$\mathbf{V}\mathbf{Q}^{(r+1)} + \mathbf{Q}^{(r+1)}\mathbf{W} = \mathbf{F}^{(r+1)} \quad (26)$$

by ADI iterations

$$(\mathbf{V} + p_j \mathbf{I})\mathbf{Q}_{j-1/2}^{(r+1)} = \mathbf{F}^{(r+1)} - \mathbf{Q}_{j-1}^{(r+1)} (\mathbf{W} - p_j \mathbf{I}) \quad (27)$$

$$\mathbf{Q}_j^{(r+1)} (\mathbf{W} + q_j \mathbf{I}) = \mathbf{F}^{(r+1)} - (\mathbf{V} - q_j \mathbf{I})\mathbf{Q}_{j-1/2}^{(r+1)} \quad (28)$$

$J = 1, 2, \dots$, and $\mathbf{Q}_0^{(r+1)} = \mathbf{Q}^{(r)}$. The coefficients p_j and q_j can be used to improve the speed of convergence, in following examples, they are set to $p_j = q_j = 1$.

Due to a normality of the resultant stochastic processes, the $100(1 - \alpha) \%$ confidence interval is given by

$$\left(\mu_{kl}^{(r)} - u_{1-\alpha/2} \sigma_{kl}^{(r)}, \mu_{kl}^{(r)} + u_{1-\alpha/2} \sigma_{kl}^{(r)} \right) \quad (29)$$

with $u_{1-\alpha/2}$ as a quantile of a standard normal distribution.

V. SIMULATION EXAMPLES IN MATLAB

A. Introductory Example - Single TL

To better explain crossing to multiconductor transmission line (MTL) models, an introductory single TL, i.e. $n = 1$, will first be considered. In this case, all variables are scalars instead of column vectors and square matrices. Besides, a possibility to utilize two-point random variables as initial stochastic process to estimate confidence interval will be verified, as well as computation of variances via Lyapunov-like ODEs and corresponding numerical technique.

Thus, let us consider TL of the length $l = 0.2$ m, with per-unit-length parameters $L_0 = 494.6$ nH/m, $C_0 = 62.8$ pF/m, $R_0 = 0.1$ Ω /m and $G_0 = 0.1$ S/m [21], whose model is composed of $m = 128$ parts. First, all voltages are set zero, i.e. $v_{ik}^*(t) = 0$, $k = 2, \dots, m+1$, except $v_{i1}^*(t) = v_S(t) + \alpha_1 \xi_1(t)$, with $\alpha_1 = 10^{-6}$, which excites a left port, while $v_S(t)$ is a 1 V trapezoidal pulse with 0.5 ns rise/fall times and 3 ns width. A source resistance $R_{i1} = R_S = 5$ Ω , and a load resistance $R_{i129} = R_L = 10$ k Ω . As no excitation sources are now connected along the TL model, remaining resistances $R_{ik} \rightarrow \infty$, $k = 2, \dots, m$. Results of these simulations are in Figs. 2 and 3 for both terminal ports.

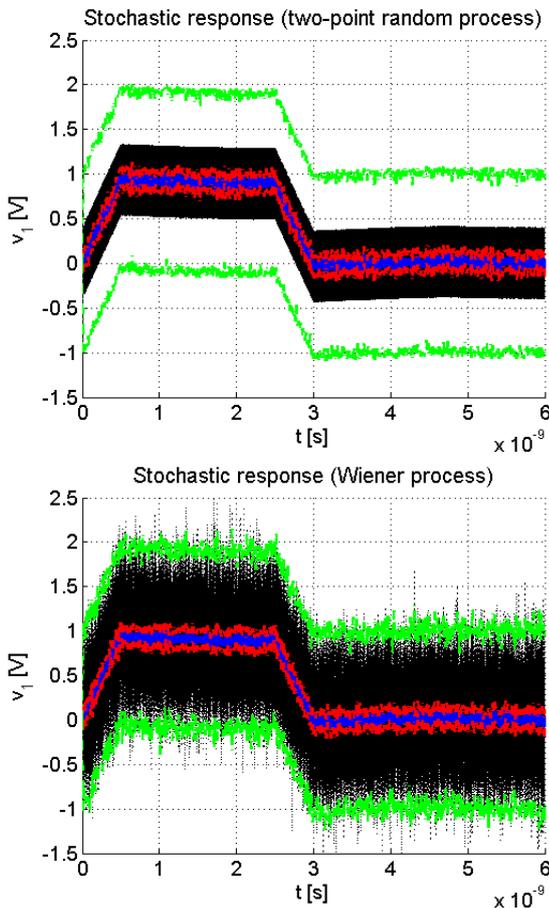


Fig. 2. Comparison of different initial stochastic processes (input port).

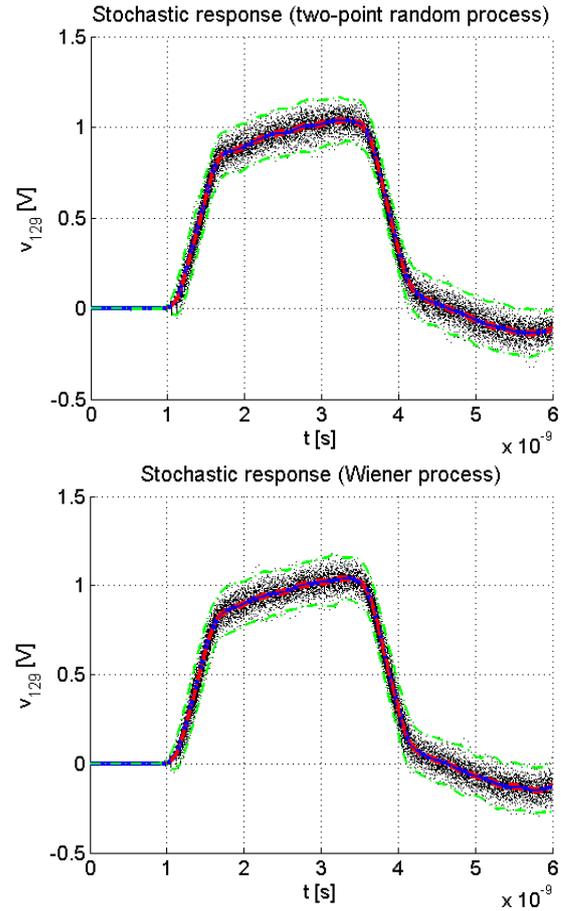


Fig. 3. Comparison of different initial stochastic processes (output port).

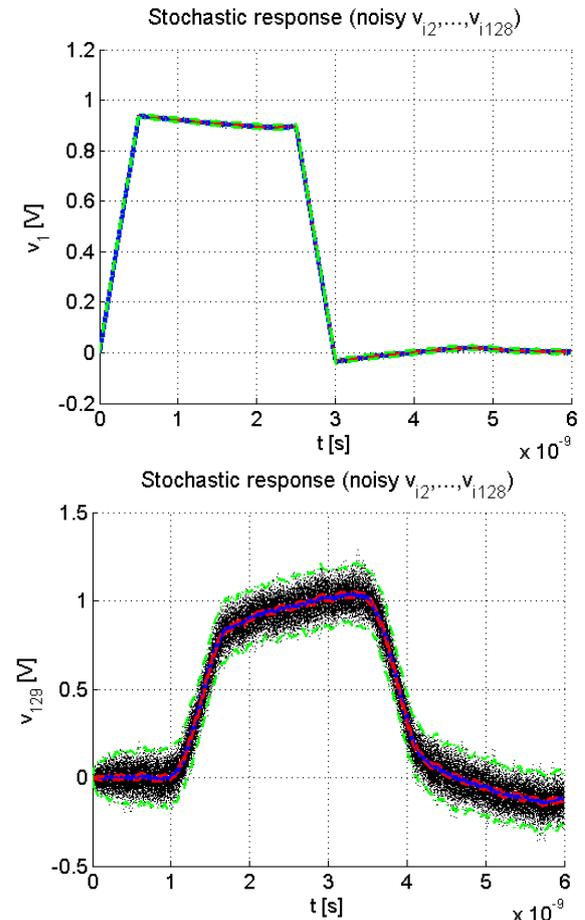


Fig. 4. Responses influenced by random disturbances along the TL.

At the model's left port in Fig. 2, differences at individual stochastic trajectories (black) are strong due to nearness of the excitation source. However, it is also evident, that confidence intervals are very similar (here 99 %, computed from 100 samples, red for sample means, green for individual samples). At the right port in Fig. 3, there is no notable difference in a character of stochastic trajectories. In light of estimate of confidence interval both the processes are well exchangeable, cp. theory in [2].

The other example in Fig. 4 considers an input voltage $v_{i1}^*(t) = v_S(t)$ as deterministic, with the same resistances at the left and right ports, however, the remaining sources are stochastic, namely $v_{ik}^*(t) = \alpha_k \zeta_k(t)$, with $\alpha_k = 10^{-3}$, and the resistances $R_{ik} = 1 \text{ M}\Omega$, $k = 2, \dots, m$. As excitation voltages are exclusively stochastic, i.e. without deterministic parts, random disturbances along the TL can e.g. be covered in this way.

B. Simulation of Simple MTL

As an example of the simulation of stochastic responses on the MTL, the uniform (2+1)-conductor TL terminated with resistive elements is considered in Fig. 5 [14].

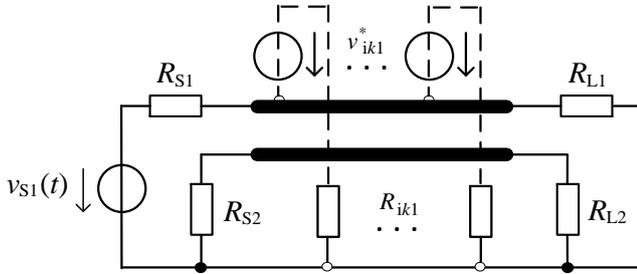


Fig. 5. MTL system with stochastic excitations v_{ik1}^* .

The MTL has the length $l = 0.4 \text{ m}$, and is characterized by p.u.l. parameters [21]

$$\mathbf{R}_0 = \begin{bmatrix} 0.1 & 0.02 \\ 0.02 & 0.1 \end{bmatrix} \Omega/\text{m}, \quad \mathbf{L}_0 = \begin{bmatrix} 494.6 & 63.3 \\ 63.3 & 494.6 \end{bmatrix} \text{ nH}/\text{m} \quad (30)$$

$$\mathbf{G}_0 = \begin{bmatrix} 0.1 & -0.01 \\ -0.01 & 0.1 \end{bmatrix} \text{ S}/\text{m}, \quad \mathbf{C}_0 = \begin{bmatrix} 62.8 & -4.9 \\ -4.9 & 62.8 \end{bmatrix} \text{ pF}/\text{m}$$

The MTL's model is composed of $m = 50$ sections, and due to the uniformity, its parameters follow (30) multiplied by l/m . The parameters of Thévenin models at terminal ports, $\mathbf{R}_S = \text{diag}(R_{S1}, R_{S2})$, $\mathbf{R}_L = \text{diag}(R_{L1}, R_{L2})$, $\mathbf{v}_S(t) = [v_{S1}(t), 0]^T$, and $\mathbf{v}_L(t) = [0, 0]^T$, correspond to those of the MTL model in Fig. 1, i.e. \mathbf{R}_{i1} , \mathbf{R}_{i51} , $\mathbf{v}_{i1}(t)$, and $\mathbf{v}_{i51}(t)$, respectively, while $R_{S1} = R_{S2} = 5 \Omega$, $R_{L1} = R_{L2} = 10 \text{ k}\Omega$, and the excitation voltage $v_{S1}(t) = \sin^2(\pi t / 2 \cdot 10^{-9})$ if $0 \leq t \leq 2 \cdot 10^{-9} \text{ s}$, and $v_{S1}(t) = 0$ otherwise. The MTL's first wire is excited from stochastic sources, as is schematically sketched by dash lines in Fig. 5. The voltage vectors $\mathbf{v}_{ik}^*(t) = [v_{ik1}^*(t), 0]^T$, with $v_{ik1}^*(t) = \alpha_k \zeta_k(t)$, and noise intensities $\alpha_k = 10^{-3}$, with zero deterministic components, and conductance matrices $\mathbf{G}_{ik} = \mathbf{R}_{ik}^{-1} = \text{diag}(R_{ik1}^{-1}, 0)$, $R_{ik1} = 1 \text{ M}\Omega$, $k = 2, \dots, m$. In short, the MTL is driven from a deterministic source on its left port, into the first wire, while stochastic disturbances act along the MTL's first wire.

The statistical characteristics of stochastic responses for the MTL's terminating ports are shown in Fig. 6, computed from sets of $J = 100$ samples via (18)-(20): the sample means by solid blue lines, the 99 % confidence intervals by

dashed red lines (for the means) and dashed green lines (for the samples). For practical usage, just estimates of moments of stochastic processes are most often needed.

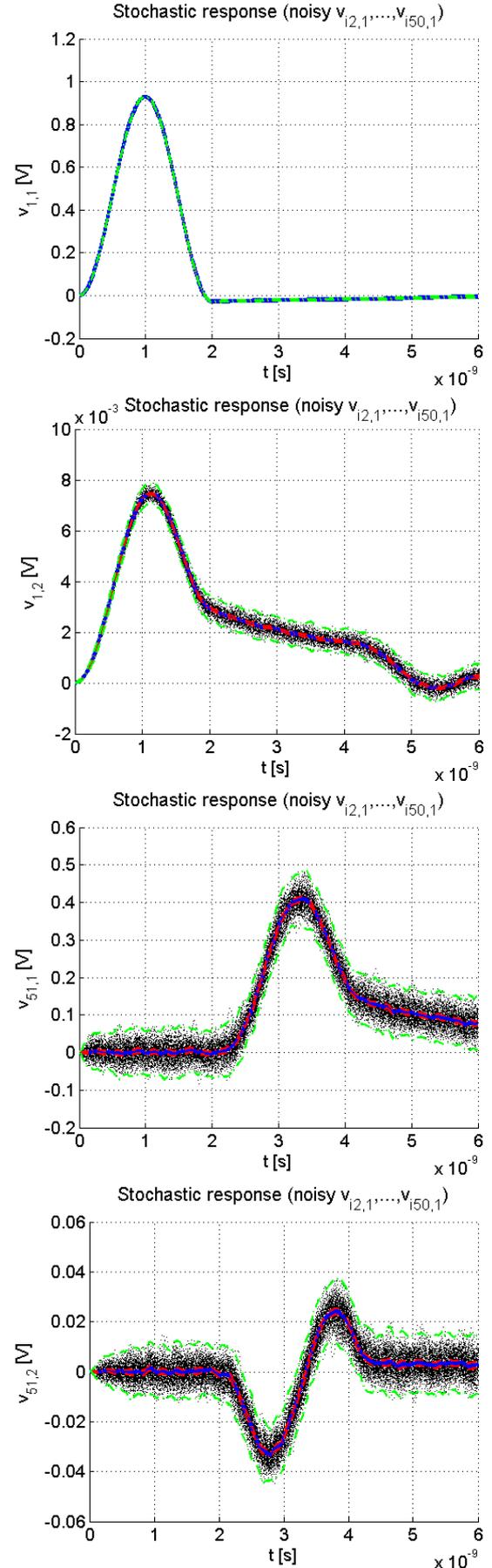


Fig. 6. Statistical characteristics of MTL's stochastic responses.

In Fig. 7, there are the results corresponding to Fig. 6, however, the confidence interval is calculated directly based on the Lyapunov-like matrix equation (25).

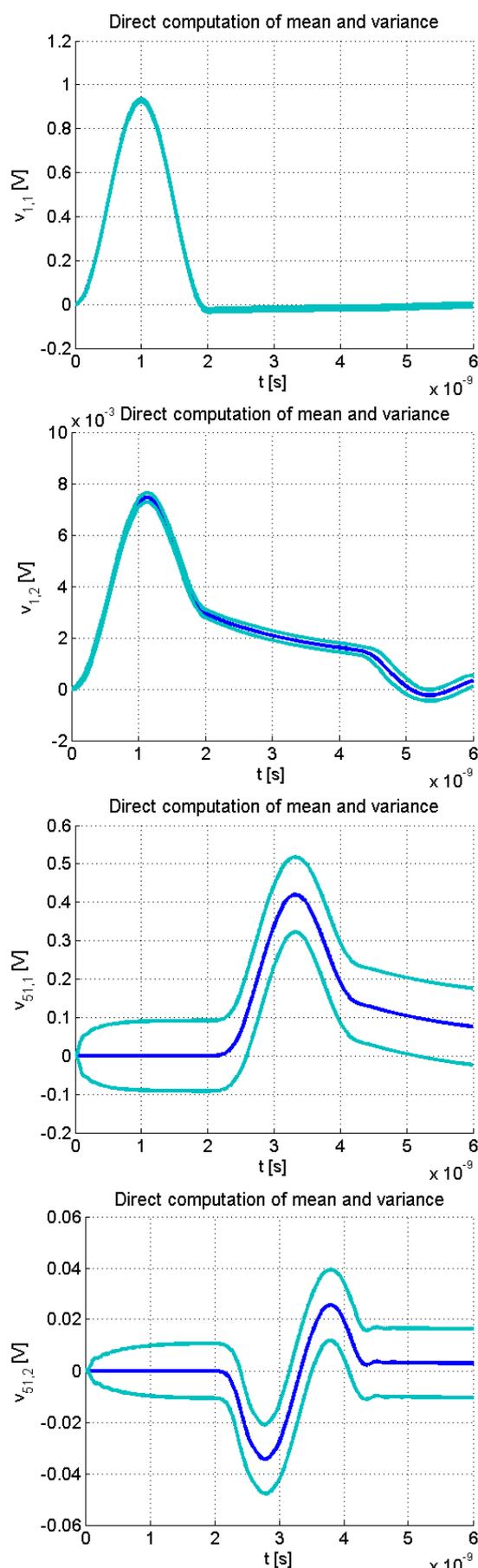


Fig. 7. Direct calculation of variances for MTL's stochastic responses.

As can be seen from Fig. 7 the confidence intervals well correspond to those in Fig. 6, but there was no need to repeatedly solve SDEs themselves. This approach is well applicable just for additive noises considered here because the normal distribution of stochastic responses is kept, and consequently, the inverse normal distribution function can be directly applied to get respective confidence intervals.

VI. CONCLUSION

The paper dealt with a method for simulation of statistical characteristics of stochastic responses at MTLs' model with excitations from multiple stochastic and/or deterministic sources. Beyond the previously published works, where only MTL's terminal ports were allowed for the excitations, the method extends it to arbitrary nodes along the MTL model, that can advantageously be used when unwanted disturbances along the wires arise. Besides two versions of initial stochastic processes were applied and the results compared – the Wiener process, needed if individual stochastic trajectories are studied, and simplified two-point random variable process, sufficient when only the moments of stochastic processes are of our interest. It was verified on the single transmission line simulation that the confidence intervals calculated via both the methods agree very well. Finally a method utilizing direct computation of variances of stochastic processes, based on the solution of a covariance matrix, was verified and compared with statistical methods. For this purpose the Lyapunov-like differential equation has been developed in relation to the MTL's model, and proper numerical technique based on an alternating-direction-implicit iteration method verified. It should be noticed that just this method seems to be most appropriate for practical purposes, to evaluate dispersions of random processes with a defined confidence level. All the computations were performed in the Matlab language, utilizing a sparse matrix notation with advantages for saving RAM and CPU time.

Methods based on the SDE theory can be interesting and efficient alternatives to other probabilistic techniques used in field of electronic circuits simulations, like e.g. widespread Monte Carlo [22], which is highly time-consuming method. In systems with distributed parameters, frequently in interconnects at high-speed digital/analog circuits, a polynomial-chaos expansion method is also often used to evaluate manufacturing random changes [23], [24], or various methods following sensitivities computations can be considered [25], [26]. It should be noticed that the SDEs approach is applicable for the analysis of further parameters, related to a physical structure of interconnects, and leading to SDEs with a multiplicative noise [10], [27]. Similarly, for more complex hybrid systems, stochastic differential algebraic equations (SDAE) can be utilized [6], [28].

REFERENCES

- [1] B. Øksendal, *Stochastic Differential Equations, An Introduction with Applications*. New York: Springer-Verlag, 2000.
- [2] P. Kloeden, E. Platen, and H. Schurz, *Numerical Solution of SDE Through Computer Experiments*. New York: Springer-Verlag, 1997.
- [3] L. Arnold, *Stochastic Differential Equations: Theory and Applications*. Malabar: Krieger Publishing, 1992.
- [4] D. Ham, A. Hajimiri, "Complete noise analysis for CMOS switching mixers via stochastic differential equations," in *Proc. IEEE Custom Integrated Circuits Conference*, Orlando, 2000, pp. 439-442.

- [5] A. Zjajo, Q. Tang, M. Berkelaar, J. P. de Gyvez, A. Di Bucchianico, N. van der Meijs, "Stochastic analysis of deep-submicrometer CMOS process for reliable circuits designs," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 58, no. 1, 2011, pp. 164-175.
- [6] K. Wang, M. L. Crow, "Numerical simulation of stochastic differential algebraic equations for power system transient stability with random loads," in *Proc. 2011 IEEE Power and Energy Society General Meeting*, San Diego, 2011, pp. 1-8.
- [7] M. P. LI, *Jitter, Noise, and Signal Integrity at High-Speed*. Upper Saddle River: Prentice Hall, 2007.
- [8] C. K. Cheng, J. Lillis, S. Lin, N. Chang, *Interconnect Analysis and synthesis*. New York: John Wiley & Sons, 2000.
- [9] C. R. Paul, *Analysis of Multiconductor Transmission Lines*. New York: John Wiley & Sons, 2008.
- [10] L. Brančík, E. Kolářová, "Stochastic differential equations approach in the analysis of MTLs with randomly varied parameters," in *Proc. 19th IEEE International Conference on Electronics, Circuits, and Systems ICECS'2012*, Sevilla, Spain, 2012, pp. 725-728.
- [11] L. Brančík, E. Kolářová, "Simulation of higher-order electrical circuits with stochastic parameters via SDEs," *Advances in Electrical and Computer Engineering*, vol. 13, no. 1, 2013, pp. 17-22.
- [12] L. Brančík, E. Kolářová, "Simulation of stochastic responses at multiconductor transmission lines with fluctuating parameters," in *Proc. 23rd International Conference Radioelektronika'2013*, Pardubice, Czech Republic, 2013, pp. 61-64.
- [13] L. Brančík, E. Kolářová, "Time-domain simulation of transmission line models with multiple stochastic excitations," in *Proc. 24th International Conference Radioelektronika'2014*, Bratislava, Slovakia, 2014, pp. 1-4.
- [14] L. Brančík, E. Kolářová, "Multiconductor transmission line models excited from multiple stochastic sources," in *37th International Conference on Telecommunications and Signal Processing TSP'14*, Berlin, Germany, 2014, pp. 282-286.
- [15] L. Brančík, "Time and Laplace-domain methods for MTL transient and sensitivity analysis," *COMPEL: The International Journal for Computation and Mathematics in Electrical and Electronic Engineering*, vol. 30, no. 4, 2011, pp. 1205-1223.
- [16] G. H. Golub, C. F. Van Loan, *Matrix computations*. Baltimore: Johns Hopkins Univ. Press, 1996.
- [17] E. Wachspress, Iterative solution of the Lyapunov matrix equation. *Appl. Math. Lett.*, vol. 1, 1998, pp. 87-90.
- [18] E. Kolářová, "Statistical estimates of stochastic solutions of RL electrical circuits," in *Proc. the IEEE International Conference on Industrial Technology ICIT'06*, Mumbai, India, 2006, pp. 2546-2550.
- [19] M. G. Bulmer, *Principles of Statistics*. Dover Publications, Revised edition, 1979.
- [20] L. Brančík, E. Kolářová, "Confidence intervals at multiconductor transmission lines with stochastic excitations," in *22nd European Conference on Circuit Theory and Design ECCTD'2015*, Trondheim, Norway, 2015, p. 1-4.
- [21] S. Lum, M. S. Nakhla, and Q. J. Zhang, "Sensitivity analysis of lossy coupled transmission lines," *IEEE Transactions on Microwave Theory and Techniques*, vol. 39, no. 12, 1991, pp. 2089-2099.
- [22] D. P. Kroese, T. Taimre, and Z. I. Botev, *Handbook of Monte Carlo methods*. New York: John Wiley & Sons, 2011.
- [23] D. Spina, F. Ferranti, T. Dhaene, et al. "Variability analysis of multiport systems via polynomial-chaos expansion," *IEEE Transactions on Microwave Theory and Techniques*, vol. 60, no. 8, 2012, pp. 2329-2338.
- [24] D. Vande Ginste, D. De Zutter, D. Deschrijver, T. Dhaene, P. Manfredi, and F. Canavero, "Stochastic modeling-based variability analysis of on-chip interconnects," *IEEE Transactions on Components, Packaging and Manufacturing Technology*, vol. 2, no. 7, 2012, pp. 1182-1192.
- [25] A. Wardzinska, W. Bandurski W., "Step response sensitivity to RLC parameters of VLSI interconnect," in *Proc. International Conference on Signals and Electronic Systems ICSES'10*, Gliwice, Poland, 2010, pp. 297-300.
- [26] H. Qinshu, L. Xinen, and X. Shifu, "A fast approximate method for parametric probabilistic sensitivity estimation," in *Proc. 3rd International Conference on Advanced Computer Theory and Engineering ICACTE'10*, Chengdu, China, 2010, pp. V3-349-V3-351.
- [27] L. Brančík, E. Kolářová, "Variance assesment at transmission lines with randomly varying parameters via SDE theory," in *Proc. 16th International Conference on Computer as a Tool EUROCON'2015*, Salamanca, Spain, 2015, pp. 287-291.
- [28] L. Brancik, "Simulation of hybrid MTL systems with random parameters based on stochastic DAEs," in *Proc. 21st European Conference on Circuit Theory and Design ECCTD'2013*, Dresden, Germany, 2013, pp. 1-4.

Benchmarking Further Single Board Computers for Building a Mini Supercomputer for Simulation of Telecommunication Systems

Gábor Lencse and Sándor Répás

Abstract—Parallel Discrete Event Simulation (PDES) with the conservative synchronization method can be efficiently used for the performance analysis of telecommunication systems because of their good lookahead properties. For PDES, a cost effective execution platform may be built by using single board computers (SBCs), which offer relatively high computation capacity compared to their price or power consumption and especially to the space they take up. A benchmarking method is proposed and its operation is demonstrated by benchmarking ten different SBCs, namely Banana Pi, Beaglebone Black, Cubieboard2, Odroid-C1+, Odroid-U3+, Odroid-XU3 Lite, Orange Pi Plus, Radxa Rock Lite, Raspberry Pi Model B+, and Raspberry Pi 2 Model B+. Their benchmarking results are compared to find out which one should be used for building a mini supercomputer for parallel discrete-event simulation of telecommunication systems. The SBCs are also used to build a heterogeneous cluster and the performance of the cluster is tested, too.

Keywords—benchmarking, closed queueing networks, cluster computing, discrete-event simulation, OMNeT++, single board computers

I. INTRODUCTION

Raspberry Pi [1] was originally aimed of encouraging basic computer science in schools, but having shipped one million units in the first year [2], its success also encouraged several vendors to design similar single board computers with somewhat better performance characteristics both for hobbyists and for commercial class applications.

Whereas a demonstration cluster made up by 64 Raspberry Pi single board computers was reported in [3], our aim is to test a number of SBCs (single board computers) from different vendors, to find out which one should be selected for building a cluster for parallel discrete-event simulation. For building such a cluster, several factors must be taken into consideration. Computing power, memory size and speed, as well as communication speed are primary factors. Heat dissipation is also important both for operation costs and especially for cooling. Size also matters, if high number of elements are built together. As for usability, the support of standard Linux distributions (e.g. Debian or Ubuntu) is essential. Last but not least, the price of the devices must also be considered.

Though vendors publish the main parameters of their devices (e.g. CPU type and clock speed, DRAM size,

technology and clock speed, NIC type, etc.) we believe that their performance concerning discrete-event simulation can be estimated the most appropriate way if we benchmark them by executing discrete-event simulation. For benchmarking, we used the OMNeT++ discrete event simulator [4] and its CQN (Closed Queueing Network) sample model. We have first used the proposed benchmarking method for estimating the computing power of the different members of a heterogeneous cluster in [5] where we also proved that PDES with the conservative synchronization method can be efficiently used in the simulation of telecommunication systems because the delay of the long distance lines ensures the good lookahead.

This paper is an extended version of our conference paper [6], where we used the proposed method to benchmark six SBCs to find out which one would be the best choice to build a suitably large cluster for simulation, however, our main aim was to validate the proposed method. The validation of our choice between the two possible performance metrics (the sequential and the parallel performance, see their details later) was done by testing the performance of a small heterogeneous cluster of the different tested single board computers. Now, we extend our previous results with the testing of four further SBCs. We also disclose our plans for future research concerning SBCs.

The remainder of this paper is organized as follows. First, we give the tested SBCs with their most important parameters. Second, we summarize the method of benchmarking with the CQN model. Third, we present the benchmarking results and discuss them. Fourth, we summarize the theoretical background of heterogeneous simulation clusters. Fifth, we present our experiments and results with the experimental heterogeneous cluster. Sixth, we present our size and power consumption measurement results and do a final comparison of the tested devices using these values, too. Seventh, we disclose our plans for future research concerning SBCs. Finally, we give our conclusion.

II. SELECTED SINGLE BOARD COMPUTERS FOR TESTING

For our conference paper [6], six SBCs were selected for comparison. Raspberry Pi was a must, as it was the first popular one. Banana Pi was chosen because it has a Gigabit Ethernet NIC, which one is not yet very common for SBCs today. Odroid-U3+ was chosen because of its high clock frequency quad-core CPU. Radxa Rock Lite was selected as an alternative with quad-core CPU. Cubieboard2 contains built in storage and also SATA II interface, which can be used for connecting SSD. And finally, Beaglebone Black was an alternative single-core SBC.

We have selected four further SBCs for the journal version of our paper. As Odroid-U3+ was the absolute

Manuscript received November 15, 2015, revised January 27, 2016.

G. Lencse is with the Department of Telecommunications, Széchenyi István University, 1. Egyetem tér, H-9026 Győr, Hungary (phone: +36-20-775-82-67; fax: +36-96-613-646; e-mail: lencse@sze.hu).

S. Répás is with the Department of Telecommunications, Széchenyi István University, 1. Egyetem tér, H-9026 Győr, Hungary (e-mail: repas.sandor@sze.hu).

doi: 10.11601/ijates.v5i1.138

TABLE I
SURVEY OF SINGLE BOARD COMPUTERS – BASIC CHARACTERISTICS

Name	Vendor URL	CPU architecture	CPU Type	Number of cores	CPU speed (MHz)
Banana Pi	http://www.lemaker.org	ARM Cortex A7	AllWinner A20	2	1000
BeagleBone Black	http://beagleboard.org	ARM Cortex A8	TI AM3359	1	1000
Cubieboard2	http://cubieboard.org	ARM Cortex A7	AllWinner A20	2	1000
Odroid-C1+	http://www.hardkernel.com	ARM Cortex A5	Amlogic S805	4	1500
Odroid-U3+	http://www.hardkernel.com	ARM Cortex A9	Samsung Exynos 4412	4	1700
Odroid-XU3 Lite	http://www.hardkernel.com	ARM Cortex A15+A7	Samsung Exynos 5422	4+4	1800+1300
Orange Pi Plus	http://www.orangepi.org	ARM Cortex A7	AllWinner H3	4	1600
Radxa Rock Lite	http://radxa.com	ARM Cortex A9	Rockchip RK3188	4	1600
Raspberry Pi Model B+	http://www.raspberrypi.org	ARM1176JZ(F)-S	Broadcom BCM2835	1	700
Raspberry Pi 2 Model B+	http://www.raspberrypi.org	ARM Cortex A7	Broadcom BCM2836	4	900

TABLE II
SURVEY OF SINGLE BOARD COMPUTERS – ADDITIONAL DATA

Name	DRAM technology	DRAM speed (MHz)	DRAM size (MB)	NIC speed (Mbps)	Storage, ports, etc.	Price (USD)
Banana Pi	DDR3	480/432	1024	1000	SD+SATA II, HDMI, 2xUSB 2.0	34.00
BeagleBone Black	DDR3	606	512	100	2/4GB+microSD, microHDMI, USB 2.0	55.00
Cubieboard2	DDR3	480	1024	100	4GB+microSD+SATA II, HDMI, 2xUSB 2.0	59.00
Odroid-C1+	DDR3	792	1024	1000	microSD+eMMC, HDMI, 4xUSB 2.0	37.00
Odroid-U3+	LPDDR3	933	2048	100	microSD+eMMC, microHDMI, 3xUSB 2.0	69.00
Odroid-XU3 Lite	LPDDR3	933	2048	100	microSD+eMMC, microHDMI, 4x USB 2.0, USB 3.0	99.00
Orange Pi Plus	DDR3	480	1024	1000	8GB+microSD+SATA II, HDMI, 4xUSB 2.0, WiFi	47.50
Radxa Rock Lite	DDR3	800	1024	100	microSD, HDMI, 2xUSB 2.0, WiFi	59.00
Raspberry Pi Model B+	?	500	512	100	microSD, HDMI, 4xUSB 2.0	32.19
Raspberry Pi 2 Model B+	LPDDR2	400	1024	100	microSD, HDMI, 4xUSB 2.0	38.71

winner from among the six SBCs, we included two other kind of Odroid SBCs: Odroid-XU3 Lite for its expected higher performance and Odroid-C1+ for its being more cost effective and also having a Gigabit Ethernet NIC. As the old Raspberry Pi showed the poorest performance among the six SBCs, now we included its improved version, Raspberry Pi 2 Model B+ to give the brand a second chance. We also found Orange Pi Plus interesting because of having 8GB built-in storage and SATAII interface. Table I and Table II give their most important CPU, memory and network parameters, as well as the storage and connection possibilities and what is also important, their current prices as of November 13, 2015. Please note that Odroid U3+ and Odroid XU3 Lite are discontinued. The latter one was replaced by Odroid XU4 using the same Samsung Exynos 5422 CPU at 2GHz and having a Gigabit Ethernet port.

III. BENCHMARKING METHOD

A. Theoretical Background

Closed Queueing Network (CQN) was originally proposed for measuring the performance of parallel discrete-event simulation using the conservative synchronization method [7].

The OMNeT++ discrete-event simulation framework [4] contains a CQN implementation among its samples. We first used this model in our paper [8]. The below description of the model is taken from there.

This model consists of N_T tandem queues where each tandem queue consists of a switch and k single-server queues with exponential service times (Fig. 1). The last queues are

looped back to their switches. Each switch randomly chooses the first queue of one of the tandems as destination, using uniform distribution. The queues and switches are connected with links that have nonzero propagation delays. The OMNeT++ model for CQN wraps tandems into compound modules.

To run the model in parallel, the tandems should be assigned to different segments (Fig. 2). Lookahead¹ is provided by delays on the marked links.

As for the parameters of the model, the preset values shipped with the model were used unless it is stated otherwise. Configuration B was chosen, the one that promised good speedup.

In our paper [8], we used this implementation for the experimental validation of the criterion defined for good speedup in [9]. This criterion gives a simple and straight forward method for the estimation of the available parallelism on the basis of values which can be easily measured in sequential execution of the simulation. Ref [9] uses the notations ev for the number of events, sec for real world time (also called execution time or wall-clock time) in seconds and $simsec$ for simulated time (model time) in seconds.

The paper uses the following quantities for assessing the available parallelism:

- P performance represents the number of events processed per second (ev/sec).

¹ Lookahead is an important parameter of the conservative discrete-event simulation: it expresses a time interval while the given segment will surely not receive a message from another segment.

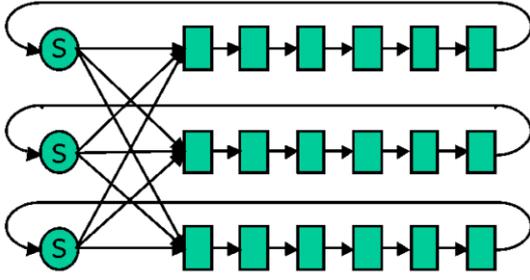


Fig. 1. $N_T=3$ tandem queues with $k=6$ single server queues in each tandem queue [8].

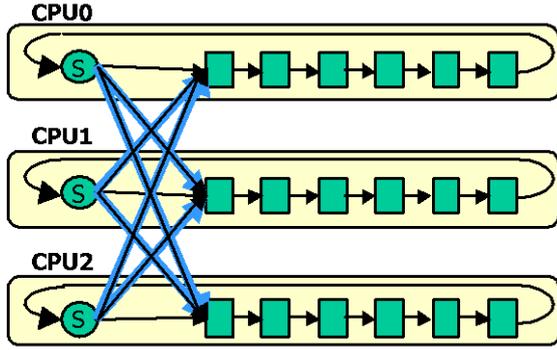


Fig. 2. Partitioning the CQN model [8].

- E event density is the number of events that occur per simulated second ($ev/simsec$).
- L lookahead is measured in simulated seconds ($simsec$).
- τ latency (sec) is the latency of sending a message from one segment to another.
- λ coupling factor can be calculated as the ratio of LE and τP :

$$\lambda = \frac{L \cdot E}{\tau \cdot P} \quad (1)$$

We have shown in [8] that if λ is in the order of several hundreds or higher then we may expect a good speedup. It may be nearly linear even for higher number of segments (N) if λ_N is also at least in the order of several hundreds, where:

$$\lambda_N = \frac{\lambda}{N} \quad (2)$$

B. Parameters of Benchmarking

We benchmarked all the single board computers by executing the CQN model sequentially (thus using only one core even if multiple cores were available) with the following parameters: $N_T=24$ tandem queues, $k=50$ single server queues, with exponential service time (having expected value of 10s), $T=10000$ simsec, $L=100$ simsec delay on the lines between the tandem queues.

We measured the execution time and calculated the average performance (P) as the ratio of the number of all the executed events (N_E) and the execution time of the sequential simulation (T_l):

$$P = \frac{N_E}{T_l} \quad (3)$$

The used Linux kernel versions and distributions are listed in Table III. OMNeT++ 4.6 and OpenMPI 1.8.4 were used.

TABLE III
LINUX KERNEL VERSIONS AND DISTRIBUTIONS

Name	Kernel version	Distribution
Banana Pi	3.4.104+ armv7l	Debian 7.8
BeagleBone Black	3.8.13-bone50 armv7l	Debian 7.8
Cubieboard2	3.4.43+ armv7l	Linaro 13.04
Odroid-C1+	3.10.67-55 armv7l	Ubuntu 14.04.3
Odroid-U3+	3.8.13.16 armv7l	Ubuntu 13.10
Odroid-XU3 Lite	3.10.69 armv7l	Ubuntu 14.04.2
Orange Pi Plus	3.4.39 armv7l	Debian 8.0
Radxa Rock Lite	3.0.36+ armv7l	Linaro 14.04
Raspberry Pi B+	3.12.35+ armv6l	Raspbian (Deb. 7.6)
Raspberry Pi 2 B+	4.1.7-v7+ armv7l	Raspbian (Deb. 7.8)

TABLE IV
SINGLE-CORE PERFORMANCE

Name	Execution Time (s)		P (ev/sec)
	average	std. dev.	
Banana Pi	46.9	0.92	33432
BeagleBone Black	68.3	1.51	22952
Cubieboard2	46.8	0.64	33494
Odroid-C1+	33.8	0.86	46370
Odroid-U3+	23.8	0.11	65839
Odroid-XU3 Lite	17.2	0.71	91281
Orange Pi Plus	36.6	0.78	42804
Radxa Rock Lite	28.6	0.26	54692
Raspberry Pi B+	177.4	1.46	8830
Raspberry Pi 2 B+	46.2	0.96	33946

IV. BENCHMARKING RESULTS

A. Single core results

First, we measured the performance of a single core only. The performance results are shown in Table IV. Odroid-XU3 Lite shows the best performance by processing 91281 events per second. Odroid-U3+, which one was winner in [6], is now the second best one (65839 ev/sec) whereas Radxa Rock Lite takes the third place (54692 ev/sec). Yet Odroid-C1+ (46370 ev/sec) and Orange Pi Plus (42804 ev/sec) excel somewhat from the rest of the SBCs. The performance of Banana Pi (33432 ev/sec) Cubieboard2 (33494 ev/sec) and Raspberry Pi 2 B+ (33946 ev/sec) are very close to each other. BeagleBone Black (22952 ev/sec) performed significantly worse and the old Raspberry Pi B+ (8830 ev/sec) is lagging behind all the others.

B. Multi core results

Second, we also tested the performance of the eight multi-core SBCs using all their available cores. The CQN model was compiled with the MPI support and the simulation model was shared into the same number of partitions as the number of CPU cores of the given single board computers had, that is two or four². Table V shows the results. We also included the speedup and the relative speedup values. According to its conventional definition, the speedup (S_N) of parallel execution is the ratio of the speed of the parallel execution in N segments (by the same number of CPU cores)

² Please note that Odroid-XU3 Lite has four A15 and four A7 cores. We used only four partitions therefore the four "smaller" cores were not utilized.

and the sequential execution by 1 CPU core which is usually calculated as the ratio of the execution time of the sequential execution (T_I) and that of the parallel execution (T_N), however now we used the ratio of the multi core performance (P_N) and the single core performance (P_I):

$$s_N = \frac{T_I}{T_N} = \frac{P_N}{P_I} \quad (4)$$

The relative speedup (r_N) can be calculated as the ratio of the speedup and the number of the CPU cores that produced the given speedup:

$$r_N = \frac{s_N}{N} \quad (5)$$

The relative speedup measures the efficiency of parallel execution. A relative speedup value of 1 means that the speedup is linear that is the computing power of the N CPU cores can be fully utilized.

Four of the SBCs show super-linear speedup, that is the relative speedup is higher than 1. This phenomenon is usually caused by caching. (E.g. the cores have they own L1 cache and partitions better fit in them than the whole model fitted into just one of them. Similar phenomenon was reported in [10], see page 95.) Now, we do not go deeper, but we plan to do further analysis of this phenomenon.

As for the ranking of the different single board computers, there is a significant change in the order (see Table V): Odroid-U3+ (279955 ev/sec) now outperformed Odroid-XU3 Lite (247956 ev/sec) and Raspberry Pi 2 B+ (167684 ev/sec) is now the third one.

As for the relative speed up, Raspberry Pi 2 B+ (1.23) is the best and Banana Pi (1.21) is very close to it. Regarding the low end, Orange Pi Plus (0.48) is the worst, and the "Light" versions of cards are also poor: Radxa Rock Lite (0.65) and Ordoid-XU3 Lite (0.68).

We believe that the results of the multi core benchmark using all the cores are to be used for characterizing the performance of the SBCs for parallel simulation because we would like to use their all cores in the simulation. We will support this in a case study with heterogeneous clusters. Please note that the case study was prepared for the conference version of the paper and therefore it does not include the further SBCs which are included in the journal version only.

V. THEORETICAL BACKGROUND FOR HETEROGENEOUS CLUSTERS

A. Load Balancing Criterion

We discussed the conditions necessary for a good speedup of the parallel simulation using the conservative synchronization method in heterogeneous execution environment in [5]. There we defined the logical topology of heterogeneous clusters as a *star shaped network of homogeneous clusters* where a homogeneous cluster may be built up by one or more instances of single-core or multi-core computers. In addition to the before mentioned coupling factor criterion that λ_N should be in the order of several hundreds, we defined another very natural criterion of load balancing that "all the CPUs (or CPU cores) should get a *fair share* from the execution of the simulation. A fair share is proportional to the computing power of the CPU *concerning the execution of the given simulation model.*"

TABLE V
ALL-CORE PERFORMANCE AND COMPARISON

Name	No. of Cores	P_I (ev/sec)	P_N (ev/sec)	Speedup	Relative Speedup
Banana Pi	2	33432	81160	2.43	1.21
BeagleBone Black	1	22952	22952	--	--
Cubieboard2	2	33494	76071	2.27	1.14
Odroid-C1+	4	46370	148967	3.21	0.80
Odroid-U3+	4	65839	279955	4.25	1.06
Odroid-XU3 Lite	4	91281	247956	2.72	0.68
Orange Pi Plus	4	42804	82452	1.93	0.48
Radxa Rock Lite	4	54692	142369	2.60	0.65
Raspberry Pi B+	1	8830	8830	--	--
Raspberry Pi 2 B+	4	33946	167684	4.94	1.23

Now, we have already benchmarked the CPUs by the CQN model.

B. Measuring the Efficiency of Parallel Simulation Executed by Heterogeneous Systems

We extended the definition of the relative speedup of parallel program execution (not only simulation) for heterogeneous execution environments in [11]. There we applied it for measuring the efficiency of *heterogeneous simulation* (that is parallel simulation executed by heterogeneous systems) and received the following formula:

$$r_h = \frac{N_E}{T_h \cdot P_c} \quad (6)$$

where the letters denote the following values:

- r_h – the relative speedup of the heterogeneous simulation compared to the sequential simulation
- N_E – the number of events in the sequential simulation
- T_h – the execution time of the heterogeneous simulation
- P_c – the cumulative sum of the performance of all the cores in the heterogeneous execution environment, which can be calculated as:

$$P_c = \sum_{j=1}^{N_{CT}} P_i \cdot N_i \quad (7)$$

where the letters denote the following values:

- N_{CT} – the number of the CPU core types
- P_i – the performance of a single core of type i
- N_i – the number of cores of type i

Similarly to the homogeneous case, the maximum (and the desired ideal) value of the relative speedup equals to 1.

VI. PERFORMANCE OF OUR HETEROGENEOUS CLUSTER

The six single board computers were interconnected by a TP-Link 26-port Gigabit Ethernet switch (TL-SG5426).

A. Partitioning of the CQN model

The performance proportional partitioning of the CQN model was done using the following formula:

$$n_i = N_T \frac{P_i}{P_c} \quad (8)$$

where the letters denote the following values:

- n_i – the number of tandems to put into a segment executed by a core of type i
- N_T – the number of tandems in the CQN model
- P_i – the performance of a single core of type i
- P_c – see (7)

TABLE VI
THE DIVISION OF THE 96 TANDEM QUEUES AMONG THE SBCs USING THE
SINGLE CORE BENCHMARK RESULTS

SBC type	P_i	N_i	n_i	tandems /core	cumulated tandems
Banana Pi	33432	2	4.95	5	10
BeagleBone Black	22952	1	3.40	3	3
Cubieboard2	33494	2	4.96	5	10
Odroid-U3+	65839	4	9.76	10	40
Radxa Rock Lite	54692	4	8.11	8	32
Raspberry Pi B	8830	1	1.31	1	1
Total number of the cores:		14	Total no. of the tandems:		96

TABLE VII
THE DIVISION OF THE 96 TANDEM QUEUES AMONG THE SBCs USING THE
ALL CORES BENCHMARK RESULTS

SBC type	$P_{ICE,i}$	N_i	n_i	tandems /core	cumulated tandems
Banana Pi	40580	2	6.37	6	12
BeagleBone Black	22952	1	3.60	3	3
Cubieboard2	38036	2	5.97	6	12
Odroid-U3+	69989	4	10.99	11	44
Radxa Rock Lite	35592	4	5.59	6	24
Raspberry Pi B	8830	1	1.39	1	1
Total number of the cores:		14	Total no. of the tandems:		96

TABLE VIII
EXECUTION TIME AND RELATIVE SPEEDUP AS A FUNCTION BENCHMARKING
METHOD

Benchmarking Method	P_c (ev/simsec)	Execution time (s)		relative speedup
		average	std. dev.	
Single core	647748	24.3	1.26	0.398
All cores	611337	18.7	0.66	0.548

The number of the tandem queues was increased to 96 to be large enough for an approximate performance proportional partitioning. Whereas (8) defines the theoretically optimal values, the number of the tandems must be integers, therefore we rounded them. Two different partitionings were made. For the first one, the P values from the single core measurements were used, see Table IV. For the second one, the same values were kept for the single core SBCs, but the P_{ICE} one core equivalent parallel performance from the all core measurements was calculated according to (9) taking the P_N and N values from Table V.

$$P_{ICE} = \frac{P_N}{N} \quad (9)$$

The division of the 96 tandem queues among the cores of the single board computers using the first and the second method are shown in Table VI and Table VII, respectively. Note that the usage of the mathematical rounding would have resulted in 97 tandem queues in Table VII therefore the number of tandem queues to be put into the segment executed by the BeagleBone Black SBC was rounded from 3.6 to 3 and not to 4.

A 10000 simsec long simulation was executed by the heterogeneous cluster 11 times and the execution time was measured for both partitionings. The relative speedup was also calculated according to (6), where the number of events in the sequential simulation was $N_E=6260606$ and P_c was calculated according to (7) taking the P_i values from Table VI and the $P_{ICE,i}$ values from Table VII for the first partitioning and for the second partitioning, respectively.

B. Results

Table VIII shows the results. Both the average execution time and the relative speedup values are significantly better for the second method. Though someone might challenge the relative speedup values stating that they were calculated using smaller P_c values in the denominator of (6), the average execution time values are unquestionably show the superiority of the second method for partitioning.

Therefore, our results justified that if there is a significant difference between the single core benchmark values and the one core equivalent parallel performance benchmark values then the latter ones are better anticipate the performance of the cores in a parallel simulation thus the latter ones are to be considered as the valid metrics.

VII. FINAL COMPARISON OF THE TESTED SBCs

A. Absolute Performance Comparison

For the comparison of the absolute performance of the ten SBC, we use their P_N all-core performance values. They are compared by using a bar chart in Fig. 3. (It is put on the same page with the relative performance comparison figures for the synoptic view and easy comparison.)

B. Size and Power Consumption

We measured the size of the SBCs together with their overhanging parts (e.g. connectors, buttons, microSD cards), thus our results in Table IX are somewhat higher than those

TABLE IX
DIMENSIONS AND POWER CONSUMPTION OF THE SINGLE BOARD COMPUTERS

Name	Dimensions			V (cm ³)	CPU is Idle			1 Core is Used			All the Cores are Used		
	(mm)	(mm)	(mm)		U (V)	I (mA)	P(W)	U (V)	I (mA)	P(W)	U (V)	I (mA)	P(W)
Banana Pi	96	..75	18	130	5.54	310	1.72	5.50	390	2.15	5.47	490	2.68
BeagleBone Black	85	..52	16	71	5.02	250	1.26	4.96	370	1.84	--	--	--
Cubieboard2	102	..58	20	118	5.57	230	1.28	5.53	345	1.91	5.49	470	2.58
Odroid-C1+	..87	..55	21	100	5.14	330	1.70	5.14	390	2.00	5.12	490	2.51
Odroid-U3+	81	..48	17	66	5.55	350	1.94	5.51	410	2.26	5.33	1000	5.33
Odroid-XU3 Lite	99	..78	22	170	5.19	560	2.91	5.11	970	4.96	5.11	1510	7.72
Orange Pi Plus	115	63	19	138	5.05	540	2.73	5.02	640	3.21	5.00	690	3.45
Radxa Rock Lite	100	..90	14	126	5.50	550	3.03	5.50	580	3.19	5.41	700	3.79
Raspberry Pi B+	90	..60	19	103	5.52	380	2.10	5.51	405	2.23	--	--	--
Raspberry Pi 2 B+	90	..60	19	103	5.16	230	1.19	5.14	300	1.54	5.11	450	2.30

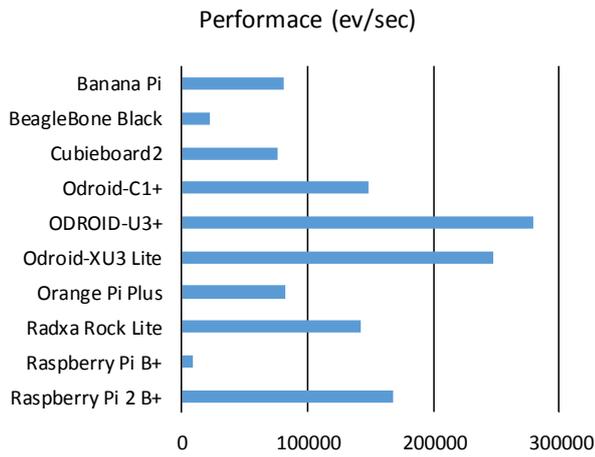


Fig. 3. Comparison of the all-core performance of the SBCs.

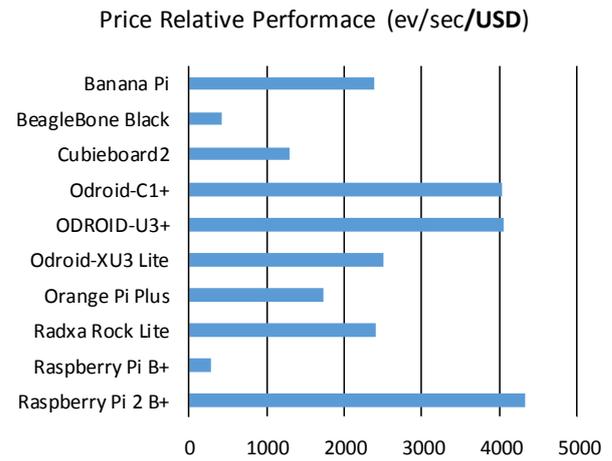


Fig. 5. Comparison of the price relative all-core performance of the SBCs.

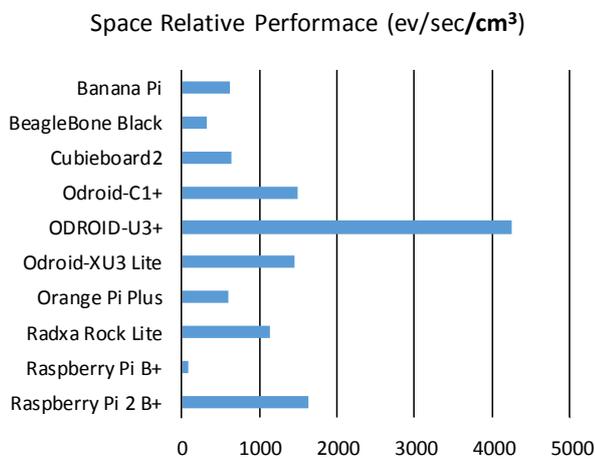


Fig. 4. Comparison of the space relative all-core performance of the SBCs.

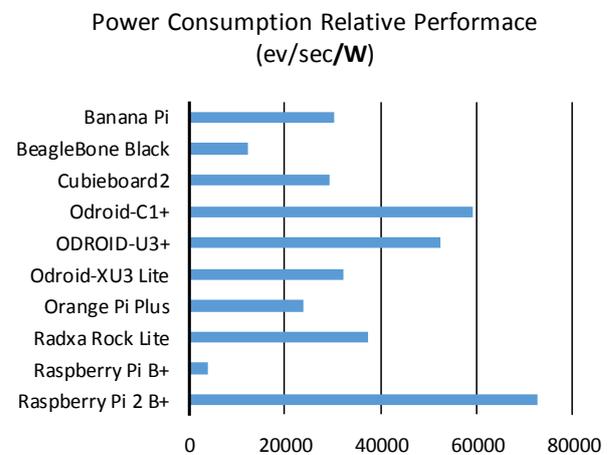


Fig. 6. Comparison of the power consumption relative all-core performance of the SBCs.

provided by the manufacturers. Please note that if SBCs are integrated into a cluster then they will occupy even larger space because both cables (Ethernet, power) and cooling need significant space.

We measured the power consumption of the SBCs under different load conditions: the system was idle, one core had full load, all cores had full load. The above detailed CQN model was used for load generation. Our results can also be found in Table IX.

TABLE X
RELATIVE ALL-CORE PERFORMANCE CHARACTERISTICS

Name	P_N / V (ev/sec/cm ³)	P_N / Price (ev/sec/USD)	$P_N / \text{Power Cons.}$ (ev/sec/W)
Banana Pi	624	2387	30284
BeagleBone Black	323	417	12474
Cubieboard2	645	1289	29485
Odroid-C1+	1490	4026	59349
Odroid-U3+	4242	4057	52524
Odroid-XU3 Light	1459	2505	32119
Orange Pi Plus	597	1736	23899
Radxa Rock Lite	1130	2413	37564
Raspberry Pi B+	86	274	3960
Raspberry Pi 2 B+	1628	4332	72906

C. Relative Performance Characteristics

We used the all core parallel performance values of the SBCs. (One may also calculate with the single core results, as we provided the necessary data for that, too.) Our results can be found in Table X. Their space, price and power consumption relative performance values are compared in Fig. 4, Fig. 5 and Fig 6, respectively.

1) Space relative performance

Concerning space relative performance, Odroid-U3+ (4242 ev/sec/cm³) seriously outperformed all other SBCs. The second one, Raspberry Pi 2 B+ (1628 ev/sec/cm³) could not reach even half of the performance of Odroid-U3+.

2) Price relative performance

Raspberry Pi 2 B+ (4332 ev/sec/USD) showed the best price relative performance, but Odroid-U3+ (4057 ev/sec/USD) and Odroid-C1+ (4026 ev/sec/USD) were close to it.

3) Power consumption relative performance

Raspberry Pi 2 B+ (72906 ev/sec/cm³/W) showed the best price relative performance being significantly better than Odroid-C1+ (59349 ev/sec/W) and Odroid-U3+ (52524 ev/sec/USD).

D. Discussion of the results

The usage of different metrics resulted in different ranking

order of the tested ten SBCs. We consider that our most important result is the testing method itself and not the ranking of the ten tested SBCs. Using our testing method, one can test other SBCs and select from among them on the basis of his/her own target function.

Three of the tested SBCs have Gigabit Ethernet NICs but they could not gain advantage from it, because our benchmarking method did not test that. When the SBCs are actually used for parallel simulation then the communication speed matters. These three cards could be better ranked in a more realistic test setup when a small cluster is built for testing purposes. For more details, see our future plans for further research.

VIII. FUTURE PLANS

A. Building a Cluster for Simulation

We plan to build a cluster of significant size (at least of 128 elements or even more), but before determining the type of the SBC, we plan to experiment with smaller clusters of 16 elements for a more realistic benchmarking of the SBCs. These small clusters makes it possible to take also the speed of communication into consideration. In addition to that we may gain more experience on the architecture of the cluster, too. For example, if we will connect high number of elements then multiple switches will have to be used. How it will influence the behavior of the cluster? We can examine this phenomenon in a small size first, e.g. by building four sub-clusters, each of which have four elements.

B. Other Areas of Application

Besides to parallel discrete-event simulation, we plan to use the SBCs for other purposes too.

1) Load generation for DNS64 and NAT64 tests

First of all, we are going to use them as a load generator in DNS64 [12] server and NAT64 [13] gateway performance tests. We have several results in this area. As for DNS64 servers, we compared the performance of BIND and TOTD in [14]. We found a bug and a security hole in TOTD and provided a patch for correcting them in [16]. Later we also included the performance analysis of Unbound and PowerDNS in [15]. We prepared an own test program called dns64perf for the performance analysis of DNS64 servers [17]. We also have and own DNS64 implementation called MTD64 [18]. As for NAT64 gateways, we compared the performance of TAYGA+iptables and of OpenBSD PF using ICMP in [19] and later also TCP and UDP in [20]. In our further experiments, we plan to use a 16 element cluster of SBCs for load generation for DNS64 and NAT64 tests. This is an area where we expect that having a Gigabit Ethernet NIC will be an advantage.

2) Testing and using as MPT servers

The MPT network layer multipath communication library [21] makes it possible to aggregate the transmission capacity of multiple interfaces of a device. Its channel aggregation capability was tested for two channels in [22], four channels in [23]–[24], and twelve channels in [25]. MPT is also a good solution for wireless network layer roaming problems [26] and changing the communication interfaces (using different transmission technologies) without packet loss [27]. We plan to test some SBCs in the role of an MPT server.

IX. CONCLUSION

A method with two variants (single core and all cores test) was described for benchmarking different computers for parallel simulation. It was shown that the values of the all cores method characterize better the parallel simulation capabilities of the computers. Ten single board computers (SBCs) were benchmarked. Their space, price and power consumption relative performance were also calculated and compared. It was found that the usage of different metrics resulted in different ranking order of the SBCs. Odroid-U3+ gave the best absolute and space relative performance whereas Raspberry Pi 2 B+ showed the best price and power consumption relative performance. Both SBCs have only 100Mbps Ethernet NICs. Different SBCs may be optimal choice for different purposes. We also gave the directions of our planned future research including building an SBC cluster for simulation, using a cluster of SBCs for load generation in DNS64 server and NAT64 gateway performance analysis and using individual SBCs as MPT servers.

REFERENCES

- [1] E. Upton and G. Halfacree, *Raspberry Pi User Guide*, 2nd ed., Wiley, 2013.
- [2] C. Edwards, "Not-so-humble Raspberry Pi gets big ideas", *Engineering & Technology*, vol. 8, no. 3, pp. 30–33, Apr. 2013. DOI: 10.1049/et.2013.0301
- [3] S. J. Cox, J. T. Cox, R. P. Boardman, S. J. Johnston, M. Scott, N. S. O'Brien, "Iridis-pi: a low-cost, compact demonstration cluster", *Cluster Computing*, vol. 17, no. 2, pp. 349–358, Jun. 2014. DOI: 10.1007/s10586-013-0282-7
- [4] A. Varga and R. Hornig, "An overview of the OMNeT++ simulation environment", in *Proc. 1st Intern. Conf. on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, Marseille, 2008, pp. 1–10.
- [5] G. Lencse, I. Derka, and L. Muka, "Towards the efficient simulation of telecommunication systems in heterogeneous distributed execution environments", in *Proc. Int. Conf. on Telecommunications and Signal Processing (TSP 2013)*, Rome, 2013, pp. 314–310. DOI: 10.1109/TSP.2013.6613941
- [6] G. Lencse and S. Répás, "Method for benchmarking single board computers for building a mini supercomputer for simulation of telecommunication systems", in *Proc. Int. Conf. on Telecomm. and Signal Processing (TSP 2015)*, Prague, 2015, pp. 246–251. DOI: 10.1109/TSP.2015.7296261
- [7] R. L. Bagrodia and M. Takai, "Performance evaluation of conservative algorithms in parallel simulation languages", *IEEE Transactions on Parallel and Distributed Systems*, vol. 11, no. 4, pp. 395–411, Apr. 2000. DOI: 10.1109/71.850835
- [8] G. Lencse and A. Varga, "Performance Prediction of Conservative Parallel Discrete Event Simulation", in *Proc. 2010 Industrial Simulation Conf. (ISC'2010)* Budapest, 2010, pp. 214–219.
- [9] A. Varga, Y. A. Sekercioglu and G. K. Egan, "A practical efficiency criterion for the null message algorithm", in *Proc. European Simulation Symposium (ESS 2003)*, Delft, 2003, pp. 81–92.
- [10] John Benzi, M. Damodaran, "Parallel Three Dimensional Direct Simulation Monte Carlo for Simulating Micro Flows", in *Parallel Computational Fluid Dynamics 2007*, Springer Lecture Notes in Computational Science and Engineering, vol. 67, pp 91–98. DOI: 10.1007/978-3-540-92744-0_11
- [11] G. Lencse and I. Derka, "Testing the Speedup of Parallel Discrete Event Simulation in Heterogeneous Execution Environments" in *Proc. ISC'2013, 11th Annu. Industrial Simulation Conf.*, Ghent, 2013, pp. 101–107.
- [12] M. Bagnulo, A. Sullivan, P. Matthews and I. Beijnum, "DNS64: DNS extensions for network address translation from IPv6 clients to IPv4 servers", IETF RFC 6147 Apr. 2011.
- [13] M. Bagnulo, P. Matthews and I. Beijnum, "Stateful NAT64: Network address and protocol translation from IPv6 clients to IPv4 servers", IETF RFC 6146, Apr. 2011.
- [14] G. Lencse and S. Répás, "Performance analysis and comparison of different DNS64 implementations for Linux, OpenBSD and

FreeBSD”, in *Proc. IEEE 27th Internat. Conf. on Advanced Information Networking and Applications (AINA 2013)*, Barcelona, Spain, 2013, pp. 877–884. DOI: 10.1109/AINA.2013.80

- [15] G. Lencse, S. Répás, “Performance analysis and comparison of four DNS64 implementations under different free operating systems”, *Telecommunication Systems*, in press.
- [16] G. Lencse and S. Répás, “Improving the performance and security of the TOTD DNS64 implementation”, *Journal of Computer Science and Technology (JCS&T)*, ISSN: 1666-6038, vol. 14, no. 1, pp. 9–15. Apr. 2014.
- [17] G. Lencse, “Test program for the performance analysis of DNS64 servers”, *Internat. J. of Advances in Telecomm., Electrotechnics, Signals and Systems*, vol. 4, no. 3, pp. 60–65. Sep. 2015. DOI: 10.11601/ijates.v4i3.121
- [18] G. Lencse and A. G. Soós, “Design of a tiny multi-threaded DNS64 server”, in *Proc. 38th Internat. Conf. on Telecommunications and Signal Processing (TSP 2015)*, Prague, 2015, pp. 27–32. DOI: 10.1109/TSP.2015.7296218
- [19] G. Lencse and S. Répás, “Performance analysis and comparison of the TAYGA and of the PF NAT64 implementations”, in *Proc. 36th Internat. Conf. on Telecommunications and Signal Processing (TSP 2013)*, Rome, 2013, pp. 71–76. DOI: 10.1109/TSP.2013.6613894
- [20] S. Répás, P. Farnadi, and G. Lencse, “Performance and stability analysis of free NAT64 implementations with different protocols”, *Acta Technica Jaurinensis*, vol. 7, no. 4, pp. 404–427. Oct. 2014. DOI: 10.14513/actatechjaur.v7.n4.340
- [21] B. Almási, A. Harman, “An overview of the multipath communication technologies”, in *Proc. Conf. on Adv. in Wireless Sensor Networks 2013 (AWSN 2013)*, Debrecen, 2013, pp. 7–11.
- [22] B. Almási, Sz. Szilágyi, “Throughput performance analysis of the multipath communication library MPT”, in *Proc. 36th Int. Conf. on Telecommunications and Signal Processing (TSP 2013)*, Rome, 2013, pp. 86–90. DOI: 10.1109/TSP.2013.6613897
- [23] B. Almási, Sz. Szilágyi, “Multipath ftp and stream transmission analysis using the MPT software environment”, *Int. J. of Advanced Research in Computer and Communication Engineering*, vol. 2, no. 11, pp. 4267–4272, Nov. 2013.
- [24] B. Almási, Sz. Szilágyi, “Investigating the performance of the MPT multipath communication library in IPv4 and IPv6”, *Internat. J. of Advances in Telecomm., Electrotechnics, Signals and Systems*, under review
- [25] G. Lencse and Á. Kovács, “Advanced measurements of the aggregation capability of the MPT multipath communication library”, *Internat. J. of Advances in Telecomm., Electrotechnics, Signals and Systems*, vol. 4, no. 2, pp. 41–48, May 2015, DOI: 10.11601/ijates.v4i2.112
- [26] B. Almási, “A simple solution for wireless network layer roaming problems”, *Carpathian Journal of Electronic and Computer Engineering*, vol. 5, no. 1, pp. 5–8, 2012.
- [27] B. Almási, “A solution for changing the communication interfaces between WiFi and 3G without packet loss”, in *Proc. 37th Int. Conf. on Telecommunications and Signal Processing (TSP 2014)*, Berlin, Jul. 2014, pp. 73–77.



Gábor Lencse received his MSc in electrical engineering and computer systems at the Technical University of Budapest in 1994, and his PhD in 2001.

He has been working for the Department of Telecommunications, Széchenyi István University, Győr, Hungary since 1997. He teaches computer networks and the Linux operating system. Now, he is an Associate Professor. He is responsible for the specialization of the information and communication technology of the BSc level electrical engineering education. He is a founding member and also core member of the Multidisciplinary Doctoral School of Engineering Sciences, Széchenyi István University. The area of his research includes discrete-event simulation methodology, performance analysis of computer networks and IPv6 transition technologies. He has been working part time for the Department of Networked Systems and Services, Budapest University of Technology and Economics (the former Technical University of Budapest), Budapest, Hungary since 2005. There he teaches computer architectures and computer networks.

Dr. Lencse is a member of IEEE, IEEE Computer Society and the Institute of Electronics, Information and Communication Engineers (IEICE, Japan).



Sándor Répás received his BA in business administration and management from the Corvinus University of Budapest, Budapest, Hungary in 2009, BSc in electrical engineering from the Óbuda University, Budapest, Hungary in 2011 and MSc in electrical engineering from the Széchenyi István University, Győr, Hungary in 2013.

He is a full time PhD student in information technology at the Széchenyi István University, Győr, Hungary. The main field of his research is the IPv6 implementation technologies. His other

favorite topics are computer networking, information security, and critical information infrastructure protection. He has several certificates from Cisco, ISACA, Microsoft, MikroTik, Novell, and other vendors.

Mr. Répás is a student member of the Association for Computer Machinery (ACM), and member of the Information Systems Audit and Control Association (ISACA), and the John von Neumann Computer Society (NJSZT).

Efficient Routing and Spectrum Allocation Considering QoT in Elastic Optical Network

Bingbing Li and Young-Chon Kim

Abstract—In recent years, Orthogonal Frequency Division Multiplexing (OFDM)-based elastic optical network (EON) has drawn increasing attention in both academia and industry. Compared to traditional optical Wavelength Division Multiplexing (WDM) network, EON is capable of supporting variable data rate, accommodating traffic demands flexibly with finer provisioning granularity, and utilizing spectrum more efficiently. Accordingly, the resource management in EON is different from that in WDM networks and addresses new challenges in network design and control. In this paper, we study the routing, modulation level and spectrum allocation (RMLSA) problem in EON. We propose an efficient link-based mixed integer linear programming (MILP) model with the objective to optimally utilize the spectrum resources while considering the constraint on Quality of Transmission (QoT). Then, the performance of the proposed model is evaluated and analyzed through case study.

Keywords— Elastic optical network, link-based model, MILP, RMLSA, QoT.

I. INTRODUCTION

With the exponential growth of end users and the emergence of bandwidth intensive applications, Internet traffic has been increasing sharply during last decades. The compound annual growth rate (CAGR) of IP traffic in backbone networks is estimated to be kept at 24~53% in the near future [1]. To meet the demand, optical Wavelength Division Multiplexing (WDM) network has been widely deployed for Internet backbone and the service providers keep on enlarging network capacity and expanding network size. The bandwidth of one wavelength has been continuously improved to 10 Gbps, 40 Gbps, and nowadays, 100 Gbps. However, traditional WDM networks adopt the ITU-T fixed-grid standard which divides the spectrum of C-band into fixed 50 GHz frequency slots (FSs) [2]. Data rate of 400 Gbps or higher for one wavelength channel cannot be achieved by the fixed grid and modulation format based on existing standard. On the other hand, the bandwidth demands among various applications show high

heterogeneity. Current optical network operating on the fixed grid has to allocate a complete wavelength even when required bandwidth is much smaller than the wavelength capacity, leading to inefficient utilization of spectrum resources. The support for 400 Gbps, 1 Tbps, and other high bit rate demands and the flexibility to accommodate heterogeneous demands drive us to develop a new paradigm which can overcome the shortages of WDM networks.

Recently, the Elastic Optical Network (EON) has been proposed. The main advantages of EON are: (1) bandwidth allocation based on finer granularity of a subcarrier rather than a wavelength; (2) ability to dynamically adapt channel data rate to required demand via bandwidth-variable transceivers (BVT) and bandwidth-variable optical crossconnect (BV-OXC); (3) high spectrum efficiency by flexibly adjusting modulation format via software. Among all enabling technology to realize EON architecture, optical Orthogonal Frequency Division Multiplexing (OFDM) has become the focus of extensive research effort. OFDM is a multi-carrier modulation technique by which the data flow is distributed over an arbitrary set of orthogonal low data rate subcarriers. These orthogonal subcarriers overlap in the frequency domain, leading to flexible resource allocation and efficient utilization of the spectrum resources. Comparing to traditional WDM networks, OFDM-based EON can achieve sub-wavelength and super-wavelength accommodation for various traffic demands. By allocating one or multiple contiguous FSs with appropriate modulation format, a spectrum path can be all-optically established between the source and destination nodes. If two spectrum paths share one or more common physical links, these spectrum paths should be separated by guard band for filtering and recovering signal. As the fundamental issue in EON, the Routing and Spectrum Allocation (RSA) problem should be taken into account, which is different from and more complex than the traditional Routing and Wavelength Assignment (RWA) problem in WDM networks.

In OFDM-based EON, each subcarrier can be processed individually through digital signal processing (DSP) implemented at both the transmitting and the receiving ends. That is, the modulation format can be adjusted according to the traffic demand and the transmission distance of optical path. Due to the accumulated signal impairment on the consecutive fiber links along the optical path, the maximum optical transmission distance (called transmission reach) is severely limited when the quality of transmission (QoT) is considered. Although optical OFDM can support significant higher channel capacity, the choice of the modulation format has to take into account the QoT. The relationship between

Manuscript received November 15, 2015; revised January 30, 2016. This work was supported by Basic Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2014-055177).

Bingbing Li is with the Department of Information Technology, Chonbuk National University, Jeonju, Jeonbuk, Korea (e-mail: bingbingli@jbnu.ac.kr).

Young-Chon Kim is with the Department of Information Technology, Chonbuk National University, Jeonju, Jeonbuk, Korea (corresponding author, phone: +82)63-271-2413; fax: +82)63-271-2413; e-mail: yckim@jbnu.ac.kr).

doi: 10.11601/ijates.v5i1.135

the capacity and transmission reach is given in [3]: an extra bit can be added per symbol, and the transmission reach should be halved for every 3 dB gain in signal-to-noise ratio (SNR). For example, modulation format 8QAM (3 bit/symbol) can be used instead of QPSK (2 bit/symbol), while the transmission reach of 8QAM signal should be reduced to half the transmission reach of QPSK. The consideration of QoT poses additional challenges on RSA: decision of appropriate modulation level.

To address all the issues mentioned above, new strategies and algorithms for Routing, Modulation Level and Spectrum Allocation (RMLSA) have to be developed. The challenges in new spectrum management schemes are:

- *Spectrum contiguity constraint*: The spectrum allocated to a request must be a block of contiguous FSs.
- *Spectrum continuity constraint*: This constraint is similar to the wavelength continuity constraint in WDM networks. The same contiguous FSs must be allocated on the consecutive links along the optical end-to-end path of a request.
- *Decision of modulation level*: The choice of modulation level is affected by required bandwidth and the limitation on transmission reach.

In this paper, we study the RMLSA problem in transparent EON. An efficient link-based MILP formulation is proposed to determine the routing, modulation level and spectrum allocation to each traffic demand with the consideration of QoT. To improve the spectrum efficiency, it tends to choose highest modulation level. However, the transmission reach of the optical path with the highest modulation level is very limited if acceptable QoT is considered. Hence, the proposed model needs to find the tradeoff among the number of required FSs, modulation level, and transmission reach. Our objective is to minimize the number of required FSs in network to accommodate all traffic demands.

The rest of this paper is organized as follows: In section II, the mathematical model is presented and explained. In section III, the MILP models are evaluated and compared by illustrative examples; and the numerical results will be analyzed. Finally, we conclude the paper in Section IV.

II. RELATED WORK

The RMLSA problem has been studied in several literatures. Reference [4, 5] introduced a path-based ILP formulation with the objective to minimize the maximum utilized spectrum slot index assigned on any link in the network. This work considered pre-computed k -shortest paths for each (s, d) pair. The constraints included: starting frequency ordering, non-overlapping spectrum allocation constraints. This model can solve routing and spectrum allocation jointly. Then, the same authors presented a method to decompose RSA into two formulations which address the routing (R) and spectrum assignment (SA) sub-problems respectively in [4]. A set of paths for each demand are predetermined as the input to R formulation. By solving the first formulation, one path per demand can be determined in order to minimize the amount of traffic flow (i.e., spectrum

use) on any link. Then, the SA formulation assigns FSs to demands so as to minimize the maximum FS index. Although solving each sub-problem separately and sequentially is more scalable than the joint ILP formulation, the joint optimal solution of the RSA problem might not be guaranteed. In [5], modulation level is considered and the RSA is decomposed into RML and SA sub-problems, which are solved sequentially. The choice of the modulation level takes into account the QoT of the connection. Due to the pre-calculation of candidate paths, the candidate modulation levels are also limited. Reference [6] proposed an ILP model with the objective to minimize total network cost. The cost is defined proportional to the total edge length and data rate of the traffic flow. And the model includes the physical capacity on each optical fiber and the traffic bounds constraints. Reference [7] proposed an MILP formulation to minimize total network energy consumption. The authors define the energy model which considers the energy cost of transponder, FS, amplifier and electronic processing. The network architecture is assumed to be the multi-hop grooming scenario. The routes of lightpaths are pre-computed and given as input parameters. The formulation includes the wavelength continuity, capacity, and maximum subcarrier constraints. In particular, the maximum subcarrier constraint considers the maximum capacity of a wavelength channel is limited by the all-optical reach. But the modulation format issue is not drawn in this work. Another path-based ILP model was presented in [8] to solve static RMLSA problem. In the model, candidate paths for each source-destination pair are pre-defined. The demand can be routed on only one of the candidate paths. The spectrum contiguity constraint is included in the ILP model, while the spectrum continuity constraint along a route is imposed implicitly since the assignment of a FS concerns the entire path. The objective is to minimize the number of FSs in the frequency spectrum that are assigned to at least one demand in the network.

Link-based ILP formulations of RSA can be viewed as a multi-commodity flow problem. Different from path-based model, there are no pre-computed candidate paths for each traffic request in link-based formulations. Hence, link-based schemes jointly decide the optimal routes and allocate spectra for all the services. Reference [9] proposed a link-based ILP model (referred to as node-arc model) for RSA with the objective to minimize the maximal index of used FSs in the entire network. To reduce the number of variables and computational complexity, the model adopted the method in [4] to define each spectrum path by using the starting and ending FS indexes. The spectrum contiguity, spectrum contiguity, non-overlapping constraints can be guaranteed in the node-arc model. Another link-based ILP model of RSA was studied in [10]. This work considers two objectives to minimize: the maximum FS index allocated on any fiber, and the total number of FSs over all fibers (summation of the maximum index of the sub-carriers over the fiber). Both [9] and [10] assumed the traffic demand in unit of FS, and the issue of modulation format decision was not considered. The model in [4] addressed the decision of modulation level. The flexibility is considerably limited due to the essence of path-based model. Once the k -shortest paths are computed, the modulation level of a path is

determined. The authors in reference [11] proposed a link-based MILP formulation to design an EON with the consideration on multiple modulation formats and noise constraint. It is assumed that the optical transmission reach of high-bit-rate lightpaths is severely limited by the signal quality degradation. Hence, the choice of modulation format depends on the threshold on the cumulative spontaneous emission noise power of the lightpath with specific modulation format. Comparing to the path-based models, more variables and constraints are needed for link-based models to determine optimal routing path. This may significantly increase the complexity of optimization models. However, link-based models can achieve better performance because no pre-determined routing paths means more feasible path candidates and spectrum allocation decisions can be searched.

In both traditional and elastic optical networks, the signal impairment is accumulated along the path which it traverses. Especially, a higher-data-rate signal can traverse a shorter distance than a lower-data-rate signal before the quality of signal is deteriorated to an unacceptable level. To keep the signal quality acceptable, the optical transmission reach must be considered to guarantee QoT. Reference [12] proposed energy efficient network design for the mixed-line-rate IP over WDM networks with limited transmission reaches. In the context of EON, [11] and [13] considered the physical layer constraint during network design and planning. In [11], authors added the spontaneous emission noise into the constraints of MILP model. As multiple modulation formats are available in EON, the different signal-to-noise rate requirements of different modulation formats should be considered during solving RMLSA problem. Reference [13] defined a physical feasibility function which identified the feasible transmission reach, given the rate, and spectrum or modulation format used for a specific BVT.

In this paper, we present a link-based MILP model to solve the RMLSA problem in EON with the constraint of optical transmission reach. The contribution of our proposed model, compared to previous works, is as follows: (1) as a unneglectable key factor during modulation decision procedure, the transmission reaches of different modulation formats are considered as constraint for RMLSA problem, which is reasonable and practical; (2) modulation format is determined jointly with routing and spectrum allocation according to the given required data rates for requests. This procedure reflects the essence and advantage of EON; (3) spectrum continuity constraint and contiguity constraint are included while determining suitable modulation format and number of FSs.

III. MATHEMATICAL MODEL

A. Problem Statement

In OFDM-based EON, the traffic demand between source and destination node pair is transmitted over multiple low-rate subcarriers which are orthogonal to each other. Given the physical topology, the traffic matrix, and the limit of transmission reach for various modulation formats as the input, we need to:

- provision all source-destination connection requests: determine the route, appropriate modulation level and spectrum allocation for each traffic demand
- optimize the spectrum utilization: minimize the sum of the maximum FS index over all fibers in network

The following assumptions are stated in the RMLSA model: (a) The fiber capacity in terms of FSs is not limited on all links; (b) Connection requests are directional, and an end-to-end all-optical path must be found for each request; (c) No specific path for a connection is given in advance, i.e., any possible path and any possible set of contiguous FSs will be evaluated while solving the model. Fig. 1 (a) shows a linear network, from node A to node E. The spectral resource on each optical fiber is divided into FSs with the granularity of 12.5 GHz. Three modulation formats can be supported: BPSK, QPSK, and 8QAM. The maximum transmission reaches of optical signal are: 2000 km (BPSK), 1000 km (QPSK), and 500 km (8QAM). The request is represented by three tuples: (s, d, BW) , including source node s , destination node d , and required bandwidth/data rate BW . In the illustrative example, there are three connection requests: R_1 (A, C, 50 Gbps), R_2 (B, D, 35 Gbps), and R_3 (A, E, 100 Gbps). To establish lightpath for R_1 , the modulation format should be determined by considering path length (A-B-C, 700 km). Among three modulation formats, BPSK and QPSK can satisfy this requirement. We chose QPSK which can achieve higher spectrum efficiency, and allocate two FSs to R_1 . For R_2 , path length is 500 km, and all three modulation formats are available. 8QAM is determined for the lightpath (B-C-D, 500 km) and 1 FSs are allocated to R_2 . For R_3 , path length is 1300 km. Only BPSK can satisfy the QoT requirement. Hence, BPSK is determined for the lightpath (A-B-C-D-E), and 4 FSs are allocated to R_3 . Fig. 1 (b) shows the spectrum allocation on each link, which satisfies the spectrum continuity and contiguity constraint. In Fig. 1 (b), FSs from index 1 to 2 on link A-B and B-C are allocated to R_1 . FS 5 on link B-C and C-D are allocated to R_2 . FS 8 to 11 on link A-B, B-C, C-D and D-E are allocated to R_3 . The guard band between two lightpaths which share a common link is 2 FSs, e.g., FS 3 to 4, 6 to 7 on link B-C, FS 6 to 7 on link C-D.

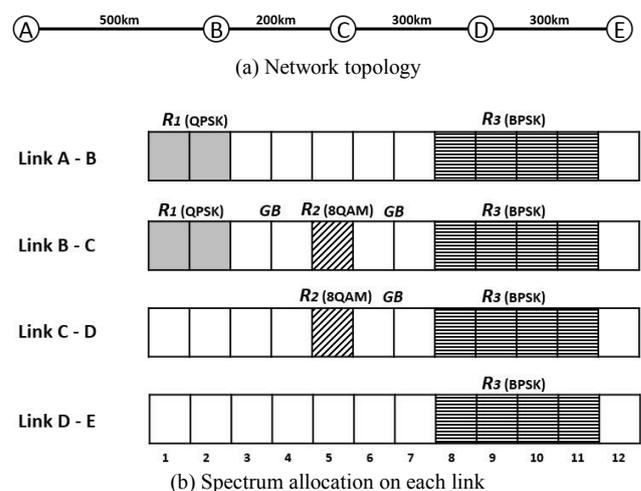


Fig. 1 RMLSA for five-node linear network

B. MILP Formulation

The notations and formulation are summarized as follows:

Indexing rules:

(s, d) - source-destination pair, s and d represent the originating and terminating nodes of a connection request.

(m, n) - node pair, m and n represent two endpoints of a fiber link in physical topology. Note that link has no directionality, i.e., (m, n) and (n, m) represent the same link in physical topology.

Given:

$G(V, E)$ - Network physical topology consisting of node set V and edge set E

λ^{sd} - Demand of connection request from s to d , $s, d \in V$

$TM = [\lambda^{sd}]$ - Traffic matrix

C - Base capacity of a FS with single bit per symbol modulation (BPSK)

R - Set of modulation levels, $R = \{1, 2, 3, \dots\}$, $r \in R$

L_{mn} - Length of physical link (m, n)

L_r - Maximum optical transmission reach of a lightpath adopting modulation level r

GB - Number of FSs for filter guard band

NE_i - Set of edges which are connected with node i

Variables:

$N_{sd,r}$ - (integer) Number of FSs allocated to serve request (s, d) with modulation level r

NFS_{sd} - (integer) Number of FSs allocated to serve request (s, d)

$NI_{mn}^{sd,r}$ - (integer) Number of FSs allocated to serve request (s, d) with modulation level r on physical link (m, n)

S_{sd} - (integer) Index of the starting FS allocated to serve request (s, d)

E_{sd} - (integer) Index of the ending FS allocated to serve request (s, d)

$X_{s'd'}^{sd}$ - (binary) equals one if the ending FS index of the lightpath between pair (s', d') is smaller than the starting FS index of the lightpath between (s, d) , i.e., $S_{sd} > E_{s'd'}$; otherwise, it takes the value of zero if the ending FS index of the lightpath between (s, d) pair is smaller than the starting FS index of the lightpath between (s', d') , i.e., $S_{s'd'} > E_{sd}$. This variable indicates the relative positions of the FSs allocated for two lightpaths.

$Y_{mn}^{sd,r}$ - (binary) equals one if request (s, d) using modulation level r is routed on physical link (m, n) ; otherwise, it takes value of zero.

$Z_{sd,r}$ - (binary) equals one if modulation level r is determined for connection request (s, d) ; otherwise, it takes value of zero.

$PN_i^{sd,r}$ - (binary) equals one if connection request (s, d) using modulation level r bypasses node i ; otherwise, it takes value of zero.

MI_{mn} - (integer) Maximum index of FS allocated on physical link (m, n)

Objective function:

$$\text{Minimize } \sum_{(m,n) \in E} MI_{mn} \quad (1)$$

The objective is to minimize the sum of the maximum index of allocated FSs on all links in the entire network.

Constraints:

1) *Single path routing constraint:*

$$\sum_{(m,n) \in NE_s} Y_{mn}^{sd,r} = 1, \forall (s, d), \forall r \in R \quad (2)$$

$$\sum_{(m,n) \in NE_d} Y_{mn}^{sd,r} = 1, \forall (s, d), \forall r \in R \quad (3)$$

$$\sum_{(m,n) \in NE_i} Y_{mn}^{sd,r} = 2 \times PN_i^{sd,r}, \forall (s, d), \forall r \in R, \forall i \in V, i \neq s, d \quad (4)$$

$$PN_i^{sd,r} + PN_j^{sd,r} \geq 2 \times Y_{mn}^{sd,r}, \forall (s, d), \forall r \in R, \forall (m, n) \in E \quad (5)$$

Constraint (2)-(5) guarantee that for each request (s, d) , only one single path can be followed, and the traffic demand cannot be split into multiple flows. Equation (2) regulates that the first-hop physical link on the lightpath for each connection request (s, d) must start from node s . Hence, the sum of all links going out from source node s must be equal to one. Equation (3) ensures that the last-hop physical link on the lightpath for each connection request (s, d) must end at node d . Similarly, the sum of all links coming in to destination node d must be equal to one. Equation (4) limits that for any intermediate node traversed by a lightpath, there must be two physical links connected with the node (one injecting into and one ejecting out from the node). Equation (5) ensures that if any physical link (m, n) is traversed by a lightpath (s, d) , the two ends (node m and n) of the link must be traversed by the lightpath as well.

2) *Flow conservation constraint:*

$$\sum_{(m,n) \in NE_s} NI_{mn}^{sd,r} = N_{sd,r}, \forall (s, d), \forall r \in R \quad (6)$$

$$\sum_{(m,n) \in NE_d} NI_{mn}^{sd,r} = N_{sd,r}, \forall (s, d), \forall r \in R \quad (7)$$

$$\sum_{(m,n) \in NE_i} NI_{mn}^{sd,r} = 2 \times N_{sd,r}, \forall (s, d), \forall r \in R, \forall i \in V, i \neq s, d \quad (8)$$

Constraint (6), (7), and (8) ensures the flow conservation in terms of number of FSs for any request (s, d) . Equation (6) regulates that for the number of FSs allocated on the first-hop physical link of the lightpath (s, d) must equals to the number of FSs allocated to connection request (s, d) , under any modulation level r . Equation (7) regulates that for the number of FSs allocated on the last-hop physical link of the lightpath (s, d) must equals to the number of FSs allocated to connection request (s, d) , under any modulation level r . Equation (8) ensures that for any intermediate node i on the lightpath (s, d) , the number of FSs allocated on the incoming and outgoing physical links must equals to twice the number of FSs required for request (s, d) under any modulation level r .

3) *Starting Frequencies ordering constraint:*

$$X_{s'd'}^{sd} + X_{sd}^{s'd'} = 1, \forall (s, d), (s', d') : sd \neq s'd' \quad (9)$$

Constraint (9) ensures that either the starting FS of (s, d)

is smaller than ending FS of (s', d') , or the starting FS of (s', d') is smaller than ending FS of (s, d) . The relative position of two connection requests is determined by $X_{s'd'}^{sd}$. If $X_{s'd'}^{sd}$ equals one (i.e., $S_{sd} > E_{s'd'}$), then $X_{sd}^{s'd'}$ must be zero; vice versa.

4) *Spectrum continuity and non-overlapping spectrum allocation constraints:*

$$E_{s'd'} - S_{sd} \leq F \times (X_{s'd'}^{sd} + 2 - Y_{mn}^{sd,r} - Y_{mn}^{s'd',r'}) - GB - 1, \quad (10)$$

$$\forall (s, d), (s', d') : sd \neq s'd', \forall (m, n) \in E$$

Constraint (9) and (10) ensure that when two lightpaths share common link(s) they must not overlap in frequency domain. In detail, when two lightpaths share a common link (m, n) ($Y_{mn}^{sd,r} = Y_{mn}^{s'd',r'} = 1$) and $S_{s'd'} > E_{sd}$ ($X_{s'd'}^{sd} = 0$), we can obtain $E_{s'd'} + GB + 1 \leq S_{sd}$, which satisfies the non-overlapping constraint; otherwise, constraint (10) always holds.

5) *Physical Link Usage Constraint:*

$$N_{mn}^{sd,r} \leq Y_{mn}^{sd,r} \cdot F, \quad \forall (s, d), \forall (m, n) \in E, \forall r \in R \quad (11)$$

Constraint (11) ensures that only the FSs on those links (m, n) which are used to route request (s, d) can be allocated. For any physical link (m, n) if $Y_{mn}^{sd,r}$ equals zero, i.e. the link is not traversed by lightpath (s, d) , then the number of FSs on link (m, n) allocated to lightpath (s, d) must be zero ($N_{mn}^{sd,r} = 0$). In contrast, if physical link (m, n) is traversed by lightpath (s, d) ($Y_{mn}^{sd,r} = 1$), the number of FSs on link (m, n) which can be allocated to lightpath (s, d) is less than a very large value F ($N_{mn}^{sd,r} \leq F$ always holds when $Y_{mn}^{sd,r} = 1$).

6) *Spectrum path MF constraint:*

$$N_{sd,r} \leq Z_{sd,r} \cdot F, \quad \forall (s, d), \forall r \in R \quad (12)$$

Constraint (12) determines which of the modulation level is used for the spectrum path between (s, d) pair. If $Z_{sd,r} = 0$, that is, modulation level r is not adopted by connection request (s, d) , the number of FSs allocated to serve request (s, d) with modulation level r must be zero ($N_{sd,r} = 0$). In contrast, if modulation level r is adopted by connection request (s, d) , the number of FSs allocated to serve request (s, d) under modulation level r is smaller than a very large value F ($N_{sd,r} \leq F$ always holds when $Z_{sd,r} = 1$).

7) *Modulation Format Constraint:*

$$\sum_{r \in R} Z_{sd,r} = 1, \quad \forall (s, d) \quad (13)$$

Constraint (13) asserts that each lightpath can adopt only one modulation level. For any connection request (s, d) , the sum of modulation levels of lightpath must be equal to one.

8) *Transmission reach constraint:*

$$\sum_{(m,n) \in E} Y_{mn}^{sd,r} \cdot L_{mn} \leq L_r, \quad \forall (s, d), \forall r \in R \quad (14)$$

Constraint (14) ensures that the path length of any request (s, d) adopting modulation level r cannot greater than the maximum optical transmission reach under r . The path

length is the sum of distance of all physical links which are traversed by the lightpath (s, d) .

9) *Max_FS_ID Constraint:*

$$MI_{mn} \geq E_{sd} - F \cdot (1 - Y_{mn}^{sd,r}), \quad (15)$$

$$\forall (s, d), \forall (m, n) \in E, \forall r \in R$$

Constraint (15) ensures that for any physical link (m, n) MI_{mn} is greater than the ending FS index of any request (s, d) which is routed on link (m, n) .

10) *Others:*

$$N_{sd,r} = Z_{sd,r} \times \left\lceil \frac{\lambda_{sd}}{r \cdot C} \right\rceil, \quad \forall (s, d), \forall r \in R \quad (16)$$

Equation (16) calculates the number of FSs for each (s, d) with modulation level r :

$$E_{sd} = S_{sd} + NFS_{sd} - 1, \quad \forall (s, d) \quad (17)$$

Equation (17) calculates the ending FS index for each request (s, d) .

$$NFS_{sd} = \sum_{r \in R} N_{sd,r}, \quad \forall (s, d) \quad (18)$$

Equation (18) calculates the number of FSs allocated for each request (s, d) .

IV. NUMERICAL RESULTS

To evaluate the performance of the proposed MILP model, we apply it on case study. The numerical results will be shown and analyzed in this section. Our results are obtained via optimization software IBM ILOG CPLEX Optimization Studio Version12.6 on the computer with Intel Core (TM) i5-2500 CPU (3.30 GHz) and 8 GB RAM.

The case study is implemented on a four-node (4N4L) ring network, and a six-node nine-link (6N9L) mesh network as shown in Fig. 2 and Fig. 3, respectively. Nodes are connected by bi-directional links. The filter guard band is $GB = 2$ FSs. The traffic demands for each source-destination pair is randomly generated between 1 and D Gbps ($D = 100, 150, 200, 250, 300, 400$). The bandwidth of one FS is $C = 12.5$ GHz.

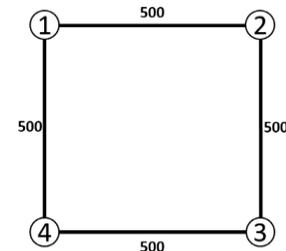


Fig. 2 Four-node ring network topology

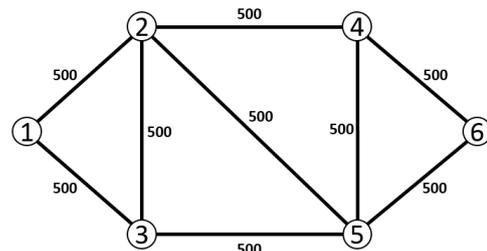


Fig. 3 Six-node nine-link network topology

Three modulation formats are considered: BPSK, QPSK, and 8QAM, and the corresponding modulation levels are 1, 2, and 3. The parameters for different modulation formats are summarized in Table I.

TABLE I
PARAMETERS FOR DIFFERENT MODULATION FORMAT

Modulation Format	Spectrum Efficiency (bps/Hz)	Data Rate per Subcarrier (Gbps)	Transmission Reach (km)
BPSK	1	12.5	2000
QPSK	2	25	1000
8QAM	3	37.5	500

Fig. 4 shows the number of required FSs to accommodate all traffic in 4N4L ring network according to different values of D (large value of D represents heavy traffic load). As a reference, we evaluate the scenario that only the modulation format BPSK is supported to quantify the spectrum usage affected by flexible choice of multiple modulation levels.

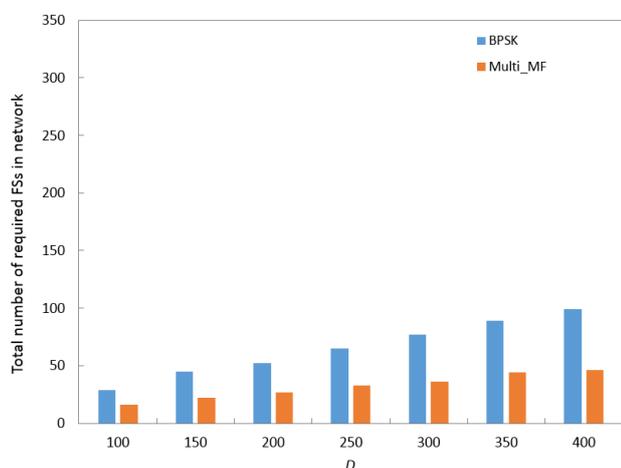


Fig. 4 Total number of required FSs in network according to different D for the 4N4L ring topology

The group of orange bars indicates the results for the case with multiple modulation formats, shorted as “Multi-MF”. The group of blue bars indicates the results for the case with single modulation format, shorted as “BPSK”. Obviously, the number of required FSs of Multi-MF is much less than that of BPSK under all different D . Multi-MF can achieve 45-53% saving on spectrum usage in terms of required FSs, comparing to the BPSK case. In addition, the saving on spectrum resources is improved with increasing network traffic load. These observations indicate that to accommodate the same network load, Multi-MF can outperform BPSK by efficiently allocating spectrum resources while satisfying the requirement of QoT.

Table II and III show the maximum index of FS on all links of 4N4L ring network based on Multi-MF and BPSK, respectively. It can be found that the difference among the maximum FS indexes of links is larger based on BPSK than that based on Multi-MF. For example, when $D = 100$ Gbps, the difference is 9 FSs between the links with the smallest and the largest indexes under Multi-MF while the difference increases to 11 FSs under BPSK. Because the number of

required FSs is determined solely on the bandwidth of request in the single MF scenario, the benefit of high spectral efficiency from OFDM cannot be exploited. Again, this difference becomes larger according to increasing the traffic load. Under $D = 400$ Gbps, the variation on the maximum FS indexes among all links based on Multi-MF and BPSK is 16 and 38, respectively. Larger variation indicates heavier load unbalance brought by BPSK scheme because the rigidity on allocate appropriate number of FSs.

TABLE II
MAXIMUM INDEX OF FS ON LINKS (MULTI-MF) FOR 4N4L NETWORK

Link	D						
	100	150	200	250	300	350	400
1->2	0	0	11	9	14	12	12
1->4	3	4	7	13	10	16	17
2->3	4	6	4	0	5	1	1
3->4	9	12	5	11	7	15	16

TABLE III
MAXIMUM INDEX OF FS ON LINKS (BPSK) FOR 4N4L NETWORK

Link	D						
	100	150	200	250	300	350	400
1->2	7	11	18	15	18	21	23
1->4	11	16	12	22	26	29	32
2->3	0	1	7	2	2	3	3
3->4	11	17	15	26	31	36	41

Fig. 5 shows the number of required FSs to accommodate all traffic as a function of different traffic load for the 6N9L mesh network. In general, Multi-MF obtains much less number of FSs than that of BPSK under all different traffic loads. Multi-MF can achieve 36-47% saving on spectrum usage in terms of required FSs, comparing to the BPSK. In addition, the saving on FSs enlarges according to increasing the traffic load.

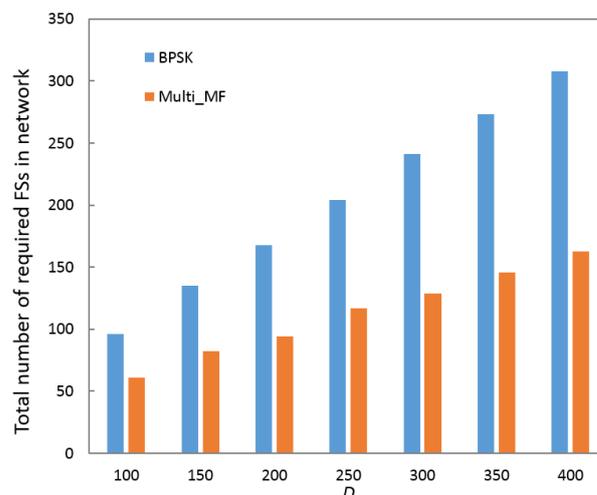


Fig. 5 Total number of required FSs in network according to different D for the 6N9L mesh topology

Table IV and V show the maximum index of FS on all links of 6N9L mesh network based on Multi-MF and BPSK, respectively. The variation on the maximum indexes of FSs which are allocated on all links is much larger based on BPSK than that of Multi-MF. Under low traffic load $D =$

100, the FS index variation is 13 based on Multi-MF. While the variation increases to 35 FSs based on BPSK. Under high traffic load $D = 400$, the FS index variation is 54 based on BPSK. While the variation based on Multi-MF is only 23, even smaller than the half of that based on BPSK. Several traditional RMLSA schemes assume single MF (higher spectral efficiency compared to WDM networks, e.g., ML=3 or 4) for simplicity, which ignores the nature of flexibility in EON. Hence this assumption is not practical.

TABLE IV
MAXIMUM INDEX OF FS ON LINKS (MULTI-MF) FOR 6N9L NETWORK

D	100	150	200	250	300	350	400
1->2	12	12	17	6	24	22	24
1->3	0	4	1	20	1	6	6
2->3	5	6	8	9	7	12	14
2->4	13	14	10	13	20	26	29
2->5	10	12	24	13	23	22	24
3->5	5	10	8	25	15	17	19
4->5	2	6	5	6	10	8	10
4->6	6	8	0	0	10	11	13
5->6	8	10	21	25	19	22	24

TABLE V
MAXIMUM INDEX OF FS ON LINKS (BPSK) FOR 6N9L NETWORK

D	100	150	200	250	300	350	400
1->2	12	20	13	27	13	30	22
1->3	4	3	12	4	23	12	23
2->3	10	14	19	19	27	31	36
2->4	12	25	20	20	27	30	36
2->5	19	22	30	46	37	57	54
3->5	14	15	29	29	47	39	53
4->5	7	11	15	23	22	26	30
4->6	0	10	0	0	0	0	0
5->6	18	15	30	36	45	48	54

V. CONCLUSION

In recent years, OFDM-based EON has been extensively studied as a promising paradigm which has high flexibility in traffic accommodation and can improve spectrum utilization. We proposed an MILP model which addresses the essential RMLSA issue in EON, focusing on determining appropriate modulation format and number of FSs for each request with the consideration of QoT. The numerical results showed that the proposed model could reduce the number of FSs required in network, comparing to the schemes which assume a fixed modulation format. Moreover, multiple modulation formats could help alleviate the uneven consumption of spectrum among fiber links.

Since the RMLSA problem is NP-hard and the computational complexity of optimization model is too high, we consider developing heuristic algorithms to solve the RMLSA problem in large-size networks. In addition, the energy efficiency, protection, fragmentation issues in EON can be studied for future work.

ACKNOWLEDGMENT

This work was supported by Basic Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2014-055177).

REFERENCES

- [1] S.K. Korotky, "Traffic trends: Drivers and measures of cost-effective and energy-efficient technologies and architectures for backbone optical networks," Optical Fiber Communication Conference and Exposition and the National Fiber Optic Engineers Conference (OFC/NFOEC), Los Angeles, CA, 2012.
- [2] O. Gerstel, "Elastic optical networking: a new dawn for the optical layer?," *IEEE Communications Magazine*, vol.50, no.2, pp.s12-s20, February 2012.
- [3] F. Tang, "Electronic Traffic Grooming in Dedicated Path Protected IP over Elastic Optical Network," Asia Communication and Photonics Conference (ACP), 2015.
- [4] K. Christodoulopoulos, I. Tomkos, E. Varvarigos, "Routing and spectrum allocation in OFDM-based optical networks with elastic bandwidth allocation," in: Proceedings of IEEE Globecom, 2010.
- [5] K. Christodoulopoulos, "Elastic Bandwidth Allocation in Flexible OFDM-Based Optical Networks," *Journal of Lightwave Technology*, vol.29, no.9, pp.1354-1366, May. 2011.
- [6] W. Wei, C. Wang, X. Liu, "Adaptive IP/optical OFDM networking design," Conference on Optical Fiber Communication, collocated National Fiber Optic Engineers Conference (OFC/NFOEC), vol. 1, no. 3, pp.21-25, March 2010.
- [7] A. Nag, T. Wang, B. Mukherjee, "On Spectrum-Efficient Green Optical Backbone Networks," *IEEE Global Telecommunications Conference (GLOBECOM)*, vol. 1, no. 5, pp.5-9, Dec. 2011.
- [8] M. Klinkowski, K. Walkowiak, "Routing and Spectrum Assignment in Spectrum Sliced Elastic Optical Path Network," *IEEE Communications Letters*, vol.15, no.8, pp.884-886, August 2011.
- [9] A. Cai, "Novel Node-Arc Model and Multi-Iteration Heuristic for Static Routing and Spectrum Assignment in Elastic Optical Networks," *IEEE/OSA Journal of Lightwave Technology*, Vol. 31, No. 21, pp. 3402 – 3413. Sept. 2013.
- [10] Y. Wang, "Towards elastic and fine-granular bandwidth allocation in spectrum-sliced optical networks," *Journal of Optical Communications and Networking*, Vol. 4, Issue 11, pp. 906–917, 2012.
- [11] K.D.R. Assis, R.C. Almeida, A.V.T. Cartaxo, A.F. dos Santos, H. Waldman, "Flexgrid optical networks design under multiple modulation formats," *International Telecommunications Symposium (ITS)*, vol. 1, no. 5, pp.17-20, Aug. 2014.
- [12] Y. Lui, G. Shen, W. Shao, and S. K. Bode, "Green IP over WDM Optical Network Design for Mixed Line Rates and Limited Transmission Reaches," in Proc. COIN 2013.
- [13] K. Christodoulopoulos, P. Soumplis, and E. Varvarigos. "Planning Flexgrid Optical Networks under Physical Layer Constraints" *Journal of Optical Communications and Networking*, Vol. 5, Issue 11, pp. 1296-1312, 2013.

Wideband Analog Transmission System Based on the External Intensity Electro-Optic Modulator

Jiri Svarny

Abstract—The work deals with design and integration of an analog electro-optic transmission system suitable for some specialized tasks of diagnostics and measurements. The system is based on principle of external intensity modulation of fiber guided laser radiation. Besides wideband and almost lossless transmission the system tolerates extreme length of the transmitting medium and ensures ultimate galvanic barrier between the input and output.

Keywords—Electro-optic modulator, fiber optics, intensity modulation, transmission system, wideband transmission.

I. INTRODUCTION

In regard to a measuring device the transmission system forms an important and integral part of the measuring chain. Its task is to deliver a sensed signal from a sensor to an instrument with the highest possible fidelity. In most of applications a coaxial cable is quite satisfactory to fulfill the needs. However, the transmission system based on the coaxial cable suffers from certain limitations:

A. Signal Attenuation

As the frequency range is low and the cable is not too long the attenuation is negligible. The higher the frequency of the signal and the longer the cable is the more severe attenuation the metallic transmission system demonstrates [1]. In the GHz range the attenuation can easily reach several dB/m depending on particular type of cable, see Fig. 1. If the transmission bandwidth is narrow the attenuation can be compensated by an additional amplification. A wideband transmission might need even more sophisticated equalization.

B. Galvanic Isolation

In case of different potentials of sensing ground and the ground of measuring instrument, the galvanic isolation is necessary. Standard galvanic isolation techniques (opto-couplers, linear isolation amplifiers, etc.) can hardly satisfy

the demands for the state of the art analog transmission system. If the barrier in the order of 10 kV is required, the above mentioned techniques are inapplicable and the transmission line has to be based on an optical link.

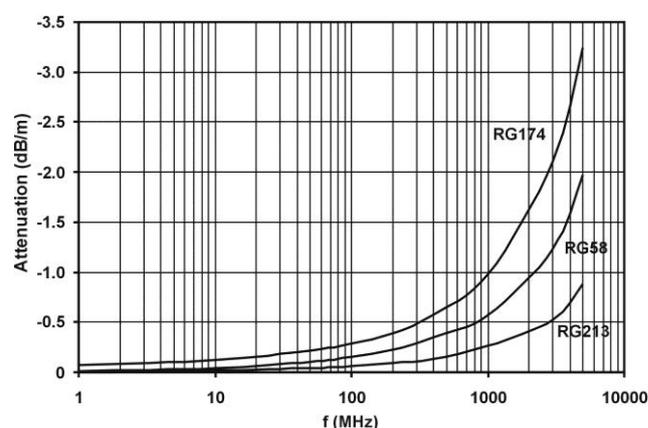


Fig. 1. Typical losses of common coaxial cables.

C. Measuring Input Protection

There can be expected some high-frequency (HF) and broadband (BB) measuring instrument at the end of the transmission link. Naturally, most of the HF oscilloscopes and spectrum analyzers use 50 Ω input with very low input voltage immunity (typically of 5 V_{pp}). The transmission system should be designed to provide the proper impedance match and the measuring instrument protection as well.

The paper brings solution of the transmission system that breaks some limits of coaxial cable and meets following requirements: The system has to be able to transmit very weak analog signals in range from μ V up to several tens of mV. Primarily, the system is aimed to measure a broadband signal from a sensor installed at the high voltage (HV) test stand and bring it to the broadband analyzer. The analyzer is located outside the HV area (10–100 m away). The input and output must be resistively matched to 50 Ω . The overall gain of the transmission system has to be positive (0 dB min.). A minimum frequency range of 10 kHz–2.5 GHz is required. The system must ensure galvanic isolation in the order of 10 kV or more.

Apparently, the only possibility is to use an analog fiber optic link (AFOL). Theory of the AFOL systems based either on directly or externally modulated laser have been discussed in many papers and books, see [2]–[10] for

Manuscript received November 10, 2015, revised January 28, 2016. This research has been supported by the European Regional Development Fund and the Ministry of Education, Youth and Sports of the Czech Republic under the Regional Innovation Centre for Electrical Engineering (RICE), project CZ.1.05/2.1.00/03.0094.

J. Svarny is with the Department of Technologies and Measurements, Faculty of Electrical Engineering / RICE, University of West Bohemia, Pilsen, Czech Republic (phone: +420-377-634-559; fax: +420-377-634-502; e-mail: svarny@ket.zcu.cz).

doi: 10.11601/ijates.v5i1.131

instance. The range of applications include: radio signal over fiber distribution, radar connection, remote antenna, EMC testing, signal waveform measurement and monitoring, wideband waveform detection, safe high voltage measurement etc. Some commercially available AFOL systems can be already found on the market (PPM Ltd., Pharad LLC, Teseo S.p.A., Spinner GmbH and other companies). They cover various frequency ranges depending on particular application. Unfortunately, there was not found any system on the market covering the all desired bandwidth (including both lower and upper cut-off frequency simultaneously). This fact was the motivation for development of the own specifically tailored solution.

II. THEORETICAL REFLECTION

To achieve adequate bandwidth and gain it was chosen a solution based on an external analog electro-optic modulator of Mach-Zehnder type (MZM), a powerful laser source and a fast photodetector with no post-amplifier.

The modulator works on principle of integrated Mach-Zehnder interferometer [11]. Maximum linearity and low distortion of the signal is got by proper biasing of the MZM at the quadrature operating point [12]. Input optical port is excited by a constant optical power generated by a distributed feedback (DFB) laser diode (LD). The measured signal is amplified and led to the radiofrequency (RF) port of the modulator. The output optical port generates the intensity modulated optical power. Finally, the optical signal is demodulated by a PIN photodiode (PD).

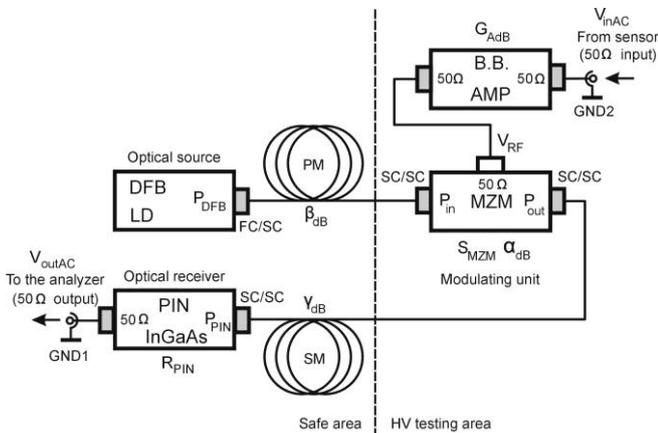


Fig. 2. Block diagram of the transmission system.

A positive overall gain G_{SdB} (1) of the transmission system is one of the vital features to accomplish with the design.

$$G_{SdB} = 20 \log \frac{V_{outAC}}{V_{inAC}} \geq 0dB \quad (1)$$

The PIN detector of the receiver is reversely biased and resistively matched to the R_L load. The AC component of the receiver output voltage V_{outAC} can be expressed by an AC component of a PIN photocurrent I_{PINAC} (2).

$$V_{outAC} = \frac{I_{PINAC}}{2} R_L \quad (2)$$

The PIN diode photocurrent I_{PINAC} is directly proportional to the detector input optical power. The R_{PIN} (responsivity of the PIN diode) represents the conversion constant between the incident optical power and the photocurrent. If the insertion loss of the single mode (SM) optical cable is γ_{dB} and the P_{outAC} stands for the AC component of the modulator output optical power, the V_{outAC} is (3).

$$V_{outAC} = \frac{R_{PIN}}{2} R_L P_{outAC} 10^{\frac{\gamma_{dB}}{10}} \quad (3)$$

Regarding the moderate modulation depth i.e. relatively low input voltage V_{RF} , the gain of the modulator can be expressed by a constant value S_{MZM} . V_{outAC} is (4) then.

$$V_{outAC} = \frac{R_{PIN}}{2} R_L 10^{\frac{\gamma_{dB}}{10}} S_{MZM} V_{RF} \quad (4)$$

The S_{MZM} parameter represents the slope efficiency (5) of the modulator for the positive quadrature operating point [13]. From mathematical point of view it is a tangent at the inflexion point of the modulator transfer chart, see Fig. 3.

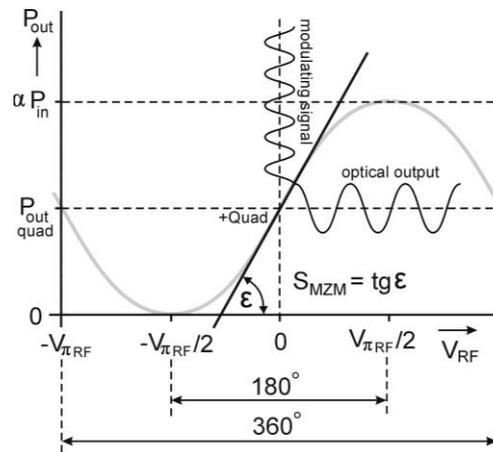


Fig. 3. Slope efficiency of the MZM biased to the positive quadrature point.

$$S_{MZM} = \frac{dP_{out}}{dV_{RF}} = tg \epsilon = \frac{P_{in} 10^{\frac{\alpha_{dB}}{10}} \pi}{2V_{\pi RF}} \quad (5)$$

The P_{in} is the input optical power, the α_{dB} is the insertion loss of fully open modulator and the $V_{\pi RF}$ is half-wave voltage of the RF port of the MZM. Provided there is used a pre-amplifier with the G_{AdB} gain in front of the MZM RF input, the equation (4) will expand to (6).

$$V_{outAC} = \frac{R_{PIN}}{2} R_L 10^{\frac{\gamma_{dB}}{10}} \frac{P_{in} 10^{\frac{\alpha_{dB}}{10}} \pi}{2V_{\pi RF}} 10^{\frac{G_{AdB}}{20}} V_{inAC} \quad (6)$$

Finally, taking into account the insertion loss of the input polarization maintenance (PM) optical cable β_{dB} , the overall gain of the electro-optic transmission system G_{SdB} can be expressed as (7).

$$G_{SdB} = G_{AdB} + 2(\alpha_{dB} + \beta_{dB} + \gamma_{dB}) + 20 \log \frac{R_{PIN} R_L P_{DFB} \pi}{4V_{\pi RF}} \quad (7)$$

Parameters R_{PIN} , R_L , α_{dB} , β_{dB} , γ_{dB} , $V_{\pi RF}$ are almost invariant constants regardless the choice of particular components. Nevertheless, the system gain G_{SdB} can be affected by the pre-amplifier gain G_{AdB} and by the optical power P_{DFB} as well. Fig. 4 depicts dependency of minimum needed gain of the RF pre-amplifier as a function of the laser optical power P_{DFB} in order to obtain the lossless transmission ($G_{SdB} = 0$ dB). The dependency was calculated for typical values of system components: $R_{PIN} = 0.7$ A/W (InGaAs photodetector @ 1550 nm), $R_L = 50 \Omega$, $\beta_{dB} = -0.5$ dB (PM patch-cord), $\gamma_{dB} = -0.3$ dB (SM patch-cord), $V_{\pi RF} = 3.7$ V, $\alpha_{dB} = -3$ dB (FA20 modulator).

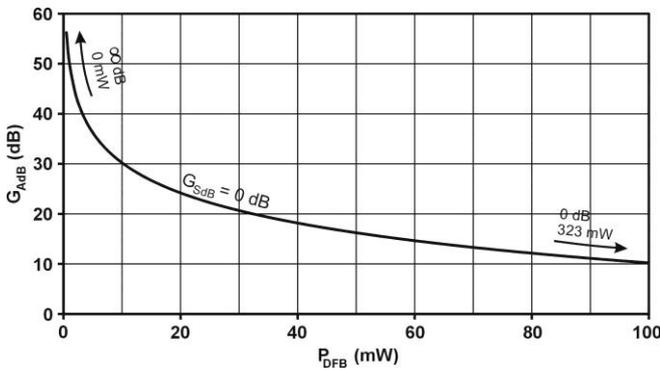


Fig. 4. Needed pre-amplification G_{AdB} as a function of P_{DFB} for lossless transmission ($G_{SdB} = 0$ dB).

Advantageously, the gain of the RF pre-amplifier can be decreased at the expense of the laser power. Unfortunately, this rule has some limits in fact. Probably the most severe one is inherent in maximum acceptable input optical power of the PIN detector P_{PINmax} . That is why, it is desirable to search for a detector that covers specified frequency range and is able to handle highest possible input power at the same time. The detector that was chosen has $P_{PINmax} = 10$ mW. As the P_{PINmax} value is defined, the maximum permissible laser power P_{DFBmax} can be stipulated by (8).

$$P_{DFBmax} = P_{PINmax} 10^{\left(\frac{\alpha_{dB} + \beta_{dB} + \gamma_{dB}}{10} \right)} \quad (8)$$

The maximum acceptable optical power P_{DFBmax} for safe operation of the PIN photodiode works out 24 mW. Consequently, in accordance with the Fig. 4, there is necessity to ensure 22.6 dB pre-amplification at minimum.

III. THE SYSTEM IMPLEMENTATION

A. Stabilized Optical Source

The pigtailed 20 mW/1550 nm DFB laser module A1905LMI [14] was used as a source of optical radiation. In addition to the LD itself, the laser module is equipped with a thermoelectric cooler, a NTC thermistor, a monitor PD and an optical isolator. The module is pigtailed with the PM fiber ended with standard FC/PC connector.



Fig. 2. DFB laser module A1905LMI.

In order to achieve desired behavior of the LD, there was necessary to design and implement effective LD drivers. The LD is operated in automatic current control regime (ACC). Simultaneously, the LD temperature is controlled by a thermoelectric cooler controller (TECC). The ACC controller is based on WLD3343 hybrid IC (Wavelength Electronics, Inc.). The TECC uses LTC1923 IC (Linear Technology, Inc.). Both the drivers are controlled by the Control Unit equipped with AT89S53 (Atmel, Inc.) microcontroller. The control unit coordinates operation of the controllers and monitors vital parameters of the laser module.

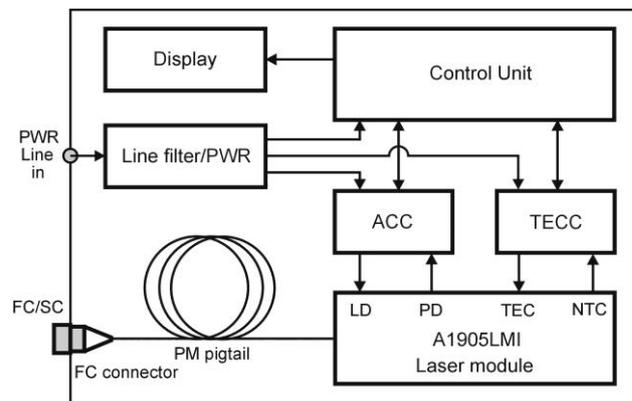


Fig. 6. Block diagram of the stabilized optical source.

A digital optical multimeter OMM6810B (by ILX Lightwave, Inc.) with InGaAs sensing head OMH6727B was used to verify the output optical power value and the stability of the laser source. It was found that the optical source generates power of 21.68 mW (i.e. tightly below acceptable maximum).

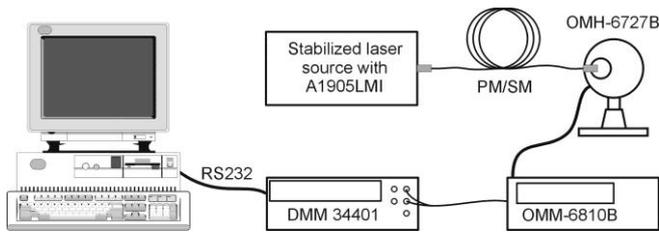


Fig. 7. The verification of the stabilized optical source.

The power fluctuation measurement was done using the Power Analog Out which is accessible on the rear panel of the OMM6810B. The Power Analog Out provides the amplified photocurrent generated by OMH6727B. An Agilent 34401 DMM was used to digitize the value. The data were measured with sampling rate of 2 Sa/s. The measurements revealed fluctuation $\Delta P_{out} = \pm 12.5 \mu\text{W}$ ($\pm 0.003 \text{ dB}$) oscillating around the average value of 21.68 mW (see Fig. 8.).

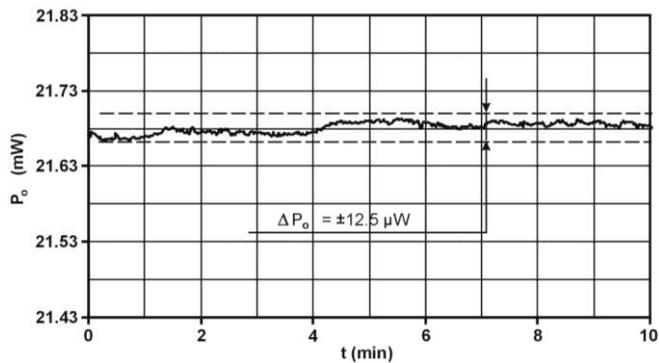


Fig. 8. Short-term stability measurements of the optical source.

Similar measurements were done to evaluate long-term stability. Result of the measurements can be seen in Fig. 9. The 3-hour-period of measurements revealed fluctuation $\Delta P_{out} = \pm 45 \mu\text{W}$ ($\pm 0.009 \text{ dB}$).

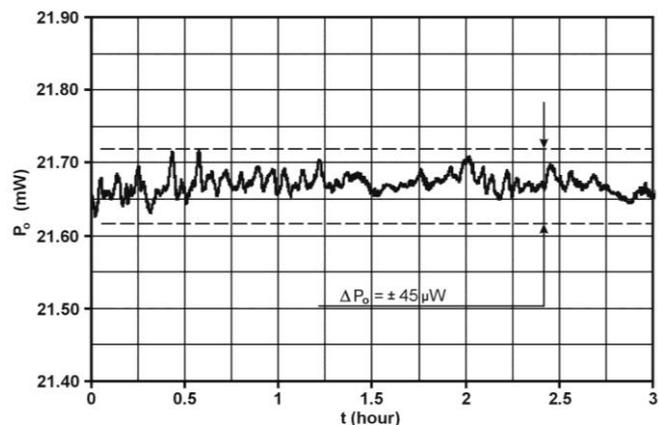


Fig. 9. Long-term stability measurements of the optical source.

The detailed description of the laser unit including the laser evaluation can be found in [15].

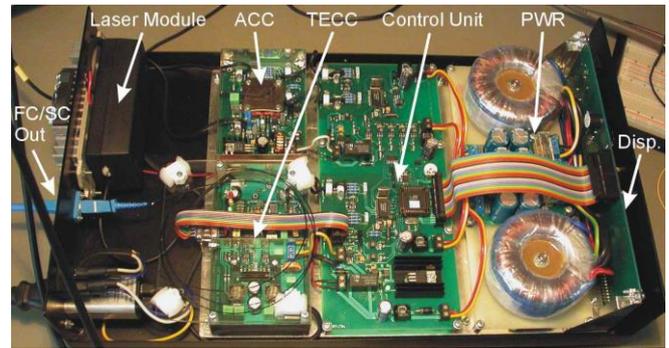


Fig. 10. Stabilized optical source.

B. External Modulating Unit

Analog intensity electro-optic modulator FA20 [16] forms a key part of the modulating unit. It is the interferometric modulator integrated in the LiNbO_3 substrate. The modulator has a standalone bias port for the operating point control and the modulating input (RF port). Besides that, the modulator is equipped with an integrated PD to monitor the output optical power. Bandwidth of the device is 13.7 GHz (-3 dB). Half-wave voltages are agreeably low (3.7 V @ RF port and $5.2 \text{ V @ bias port}$). Extinction ratio is relatively high (31.4 dB).

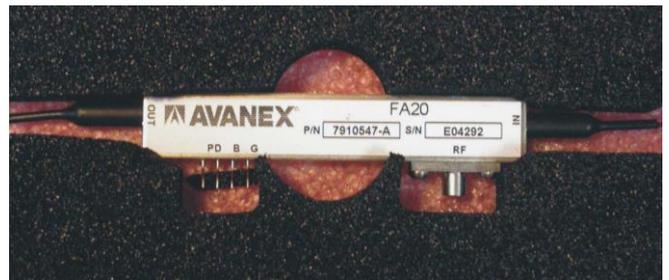


Fig. 11. The FA20 analog intensity modulator.

Inner circuitry of the modulating unit consists of three parts (a MZM baseboard, a RF pre-amplifier & power supply block and a bias driver block). The MZM baseboard comprises the modulator, protection circuits, a bias port buffer and a transimpedance amplifier of the MZM inner PD. The power supply block (battery pack) is integrated with a charger and the low-noise, broadband pre-amplifier ABL0300 (9 kHz–3 GHz) [17]. Nominal gain of the pre-amplifier (32 dB) has a sufficient headroom over the calculated G_{AdB} minimum.

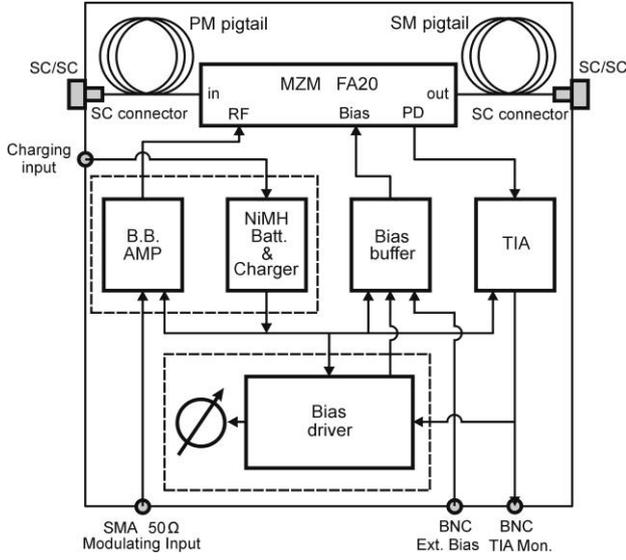


Fig. 12. Block diagram of the external modulating unit.

Desired response of the MZM is achieved by proper adjustment of the operating point to the quadrature position. This task is solved by the bias driver. The bias driver takes advantage of known frequency response of the modulator biased at the proximity of quadrature point. Provided the input bias voltage is formed by DC component V_{DC} and superposed AC harmonic component with V_{AC} amplitude (9), the output optical power P_o of the MZM can be described by (10).

$$V_{in} = V_{DC} + V_{AC} \sin(\omega_{AC} t) \quad (9)$$

$$P_o = \frac{\alpha P_{in}}{2} + \frac{\alpha P_{in}}{2} \cos\left(\frac{V_{DC}}{V_{\pi}} \pi\right) J_0\left(\frac{V_{AC}}{V_{\pi}} \pi\right) +$$

$$+ \alpha P_{in} \cos\left(\frac{V_{DC}}{V_{\pi}} \pi\right) \sum_{k=1}^{\infty} J_{2k}\left(\frac{V_{AC}}{V_{\pi}} \pi\right) \cos(2k\omega_{AC} t) -$$

$$- \alpha P_{in} \sin\left(\frac{V_{DC}}{V_{\pi}} \pi\right) \sum_{k=1}^{\infty} J_{2k-1}\left(\frac{V_{AC}}{V_{\pi}} \pi\right) \sin[(2k-1)\omega_{AC} t], \quad (10)$$

where P_{in} is the input optical power of the MZM, α is the insertion loss of the MZM, V_{π} is half-wave voltage of the bias port of the MZM and $J_k(x)$ is a k^{th} order Bessel function. For detailed derivation see [18]. From the equation (10) formulas for computing the magnitude level of particular n^{th} harmonic component (11), (12) can be easily extracted.

$$P_{o-n-odd} = \left| \alpha P_{in} \sin\left(\frac{V_{DC}}{V_{\pi}} \pi\right) J_n\left(\frac{V_{AC}}{V_{\pi}} \pi\right) \right|, \quad (11)$$

where $n \in \langle 1, 3, 5, \dots \rangle$

$$P_{o-n-even} = \left| \alpha P_{in} \cos\left(\frac{V_{DC}}{V_{\pi}} \pi\right) J_n\left(\frac{V_{AC}}{V_{\pi}} \pi\right) \right|, \quad (12)$$

where $n \in \langle 2, 4, 6, \dots \rangle$

Equations (11) and (12) can be used to visualize the levels of particular harmonic components at the output of MZM as a function of DC level at the bias port. The amplitudes of the first three harmonics were depicted in Fig. 13. The curves were computed for input optical power $P_{in} = 21.68$ mW, the FA20 parameters ($\alpha = 0.5$, $V_{\pi} = 5.2$ V) and modulating voltage $V_{AC} = 500$ mV.

It is clear that the magnitude of 2^{nd} harmonic component reaches its minimum just at the quadrature point. Moreover, the 2^{nd} harmonic reflects the position of the desired operating point around the quadrature region with an extraordinary sensitivity. It brings the possibility to use the 2^{nd} harmonic component as an indicator of proper setup. The implemented bias driver utilizes the phenomenon.

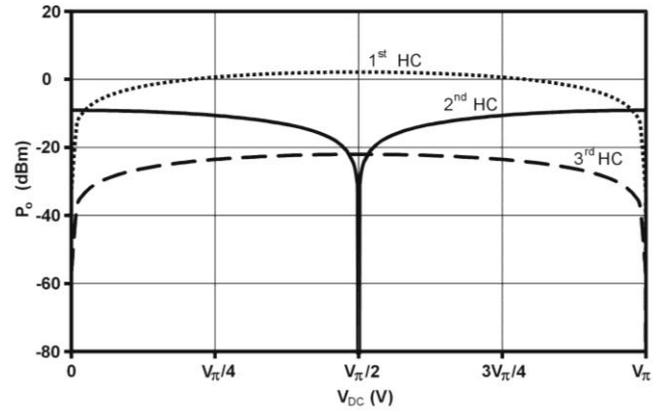


Fig. 13. Dependency of 1^{st} , 2^{nd} and 3^{rd} harmonics on DC bias V_{DC} .

The bias input port of the modulator is excited by a manually adjustable DC level and superimposed LF harmonic signal. Simultaneously, the inner PD of the MZM detects output signal of the modulator. Following circuitry analyses presence of 2^{nd} harmonic component in the spectrum of detected signal. The detailed structure of the circuit is depicted in Fig. 14.

The DC level is generated by a voltage reference (VREF) and manually adjustable divider (DC Bias). The AC part generates 1 kHz sinus signal with amplitude of 500 mV. Purity of the AC signal is important. That is why there was used method based on filtration of square wave signal. The quartz oscillator (XO) generates 4.096 MHz digital signal that is divided and shaped by a binary 12-stage ripple counter (DIV). As the spectrum of the generated square wave consists of odd harmonics only, the problem of absence of second harmonic is resolved spontaneously then. The higher odd harmonics are cut-off by a narrow band-pass filter BPF1 with center frequency of 1 kHz.

The signal from BPF1 block is mixed with DC level from the DC Bias block by means of summing amplifier Σ_1 . The following stage gives a π phase shift to the signal. This is vital for analysis of the signal detected by the inner monitor photodiode PD.

The measuring chain has to analyze presence of 2^{nd} harmonic in the output spectrum and visualize its magnitude. The inner PD of the MZM generates current that is inversely proportional to the output optical power of the modulator.

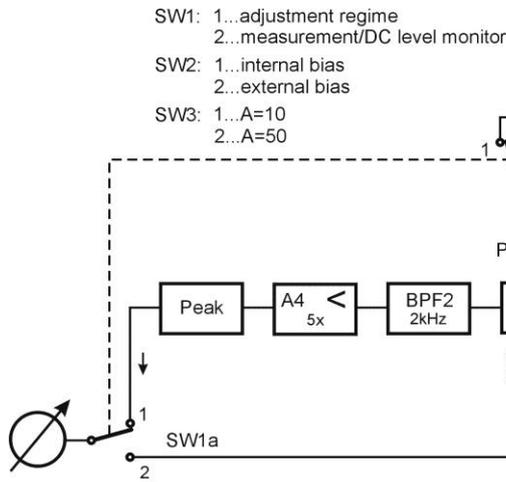


Fig. 14. Block diagram of the bias driver.

The signal of the PD is conditioned by means of transimpedance amplifier (TIA). Gain of the TIA was experimentally set to -470 V/mA. The DC level of the TIA output signal is excluded by amplifier with integrating feedback (AC couple stage). To derive 2nd harmonic from the spectrum, there is necessary to eliminate fundamental in received spectrum at first. This is carried out by summing amplifier Σ_2 . Due to the phase shift of the received signal the summing amplifier Σ_2 works as a difference amplifier in fact. At the output of the Σ_2 the difference between the received AC signal and the exciting signal can be found. (As there has to be set-up certain level of attenuation of exciting signal to achieve substantial decimation of fundamental at the output of Σ_2 block the exciting signal is attenuated by the A2 block.) The signal is amplified by the A3 amplifier and filtered by BPF2 filter then. The BPF2 stage forms a band-pass filter tuned to 2nd harmonic of the exciting signal. After an additional amplification in A4 block the signal is detected by a peak detector (Peak) and sent to the deflective measuring instrument.

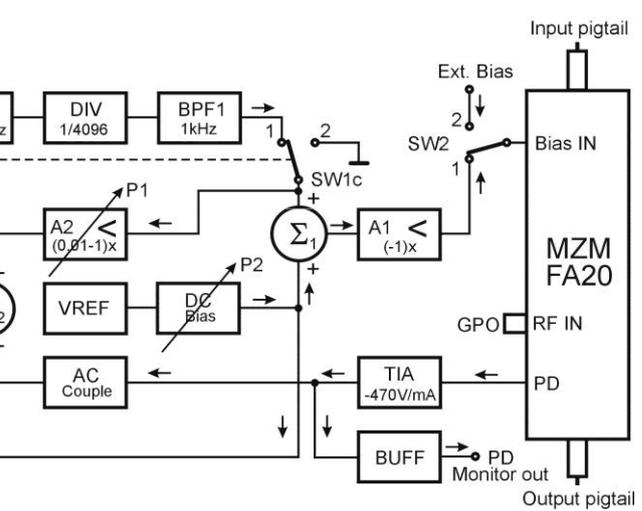
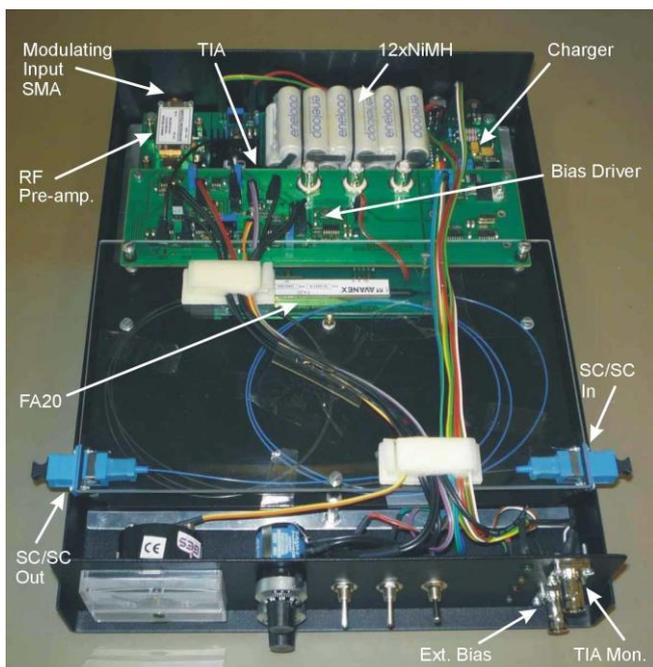


Fig. 15. External modulating unit.

A. Receiver

The receiver is formed by an optical detector which works as a demodulator. The detector converts the intensity modulated optical power to an electrical signal. Wide bandwidth and high linearity of the receiver is achieved thanks to operation in passive regime (i.e. with no post-amplifier).

The overall gain of the transmission system is concentrated partially in the RF pre-amplifier of the modulator and partially in the high optical power of the laser. That is why it was necessary to use a detector with the linear response up to 10 mW of input optical power. There was used a special broadband telecommunication PIN photodiode 2522A (Emcore, Inc.) [19]. The PD is working with a negative bias and is internally resistively matched to 50 Ω . Bandwidth of the photodiode is DC–15 GHz and minimum responsivity is 0.7 A/W @ 1550 nm. The photodiode module is equipped with the SM pigtail ended with standard SC/PC connector.

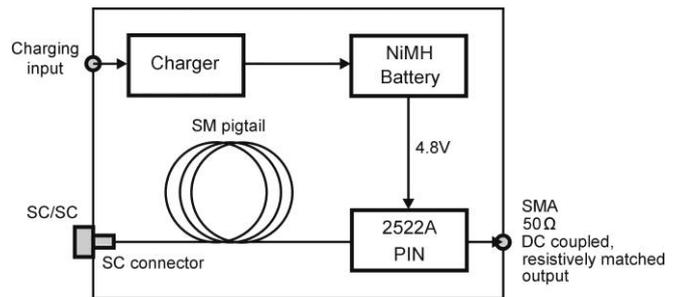


Fig. 16. Block diagram of the receiver.

The receiver uses a battery pack of 4 NiMH cells as a power supply. A battery charger is integrated on the circuit board. Low supply voltage and galvanic isolation from the rest of the system, make the receiver the absolutely safe source of signal to a sensitive frontend of any prospective BB analyzer or a HF oscilloscope.

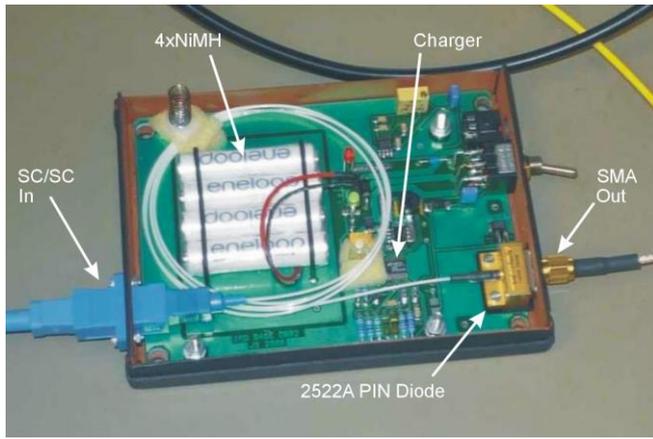


Fig. 17. Broadband optical receiver.

IV. RESULTS

Based on theoretical consideration there were designed and implemented all the three parts of the broadband electro-optic transmission system. Subsequently, measurements of the frequency response were carried out. Lower cut-off frequency was tested by the oscilloscope. Upper part of the range (above 300 kHz) was tested by the ZVB8 network analyzer.

The measured frequency range of the system is 9 kHz–3.45 GHz (-3 dB). In accordance with (7), the theoretical value of the overall gain should be 8.5 dB. Nevertheless, the measurement revealed the average gain of 6 dB. Frequency chart is relatively flat and well balanced (6 dB ±1.5 dB).

The difference between expected and real value of the gain is relatively small (2.5 dB). The divergence can be justified by a sum of several factors. Firstly, the insertion loss of the optical patch-cords may slightly differ from the nominal value. Furthermore, to ensure demountable connection between the units there have been implemented the SC/SC optical cable adapters. Two of them can be found between the laser and the modulator and the next two between the modulator and the detector. Each of the adapters has power to bring an additional insertion loss uncertainty. Last but not least, it must be kept in the mind that all the calculations were made on basis of typical data sheet parameters that may slightly differ from reality.

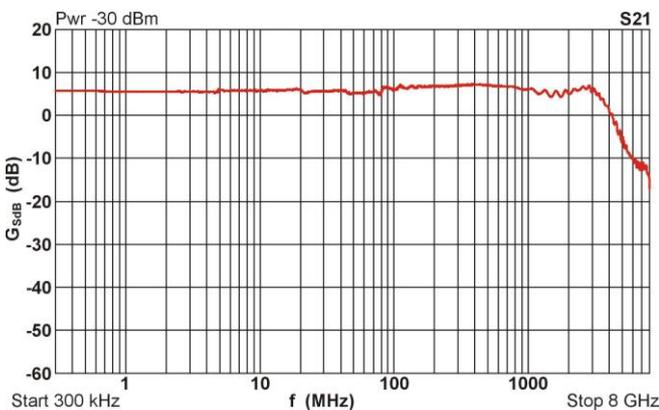


Fig. 18. The frequency response of the transmission system measured by the ZVB8 network analyzer.

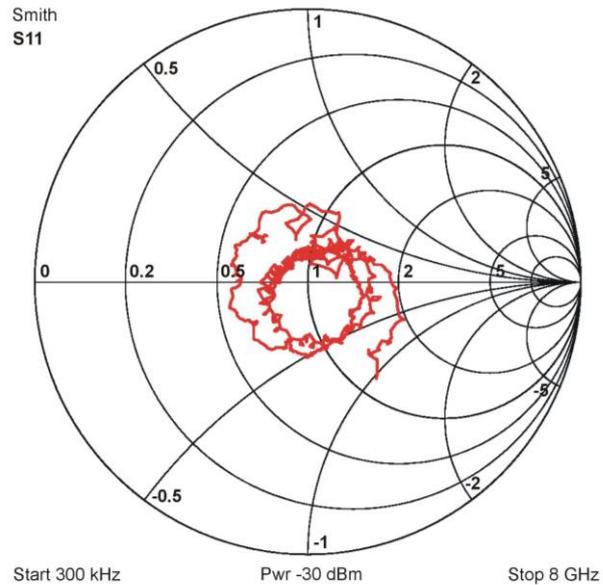


Fig. 19. The Smith chart of S11 parameter of the transmission system measured by the ZVB8 network analyzer.

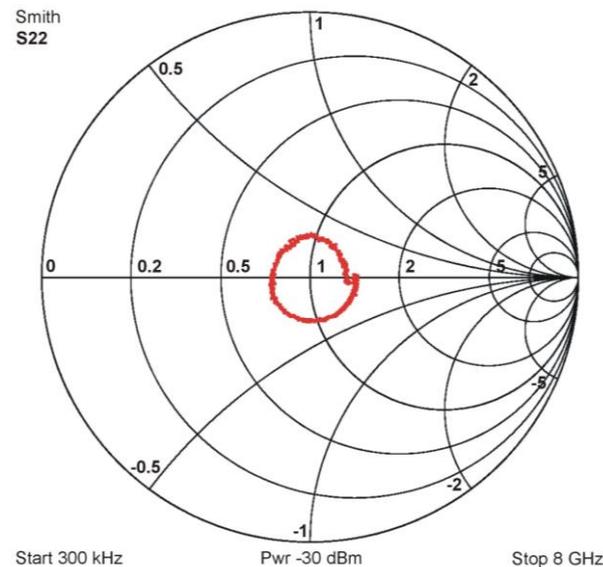


Fig. 20. The Smith chart of S22 parameter of the transmission system measured by the ZVB8 network analyzer.

The network analyzer was also used to evaluate the input and output impedance matching of the designed transmission system. There were measured S11 and S22 parameters (Fig. 19, Fig. 20). The values of the measured S-parameters were used to calculate the voltage standing wave ratio (VSWR) for input and output port respectively and for particular termination of the system, see Fig. 21 and Fig. 22.

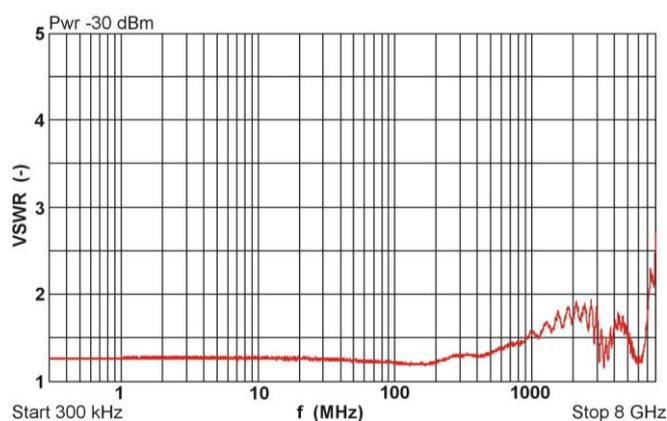


Fig. 21. The voltage standing wave ratio for the transmission system input port (50 Ω termination of the input).

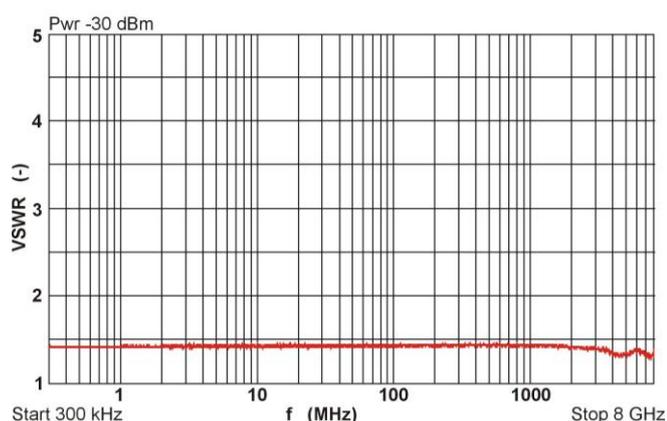


Fig. 22. The voltage standing wave ratio for the transmission system output port (50 Ω termination of the output).

Taking into account the upper cut-off frequency of the system (3.45 GHz), the matching of the input to the 50 Ω source is characterized with VSWR of 1.2:1 up to 1.9:1. The matching of the output of the system to the 50 Ω load is characterized with VSWR of 1.3:1 up to 1.4:1.

TABLE I
COMPARISON OF THE RESULTS

System	Company	Bandwidth [MHz]	Gain [dB]	Flatness [dB]	VSWR [-]
K series [20]	PPM	0.002–1350	0	± 3.0	1.5
S series [20]	PPM	10–3000	0	± 1.5	1.5
Eco Line [21]	Spinner	50–2400	5	± 0.5	2
PXR001-190 [22]	Pharad	3–19000	15	± 2.0	2
PXR005-030 [23]	Pharad	500–3000	0	± 1.0	2
OAM208 [24]	Teseo	0.5–3000	0	± 4.0	1.4
Presented solution	RICE	0.009–3450	6	± 1.5	1.9

Table I resumes a brief comparison of our developed system (last line) with the similar systems that are commercially available on the market. Apparently, the main advantage of our system is inherent in the remarkably favorable lower cut-off frequency and relatively high gain. The VSWR column gives the worst case values across the frequency range of the particular system. In case of our solution the VSWR value was mostly affected by behavior of the input port at the very end of the frequency range. For bottom and middle part of bandwidth of the system (up to

1 GHz approximately) the impedance matching is apparently better. Across the measured bandwidth the VSWR of the output port itself works out significantly better in comparison to the presented value as well.

V. CONCLUSION

There was designed and implemented unique analog transmission system for the safe connection of the HF 2.5 GHz oscilloscope to a sensor which works at very high potential. Problem of ultimate galvanic isolation and oscilloscope protection was solved by implementation of an optical fiber as the transmission media and battery-powered units. Unlike the metallic cable the length of the used medium can be prolonged up to hundreds of meters with virtually no impact to the signal quality. Upper and lower cut-off frequencies are mostly given by the broadband RF pre-amplifier features. (The frequency range of the modulator and the detector itself is much higher.) Thanks to the external modulation, the overall gain of the system would be increased by an additional increase of the laser power. Unfortunately, the method assumes use of a detector with even higher input power capability. Because such a detector is nowadays unavailable, the system works at its optical power maximum.

REFERENCES

- [1] *Coaxial Cable Attenuation ratings*, National Wire and Cable Corp., [Online]. Available: <http://www.nationalwire.com/pdf/COAXIAL-ATTENUATION.pdf>
- [2] E. I. Ackerman, C. H. Cox III, "RF fiber-optic link performance," *IEEE Microwave Magazine*, vol. 2, pp. 50–58, December 2001.
- [3] C. Cox III, E. Ackerman, R. Helkey, G. E. Betts, "Techniques and performance of intensity-modulation direct-detection analog optical link," *IEEE Trans. on Microwave Theory and Techniques*, vol. 45, no. 8, pp. 1375–1383, August 1997.
- [4] E. I. Ackerman, W. K. Burns, G. E. Betts, J. X. Chen, J. L. Prince, M. D. Regan, H. V. Roussel, C. H. Cox III, "RF-over-fiber links with very low noise figure," *IEEE Journal of Lightwave Technology*, vol. 26, no. 15, pp. 2441–2448, August 2008.
- [5] C. H. Cox III, E. I. Ackerman, G. E. Betts, J. L. Prince, "Limits on the performance of RF-over-fiber links and their impact on device design," *IEEE Transactions on Microwave Theory and Techniques*, vol. 54, no. 2, February 2006.
- [6] I. L. Newberg, "High-performance lossless RF fiber optic link," in *Proc. International Conference on Phased Array Systems and Technology*, Dana Point, CA, 2000, pp. 375–378.
- [7] E. I. Ackerman, C. H. Cox III, "State of the art in analog fiber-optic link technology," in *Proc. URSI International Symposium on Signals, Systems and Electronics ISSSE98*, Pisa, 1998, pp. 372–377.
- [8] J. M. Senior, *Optical Fiber Communications—Principles and Practice*, Prentice Hall, 1992.
- [9] C. H. Cox III, *Analog Optical Links—Theory and Practice*, Cambridge University Press, 2004.
- [10] A. Brilliant, *Digital and Analog Fiber Optic Communications for CATV and FTTx Applications*, SPIE Press, 2008.
- [11] A. Chen, E. J. Murphy, *Broadband optical Modulators—Science, Technology and Applications*, CRC Press, 2012.
- [12] A. Hilt, "Microwave harmonic generation in fiber-optical links," *Journal of Telecommunications and Information Technology*, vol. 1/2002, pp. 22–28, 2002.
- [13] J. Svamy, "Analysis of quadrature bias-point drift of Mach-Zehnder electro-optic modulator," in *Proc. International 12th Biennial Baltic Electronics Conference BEC2010*, Tallinn, 2010, pp. 231–234.
- [14] *PowerSource™ 1905LMI CW laser module with optical isolator, Up to 30 mW, C-Band*, Avonex Inc., 2005, [Online]. Available: http://www.lightwavestore.com/product_datasheet/OSC-LDPM-C-011C_pdf1.pdf

- [15] J. Svarny, "Highly stable 20 mW infrared laser source," in *Proc. International Conference Applied Electronics 09*, Pilsen, 2009, pp. 249–252.
- [16] *PowerLog™ FA-20, 20 GHz Analog Intensity Modulator*, Avanex Inc., 2009, [Online]. Available: http://www.amstechnologies.com/fileadmin/amsmedia/downloads/3510_Oclaro_PowerLog_FA20_v2_1.pdf
- [17] *Broadband Low Noise Amplifier ABL0300-00-3230*, Wenteq Microwave Corp., [Online]. Available: <http://www.wenteq.com/Amplifier-PDF/ABL0300-00-3230.pdf>
- [18] J. Svarny, "Specialized Compact External Electro-Optic Modulating Unit," in *Proc. 36th International Conference on Telecommunications and Signal Processing TSP2013*, Rome, 2013, pp. 227–230.
- [19] *2522 Microwave Packaged Photodiode*, Emcore Corp., 2007, [Online]. Available: <http://www.emcore.com/wp-content/uploads/25221.pdf>
- [20] *Point2point—AC Coupled Fiber Optic Link*, PPM Ltd., 2011, [Online]. Available: <http://ppmtest.com/wp-content/uploads/point2point-AC-Link-Datasheet-PAx-DS-7.pdf>
- [21] *Eco Line Analog Fiber Optic Link*, Spinner GmbH, 2008, [Online]. Available: http://www.spinner-group.com/upload/de_D_FO_ECO_304.pdf
- [22] *HF – K-band Photonic Transceiver 0.003 GHz–19 GHz*, Pharad, 2013, [Online]. Available: <http://www.pharad.com/pdf/hf-k-band-rf-photonic-transceiver-datasheet.pdf>
- [23] *UHF – S-band Photonic Transceiver 0.5 GHz–3 GHz*, Pharad, 2013, [Online]. Available: <http://www.pharad.com/pdf/uhf-s-band-rf-photonic-transceiver-datasheet.pdf>
- [24] *OAM208 Optical Acquisition Module 500 kHz–3 GHz*, Teseo S.p.A., 2007, [Online]. Available: <http://www.teseo.net/lang1/files/ds294ab.pdf>

Investigating the Performance of the MPT Multipath Communication Library in IPv4 and IPv6

Béla Almási, Szabolcs Szilágyi

Abstract—The currently used mobile devices (laptops, tablets, mobile phones) contain many built-in network cards for communication (e.g. Wi-Fi, 3G, Bluetooth, etc.). A natural request could be combining the resources of the different network connection possibilities in order to increase the throughput of the communication. Unfortunately the standard IP communication technology does not support it: the communication is restricted to one IP address (i.e. to one interface). The Multipath TCP (MPTCP) specification (appeared in January 2013) offers a Transport layer solution of using more than one interface in a TCP communication session. In this paper we investigate a Network layer solution. The MPT multipath communication library opens the multipath communication possibility in the Network layer. Using the MPT library, applications built on the UDP protocol are also able to perform multipath communication. The MPT library was developed by using a full dual-stack technology, which means the MPT based multipath environment can be used both in IPv4 and IPv6. Protocol version change is also possible: an IPv6 based application is able to run in an IPv4 multipath environment, and an IPv4 application can be used in an IPv6 multipath environment. In this paper we give a short overview on the MPT communication library's working mechanism and detailed numerical examples will be shown to present how the MPT library aggregates the paths' throughput in IPv4 and IPv6 environments. The main contribution of the paper is to demonstrate the effective throughput aggregation property of the MPT library in IPv6 and in mixed (i.e. protocol version change) environments.

Keywords—IPv6, Multipath communication, throughput performance, tunnel.

I. INTRODUCTION

The traditional IP communication infrastructure is restricted to use a single interface on the communication endpoints. The IP address of the interface is used not only to identify the node, but it is also used to identify the communication session (socket ID). Distributing a communication session between different paths is an interesting question, and it is a focused research area today (see e.g. [6] – [8]). If the communication session is terminated on a moving node (e.g. on a computer located in a moving car) then it may request for establishing an efficient L3 roaming communication (see e.g. [3]). Opening the possibility of changing the IP address

of the end node (with the assumption that the communication session must continue), could open a quite new conceptual solution idea for well-known handover problems (see e.g. [2]): The moving computer could easily change its IP address without losing the communication session's state by changing a path only.

In this paper we investigate the performance of the MPT software library which was developed at the Faculty of Informatics, University of Debrecen in Hungary. The MPT software library offers a Network layer multipath communication possibility for the computers (typically having multiple network interfaces). The MPT software creates a logical interface (tunnel interface) on the host. The communication of the logical interface is mapped to the physical interfaces dynamically by the MPT software. The applications use the IP address of the tunnel interface for the communication session's identification, so there is no need for modification in the applications' communication software. When an application sends an IP packet, it will use the address of the logical interface (i.e. the address of the tunnel interface) as the sender address. This packet will be encapsulated into a new UDP segment and IP packet by the MPT software. The new IP packet can be dynamically assigned to a physical interface of the host, i.e. the new packet will use the IP address of a physical interface as the sender address. The MPT library covers the task of mapping between the tunnel interface and the physical interfaces. If we change the IP address of the physical interface (or even we change the physical interface itself) the application will not sense this change, it will continue the work over the tunnel interface. The MPT software will recognize the changing and will reorganize the mapping from the tunnel interface to the physical interface, according to the new situation. The layered structure of the MPT networking system can be seen in Figure 1.

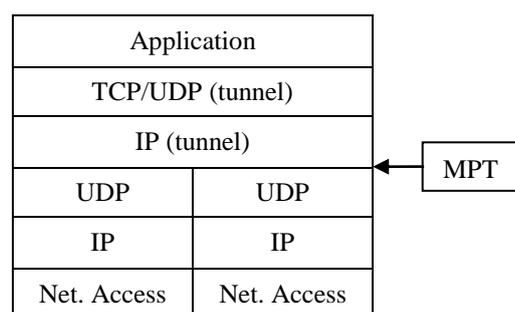


Fig. 1. The layered structure of the MPT multipath environment

Manuscript received November 15, 2015, revised February 25, 2016.
 B. Almási, is with the Faculty of Informatics, University of Debrecen, Debrecen, Hungary (e-mail: almasi.bela@inf.unideb.hu).
 Sz. Szilágyi is with the Faculty of Informatics, University of Debrecen, Debrecen, Hungary (e-mail: szilagyi.szabolcs@inf.unideb.hu).
 doi: 10.11601/ijates.v5i1.148

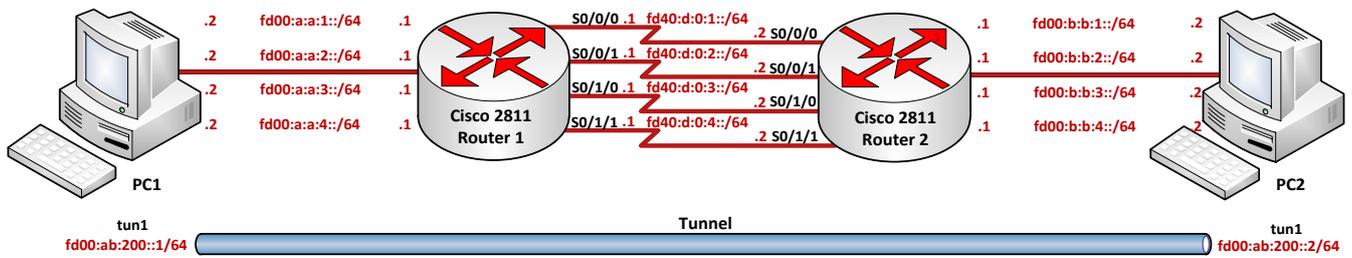


Fig. 2. The four paths measurement laboratory environment

It is easy to see that the tunnel interface and the physical interface may use different IP versions: the application may use the IPv4 address of the tunnel interface while the physical network environment may use IPv6 addresses on the physical interfaces. The protocol change is automatically performed by the MPT software.

It must be mentioned, that the RFC 6824 document (see [7], [8]) also introduces a multipath communication technology, but it works in the Transport layer, and the application is restricted to use the TCP protocol. The MPT library works in the Network layer and the application is able to use the UDP protocol too (e.g. for voice or media content transmission).

In order to precisely measure the throughput aggregation performance of the MPT library we established a measurement test-network environment. The measurement laboratory contains 4 paths between the endpoints, and is able to perform communication in IPv4 and IPv6 (offering the possibility of study mixed protocol versions.) Although the aggregation efficiency of the paths' throughputs of the different IP versions are not the same, the results show that the MPT environment successfully aggregates the paths' throughput in IPv4, IPv6 and mixed protocol versions too.

The rest of the paper is organized as follows: Section 2 describes the measurement laboratory network environment. Section 3 shows the measurement results performed in IPv4. Section 4 discusses the measurement results using IPv6 and section 5 will show the measurement results of a mixed protocol environment: in this section the application uses IPv4 (over the tunnel interface) and the real network environment uses IPv6 (on the physical interfaces).

This paper is some kind of continuation of paper [6]: the authors studied the handover capabilities of the MPT software library on the 37th TSP Conference in 2014. In this paper we make a step forward, and investigate the performance of the MPT library in a multiprotocol (IPv4/IPv6) environment.

II. THE MEASUREMENT NETWORK ENVIRONMENT

The measurement test-laboratory contained two PCs (having 8 GB of main memory and Intel Core i5 processor with 2.5GHz, and 6MB cache; using the operating system of Ubuntu 12.04). The PCs were equipped with four interfaces (eth0, eth1, eth2 and eth3). The four interfaces of the PCs were connected to each other by four different paths. The paths were realized by using two Cisco 2811 type routers. The routers were connected to each other by four serial links, thus establishing 4 different paths.

TABLE I
IPv4 AND IPv6 ADDRESSING

Dev	Inter- face	IPv4/IPv6 address/prefix	Default gateway
PC1	eth0	172.16.1.2/24 fd00:a:a:1::2/64	172.16.1.1/24 fd00:a:a:1::1/64
	eth1	172.16.2.2/24 fd00:a:a:2::2/64	172.16.2.1/24 fd00:a:a:2::1/64
	eth2	172.16.3.2/24 fd00:a:a:3::2/64	172.16.3.1/24 fd00:a:a:3::1/64
	eth3	172.16.4.2/24 fd00:a:a:4::2/64	172.16.4.1/24 fd00:a:a:4::1/64
	tun1	1.2.3.2/24 fd00:ab:200::1/64	-
PC2	eth0	10.150.1.2/24 fd00:b:b:1::2/64	10.150.1.1/24 fd00:b:b:1::1/64
	eth1	10.150.2.2/24 fd00:b:b:2::2/64	10.150.2.1/24 fd00:b:b:2::1/64
	eth2	10.150.3.2/24 fd00:b:b:3::2/64	10.150.3.1/24 fd00:b:b:3::1/64
	eth3	10.150.4.2/24 fd00:b:b:4::2/64	10.150.4.1/24 fd00:b:b:4::1/64
	tun1	1.2.3.3/24 fd00:ab:200::1/64	-
R1	FE 0/0.1	172.16.1.1/24 fd00:a:a:1::1/64	-
	FE 0/0.2	172.16.2.1/24 fd00:a:a:2::1/64	-
	FE 0/0.3	172.16.3.1/24 fd00:a:a:3::1/64	-
	FE 0/0.4	172.16.4.1/24 fd00:a:a:4::1/64	-
	serial 0/0/0	192.168.1.1/30 fd40:d:d:0:1::1/64	-
	serial 0/0/1	192.168.2.1/30 fd40:d:d:0:2::1/64	-
	serial 0/1/0	192.168.3.1/30 fd40:d:d:0:3::1/64	-
R2	FE 0/0.1	10.150.1.1/24 fd00:b:b:1::1/64	-
	FE 0/0.2	10.150.2.1/24 fd00:b:b:2::1/64	-
	FE 0/0.3	10.150.3.1/24 fd00:b:b:3::1/64	-
	FE 0/0.4	10.150.4.1/24 fd00:b:b:4::1/64	-
	serial 0/0/0	192.168.1.2/30 fd40:d:d:0:1::2/64	-
	serial 0/0/1	192.168.2.2/30 fd40:d:d:0:2::2/64	-
	serial 0/1/0	192.168.3.2/30 fd40:d:d:0:3::2/64	-
serial 0/1/1	192.168.4.2/30 fd40:d:d:0:4::2/64	-	

The physical link of the Ethernet connection was common in the paths, but the high speed of this common link (100 Mbps) made it sure that the bottleneck point of the paths was not in the common part of the network. (The maximum clock rate of the serial links was set to 2.000.000 cycles per seconds. The clock rate setting of the DCE serial interfaces was used to tune the bandwidth of the paths independently to each other. The PCs were connected to the routers using 100 Mbps Ethernet links, so the bottleneck point of the communication was realized on the serial links between the routers.). All the routing settings were implemented by static entries both in the routers and in the PCs. The IP addressing scheme of the measurement network can be seen in Table I.

III. MEASUREMENT RESULTS – IPV4 ONLY NETWORK

In order to test the throughput of the network system two types of measurements have been carried out. The first type of the measurement used symmetrical paths with clock rate values of 1.000.000 and 2.000.000 cycles per second respectively (see Table II, cases 1-4). The second type of measurement used non-symmetrical paths: the four links between the serial interfaces used all the possible combination of the clock rate values of 1.000.000 and 2.000.000 (see Table II, cases 5-10). All measurement types contained two cases, which differed only in the size of the transmitted file: in the first case the transmitted file's size was 10 MB, and it was 20 MB in the second one. For all cases (assumed also in the following sections) the efficiency in the tunnel has been evaluated as:

$$\text{Tunnel efficiency [\%]} = \frac{\text{throughput value measured on tunnel interface}}{\text{sum of the throughput values measured on physical interfaces}} * 100 \quad (1)$$

The measurement tests were always repeated ten times for each type of measurement and for each data size. The results were constantly the same: the differences between the measured throughput values were less than 3%. The host PC1 was used as the FTP server starting the built in FTP server daemon of the operating system (vsftpd). The built-in FTP client was used on PC2 to download the files. The System Monitor application was used to create the measurement reports. The detailed measurements' results are shown in Table II. and Figures 3. – 10. The figures show the interface throughput values for the test cases using 10 and 20 MB file sizes. The variance of the interface throughput increases a little bit at the aggregation. The results show the same performance for both file sizes: it is easy to see that the transmission time increases linearly with the data size on the physical interfaces (on the tunnel interface too), i.e. the throughput aggregation does not depend on the data size. (The difference is less than 3% in all cases.) Concerning the user's point of view, the Application layer's throughput is much more interesting than the interface throughput. The values of the throughput measured in the Application layer (i.e. dividing the transmitted data size with the transmission time, measured in seconds) can be seen in Table II (the transmitted data size is measured in 1024 bytes unit). Of course, the interface throughput values (in Figures 3. – 10.) are a little bit higher than the Application layer's one, because of the additional header information appearing on

the interfaces.

TABLE II
FTP FILE TRANSMISSION RESULTS – IPV4 ONLY NETWORK

Case	Interface	Time (sec)	Throughput (KB/s)	Efficiency (%)
Case 1. 10 MB 1 M / 1 M 1 M / 1 M	tun1	22	465,5	99,9
	eth0-3	88	116,4	
Case 2. 20 MB 1 M / 1 M 1 M / 1 M	tun1	45	455,1	98,3
	eth0-3	177	115,7	
Case 3. 10 MB 2 M / 2 M 2 M / 2 M	tun1	11	930,9	99,9
	eth0-3	44	232,8	
Case 4. 20 MB 2 M / 2 M 2 M / 2 M	tun1	22	930,9	99,9
	eth0-3	88	232,8	
Case 5. 10 MB 2 M / 1 M 1 M / 1 M	tun1	18	568,9	97,8
	eth0	44	232,8	
	eth1-3	88	116,4	
Case 6. 20 MB 2 M / 1 M 1 M / 1 M	tun1	36	568,9	98,1
	eth0	88	232,8	
	eth1-3	177	115,7	
Case 7. 10 MB 2 M / 2 M 1 M / 1 M	tun1	15	682,7	97,8
	eth0-1	44	232,8	
	eth2-3	88	116,4	
Case 8. 20 MB 2 M / 2 M 1 M / 1 M	tun1	30	682,7	98,0
	eth0-1	88	232,8	
	eth2-3	177	115,7	
Case 9. 10 MB 2 M / 2 M 2 M / 1 M	tun1	13	787,7	96,7
	eth0-2	44	232,8	
	eth3	88	116,4	
Case 10. 20 MB 2 M / 2 M 2 M / 1 M	tun1	26	787,7	96,8
	eth0-2	88	232,8	
	eth3	177	115,7	

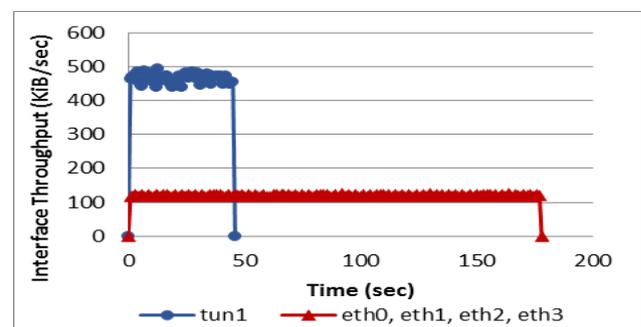


Fig. 3. IPv4 Test case 2: Data size: 20 MB, Clock rates: 1.000.000 / 1.000.000 / 1.000.000 / 1.000.000

It can be seen from the measurement results that the throughput capacity of the four paths are summed efficiently on the tunnel interface by using the MPT library. This statement holds both for the interface throughput and for the Application layer's throughput: the efficiency is better than 96% in all cases (see Table II).

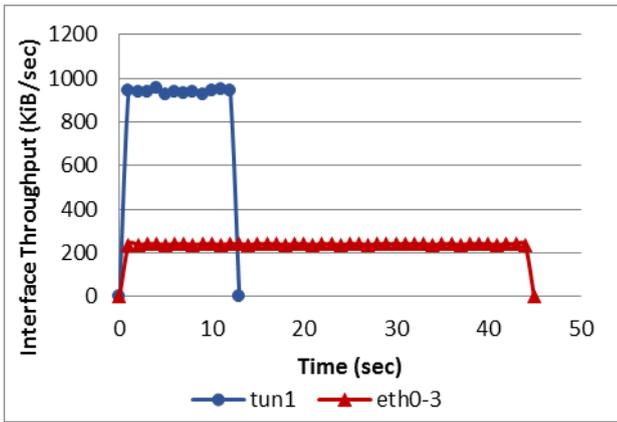


Fig. 4. IPv4 Test case 3: Data size: 10 MB, Clock rates: 2.000.000 / 2.000.000 / 2.000.000 / 2.000.000

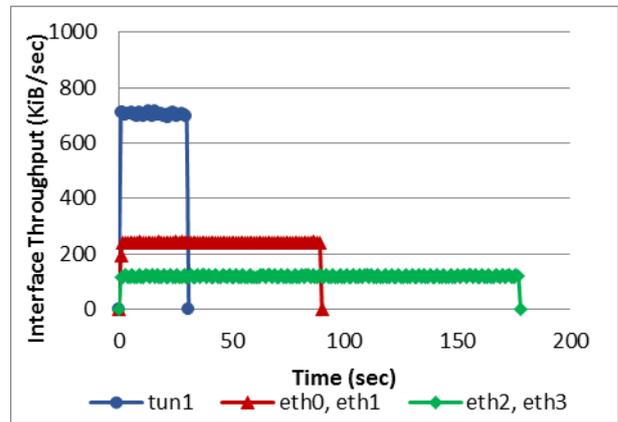


Fig. 8. IPv4 Test case 8: Data size: 20 MB, Clock rates: 2.000.000 / 2.000.000 / 1.000.000 / 1.000.000

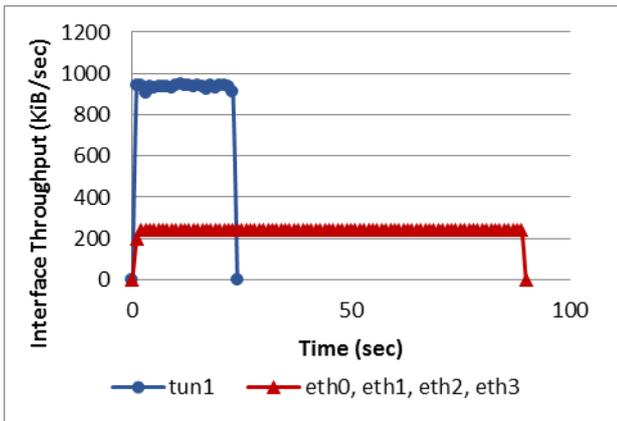


Fig. 5. IPv4 Test case 4: Data size: 20 MB, Clock rates: 2.000.000 / 2.000.000 / 2.000.000 / 2.000.000

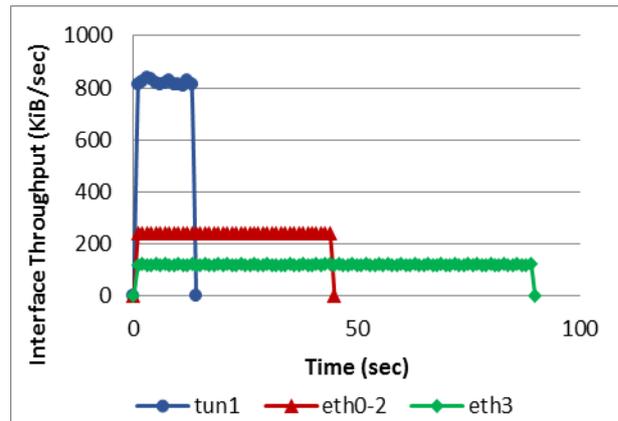


Fig. 9. IPv4 Test case 9: Data size: 10 MB, Clock rates: 2.000.000 / 2.000.000 / 2.000.000 / 1.000.000

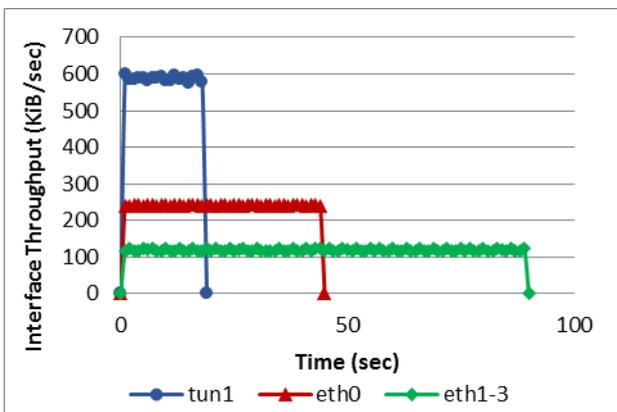


Fig. 6. IPv4 Test case 5: Data size: 10 MB, Clock rates: 2.000.000 / 1.000.000 / 1.000.000 / 1.000.000

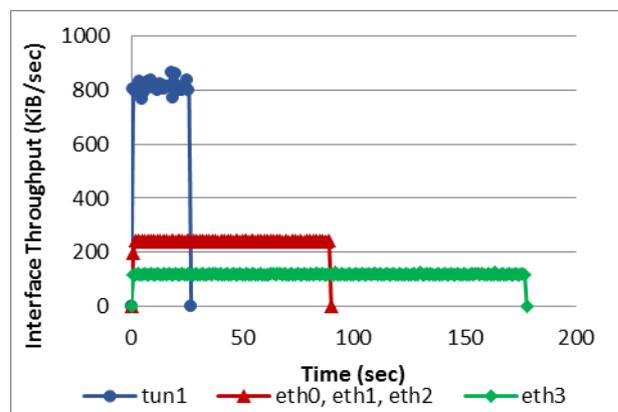


Fig. 10. IPv4 Test case 10: Data size: 20 MB, Clock rates: 2.000.000 / 2.000.000 / 2.000.000 / 1.000.000

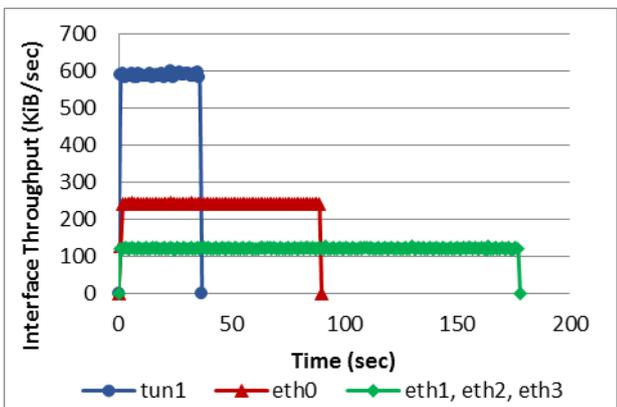


Fig. 7. IPv4 Test case 6: Data size: 20 MB, Clock rates: 2.000.000 / 1.000.000 / 1.000.000 / 1.000.000

Also, the figures show that the variance of the interface throughput is a little bit higher in the non-symmetrical cases. Further IPv4 measurement results can be found in [1].

IV. MEASUREMENT RESULTS – IPV6 ONLY NETWORK

Using IPv6 both over the tunnel and under the tunnel changes the measurement situation: the additional IP encapsulation will use a longer IPv6 header, so the efficiency decrease can be expected in this case.

The Physical and Data-link layer properties of the measurement environment remained the same as it was in the previous chapter (i.e. clock rates, file sizes). Only the Network layer protocol was changed from IPv4 to IPv6.

The measurements' results of the interfaces' throughput

can be seen in Figure 11. – 18. The numerical values of the application’s layer throughput can be seen in Table III. (i.e. the user’s point of view).

TABLE III
FTP FILE TRANSMISSION RESULTS – IPV6 ONLY NETWORK

Case	Interface	Time (sec)	Through-put (KB/s)	Efficiency (%)
Case 1. 10 MB 1M / 1M 1M / 1M	tun1	23	445,2	97,8
	eth0-3	90	113,8	
Case 2. 20 MB 1M / 1M 1M / 1M	tun1	47	435,7	95,7
	eth0-3	180	113,8	
Case 3. 10 MB 2M / 2M 2M / 2M	tun1	12	853,3	93,7
	eth0-3	45	227,6	
Case 4. 20 MB 2M / 2M 2M / 2M	tun1	23	890,4	97,8
	eth0-3	90	227,6	
Case 5. 10 MB 2M / 1M 1M / 1M	tun1	19	538,9	94,7
	eth0	45	227,6	
	eth1-3	90	113,8	
Case 6. 20 MB 2M / 1M 1M / 1M	tun1	38	538,9	94,7
	eth0	90	227,6	
	eth1-3	180	113,8	
Case 7. 10 MB 2M / 2M 1M / 1M	tun1	16	640,0	93,7
	eth0-1	45	227,6	
	eth2-3	90	113,8	
Case 8. 20 MB 2M / 2M 1M / 1M	tun1	32	640,0	93,7
	eth0-1	90	227,6	
	eth2-3	180	113,8	
Case 9. 10 MB 2M / 2M 2M / 1M	tun1	14	731,4	91,8
	eth0-2	45	227,6	
	eth3	90	113,8	
Case 10. 20 MB 2M / 2M 2M / 1M	tun1	27	758,5	95,2
	eth0-2	90	227,6	
	eth3	180	113,8	

It is easy to see that the efficiency of the IPv6 throughput aggregation is a little bit lower than it was in the case of IPv4. All the efficiency values are smaller, the difference is maximum 5 percent in each case. As it can be seen in Table III. all the efficiency measurement numbers are greater than 90 percent in the IPv6 cases, so the aggregation performance is good also in the case of IPv6 only network environment.

Similarly to the IPv4 results the interface throughput is a little bit greater than the application’s layer throughput in the case of IPv6 protocol too.

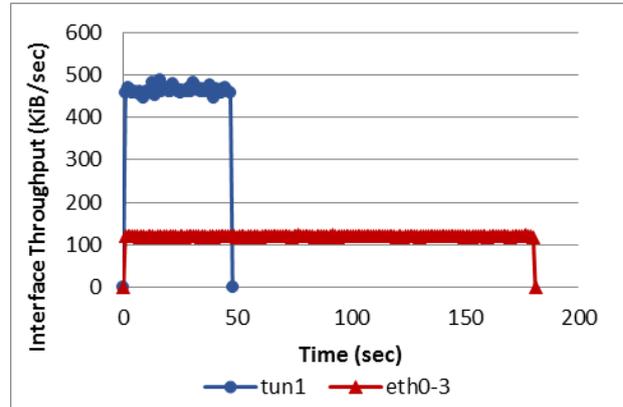


Fig. 11. IPv6 Test case 2: Data size: 20 MB, Clock rates: 1.000.000 / 1.000.000 / 1.000.000 / 1.000.000

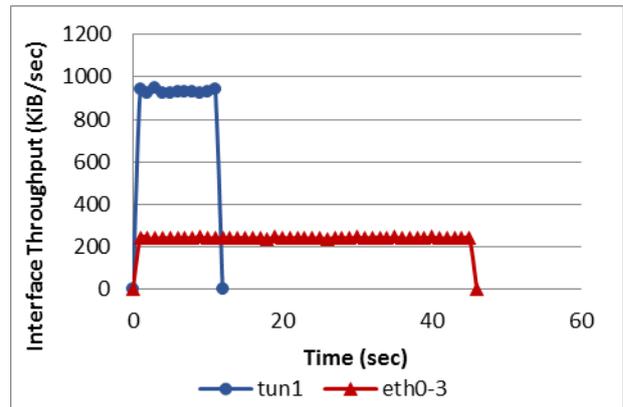


Fig. 12. IPv6 Test case 3: Data size: 10 MB, Clock rates: 2.000.000 / 2.000.000 / 2.000.000 / 2.000.000

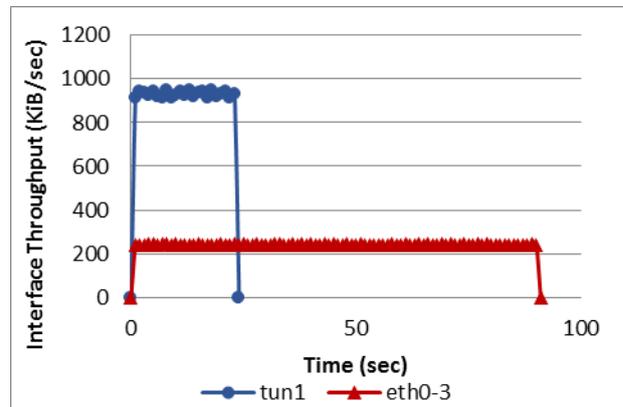


Fig. 13. IPv6 Test case 4: Data size: 20 MB, Clock rates: 2.000.000 / 2.000.000 / 2.000.000 / 2.000.000

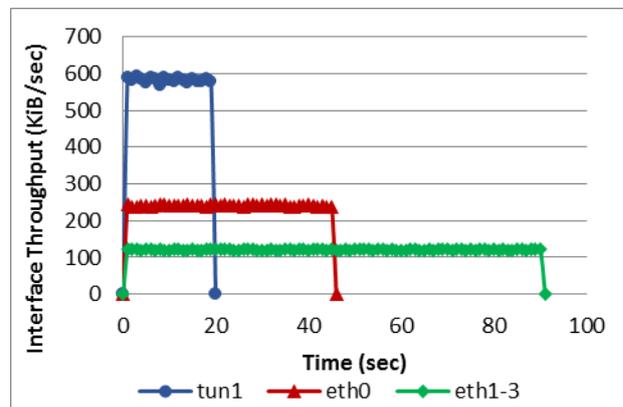


Fig. 14. IPv6 Test case 5: Data size: 10 MB, Clock rates: 2.000.000 / 1.000.000 / 1.000.000 / 1.000.000

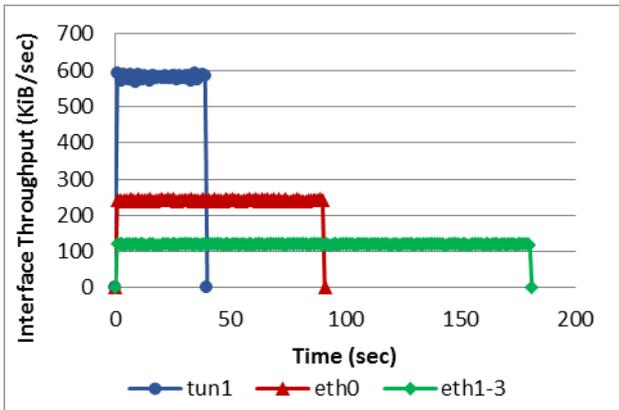


Fig. 15. IPv6 Test case 6: Data size: 20 MB, Clock rates: 2.000.000 / 1.000.000 / 1.000.000 / 1.000.000

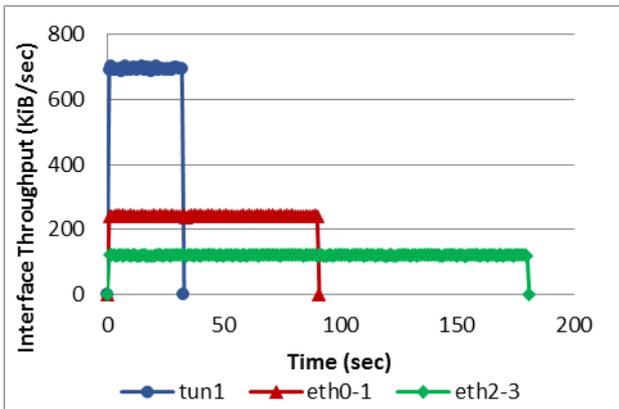


Fig. 16. IPv6 Test case 8: Data size: 20 MB, Clock rates: 2.000.000 / 2.000.000 / 1.000.000 / 1.000.000

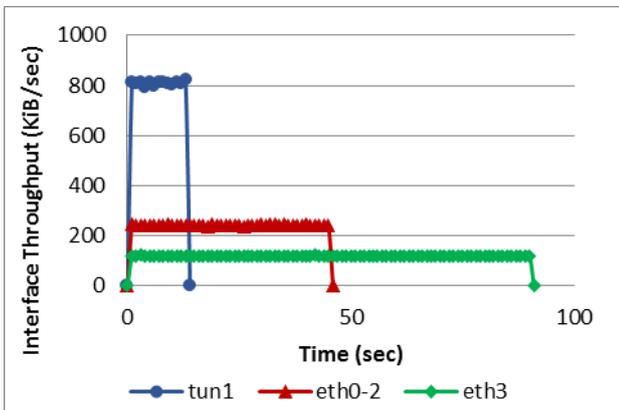


Fig. 17. IPv6 Test case 9: Data size: 10 MB, Clock rates: 2.000.000 / 2.000.000 / 2.000.000 / 1.000.000

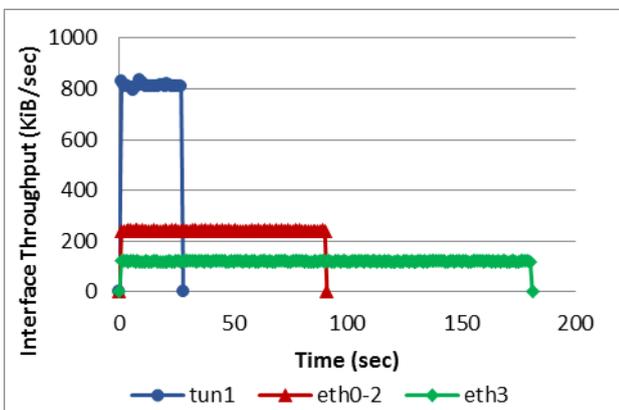


Fig. 18. IPv6 Test case 10: Data size: 20 MB, Clock rates: 2.000.000 / 2.000.000 / 2.000.000 / 1.000.000

V. MEASUREMENT RESULTS – MIXED NETWORK (IPv4 OVER IPv6)

The IPv4 address space has been exhausted in 2012 (i.e. all the IPv4 network id is assigned to ISPs, see [4],[9]). This fact may accelerate the IPv6 usage on the backbone and in the end user area too. In the future the need of special applications, which are not upgraded to the IPv6 protocol, may occur in special networking environments, where only IPv6 network is available. One solution for these special situations can be the usage of MPT: The MPT environment offers the possibility to use the IPv4 protocol on the logical tunnel interfaces (i.e. the applications will use IPv4) while the physical interfaces are connected to an IPv6 only network. This chapter evaluates the performance of the MPT library in a mixed protocol environment. The Physical and Data link layer parameters remain the same as it was in the previous chapters.

TABLE IV
MEASUREMENT RESULTS – MIXED NETWORK (IPv4 OVER IPv6)

Case	Interface	Time (sec)	Throughput (KB/s)	Efficiency (%)
Case 1: 10MB 1M / 1M 1M / 1M	tun1	23	445,2	97,8
	eth0-3	90	113,8	
Case 2: 20MB 1M / 1M 1M / 1M	tun1	46	445,2	97,8
	eth0-3	180	113,8	
Case 3: 10MB 2M / 2M 2M / 2M	tun1	12	853,3	93,7
	eth0-3	45	227,6	
Case 4: 20MB 2M / 2M 2M / 2M	tun1	23	890,4	97,8
	eth0-3	90	227,6	
Case 5: 10MB 2M / 1M 1M / 1M	tun1	19	538,9	94,7
	eth0	45	227,6	
	eth1-3	90	113,8	
Case 6: 20MB 2M / 1M 1M / 1M	tun1	38	538,9	94,7
	eth0	90	227,6	
	eth1-3	180	113,8	
Case 7: 10MB 2M / 2M 1M / 1M	tun1	16	640,0	93,7
	eth0-1	45	227,6	
	eth2-3	90	113,8	
Case 8: 20MB 2M / 2M 1M / 1M	tun1	31	660,6	96,7
	eth0-1	90	227,6	
	eth2-3	180	113,8	
Case 9: 10MB 2M / 2M 2M / 1M	tun1	13	787,7	98,8
	eth0-2	45	227,6	
	eth3	90	113,8	
Case 10: 20MB 2M / 2M 2M / 1M	tun1	27	758,5	95,2
	eth0-2	90	227,6	
	eth3	180	113,8	

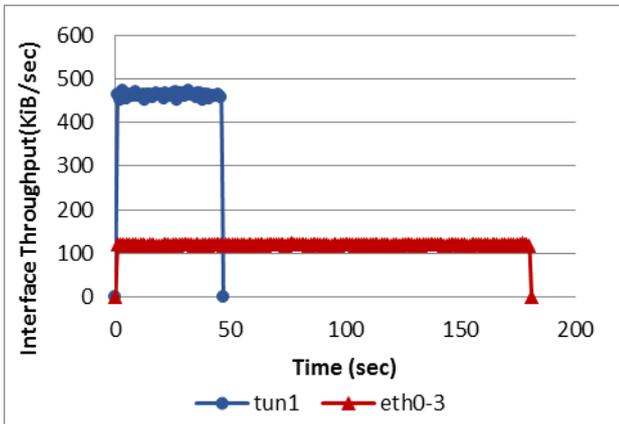


Fig. 19. Mixed Test case 2: Data size: 20 MB, Clock rates: 1.000.000 / 1.000.000 / 1.000.000 / 1.000.000

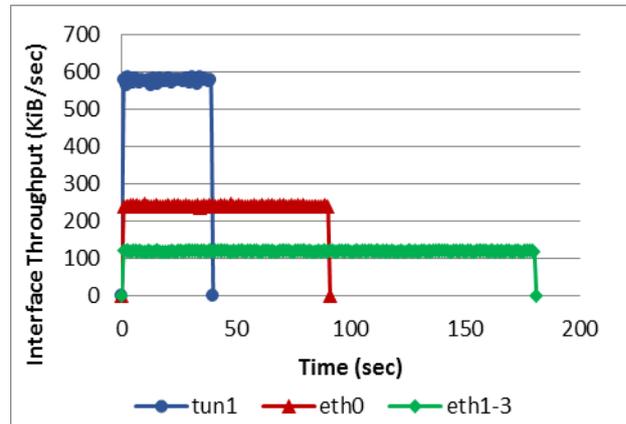


Fig. 23. Mixed Test case 6: Data size: 20 MB, Clock rates: 2.000.000 / 1.000.000 / 1.000.000 / 1.000.000

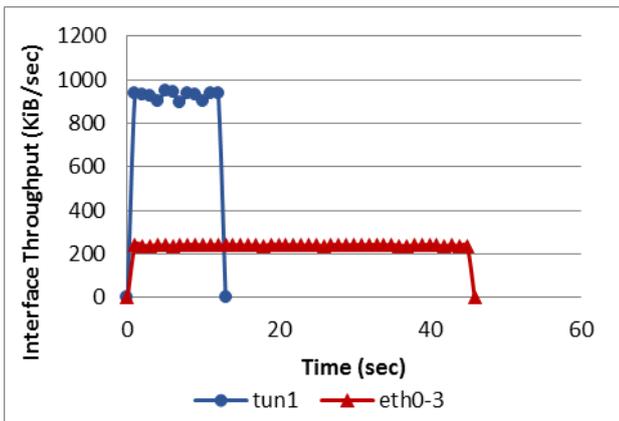


Fig. 20. Mixed Test case 3: Data size: 10 MB, Clock rates: 2.000.000 / 2.000.000 / 2.000.000 / 2.000.000

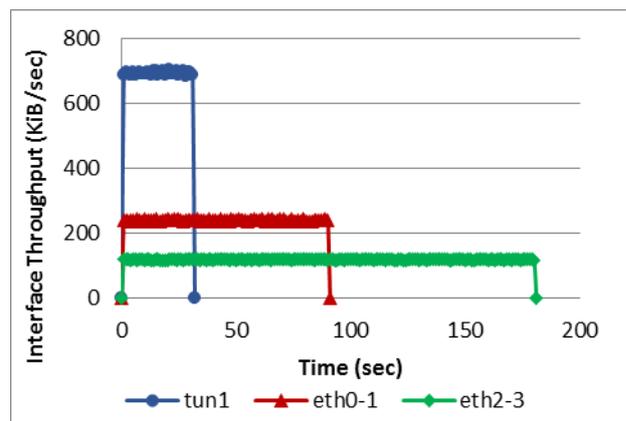


Fig. 24. Mixed Test case 8: Data size: 20 MB, Clock rates: 2.000.000 / 2.000.000 / 1.000.000 / 1.000.000

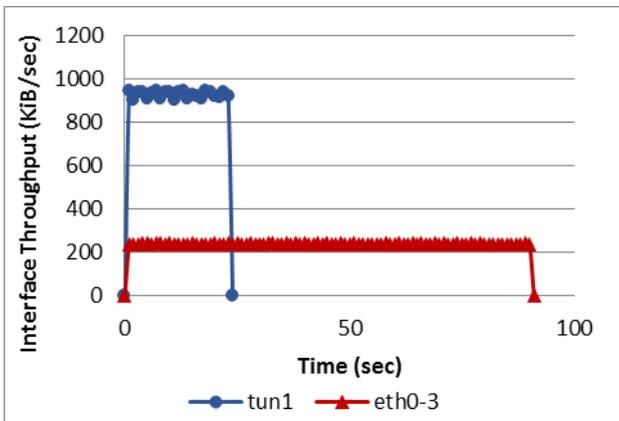


Fig. 21. Mixed Test case 4: Data size: 20 MB, Clock rates: 2.000.000 / 2.000.000 / 2.000.000 / 2.000.000

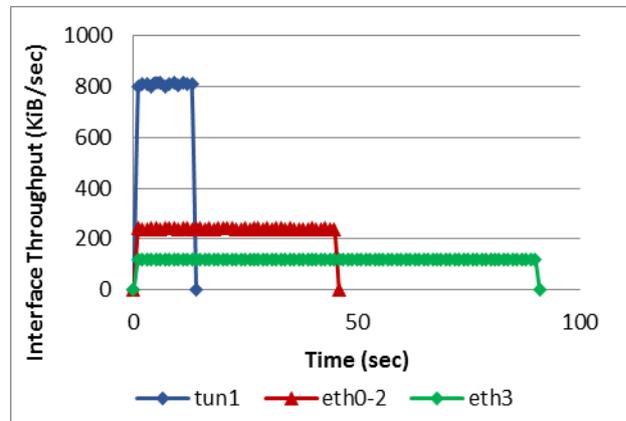


Fig. 25. Mixed Test case 9: Data size: 10 MB, Clock rates: 2.000.000 / 2.000.000 / 2.000.000 / 1.000.000

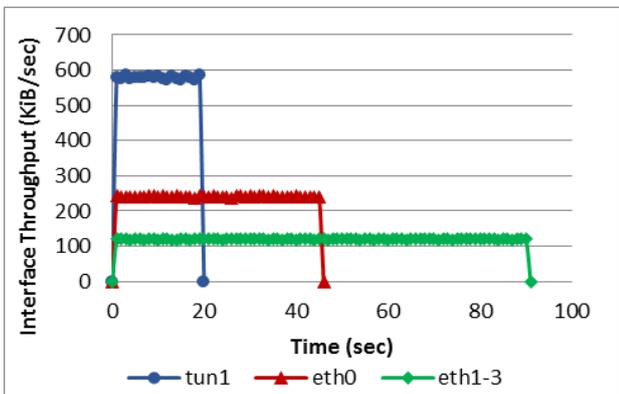


Fig. 22. Mixed Test case 5: Data size: 10 MB, Clock rates: 2.000.000 / 1.000.000 / 1.000.000 / 1.000.000

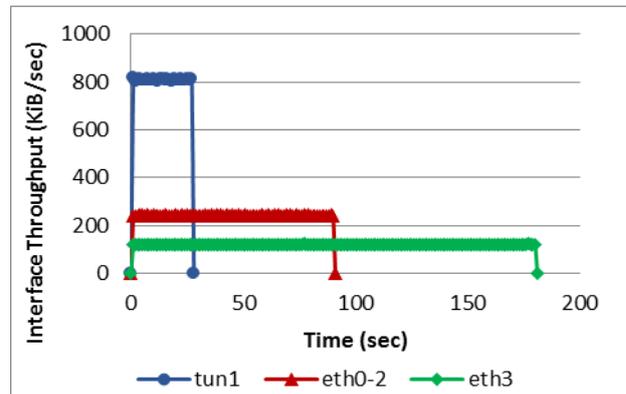


Fig. 26. Mixed Test case 10: Data size: 20 MB, Clock rates: 2.000.000 / 2.000.000 / 2.000.000 / 1.000.000

The measurements' results are shown in Figure 19. – 26. These figures show the interface throughput values for the test cases using 10 and 20 MB file sizes.

Table IV shows the Application layer throughput in the mixed protocol environment: The results are quite similar to the results of the IPv4 and IPv6 only networks measurement: in some cases the results are similar to the IPv4 environment (see cases 8, 9), other test produced numerical results like it was in the IPv6 only measurement (see cases 3 – 7). It means, that the mixed network environment produced numerical results between the IPv4 and IPv6 only measurements (as it could be expected).

VI. CONCLUSION

In this paper we investigated the throughput aggregation property of the multipath a software library MPT. The applications over the MPT tool may use any kind of transport layer protocol: the usage of both TCP and UDP is allowed. The focused purpose of the paper was to investigate the throughput performance of the MPT tool using IPv4, IPv6 and mixed network environments. We established a measurement laboratory environment which provided four independent connection paths for the communicating hosts. The throughput performance was analyzed using symmetrical and non-symmetrical bandwidth rates, and different transmitted data sizes. Although the results showed some difference in the different protocol versions, the test measurements showed that the MPT multipath environment successfully aggregates the physical paths throughput capacity.

REFERENCES

- [1] B. Almási, Sz. Szilágyi, "Multipath FTP and Stream Transmission Analysis using the MPT Software Environment", *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2. no. 11, pp. 4267-4272, Nov. 2013.
- [2] N. C. Wang, Y. K. Chiang, S. M. Wei, "RSVP Extensions for Seamless Handoff in Heterogeneous WLAN/WiMAX Networks", *Journal of Applied Research and Technology*, vol. 11, no. 4. pp. 540-548, 2013.

- [3] O. H. Sabrie, H. S. Hasan, R. Salleh, "Fast Handoff for 802.11 Wireless Network", *Communications and Network*, vol. 3, pp. 250-256, 2011.
- [4] G. Goth, "The End of IPv4 is Nearly Here", *IEEE J. Internet Computing*, vol. 16, no. 2, pp. 7-11, 2012.
- [5] B. Almási, "Multipath Communication – a new basis for the Future Internet Cognitive Infocommunication", *Proceedings of the CogInfoCom 2013 Conference, Budapest, Hungary, 2013*, pp. 201-204.
- [6] B. Almási, "A Solution for Changing the Communication Interfaces between WiFi and 3G without Packet Loss", *Proceedings of the 37th International Conference on Telecommunications and Signal Processing, Berlin, Germany, 2014*, pp. 73-77.
- [7] A. Ford, C. Raiciu, M. Handley, and O. Bonaventure. (2013). TCP Extensions for Multipath Operation with Multiple Addresses, IETF RFC-6824. Available: <http://tools.ietf.org/html/rfc6824>
- [8] M. Handley, O. Bonaventure. (2014, January). TCP Extensions for Multipath Operation with Multiple Addresses draft-ietf-mptcp-rfc6824bis-02. IETF Internet-Draft. Available: <https://datatracker.ietf.org/doc/draft-ietf-mptcp-rfc6824bis/>
- [9] Global Policy for Post Exhaustion IPv4 Allocation Mechanisms by the IANA. (Ratified 6 May 2012). Available: <https://www.icann.org/en/resources/policy/global-addressing/allocation-ipv4-post-exhaustion>



Béla Almási received MSc and PhD in mathematics and computer science from University of Debrecen, Hungary in 1989 and 1996 respectively.

He works as an associate professor at the Department of Informatics Systems and Networks, Faculty of Informatics at the University of Debrecen, Hungary. His research interests include the establishment and performance evaluation of stochastic queueing models for communication systems and investigating the multipath communication technologies. He is the head of the Multipath Communication Research Group at the Faculty of Informatics, University of Debrecen.



Szabolcs Szilágyi received his MSc in electrical engineering and computer science at the University of Oradea in 2009, and his PhD in 2015.

He has been working for the Department of Informatics Systems and Networks, Faculty of Informatics, University of Debrecen since 2013. He teaches Computer networks, and Cisco CCNA Routing and Switching. Now, he is a Senior Lecturer. The area of his research includes performance analysis of infocommunication networks.

ISSN 1805-5443



9 771805 544167