# Infocommunications Journal

A PUBLICATION OF THE SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS (HTE)

JUNE 2018 Volume X Number 2 ISSN 2061-2079

*PAPERS FROM OPEN CALL*

*PRACTICAL PAPERS OF APPLIED RESEARCH*

*CALL FOR PAPERS / PARTICIPATION*

*ADDITIONAL*

Technically Co-Sponsored by

IEEE ComSoc™
IEEE Communications Society

hte

IEEE
HUNGARY SECTION

## Indexing information

Infocommunications Journal is covered by Inspec, Compendex and Scopus.
**Infocommunications Journal is also included in the Thomson Reuters – Web of ScienceTM Core Collection, Emerging Sources Citation Index (ESCI)**

**Infocommunications Journal**

Technically co-sponsored by IEEE Communications Society and IEEE Hungary Section

**Supporters**

FERENC VÁGUJHELYI – president, National Council for Telecommunications and Information Technology (NHIT)
GÁBOR MAGYAR – president, Scientic Association for Infocommunications (HTE)

**Editorial Office** (Subscription and Advertisements)**:**
Scientic Association for Infocommunications
H-1051 Budapest, Bajcsy-Zsilinszky str. 12, Room: 502
Phone: +36 1 353 1027
E-mail: info@hte.hu • Web: www.hte.hu

**Articles can be sent also to the following address:**
Budapest University of Technology and Economics
Department of Telecommunications and Media Informatics
Tel.: +36 1 463 1102, Fax: +36 1 463 1763
E-mail: vida@tmit.bme.hu

**Subscription rates for foreign subscribers:** 4 issues 10.000 HUF + postage

Publisher: PÉTER NAGY

HU ISSN 2061-2079 • Layout: PLAZMA DS • Printed by: FOM Media

**www.infocommunications.hu**

# Wired-Wireless Converged Passive Optical Network with 4-PAM and Multi-sub-bands FBMC

Hum Nath Parajuli and Eszter Udvary, *Member, IEEE*

***Abstract*— Future 5G based passive optical networks (PON) are expected as capable of the simultaneous provision of wired and wireless services for multi-users. In this paper, for the first time, we propose and demonstrate the simultaneous delivery of wired 4-pulse amplitude modulation (4-PAM) and wireless multi-sub-bands filter bank multicarrier (FBMC) signals in one wavelength using one laser source for the future 5G PON. The 4-PAM can be used in cost-efficient intensity modulation direct detection (IM/DD) systems and it provides the double bandwidth efficiency compared to conventional on-off keying (OOK). FBMC is considered as a potential candidate for future wireless 5G due to its high suppression for out of band emissions, which allows combining multiple sub-bands with very narrow band-gaps. Using multi-sub-bands with a narrow band gap, the overall transmission capacity can be increased. In the designed system, the composite wired 4-PAM and wireless multi-sub-bands FBMC signal is generated and transmitted with intensity modulation in optical line terminal (OLT). In the optical network unit (ONU) the wired and wireless signals from the received composite signal are extracted using an electrical square band-pass filter and separately demodulated using digital signal processing techniques. The designed 4-PAM has baseband bandwidth of 4.8 GHz and multi-sub-bands FBMC consists of 4 sub-bands of 500 MHz each, having very narrow inter-sub-bands gap of 488.28 kHz and the aggregate bandwidth of 2.0015 GHz. The bit error rate (BER) has been evaluated for the performance analysis of the 4-PAM and multi-sub-bands FBMC for two cases (a) separate transmission and (b) composite transmission.**

***Index Terms*— passive optical network, filter bank multi-carrier, wired-wireless convergence, fifth generation**

## I. Introduction

The passive optical network (PON) provides the high capacity and flexibility in signal delivery through the fixed access network. PON is considered as an effective solution for 5G based wireless signals backhauling and fronthauling [1-3]. The future 5G systems should be capable of supporting multi-services/signals to keep the compatibility with the current legacy wired/wireless services. In this regard, it is important to study and analyze the convergence and delivery of potential 5G wireless signals with wired signals in the future PON systems.

Future 5G networks are expected to provide 1-10 Gbps wireless access to the end users [4-6]. The multicarrier modulation formats are potential solutions to increase the spectral efficiency in future 5G based wireless communication system. One of the widely studied modulation format in a multicarrier system is orthogonal frequency division multiplexing (OFDM) because of its advantages such as better spectral efficiency and robustness to the fiber optic impairments such as chromatic dispersion (CD) [7, 8]. However, OFDM requires a cyclic prefix (CP) in the overhead to reduce the inter symbol interference (ISI) and inter carrier interference (ICI), which reduces the spectral efficiency. Moreover, large out of band emission of the OFDM subcarriers require large guard bands in multi-sub-bands systems. These problems can be overcome through filter bank multicarrier (FBMC) system [9, 10]. The side lobe suppression of FBMC is about 40 dB in comparison with OFDM which is about 13 dB [10]. Sufficient reduction of out of band emission and the combination of the filter banks and offset-QAM (OQAM) leads to no need of the CP overhead. The feature of suppression of side lobes in large extent in FBMC enables asynchronous carrier aggregation very efficiently with a very low effect of interference in comparison with other multi-carrier systems [9-13].

4-pulse amplitude modulation (4-PAM) supports the current intensity modulation and direct detection (IM/DD) system and provides the double bandwidth efficiency compared to the on-off keying (OOK). Due to these benefits, recently huge research interests are shown on this modulation format for cost-effective optical access network design [14-16].

OFDM and FBMC based passive optical network was experimentally demonstrated in [17]. The performance comparison of OFDM and FBMC carrier aggregated signals at mm-wave frequencies was studied with the aggregated bandwidth of less than 1.5 GHz [10, 12]. These demonstrations show that the FBMC outperforms the OFDM for equivalent design parameters. Adaptively modulated FBMC was also demonstrated in the wired-wireless converged network with the aggregated bandwidth of 1.507 GHz [18]. This demonstration deals with the OFDM and FBMC both modulation formats as a wired/wireless converged system. The convergence of potential 5G modulation formats such as universal filter multi-carrier (UFDM) and generalized filter multi-carrier (GFDM) as wireless signals and 4-PAM signal as a wired signal in a PON has been demonstrated [19]. This demonstration deals with the single sub-band UFDM and GFDM modulation formats with a very low bandwidth of 1.95 MHz for each modulation format.

All of the above mentioned recent demonstrations of wired/wireless convergence in PON have not been dealt with the convergence of multi-sub-bands FBMC as a wireless and 4-PAM as a

This work has been carried out within the project FiWiN5G, supported from European Union’s Horizon 2020 research and innovation program.

Hum Nath Parajuli is a Marie Curie early stage researcher in Budapest University of Technology and Economics, Budapest, Hungary (e-mail: hum.nath.parajuli@hvt.bme.hu).

Eszter Udvary is an Associate Professor in Budapest University of Technology and Economics, Budapest, Hungary (e-mail: udvary@hvt.bme.hu).

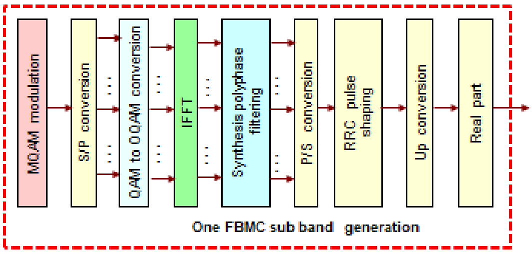
DOI: 10.36244/ICJ.2018.2.1

wired signal. In this paper, we demonstrate the convergence of 4 sub-bands FBMC as a wireless signal and 4-PAM as a wired signal in a PON. The aggregate bandwidth of the designed 4 sub-bands FBMC signal is 2.0015 GHz with inter-sub-band gap frequency of 488.28 kHz. The bandwidth of the designed 4-PAM baseband signal is 4.8 GHz. The 4-PAM and FBMC sub-bands are extracted and demodulated in the receiver by using digital signal processing (DSP) techniques. The aggregate data rate with 16QAM modulation order for 4-sub-bands FBMC is 4 Gbps and 4-PAM is 8 Gbps. We evaluate the performance of the converged signals by simulating various design parameters using bit error rate (BER) calculations.

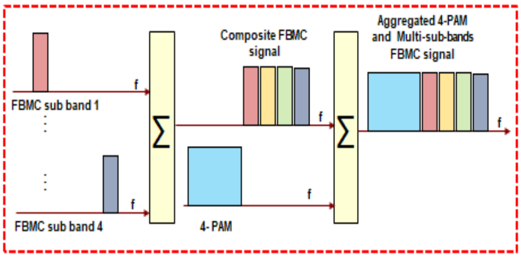
The organization of this paper is as follows. In section II, 4-PAM and FBMC multi-sub-bands signal generation method is given. In section III, the description of the implemented system model of optical transmission setup is given. Section IV presents the signal processing methods for received converged signal extraction and demodulation. Section V illustrates the simulation results and discussions. Finally, section VI concludes the paper.

## II. Converged 4-PAM and Multi-Sub-Bands FBMC Signal Generation

The MATLAB routines are developed to generate offline code for 4-PAM and multi-sub-bands FBMC signals. The baseband 4-PAM signal is generated with 4 GHz bandwidth. The sampling frequency is 32 GS/s and each 4-PAM symbol is upsampled with 4 samples for each 4-PAM symbol. After this, the root raised cosine (RRC) filter with a roll-off factor of 0.2 is used for pulse shaping.



(a)



(b)

Fig. 1. Functional block diagram of (a) FBMC signal generation for single sub-band (b) 4 sub-band FBMC signals and 4-PAM signal aggregation.

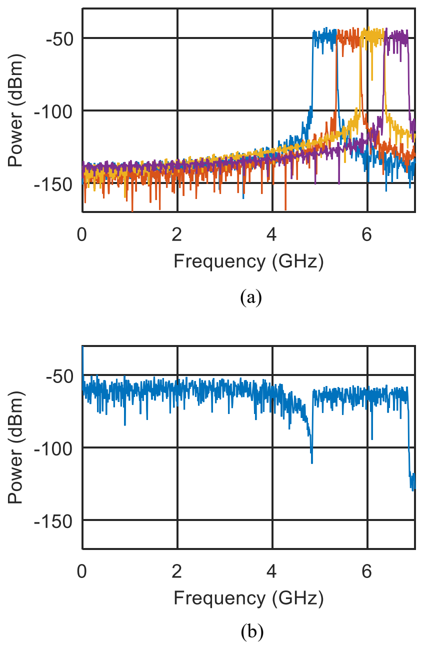
Fig.1 (a) shows the simplified DSP block diagram for generating single sub-band FBMC signal. First, the input data stream is mapped into M quadrature amplitude modulation (M-QAM) format, and then it is converted from serial to parallel (S/P) streams. Then, the QAM to offset QAM (OQAM) conversion is achieved by making the adjacent symbols with half symbol period offset to each other. After this, inverse fast Fourier transform (IFFT) is applied. Each subcarrier is filtered with well-designed prototype filter (in our case we use prototype filter proposed in [13]), this process is called synthesis polyphase filtering (SPF). After the parallel to serial (P/S) conversion process, root raised cosine (RRC) filter is applied to optimize the signal to noise ratio (SNR). Then, the baseband FBMC signal is up-converted to the desired carrier frequency. After this, the real part of the signal is taken. In this way, 4 sub-bands are generated and added up to generate 4 sub-bands’ composite FBMC signal. The 4-PAM signal is added up with composite FBMC signal to generate multiplexed 4-PAM and 4 sub-bands FBMC signal as shown in Fig. 1 (b).

**Table 1. Design parameters of 4 sub-bands FBMC and 4-PAM signals generation**

| **Parameters** | **Values** | |
|---|---|---|
| **Modulation format** | FBMC | 4-PAM |
| **No. of bits** | 32768 | 131072 |
| **Bit rate** | 4 Gbps | 8 Gbps |
| **No of sub-bands** | 4 | 1 |
| **Sub-bands spacing** | 488.28 kHz | - |
| **BW** | 2.0015 GHz | 4.8 GHz |
| **Sampling frequency** | 32 GS/s | |
| **Time window** | 8.192µs | |

The multi-sub-bands FBMC and 4-PAM signals design parameters are given in Table 1. The sampling frequency is 32 GS/s and each OQAM symbol is upsampled with 64 samples for each OQAM symbol. IFFT/FFT size of 1024 is used. 4 FBMC symbols are created which form one FBMC sub-band. Each sub-band has a bandwidth of 500 MHz. 4 sub-bands are added up to constitute the composite multi-sub-bands FBMC signal of bandwidth 2.0015 GHz with gap frequency of 488.28 kHz between each sub-band. The slight broadening of bandwidth in the composite FBMC signal is due to the pulse shaping roll-off factor of 0.2. The central frequency of first sub-band is chosen to be 5.1 GHz. With the equal gap frequency of 488.28 kHz between each sub-band, the central frequencies of the second and subsequent sub-bands are 5.6005 GHz, 6.1010 GHz, and 6.6015 GHz. Because of the multiplexing in frequency domain the time window of 4-PAM, single-sub-band FBMC and multi-sub-bands signals are identical and equal to 8.192µs.

The 4-PAM signal has been broadened up to 4.8 GHz due to the pulse shaping roll-off factor of 0.2. Also, the multi-sub-bands FBMC signal has been broadened and started from 4.8 GHz. There is no gap frequency between the 4-PAM and FBMC signal. The total bandwidth of aggregated 4-PAM and multi-sub-bands FBMC from dc is 6.9015 GHz. The total number of bits used for the case of FBMC is 32768 and for the case of 4-PAM is 131072. For 4-PAM and for each sub-bands generation in FBMC, uncorrelated bits sequences are used. Fig. 2 (a) shows the offline generated spectra of 4 sub-bands FBMC signal and (b) shows the aggregated 4-PAM and FBMC signal. As shown in Fig. 2 (a) the sidelobes suppression of FBMC sub-band is about 40 dB which allows tight packing of sub-bands without significant interference.



(a)

(b)

Fig. 2. Offline generated spectra of (a) 4 sub-bands FBMC (b) multiplexed 4-PAM and 4 sub-bands FBMC signal.

## III. Optical Transmission System

The idea of the proposed method of wired-wireless convergence in PON system is given in Fig. 3. The setup consists of optical line terminal (OLT) and optical network unit (ONU) connected through an optical fiber. In the OLT, the 4-PAM and multi-sub-bands FBMC composite signal is amplified and fed to the intensity modulator (IM) and sent through an optical fiber. In the ONU, the received composite signal is detected by the photodetector and processed offline using DSP techniques for demodulation. The typical PON system includes power splitter in ONU and fiber between OLT and ONU. The power splitter cannot separate individual signals from converged signal carried by fiber. To separate the individual signals through converged signal after photodetector one need to employ analog electrical filter with center frequency as corresponding signal's frequency. In our case, we use the digital bandpass filter to separate the signals in ONU.

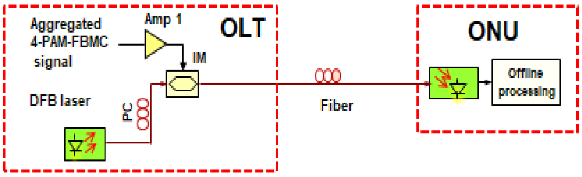
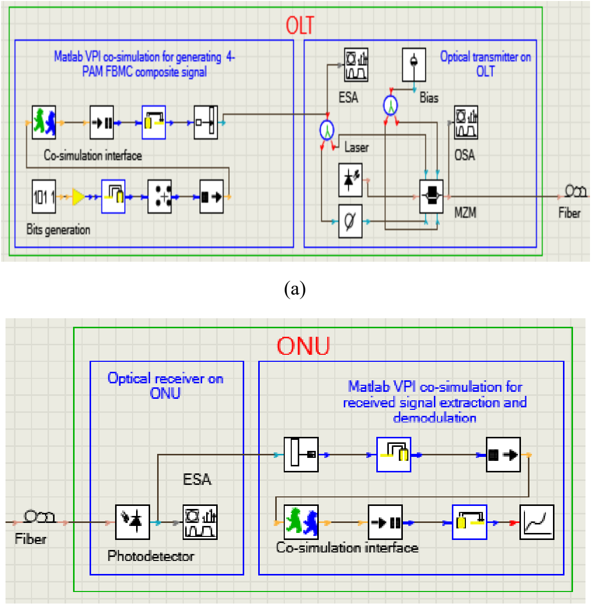


Fig. 3. Block diagram of PON setup with OLT and ONU.

VPItransmissionMaker simulator along with MATLAB co-simulation is used to implement and evaluate the performance with various design parameters. As shown in Fig. 4 (a), in the OLT setup, a continuous wave DFB laser is operated at 5 mW output power and wavelength of 1553.6 nm. The linewidth of the laser is set to 10 MHz. The Mach Zehnder modulator (MZM) is a chirp less modulator. The half wave voltage of MZM is at 8 V. The driving signal for modulator is a composite 4-PAM and multi-sub-bands FBMC signal which is generated offline developing MATLAB routines as described in section II. The MZM is biased at the quadrature point. The modulated optical signal is then transmitted through the optical fiber. The used optical fiber is a standard single mode fiber (SMF). The fiber dispersion is 18 ps/(nm km).


OLT
Matlab VPI co-simulation for generating 4-PAM FBMC composite signal
Co-simulation interface
Bits generation
ESA
Bias
Optical transmitter on OLT
Laser
OSA
MZM
Fiber
ONU
Optical receiver on ONU
Matlab VPI co-simulation for received signal extraction and demodulation
ESA
Fiber
Photodetector
Co-simulation interface

(a)

(b)

Fig. 4. Design of PON setup in VPItransmissionMaker simulator with MATLAB co-simulation. (a) OLT (b) ONU. ESA: electrical spectrum analyzer, OSA : optical spectrum analyzer, MZM: Mach Zehnder modulator

As shown in Fig. 4 (b), in the ONU, the signal is detected with positive intrinsic negative (p-i-n) photodiode with a thermal noise parameter of $10^{-12}$ pA/Hz$^{1/2}$. The signal is then processed offline using MATLAB routines. Fig. 5 shows the generated optical spectrum after MZM in OLT, which shows the aggregated baseband 4-PAM signal along with the multi-sub-bands FBMC signal in the optical double sidebands.

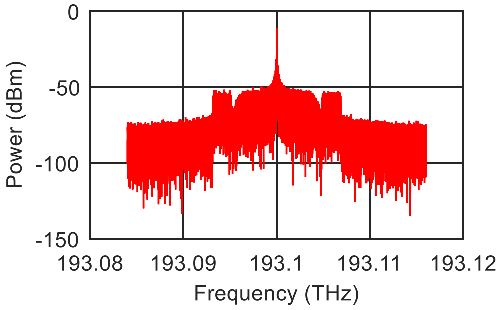


Fig. 5. Generated optical spectrum after MZM in OLT.

## IV. DSP Receiver Offline Processing

The received signal after photodetector in ONU is captured at 32 GS/s whose spectrum is shown in Fig. 6. The 4-PAM and multi-sub-bands FBMC signals are extracted and demodulated separately. For the multi-sub-bands FBMC, the signal at baseband is achieved after downconverting with the corresponding sub-bands intermediate frequency (IF) along with the RRC low pass filtering. After this, the resampling is applied to downsample the signal at 2 samples for each OQAM symbols. The FBMC decoding routines are applied as shown in Fig. 7, as explained in [10, 13]. The decoding process involves S/P conversion, analysis filter bank, FFT, OQAM-QAM conversion and P/S conversion. The training length of first 16 QAM samples from each sub-bands are used to calculate the channel response which is used to equalize the signal. Furthermore, simple 1 tap recursive least square (RLS) equalizer with forgetting factor of 0.9 is used to optimize the equalization process. After the equalization, the performance of the signal is evaluated with BER calculation.

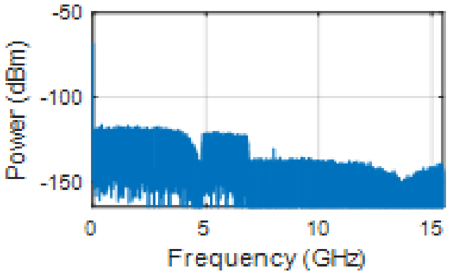


Fig. 6. Received photo-detected signal in ONU after 40 km fiber length.

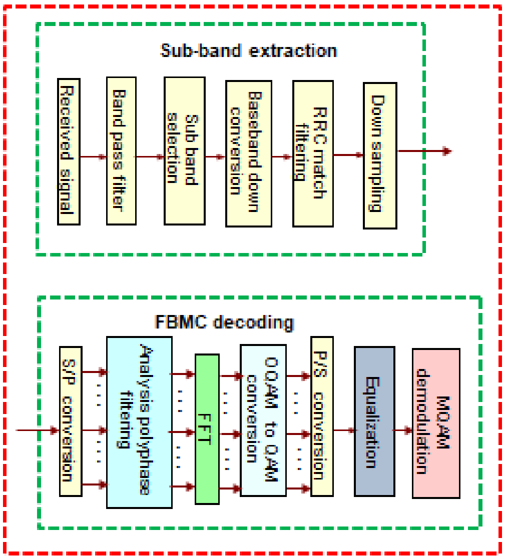


Fig. 7. FBMC sub-bands extraction and decoding.

Fig. 8 (a) describes the 4-PAM signal extraction and demodulation steps in ONU. Square bandpass filter with center frequency at 0 Hz and bandwidth of 9.6 GHz is applied to the received signal which extracts the two sidebands of the received 4-PAM signal as shown in Fig. 8 (b). Thus extracted 4-PAM signal is equalized with the 9 taps adaptive feed forward finite impulse response (FIR) equalizer (FFE) with least mean square (LMS) adaptation. The first 64 samples of the 4-PAM signal are used as a training length for the adaptation of LMS algorithm. After equalization, the performance of the 4-PAM signal is evaluated with BER calculation.

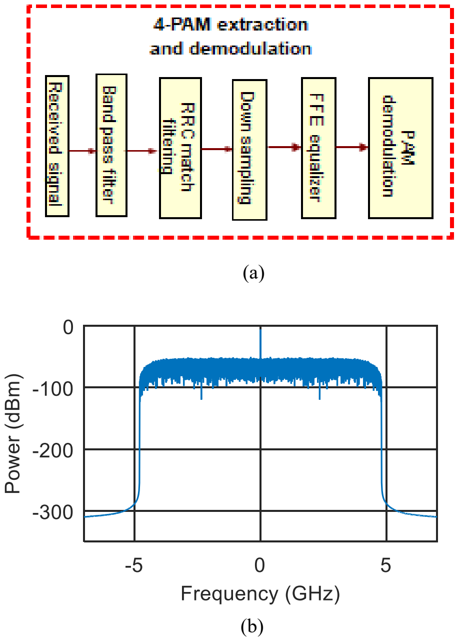


Fig. 8. (a) 4-PAM signal extraction and demodulation process. (b) Extracted 4-PAM signal.

## V. Results and Discussions

Fig. 9 shows the BER versus received optical power (ROP) performance for separate transmission of 4-PAM and 4 sub-bands FBMC at the fiber length of 40 km and 10 MHz laser linewidth.

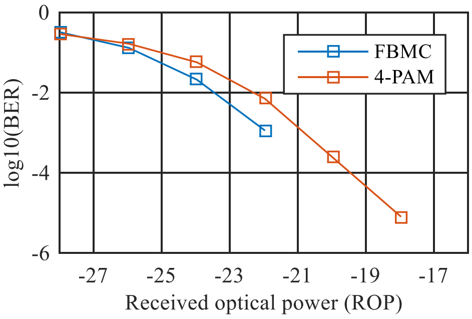


Fig. 9. BER versus ROP performance of separate 4-PAM and 4 sub-bands FBMC signal transmission.

If 4-PAM and FBMC signals are separately transmitted (without mixing), for the equivalent design parameters, FBMC shows better performance compared to the 4-PAM as shown in Fig. 9. The BER of $10^{-3}$ can be obtained at ROP of -22 dBm for the case of FBMC and -21 dBm for the case of 4-PAM. For the ROP values greater than -22 dBm, the BER of FBMC becomes 0. Similarly, for the ROP values greater than -18 dBm, the BER of 4-PAM becomes 0. From this simulation result, it can be concluded that the 4 sub-bands FBMC shows the better performance than 4-PAM for the equivalent design parameters.

The 4 sub-bands FBMC and 4-PAM signals are now multiplexed and the composite signal is transmitted. The 4-PAM and FBMC signals were extracted separately from the received composite signal using square bandpass filter. The BER with different received optical power (ROP) is evaluated as shown in Fig. 10 with 10 MHz linewidth and 40 km fiber length for the extracted 4-PAM and 4 sub-bands FBMC signals. By varying ROP, for lower values of ROP, both modulation schemes show the similar performance. For the ROP of -16 dBm, the BER of $10^{-3}$ can be obtained for both the modulation schemes. As the ROP increases the 4-PAM signal shows better performance than 4 sub-bands FBMC signal indicating the fact that FBMC is more affected by the signal mixing effect (interference) compared to 4-PAM in the composite signal case.

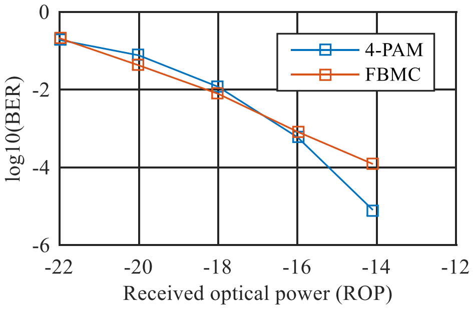


Fig. 10. BER versus ROP performances of 4-PAM and FBMC signals.

The BER versus fiber length performance is evaluated for the extracted 4-PAM and 4 sub-bands FBMC signal with the laser linewidth of 10 MHz as shown in Fig. 11. The FBMC has degraded performance compared to 4-PAM. In this simulation also, in the case of the composite signal, the FBMC signal is more affected by the interference compared to the 4-PAM signal.

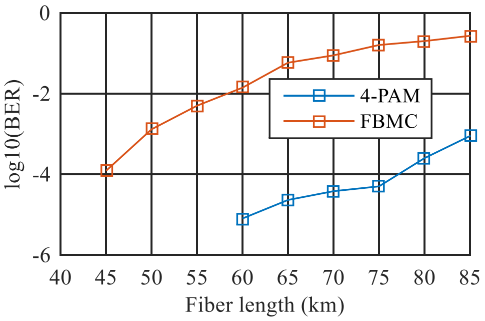


Fig. 11. BER versus fiber length performances of 4-PAM and 4 sub-bands FBMC signals.

Fig. 12 (a) and (b) show the constellation diagrams of the extracted 4 sub-bands FBMC and 4-PAM signals at 40 km and 60 km fiber lengths respectively. At 40 km fiber length, the constellations of the 4 sub-bands FBMC and 4-PAM signals are less distorted which corresponds to the BER of less than $10^{-6}$ for both the modulation schemes. As the fiber length increases the constellation of the FBMC is distorted more. For the 60 km fiber length, the 4-PAM signal BER is in the order of $10^{-5}$ as compared to $10^{-2}$ for the case of 4 sub-bands FBMC.

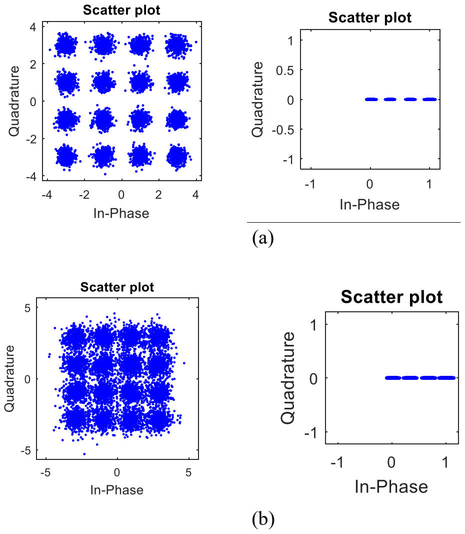


Fig. 12. Constellation diagrams of extracted 4 sub-bands FBMC and 4-PAM signals after (a) 40 km fiber length (b) 60 km fiber length.

## VI. CONCLUSION

In this paper, by using FBMC signal of 4 sub-bands of 500 MHz each with the aggregated bandwidth of 2.0015 GHz and 4-PAM of 4.8 GHz we demonstrated the performance of converged wired-wireless signal transmission in the PON. The 4 sub-bands FBMC signal has the bit rate of 4 Gbps and 4-PAM has the bit rate of 8 Gbps. The narrow-band gap of 488.28 kHz is used to separate each sub-bands in 4 sub-bands FBMC. With very low-performance degradation (BER < $10^{-6}$) the converged signal can be transmitted for a distance of up to 40 km for the received optical power (ROP) of -4.1 dBm with the laser linewidth of 10 MHz. The BER of $10^{-3}$ can be obtained at ROP of -22 dBm for the case of 4 sub-bands FBMC and -21 dBm for the case of 4-PAM at 40 km fiber length and laser linewidth of 10 MHz.

The FBMC shows better performance compared to 4-PAM for separate transmission. However, FBMC is more affected by the laser linewidth and the interference effect compared to 4-PAM in the converged signal transmission scenario. Also, due to the double bandwidth efficiency of the 4-PAM, it will be attractive candidate compared to conventional OOK in baseband signal transmission scenario. We believe that the convergence of multi-sub-bands FBMC and 4-PAM will make expected 5G high bandwidth multi-user, multi-bands wireless services feasible.

## REFERENCES

[1] J. Y. Sung, C. W. Chow, C. H. Yeh, Y. Liu and G. K. Chang, "Cost-effective mobile backhaul network using existing ODN of PONs for the 5G wireless systems," in *IEEE Photonics Journal*, vol. 7, no. 6, pp. 1-6, Dec. 2015. doi: 10.1109/JPHOT.2015.2497222.

[2] B. Skubic, M. Fiorani, S. Tombaz, A. Furuskär, J. Mårtensson and P. Monti, "Optical transport solutions for 5G fixed wireless access [Invited]," in *IEEE/OSA Journal of Optical Communications and Networking*, vol. 9, no. 9, pp. D10-D18, Sept.2017.doi:10.1364/JOCN.9.000D10

[3] X. Liu and F. Effenberger, "Emerging optical access network technologies for 5G wireless [invited]," in *IEEE/OSA Journal of Optical Communications and Networking*, vol. 8, no. 12, pp. B70-B79,2016. doi:10.1364/JOCN.8.000B70.

[4] T. S. Rappaport *et al.*, "Millimeter wave mobile communications for 5G cellular: It will work!," in *IEEE Access*, vol.1, pp.335-349, 2013. doi: 10.1109/ACCESS.2013.2260813

[5] A. Tzanakaki *et al.*, "Wireless-optical network convergence: enabling the 5G architecture to support operational and end-user services," in *IEEE Communications Magazine*, vol. 55, no. 10, pp. 184-192, OCTOBER 2017. doi: 10.1109/MCOM.2017.1600643.

[6] B. Skubic, M. Fiorani, S. Tombaz, A. Furuskär, J. Mårtensson and P. Monti, "Optical transport solutions for 5G fixed wireless access [Invited]," in *IEEE/OSA Journal of Optical Communications and Networking*, vol. 9, no. 9, pp. D10-D18, Sept. 2017. doi: 10.1364/JOCN.9.000D10.

[7] E. P. Martin *et al.*, "25-Gb/s OFDM 60-GHz radio over fiber system based on a gain switched laser," in *Journal of Lightwave Technology*, vol. 33, no. 8, pp. 1635-1643, April15, , 2015. doi: 10.1109/JLT.2015.2391994.

[8] H. Shams and J. Zhao, "First investigation of fast OFDM radio over fibre system at 60 GHz using direct laser modulation," *2013 Conference on Lasers & Electro-Optics Europe & International Quantum Electronics Conference CLEO EUROPE/IQEC*, Munich, 2013, pp. 1-1.

[9] P. Banelli, S. Buzzi, G. Colavolpe, A. Modenini, F. Rusek and A. Ugolini, "Modulation formats and waveforms for 5G networks: who will be the heir of OFDM?: An overview of alternative modulation schemes for improved spectral efficiency," in *IEEE Signal Processing Magazine*, vol. 31, no. 6, pp. 80-93, Nov. 2014. doi: 10.1109/MSP.2014.2337391.

[10] J. Zhang *et al.*, "Full-duplex quasi-gapless carrier aggregation using FBMC in centralized radio-over-fiber heterogeneous networks," in *Journal of Lightwave Technology*, vol. 35, no. 4, pp. 989-996, Feb.15, 15 2017. doi: 10.1109/JLT.2016.2608138.

[11] T. T. Nguyen, S. T. Le, Q. He, L. V. Compernolle, M. Wuilpart and P. Mégret, "Multicarrier approaches for high-baudrate optical-fiber transmission systems with a single coherent receiver," in *IEEE Photonics Journal*, vol. 9, no. 2, pp. 1-10, 2017. doi: 10.1109/JPHOT.2017.2672041.

[12] M. Xu *et al.*, "FBMC in next-generation mobile fronthaul networks with centralized pre-equalization," in *IEEE Photonics Technology Letters*, vol. 28, no. 18, pp. 1912-1915, Sept.15, 15 2016. doi: 10.1109/LPT.2016.2575060.

[13] M. Bellanger, D. Le Ruyet, et al.,"FBMC physical layer: a primer," *PHYDYAS, Project Document*, Jan. (2010). [Online available: http://www.ict-phydyas.org/]

[14] I. Lazarou, S. Dris, P. Bakopoulos, B. Schrenk and H. Avramopoulos, "Full-duplex 4-PAM transmission for capacity upgrade in loop-back PONs," in *IEEE Photonics Technology Letters*, vol. 25, no. 12, pp. 1125-1128, June 15, 2013. doi: 10.1109/LPT.2013.2260533.

[15] H. K. Shim, H. Kim and Y. C. Chung, "20-Gb/s polar RZ 4-PAM transmission over 20-km SSMF using RSOA and direct detection," in *IEEE Photonics Technology Letters*, vol. 27, no. 10, pp. 1116-1119, May 15, 2015. doi: 10.1109/LPT.2015.2408376.

[16] C. Stamatiadis, R. Matsumoto, Y. Yoshida, A. Agata, A. Maruta and K. I. Kitayama, "Full-duplex RSOA-based PONs using 4-PAM with pre-equalization," in *IEEE Photonics Technology Letters*, vol. 27, no. 1, pp. 73-76, Jan.1,2015. doi: 10.1109/LPT.2014.2361922.

[17] A. Saljoghei, F. A. Gutiérrez, P. Perry, D. Venkitesh, R. D. Koipillai and L. P. Barry, "Experimental comparison of FBMC and OFDM for multiple access uplink PON," in *Journal of Lightwave Technology*, vol.

**Hum Nath Parajuli** is a Marie Curie early stage researcher in Budapest University of Technology and Economics, Budapest, Hungary. He received his B.Eng. degree from Pokhara University, Nepal in 2008 and joint M.Sc. degree from Osaka University, Japan and Scula Superiore Sant' Anna, Italy in 2012. His current research interests include design of high capacity optical wireless links, millimeter wave communication, digital signal processing for optical communication and design of optoelectronic systems.

**Eszter Udvary** received Ph.D. degree in electrical engineering from Budapest University of Technology and Economics (BME), Budapest, Hungary, in 2009. She is currently an Associate Professor at BME, Department of Broadband Info-communications and Electromagnetic Theory, where she leads the Optical and Microwave Telecommunication Lab. Dr. Udvary's research interests are in the broad areas of optical communications, include optical and microwave communication systems, Radio over fibre systems, optical and microwave interactions and applications of special electro-optical devices.

# Advanced Approximation of Channel Quality in a VLC CDM System

Gabor Szabo and Eszter Udvary

***Abstract*—Expanding the functionality of LED indoor lighting with visible light communication (VLC) allows an additional communication channel beside wireless radio in buildings. This service may be based on various channel access methods and modulation types. Code division multiplexing (CDM) is a suitable method to such an application, but it is complicated to measure the signal quality which is essential to compare different codes and settings, and necessary for some applications like position-dependent information services. Computing crest factor is a suitable method to estimate quality, but it may be inaccurate in some cases. This paper presents novel methods to approximate the quality of received CDM signals along with the crest factor, aiding the more accurate investigation of the VLC CDM technique.**

***Index Terms*—visible light communication, code division multiplexing, signal quality, characterization, OOC, Gold codes**

## I. INTRODUCTION

Visible light communication (VLC) refers to free space optical transmission with light emitting diodes (LEDs), adding an alternative functionality to lighting or visible light indicator devices [1], [2], [3]. So these light sources, beside their main purposes, can invisibly embed data in their light output, which is immune to radio interferences, does not have environmental and human health risks, and is able to provide a high data rate connection. Due to its benefits this technology has recently attracted significant attention as a promising complementary technology for short range radio frequency communications [2], [4], [5], [6].

Using the indoor lighting system to positioning purposes via VLC may be a convenient and cost-efficient way to determine the location of portable devices, because the internal areas of a building are usually fully covered with light sources. A mobile node can be located with VLC on several different ways. With the angle of arrival (AoA) method [8] very good accuracy may be achieved. Its main disadvantage is that it requires an image sensor array, which is far more expensive and has a lower bandwidth than a single photodiode [7]. The signal traveling time measurement techniques, such as time of arrival (ToA) and time difference of arrival (TDoA), require not only ultra high speed circuits on the receiver side, but also synchronization between at least the transmitters, increasing the installation and circuit costs [7]. A less accurate but cost-efficient localization method is based on the received signal strength (RSS), which eliminates the need of any synchronization and complex optical devices, [9], [10], [11].

As LEDs used in indoor lighting can be modulated efficiently only up to tens of MHz [12], inter-symbol interference (ISI) caused by multi-path propagation does not affect the operation. Moreover, one of the main drawbacks of the VLC – its relatively short range – can be converted into advantage in some location-dependent applications, as the distant illumination devices interfere less with the relevant signals.

In most of the applications the signals of different transmitters (lamps) have to be separated on the receiver side, so some kind of multiplexing methods should be used. With phosphor-converted white LEDs of illumination devices wavelength-division multiplexing (WDM) is not feasible without interfering with the lighting function. Using simple intensity modulation with direct detection (IM/DD) in an undivided space three fundamental multiplexing methods are possible. Time-division multiplexing (TDM) means that the participants do not communicate in the same time, but alternately, so the other communication parameters (e.g. frequency domain) may be the same for all transmitters. In the case of frequency-division multiplexing (FDM), different nodes transmit on different frequency bands even simultaneously, but this also makes the continuous reception of several signals more difficult. As for code-division multiplexing (CDM), the communication can be in the same time and on same frequency band, because the transmitters use different codes to identify their signals. This method enables the possibility of continuous communication with minimal bandwidth, which is suitable for also an indoor positioning system along with other broadband VLC services.

This paper presents the CDM technique in aspects of the usage in VLC systems, including the introduction of the main code types like optical orthogonal codes (OOCs) and pseudo-noise codes. In the followings the problems of CDM channel quality approximation are negotiated, introducing two new quality indication methods. Finally, for an example, a novel quality indicator measure is used to compare noise sensitivity of different code sets with CDM.

## II. CODE DIVISION MULTIPLEXING

Code division multiplexing is a digital multiplexing method based on binary code sets having special

G. Szabo and E. Udvary are with the Department of Broadband Infocommunication and Electromagnetic Theory, Budapest University of Technology and Economics, Egry József utca 18, Budapest 1111, Hungary. (e-mail: gabor.szabo@hvt.bme.hu, udvary@hvt.bme.hu ¤ URL: http://hvt.bme.hu )

DOI: 10.36244/ICJ.2018.2.2

autocorrelation and cross-correlation properties. If the length of codes is *n*, every bit of data is converted on the transmitter side to *n* chips. In a possible realization, the transmitter puts out its own code or its bitwise negative on every bit, according to the actual data bit value. The detector receives all signals at the same time (superposition), and correlates this compound signal with each code. The polarity of correlation peak values indicates the bits sent.

In synchronous CDM systems, where the transmitter nodes are synchronized, it is possible to use orthogonal code sets, e.g. orthogonal variable spreading factor (OVSF) codes. In this case of perfect orthogonality the crosstalk between CDM channels is zero, but the synchronization requirements make this mode not suitable for a simple VLC system.

The asynchronous CDM technique does not need any synchronization between the transmitters; it is based on quasi-orthogonal codes, like the bipolar Gold codes and the unipolar OOCs. These codes are not orthogonal, but their circular cross-correlation peak is low, also having low circular auto-correlation peak. Due to the lack of orthogonality there is some crosstalk between the CDM channels, but using appropriate codes the signal-to-interference-plus-noise-ratio (SINR) can be high enough to achieve good results.

Our experiments are focused on asynchronous CDM transmission due to the suitability for VLC systems.

## III. Optical Orthogonal Codes

OOCs are unipolar quasi-orthogonal binary codes which can be represented with four parameters, usually written in the following format: (n, w, $\lambda_a$, $\lambda_c$), where *n* is the code length, *w* is the code weight (number of ones), $\lambda_a$ is the upper bound of the circular autocorrelation function, $\lambda_c$ is the upper bound of the circular cross-correlation function between the elements of the code set [13].

$$C_{xx}(\tau)=\sum_{i=0}^{n-1} x_i x_{i\oplus\tau} =\begin{cases} w, & \tau=0 \\ \leq \lambda_a, & 1\leq\tau\leq n-1 \end{cases} \quad (1)$$

$$C_{xy}(\tau)=\sum_{i=0}^{n-1} x_i y_{i\oplus\tau} \quad \leq \lambda_c \quad 0\leq\tau\leq n-1 \quad (2)$$

Unipolarity means that the codes comprise zeros (‘0’) and ones (‘1’), in contrast with bipolar codes, which consist of ‘–1’ and ‘+1’ elements. Due to this fact the minimum value of OOC correlation parameters is 1, slightly limiting the maximal SINR compared to bipolar code sets. Nevertheless, the algorithmic efficiency of an OOC correlator can be very good especially for low weight OOCs, because a point of the correlation function is virtually just a sum of *w* values (multiplication with ones and zeros). This is an advantage when using a low performance portable device for VLC CDM indoor localization.

It is important to mention that the inverse of an OOC (ones and zeros swapped) is not guaranteed to have as good correlation properties as the original. This is particularly right correlation properties as the original. This is particularly right for low weight OOCs: inverting a sequence of few ones and lots of zeros would obviously lead to a $\lambda_a$ which is almost *n*. So the data transmission method using a code and its inverse as two different symbols is not feasible with OOCs.

## IV. Bipolar Pseudo Noise Codes

A bipolar binary code differs from a unipolar one in its elements: it is a sequence of ‘–1’ and ‘+1’ chips. A pseudo noise (PN) code of this type has a spectrum similar to a random binary sequence, but it is deterministically generated. Of course, when using in a CDM system, we must introduce similar restrictions in the correlation properties of a code set as in OOCs.

A general format for PN codes is (n, $\lambda_a$, $\lambda_c$), where *n* is the code length, $\lambda_a$ is the upper bound of the circular autocorrelation function, $\lambda_c$ is the upper bound of the circular cross-correlation function between the elements of the code set. The code weight is not a relevant parameter for PN codes, because the number of –1s and +1s are nearly equal due to pseudo-random distribution.

The equations for correlation limits are similar to (1) and (2), with the exception of the maximum value of the autocorrelation function.

$$C_{xx}(\tau)=\sum_{i=0}^{n-1} x_i x_{i\oplus\tau} =\begin{cases} n, & \tau=0 \\ \leq \lambda_a, & 1\leq\tau\leq n-1 \end{cases} \quad (3)$$

$$C_{xy}(\tau)=\sum_{i=0}^{n-1} x_i y_{i\oplus\tau} \quad \leq \lambda_c \quad 0\leq\tau\leq n-1 \quad (4)$$

Why cannot we use low weight bipolar codes as in case of unipolar OOCs? It is not an arbitrary decision that we use PN codes when bipolar codes are needed. In a good bipolar code set bipolarity reduces the side lobes of the circular correlation functions, because positive and negative values cancel each other on summation. A low weight bipolar code faces with the same problems as an inverted low weight OOC. When almost the whole code consists of one symbol the positive-negative cancellation effect cannot work, so $\lambda_a$ will be very close to *n*.

There are many different types of PN code sets. Maximum length sequences (sometimes also called m-sequences) can be generated with linear feedback shift registers, but additional selection of codes is required to form appropriate code sets. Other famous types such as Gold [14] and Kasami codes also based on m-sequences, but they define exact methods to generate the elements of a set from the starting codes.

It may be a question how to use bipolar codes for VLC, as the communication medium – the light intensity – can not have negative values, destructive interference can not occur between signals. This problem can be easily eliminated by DC-biasing the light source, e.g. driving the transmitter LED with a class-A amplifier. Suppose two light signals, $l_1$ and $l_2$:

$$l_1(t)=a_1+c\cdot x_1(t) \quad (5)$$

$$l_2(t)=a_2+c\cdot x_2(t) \quad (6)$$

where $a$ is the DC component, $c$ is the device-dependent linear conversion factor between the electrical signal amplitude and light intensity, $x$ is the electrical signal. Suppose that the DC bias is large enough in both signals:

$$a \geq \left| c \cdot x(t) \right| \tag{7}$$

The superposition of the light signals ($l_1 + l_2$) will be:

$$l_s(t) = a_1 + a_2 + c \cdot \left( x_1(t) + x_2(t) \right) \tag{8}$$

So this way either constructive or destructive interferences may occur while the light intensity is always non-negative.

## V. Quality of an Asynchronous CDM Signal

Channel quality is such an important thing characterizing CDM signals as received signal strength (RSS) of TDM or FDM signals. This parameter is not only useful when comparing experimental settings and different codes, but inevitable when using a VLC CDM system also to simple indoor localization purposes.

Using either TDM or FDM if it is supposed that the noise and interference levels are steady, the RSS indicates also the quality of the signal. Being acquainted with the noise level, interference level and the RSS, signal-to-interference-plus-noise-ratio (SINR) can be computed.

The situation is more complicated in case of CDM, where multiple communication channels share the same frequency band at the same time. The existence of some signal just means that at least one CDM channel is received, and the RSS value is the total (sum) strength of all received signals. Information about a specified channel may be acquired only from the corresponding pre-decoded data stream. This term is introduced (and used also in the followings) for the output data of the moving window correlation between the input compound CDM signal and a channel code:

$$PDDS_i = \sum_{j=1}^{clen} CCSS_{i+j-1} \times CODE_j \tag{9}$$

where $PDDS$ is the pre-decoded data stream of the channel, $CCSS$ is the compound CDM signal stream, $CODE$ is the channel code and $clen$ is the channel code length.

There is an example for a pre-decoded data stream of an asynchronous CDM communication on Fig. 1. Due to the lack of synchronization the starting position (“$s$”) of the right correlation peaks (“$r$”) is random, and 4x oversampling is used to reduce the chip sampling uncertainty. So with the code length of 511 one bit consists of $511 \times 4 = 2044$ samples (“$a$”). The presence of positive and negative right correlation peaks indicates bipolar encoding mode, this allows supposing that bipolar codes are used.

The noise (“$n$”) around zero is originated from the interference caused by the other channels on decoding (quasi-orthogonal codes). False correlation peaks (“$f$”) may grow out of the noise, and they can mislead the bit restoring algorithm if they are comparable to the right peaks. So the larger the right correlation peaks compared to noise and false peaks, the better the quality of a CDM channel is.

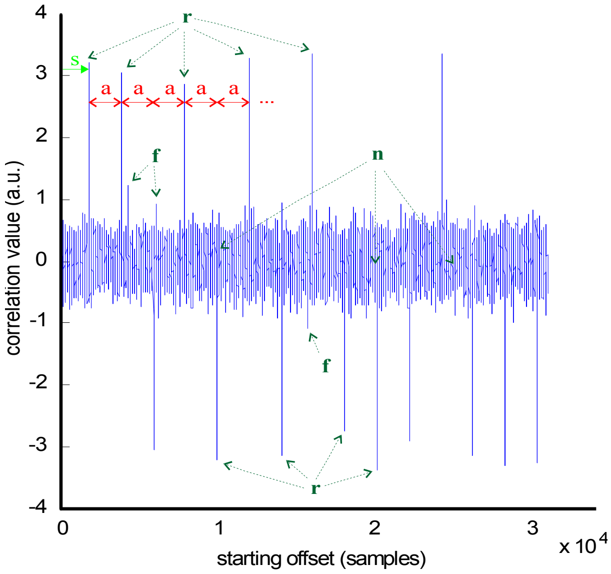


**Fig. 1.** Pre-decoded data stream example (bipolar PN code, length: 511, oversampling: 4x)

The next sub-sections show different methods to evaluate the quality of an asynchronous CDM signal from the pre-decoded data stream. It should be mentioned that any d. c. offset of the pre-decoded data should be eliminated regardless of the chosen method, because it contains no information, but it may also corrupt the calculation. This is considered done in the followings.

### A. Crest Factor

Computing the crest factor of the pre-decoded data stream is a simple method to estimate the signal quality of a CDM channel. The formula for a finite-sized block of the data stream is

$$C = \frac{|x|_{peak}}{\sqrt{\frac{1}{n}\sum_{i=1}^{n} x_i^2}} \tag{10}$$

where $|x|_{\text{peak}}$ is the absolute maximum value in the block, $x_i$ is the $i$-th element of the block and $n$ is the block size (element count).

This measure often gives a good estimation for the signal quality, but it has a problem in some special circumstances. It may also indicate good signal quality when the stream is full of false peaks what jeopardizes the success of decoding the bits. However, computing the crest factor does not require preliminary knowledge about the CDM signal, and the resource requirements of the calculation are fairly low.

Fig. 2 and Fig. 3 are an example for a case where the crest factor does not indicate the signal quality properly – as recently mentioned. Both pre-decoded data stream have a crest factor of ≈9.2 despite the visible difference in quality: the signal represented by Fig. 2 was significantly better.

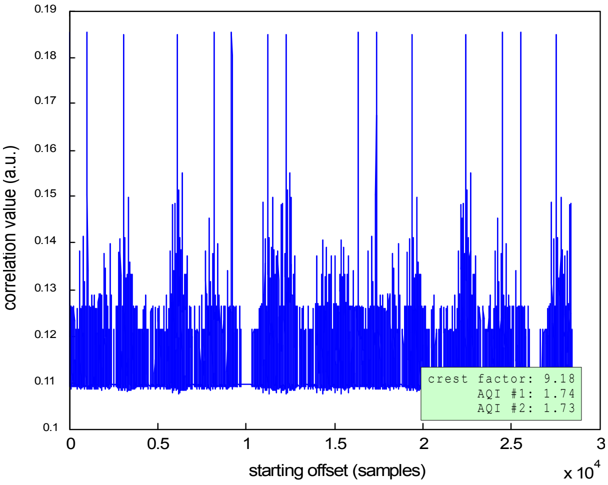


**Fig. 2.** Pre-decoded data stream example with computed quality indicator values (unipolar OOC, length: 255, oversampling: 4x)

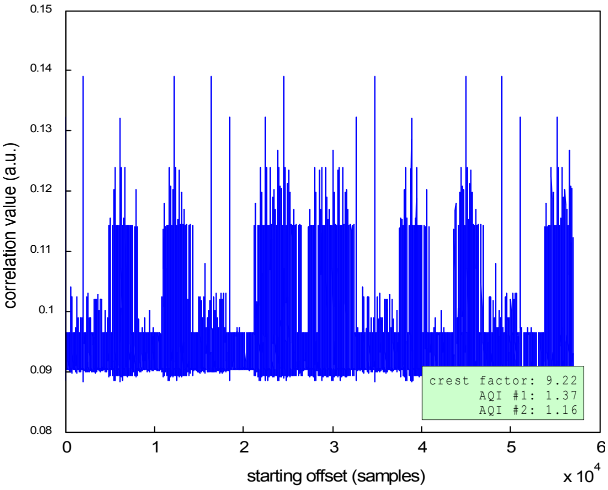


**Fig. 3.** Pre-decoded data stream example with computed quality indicator values (unipolar OOC, length: 511, oversampling: 4x)

### *B. Advanced Quality Indicator #1*

Knowing the parameters of the CDM signal allows more sophisticated computation to estimate the signal quality of a CDM channel. We developed two new measures to eliminate the false peak problem of crest factor. The less strict quantity called Advanced Quality Indicator #1 (AQI1) can be calculated with the following steps.

1. Suppose that the absolute maximum value $m$ in the pre-decoded data stream is a (right) correlation peak.
2. When the sample rate of the transmitter and the receiver are equal, the correlation peak interval is $OVSF \times n$, where $OVSF$ is the oversampling factor (samples per chip) and $n$ is the code length. All possible locations of the correlation peaks can be computed by this peak interval and the position of the highest peak.
3. Find the highest absolute value peak $f$ that is not in the epsilon neighborhood of any previously computed correlation peak locations. Consider $f$ the highest false correlation peak. (Epsilon radius allows a minor sample rate deviation between the transmitter and the receiver.)
4. AQI1 is the absolute value ratio of the highest right correlation peak value and this highest false peak value ($AQI1 = |m|/|f|$).

So AQI1 indicates how close are the false correlation peaks to be mis-identified as the highest right peak. Using the presented computation method the worst AQI1 value is 1.

In contrast to the crest factor, AQI1 is significantly different in case of the previous examples on Fig. 2 and Fig. 3. The AQI1 of the better quality CDM channel is 1.74, which is ≈27% higher than the other value.

### *C. Advanced Quality Indicator #2*

The Advanced Quality Indicator #2 (AQI2) is a variant of AQI1, which compares the highest false correlation peak to the lowest right peak that is bigger than it. So AQI2 will be large only if most right correlation peaks are much bigger than the highest false peak. Though, a good AQI2 value neither guarantees that some right peaks are lower than the highest false peak. The calculation steps of AQI2 are below.

1. Suppose that the absolute maximum value $m$ in the pre-decoded data stream is a (right) correlation peak.
2. When the sample rate of the transmitter and the receiver are equal, the correlation peak interval is $OVSF \times n$, where $OVSF$ is the oversampling factor (samples per chip) and $n$ is the code length. All possible locations of the correlation peaks can be computed by this peak interval and the position of the highest peak.
3. Find the highest absolute value peak $f$ that is not in the epsilon neighborhood of any previously computed correlation peak locations. Consider $f$ the highest false correlation peak. (Epsilon radius allows a minor sample rate deviation between the transmitter and the receiver.)
4. Find the highest absolute value peaks locally in the epsilon neighborhood of all previously computed correlation peak locations. Select the lowest absolute value $z$ that is greater than or equal to $f$.
5. AQI2 is the absolute value ratio of this right correlation peak value and the highest false peak value ($AQI2 = |z|/|f|$).

As it is in the examples on Fig. 2 and Fig. 3, AQI2 shows the difference between the two channels even better than AQI1. The AQI2 of the better quality CDM channel is 1.73, which is ≈49% higher than the other value.

## VI. Comparison of Codes with Simulation Using AQIs

A VLC CDM system can be implemented with several types of code sets as it is discussed formerly, but these code sets may not perform similarly in all circumstances. The introduced new measures allow a more reliable comparison between the performances of different codes. In case of a general comparison AQI1 is recommended. AQI2 is a stricter indicator, so it makes less difference between closely similar lower quality channels.

In this section two different code set types are compared with AQI1 in aspect of their noise immunity: low weight

OOCs and Gold codes. The results of multiple actual code sets of both types are averaged on the diagrams, which are presented in function of the code length. Although the codes were simulated at several noise levels, the representation would have too many dimensions plotting the full scale (AQI1 in function of code type, code length and noise level), so the results are presented in separate graphs of selected noise levels.

Before looking at the results, it is important to talk about CDM "unipolar mode" and "bipolar mode". In case of unipolar mode for one symbol (e.g. '1') the code will be transmitted, for the other (e.g. '0') only zeros will be output. At receiver side the signal is treated as unsigned. But in bipolar mode for one symbol the code itself, for the other the negative of the code will be transmitted. At receiver side the signal is treated as signed. Bipolar codes may give good results in both modes, but unbalanced (low weight) unipolar codes like OOCs perform well only in unipolar mode. This is the reason why bipolar codes are examined in unipolar and bipolar mode and OOCs only in unipolar mode.

To discover the typical noise immunity of code set types, a zero noise simulation should be done first. The further results then may be given in relative values to demonstrate the actual deterioration of signals caused by the noise. Examples for the interpretation of relative values (AQI1 ratios): 1.0 means that the current AQI1 value is equal to the noise-free AQI1 value, 0.6 means that the current AQI1 value is 60 percent of the noise-free AQI1 value etc. So a higher value shows better noise immunity.

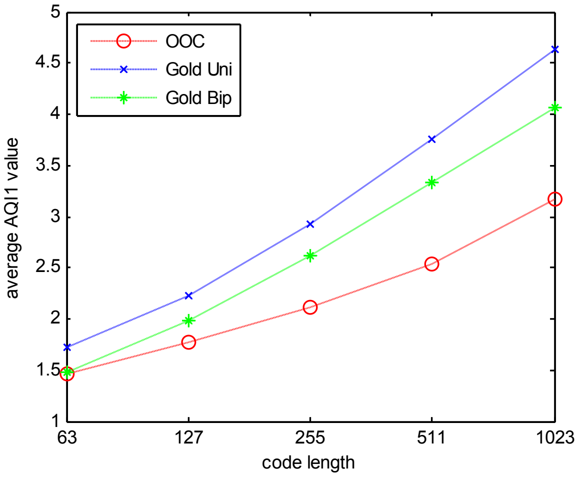


**Fig. 4.** The average AQI1 values with code sets of various lengths, noise-free simulation

Fig. 4 shows the average AQI1 values in case of zero noise. The Gold codes are proved to perform better, especially at longer code lengths. It may be a question why are Gold codes in unipolar CDM mode better than in bipolar mode, despite the fact that Gold codes are bipolar codes. It is a possible answer that CDM unipolar mode encodes one of two symbols with zeros (no actual transmission), so the other symbols represented by the code itself often have "quiet neighbors" that reduces the false peak levels on correlation. So the result will be higher channel quality.

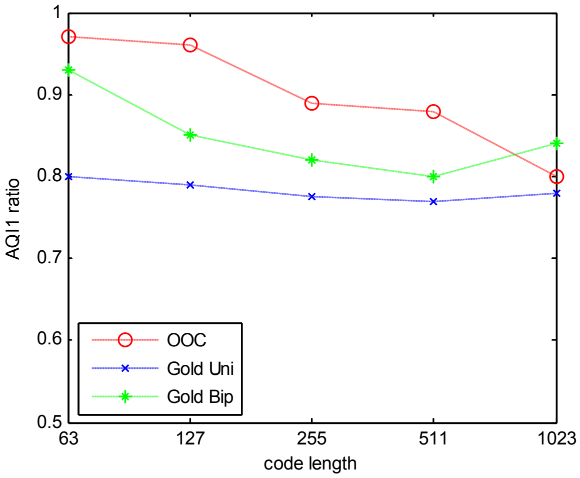


**Fig. 5.** The noisy vs. noise-free AQI1 ratio with code sets of various lengths, SNR = 6 dB simulation

However as the AQI1 ratio can be seen on Fig. 5 and Fig. 6, the ranking is quite different compared to the previous graph. Increasing the code length the achievable best correlation properties of OOCs improve at a lower rate than Gold codes (can be observed also on Fig. 4). But the deteriorative effect of the noise is also increases with the code length. In case of OOCs the negative effect may dominate, so it shows a decreasing tendency in noise immunity in function of code length despite its superiority at shorter codes, and probably underperforms the others at even longer codes (not in the graphs).

The improvement of correlation properties of Gold codes might be non-linear in function of code length, resulting in a degradation in noise immunity under 511 length, and an increment at 1023. The noise tolerance in bipolar mode proved to be better, in spite of the superiority of unipolar mode in noise-free simulation.

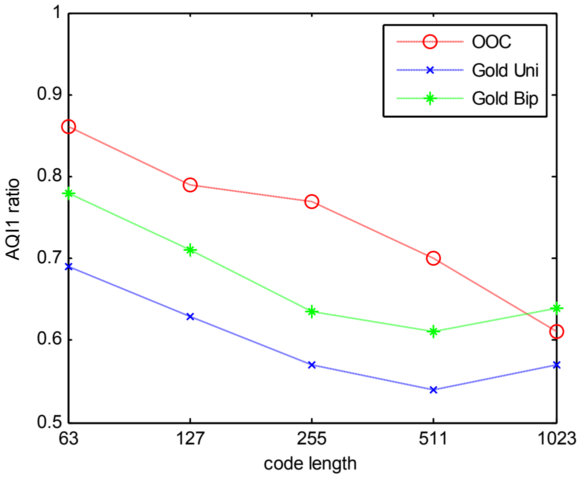


**Fig. 6.** The noisy vs. noise-free AQI1 ratio with code sets of various lengths, SNR = 0 dB simulation

So the conclusion for a real noisy environment is that the longer the codes the better the Gold code sets are, but under a certain code length the performance of Gold codes and OOCs may be similar.

## VII. Conclusion

In this paper the VLC related CDM problems are discussed, focusing on the asynchronous mode CDM which is more suitable for a simple VLC system. The description of the most common code set types, the unipolar OOCs and bipolar PN codes, showed the benefits, disadvantages and possibilities of these codes. Obtaining information about a CDM channel quality is not as easy as measuring RSS on a single RF signal. It was showed that the most common quality indicator measure, the crest factor, may be misleading in some cases. A possible solution is proposed for this problem, introducing two novel advanced quality indicator (AQI) measures. Computing these new measures along with the crest factor gives a better approximation to the CDM channel quality. With AQI1 the noise immunity of a CDM transmission using Gold codes and OOCs are compared, in function of the code length. These AQIs, for example, may improve the precision of a channel quality based VLC CDM indoor positioning system, and allows more reliable practical comparison between various code sets.

## Acknowledgment

The authors would like to thank Dr. Kari Kärkkäinen from the University of Oulu, Finland for the freely downloadable bipolar pseudo-noise code bank, which was a great help for the CDM simulations.

## References

[1] B. M. Masini, A. Bazzi and A. Zanella, "Vehicular Visible Light Networks with Full Duplex Communications," IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), pp. 98-103, 2017.

[2] S. Randel, F. Breyer, S. C. Lee, and J. W. Walewski, "Advanced Modulation Schemes for Short-Range Optical Communications", IEEE Journal of Selected Topics in Quantum Electronics, vol. 16, no. 5, pp. 1280–1289, 2010.

[3] A. Street, P. Stavrinou, D. O'brien, and D. Edwards, "Indoor optical wireless systems – a review", Optical and Quantum Electronics, vol. 29, no. 3, pp. 349–378, 1997.

[4] T. Komine and M. Nakagawa, "Integrated system of white LED visible-light communication and power-line communication", IEEE Transactions on Consumer Electronics, vol. 49, no. 1, pp. 71–79, 2003.

[5] S. Rajagopal, R. D. Roberts, and S.-K. Lim, "IEEE 802.15.7 visible light communication: modulation schemes and dimming support", IEEE Communications Magazine, vol. 50, no. 3, pp. 72–82, 2012.

[6] M. Kavehrad, "Broadband Room Service by Light", Scientific American, vol. 297, no. 1, pp. 82–87, 2007.

[7] T. Do, J. Hwang, and M. Yoo, "TDoA Based Indoor Visible Light Positioning System", Fifth International Conference on Ubiquitous and Future Networks (ICUFN), 2013.

[8] W. D. Zhong, C. Chen, H. Yang and P. Du, "Performance Analysis of Angle Diversity Multi-Element Receiver in Indoor Multi-Cell Visible Light Communication Systems", International Conference on Transparent Optical Networks (ICTON), 2017.

[9] S. Shawky, M.A. El-Shimy, Z. A. El-Sahn, M. R. M. Rizk and M. H. Aly, "Improved VLC-based Indoor Positioning System Using a Regression Approach with Conventional RSS Techniques", International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 904-909, June 2017.

[10] S. Yang, E. Jeong, D. Kim, H. Kim, Y. Son, and S. Han, "Indoor three-dimensional location estimation based on LED visible light communication", Electronics Letters, vol. 49, no. 1, pp. 54–56, January 2013.

[11] S. Jung, C. Choi, S. Heo, S. Lee, and C. Park, "Received Signal Strength Ratio Based Optical Wireless Indoor Localization Using Light Emitting Diodes for Illumination", IEEE International Conference on Consumer Electronics (ICCE), pp. 63–64, January 2013.

[12] M. Mukherjee, "Wireless Communication – Moving from RF to Optical," International Conference on Computing for Sustainable Global Development (INDIACom), pp. 788-795, 2016.

[13] S. De Lausnay, L. De Strycker, J-P. Goemaere, N. Stevens, B. Nauwelaers, "Optical CDMA Codes for an Indoor Localization System using VLC", 3rd International Workshop on Optical Wireless Communications (IWOW), pp. 50–54, September 2014.

[14] R. Gold, "Optimal Binary Sequences for Spread Spectrum Multiplexing", IEEE Transactions on Information Theory, vol. 13, no. 4, pp. 619–621, October 1967.

**Gábor Szabó** was born in Győr, Hungary, 1990. He received his M. Sc. degree from the Budapest University of Technology and Economics in 2015. His research interests include optoelectronics and visible light communication.

**Eszter Udvary** was born in Budapest, Hungary. She received her Ph. D. degree in 2009 from Budapest University of Technology and Economics. Her research interests include microwave circuits, fiber optics and optoelectronics.

# Methodology for DNS Cache Poisoning Vulnerability Analysis of DNS64 Implementations

G. Lencse, and Y. Kadobayashi, *Member, IEEE*

*Abstract*—**The trustworthy operation of the DNS service is a very important precondition for a secure Internet. As we point it out, DNS cache poisoning could be even more dangerous if it is performed against DNS64 servers. Based on RFC 5452, we give an introduction to the three main components of DNS cache poisoning vulnerability, namely Transaction ID prediction, source port number prediction, and a birthday paradox based attack, which is possible if a DNS or DNS64 server sends out multiple equivalent queries (with identical QNAME, QTYPE, and QCLASS fields) concurrently. We design and implement a methodology and a testbed, which can be used for the systematic testing of DNS or DNS64 implementations, whether they are susceptible to these three vulnerabilities. We perform the tests with the following DNS64 implementations: BIND, PowerDNS, Unbound, TOTD (two versions) and mtd64-ng. As for the testbed, we use three virtual Linux machines executed by a Windows 7 host. As for tools, we use VMware Workstation 12 Player for virtualization, Wireshark and tshark for monitoring, dns64perf for Transaction ID and source port predictability tests, and our currently developed "birthday-test" program for concurrently sent multiple equivalent queries testing. Our methodology can be used for DNS cache poisoning vulnerability analysis of further DNS or DNS64 implementations. A testbed with the same structure may be used for security vulnerability analysis of DNS or DNS64 servers and also NAT64 gateways concerning further threats.**

*Index Terms*—**DNS cache poisoning, DNS64, IPv6 transition technologies, NAT64, security, testbed, virtualization.**

## I. INTRODUCTION

SEVERAL *IPv6 transition technologies* [1] were developed to support the transition from IPv4 to IPv6, which we are currently faced with, and which is expected to last for several years or even decades. On the one hand, IPv6 transition technologies are important solutions for several different problems, which arise from the incompatibility of IPv4 and IPv6: they can enable communication in various scenarios [2]. However, on the other hand, they also involve a high number of security issues [3]. We have surveyed 26 IPv6 transition technologies, and prioritized them in order to be able to analyze the security vulnerabilities of the most important ones first [2]. DNS64 [4] and stateful NAT [5] were classified as having utmost importance, because they together provide the only solution for a communication scenario, which is very important now because of the exhaustion of the public IPv4 address pool, namely, they enable IPv6-only clients to communicate with IPv4-only servers.

We have also developed a methodology for the identification of potential security issues of different IPv6 transition technologies [6]. Ref. [3] follows the STRIDE approach, which is a general software security solution and it uses the DFD (Data Flow Diagram) model of the systems to facilitate the discovery of various threats. We have found this approach useful and amended the method in [6], where we have also shown that it is necessary to examine the most important implementations of the given IPv6 transition technologies, whether they are susceptible to the various threats that were discovered by using the STRIDE approach. We have pointed out that DNS64 is theoretically susceptible to *DNS cache poisoning* [7], and now the important practical question is, whether its different implementations are actually susceptible to DNS cache poisoning or not.

The purpose of this paper is to develop a simple and efficient methodology for DNS cache poisoning vulnerability analysis of DNS64 implementations. This paper is based on our workshop paper [8], in which we have presented our testbed and our method for Transaction ID prediction attack as well as our results for some specific DNS64 implementations. Now we give a more detailed introduction to cache poisoning including its further two components (source port number prediction, and the birthday paradox based attack), and also design and carry out their testing methods. Besides the DNS64 implementations included in our workshop paper, now we also include Unbound, because it showed much better performance than BIND [9].

The remainder of this paper is organized as follows. In section II, we examine, why DNS cache poisoning is so crucial

Submitted: December 28, 2017. This work was supported by the International Exchange Program of the National Institute of Information and Communications Technology (NICT), Japan.

G. Lencse was with the Laboratory of Cyber Resilience, Nara Institute of Science and Technology, 8916-5 Takayama, Ikoma, Nara, 630-0192 Japan. He is permanently with the Széchenyi István University, Győr, H-9026, Hungary. (e-mail: lencse@sze.hu)

Y. Kadobayashi, is with the Laboratory of Cyber Resilience, Nara Institute of Science and Technology, 8916-5 Takayama, Ikoma, Nara, 630-0192 Japan. (e-mail: youki-k@is.naist.jp).

DOI: 10.36244/ICJ.2018.2.3

concerning the DNS64 technology and we also elaborate the attack model of DNS cache poisoning. In section III, we survey the available test tools for DNS cache poisoning analysis and point out that they are not suitable for our purposes. In section IV, we design and implement a testbed for security analysis of DNS64 implementations. In section V, we select the DNS64 implementations to be tested and also present their setup. In sections VI, VII, and VIII, we design and carry out different tests for the possible components of the DNS cache poisoning vulnerability, namely, we test Transaction ID and source port predictability, as well as whether the DNS64 implementations send out multiple equivalent queries simultaneously, which would give an opportunity for an attack based on the birthday paradox. In section IX, we summarize and discuss our results, as well as we make suggestions for the elimination of the uncovered vulnerabilities. Section X concludes our paper.

## II. Cache Poisoning Vulnerability of DNS64

The trustworthy operation of the DNS service is a very important precondition for a secure Internet. The ultimate mitigation for DNS cache poisoning, as well as for all other tampering type attacks against DNS, is DNSSEC [10]. However, concerning the cache poisoning vulnerability of DNS64 servers we cannot rely on DNSSEC for two reasons. First of all, its deployment rate is still very low. (As of 2016, it was 1.7% among the Alexa top 1 million web servers [11].) The other reason is DNS64 specific. The task of a DNS64 server is to synthesize an *IPv4-embedded IPv6 address* [12] for the domain names that do not have a AAAA record (IPv6 address). However, this a forged address from the DNSSEC point of view. Thus, a *security aware* and *validating* DNS client has to discard it. The best possible mode of operation is, when a security aware client asks the DNS64 server to perform the validation, see section 3 of [4]. In this case, the client has to trust in the DNS64 server. (And of course, tampering may happen while the packet travels from the DNS64 server to the client.)

Thus for protecting our DNS64 servers from DNS cache poisoning, we need to rely on the guidelines laid down in RFC 5452 [13]. Before addressing them, we need to clarify the attack model, that is, the conditions of a DNS cache poisoning attack. We always consider *blind spoofing*, which means that the attacker may not intercept the DNS requests from the attacked DNS server to the authoritative DNS server. The attacker may send DNS requests (for any domain name) and forged replies to the attacked DNS server.

Now, we first quote the most important conditions from RFC 5452, when a DNS server (called as "resolver" in the text) may accept information from a DNS reply packet, and then interpret them for our situation.

"DNS data is to be accepted by a resolver if and only if:

1. The question section of the reply packet is equivalent to that of a question packet currently waiting for a response.
2. The ID field of the reply packet matches that of the question packet.
3. The response comes from the same network address to which the question was sent.
4. The response comes in on the same network address, including port number, from which the question was sent.

In general, the first response matching these four conditions is accepted." (from section 3 of [13])

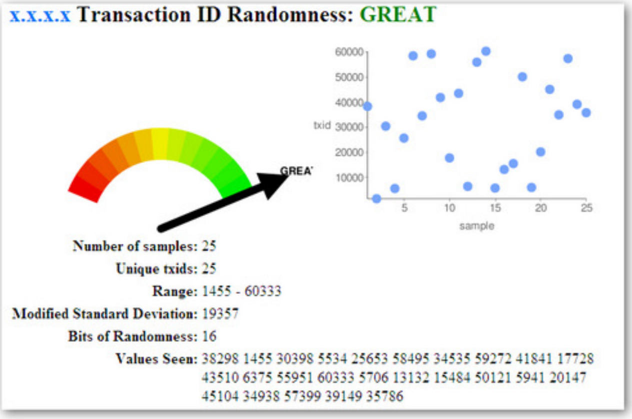
Condition 1 gives a very important protection against spoofed answers by setting up a time limit. This *time interval* is equal to the round trip time between the given DNS server and the authoritative DNS server plus the response time of the authoritative DNS server. (The latter may be increased by the attacker by a DoS attack against the authoritative DNS server.) In its calculations, the RFC uses 100ms as a typical value for the length of this time interval. Of course, an attacker may attempt to initiate the opening of this time window at any time by sending a request for an arbitrarily chosen domain name. However, if a domain name is already cached, it is usually protected, until its TTL expires.

Condition 2 significantly hardens the task of the attacker: the attacker has to guess the *Transaction ID* for a successful attack. To support guessing, the attacker may send DNS resolution requests to the DNS server for any domain names, including domain names, the authoritative DNS servers of which is under the control of the attacker, thus the attacker may observe an arbitrarily long sequence of the Transaction IDs generated by the attacked DNS server. Therefore, DNS servers must use hard to predict (cryptographic) random number generators to prevent the attacker from being able to predict the Transaction IDs. Thus, on average, a number of $2^{15}$ trials are necessary for a successful guess for the 16 bit long Transaction ID (within the given time period of about 100ms).

Condition 3 further hardens the task of the attacker, but not very significantly. There may be a few authoritative DNS servers for a domain, the IP address of which are known for the attacker, and the DNS server may use them in a round robin manner. The attacker needs to spoof exactly the right one. As their number is usually small, this condition contributes only with a small multiplication factor. As for the spoofing itself, there are some countermeasures against source IP address spoofing, such as reverse path checking by routers or firewalls. However, we may not rely on this optional protection: we suppose that it is not switched on, or the attacker is able to send the forged replies from the "right" direction.

Condition 4 has two contributions. The attacked DNS server may have more than one network interfaces (or more than one IP addresses may be assigned to the same interface), but this number is limited, thus it may be only a small factor. The *source port number* can be another significant factor, if the DNS server uses different, hard to predict source port numbers for sending out its every single request. As port numbers from 0 to 1023 cannot be used, the entropy is somewhat less than 16 bits.

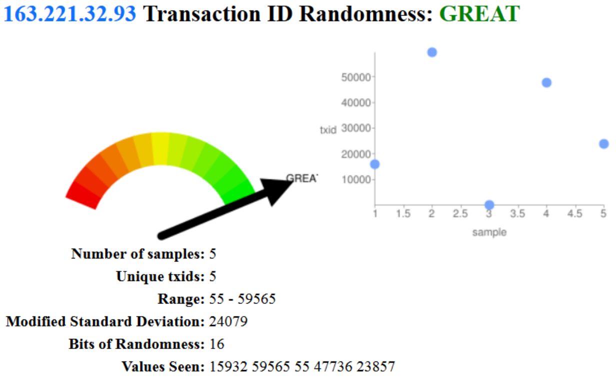
We note that NAT (more exactly: NAPT) devices may remove the entropy of the source port numbers, thus DNS servers should never be placed behind NAPT devices unless the NAPT devices are known to comply with RFC 6056 [14], which requires randomized source port number selection.



x.x.x.x Transaction ID Randomness: GREAT

Number of samples: 25
Unique txids: 25
Range: 1455 - 60333
Modified Standard Deviation: 19357
Bits of Randomness: 16
Values Seen: 38298 1455 30398 5534 25653 58495 34535 59272 41841 17728 43510 6375 55951 60333 5706 13132 15484 50121 5941 20147 45104 34938 57399 39149 35786

Fig. 1. Sample Transaction ID randomness testing results of the DNS-OARC DNS entropy testing tool. [20]



163.221.32.93 Transaction ID Randomness: GREAT

Number of samples: 5
Unique txids: 5
Range: 55 - 59565
Modified Standard Deviation: 24079
Bits of Randomness: 16
Values Seen: 15932 59565 55 47736 23857

Fig. 2. Our Transaction ID randomness test result produced by the DNS-OARC DNS entropy testing tool.

RFC 5452 [13] describes another form of attack, which is based on the birthday paradox. If the attacker may achieve that the DNS server sends out *multiple equivalent queries*, that is queries with identical QNAME, QTYPE, and QCLASS fields, *concurrently* (a new query is sent while another one still waits for an answer) then the forged replies of the attacker may match any of them, which significantly eases the attack. For further details, please refer to the CERT vulnerability note [15].

To sum up the essence of the above conditions, we need to check whether the analyzed DNS64 server implementations use hard to predict random numbers for both Transaction IDs and source port numbers and they do not send multiple equivalent queries concurrently.

## III. Tools for Cache Poisoning Vulnerability Testing

Although Daniel J. Bernstein already disclosed the vulnerability of the DNS system as well as the possible solution in 1999 [16], and there was a CERT notification about the possibility of the birthday paradox based attacks in 2002 [15], some mainstream DNS servers implementations including BIND did not address the issue properly until the CERT notification in 2008 [17], which was triggered by Dan Kaminsky, who invented a more powerful cache poisoning method. His attack is built upon two ideas: it bypasses the protection of the TTL by using different random names from the attacked domain, and goes one hierarchy level higher: instead of trying to insert a forged "A" record into the cache of the attacked DNS server, it hijacks the whole attacked zone by including the IP address of a DNS server controlled by the attacker as an IP address of a DNS server for the attacked domain into an Authority record of a forged answer for a query for a random name from the attacked zone (to trick the bailiwick rule), see [18] for an in depth and well-illustrated description of the attack.

Then the alert was taken seriously, and patches were prepared for all those major DNS implementations that were still vulnerable. Also vulnerability testing tools were prepared and released.

A contemporary web based Transaction ID and source port randomness tester by DNS-OARC is still available [19]. It is documented and highly suggested by [20]. Although the demonstration screen at the documentation does not seem to be so bad, see Fig. 1, our experience was rather poor. When we tried it out, among others, we received the results shown in Fig. 2. We contend that it is not enough to test only five Transaction IDs. But we do not have an opportunity to tune the tests.

Another web-based testing tool is mentioned in the ICANN presentation of Kim Davies [21], but the tool is no more available at the URL mentioned on slide 33 of the presentation: http://recursive.iana.org/.

And there is another problem with these web-based tools: they require that the DNS server is configured in a live system.

We rather decided to build a *testbed*, that is, an isolated environment, where we can check whether the examined DNS64 implementations indeed have the presumed vulnerabilities by using any kind of tests with any parameters we consider necessary.

## IV. Testbed Design and Implementation

### A. General Considerations

Although we intended to design a testbed for the security analysis of DNS64 server implementations, we made our considerations with a broader mindset, so that the testbed may also be used for the security analysis of other IPv6 transition technologies, especially NAT64.

In general, the requirements for such a testbed usually include the following:

1. isolated environment, where attacks may be performed
2. ease of use
3. low cost.

A testbed for the security analysis of different IPv6 transition technologies should contain the fundamental basic blocks of the systems in which the given solutions are used. Practically it means that we need a few computers which are interconnected by IPv4 and/or IPv6 network(s). Such systems can be built in

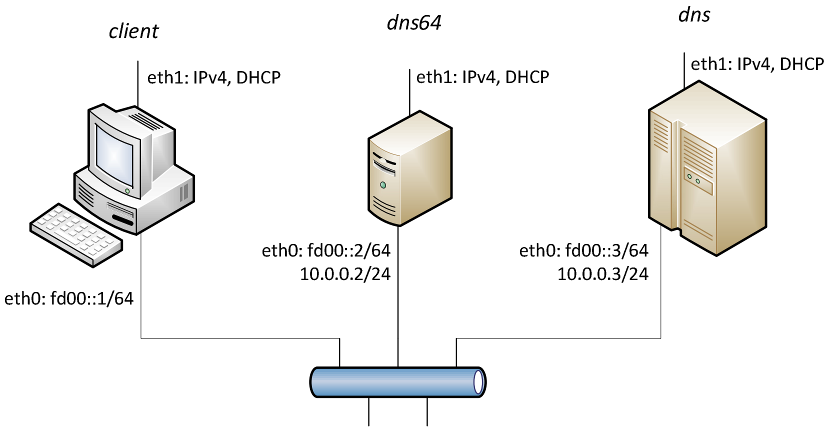


Fig. 3. Topology of the test network.

Table 1. Linux and VMware Network Settings for Virtual Machines.

| Virtual machine name | `client` | `dns64` | `dns` |
|---|---|---|---|
| Role | IPv6-only client | DNS64 server | Authoritative DNS server |
| `eth0` Linux settings | IPv6 static: fd00::1/64 | IPv6 static: fd00::2/64<br>IPv4 static 10.0.0.2/24 | IPv6 static: fd00::3/64<br>IPv4 static: 10.0.0.3/24 |
| `eth1` Linux settings | IPv4 DHCP | IPv4 DHCP | IPv4 DHCP |
| `eth0` VMware settings | VMnet1 | VMnet1 | VMnet1 |
| `eth1` VMware settings | NAT | NAT | NAT |

several ways, including the usage of:

1. server computers
2. desktop or laptop computers
3. single-board computers [22]
4. virtual machines.

We contend that the consecutive solutions result in less cost and higher comfort in use including easy mobility. Our decision was also influenced by the fact that we have been successfully using virtual Linux boxes (executed under Windows 7) for the practical education of DNS64 and NAT64 IPv6 transition technologies at the Budapest University of Technology and Economics since 2015.

As the existing virtual machine images were suitable for our current testing purposes, it was a convenient solution to reuse them. The virtual machine images were prepared by a script called **`debian-vm`**, written by Dániel Bakai [23]. (This script creates a small, low memory usage, user-defined Debian virtual machine disk image, which can be used in various hypervisors including VMware and KVM.) They contain Debian 8 distributions, which were now updated to Debian version 8.9. They were executed by VMware Workstation 12 Player.

### *B. Topology of the Test Network*

We propose the structure of a simple testbed suitable for the security analysis of the DNS64 and the stateful NAT64 IPv6 transition technologies. Similar testbeds can be built for the security analysis of other IPv6 transition technologies.

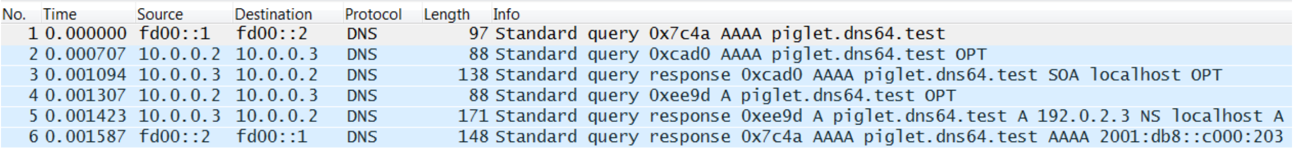
The testing of DNS64 or NAT64 requires a network of three hosts. As for DNS64, they are: client, DNS64 server and authoritative DNS server, where the DNS64 server should be interconnected with both the client and the authoritative DNS server. As for NAT64, only the roles are different: client, NAT64 gateway and IPv4-only server; the topology is the same. Thus the same network can be used for the testing of the different implementations of both IPv6 transition technologies, only some software components need to be changed.

As for the attacker, two further hosts could have been added, one for tampering with each connections, but we eliminated them with a trick. First of all, we used a single shared medium to interconnect the three computers, see Fig. 3, thus only one extra device would have been enough. However, as in our current tests we used only wiretapping, it could be done at any of the three computers, thus no further computer was necessary.

### *C. Implementation of the Test Network*

We have implemented the test network shown in Fig. 3 by three virtual machines, each of which had a single CPU core, 128MB of RAM, and (theoretically) 40GB of hard disks, but the starting size of the images were under 1GB. (They were growing during the experiments, but remained under 3GB.) Table 1 shows the Linux and WMware settings used for the virtual machines.

We note that the IP version between the client, which is an IPv6-only client, and the DNS64 server must be 6. There is no restriction for the IP version between the DNS64 server and the DNS server, but when testing NAT64, IPv4 must be used between the NAT64 gateway and the IPv4-only server. Although we used IPv4 between the DNS64 server and the



```
No.  Time      Source    Destination  Protocol  Length  Info
   1 0.000000  fd00::1   fd00::2      DNS           97 Standard query 0x7c4a AAAA piglet.dns64.test
   2 0.000707  10.0.0.2  10.0.0.3     DNS           88 Standard query 0xcad0 AAAA piglet.dns64.test OPT
   3 0.001094  10.0.0.3  10.0.0.2     DNS          138 Standard query response 0xcad0 AAAA piglet.dns64.test SOA localhost OPT
   4 0.001307  10.0.0.2  10.0.0.3     DNS           88 Standard query 0xee9d A piglet.dns64.test OPT
   5 0.001423  10.0.0.3  10.0.0.2     DNS          171 Standard query response 0xee9d A piglet.dns64.test A 192.0.2.3 NS localhost A
   6 0.001587  fd00::2   fd00::1      DNS          148 Standard query response 0x7c4a AAAA piglet.dns64.test AAAA 2001:db8::c000:203
```

Fig. 4. Wireshark capture taken during the functional checking of the DNS64 testbed.

authoritative DNS server during our DNS64 vulnerability tests, we set also an IPv6 address at the authoritative DNS server to be able to reach it directly from the client for testing its operability.

We also note that the **eth1** interfaces were not necessary for the tests, we used them for providing the virtual machines with Internet access, which was sometimes necessary, e.g. for installing various packages under Debian Linux. We have separated this communication from the testing communication, which happened always through the **eth0** interfaces of the virtual computers.

### *D. Setup of a Basic DNS64 Testbed*

The purpose of this setup was to check whether the testbed works properly. We have installed BIND9 [24] to both the **dns64** and the **dns** virtual machines.

#### *1) 1. Setup of the DNS64 Server*

The **/etc/bind/named.conf.options** file was used to set up the DNS64 function. The relevant settings were:

```
dns64 2001:db8:1::/96 { };
forwarders { 10.0.0.3;};
dnssec-validation no
```

#### *2) 2. Setup of the Authoritative DNS Server*

The **/etc/bind/named.conf.local** file was used to set up the authoritative DNS server. The relevant settings were:

```
zone "dns64.test" {
  type master;
  file "/etc/bind/db.dns64.test";
};
```

The content of the **db.dns64.test** file was:

```
$ORIGIN dns64.test.
$TTL 86400
@  IN  SOA  localhost.  root.localhost.  (
           2017090702    ; Serial
                14400    ; Refresh
                 7200    ; Retry
                72000    ; Expire
                 3600  ) ; Negative Cache TTL
;
@       IN      NS      localhost.

kanga   IN      A       192.0.2.1
owl     IN      A       192.0.2.2
piglet  IN      A       192.0.2.3
rabbit  IN      A       192.0.2.4
winnie  IN      A       192.0.2.5
```

### *E. Functional Checking of the Test Network*

In this section, we demonstrate the correct operation of the test system, and also introduce the operation of DNS64 servers, which will be important later.

We tested the operation of the testbed by issuing the following command on the **client** computer:

```
host -t AAAA piglet.dns64.test dns64
```

The **host** Linux command was used to request a AAAA record for the **piglet.dns64.test** domain name from the DNS64 server executed by the host named **dns64**.

The DNS messages were captured by **Wireshark** on the **VMnet1** interface using the **port 53** capture filter. The six captured packets are shown in Fig. 4. Now we shall identify the six messages and observe their Transaction IDs, which are used to match the answer with the query. We will experiment with them later.

1. Request for a AAAA record from the client to the DNS64 server with Transaction ID 0x7c4a, generated by the **host** command.
2. Request for a AAAA record from the DNS64 server to the authoritative DNS server with a different Transaction ID, 0xcad0, generated by BIND.
3. An "empty" reply for the AAAA record request sent by the authoritative DNS server to the DNS64 server, and its Transaction ID is the same as that of the corresponding request.
4. Request for an A record from the DNS64 server to the authoritative DNS server with a different Transaction ID, 0xee9d, generated by BIND.
5. A valid reply with an A record sent by the authoritative DNS server to the DNS64 server, and its Transaction ID is the same as that of the corresponding request.
6. The reply of the DNS64 server to the client containing the synthesized *IPv4-embedded IPv6 address* [12] with the same Transaction ID as message 1.

Thus we have found that the testbed worked fine, and it was ready for testing.

## V. DNS64 IMPLEMENTATION SELECTION AND SETUP

We have laid down our implementations selection guidelines in [2] as follows:

"As for the implementations, we only deal with those that are free software [25] (also called open source [26]) for multiple reasons:

- The licenses of certain vendors (e.g. [27] and [28]) do not allow reverse engineering and sometimes even the publication of benchmarking results is prohibited.
- Free software can be used by anyone for any purposes thus our results can be helpful for anyone.
- Free software is available free of charge for us, too.

Within the category of the free software implementations, we give further priority to those, which are used widespread and/or are known to be stable and high performance (if such information is available).” [2]

Although several DNS implementations exist, only very few of them can do DNS64, thus finding such DNS64 implementations was not an easy task. We selected the following DNS64 implementations for testing:

1. BIND 9.9.5-9+deb8u12-Debian [24]
2. TOTD 1.5.2 (referred later as OLDTOTD) [29]
3. TOTD 1.5.3 (referred later as NEWTOTD) [30]
4. mtd64-ng 1.1.0 [31]
5. PowerDNS Recursor 3.6.2 [32]
6. Unbound 1.6.0 [33]

Remarks:

- Including BIND9 was a must as it is the de facto industry standard DNS server, therefore, it is very likely wide-spread used for DNS64 purposes, too.
- Some years before we have prepared a patch for TOTD, which resolved some security issues [30], and now we tested its both patched and unpatched versions.
- We also have a new tiny DNS64 proxy called mtd64-ng [31], which is currently developed in an ongoing university project. Although it is not yet ready for deployment, we have also included it.

We have already introduced the DNS64 configuration of BIND in section IV.D.1.

The configuration of both versions of TOTD was done in the **`/usr/local/etc/totd.conf`** file, the relevant settings were:

```
forwarder 10.0.0.3
prefix 2001:db8:404d::
```

The configuration of the mtd64-ng DNS proxy was done in the **`/etc/mtd64-ng.conf`** file, where the relevant settings were:

```
nameserver 10.0.0.3
prefix 2001:db8::/96
num-threads 1
```

The DNS64 configuration of PowerDNS was a bit more complex.

In the **`/etc/powerdns/recursor.conf`** file, we made the following relevant settings:

```
allow from=::/0
forward-zones=dns64perf.test=10.0.0.3
local-address=fd00::2
lua-dns-script=/etc/powerdns/dns64.lua
```

The content of the **`/etc/powerdns/dns64.lua`** file was:

```
function nodata ( remoteip, domain, qtype, records )
if qtype ~= pdns.AAAA then return pdns.PASS, {} end
setvariable()
return "getFakeAAAARecords", domain, "2001:db8::"
end
```

As for Unbound, its 1.4.22 version distributed in Debian 8.9 did not contain the DNS64 module, which was included from its next version, namely 1.5.0. Therefore we upgraded the **`dns64`** host to Debian 9.3 after the execution of all the experiments with the other DNS64 implementations.

As for its configuration, we have added the following lines to the **`/etc/unbound/unbound.conf`** file:

```
access-control: ::/0 allow
module-config: "dns64 iterator"
dns64-prefix: 2001:db8:bd::/96
forward-zone:
  name: dns64perf.test.
  forward-addr: 10.0.0.3
server:
  interface: fd00::2
```

## VI. Transaction ID Prediction Vulnerability Testing

### A. *Details of the Measurements*

We extended the configuration of our testbed to be able to examine the Transaction IDs of a high number of messages even if the examined DNS64 implementations use caching.

#### 1) *Name Space and Configuration for Testing*

To be able to perform a high number of tests, we needed a name space which can be generated systematically. We have found that the name space used in our earlier DNS64 tests [34] would be appropriate. It was the following name space:

10-a-b-c.dns64perf.test, where a, b, c are integers from the [0, 255] interval.

We have used only the 10-0-{0..255}-{0..225} part of it. For generating the zone file, we used the modified version of the zone file generator script called **`gen-zonefile`**, which is shipped together with the **`dns64perf`** program (documented in [34] and available from [35]).

The **`/etc/bind/named.conf.local`** file of the authoritative DNS server was modified as follows:

```
zone "dns64perf.test" {
  type master;
  file "/etc/bind/db.dns64perf.test";
};
```

Thus, BIND used our newly generated zone file after its being restarted.

#### 2) *Execution of the Measurements*

The measurements were performed by the **`dns64perf`** [34] program, which used sequential Transaction IDs from 0 to 65535. The command line of the test program was:

```
./dns64perf 0 1 1 dns64
```

The first argument specified the “a” parameter described above, the second argument meant that the test program needed to use only one thread, the third one specified the timeout of 1 second, and the last one was the host name of the DNS64 server to be tested.

The traffic was captured by the **`tshark`** program executed by the **`dns64`** host, the memory size of which was raised to 256MB, because 128MB was not enough and the **`tshark`** program exited during the measurement. All the packets from the **`eth0`** interface that matched the **`port 53`** capture filter were saved to a file. The following command line was used:

```
tshark -i eht0 -f "port 53" > imp-full
```

where the *imp* string was replaced by the name of the tested DNS64 implementation.

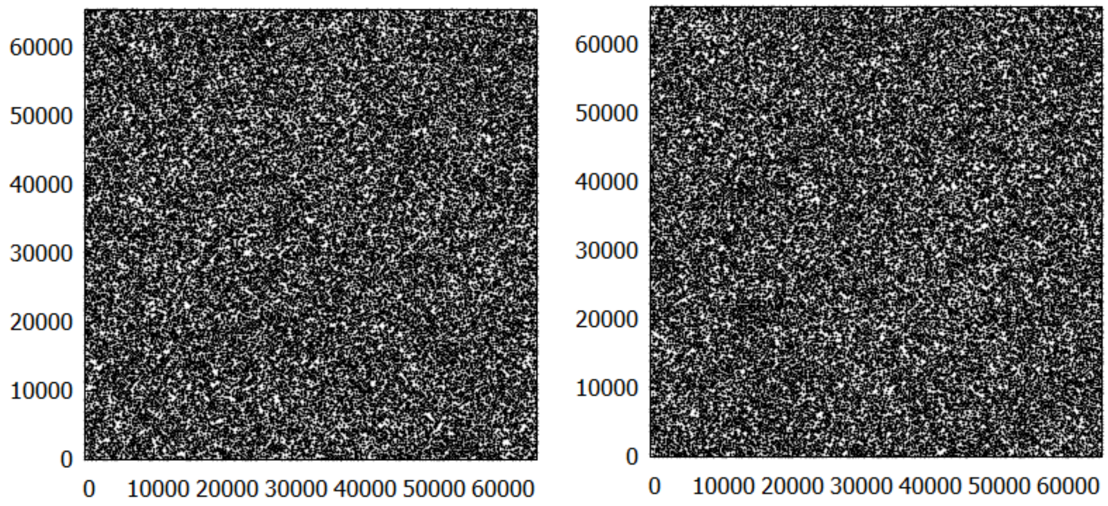


Fig. 5. BIND, Transaction ID input correlation (left) and autocorrelation (right)

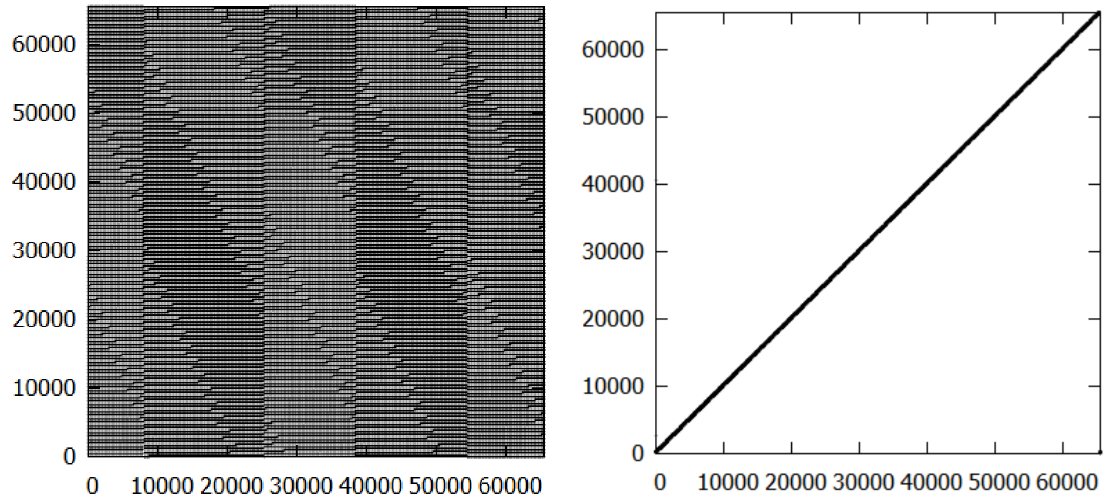


Fig. 6. OLDTOTD, Transaction ID input correlation (left) and autocorrelation (right)

### *B. Evaluation Method*

Predictability of the Transaction IDs is a hard question. E.g. if pseudorandom numbers are used that were generated by a linear congruential generator (LCG), then they are predictable. There are a high number of methods described for testing randomness both in university lecture notes [36] and research papers [37].

Since our solution of using a testbed ensures us full control of the testing method, and gives us access to the raw results, we have the possibility to use multiple methods for evaluation if needed. We decided to use first a simple, graphical method, which is somewhat similar to that of the earlier mentioned entropy tester of DNS-OARC [19], but we contend that our method is more thorough than that.

We have checked two kinds of correlations using visualization. Before introducing them, let us define some notations first. Let $i$ denote the ordinal number of a message in the message sequence introduced in section IV.E, where $i$ is in [1, 6]. Let $j$ denote the ordinal number of the AAAA record request sent by the **dns64perf** program, where $j$ is in [0, 65535]. Let $T_{ij}$ denote the Transaction ID of the $i$-th message from the six messages used to resolve the $j$-th query of the **dns64perf** program. As the test program uses sequential Transaction IDs from 0, it is sure that: $T_{1j} = T_{6j} = j$.

We use two graphs. An (x, y) plot of the ($T_{1j}$, $T_{2j}$) pairs may reveal correlation between the Transaction ID used by the **dns64perf** program and the first Transaction ID generated by the DNS64 program. An (x, y) plot of the ($T_{2j}$, $T_{4j}$) pairs may reveal correlation between the consecutive Transaction IDs generated by the DNS64 program. For simplicity, we will refer to the first one as *input correlation*, and the second one as *autocorrelation*.

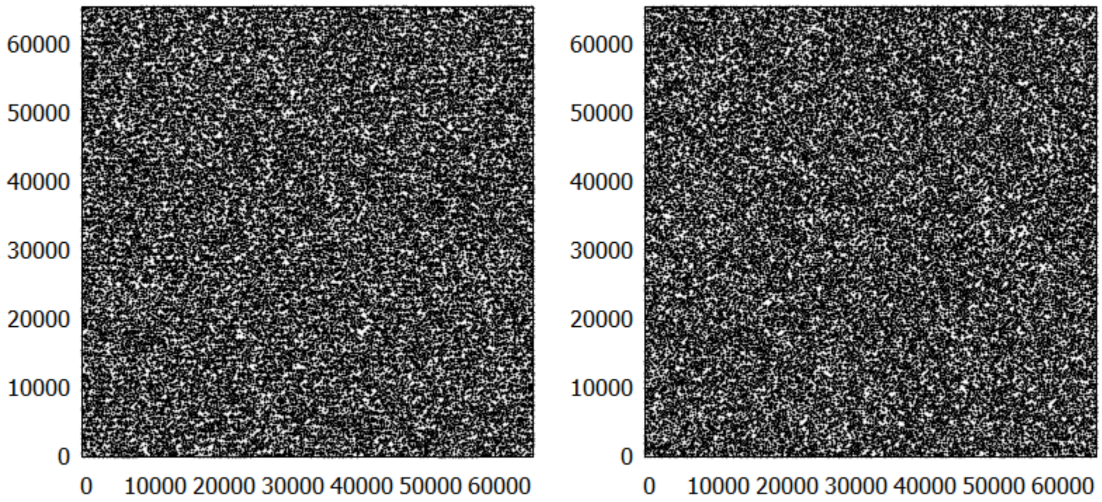


Fig. 7. NEWTOTD, Transaction ID input correlation (left) and autocorrelation (right)

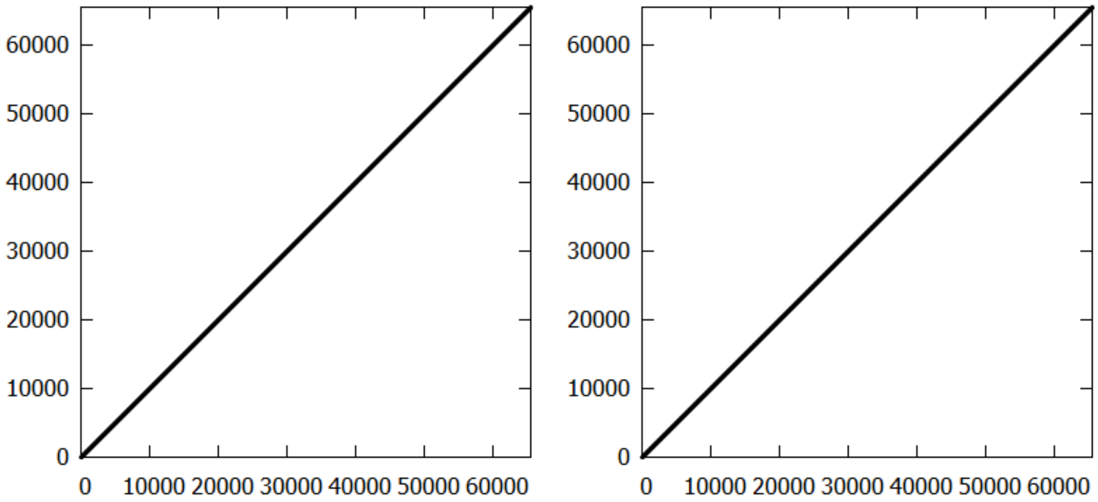


Fig. 8. mtd64-ng, Transaction ID initial correlation (left) and autocorrelation (right)

We used **awk** scripts to extract the appropriate Transaction IDs from the text file output of the **tshark** program, and the graphs were prepared by **gnuplot**.

### C. Measurement Results

Fig. 5 shows the input correlation and the autocorrelation of the Transaction IDs of BIND. They seem to be like noise, thus we can say that no predictability problems were revealed by our simple evaluation method.

The left graph of Fig. 6 shows the input correlation of the Transaction IDs of OLDTOTD. The regular patterns indicate that there is a problem with the predictability of the Transaction IDs. Before giving the explanation, let us have a look at the autocorrelation of the Transaction IDs of OLDTOTD on the right side of Fig. 6. Now, the predictability is even more deliberate. Let us look into the CSV file containing the ($T_{1j}$, $T_{2j}$) pairs for input correlation checking:

```
0, 55745
1, 56257
2, 56769
3, 57281
4, 57793
```

Whereas the $T_{1j}$ Transaction IDs start from 0 and increase by 1, the $T_{2j}$ Transaction IDs start from a different number and increase by 512. The CSV file containing the ($T_{2j}$, $T_{4j}$) pairs for autocorrelation checking can give us further help:

```
55745, 56001
56257, 56513
56769, 57025
57281, 57537
57793. 58049
```

where the *imp* string was replaced by the name of the tested DNS64 implementation.

Table 2. Source Port Randomness Test Results

| DNS64 Implementation | source ports observed in the experiments | | |
|---|---|---|---|
| | minimum | maximum | std. dev. |
| BIND | 1024 | 65535 | 18635 |
| OLDTOTD | 53 | 53 | 0 |
| NEWTOTD | 53 | 53 | 0 |
| mtd64-ng | 32768 | 61000 | 8136 |
| PowerDNS | 1025 | 65534 | 18655 |
| Unbound | 1024 | 65535 | 17467 |

It is well visible that the consecutive Transaction IDs always increase by 256. And now we give the explanation. As we disclosed it in [30], the old version of TOTD generated sequential numbers as Transaction IDs. The increase of 256 is the result of the facts that the notebook used for testing has an Intel CPU, which uses LSB byte order (least significant byte first), whereas the network byte order is MSB (most significant byte first). The programmer could have been used the standard **htons()** function for the conversion, but omitting it is just a feature and not a bug, as Transaction IDs are just identifiers and they do not convey any special meaning. For more information about the bug, which randomly caused an unresponsiveness of the old version of TOTD, and for its correction, please refer to [30], where we have also described the elimination of its vulnerability for Transaction ID prediction attack.

Fig. 7 shows the input correlation and autocorrelation of the Transaction IDs of NEWTOTD. They seem to be like noise, which is exactly what we expected.

Fig. 8 shows the input correlation and autocorrelation of the Transaction IDs of mtd64-ng. They are two completely identical graphs, as the two CSV files were found also completely identical. It is visibly the graph of y=x function, because mtd64-ng reuses the Transaction ID of the received query and sends both of its own queries with the same Transaction ID, which is a serious vulnerability.

As we already mentioned, mtd64-ng is a result of an ongoing university project and it not yet ready to be used in production systems [31].

As for PowerDNS and Unbound, we have also performed the tests and evaluated the results. All their plots looked like the plots of BIND or NEWTOTD, thus we can state that we found no signs of Transaction ID predictability. (We omit the four plots, because we see no point in including further four "random art" images.)

## VII. SOURCE PORT NUMBER RANDOMNESS TESTING

The results of the Transaction ID prediction tests could have been used also for port number randomness tests, but **tshark** did not include the port numbers in its output. (Its default output contains the same data as the Wireshark screen shown in Fig. 4.) Therefore, we had to make a new series of measurements using a different command line for **tshark** as follows:

```
tshark -i eth0 -f "src host 10.0.0.2 and
udp dst port 53" -T fields -e udp.srcport
> imp-srcports
```

The capture filter ensured that only IPv4 packets sent from the DNS64 server program at **dns64** (with source IP address 10.0.0.2) to the authoritative DNS server program (listening at port 53 of **dns**) be included. The output file contained only the source port numbers. As expected, the result files contained 131072 numbers, except for BIND, in the case of which there were 131073 numbers in the file. We have investigated the case and found that it was so because BIND also sent a query for the IP addresses of the root DNS servers. None of the other implementations did so.

We have summarized our results in Table 2. BIND, PowerDNS and Unbound follow the guidelines of RFC 5452 [13] and choose a source port number randomly from the largest available range of [1024, 65535]. Both versions of TOTD use source port 53 for all outgoing queries. This is trivially predictable. As for mtd64-ng, what can be seen from Table 2, is that the source port number range is [32768, 61000]. What cannot be seen from the table is that the same source ports are used for querying the AAAA record and the A record for the same domain name. This is deliberate from the raw measurement results, we show only the first 6 lines:

```
48926
48926
41556
41556
42713
42713
```

And it is also deliberate from the source code [38]. Although, this phenomenon does not mean predictability in the bind spoofing attack model, we recommend the usage of different source ports for the AAAA and A record queries.

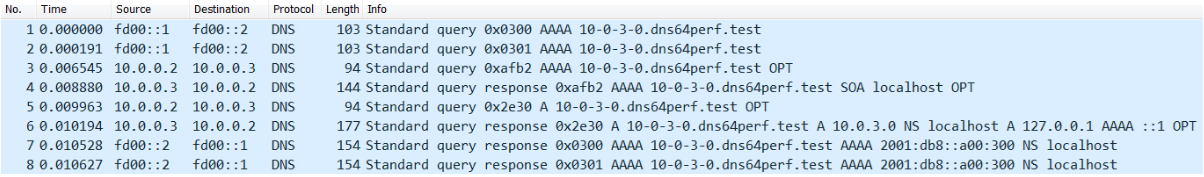
It can also be seen from the source code, that mtd64-ng entrusts the source port selection to the operating system. It can be satisfactory, if the operating system complies with RFC 6056 [14], but we contend that is safer if source port randomization is done by the DNS or DNS64 implementation itself.

## VIII. MULTIPLE EQUIVALENT QUERIES VULNERABILITY TESTING

To be able to test, whether the examined DNS64 implementations send multiple equivalent queries concurrently, we had to modify the test program so that it can send multiple queries for the same domain name.

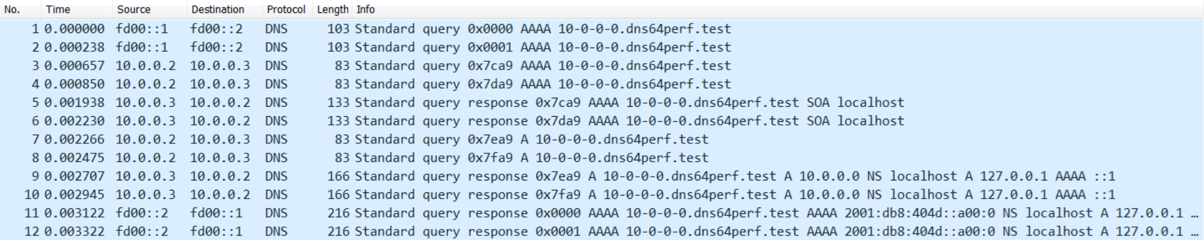
### *A. Test Program for Checking Birthday Attack Vulnerability*

The **dns64perf** [35] test program was used as a starting point of our new **birthday-test** program. Its arguments are: **b**, **n**, **timeout**, **IPv6Addr** and **port**. Parameter **b** can be used to perform multiple tests with a different domain name in each test. It is for convenience: when multiple tests are done, the DNS64 server may cache the previously used domain names and it is easier to use a different one for a new test, than restarting the DNS64 server. Parameter **n** specifies the number of queries to be sent. The rest of the parameters are to be interpreted as that of the original test program, that is,



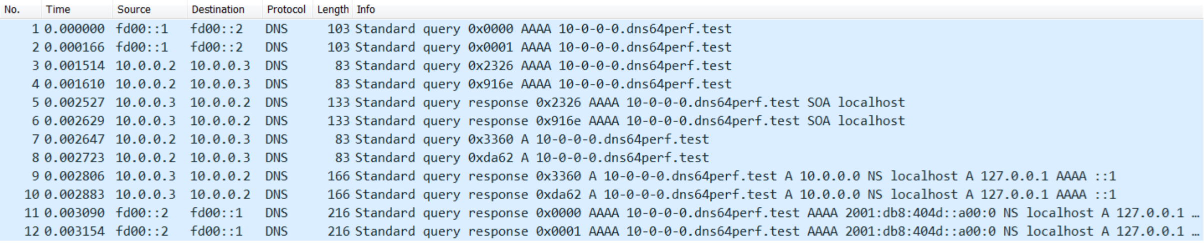
```
No.  Time     Source   Destination Protocol Length Info
  1 0.000000 fd00::1   fd00::2     DNS      103 Standard query 0x0300 AAAA 10-0-3-0.dns64perf.test
  2 0.000191 fd00::1   fd00::2     DNS      103 Standard query 0x0301 AAAA 10-0-3-0.dns64perf.test
  3 0.006545 10.0.0.2  10.0.0.3    DNS       94 Standard query 0xafb2 AAAA 10-0-3-0.dns64perf.test OPT
  4 0.008880 10.0.0.3  10.0.0.2    DNS      144 Standard query response 0xafb2 AAAA 10-0-3-0.dns64perf.test SOA localhost OPT
  5 0.009963 10.0.0.2  10.0.0.3    DNS       94 Standard query 0x2e30 A 10-0-3-0.dns64perf.test OPT
  6 0.010194 10.0.0.3  10.0.0.2    DNS      177 Standard query response 0x2e30 A 10-0-3-0.dns64perf.test A 10.0.3.0 NS localhost A 127.0.0.1 AAAA ::1 OPT
  7 0.010528 fd00::2   fd00::1     DNS      154 Standard query response 0x0300 AAAA 10-0-3-0.dns64perf.test AAAA 2001:db8::a00:300 NS localhost
  8 0.010627 fd00::2   fd00::1     DNS      154 Standard query response 0x0301 AAAA 10-0-3-0.dns64perf.test AAAA 2001:db8::a00:300 NS localhost
```

Fig. 9. Wireshark capture taken during the birthday attack vulnerability test of BIND.



```
No.  Time     Source   Destination Protocol Length Info
  1 0.000000 fd00::1   fd00::2     DNS      103 Standard query 0x0000 AAAA 10-0-0-0.dns64perf.test
  2 0.000238 fd00::1   fd00::2     DNS      103 Standard query 0x0001 AAAA 10-0-0-0.dns64perf.test
  3 0.000657 10.0.0.2  10.0.0.3    DNS       83 Standard query 0x7ca9 AAAA 10-0-0-0.dns64perf.test
  4 0.000850 10.0.0.2  10.0.0.3    DNS       83 Standard query 0x7da9 AAAA 10-0-0-0.dns64perf.test
  5 0.001938 10.0.0.3  10.0.0.2    DNS      133 Standard query response 0x7ca9 AAAA 10-0-0-0.dns64perf.test SOA localhost
  6 0.002230 10.0.0.3  10.0.0.2    DNS      133 Standard query response 0x7da9 AAAA 10-0-0-0.dns64perf.test SOA localhost
  7 0.002266 10.0.0.2  10.0.0.3    DNS       83 Standard query 0x7ea9 A 10-0-0-0.dns64perf.test
  8 0.002475 10.0.0.2  10.0.0.3    DNS       83 Standard query 0x7fa9 A 10-0-0-0.dns64perf.test
  9 0.002707 10.0.0.3  10.0.0.2    DNS      166 Standard query response 0x7ea9 A 10-0-0-0.dns64perf.test A 10.0.0.0 NS localhost A 127.0.0.1 AAAA ::1
 10 0.002945 10.0.0.3  10.0.0.2    DNS      166 Standard query response 0x7fa9 A 10-0-0-0.dns64perf.test A 10.0.0.0 NS localhost A 127.0.0.1 AAAA ::1
 11 0.003122 fd00::2   fd00::1     DNS      216 Standard query response 0x0000 AAAA 10-0-0-0.dns64perf.test AAAA 2001:db8:404d::a00:0 NS localhost A 127.0.0.1 …
 12 0.003322 fd00::2   fd00::1     DNS      216 Standard query response 0x0001 AAAA 10-0-0-0.dns64perf.test AAAA 2001:db8:404d::a00:0 NS localhost A 127.0.0.1 …
```

Fig. 10. Wireshark capture taken during the birthday attack vulnerability test of OLDTOTD.



```
No.  Time     Source   Destination Protocol Length Info
  1 0.000000 fd00::1   fd00::2     DNS      103 Standard query 0x0000 AAAA 10-0-0-0.dns64perf.test
  2 0.000166 fd00::1   fd00::2     DNS      103 Standard query 0x0001 AAAA 10-0-0-0.dns64perf.test
  3 0.001514 10.0.0.2  10.0.0.3    DNS       83 Standard query 0x2326 AAAA 10-0-0-0.dns64perf.test
  4 0.001610 10.0.0.2  10.0.0.3    DNS       83 Standard query 0x916e AAAA 10-0-0-0.dns64perf.test
  5 0.002527 10.0.0.3  10.0.0.2    DNS      133 Standard query response 0x2326 AAAA 10-0-0-0.dns64perf.test SOA localhost
  6 0.002629 10.0.0.3  10.0.0.2    DNS      133 Standard query response 0x916e AAAA 10-0-0-0.dns64perf.test SOA localhost
  7 0.002647 10.0.0.2  10.0.0.3    DNS       83 Standard query 0x3360 A 10-0-0-0.dns64perf.test
  8 0.002723 10.0.0.2  10.0.0.3    DNS       83 Standard query 0xda62 A 10-0-0-0.dns64perf.test
  9 0.002806 10.0.0.3  10.0.0.2    DNS      166 Standard query response 0x3360 A 10-0-0-0.dns64perf.test A 10.0.0.0 NS localhost A 127.0.0.1 AAAA ::1
 10 0.002883 10.0.0.3  10.0.0.2    DNS      166 Standard query response 0xda62 A 10-0-0-0.dns64perf.test A 10.0.0.0 NS localhost A 127.0.0.1 AAAA ::1
 11 0.003090 fd00::2   fd00::1     DNS      216 Standard query response 0x0000 AAAA 10-0-0-0.dns64perf.test AAAA 2001:db8:404d::a00:0 NS localhost A 127.0.0.1 …
 12 0.003154 fd00::2   fd00::1     DNS      216 Standard query response 0x0001 AAAA 10-0-0-0.dns64perf.test AAAA 2001:db8:404d::a00:0 NS localhost A 127.0.0.1 …
```

Fig. 11. Wireshark capture taken during the birthday attack vulnerability test of NEWTOTD.

**`timeout`**, **`IPv6Addr`** and **`port`** specify the timeout value of the receive function, the IPv6 address (or host name) of the DNS64 server to be tested and the port number, where the DNS64 server listens, respectively. (The port number is optional, its default value is 53.)

The program sends **`n`** number of AAAA record requests for the 10-0-b-0.dns64perf.test domain name, where **`n`** and **`b`** should be in the [0, 255] interval. After sending all the queries, it also receives the replies, but it does not use them for any purposes. It receives them only to avoid the annoying "Destination Unreachable (Port Unreachable)" ICMP error messages.

The source code of the test program is available from [39].

### B. *Measurements and Results*

The concurrently sent multiple equivalent queries vulnerability tests were performed in the same testbed as the previous two measurements. Wireshark (executed on the host computer under Windows) was used to monitor the behavior of the DNS64 implementations. We captured the packets on the VMnet1 interface using the **`port 53`** capture filter.

The usual command line was:

```
./birthday-test 0 2 1 dns64
```

(However, sometimes different values were used for **`b`**, e.g. 3 instead of 0 in the case shown in Fig. 9.)

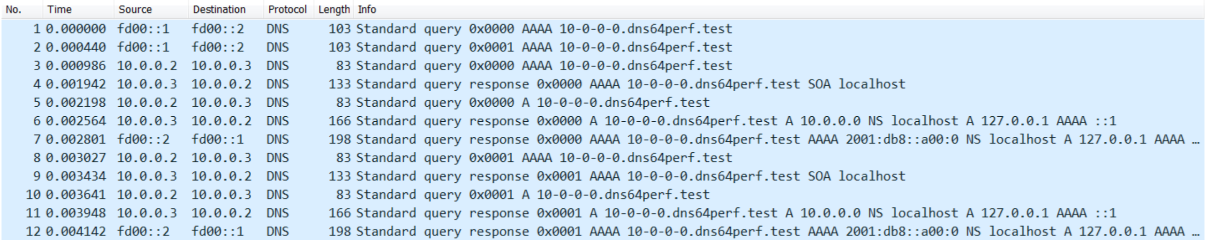
The results produced by BIND can be seen in Fig. 9. Although we sent two queries for the AAAA record of the same domain name, BIND sent only one request to the authoritative DNS server for the AAAA record of the given domain name. (Its next query is for the A record.) Thus BIND is not vulnerable to the "birthday attack".

The results produced by OLDTOTD can be seen in Fig. 10. It sent two equivalent queries for the same resource records (first for AAAA records and then for A records). It can be also observed that the Transaction IDs were incremented by 0x100, as they took the values: 0x7ca9, 0x7da9, 0x7ea9, 0x7fa9.

We note that none of them is a serious problem, because TOTD does not use caching. Thus no cache poisoning attack against TOTD is possible. The attacker can at most achieve that a single client receives forged answer.

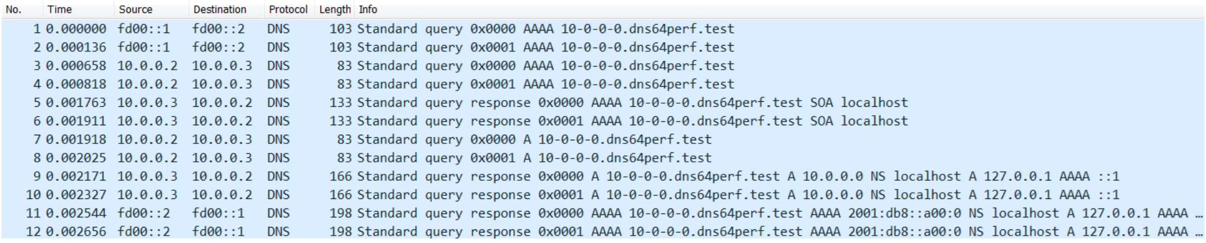
The results produced by NEWTOTD can be seen in Fig. 11. The only improvement over OLDTOTD is the proper Transaction ID randomization.

We performed two measurements with mtd64-ng because of the following reasons. As only one CPU core was assigned to the **`dns64`** virtual machine in the testbed, originally we set the number of working threads of mtd64-ng to 1. Due to this setting, mtd64-ng serialized the processing of the requests from our test program, as shown in Fig. 12. However, the DNS64 server of a large network with a high number of users should use multiple threads, therefore we executed the test also with two threads. The results in Fig. 13 reveal that mtd64-ng sends separate AAAA and A record requests for each client request. Although mtd64-ng currently does not support caching, thus it is not a serious vulnerability, the problem must be addressed



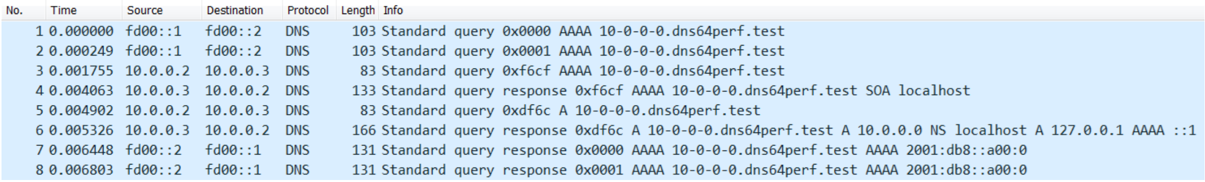
```
No.  Time      Source    Destination Protocol Length Info
   1 0.000000  fd00::1   fd00::2     DNS      103 Standard query 0x0000 AAAA 10-0-0-0.dns64perf.test
   2 0.000440  fd00::1   fd00::2     DNS      103 Standard query 0x0001 AAAA 10-0-0-0.dns64perf.test
   3 0.000986  10.0.0.2  10.0.0.3    DNS       83 Standard query 0x0000 AAAA 10-0-0-0.dns64perf.test
   4 0.001942  10.0.0.3  10.0.0.2    DNS      133 Standard query response 0x0000 AAAA 10-0-0-0.dns64perf.test SOA localhost
   5 0.002198  10.0.0.2  10.0.0.3    DNS       83 Standard query 0x0000 A 10-0-0-0.dns64perf.test
   6 0.002564  10.0.0.3  10.0.0.2    DNS      166 Standard query response 0x0000 A 10-0-0-0.dns64perf.test A 10.0.0.0 NS localhost A 127.0.0.1 AAAA ::1
   7 0.002801  fd00::2   fd00::1     DNS      198 Standard query response 0x0000 AAAA 10-0-0-0.dns64perf.test AAAA 2001:db8::a00:0 NS localhost A 127.0.0.1 AAAA …
   8 0.003027  10.0.0.2  10.0.0.3    DNS       83 Standard query 0x0001 AAAA 10-0-0-0.dns64perf.test
   9 0.003434  10.0.0.3  10.0.0.2    DNS      133 Standard query response 0x0001 AAAA 10-0-0-0.dns64perf.test SOA localhost
  10 0.003641  10.0.0.2  10.0.0.3    DNS       83 Standard query 0x0001 A 10-0-0-0.dns64perf.test
  11 0.003948  10.0.0.3  10.0.0.2    DNS      166 Standard query response 0x0001 A 10-0-0-0.dns64perf.test A 10.0.0.0 NS localhost A 127.0.0.1 AAAA ::1
  12 0.004142  fd00::2   fd00::1     DNS      198 Standard query response 0x0001 AAAA 10-0-0-0.dns64perf.test AAAA 2001:db8::a00:0 NS localhost A 127.0.0.1 AAAA …
```

Fig. 12. Wireshark capture taken during the birthday attack vulnerability test of mtd64-ng with 1 working thread.



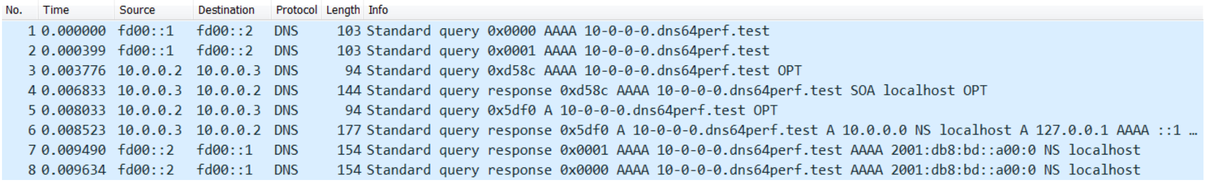
```
No.  Time      Source    Destination Protocol Length Info
   1 0.000000  fd00::1   fd00::2     DNS      103 Standard query 0x0000 AAAA 10-0-0-0.dns64perf.test
   2 0.000136  fd00::1   fd00::2     DNS      103 Standard query 0x0001 AAAA 10-0-0-0.dns64perf.test
   3 0.000658  10.0.0.2  10.0.0.3    DNS       83 Standard query 0x0000 AAAA 10-0-0-0.dns64perf.test
   4 0.000818  10.0.0.2  10.0.0.3    DNS       83 Standard query 0x0001 AAAA 10-0-0-0.dns64perf.test
   5 0.001763  10.0.0.3  10.0.0.2    DNS      133 Standard query response 0x0000 AAAA 10-0-0-0.dns64perf.test SOA localhost
   6 0.001911  10.0.0.3  10.0.0.2    DNS      133 Standard query response 0x0001 AAAA 10-0-0-0.dns64perf.test SOA localhost
   7 0.001918  10.0.0.2  10.0.0.3    DNS       83 Standard query 0x0000 A 10-0-0-0.dns64perf.test
   8 0.002025  10.0.0.2  10.0.0.3    DNS       83 Standard query 0x0001 A 10-0-0-0.dns64perf.test
   9 0.002171  10.0.0.3  10.0.0.2    DNS      166 Standard query response 0x0000 A 10-0-0-0.dns64perf.test A 10.0.0.0 NS localhost A 127.0.0.1 AAAA ::1
  10 0.002327  10.0.0.3  10.0.0.2    DNS      166 Standard query response 0x0001 A 10-0-0-0.dns64perf.test A 10.0.0.0 NS localhost A 127.0.0.1 AAAA ::1
  11 0.002544  fd00::2   fd00::1     DNS      198 Standard query response 0x0000 AAAA 10-0-0-0.dns64perf.test AAAA 2001:db8::a00:0 NS localhost A 127.0.0.1 AAAA …
  12 0.002656  fd00::2   fd00::1     DNS      198 Standard query response 0x0001 AAAA 10-0-0-0.dns64perf.test AAAA 2001:db8::a00:0 NS localhost A 127.0.0.1 AAAA …
```

Fig. 13. Wireshark capture taken during the birthday attack vulnerability test of mtd64-ng with 2 working threads.



```
No.  Time      Source    Destination Protocol Length Info
   1 0.000000  fd00::1   fd00::2     DNS      103 Standard query 0x0000 AAAA 10-0-0-0.dns64perf.test
   2 0.000249  fd00::1   fd00::2     DNS      103 Standard query 0x0001 AAAA 10-0-0-0.dns64perf.test
   3 0.001755  10.0.0.2  10.0.0.3    DNS       83 Standard query 0xf6cf AAAA 10-0-0-0.dns64perf.test
   4 0.004063  10.0.0.3  10.0.0.2    DNS      133 Standard query response 0xf6cf AAAA 10-0-0-0.dns64perf.test SOA localhost
   5 0.004902  10.0.0.2  10.0.0.3    DNS       83 Standard query 0xdf6c A 10-0-0-0.dns64perf.test
   6 0.005326  10.0.0.3  10.0.0.2    DNS      166 Standard query response 0xdf6c A 10-0-0-0.dns64perf.test A 10.0.0.0 NS localhost A 127.0.0.1 AAAA ::1
   7 0.006448  fd00::2   fd00::1     DNS      131 Standard query response 0x0000 AAAA 10-0-0-0.dns64perf.test AAAA 2001:db8::a00:0
   8 0.006803  fd00::2   fd00::1     DNS      131 Standard query response 0x0001 AAAA 10-0-0-0.dns64perf.test AAAA 2001:db8::a00:0
```

Fig. 14. Wireshark capture taken during the birthday attack vulnerability test of PowerDNS.



```
No.  Time      Source    Destination Protocol Length Info
   1 0.000000  fd00::1   fd00::2     DNS      103 Standard query 0x0000 AAAA 10-0-0-0.dns64perf.test
   2 0.000399  fd00::1   fd00::2     DNS      103 Standard query 0x0001 AAAA 10-0-0-0.dns64perf.test
   3 0.003776  10.0.0.2  10.0.0.3    DNS       94 Standard query 0xd58c AAAA 10-0-0-0.dns64perf.test OPT
   4 0.006833  10.0.0.3  10.0.0.2    DNS      144 Standard query response 0xd58c AAAA 10-0-0-0.dns64perf.test SOA localhost OPT
   5 0.008033  10.0.0.2  10.0.0.3    DNS       94 Standard query 0x5df0 A 10-0-0-0.dns64perf.test OPT
   6 0.008523  10.0.0.3  10.0.0.2    DNS      177 Standard query response 0x5df0 A 10-0-0-0.dns64perf.test A 10.0.0.0 NS localhost A 127.0.0.1 AAAA ::1 …
   7 0.009490  fd00::2   fd00::1     DNS      154 Standard query response 0x0001 AAAA 10-0-0-0.dns64perf.test AAAA 2001:db8:bd::a00:0 NS localhost
   8 0.009634  fd00::2   fd00::1     DNS      154 Standard query response 0x0000 AAAA 10-0-0-0.dns64perf.test AAAA 2001:db8:bd::a00:0 NS localhost
```

Fig. 15. Wireshark capture taken during the birthday attack vulnerability test of Unbound.

later, because including caching is among the midterm development plans of mtd64-ng.

The results of PowerDNS and Unbound are shown in Fig. 14 and Fig. 15, respectively. None of them send out multiple equivalent queries, thus they are not vulnerable to birthday attacks.

## IX. SUMMARY, RECOMMENDATIONS AND DISCUSSION

We have summarized the results of the three kind of measurements in Table 3. As for BIND, PowerDNS, and Unbound, we have not found any vulnerabilities that could lead to cache poisoning. Although TOTD and mtd64-ng have several vulnerabilities that could lead to cache poisoning, they do not implement caching, thus cache poisoning is not possible in their cases.

As the implementation of caching is included in the midterm development plans of mtd64-ng, the protection against all three vulnerabilities must also be included. We recommend the usage of cryptographically secure random number generators [40] for generating Transaction IDs and source port numbers. The elimination of the vulnerability to birthday attacks seems to be a more difficult problem, as now the performance of mtd64-ng benefits from the solution that the requests from the clients are not stored in a central database, but they are distributed to the working threads. However, it will be necessary to centrally keep track of the queries sent by mtd64-ng to the authoritative DNS servers and are currently awaiting for an answer, in order to eliminate the possibility of sending out multiple equivalent queries concurrently.

We note that all the examined DNS64 implementations are free software [25] (also called open source [26]), thus their source code may also be studied, as we did it in the case of TOTD [30]. The significance of our testing method is that it may also be used for closed source software, or in the cases when the subject of the study also includes the interaction with the random number generator of the operating system.

The very same framework could be used for the analysis of NAT64 gateways.

Table 3. Summary of the Vulnerability Test Results

| DNS64 Implementation | Attack Type | | | |
|---|---|---|---|---|
| | Transaction ID Prediction | Source Port Number Prediction | Multiple Equivalent Queries | DNS Cache Poisoning |
| BIND 9.9.5 | no problem found | no problem found | protected | no problem found |
| TOTD 1.5.2 | vulnerable | vulnerable | vulnerable | not applicable |
| TOTD 1.5.3 | protected | vulnerable | vulnerable | not applicable |
| mtd64-ng 1.1.0 | vulnerable | vulnerable | vulnerable | not applicable |
| PowerDNS 3.6.2 | no problem found | no problem found | protected | no problem found |
| Unbound 1.6.0 | no problem found | no problem found | protected | no problem found |

## X. CONCLUSION

We have shown that DNS cache poisoning may be a crucial vulnerability of DNS64 servers and we have given an introduction to the three main components of DNS cache poisoning vulnerability, namely Transaction ID prediction, source port number prediction, and a birthday paradox based attack, which is possible if a DNS or DNS64 server sends out multiple equivalent queries concurrently.

After surveying the available test tools for DNS cache poisoning vulnerability analysis and pointing out that they are not suitable for our purposes, we have designed a methodology and implemented it in a testbed, which can be used for the systematic testing of DNS or DNS64 implementations, whether they are susceptible to the above mentioned three vulnerabilities.

We have selected BIND, PowerDNS, Unbound two versions of TOTD, and mtd64-ng for testing and also presented their setup. We have carried out their testing concerning the three possible components of the DNS cache poisoning vulnerability. We have pointed out several vulnerabilities in TOTD and mtd64-ng. As they do not currently support caching, thus, cache poisoning is not possible in their cases. As the implementation of caching is included in the midterm development plans of mtd64-ng, we have also given recommendations for the elimination of its uncovered vulnerabilities.

As for BIND, PowerDNS, and Unbound, we have not found any vulnerabilities that could lead to cache poisoning.

## REFERENCES

[1] E. Nordmark, R. Gilligan, "Basic transition mechanisms for IPv6 hosts and routers", IETF RFC 4213, October 2005. DOI: 10.17487/rfc4213

[2] G. Lencse, Y. Kadobayashi, "Survey of IPv6 transition technologies for security analysis", IEICE Technical Committee on Internet Architecture (IA) Workshop, Tokyo Japan, Aug. 28, 2017, *IEICE Tech. Rep.* vol. 117, no. 187, pp. 19–24.

[3] M. Georgescu, H. Hazeyama, T. Okuda, Y. Kadobayashi, and S. Yamaguchi, "The STRIDE towards IPv6: A comprehensive threat model for IPv6 transition technologies", *Proc. 2nd International Conference on Information Systems Security and Privacy*, Rome, Feb. 2016. DOI: 10.13140/RG.2.1.2781.6085

[4] M. Bagnulo, A Sullivan, P. Matthews and I. Beijnum, "DNS64: DNS extensions for network address translation from IPv6 clients to IPv4 servers", RFC 6147, Apr. 2011. DOI: 10.17487/rfc6147

[5] 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. DOI: 10.17487/rfc6146

[6] G. Lencse, Y. Kadobayashi, "Methodology for the identification of potential security issues of different IPv6 transition technologies: Threat analysis of DNS64 and stateful NAT64", *Computers & Security*, vol. 77, no. 1, pp. 397-411, August 1, 2018, DOI: 10.1016/j.cose.2018.04.012

[7] S. Son and V. Shmatikov, "The hitchhiker's guide to DNS cache poisoning", in *Proc. Security and Privacy in Communication Networks - 6th International ICST Conference (SecureComm 2010)*, Singapore, Sep. 7–9, 2010, pp. 466–483, DOI: 10.1007/978-3-642-16161-2_27

[8] G. Lencse and Y. Kadobayashi, "Testbed for security analysis of the DNS64 IPv6 transition technology in virtual environment", IEICE Communications Society Internet Architecture Workshop, Tokyo, Japan, Oct. 13, 2017, *IEICE Tech. Rep.*, vol. 117, no. 239, pp. 19-24.

[9] G. Lencse and Y. Kadobayashi, "Benchmarking DNS64 Implementations: Theory and Practice", *Computer Communications*, vol. 127, no. 1, pp. 61-74, September 1, 2018, DOI: 10.1016/j.comcom.2018.05.005

[10] R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, "DNS Security Introduction and Requirements", IETF RFC 4033, Mar. 2005. DOI: 10.17487/rfc4033

[11] J. Linkova, "Let's talk about IPv6 DNS64 & DNSSEC", APNIC Blog, 2016, https://blog.apnic.net/2016/06/09/lets-talk-ipv6-dns64-dnssec/

[12] C. Bao, C. Huitema, M. Bagnulo, M Boucadair and X. Li, "IPv6 addressing of IPv4/IPv6 translators", IETF RFC 6052, Oct. 2010. DOI: 10.17487/rfc6052

[13] A. Hubert, R. van Mook, "Measures for making DNS more resilient against forged answers", IETF RFC 5452, Jan. 2009. DOI: 10.17487/rfc5452

[14] M. Larsen, F. Gont, "Recommendations for transport-protocol port randomization", IETF RFC 6056, Jan. 2011. DOI: 10.17487/rfc6056

[15] CERT, "Various DNS service implementations generate multiple simultaneous queries for the same resource record", Vulnerability Note VU#457875, [Online]. Available: https://www.kb.cert.org/vuls/id/457875

[16] D. J. Bernstein, "DNS forgery", [Online]. Available: http://cr.yp.to/djbdns/forgery.html

[17] CERT, "Multiple DNS implementations vulnerable to cache poisoning", Vulnerability Note VU#800113 [Online]. Available: http://www.kb.cert.org/vuls/id/800113

[18] S. Friendl, "An Illustrated Guide to the Kaminsky DNS Vulnerability", *Unixwiz.net*, [Online]. Available: http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

[19] DNS-OARC, “Test my DNS”, web based Transaction ID and source port randomness tester, [Online]. Available: https://www.dns-oarc.net/oarc/services/dnsentropy

[20] InfosecEvents, “More DNS cache poisoning testing tools”, [Online]. Available: http://infosecevents.net/2008/07/24/more-dns-cache-poisoning-testing-tools/

[21] Kim, Davies, “DNS cache poisoning vulnerability: Explanation and remedies”, ICANN presentation, Viareggio, Italy, Oct. 2008, [Online]. Available: https://www.iana.org/about/presentations/davies-viareggio-entropyvuln-081002.pdf

[22] G. Lencse, S. Répás, “Benchmarking further single board computers for building a mini supercomputer for simulation of telecommunication systems”, *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, vol. 5. no. 1, 2016, pp. 29–36, DOI: 10.11601/ijates.v5i1.138

[23] D. Bakai, “Debian-VM”, [Online]. Available: https://git.sch.bme.hu/bakaid/debian-vm

[24] Internet Systems Consortium, “BIND: Versatile, Classic, Complete Name Server Software”, [Online]. Available: https://www.isc.org/downloads/bind

[25] Free Software Foundation, “The free software definition”, [Online]. Available: http://www.gnu.org/philosophy/free-sw.en.html

[26] Open Source Initiative, “The open source definition”, [Online]. Available: http://opensource.org/docs/osd

[27] Cisco, “End user license agreement”, [Online]. Available: http://www.cisco.com/c/en/us/products/end-user-license-agreement.html

[28] Juniper Networks, “End user license agreement”, [Online]. Available: http://www.juniper.net/support/eula/

[29] The 6NET Consortium, Ed. M. Dunmore, “An IPv6 Deployment Guide”, Sep. 2005. [Online]. Available: http://www.6net.org/book/deployment-guide.pdf

[30] G. Lencse and S. Répás, “Improving the performance and security of the TOTD DNS64 implementation”, *Journal of Computer Science and Technology* (*JCS&T*, Argentina), vol. 14, no. 1, Apr. 2014, ISSN: 1666-6038, pp. 9–15. http://journal.info.unlp.edu.ar/journal/

[31] G. Lencse and D. Bakai, “Design, implementation and performance estimation of mtd64-ng a new tiny DNS64 proxy”, *Journal of Computing and Information Technology*, vol. 25, no. 2, Jun. 2017, pp. 91–102, DOI:10.20532/cit.2017.1003419

[32] Powerdns.com BV, “PowerDNS”, [Online]. Available: http://www.powerdns.com

[33] NLnet Labs, “Unbound”, [Online]. Available: http://unbound.net

[34] G. Lencse, “Test program for the performance analysis of DNS64 servers”, *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, vol. 4, no. 3, 2015, pp 60–65. DOI: 10.11601/ijates.v4i3.121

[35] G. Lencse, “dns64perf source code”, http://ipv6.tilb.sze.hu/dns64perf/

[36] R. Jain, “Testing random number generators”, Washington University, Saint Louis, lecture notes, 2008, [Online]. Available: https://www.cse.wustl.edu/~jain/cse567-08/ftp/k_27trg.pdf

[37] I. Petrila, V. Manta, F. Ungureanu, “Uniformity and correlation test parameters for random numbers generators”, *Proc. 2014 18th International Conference on System Theory, Control and Computing (ICSTCC)*, Sinaia, Romania, Oct. 17–19, 2014, DOI: 10.1109/ICSTCC.2014.6982421

[38] D. Bakai, “mtd64-ng: A lightweight multithreaded C++11 DNS64 server”, [Online]. Available: https://github.com/bakaid/mtd64-ng/

[39] G. Lencse, “birthday-test source code”, http://ipv6.tilb.sze.hu/DNS-birthday-test/

[40] M. Welschenbach, “Large Random Numbers”, In: *Cryptography in C and C++*, 2nd Ed, Apress, Berkeley, CA, 2013. DOI: 10.1007/978-1-4302-5099-9_12

**Gábor Lencse** received his MSc and PhD in computer science from the Budapest University of Technology and Economics, Budapest, Hungary in 1994 and 2001, respectively.

He has been working full time for the Department of Telecommunications, Széchenyi István University, Győr, Hungary since 1997. Now, he is an Associate Professor. He has been working part time for the Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, Hungary as a Senior Research Fellow since 2005. At the time of writing this paper he was a Guest Researcher at the Laboratory for Cyber Resilience, Nara Institute of Science and Technology, Japan, where his research area was the security analysis of IPv6 transition technologies.

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

**Youki Kadobayashi** received his Ph.D. degree in computer science from Osaka University, Japan, in 1997. He is currently a Professor in the Graduate School of Information Science, Nara Institute of Science and Technology, Japan. Since 2013, he has also been working as the Rapporteur of ITU-T Q.4/17 for cybersecurity standardization. His research interests include cybersecurity, web security, and distributed systems.

Dr. Kadobayashi is a member of IEEE Communications society.

# Demonstration of Multimode Optical Fiber Communication System using 1300 nm Directly Modulated VCSEL for Gigabit Ethernet

[1]Tomáš Huszaník, [2]Ján Turán, and [3]Ľuboš Ovseník

***Abstract*— In the recent years, the optical networks have grown to unexpected dimensions. The growth of active users and growing demand for data services set high requirements to network providers. Driving forces of this growth are multimedia, cloud computing and web services which set high bandwidth demand. The majority of currently deployed optical networks utilize passive or active network structure using dominantly singlemode optical fiber (SMF). SMF is believed to be the better choice over multimode optical fiber (MMF) for high speed optical fiber communication systems. And in some applications it definitely is. MMF has found use especially for short distance communication as it easily supports distances required for interconnecting buildings, data centres or campuses. Considering MMFs lower cost over SMF it became an interesting alternative for Ethernet connection in buildings or campuses. In this paper we present a simulation model of 1000BASE-LX Ethernet with MMF using different optical modulation techniques. The aim of this article is to demonstrate possibilities of MMF based 1000BASE-LX Ethernet with directly modulated vertical-cavity surface-emitting laser (VCSEL).**

***Keywords*—Bit error rate, Ethernet, multimode optical fiber, optical modulation, singlemode optical fiber, VCSEL**

## I. Introduction

The first generation of optical networking started in the late 1970s. The first generation lightwave operated systems used GaAs semiconductor lasers and operated at 0.8 μm wavelength. The first optical fiber systems used multimode fibers with core diameters of about 50 to 85 μm. A bit rate was not exceptionally high to these days - 45 Mbps and maximum distance was up to 10 km. The second generation came on scene in the early 1980s. The bit rate of these early systems was limited to 100 Mbps mainly because of fiber dispersion in multimode fibers (MMF). This limitation was quickly overcome by the use of singlemode optical fibers (SMF). Fiber dispersion is a very important design issue of optical fiber communication systems. Fiber dispersion leads to broadening of individual light pulses with propagation which cause inter-symbol interference (ISI). With the interfered signal, it becomes impossible to recover signal accurately [1][2]. This problem is more obvious in the case of MMF, since different fiber modes spread different ways and different speeds. For this reason, majority of currently deployed optical systems use SMF. Despite historical development, the use of MMF over SMF can be still beneficial, especially for short distance transmissions. The most promising application of MMF is high-speed ethernet network, local and storage area networks [3]. As we prove in our experimental setup, MMF based Ethernet reaches today's requirements for BER and OSNR (optical signal-to-noise ratio) and in some cases, goes even further [4][5][6]. The conclusions discussed in this work are based on the facts published in the following publications [7][8][9].

The section 2 provides a closer look at differences between MMF and SMF, detailed look at MMFs limitation factors and applications. In this article, we also present the practical application of MMF for the Ethernet connection. To show the performance of MMF based 1000BASE-LX Ethernet, we designed a simulation model using OptSim software. OptSim software is a professional program suite for advanced simulation of optical fiber systems. Thanks to the extension ModeSYS, we are able to fully evaluate multimode optical communication systems.

## II. Description of multimode optical fiber communication

There are three basic types of optical fibers as shown in Fig.1: multimode fiber with step index, multimode fiber with graded index and singlemode fiber with step index.

Singlemode optical fiber allows only single light wave, also called lowest-order mode to propagate. The core diameter of singlemode optical fiber is 5-10 μm, the typical diameter of cladding is 125 μm. SMF is required for high data rate applications with low signal loss. The major advantage of SMF over MMF is that it does not suffer from modal dispersion that is the main limitation factor of MMF. However, there is still chromatic dispersion that limits the performance of SMF [6].

Affiliation: Department of Electronics and Multimedia Telecommunications, Technical University of Košice, Faculty of Electrical Engineering and Informatics, Košice, Slovakia. (corresponding author, e-mail: tomas.huszanik@tuke.sk)

DOI: 10.36244/ICJ.2018.2.4

The term multimode refers to the multiple modes or paths that are possible to transmit through the fiber. The typical core diameter of a multimode fiber used for telecommunication purposes is 50/62.5/125 µm. There are two principle types of multimode fiber – step index and graded index [6].

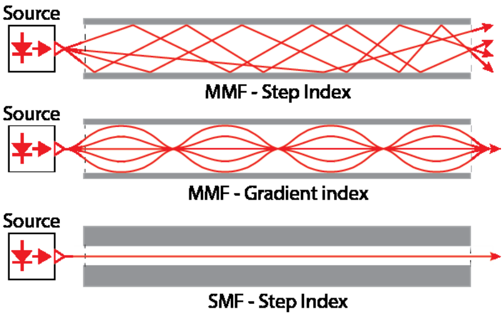


Fig. 1 Three types of optical fiber

The index of refraction profile of step index multimode fiber steps from low to high to low (from cladding to core to cladding). This type of fiber has large core diameter and numerical aperture. Step index multimode fiber is used for high bandwidth applications (over 1 GHz) supporting maximum 3 km transmission distance [10][11]. The number of modes propagating in a multimode step index fiber can be expressed as:

$$M_n = V^2/2 \qquad (1)$$

In this equation, *V* represents normalized frequency and it strongly relates to the size of fiber, refractive index and wavelength. Normalized frequency can be expressed in two ways:

$$V = [2\pi a/\lambda] \times NA, \qquad (2)$$

$$V = [2\pi a/\lambda] \times n_1 \times (2\Delta)^{1/2}, \qquad (3)$$

where *a* is the fiber core radius, *λ* is operating wavelength, *NA* is numerical aperture, $n_1$ is the refractive index of a core and finally, *Δ* is the relative refractive index difference between the core and cladding of an optical fiber [2][6][10]. The relationship between the angle of incoming light wave *θi* and the refracted wave *θr* inside step index MMF is:

$$n_0 sin\theta_i = n_1\theta_r \qquad (4)$$

Refraction is possible only for an angle *ϕ* meeting the following condition:

$$sin\phi < n_2/n_1, \qquad (5)$$

where $n_2$ is the refractive index of cladding and $n_1$ is the refractive index of core. Then the propagation of light wave inside the step index MMF is in Fig. 2 [10].

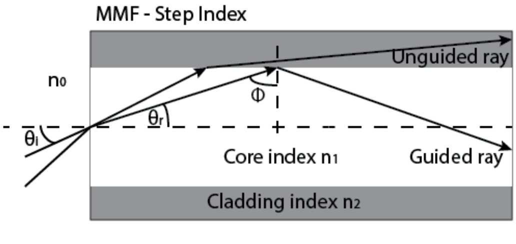


Fig. 2 Propagation of a light wave in step index MMF

Refractive index of the core of the graded index MMF decreases gradually from its maximum $n_1$ value at the core to its minimum value $n_2$ at the fibers cladding. This results into following light propagation – light wave travels faster at the edge of the core and slower in the center of the core. Individual modes travel in sinusoidal paths with equal travel time [6][9]. In comparison to step index MMF, the already mentioned travel pattern of light modes in graded index MMF significantly reduces modal dispersion. The light wave propagation in graded indexed MMF is illustrated in Fig. 3 [2][12].

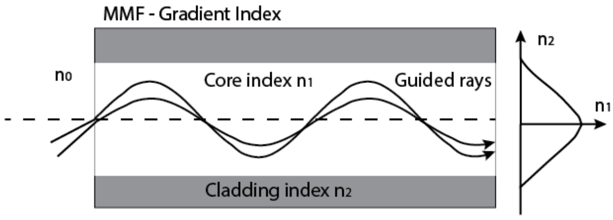


Fig. 3 Propagation of a light wave in graded index MMF

The major limitation in multimode fiber optic communication system is intersymbol interference (ISI) due to modal dispersion. This phenomenon is reduced in graded index MMFs, but it is still present. Modal dispersion can be eliminated using light sources that excite only the desired light modes which can be achieved by using spatial light modulators [12]. There are two main approaches when avoiding the signal degradation caused by modal dispersion. The first one is a mode filtering method. This method reduces higher order mode in the receiver. The second approach is a center-launching method which launches light directly into the center of the core of MMF which prevents the higher order mode occurrence.

Because of dispersion limitation, multimode fibers could be used especially for short links, for example in Ethernet networks. Later in this paper we present a simulation model of such a network. 1000BASE-LX is a fiber optic Gigabit Ethernet standard specified in IEEE 802.3 Clause 38. It has been developed for implementing Gigabit ethernet networks. Specification of optical interface for 1000BASE-LX is shown in Table 1 [13].

## III. EXPERIMENTAL MODEL OF 1000BASE-LX ETHERNET

For the purpose of evaluating performance of 1000BASE-LX Ethernet with MMF we used OptSim software and extention module ModeSYS. When building this model, we respected IEEE 802.3 Clause 38 which specifies 1000BASE-

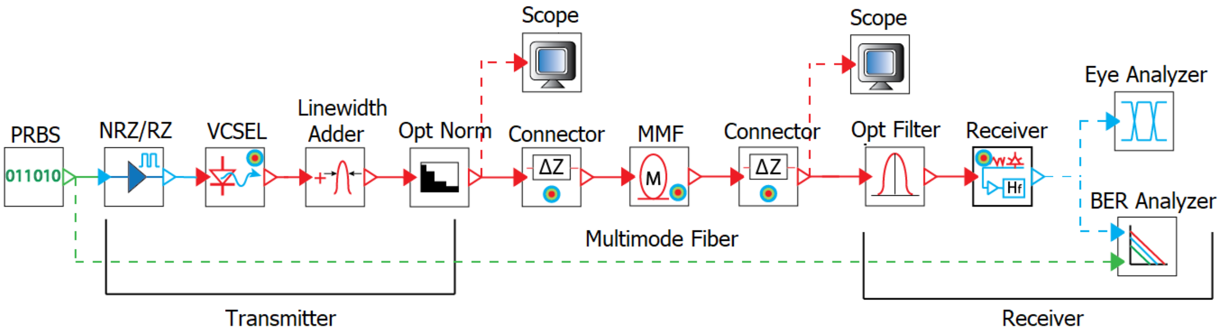


Fig. 4 Block scheme of 1000BASE-LX Ethernet simulation model

LX standard. Block scheme of designed 1000BASE-LX Ethernet network with MMF and the vertical-cavity surface-emitting laser (VCSEL) is shown in Fig. 4. Detailed description of simulation scheme is in the following subsections.

TABLE I. Specifications of 1000BASE-LX Ethernet

| Parameter | Value |
|---|---|
| Bitrate | 1/1.25 Gbps |
| Optical interface | MMF and SMF |
| Fiber diameter | 50/62.5/125 µm (MMF), 9/10 µm (SMF) |
| Transmission distance | 550 m for 62.5/125 and 50/125 for MMF cable<br>10 km for 9/125 SMF cable |
| Operating wavelength | 1270 – 1355 nm |
| Launch power | -11.5 to -3 dBm |
| Receive power | -19 to -3 dBm |
| Receiver saturation | -3 dBm |
| Receiver sensitivity | -19 dBm |

## A. *Transmitter section*

Transmitter of proposed multimode fiber based 1000BASE-LX Ethernet consists of pseudorandom binary sequence (PRBS) generator which is difficult to predict and exhibit statistical behaviour. Transmission rate is 1.25 Gbps. Data are then modulated using electrical modulator driver – NRZ or RZ, depending on simulation setup. NRZ/RZ signal is then modulated to an optical carrier using VCSEL. A vertical-cavity surface-emitting laser (VCSEL) is a high efficiency semiconductor- based laser optimized for use with multimode fibers. VCSEL emits beam verticaly from its top surface. High speed fiber links based on multimode fiber use VCSELs and GaAs photodetectors. Development of these components is extremely important for future multimode fiber systems development [8]. Central wavelength of VCSEL in our scheme is 1300 nm. Excitation ratio is 9 dB, linewidth is 4nm and launch power is -11.5 dB. Transverse mode of VCSEL used in our simulation model is shown in Fig. 5.

Next in the chain is optical linewidth adder and optical power normalizer. To simulate insertion loss between optical transmitter and optical fiber we used connector components with insertion loss 0.75 dB.

## B. *Transmission section*

To eliminate modal dispersion, we opted for gradient index multimode fiber. Multimode fiber used in our simulation is 550 m long, which is the maximum excepted length, with diameter of 50 µm and attenuation of 1.5 dB/km. Fiber bandwidth is 500 MHz. Peak refractive index is 1.475 and index step is 1%. Dispersion slope is 0.11 ps/km nm$^2$. Plot of refractive index of MMF is illustrated on Fig. 6.

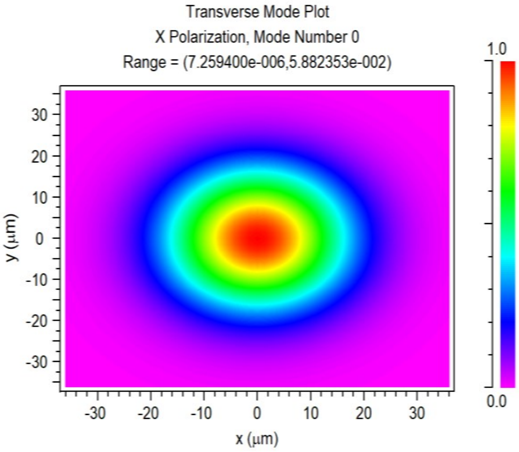


Fig. 5 Transverse mode of VCSEL

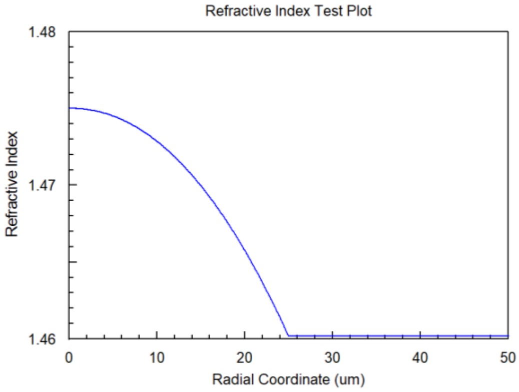


Fig. 6 Refractive index of MMF

### *C. Receiver section*

Receiver section is formed with optical low pass Bessel filter and APD (avalanche photodiode) detector with 0.8 quantum efficiency. This compound component also contains optical preamplifier and electrical Bessel filter. Receiver sensitivity is set to -19 dBm and electrical filter bandwidth is 1.5 GHz. Optical scopes are used to analyze optical spectrums. Eye analyzer is used to observe eye diagram display. BER analyzer calculates BER and Q factor performance.

## IV. RESULTS AND DISCUSSION

To evaluate performance of 1000BASE-LX Ethernet we established two experimental setups. First experimental setup uses NRZ encoding method and VCSEL optical direct modulation. NRZ encoding scheme is defined as follows – higher signal value is represented by logic 1 and the lower value is always logic 0 and the duration of the bit interval does not change. The change occurs by changing the value of the following information bit. The second experimental setup uses RZ encoding scheme with VCSEL optical direct modulation. With RZ encoding scheme, duration of information bit is reduced to half. RZ encoding scheme requires double bandwidth compared to NRZ which is the reason why are RZ pulses are broadened more by fiber dispersion.

To fully evaluate system performance, we scanned various parameters of proposed simulation model that are key to the system performance. Input optical spectrums for NRZ and RZ encoding scheme are shown in Fig.7 and Fig. 8.

Performance of the system was evaluated using BER and Q factor measurement. These measurements were obtained by analyzing eye diagram display. Eye diagram is used to observe the quality of received signal in digital domain. We can extract a lot of parameters just by analyzing the display. The most obvious one is eye opening - the most open part means the best OSNR (optical signal-to-noise ratio). Q factor, function of OSNR, is another parameter that can be extracted. Q factor provides a qualitative description of receiver performance.

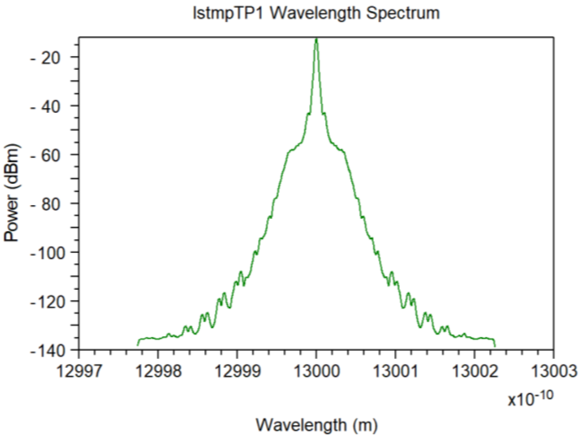


Fig. 7 Input optical spectrum for NRZ

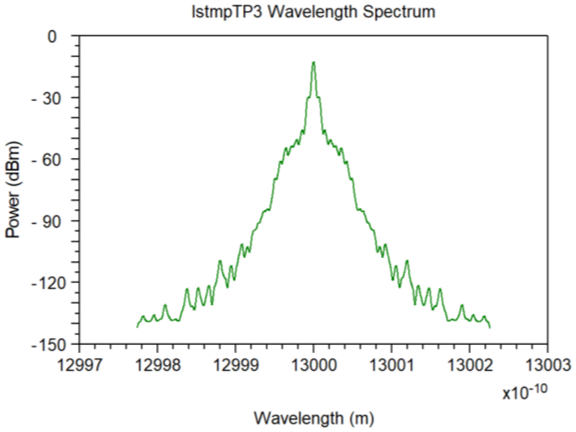


Fig. 8 Input optical spectrum for RZ

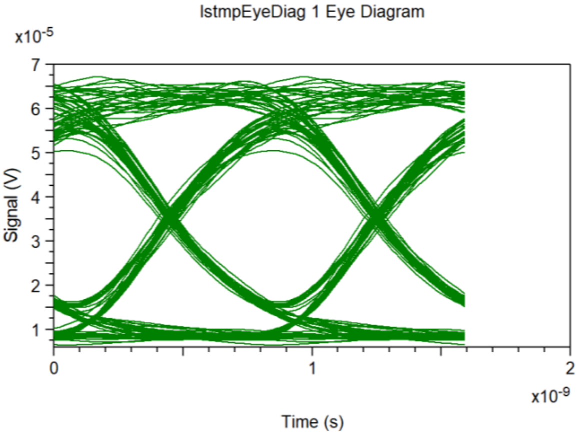


Fig. 9 Eye diagram for NRZ and 550 m MMF

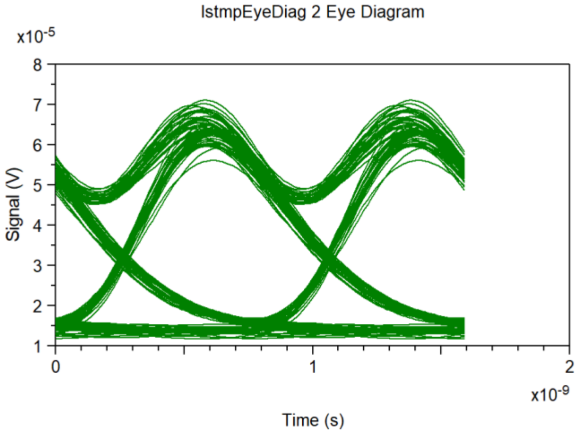


Fig. 10 Eye diagram for RZ and 550 m MMF

First experimental run was performed for 550 m MMF with 1.5 dB/km attenuation while launch power was -11.5 dB and operating wavelength 1300 nm. From the obtained eye diagrams shown in Fig. 9 and Fig. 10 one can say, that system performance in these conditions are exceptionally good. Values of BER and Q factor are provided in Table 2.

TABLE II. BER and Q factor results

| Parameter | NRZ - Value | RZ – Value |
|---|---|---|
| Measured BER | 8.5438e-012 | 1.01e-027 |
| Measured Q factor | 16.56 dB | 20.71 dB |
| System margin | -0.39 | 3.76 |
| Required BER | 1e-012 | |
| Required Q factor | 16.94 dB | |

System performance of 1000BASE-LX Ethernet is examined for different lengths of optical fiber, fiber loss, launch powers and bitrate. The values of BER has been recalculated for different operating points. The aim of this experimental setup is to find out limitations of multimode fiber and to determine which one of two encoding schemes remains the best performance. BER values of NRZ based 1000BASE-LX Ethernet depending on fiber length, fiber loss, transmitter power and bitrate are shown in the following figures (Fig.11 – Fig. 14).

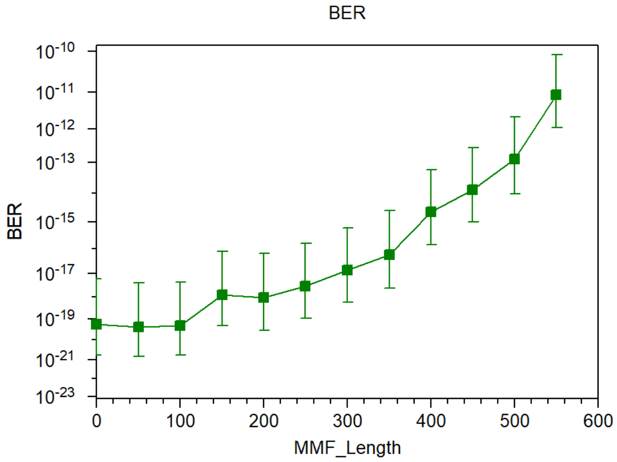


Fig. 11 NRZ - BER vs MMF length

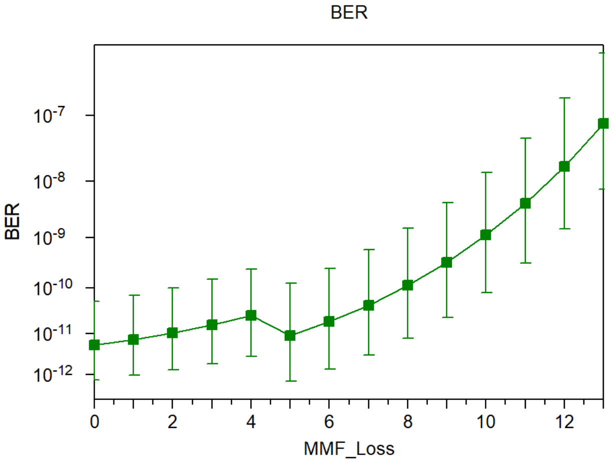


Fig. 12 NRZ - BER vs MMF loss

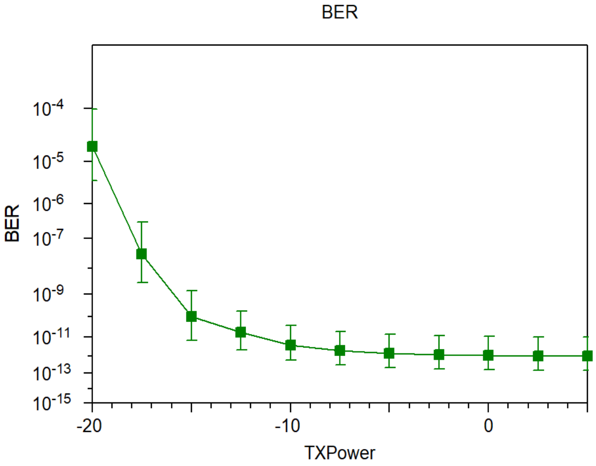


Fig. 13 NRZ - BER vs transmitter power

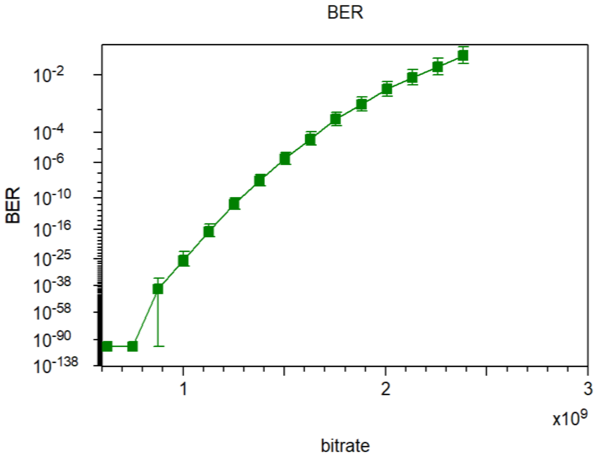


Fig. 14 NRZ - BER vs bitrate

The performance of proposed system decreases as the length of fiber increases. Fiber length varies from 0.1 m to 550 m with 50 m step. Maximum BER value is 5.7182e-020, Q factor is 19.156 dB.

When increasing fiber loss, from 0 to 13 dB/km, the BER gradually decreases. In this case length of MMF was 550m and did not changed during the simulation process. BER reaches 5.3567e-012 for 0 dB/km loss and maximum value is 7.6645e-008 for 13 dB/km. In this case system margin increases gradually. BER is inverse proportional to transmitter power. It means that the probability of error decreases as the power increases as seen in Fig. 13. Tested power ranges from -20 dBm to 5 dBm. In the last experiment in this section we tested how different bitrates affect BER performance. The premise is that probability of error increases proportionally to bitrate. Bitrate varied form 0.6255 Gbps to 2.3825 Gbps. BER value for 1.1275 Gbps is 4.0233e-017 and 1.1700e-011 for 1.2530 Gbps. For 1.3785 Gbps transmission rate probability of error is 1.7713e-008 which does not fit in to the requirements for high speed optical networks. As the bit rate increases, BER increases as well.

The last experimental setup facilitates 1000BASE-LX Ethernet with RZ encoding scheme. BER values of RZ based 1000BASE-LX Ethernet depending on fiber length, fiber loss, transmitter power and bitrate are shown in Fig.15 – Fig. 18.

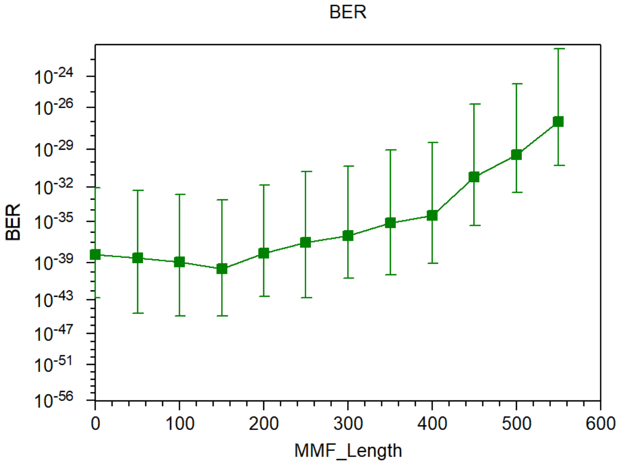


Fig. 15 RZ - BER vs MMF length

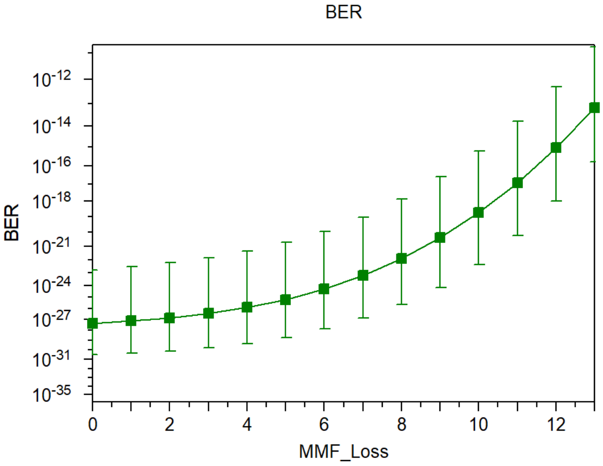


Fig. 16 RZ - BER vs MMF loss

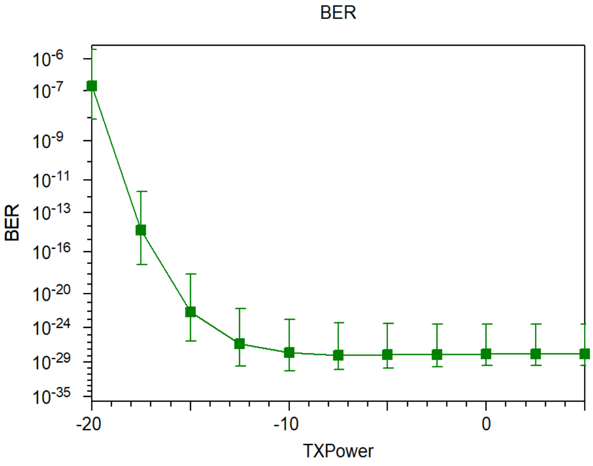


Fig. 17 RZ - BER vs transmitter power

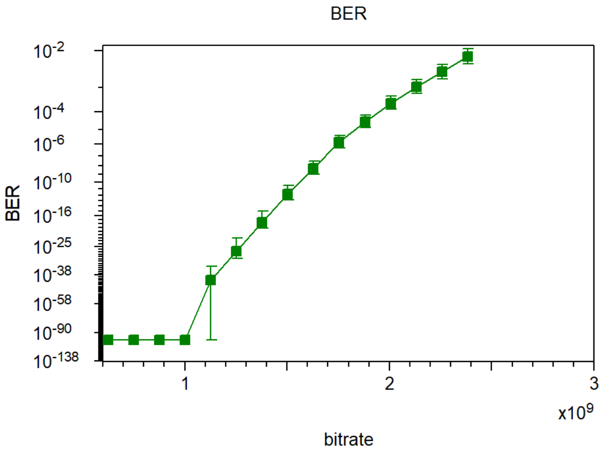


Fig. 18 RZ - BER vs bitrate

Performance of 1000BASE-LX Ethernet has significantly improved just by implementation of RZ encoding scheme. This phenomenon can be seen in Fig. 15. RZ based 1000BASE-LX Ethernet system reaches much lower BER values than NRZ based one.

As in the previous case, BER is proportional to the length of multimode fiber. Minimal value of BER is 1.01e-027 for 550 meters of fiber and maximal value is 6.32e-039 for 0.1 meters of fiber. Probability of error is proportional to the fiber loss as well. BER increases almost exponentialy to the fiber loss. In this case fiber length was 550 meters. All BER values obtained in this experimental setup are acceptable for real-life applications. When increasing transmitter power BER decreases. Transmitter power varied form -20 to 5 dBm. Finally, the growth of BER depending on increasing bitrate is very similar to the one for NRZ encoding scheme. Bitrate varied form 0.6255 Gbps to 2.3825 Gbps. Maximum reachable bitrate, excepting BER requirements, is 1.504 Gbps which gives 1.4221e-012.

Please notice that OptSim works in ideal conditions. Optsim software is used to design optical networks and to verify attributes of real optical systems. Simulation results may vary from the real equivalent optical systems [14].

## V. Conclusion

In this paper, we examined the application of multimode optical fibers for 1000BASE-LX Ethernet with direct optical modulation using VCSEL. Experimental results proof superior performance of multimode optical system on short distances. Obtained results show that we can ensure requirements for BER and Q factor for today's optical communication systems by carefull choice of fiber lenght, transmitter power, bitrate or fiber loss. As a result of simulation, we can say that RZ encoding scheme improves the transmission quality of multimode optical system.

## Acknowledgment

This work was supported by following research grants: KEGA 023TUKE-4/2017 and VEGA 1/0772/17.

## References

[1] R. Ramaswami, K. N. Sivarajan, and G. H. Sasaki, Optical Networks. 2010.

[2] G. P. Agrawal, Fiber-Optic Communications Systems, Third Edition., vol. 6. 2002.

[3] R. E. Freund, C. Caspar, C. A. Bunge, N. N. Ledentsov, and D. Molin, "High-Speed Transmission in Multimode Fibers," J. Light. Technol., vol. 28, no. 4, pp. 569–586, 2010.

[4] J. Ružbarský, J. Turán, and Ľ. Ovseník, "Different Types of Coding Input Data In Optical Transmission Systems," Carpathian J. Electron. Comput. Eng., vol. 2, pp. 3–6, 2016.

[5] T. Huszaník, Ľ. Ovseník, and J. Turán, "Performance Analysis of Optical Modulation Formats for 10 Gbit / s DWDM System," Carpathian J. Electron. Comput. Eng., vol. 2, no. 10, pp. 3–8, 2017.

[6] N. Massa, "Fiber Optic Telecommunication," Fundam. Photonics, pp. 293–347, 2008.

[7] J. Tóth, Ľ. Ovseník, J. Turán, "Limitations of Dispersion and Pulse Broadering in Optical Fiber,"Electrical engineering and Informatics 5: Proceedings of the Faculty of Electrical Engineering and Informatics of the Technical University Of Kosice, pp. 399 - 404, 2014.

[8] X. Chen, J. E. Hurley and M. J. Li, "Bandwidth of multimode fibers obtained from system performance," *OFC/NFOEC*, Los Angeles, CA, pp. 1-3, 2012.

[9] J. Lavrencik, J. S. Gustavsson, E. Haglund, A. Larsson and S. E. Ralph, "Optimum VCSEL Apertures for High-Speed Multimode Fiber Links," *2018 Optical Fiber Communications Conference and Exposition (OFC)*, San Diego, CA, pp. 1-3, 2018.

[10] S. Pachnicke, "Fiber-Optic Transmission Networks," 2012.

[11] J. M. Castro, R. Pimpinella, B. Kose, P. Huang, B. Lane, K. Szczerba, P. Westbergh, T. Lengyel, J. S. Gustavsson, A. Larsson, and P. A. Andrekson, "Investigation of 60 Gb/s 4-PAM Using an 850 nm VCSEL and Multimode Fiber," J. Light. Technol., vol. 34, no. 16, pp. 3825–3836, 2016.

[12] D. R. S. Montero, "Multimode Graded-Index Optical Fibers for Next-Generation Broadband Access," no. June 2010, 2011.

[13] Cisco, "Cisco SFP Optics For Gigabit Ethernet Applications," pp. 1–9, 2016.

[14] RSoft Design Group, Inc., "Optsim Application Notes and Examples," 2009.

## About the Authors

**Tomáš Huszaník** (Ing.) received Ing. (MSc.) degree in telecommunications with honours from Technical University of Košice at Department of Electronics and Multimedia Telecommunications, in 2017. Since September 2017 he has been at Technical University of Košice as PhD. student. His research interest is mainly focused on all optical fiber networks and mitigation and degradation mechanisms in all optical WDM systems.

**Ján Turán** (Dr.h.c., prof., RNDr., Ing., DrSc.) received Ing. (MSc.) degree in physical engineering with honours from the Czech Technical University, Prague, Czech Republic, in 1974, and RNDr. (MSc.) degree in experimental physics with honours from Charles University, Prague, Czech Republic, in 1980. He received a CSc. (PhD.) and DrSc. degrees in radioelectronics from University of Technology, Košice, Slovakia, in 1983, and 1992, respectively. Since March 1979, he has been at the University of Technology, Košice as Professor for electronics and information technology. His research interests include digital signal processing and fiber optics, communication and sensing.

**Ľuboš Ovseník** (doc., Ing., PhD.) received Ing. (MSc.) degree in radioelectronics from the University of Technology, Košice, in 1990. He received PhD. degree in electronics from University of Technology, Košice, Slovakia, in 2002. Since February 1997, he has been at the University of Technology, Košice as Associate Professor for electronics and information technology. His general research interests include optoelectronic, digital signal processing, photonics, fiber optic communications and fiber optic sensors.

# IEEE International Conference on Computer Communications

## 29 Apr - 2 May 2019 // Paris, France

## CALL FOR PAPERS

IEEE INFOCOM 2019 solicits research papers describing significant and innovative research contributions to the field of computer and data communications networks. We invite submissions on a wide range of research topics, spanning both theoretical and systems research. Topics include but not limited to:

5G networks
Big data and machine learning for networks
Cellular networks
Cloud computing/mobile cloud computing
Cognitive radio networks
Cross-layer optimization and control
Crowdsourcing
Cyber-physical systems
Datacenter networking
Energy efficiency in networks
Edge and fog computing/networking
Fault tolerance, reliability and survivability
Information security and privacy
Information-centric networking
Interference management and mitigation
Internet architecture
Internet of Things
Localization and location-based services
Medium access control
MIMO-based networking
mmWave, VLC, full duplex communication networks
Mobile sensing and applications
Mobility management and models
Multimedia networking
Network economics and pricing
Network management
Network measurement and analysis
Network security and privacy
Network virtualization
Optical networks
Overlay and peer-to-peer networks
Quality-of-service and resource management
Router and switch design
Routing and multicast
Scaling laws and fundamental limits
Smart grid applications
Social computing and networks
Software-defined networking
Vehicular networks
Web applications and content distribution
WLAN, WPAN, RFID, and NFC
Wireless sensor networks

Accepted and presented papers will be published in the IEEE INFOCOM 2019 Conference Proceedings and submitted to IEEE Xplore®. Full details of submission procedures and requirements for authors of accepted papers are available at http://infocom2019.ieee-infocom.org.

### Important dates:

**Abstract Due:**
Tuesday, 24 July 2018
(11:59pm EDT)

**Full Paper Due:**
Tuesday, 31 July 2018
(11:59pm EDT)

**Notification of Acceptance:**
Friday, 30 November 2018

### General Chairs

Marcelo Dias de Amorim
Sorbonne Université, France
Serge Fdida
Sorbonne Université, France

### Technical Program Chairs

Wenjing Lou
Virginia Tech, USA
Giovanni Pau
Sorbonne Université / UCLA
Tilman Wolf
Univ. of Mass. Amherst, USA

### Technical Program Vice-Chair for Information System

Jian Tang
Syracuse University, USA

For more information, visit http://infocom2019.ieee-infocom.org

# CALL FOR PAPERS

IEEE

## 18th IEEE International Symposium on Computational Intelligence and Informatics

**Founding Honorary Chair**
*I. J. Rudas*, Óbuda University, Budapest

**Honorary Chairs**
*M. Réger*, Óbuda University, Budapest
*C. L. Philip Chen,* Univ. of Macau
*B. M. Wilamowski,* IEEE Division II

**Honorary Committee**
*R. Fullér*, HFA President
*L. T. Kóczy, HFA Honorary President*

**General Chair**
*L. Kovács*
Óbuda University, Budapest, Hungary

**Technical Program Committee Chairs**
*R. Andoga*, Tech. Univ. of Košice, Slovakia
*L. Kovács,* Óbuda University, Hungary

**Technical Program Committee**
*R. Andoga,* Tech. Univ. of Košice
*P. Baranyi*, BME
*J. Dombi*, University of Szeged
*Gy. Eigner*, Óbuda University
*I. Felde*, Óbuda University
*L. Főző,* Tech. Univ. of Košice
*P. Galambos*, Óbuda University
*T. D. Gedeon,* Murdoch University
*T. Haidegger*, Óbuda University
*L. Hluchý*, Slovak Academy of Sciences
*L. Horváth*, *Óbuda* University, Budapest
*S. Jenei*, University of Pécs
*Zs. Cs. Johanyák*, John von Neumann University
*J. Kelemen*, Silisian University
*P. Korondi,* BME
*L. Kovács*, University of Miskolc
*Sz. Kovács*, University of Miskolc
*L. Nádai*, Óbuda University, Budapest
*I. Stajner-Papuga*, University of Novi Sad
*Sz. Pletl,* Subotica Tech, Serbia
*S. Preitl,* Politehnica University in Timişoara
*R.-E. Precup*, Politehnica University in Timişoara
*P. Sinčák*, Tech. Univ. of Košice
*M. Takács*, Óbuda University
*J. K. Tar*, Óbuda University
*J. Tick*, Óbuda University
*A. R. Várkonyi-Kóczy*, Óbuda University

**Secretary General**
*Anikó Szakál,* Óbuda University, Budapest
szakal@uni-obuda.hu

**Organizing Committee Chair**
*J. Gáti*, Óbuda University, Budapest

**Organizing Committee**
*F. Hegyesi,* Óbuda University
*Gy. Kártyás,* Óbuda University
*K. Némethy*, Óbuda University
*Á. Takács*, Óbuda University

November 21-22, 2018

Óbuda University
Budapest, Hungary

**Sponsored by:**

***IEEE Hungary Section***
***IEEE Joint Chapter of IES and RAS, Hungary***
***IEEE Computational Intelligence Chapter, Hungary***
***IEEE SMC Chapter, Hungary***

**Technical Sponsors:**

***IEEE Systems, Man, and Cybernetics Society***
***Hungarian Fuzzy Association***

**Organizer:**

***Hungarian Fuzzy Association***

**The Symposium is organized with the focus of bringing together scientists from all over the world working on computational intelligence and its applications with the aims at providing an opportunity for sharing and discussing the recent research developments in this field.**

### Venue

The Symposium will be held in building of Óbuda University (Rooms F7, F8 and F9, Bécsi út 96/b, H-1034 Budapest, Hungary).

### Language

The official language of the Symposium is English. All the camera-ready manuscripts should be submitted in English.

### Submission of Papers

There are invited and regular papers. Authors are kindly asked to submit their paper through electronic paper submission system on the website. Papers sent by e-mail are not acceptable.

### Instructions for Authors

To reach the format of the final manuscript and instructions please log on to http://conf.uni-obuda.hu/cinti2018.

### Author's Schedule

| | |
|---|---|
| Full paper submission | August 31, 2018 |
| Notification | October 2, 2018 |
| Final manuscript submission | October 26, 2018 |

http://conf.uni-obuda.hu/cinti2018

# IEEE Wireless Communications and Networking Conference 2019

15-18 April 2019 // Marrakech, Morocco

IEEE WCNC is one of the main venues for researchers, industry professionals, and academics interested in the most advanced and recent contributions to wireless communications, especially regarding the design and development of wireless systems and networks. Sponsored by the IEEE Communications Society, IEEE WCNC has a long history of connecting industry, academia, and regulatory bodies. In 2019, other than mesmerizing its visitors by its beauty, Marrakesh as a major city of Morocco will become the premium venue of the wireless by hosting WCNC'19. The conference will include technical sessions, tutorials, workshops, and technology/business panels. You are invited to submit papers in all areas of wireless communications and networks. Potential topics include, but are not limited to:

## Track 1: PHY and Fundamentals

- Channel modeling, characterization and estimation
- Modulation, coding, diversity, equalization, synchronization
- OFDM, multi-carrier modulation, waveform design
- Interference modeling, management, cancellation and alignment
- PHY strategies for low-rate, sporadic and asynchronous communications
- MIMO, massive MIMO and cloud-RAN
- Cooperative, device-to-device and multi-hop communication
- Cognitive radio, spectrum sensing
- Content caching and storage in wireless networks
- PHY layer design for cellular, wireless LAN, ad hoc and sensor networks
- Energy efficient and energy harvesting PHY layer design
- Joint information and energy transmission
- PHY layer security and privacy, ultra-wideband, mmWave and sub-THz communication
- Information-theoretic aspects of wireless communications
- Signal processing for wireless communications
- Molecular and nano communications

## Track 2: MAC and Cross-Layer Design

- Wireless MAC protocols for 5G: design, analysis, and optimization
- Cognitive and cooperative MAC
- MAC for mesh, ad hoc, relay and sensor networks
- Scheduling and radio resource management
- Cross-layer MAC design
- Software defined radio, RFID MAC
- QoS support and energy efficient MAC
- MAC protocol for energy harvesting wireless networks
- MAC design for multitier cellular/small cell networks
- Multiple access in machine-to-machine communication
- MAC for cloud-RAN
- MAC protocols for molecular and nano networks
- MAC protocols for mmWave networks
- Full-duplex MAC design
- Cross-layer design for massive MIMO and multiuser MIMO networks

## Track 3: Wireless Networks

- Software-defined mobile/wireless networks
- Wireless Network Functions Virtualization
- Virtual network management and orchestration
- Mobile cloud
- Fog computing and networking
- Mobile Edge Computing
- Mesh, relay, sensor and ad hoc networks
- Routing in wireless networks
- Cognitive radio and networking
- Resource management and optimization
- Big Data enabled Self-Organized Networking
- Mobile big data and network data analytics
- Integrated Wireless/Optical networks
- Mobility, location, and handoff management
- Multimedia QoS and traffic management
- Wireless broadcast, multicast and streaming
- Congestion and admission control
- Wireless network security and privacy
- Mobile social networks
- Wireless network measurements and characterization

## Track 4: Emerging Technologies, Architectures and Services

- Mobile/Wireless network support for vertical industries
- Adaptive content distribution in on-demand services
- Context and location-aware wireless services and applications
- User-centric networks and adaptive services
- Wireless body area networks and e-health services
- Intelligent transportation systems
- Dynamic sensor networks for urban applications
- Wireless emergency and security systems
- Ultra-reliable communication
- Enabling regulations, standards, spectrum management
- Hybrid licensed/unlicensed spectrum access schemes (e. g. licensed-assisted access)
- Technologies, architectures and enabling business models for rural communications
- Satellite-based mobile access and backhaul
- Hybrid satellite-terrestrial networks
- Full duplexing
- Joint access and backhaul schemes
- Testbed and prototype implementation of wireless services

## CALL FOR PANELS

Panel proposals are also solicited on technical, business and policy-related issues and opportunities for the wireless communications industry.

Accepted and presented papers will be published in the IEEE WCNC 2019 Conference Proceedings.

## IMPORTANT DATES

Paper Submission Deadline: September 25, 2018

Notification of Acceptance: December 25, 2018

Camera-Ready Submission: January 25, 2019

Panel Proposals: October 15, 2018

Tutorial Proposals: October 15, 2018

Workshop Proposals: October 15, 2018

## EXECUTIVE GENERAL CHAIR

- Prof. Tarik Taleb, Aalto University, Finland

## TECHNICAL PROGRAM COMMITTEE Co-CHAIRS

- Prof. Muriel Médard, MIT, USA
- Prof. Ross Murch, The Hong Kong University of Science and Technology, Hong Kong
- Prof. Nelson Fonseca, The State University of Campinas, Brazil

## STEERING COMMITTEE CHAIR

- Prof. Khaled B. Letaief, Hong Kong University of Science & Technology, Hong Kong

# Guidelines for our Authors

## Format of the manuscripts

Original manuscripts and final versions of papers should be submitted in IEEE format according to the formatting instructions available on

*http://www.ieee.org/publications_standards/publications/authors/authors_journals.html#sect2,*

"Template and Instructions on How to Create Your Paper".

## Length of the manuscripts

The length of papers in the aforementioned format should be 6-8 journal pages.

Wherever appropriate, include 1-2 figures or tables per journal page.

## Paper structure

Papers should follow the standard structure, consisting of *Introduction* (the part of paper numbered by "1"), and *Conclusion* (the last numbered part) and several *Sections* in between.

The Introduction should introduce the topic, tell why the subject of the paper is important, summarize the state of the art with references to existing works and underline the main innovative results of the paper. The Introduction should conclude with outlining the structure of the paper.

## Accompanying parts

Papers should be accompanied by an *Abstract* and a few *index terms (Keywords)*. For the final version of accepted papers, please send the *short cvs* and *photos* of the authors as well.

## Authors

In the title of the paper, authors are listed in the order given in the submitted manuscript. Their full affiliations and e-mail addresses will be given in a footnote on the first page as shown in the template. No degrees or other titles of the authors are given. Memberships of IEEE, HTE and other professional societies will be indicated so please supply this information. When submitting the manuscript, one of the authors should be indicated as corresponding author providing his/her postal address, fax number and telephone number for eventual correspondence and communication with the Editorial Board.

## References

References should be listed at the end of the paper in the IEEE format, see below:

a) Last name of author or authors and first name or initials, or name of organization
b) Title of article in quotation marks
c) Title of periodical in full and set in italics
d) Volume, number, and, if available, part
e) First and last pages of article
f) Date of issue

*[11] Boggs, S.A. and Fujimoto, N., "Techniques and instrumentation for measurement of transients in gas-insulated switchgear," IEEE Transactions on Electrical Installation, vol. ET-19, no. 2, pp.87–92, April 1984.*

Format of a book reference:

*[26] Peck, R.B., Hanson, W.E., and Thornburn, T.H., Foundation Engineering, 2nd ed. New York: McGraw-Hill, 1972, pp.230–292.*

All references should be referred by the corresponding numbers in the text.

## Figures

Figures should be black-and-white, clear, and drawn by the authors. Do not use figures or pictures downloaded from the Internet. Figures and pictures should be submitted also as separate files. Captions are obligatory. Within the text, references should be made by figure numbers, e.g. "see Fig. 2."

When using figures from other printed materials, exact references and note on copyright should be included. Obtaining the copyright is the responsibility of authors.

## Contact address

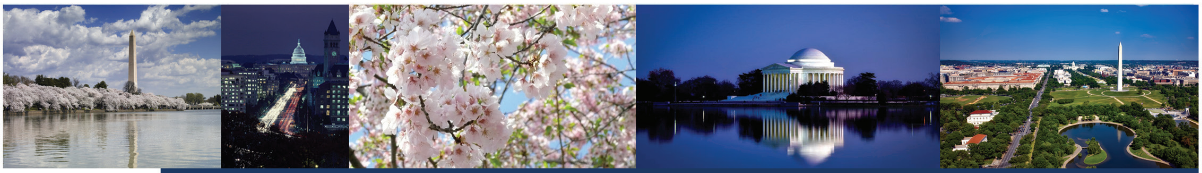
Authors are requested to submit their papers electronically via the EasyChair system. The link for submission can be found on the journal's website:

www.infocommunications.hu/for-our-authors

If you have any question about the journal or the submission process, please do not hesitate to contact us via e-mail:

Rolland Vida – Editor-in-Chief:
vida@tmit.bme.hu

Árpád Huszák – Associate Editor-in-Chief:
huszak@hit.bme.hu



# IFIP/IEEE International Symposium on Integrated Network Management

8-12 April 2019 // Washington DC // USA

*http://im2019.ieee-im.org/*

## Call for Papers

*The 16th IFIP/IEEE Symposium on Integrated Network and Service Management (IM 2019) will be held 8-12 April 2019 in Washington DC, USA. Held in odd-numbered years since 1989, IM 2019 follows the 31 years tradition of NOMS and IM as the primary IEEE Communications Society's forum for technical exchange on management of information and communication technology focusing on research, development, integration, standards, service provisioning, and user communities. IM 2019 will focus on the theme "Intelligent Management for the Next Wave of Cyber and Social Networks", reflecting the increasing convergence of both technical network infrastructure and infrastructure for social interactions as well as the emergence of new waves of communications technology involving areas as varied as cyber-physical systems, ultra-low latency services, and converged management and control planes. IM 2019 will offer five types of sessions: technical, experience, poster, panel and dissertation. High quality will be assured through a well-qualified Technical Program Committee and stringent peer review of paper submissions. A special call for demonstrations is organized to allow industry partners and researchers to demonstrate early products and prototypes.*

### *Topics of Interest*

*Authors are invited to submit papers that fall into or are related to the topic areas that are listed below. In addition, we invite submissions of proposals for demonstrations, exhibits, technical panels, tutorials and workshops, as well as experience session papers and dissertation papers.*

#### *Management and Control of Networks*

- *Enterprise and Campus Networks*
- *Data Center Networks*
- *Industrial Networks and TSN*
- *Cyber Physical Systems*
- *Software-Defined Networks*
- *IP Networks*
- *5G*
- *Wireless Networks*
- *Optical Networks*
- *Overlay Networks*
- *Home Networks*
- *Access Networks*
- *SCADA Networks and DCS*
- *Sensor Networks*
- *Internet of Things*
- *Information-Centric Networks*

#### *Management and Control of Communication Services*

- *Information Technology Services*
- *Virtual Networking Services*
- *XaaS and Cloud Services*
- *Multimedia Services*
- *Content Delivery Services*
- *Social Networking Services*
- *Security Services*
- *Privacy Services*
- *IoT Services*
- *VR/AR Services*
- *Network Resilience and High-Precision Networks*

#### *Network Programming and Automation*

- *Software-Defined Networking*
- *DevOps*
- *Data-Driven Automation, Intelligence-Assisted Networking*
- *Network Automation*
- *Network Telemetry Collection*
- *Help Desk Automation*
- *Novel Network Programming Approaches*
- *Web Service Technologies for Service Creation*

#### *Management Algorithms and Architectures*

- *Centralized Management*
- *Distributed Management*
- *Autonomic networks and self-management*
- *Middleware*
- *Management protocols*
- *Fog and Mobile Edge Computing*
- *Lambda Functions and Elastic Management*
- *Machine Learning Applications for Networking*
- *Federated Learning and Artificial Intelligence*
- *Data Analytics for Management*
- *Policy-Based Management, Intent-Driven Management*
- *Probability, stochastic processes, queuing theory*
- *Data, information, semantic modeling*
- *Model-Driven Management*
- *Control Theory*
- *Network Optimization*
- *Design and Simulation*

#### *Management Functions and Practical Approaches*

- *Case Studies and Practical Experiences*
- *Integration Issues*
- *Business-Driven Management*
- *Service Assurance*
- *Fault and Performance Management*
- *Measurement and Validation*
- *SLA Management, QoS and QoE*
- *Compliance*
- *Accounting*
- *Billing*
- *Service Fulfillment*
- *Energy Management*
- *Deployment of Services*
- *Operations Support Systems*

***Contact TPC Co-chairs for more information:*** *im2019tpc@gmail.com*

#### *Important Dates*

*Paper Submission Deadline:* ***August 19, 2018***
*Notification of Acceptance:* ***November 15, 2018***
*Please note that dates are almost a month earlier than in the past due to early April conference date*

#### *General Co-chairs*

*Joe Betser, The Aerospace Corporation, USA*
*Carol Fung, Virginia Commonwealth Univ., USA*

#### *TPC Co-chairs*

*Shingo Ata, Osaka City Univ., Japan*
*Alexander Clemm, Huawei, USA*
*Jérôme François, INRIA Nancy Grand Est, France*

# SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS

hte

FOUNDED IN 1949

SCIENTIFIC
ASSOCIATION FOR
INFOCOMMUNICATIONS
HUNGARY

## Who we are

Founded in 1949, the Scientific Association for Infocommunications (formerly known as Scientific Society for Telecommunications) is a voluntary and autonomous professional society of engineers and economists, researchers and businessmen, managers and educational, regulatory and other professionals working in the fields of telecommunications, broadcasting, electronics, information and media technologies in Hungary.

Besides its 1000 individual members, the Scientific Association for Infocommunications (in Hungarian: Hírközlési és Informatikai Tudományos Egyesület, HTE) has more than 60 corporate members as well. Among them there are large companies and small-and-medium enterprises with industrial, trade, service-providing, research and development activities, as well as educational institutions and research centers.

HTE is a Sister Society of the Institute of Electrical and Electronics Engineers, Inc. (IEEE) and the IEEE Communications Society.

## What we do

HTE has a broad range of activities that aim to promote the convergence of information and communication technologies and the deployment of synergic applications and services, to broaden the knowledge and skills of our members, to facilitate the exchange of ideas and experiences, as well as to integrate and harmonize the professional opinions and standpoints derived from various group interests and market dynamics.

To achieve these goals, we…

- contribute to the analysis of technical, economic, and social questions related to our field of competence, and forward the synthesized opinion of our experts to scientific, legislative, industrial and educational organizations and institutions;
- follow the national and international trends and results related to our field of competence, foster the professional and business relations between foreign and Hungarian companies and institutes;
- organize an extensive range of lectures, seminars, debates, conferences, exhibitions, company presentations, and club events in order to transfer and deploy scientific, technical and economic knowledge and skills;
- promote professional secondary and higher education and take active part in the development of professional education, teaching and training;
- establish and maintain relations with other domestic and foreign fellow associations, IEEE sister societies;
- award prizes for outstanding scientific, educational, managerial, commercial and/or societal activities and achievements in the fields of infocommunication.

## Contact information

President: **GÁBOR MAGYAR, PhD** • *elnok@hte.hu*

Secretary-General: **ERZSÉBET BÁNKUTI** • *bankutie@ahrt.hu*

Operations Director: **PÉTER NAGY** • *nagy.peter@hte.hu*

International Affairs: **ROLLAND VIDA, PhD** • *vida@tmit.bme.hu*

Address: H-1051 Budapest, Bajcsy-Zsilinszky str. 12, HUNGARY, Room: 502
Phone: +36 1 353 1027
E-mail: *info@hte.hu*, Web: *www.hte.hu*