Infocommunications Journal

A PUBLICATION OF THE SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS (HTE)

June 2023 Volume XV Number 2 ISSN 2061-2079

MESSAGE FROM THE EDITOR-IN-CHIEF

PAPERS FROM OPEN CALL

CALL FOR PAPER / PARTICIPATION

ADDITIONAL

Technically Co-Sponsored by
IEEE ComSoc™
IEEE Communications Society

hte

IEEE
HUNGARY SECTION

Editorial Board

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, Scientific Association for Infocommunications (HTE)

The publication was produced with the support of
the Hungarian Academy of Sciences and the NMHH

MAGYAR TUDOMÁNYOS AKADÉMIA 1825

NMHH
National Media and Infocommunications Authority • Hungary

Editorial Office (Subscription and Advertisements)**:**
Scientific 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
Phone: +36 1 463 4189 • E-mail: pvarga@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

A note on using generative tools for research papers at the Infocommunications Journal

Pal Varga

THERE is a new emerging trend of using large language model-based applications – such as ChatGPT, Bard, Claude or LLama – in the research and innovation processes. This reaches from data processing through writing (parts of) reports to using them in reviewing scientific articles.

The policy of Infocommunications Journal is to follow general guidelines of professionalism and the Codes of Conduct provided by ACM, IEEE and others. When it comes to the usage of ChatGPT and similar tools, they should be used as professional tools, as these make work easier. Still, authors should make sure that the output is scientifically supported and in general, true. When it comes to text editing, both authors and reviewers can use them for *light text-editing* purposes. When authors generate text or multimedia content with such tools, it must be properly quoted and cited, following the publication rules that are anyway applicable for works not part of the authors' contribution.

With this in mind, let's take an overview of the current issue – with the help of ChatGPT, and manual verification, indeed.

Marwah Haleem Jwair and Taha A. Elwi propose a metasurface antenna structure for 5G communication networks. They demonstrate that the proposed antenna design, utilizing twelveunit metasurface unit cells, effectively miniaturizes the antenna size to 30×35mm2 while covering the frequency bands from 3.15GHz-3.63GHz and 4.8GHz-5.1GHz. The numerical simulations validate the antenna's performance, showing improved impedance bandwidth and achieving gains of 3.5dBi and 4.8dBi at 3.5GHz and 5GHz respectively. The proposed antenna is deemed highly suitable for modern wireless communication networks.

The paper by András Mihály and László Bacsárdi focuses on the use of satellite channels in creating a quantum network with extended coverage compared to optical fiber networks. By minimizing the number of satellites required for an efficient quantum network, the costs associated with launching and maintaining satellites can be reduced, enabling a more affordable quantum internet. The authors present an optical transmittance-based routing algorithm that facilitates successful quantum entanglement transfer between terrestrial nodes. They present the performance differences between various satellite architectures and systems, highlighting the potential of non-continuous communication channels in realizing a quantum network over sparsely populated satellite systems.

In their paper, Naseer-Al-Imareen and Gábor Lencse explore the impact of path QoS metrics and path weight settings on the throughput aggregation capability of the MPT network layer multipath communication library. The study involves testing the library's channel aggregation capability using both symmetric and asymmetric paths, while considering various QoS metrics such as latency, transmission speed, packet loss rate, and jitter. The research findings indicate that the distribution of outgoing packets based on weights contributes to achieving a tunnel throughput close to the sum of the individual path throughputs. However, inappropriate weights and degraded performance in one of the paths can negatively affect the tunnel's throughput.

Gergely Hollósi and István Moldován study the use of Ultra Wideband (UWB) communication for clock synchronization in Time-Sensitive Networking (TSN) applications. Their paper explores wireless synchronization possibilities using UWB, which offers high accuracy timestamping even in the presence of multipath propagation. Their evaluation uses affordable hardware, and they reach sub-10-nanosecond accuracy, which is comparable to wired solutions. The paper highlights UWB as a cost-effective and wireless solution for accurate Precision Time Protocol (PTP) master clock synchronization, with potential for further improvements in synchronization accuracy.

Next, Dubem Ezeh and Jaudelice de Oliveira present a framework for anomaly detection in SDN environments using a Generative Adversarial Network (GAN) ensemble algorithm. Their contributions include proposing an SDN Controllerbased framework that deploys the GAN ensemble approach for network anomaly detection. The authors evaluate the framework's performance using both publicly available datasets and the newly created dataset by themselves, demonstrating its potential for detecting a wide range of anomalies. Their evaluation is conducted on a real testbed with geographicallyseparated nodes, adding to the robustness of the findings.

Sandor R. Repas analyzes the encryption capabilities of ARM-based single board microcomputers. His study evaluates ten different microcomputers for encryption tasks and concludes that even the slowest SBCs are sufficient for normal applications. His recommendations are provided based on performance characteristics, and the study also examines the random number generators of the microcomputers. Overall, Sandor's paper highlights the suitability of these microcomputers for encryption applications.

Khadija Touya et. al. introduces a game theoretic framework to control user behavior on social networking sites in their pursuit of popularity. By formulating the competition as a non-cooperative game, their study aims to find an equilibrium point. Their focus is on solving the popularity competition problem and proposing an efficient algorithm to learn the equilibrium point.

With this overview, let us all enjoy the summer – and the Infocommunications Journal papers in the 2nd issue of 2023.

Pal Varga is the Head of Department of Telecommunications and Media Informatics at the Budapest University of Technology and Economics. His main research interests include communication systems, Cyber-Physical Systems and Industrial Internet of Things, network traffic analysis, end-to-end QoS and SLA issues – for which he is keen to apply hardware acceleration and artificial intelligence, machine learning techniques as well. Besides being a member of HTE, he is a senior member of IEEE, where he is active both in the IEEE ComSoc (Communication Society) and IEEE IES (Industrial Electronics Society) communities. He is Editorial Board member in many journals, and the Editor-in-Chief of the Infocommunications Journal.

Metasurface Antenna Circuitry for 5G Communication Networks

Marwah Haleem Jwair[1], and Taha A. Elwi[2]

***Abstract*—In this article, the proposed antenna structure is designed for modern wireless communication systems. The antenna structure is consistent of twelve-unit metasurface (MTS) unit cells. Therefore, the antenna size is miniaturized effectively to 30×35mm^2 which is equivalently about 0.2λo, where λo is the free space wavelength at 3.5GHz. This is achieved by conducting the use of Hilbert shape MTS structure with T-resonator induction structure. The antenna structure is printed on a single side substrate to cover the frequency bands from 3.15GHz-3.63GHz and 4.8GHz-5.1GHz. Such antenna is found to provide a maximum gain of 3.5dBi and 4.8dBi at 3.5GHz and 5Ghz, respectively. Next, proposed antenna is found to be circularly polarized at 3.5GHz and 5GHz. The proposed antenna performance is simulated numerically using CST MWS software package with all design methodology that is chosen to arrive to the optimal performance. Then, the optimal antenna design is tested numerically using HFSS software package for validation. Finally, an excellent agreement is achieved between the two conducted software results.**

***Index Terms*—MTS, circularly polarized, Hilbert.**

I. Introduction

Due to the recent growth in modern communication systems, several requirements are demanded to satisfy the current state of the arts in the antenna design [1]. The emergence and development of the concept of artificial materials throughout years led to a revolution microwave researches [1]. So, an antenna is an element of a cellular transmission line and is one of the most critical components of wireless communications systems. Dipoles/monopoles, slot/horn antennas, loop antennas, microstrip antennas, reflector antennas, helical antennas, dielectric/lens antennas, log periodic antennas, and frequency-independent antennas are nine different kinds of antennas that have been developed in the last fifty years for both communication and navigation systems. Each type is better suited to a specific application than the others. Because of its low cost, light weight, and ease of fabrication, microstrip antennas are the most commonly used in reconfigurable antenna designs [2].

The idea of reconfigurable antennas can be traced back to a D. Schubert patent from 1983 [2]. In 1999, the United State Defense Advanced Research Projects Agency (DARPA) funded a project called "Reconfigurable Aperture Program (RECAP)" to look into the subject in applications of reconfigurable antennas [3]. Reconfigurable antennas have also been used in applications such as broadband networking, cognitive radio, MIMO systems, and others.

So, changing the frequency, polarization, or radiation characteristics of an antenna may be used to reconfigure it. The majority of antenna reconfigurability techniques redistribute antenna currents, changing the electromagnetic fields of the antenna's efficient aperture [4]. Recently, reconfigurable patch antennas are the most commonly produced reconfigurable style antennas due to the ease of fabrication and incorporation into small electronic devices such as mobile phones and laptops. A standard reconfigurable patch antenna is made up of several separate metalized regions that are carried out on a plane and connected through switches or tuning components [4]. Different metalized parts can be brought in contact with each other by dynamically regulating the state of the switches, thus altering the overall antenna's radiation efficiency [5].

However, antennas with Multiple Inputs and Multiple Outputs (MIMO) are used to improve wireless channel capacity [5]. For spatial diversity characteristics, the adopted MIMO technology provides an efficient, high data rate that is split into multiple lower-rate streams. Many wire-free communication technologies, such as WLAN, 3G, LTE, and WiMAX (4G), depend on MIMO antennas where many researchers developed with various shapes to cover a wide range of frequency bands [6].

Moreover, a MIMO antenna with a small size, high gain and performance, and CP radiation, as well as a large impedance bandwidth, is needed for many wireless communication systems [7]. Additionally, MIMO systems have been proposed to mitigate multipath fading effects [8], however adjacent antennas coupling within a short separation distance may be the most significant drawback, especially in portable recent MIMO devices and systems [9].

In MIMO systems, this coupling must be reduced to improve antenna impedance matching and radiation properties [10], where mutual coupling refers to electromagnetic losses caused by surface wave interactions between antenna elements [11]. Mutual coupling can be thought of as surface wave leakage in this case; however, it is highly dependent on antenna geometry, array structure, and separation distances [12].

II. Antenna Geometrical Details

The proposed antenna, see Fig. 1, is constructed from circular patch geometry mounted on a Techtronic FR4 substrate. The antenna patch is fed with a coplanar waveguide (CPW) microstrip line printed on the same panel with the patch from the antenna substrate. The transmission line is designed as a triangular coplanar waveguide to maintain high coupling efficiency between the patch structure and the source over a wide frequency range [4].

For the proposed MTS structure, the array is oriented around the patch edges to suppress the surface waves in which

[1] Department of Information and Communication Engineering, College of information engineering, Al-Nahrain University, Baghdad, Iraq,

[2] International Applied and Theoretical Research Center (IATRC), Baghdad Quarter, Iraq (E-mail: taelwi82@gmail.com)

DOI: 10.36244/ICJ.2023.2.1

an excellent enhancement can be achieved in terms of the antenna gain-bandwidth product [10]. The proposed array is constructed from twelve-unit cell that are distributed with a certain separation distance to achieve capacitive coupling effects that magnifies the electrical field fringing and return reduces the antenna size [4]. The individual unit cell is constructed from Hilbert curve fractal geometry to maintain high surface current density within a limited area [3]. The frequency resonance of the individual unit cell can be tuned with a T-resonator structure through controlling the total impedance with a variable capacitor [9].

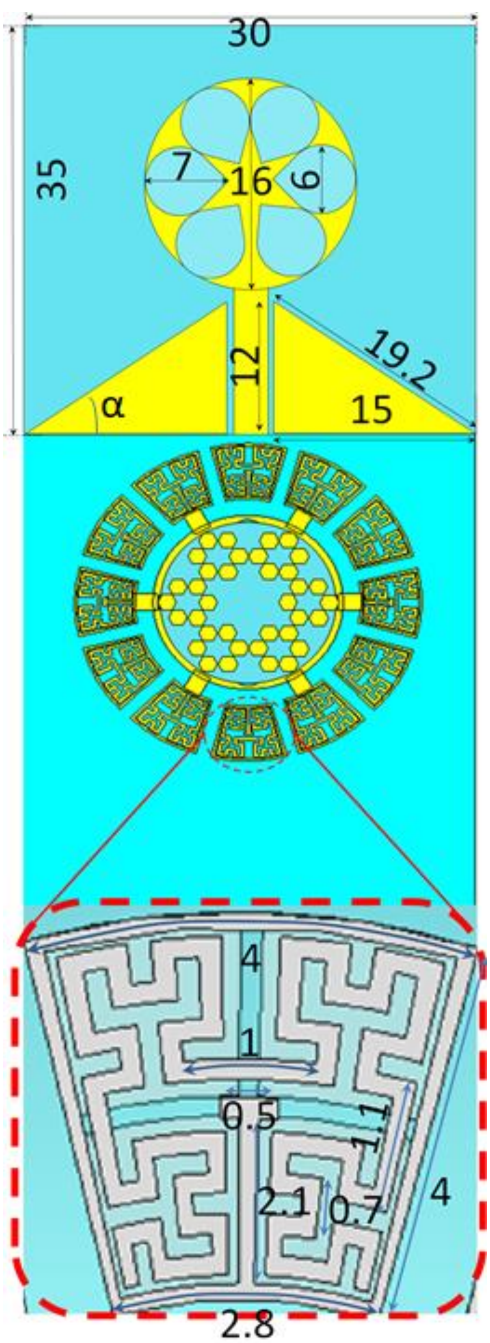


Fig. 1: Antenna and MTS structures that are proposed in this work in mm scale.

III. MTS CHARACTERIZATIONS

Now, to realize the performance of the proposed MTS unit cell, a numerical analysis is conducted based on CST MWS of a finite integral technique. The authors evaluated the proposed MTS unit cell S_{11} spectra using HFSS software package to be compared to their relative results from CST MWS. For this, a comparison study in terms of S-parameters spectra are presented in Fig. 2. First of all, we found that the obtained results from both software packages agree very well to each other. Also, the frequency resonance is found to be very close to the frequency band of interest. This motivated the authors to consider this unit cell to be an excellent intimate to the proposed design that realizes an excellent reduction in the antenna surface waves from the patch edges [7]. The surface wave reduction is achieved by the effects of the proposed unit cell which suppresses the surface wave significantly at the frequency band of interest [9].

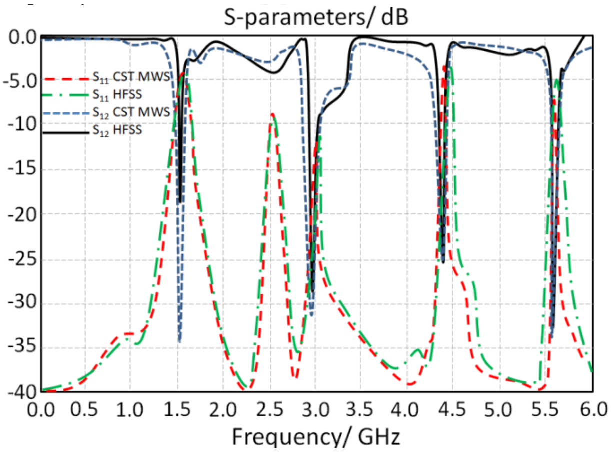


Fig. 2: Evaluated S-parameters spectra from both considered software packages.

IV. TRIANGULAR CPW DETAILS

The triangular CPW is designed to the proposed antenna to ensure bandwidth enhancement with maximum coupling. Moreover, the proposed CPW is structured with a triangular ground plane of certain slop angle (α). Therefore, the authors, partially, studied the effects of changing the goun plane slop angle by varying α from 36° to 40° with a step of 2° as seen in Fig. 3. It is observed that increasing the number of stages realizes a significant enhancement on the antenna bandwidth. This technique is invoked to maintain the antenna gain-bandwidth enchantments as shown in Fig. 4. This is in fact is achieved by eliminating the accumulated surface charges on the proposed CPW edges [8]. The slope of the suggested land causes the charge accumulation to increase up [5]. Consensually, tripping the electromagnetic energy within the substrate layer [6], that refer band with decrease by lowering the patch's surface resistance to actualize inconsistency between the load and the source's input impedance [2]. The authors did this because the suggested CPW has a substantial impact on the antenna bandwidth and gain by placing the SMA port in a specific orientation. The reverse side of the hypothesized CPW impact on discharging the accumulated surface charge is used in this approach, and it does actually deliver these improvements [7].

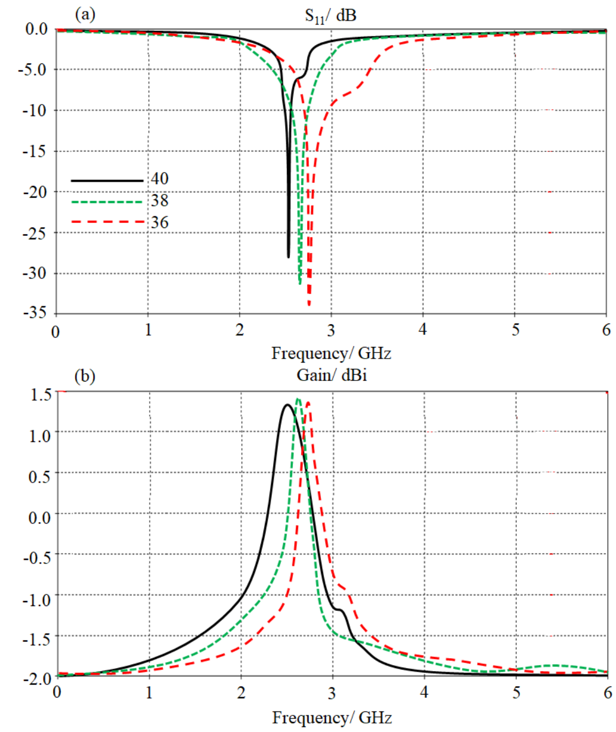


Fig. 3; Evaluated S_{11} and gain spectra based on the parametric study: (a) S_{11} and (b) Gain.

V. Design Methodology

The proposed antenna design methodology is presented in Fig 4 by considering a parametric-study based on flowchart. The optimal antenna performance of the proposed system is characterized according to S-parameters and gain spectra.

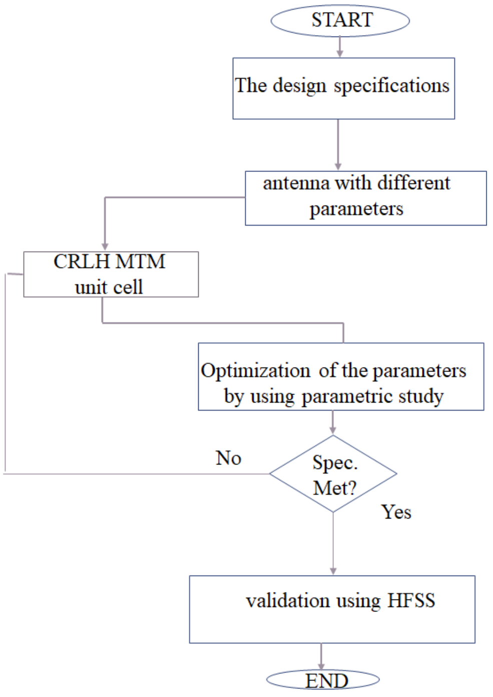

START
The design specifications
antenna with different parameters
CRLH MTM unit cell
Optimization of the parameters by using parametric study
No
Spec. Met?
Yes
validation using HFSS
END

Fig. 4; The considered design methodology flowchart.

For this, the parametric study is invoked to change the substrate height (h), outer radius (R) of the main antenna patch, separation distance (G) between the antenna patch and MTS layer, and the spacing between the proposed CRLH with respect to the antenna middle ring (w). These antenna parameters are studied as following:

A. *Basic Antenna Design (h and R)*

The main basic parameters are considered because they have significant effects on the antenna matching bandwidth and gain. As seen in Fig. 5, the proposed antenna performances variations with respect to h and R. It is found that the antenna frequency resonance is slightly shifted without significant variation in the antenna gain relative to varying the antenna substrate height (h) from 1mm to 3mm as seen in Fig. 5(a). However, the antenna frequency and gain spectra are affected with changing the main patch radius (R) from 15mm to 17mm as shown in Fig. 5(b).

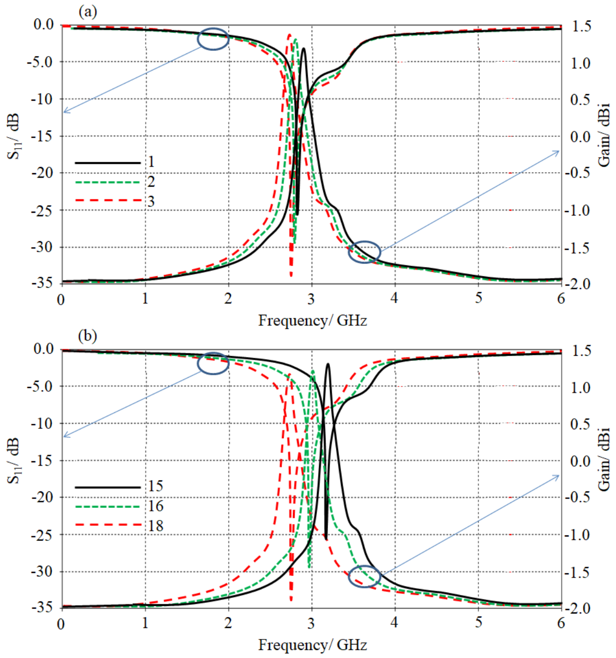


Fig. 5; Evaluated S11 and gain spectra based on the parametric study with varying: (a) h and (b) R.

B. *MTS Effects*

From the evaluated results in terms of S_{11} and gain spectra, see Fig. 5, we found that the proposed antenna provides a resonance mode around 3.5GHz with another band at 5GHz. These two frequency bands are very suitable for modern applications including 5G networks. Nevertheless, the antenna gain is found to be in the range of 3.2dBi and 4.8dBi, respectively.

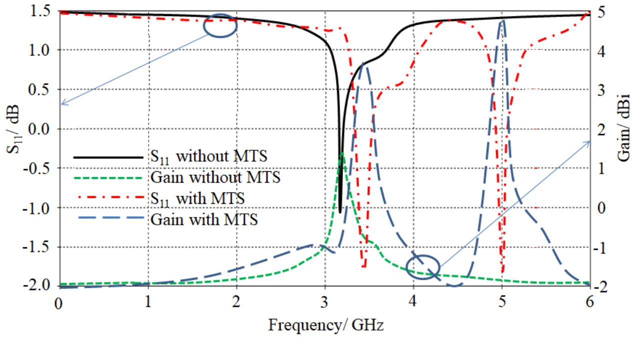


Fig. 6; Evaluated antenna performance in terms of S11 and gain spectra.

C. *Optimization Process based Convolution Neural Network*

Now, the design methodology is invoked to be *studied* parametrically using neural network architecture. For this network, convolution neural network model is designed for the proposed antenna structure to suite sub-6GHz bands. In Fig. 7, a synthesis model is defined as to obtain dimensions (G, w, h) of the antenna while providing the resonant frequency (f_r), gain (G_o), bandwidth (B.W), Quality factor (Q), and return loss spectra (S_{11}) at the input of the proposed model.

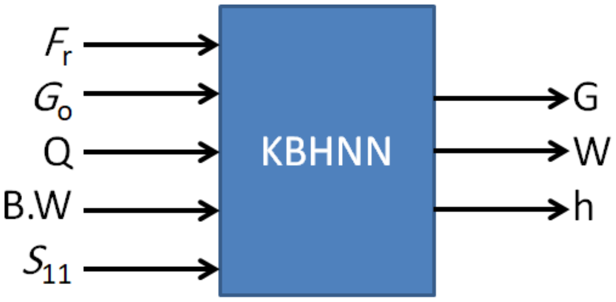


Fig. 7; The synthesis of proposed antenna using neural network.

Artificial neural networks are commonly employed to solve problems that include a lot of nonlinearity and many variables. They are also used to empower sensors for the more complex sensing applications [7]. Because the developing system of linear equations by using curve fitting for calculating the effective permittivity of the microwave resonators ambient is extremely difficult, because it depends on multi-variable multi-resonances, and depends on many parameters such as the shape of the field, the container, the overall mixture permittivity [9]. In order to solve these problems that were mentioned above by using feedforward multi-layer could be a good alternative. As training data for the proposed neural network, about 200 samples are collected by varying the dimensions of the proposed microstrip patch antenna using the numerical results from CST MWS software package. To classify the input data from regression, the results from the Matlab code is involved to show the classification of the input data according to their category. In this category, the input data is classification by the neural network to three intervals mainly a cording to the regression rate. In this classification, the first third of the input values are determent as low gain. The second interval is considered the intermediate gain level. The last interval is considered for the high gain.

From Fig. 8, the data regression is found to be excellently fitting to the output data. Also, it is very ovals the regression subject, the proposed sensor best on the neural network realizes excellent matching with the classifications at low and high gain. However, this observation is limited to intermediate values, which could be realized high error. To realize an effective solution, more points are required to recognize the best fitting for this interval. It is good to mention, such discrepancy in the intermediate interval is observed in the Fig. 8 that shows a break point in the middle of the values from the simulation that agrees with measured data. Table I lists the best values obtained for the most commonly used neural parameters.

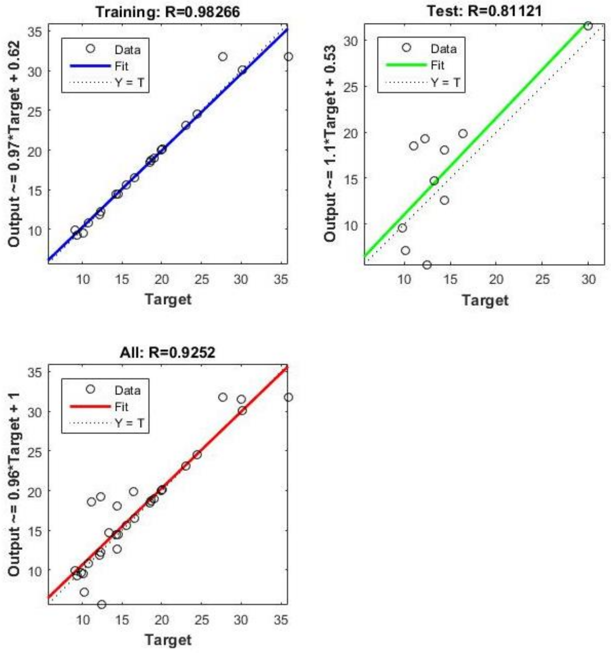


Fig. 8 Findings from the regression analysis.

TABLE I
THE NEURAL NETWORK PARAMETERS.

Neural Network parameters	Neural Network for simulation
Number of Input layer nodes	5
Number of Hidden layer nodes	3
Number of Output Layer nodes	1
Transfer function	logsig
Training function	pureline
Learning rate	0.001
Maximum number of Epochs	88

VI. RESULTS VALIDATION AND DISCUSSIONS

The obtained results from CST are compared to those obtained from HFSS for validation. The comparison reviles an excellent agreement between the considered software packages as seen in Fig. 9. The antenna performance, in terms of S_{11} and gain spectra with radiation patterns are tested numerically. The simulated S_{11} and gain spectra of the proposed antenna from both software packages are compared to the each other. The obtained results are found to agree to each other excellently. It is found that the proposed antenna provides a bandwidth from 3.15GHz to 3.63GHz and 4.8GHz to 5.1GHz with gain of 3.5dBi and 4.8dBi, respectively.

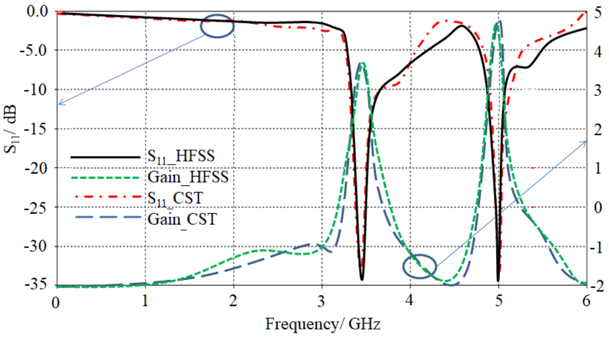


Fig. 9; Antenna performance validation.

The antenna radiation patterns at 3.5GHz and 5GHz are presented in Fig. 10(a). We found the antenna radiation patterns are almost Omni-directional around the antenna transmission line. This due to the fact of the proposed antenna structure is designed without back panel ground plane [3]. Therefore, the surface current distribution on the antenna patch is distributed symmetrically as seen in Fig. 10(b).

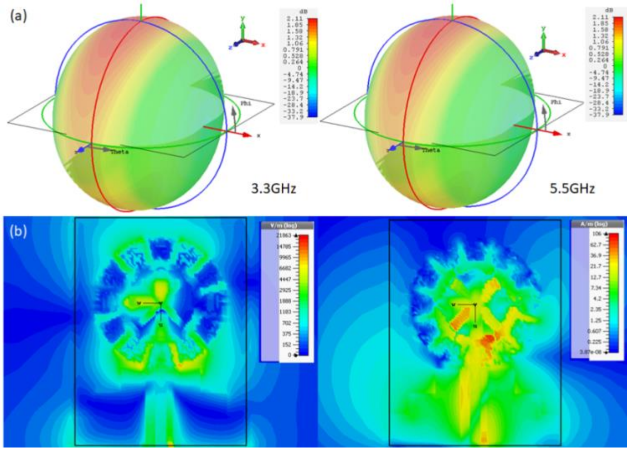


Fig. 10; Antenna field distribution: (a) Radiation patters and (b) surface current.

The proposed antenna is designed to realize a circular polarization feature at 3.5GHz and 5GHz as seen from the axial ratio (AR) in Fig. 11. The evaluated results from both CST MWS and HFSS are compared to each other. It is found that the evaluated results agree very well to each other.

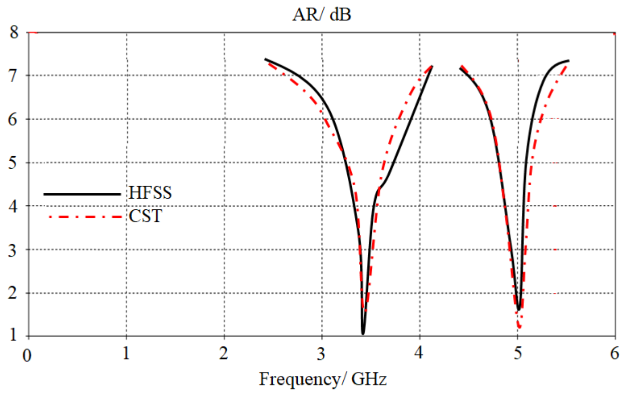


Fig. 11; Antenna AR spectra validation.

Finally, the proposed antenna performance is compared to other published results in the literature as listed in Table II. It is found from such comparison, that the proposed antenna system maintains an excellent gain-bandwidth product over other published results with small size. Nevertheless, the antenna shows an excellent AR in comparison to other listed antennas.

TABLE II
A comparison between the proposed antenna performance and other published designs.

Ref.	Freq./GHz	Gain/dBi	Size(mm^2)	AR
[13]	3.4-3.7	8.3	15×440	×
[14]	2.49/3.45	4, 6	80×80	×
[15]	3.9	8	170.8×40	×
[16]	3.3-4.2/4.8-5.9	7.24, 3.74	40×204	×
This work	3.15-3.63, 4.8-5.1	3.5, 4.8	30×35	√

VII. Conclusion

The proposed antenna performance is numerically validated with respect to different software packages. It is found that the proposed antenna realizes a significant enhancement in the antenna matching impedance bandwidth. Such enhancement is achieved by introducing the proposed MTS unit cells. We found that the proposed antenna provides a bandwidth at two frequency bands 3.15GHz-3.63GHz and 4.8GHz-5.1GHz with gain of 3.5dBi and 4.8dBi, respectively. This is in fact attributed to the surface plasmon current motion on the antenna patch with a significant reduction in the surface waves. This is achieved when; the proposed antenna structure is fetched to the patch structure. Therefore, the charge accumulation on the substrate is converted as plasmonic current on the patch surface. For this, the antenna bandwidth is improved through the proposed MTS introduction. Finally, it is found that the proposed antenna is an excellent candidate for the modern wireless communication networks.

References

[1] H. H. Al-Khaylani, T. A. Elwi, and A. A. Ibrahim, "A Novel Miniaturized Reconfigurable Microstrip Antenna Based Printed Metamaterial Circuitries for 5G Applications", Progress In *Electromagnetics Research C*, Vol. 120, 1-10, 2022, doi: 10.2528/PIERC22021503.

[2] M. H. Jwair and T. A. Elwi, "Circularly Polarized Metamaterial Patch Antenna Circuitry for Modern Applications", *International Journal of Emerging Technology and Advanced Engineering*, Volume 12, Issue 12, December 2022, doi: 10.46338/ijetae1222_05.

[3] A. Abdulmjeed, T. A. Elwi, and S. Kurnaz, "Metamaterial Vivaldi Printed Circuit Antenna Based Solar Panel for Self-Powered Wireless Systems", Progress In *Electromagnetics Research M*, Vol. 102, 181-192, 2021. doi: 10.2528/PIERM21032406.

[4] A. I. Imran, T. A. Elwi, and Ali J. Salim, "On the Distortionless of UWB Wearable Hilbert-Shaped Metamaterial Antenna for Low Energy Applications", Progress In *Electromagnetics Research M*, Volume 101, pp. 219-239, March 2021. doi: 10.2528/PIERM20113008.

[5] T. A. Elwi, "A Further Realization of a Flexible Metamaterial-Based Antenna on Nickel Oxide Polymerized Palm Fiber Substrates for RF Energy Harvesting", *Wireless, Personal Communications*, Volume 10, no. 12, pp.1-15, August 2020. doi: 10.1017/S1759078720000665.

[6] Y. Alnaiemy, T. A Elwi, L. Nagy, "An end fire printed monopole antenna based on electromagnetic band gap structure," *Automatika*, volume 61, issue 3, pp. 482-495. doi: 10.1080/00051144.2020.1785783.

[7] T. A. Elwi, "Remotely Controlled Reconfigurable Antenna for Modern Applications", *Microwave and optical letters*, Volume 6, issue 1, pp. 1-19, April 2020, doi: 10.1002/mop.32505.

[8] T. A. Elwi, "Further Investigation on Solant-Rectenna based Flexible Hilbert-Shaped Metamaterials", *IET Nanodielectrics*, Volume 4, issue 12, pp. 1-12, March 2020, DOI: 10.1049/iet-nde.2020.0013.

[9] T. A. Elwi and A. M. Al-Saegh, "Further realization of a flexible metamaterial-based antenna on indium nickel oxide polymerized palm fiber substrates for RF energy harvesting", *International Journal of Microwave and Wireless Technologies*, Cambridge, Volume 5, issue 4, pp. 1-9, May 2020, DOI: 10.1017/S1759078720000665.

[10] T. A. Elwi, D. A. Jassim, H. H. Mohammed, "Novel miniaturized folded UWB microstrip antenna-based metamaterial for RF energy harvesting", *International Journal of Communication Systems*, Volume 1, issue 2, January 2020, DOI: 10.1002/dac.4305.

[11] Y. Alnaiemy, T. A. Elwi, L. Nagy, "Mutual Coupling Reduction in Patch Antenna Array Based on EBG Structure for MIMO Applications", *Periodica Polytechnica Electrical Engineering and Computer Science*, Volume 1, number 4, pp.1-11, Sep. 2019, DOI: 10.3311/PPee.14379.

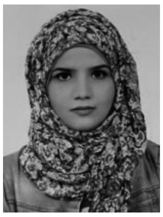
[12] R. K. Abdulsattar, T. A. Elwi, Z. A. Abdul Hassain, "A New Microwave Sensor Based on the Moore Fractal Structure to Detect Water Content in Crude Oil", MDPI *Sensors, Vol. 21*, pp. 7143. DOI: 10.3390/s21217143.

[13] Jwair, MH, Elwi, TA. "Steerable composite right–left- hand-based printed antenna circuitry for 5G applications", *Microw Opt Technol Lett*. 2023; 1- 8. DOI: 10.1002/mop.33666.

[14] J. Zhang, S. Yan and G. A. E. Vandenbosch, "Realization of Dual-Band Pattern Diversity With a CRLH-TL-Inspired Reconfigurable Metamaterial", in *IEEE Transactions on Antennas and Propagation*, vol. 66, no. 10, pp. 5130-5138, Oct. 2018, DOI: 10.1109/TAP.2018.2859917.

[15] C. Caloz, T. Itoh and A. Rennings, "CRLH metamaterial leaky-wave and resonant antennas", in *IEEE Antennas and Propagation Magazine*, vol. 50, no. 5, pp. 25-39, Oct. 2008, DOI: 10.1109/MAP.2008.4674709.

[16] M. Ismail, T. Elwi and A. Salim, "A Miniaturized Printed Circuit CRLH Antenna-based Hilbert Metamaterial Array", in *Journal of Communications Software and Systems*, vol. 18, no. 3, pp. 236-243, July 2022, DOI: 10.24138/jcomss-2022-0030.



Marwah Haleem Jwair was born in 1986 in Baghdad, Iraq. She earned the bachelor and master degrees in Information Engineering College from AL-Nahrain University, Baghdad, Iraq in 2016 and 2018 respectively. She is pursuing her PhD at AL-Nahrain University since 2021. Her main research interests are in Antennas, Microwave devices, Analog and Digital Electronics.

Taha A. Elwi received his B.Sc. in Electrical Engineering Department (2003) (Highest Graduation Award), Postgraduate M.Sc. in Laser and Optoelectronics Engineering Department (2005) (Highest Graduation Award) from Nahrain University Baghdad, Iraq. From April 2005 to August 2007, he was working with Huawei Technologies Company, Baghdad, Iraq. On January, 2008, he joined the University of Arkansas at Little Rock and he obtained his Ph.D. in December 2011 from the system engineering and science. His research areas include wearable and implantable antennas for biomedical wireless systems, smart antennas, WiFi deployment, electromagnetic wave scattering by complex objects, design, modeling and testing of metamaterial structures for microwave applications, design and analysis of microstrip antennas for mobile radio systems, precipitation effects on terrestrial and satellite frequency re-use communication systems, effects of the complex media on electromagnetic propagation and GPS. The nano-scale structures in the entire electromagnetic spectrum are a part of his research interest.

Optical transmittance based store and forward routing in satellite networks

András Mihály, and László Bacsárdi, *Member, IEEE*

***Abstract*—Quantum computing will play a crucial part in our security infrastructure for the coming years. Quantum networks can consist of direct optical fiber or free-space links. With the use of satellite channels, we can create a quantum network with higher coverage than using optical fibers where the distances are limited due to the properties of the fiber. One of the highest drivers of cost for satellite networks, apart from the cost of the technology needed for such systems, are the costs of launching and maintaining said satellites. By minimizing the satellites needed for a well-functioning quantum network, we can decrease said network's cost, thus enabling a cheaper quantum internet. In this paper, we present an optical transmittance-based routing algorithm with which it is possible to conduct successful quantum entanglement transfer between terrestrial nodes.**

***Index Terms*—quantum satellite, quantum satellite network, routing in scarce satellite networks, quantum entanglement**

I. Introduction

PUBLIC-key cryptography is a part of our everyday life. It is used as a key security component in banks, websites, and almost everything where there is a need to provide secure communication to multiple clients. With the impending arrival of quantum computers, with which (thanks to algorithms like Shor's [1]) we will be able to crack most of the public-key encryptions used today, there is an ever-growing risk to these systems.

By utilizing quantum computing, we can not only break one of today's most used encryptions (RSA) but also speed up the calculation of various problems. Using Groover's algorithm, we can find a record in unordered data in $\sqrt{N}$ time [2], or even extreme values [3]. With the help of quantum computing, we can solve problems like multi-user detection [3] or optimal resource distribution [4]. Quantum key distribution (QKD) is a part of quantum communication with which we can create theoretically unbreakable networks. These key distribution protocols suppose that the other party can and will use every tool that our current understanding of physics does not forbid. Hence it can provide lasting future proof of security.

Quantum networks although, provide one of the most secure environments for communication, their physics-enabled security has its drawbacks against classical networks. The greatest one is what provides most of its security, is the no-cloning theorem [5]. This theorem states that we cannot measure the complete state of a quantum bit without destroying it, thus we cannot make deep copies of it. This prevents us from creating routers or signal enhancers like in classical networks or broadcast quantum information. This, however, doesn't mean that we cannot create quantum communication networks. For example, by using the side effect of the bell state measurement [6], we can swap the entanglement of quantum bits [7]. This is the basis for the quantum repeaters referred to in this paper, which are detailed in the Section III-C.

Although the aforementioned quantum systems are still years away, one could, for example, save the encrypted traffic going through a busy node for him to decrypt it later. The validity of this attack vector can be easily noticed as internet users transmit information that can be valuable even in years [8]. For example, if somebody would collect the Social Security Number (SSN) of millions of American residents, it could be devastating even if the information would only be available in 20 years.

In light of these facts, there are multiple projects all over the world, from China to Europe [9–12], to build secure quantum communication networks. These early plans primarily rely on free-space quantum communication channels, which provide better coverage at a lesser infrastructure cost. We can further increase our transmission rate by using low earth orbit (LEO) satellites.

Satellite-based networks have better coverage and in some cases, a better noise rate to the channel length. Not considering the cost of technology development which is needed for a high-reliability satellite-based quantum system, one of the highest drivers of cost for these networks is the cost of launching and maintaining satellites.

With the evolution of quantum memories[13], quantum systems do not require a consistent stream of quantum bits to function. As such we could create a satellite-based quantum network that transfers the quantum data at a reasonable rate but not continuously. With this, we could enable a quantum network with as little as 32 quantum satellites instead of the hundreds needed for continuous communication [14]. In our work, we created an algorithm that maximizes the transfer rate of entangled quantum bits over scarce satellite networks. This was achieved by making every node keep its ”cargo” until the best possible next node becomes available.

The structure of the paper is as follows: in Section II we detail our data structure and the setup of the simulation. In Section III, we present our algorithm for generating routes in scarce satellite networks. Section IV concludes our paper.

The authors are with the Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, Hungary. (e-mail: andras.mihaly.1998@gmail.com, bacsardi@hit.bme.hu)

The research was supported by the Ministry of Culture and Innovation and the National Research, Development and Innovation Office within the Quantum Information National Laboratory of Hungary (Grant No. 2022-2.1.1- NL-2022-00004). L. Bacsardi thanks the support of the Janos Bolyai Research Scholarship of the Hungarian Academy of Sciences.

DOI: 10.36244/ICJ.2023.2.2

II. Related works

Satellite-based quantum networks and optimal architectures for such systems are a hot topic even in recent years. It comes as no surprise since such a network could provide global coverage. Most quantum satellite architectures fall into two categories. The first architecture exists only for creating keys between the end-nodes. This is done by generating keys between the intermediary nodes. With the use of those keys, it is possible to create a key between the end nodes. The benefits of using this architecture are a cheaper cost and simple implementation. On the other hand, this type of system can only be used for QKD and requires the users to trust each node. The second type of satellite communication architecture uses a technique called nested purification or purify-and-swap[15]. With the help of nested purification, it is possible to create entangled quantum bits in distant nodes. By using the entangled quantum bits, the end nodes can use quantum teleportation to exchange quantum bits between each other. This architecture can be used not only for QKD but for communication between quantum computers. This architecture is complex and limited by the evolution of more quantum components such as the quantum memory and the quantum entanglement generator.

One of the few recent publications that use a QKD-only architecture is the one published by the University of California and Beijing University of Posts and Telecommunications[16]. In a joint paper, the two universities proposed a two-layer satellite network. The lower layer is composed of 66 LEO satellites and the upper layer is composed of 3 geosynchronous earth orbit (GEO) satellites. In their research, they also proposed an algorithm for calculating optimal routes. As hinted before, this architecture uses a trusted node-based architecture. Using this kind of architecture means the hardware needed for the satellites is less complex. On the other hand, compromising a single intermediary node can lead to the compromise of the whole system.

As we mentioned in the first paragraph of this chapter, most research today uses an entanglement-based architecture. A highly influential research paper using this architecture was released in December 2019. ”Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet” [14] was a joint work by multiple universities around the globe. The article proposed an algorithm for determining optimal satellite configurations while maintaining continuous coverage. Their simulation consisted of 200 satellites and could achieve an average entangled quantum bit transfer of 1321/sec, which is 4755600 entangled quantum bits every hour. Due to the properties of the purify and swap architecture, the resulting satellite system's security cannot be compromised by a rouge or hacked intermediary node.

By looking at the current state of quantum satellite networks, it is clear that we will reach a working product in the near future, but it is also evident that most constellations work with a high satellite count and almost continuous coverage. These properties of the network result in an increase in its cost. In our research, we tried to minimalize the price of a network by suggesting a network composition that would require significantly fewer satellites. But with the low satellite count, our satellite architecture needs a new type of routing to function. This algorithm is detailed later in our paper.

III. Our setup

Our setup consists of two main modules: an orbital propagation and a routing module. The orbital propagation module is responsible for the simulation of satellite orbits. In addition, the routing module's main task is finding an optimal route through the satellite network.

A. Time-dependent graphs

Time-dependent graphs [17] can be related to many names, including temporal graphs, evolving graphs, time-varying graphs, historical graphs, and many more. In our research, we will use the term time-varying graphs. Time-varying graphs are perfect for modeling data networks, which change over time. We used the approach in which the weights on the edges are the time instances they are available. Meaning the edge $\xrightarrow{<t_1,t_2>}$ between nodes n_1 and n_2 shows that the node n_1 will have a valid edge to node n_2 in the time instances t_1 and t_2. Instead of time instances, it is also possible to time arrays to define a larger timeframe.

B. Data representation

In our research, we needed a structure to model the changing network of satellites. For this purpose, we have chosen the time-varying graph (TVG). Time-varying graphs are special types of graphs that change over time in a predetermined manner. In our model, the graph nodes represent the satellite and terrestrial nodes in the network. As it is illustrated in Figure 1, between nodes n_1 and n_2 we draw an edge $\xrightarrow{[t_1,t_2]\ \mu[...]}$, if there is a time interval $[t_1, t_2]$ where n_1 and n_2 are visible to each other and in that interval, the optical transmittance is $\mu_1, \mu_2, ..., \mu_{t_2-t_1}$.

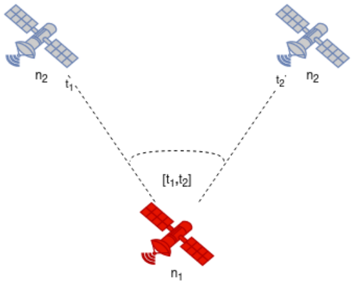


Fig. 1. Visualization of the data representation. The satellites n_1 and n_2 are represented as nodes. The changes in the visibility between them are modeled as the edge between these nodes.

C. Theoretical architecture of the quantum satellite nodes

In our work, we used an abstracted view of quantum satellites. These satellites, as detailed in Figure 2, consist of three main modules:

1) **Quantum CPU:** the quantum processor's main job is to perform the bell state measurement on the two quantum memories, swapping their entanglement [18].
2) **Quantum memory:** the quantum memory is being used to store the entangled quantum bits received from the previous node and the current node.
3) **Entangled quantum bit generator:** the entangled bit generator is responsible for providing the entangled quantum bits for the current and the next node.

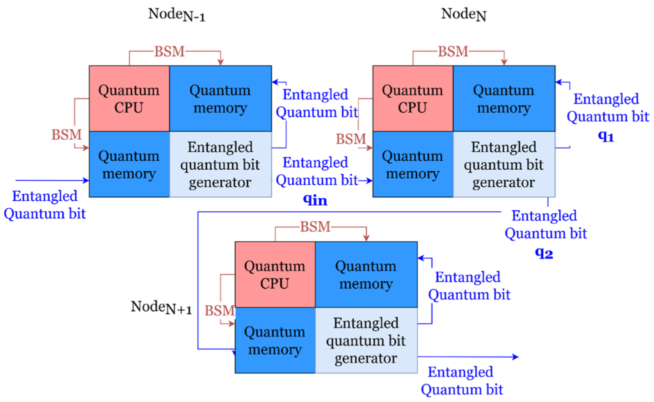


Fig. 2. Abstract model of the quantum satellite architecture consisting of three nodes.

The system works as follows: First, the entangled quantum bit generator provides an entangled pair of quantum bits q_1 and q_2 for the current Node$_N$ and the next Node$_{N+1}$. These quantum bits then are stored in the quantum memories of the nodes. Node$_N$ can transfer the q_{in} input quantum entanglement to Node$_{N+1}$ by swapping the entanglement between quantum q_{in} and q_1. After the procedure, the quantum bit at the Node$_{N+1}$ will be entangled with the quantum bit located in the quantum memory of Node$_{N-1}$.

D. Orbital propagation module

The orbital propagation module has multiple satellite orbit-related tasks. These are in the order of usage:

1) Loading the Keplerian orbital data for the satellite orbits.
2) Calculate the changes in the satellite system provided, using the orekit space dynamics library [19].
3) Generating the visibility intervals between each node.
4) Calculating the optical transmittance for each visibility interval.
5) From the optical transmittance values and visibility intervals create the time-varying graph of the system.

E. Routing module

The routing module uses the time-varying graph generated by the orbital propagation module. By using the algorithms described in Section IV, this module calculates an optimal sequence of nodes to transmit our quantum data through. The specialty of our algorithm is that it does not require the created path to be continuous between the two end nodes. It can be thought of as a postal service sending packets of quantum data (eg., quantum entanglements) between nodes, resting the data at one node until the next optimal one becomes available.

IV. Optical Transmittance Based Store and Forward Routing Algorithm

As mentioned before, our research and thus our algorithm focuses on finding the best route in sparsely populated satellite networks. We modeled the network with the use of time-varying graphs, where edges represent visibility between nodes. The edges contain the timeframes of the visibility and the optical transmittance for each timeframe. The optical transmittance was calculated with the help of QSCS [20]. The result is an extended time-varying graph (ETVG).

Our algorithm can be divided into main 4 parts:

- **Main loop**
- **FindBestRoute**
- **isViableEdge**
- **Optimize**

A. Main loop

The main loop is the starting point of our algorithm, it calls the *FindBestRoute* algorithm for each input's node each edge.

Algorithm 1 Main loop

```
    Input: ETVG, $N[...]$ list of nodes to generate paths between
    Output: Optimal paths
for each $n$ node in $N$ do
    for index $i$ of edges in $n$ do
        $FindBestRoute(ETVG, n, i)$
    end for
end for
```

B. FindBestRoute

This sub-algorithm calculates the best path for each edge of the starting node.

Algorithm 2 FindBestRoute

```
    Input: ETVG, node $n$ and index $i$
    Output: Optimal paths
$paths \leftarrow$ $i$-th edge of the start node
$out \leftarrow \{\}$
$tmp \leftarrow \{\}$
while paths can be increased do
    for $path$ in paths do
        for $edge$ in $path$ do
            if $isViableEdge(edge, path)$ then
                $opt \leftarrow Optimize(edge, path)$
                if $edge$ point to destination then
                    $out \leftarrow opt$
                else if then
                    $tmp \leftarrow opt$
                end if
            end if
        end for
    end for
end while
```

C. *isViableEdge*

The algorithm checks if the edge with the given path meets the criteria for a valid path. The path needs to meet the following criteria for the edge to be counted as a valid extension:

- The time distance between the paths first edges end and last edges start should be less than the maximum allowed.
- The edge should lead to a node the path doesn't already contain.
- The new edges end has to be later than the previous paths last edges start time

Algorithm 3 isViableEdge

```
  Input: Edge, Path
  Output: True/False
$\delta \leftarrow$ edge.startTime $-$ firstEdgeOfPath.endTime
if $\delta \geq$ global maximum path duration then
    return False
end if
if Path doesn't contain the node the edge is leading to then
    return edge.endTime $>$ lastEdgeOfPath.startTime
end if
return False
```

D. *Optimize*

This sub-algorithm uses a subset of the 13 base relations between two intervals proposed by Allen [21]. Optimization is needed in two cases. The first when the second edge finishes faster than the first one. This would mean that we are still sending data to a node that stopped transmitting forward, hence the need to cut down the said part. The second is when the second edge starts earlier than the first one. In that case, we need to cut down that part, since we cannot forward transmission that hasn't even been sent.

Algorithm 4 Optimize

```
  Input: Edge, Path
  Output: Optimized path
$path \leftarrow Path + Edge$
for each $e_1$ $e_2$ adjacent edge pairs in the path do
    $t_1 \leftarrow e1.startTime$
    $t_2 \leftarrow e1.endTime$
    $t_3 \leftarrow e2.startTime$
    $t_4 \leftarrow e2.endTime$
    if $t_4 < t_2$ then
        cut the end of $e_1$ by $t_2 - t_4$
    end if
    if $t_3 < t_1$ then
        cut the start of $e_2$ by $t_1 - t_3$
    end if
end for
```

V. RESULTS

In our research, we compared our algorithm across multiple types of satellite constellations. We used two main architecture types, cross, and retrograde, along four-four constellations. We simulated multiple ground stations covering the whole globe to get a more in-depth understanding of our algorithm. We have chosen a starting ground station, for each architecture and calculated the optical throughput for every other ground station.

By multiplying the optical transmittance for each timeframe with the current best realized photonic entangled quantum bit generators output [22] we calculated the throughput for every edge. The overall throughput of a path was determined by finding its smallest edges throughput. In our simulations, we used the following default values:

- **Default satellite orbit:** $a : 1000[km],\ e : 0.0002090,\ i : 56.0568°,\ \Omega : 0°,\ \omega : 0°,\ \theta : 18.0$
- **Max path duration:** 3600 [s]
- **Efficiency of the entangled quantum bit generator:** 3.5 [kHz]
- **Simulation Time:** 14400 [s].
- **Test ground station's locations:** Lattitude: one for every 10°, Longitude: one for every: 15°
- **Starting ground station location:** Lattitude: 0°, Longitude: 0°

A. *Input Orbits*

In our research, we modeled two types of satellite architectures along with four satellite systems with a varying number of satellites. The first one, we called Retrograde architecture since every second satellite's inclination was rotated by $180°$. The second architecture we used was the Cross architecture, here every second satellite's inclination was rotated by $90°$.

The four satellite systems we used were composed of a default Keplerian orbit rotated along the longitude of the ascending node (Ω) and argument of periapsis (ω) in increments of $45°$. The differences between the four systems are the intervals of these rotations, as detailed in Table I.

TABLE I
THE SATELLITES SYSTEMS USED IN THE SIMULATIONS. THE TABLE CONTAINS THE FOLLOWING FOR EACH SYSTEM: NAME, NUMBER OF SATELLITES, THE LONGITUDE OF THE ASCENDING NODE (Ω), AND ARGUMENT OF PERIAPSIS (ω).

Name	Number of satellites	Ω interval	ω interval
Low	12	$0 - 180°$	$0 - 180°$
LOWMid$_1$	32	$0 - 180°$	$0 - 360°$
LOWMid$_2$	32	$0 - 360°$	$0 - 180°$
MID	64	$0 - 360°$	$0 - 360°$

B. *Retrograde architecture*

The retrograde satellite architecture uses the default satellite orbit, which had its inclination shifted by $180°$ for every second satellite. By rotating the inclination of the satellite by $180°$, we get an almost frontal collision track for our satellites. Consequently, the resulting satellite visibility intervals will be the shortest that is possible at these speeds. In other words, retrograde architecture works with visibility intervals that are shorter in time but have a higher occurrence ratio. The average throughput of the systems can be seen in Figure 3. The averages here indicate the cumulation of the whole systems throughput between every terrestrial node (in this case, cities). As it can also be seen in the mentioned Figure, despite both consisting of 32 satellites, systems LOWMID1 and LOWMID2 have a different rate of average entangled quantum bits per hour (AEQ/h). As these systems differ only in the intervals of the used Ω and ω values, so we can conclude that the values used for said intervals can affect the systems AEQ/h. Apart from said differences, we can see that using the retrograde architecture, with only 32 satellites we can create a system that has an average AEQ/h of 9800. In the case of the bigger (MID) system, it could reach an average AEQ/h of almos 20000.

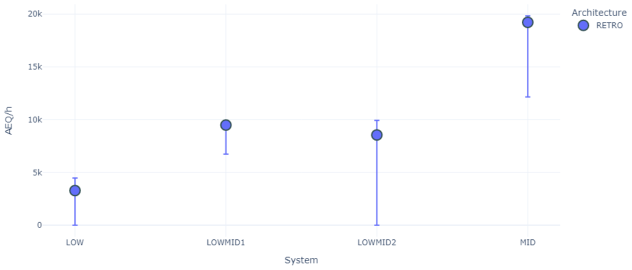


Fig. 3. Error bar plots showing the average, minimum, and maximum AEQ/h generated between the starting ground station and the test nodes for each retrograde architecture-based system. The average is noted with the blue marker, while the minimum and maximum values are indicated with the error bars.

C. Cross architecture

The cross satellite orbit architecture, like the retrograde, uses the default satellite orbit. Unlike retrograde architecture, cross-architecture shifts its orbits inclination only by 90°. By shifting by a significantly smaller value, the resulting network will produce visibility intervals that are longer in time but rarer in occurrence.

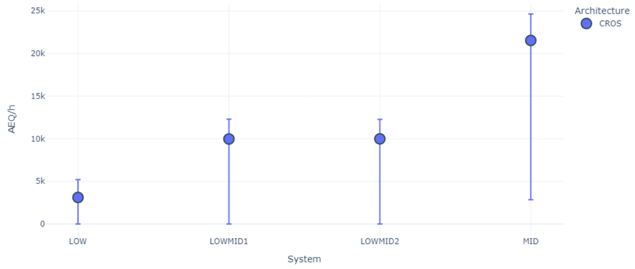


Fig. 4. Error bar plots showing the average, minimum, and maximum AEQ/h generated between the starting ground station and the test nodes for each cross architecture-based system. The average is noted with the blue marker, while the minimum and maximum values are indicated with the error bars.

As we can see in Figure 4, the resulting averages and intervals of the simulated network are significantly different. Neither LOWMID1 nor LOWMID2 satellite systems provide a full coverage, as both of their minimal AEQ/h value is 0. As it can also be seen in Figure 4, using 64 satellites we can reach an average AEQ/h of 21000, with a maximum value of more than double.

VI. Conclusion

In our research, we created 4-4 systems using two architectures. The architectures only differed in the angle of intersection between satellites. These angles were 180° in the case of the retrograde architecture and 90° in the case of the cross-architecture. All satellites systems used were only different in the intervals used for Ω and ω. Creating the systems in such a way, we could locate the variables responsible for changes in the throughput of the system. Looking at Figure 5, we can observe the differences between the two architectures. The first difference is one that was touched on in the previous chapter. By only changing the architecture used in systems LOWMID1 and LOWMID2, they performed differently in comparison to each other. In the case of cross-architecture, the both systems performed at the almost the same level but in the case of retrograde architecture, the LOWMID2 architecture performed significantly worse. Meaning different architectures synergize better with different types of systems. We can also see in Figure 5, that architectures perform differently compared to each other. In the case of systems with 16 satellites, the retrograde architecture slightly outperforms the cross-architecture, while using architectures compromised of 32 and 64 satellites, the clear winner is the cross-architecture.

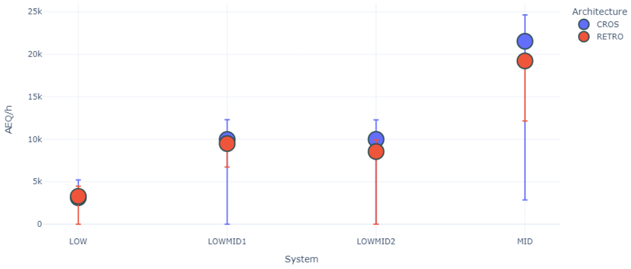


Fig. 5. The two main architectures side by side. The cross architecture-based systems are marked with blue, while the retrograde architecture-based systems are marked in red. The markers tag the average AEQ/h of the system, while the error bars visualize the minimum and maximum of said system.

In this paper, we demonstrated that by using non-continuous channels of communication it is possible to realize a quantum network over scarcely populated satellite systems.

The satellite systems presented here provide a great overview of the possible interactions between architectures and systems. Even though these interactions should be more deeply researched in their own paper.

REFERENCES

[1] Peter Shor. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”. In: *Proceedings of 35th Annual Symposium on Foundations of Computer Science* (Oct. 1996). DOI: 10.1109/SFCS.1994.365700.

[2] Lov Grover. “From Schro ̈dinger’s equation to the quan- tum search algorithm”. In: *Pramana-journal of Physics - PRAMANA-J PHYS 56* (Feb. 2001). DOI: 10.1007/s12043-001-0128-3.

[3] S. Imre. “Quantum Existence Testing and Its Ap- plication for Finding Extreme Values in Unsorted Databases”. In: *IEEE Transactions on Computers 56* (2007). DOI: 10.1109/TC.2007.1032.

[4] Sara Gaily and Sándor Imre. “Quantum Optimization of Resource Distribution Management for Multi-Task, Multi-Subtasks”. In: *Infocommunications Journal 11* (Jan. 2019), pp. 47–53. DOI: 10.36244/ICJ.2019.4.7.

[5] W. K. Wootters and W. H. Zurek. “A single quantum cannot be cloned”. en. In: *Nature* 299.5886 (Oct. 1982), pp. 802–803. ISSN: 1476-4687. DOI: 10.1038/299802a0. URL: https://www.nature.com/articles/299802a0.

[6] Charles H. Bennett and Stephen J. Wiesner. “Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states”. In: *Phys. Rev. Lett. 69* (20 1992), pp. 2881–2884. DOI: 10.1103/PhysRevLett.69.2881. URL: https://link.aps.org/doi/10.1103/PhysRevLett.69.2881.

[7] Matthäus Halder et al. “Entangling independent photons by time measurement”. en. In: *Nature Physics 3.10* (Oct. 2007), pp. 692–695. ISSN: 1745-2473, 1745-2481. DOI: 10.1038/nphys700. URL: http://www.nature.com/articles/nphys700.

[8] I. S. Kabanov et al. “Practical cryptographic strategies in the post-quantum era”. In: *Moscow, Russia, 2018*, p. 020021. DOI: 10.1063/1.5025459. URL: http://aip.scitation.org/doi/abs/10.1063/1.5025459.

[9] *Secure communication via quantum cryptography*. URL: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Secure_communication_via_quantum_cryptography.

[10] Sheng-Kai Liao et al. “Satellite-Relayed Intercontinental Quantum Network”. In: *Phys. Rev. Lett. 120* (3 2018), p. 030501. DOI: 10.1103/PhysRevLett.120.030501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.120.030501.

[11] *European Quantum Communication Infrastructure (EuroQCI) | Shaping Europe’s digital future*. en. URL: https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci (visited on 12/12/2021).

[12] Canadian Space Agency. Quantum Encryption and Science Satellite (QEYSSat). 2020. URL: https://www.asc-csa.gc.ca/eng/satellites/qeyssat.asp.

[13] Pengfei Wang et al. “Single ion qubit with estimated coherence time exceeding one hour”. en. In: *Nature Communications 12.1* (Dec. 2021), p. 233. ISSN: 2041-1723. DOI: 10.1038/s41467-020-20330-w. URL: http://www.nature.com/articles/s41467-020-20330-w.

[14] Sumeet Khatri et al. “Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet”. en. In: *npj Quantum Information 7.1* (Dec. 2021), p. 4. ISSN: 2056-6387. DOI: 10.1038/s41534-020-00327-5. URL: http://www.nature.com/articles/s41534-020-00327-5.

[15] H.-J. Briegel et al. “Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication”. en. In: *Physical Review Letters 81.26* (Dec. 1998), pp. 5932–5935. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.81.5932. URL: https://link.aps.org/doi/10.1103/PhysRevLett.81.5932.

[16] Donghai Huang et al. “Quantum Key Distribution Over Double-Layer Quantum Satellite Networks”. In: *IEEE Access 8* (2020), pp. 16087–16098. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.2966683. URL: https://ieeexplore.ieee.org/document/8959199/

[17] Yishu Wang et al. “Time-Dependent Graphs: Definitions, Applications, and Algorithms”. en. In: *Data Science and Engineering 4.4* (Dec. 2019), pp. 352–366. ISSN: 2364-1185, 2364-1541. DOI: 10.1007/s41019-019-00105-0. URL: http://link.springer.com/10.1007/s41019-019-00105-0.

[18] Jian-Wei Pan et al. “Experimental Entanglement Swapping: Entangling Photons That Never Interacted”. en. In: *Physical Review Letters 80.18* (May 1998), pp. 3891–3894. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.80.3891. URL: https://link.aps.org/doi/10.1103/PhysRevLett.80.3891.

[19] Luc Maisonobe, Véronique Pommier, and Pascal Parraud. “Orekit: an open-source library for operational flight dynamics applications”. In: *Proceedings of the 4th International Conference of Astrodynamics Tools and Techniques*. Apr. 2010.

[20] Quantum Satellite Communication Simulator. URL: https://www.mcl.hu/quantum-old/simulator/(visited on 10/03/2021).

[21] James F. Allen. “Maintaining knowledge about temporal intervals”. en. In: *Communications of the ACM 26.11* (Nov. 1983), pp. 832–843. ISSN: 0001-0782, 1557-7317. DOI: 10.1145/182.358434. URL: https://dl.acm.org/doi/10.1145/182.358434.

[22] Zichang Zhang et al. “High-performance quantum entanglement generation via cascaded second-order non-linear processes”. en. In: *npj Quantum Information 7.1* (Dec. 2021), p. 123. ISSN: 2056-6387. DOI: 10.1038/s41534-021-00462-7. URL: https://www.nature.com/articles/s41534-021-00462-7.

András Mihály graduated from Göllner Mária Regional Waldorf secondary school and earned his BSc degree in 2021. In 2020, he achieved 3rd place in the local Scientific Student Conference. He attended the 73rd International Astronautical Congress as a speaker. In 2022 he received 2nd place in the same Scientific Student Conference. He then completed his MSc in Computer Engineering at the Budapest University of Technology and Economics (BME) at the beginning of 2023. Currently, András is conducting research in the field of quantum computing.

László Bacsárdi (M’07) received his MSc degree in 2006 in Computer Engineering from the Budapest University of Technology and Economics (BME) and his PhD in 2012. He is a member of the International Academy of Astronautics (IAA). Between 2009 and 2020, he worked at the University of Sopron, Hungary in various positions including Head of Institute of Informatics and Economics. Since 2020, he is associate professor at the Department of Networked Systems and Services, BME and head of Mobile Communications and Quantum Technologies Laboratory. His current research interests are quantum computing, quantum communications and ICT solutions developed for Industry 4.0. He is the past chair of the Telecommunications Chapter of the Hungarian Scientific Association for Infocommunications (HTE), Vice President of the Hungarian Astronautical Society (MANT). Furthermore, he is member of AIAA, IEEE and HTE as well as alumni member of the UN established Space Generation Advisory Council (SGAC). In 2017, he won the IAF Young Space Leadership Award from the International Astronautical Federation.

Effect of Path QoS on Throughput Aggregation Capability of the MPT Network Layer Multipath Communication Library

Naseer Al-Imareen, and Gábor Lencse

***Abstract*—An increase in the use of smart and portable devices like smartphones, laptops, and tablets has led to a rise in the number of network interfaces and thus the number of possible channels for communication. However, the current approach over the Internet only employs a single path for a communication session. As an innovative and promising method for real-time transmission based on GRE-in-UDP encapsulation, which provides an IPv4 or IPv6 tunneling mechanism, this paper presents multipath throughput testing for the MPT network layer multipath communication library. We investigated the effectiveness of MPT's channel capacity aggregation while dealing with wired channels and examined scenarios in symmetric and asymmetric paths. Our network throughput measurements showed that MPT can efficiently aggregate the capacities of both symmetric and asymmetric paths. In this paper, we established a network topology that included a server, which we used for generating various quality of service (QoS) metrics. We measured how latency, transmission speed, packet loss rate, jitter, and the setting of the path weights influence throughput aggregation capability of the MPT communication library.**

***Index Terms*—GRE-in-UDP, MPT, MPTCP, Tunneling, Throughput, QoS.**

I. Introduction

Many factors contribute to the popularity of multipath approaches. We use many IT gadgets daily (smartphones, tablets, laptops) with more than one network interface (Wi-Fi, 4G/5G, Ethernet). However, the TCP/IP protocol stack was designed to support only a single interface per communication session. Thus, the current environment of the Internet allows only a single path to transfer packets in a communication session. The single-path connection technologies cannot use the advantages of multiple interfaces. This calls for the creation of multipath-friendly infrastructure and protocols for use in the communication session. Multipath communication has emerged as a hot research topic in recent years. When multiple interfaces are allowed in a single communication session, throughput increases dramatically and generally. The multipath technique has several promising solutions, such as MPT [1] and MPTCP [2]. MPT can be a key technology for making the most of the various connection points offered by today's electronic gadgets for exchanging information. MPT operates at the network layer via the GRE-in-UDP encapsulation. In contrast, MPTCP implements the TCP protocol at the transport layer [3]. Using the network layer for multipath communication is the focus of our paper. The 32-bit and 64-bit versions of MPT are available for free download from [4].

This paper is an extension of our former conference paper [5] in which we studied the efficiency of channel capacity aggregation of MPT using a single physical switch. In this paper, we use a more complex test network to measure how latency, transmission speed, packet loss rate, and jitter affect the throughput aggregation of MPT. The main contribution of our paper is analyzing how the various path quality of service (QoS) metrics, and the setting of the path's weights, affect the throughput aggregation capability of the MPT network layer communication library using both symmetric and asymmetric paths.

The rest of this paper is organized as follows. In section II, we give a brief introduction to MPT. In the third section, we provide an overview of the related work. The fourth section explains our experimental test environments in both hardware and software configuration. The fifth section includes the various MPT measurements and results. Finally, the sixth section is a discussion and future directions of research, and this is followed by the conclusion.

II. Brief Overview of MPT

MPT implements multipath communication in the network layer. It was developed and designed by a research group at the University of Debrecen, Hungary [1]. MPT takes advantage of GRE-in-UDP capabilities to provide multipath tunneling. MPT can act as a router through which packets can be routed between different networks through tunnel endpoints. This feature is the establishment of a multipath connection from one site to another. The IP version of the tunnel is independent of the IP version of the path so that the MPT can be used for IPv6 transition purposes [6], [7] and [8].

The MPT library creates a tunnel interface to serve as a logical interface for communication between hosts. The logical interface is mapped to the physical interfaces directly by MPT software [9][10]. When an application sends an IP

Naseer Al-Imareen, is with the Department of Telecommunications, Széchenyi István University, Győr, Hungary; Computer Science, Al-Qadisiyah University, Iraq (e-mail: al-imareen.naseer@sze.hu).

Gabor Lencse is with the Department of Telecommunications, Széchenyi István University, Győr, Hungary (e-mail: lencse@sze.hu).

DOI: 10.36244/ICJ.2023.2.3

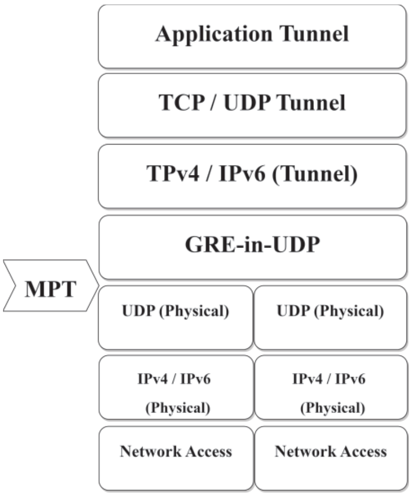


Fig. 1. The Conceptual Architecture of MPT-GRE [1].

packet, it uses the address of the tunnel path, i.e., the address of the logical interface. Thus, there is no need to modify the applications.

The fact that the MPT library enables communication through the tunnel interface helps in mapping between the tunnel interface and physical interfaces. For example, when changing the physical interface address or the physical interface itself, the application does not know about this change. It continues to work through the tunnel interface where the MPT library reorganizes the mapping from the logical interface to the physical interface based on the latest update. Transmission of video in high quality in real-time is one of the challenges that can be solved using multipath technology. The developers and researchers of solutions have proposed to produce and develop technologies for the multipath problem that are essential in facing this challenge.

The MPT library provides a typical solution for multipath by giving a logical path (tunnel) that is initialed in the terminal hosts to define the socket where the MPT library reads the packets coming at the logical interface (IPv4 or IPv6) originating from the sender host. This packet will be wrapped in a new GRE on the UDP part before being sent over a potential physical route [11]. The MPT-GRE conceptual architecture can be seen in Fig. 1. This figure displays the MPT's layered design. MPT expands upon the GRE-in-UDP design by permitting multiple physical channels [12]. MPT is comparable to MPTCP in this regard, but unlike MPTCP, it employs UDP in the underlying layer, builds on GRE-in-UDP, and provides a tunnel IP layer over which both UDP and TCP can be used.

III. Literature Review

The aggregation capability of the MPT network layer communication library is among the main challenges in different fields that help examine the efficiency of multipath technology. Almási and Szilágyi [13] proved the MPT library's effective throughput aggregation property in IPv6 and mixed (i.e., protocol version transition) contexts. The main goal was to check how well the MPT tool handled throughput in IPv4, IPv6, and hybrid network environments. They set up a measurement system with four connection pathways for communication hosts. Different data transmission sizes and symmetrical and asymmetrical bandwidth rates were used to test the throughput performance. The test results showed that the MPT multipath environment correctly adds up the throughput capacity of each physical path, even though the results from the dissimilar protocol versions were different.

Kovács [14] tested the ability to throughput aggregate an MPT communication library and compared it with multipath in TCP up to 12 connections with all possible combinations of IPv4 and IPv6. He found that throughput scaled up linearly. The researcher also found the possibility of using 12 NICs using the MPT communications library at a speed of 100Mbps on relatively old computers. The same author has expanded his measurements to 1 Gbps speed links, and he has also prepared a mathematical model for the throughput aggregation capability of MPT and MPTCP in [15].

Using multiple scenarios carried out on quad-path Gigabit Ethernet and IPv4/IPv6 connections, the authors of [8] compared the MPT solution to the MPTCP, which was used as a benchmark. The primary benefit and ideal use of the MPT is UDP multimedia transport. However, the solution's throughput performance is more than sufficient.

Szilágyi et al. [16] compared two technologies MPTCP and MPT that support multipath communication sessions. The researchers performed an efficiency analysis of the 10 Gigabit Ethernet dual-path scenario for two techniques providing multipath connectivity. This could be helpful in data center environments by increasing efficiency and enhancing user experience in the cloud. Also, these multipath technologies can improve Gigabit Ethernet throughput in the data center.

The authors of [17] addressed guaranteeing the QoS of transmission of Network-based solutions for Multipath TCP. By using the advantage of Software-defined networking technology, they created a method that can allocate the available paths deterministically by combining network sites from the network's perspective, metrics like link bandwidth and latency can be gathered to assess the overall health of the system. By comparing the needed and the available resources in the controller, the endpoint will be given the optimum number of subflows. Their improved method addresses some multithreading issues and has been shown to increase network throughput. To lower the latency of the client-server connection, Google recently developed the Quick UDP Internet Connection (QUIC) protocol, which integrates the features of HTTP/2, TLS, and TCP directly via UDP [18]. The authors [19] suggested a new technique for measuring QUIC's passive delay that combines a delay bit and a spin bit. They have demonstrated that this new methodology can solve the drawbacks of measurements based solely on the spin bit. However, this brand-new delay-bit technique only adds one bit to the spin bit.

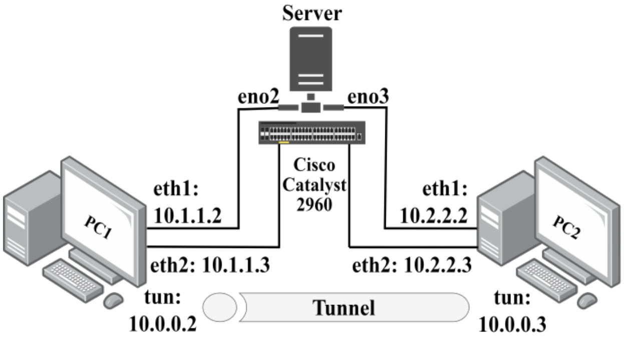


Fig. 2. Measurement Network Topology.

IV. Experimental Test Environment

A. Hardware and Fundamental Configurations

We have built a test system for measurements and analysis as shown in Fig 2. We used two Dell Precision Workstation computers with the following specification:

- Motherboard with Intel 5000X chipset.
- 8 GB 533MHz DDR2 SDRAM.
- Intel Xeon 5140 2.33 GHz dual core processors.
- NIC 1: Broadcom NetXtreme BCM5752 Gigabit Ethernet controller.
- NIC 2: Intel PT Quad 1000 type four-port Gigabit Ethernet controller. (Two ports were used for the experiments.)

We used a server to emulate various QoS issues and a Cisco Catalyst 2960 switch [20] to link the other two interfaces and limit the transmission speed to 100Mbps. The IP address configuration of our test network is also shown in Fig. 2. Two independent paths were established between the two hosts (eth1, eth2) and the logical interface (tun0) was provided by the MPT software. Debian 8.11 GNU / Linux operating system was installed on both computers, as this version is compatible with precompiled library files from 2019. The intent of this measurement network was to examine the throughput aggregation efficiency of the MPT software and to monitor and verify the effect of various QoS parameters.

B. MPT Software Configuration

The MPT implementation contains two versions (32-bit and 64-bit). In our paper, the mpt-gre-lib64-2019.tar.gz version was used. We have downloaded the MPT from [4]. We had to edit two configuration files (the paths are relative to the installation directory of MPT). The first file `conf/interface.conf` was:

```
; ####### General Interface Information #######
  60456         # The local cmd UDP port number
  2             # the interfaces number
  1             # Accept remote request
; MPT software make mptsrv as a server
  25            # cmd_timeout
; ############ Information tun0 ##############
  tun0          # Name of tunnel interface
  1440          # Maximum Transfer Unit
  10.0.0.2/24   # IPv4 address and prefix length
```

The same configuration method in the above file was used for the other interface on the second computer. Different types of tunnels files were placed in independent connection files. Moreover, all the information regarding IP addresses and a prefix length for each tunnel created by MPT software were prepared.

Additionally, the session connection file was prepared and configured in which the connection configurations IPv4 over IPv4 are defined in the `conf/connections /IPv4.conf` file:

```
; ####### Connections Info. ########
  1             # Connections Num.
; ####### Connection Details #######
MPT_Connection  # Connection Name
3               # Permission Send (1)/Receive (2)
4               # The Version of IP
10.0.0.2        # Local_IP
50230           # Local_Port
10.0.0.3        # Remote_IP
50230           # RDP (Remote_Data_Port)
60456           # UDP Port Number_Remote
2               # Paths_Num.
0               # Networks_Num
5               # Time of Keepalive Message
5               # Dead_Timer (sec)
0               # Status of Connection
0               # Auth_Type
0               # Auth_Key
; ########### Path0 info. ##########
eth1            # Interface Name
4               # The Version of IP
10.1.1.2/24     # Public IP
10.1.1.2        # Gateway_IP
10.1.1.3/24     # Remote IP
5               # Keepalive Time
25              # Dead Time
100             # Weight_out
100             # Weight_in
1               # CMD_default
; ####### Path1 information ########
eth2            # Interface Name
4               # IP_Version
10.2.2.2/24     # Public IP
10.2.2.2        # Gateway_IP
10.2.2.3/24     # Remote IP
5               # Keepalive Time
25              # Dead Time
100             # Weight_out
1               # Weight_in
1               # CMD_default
0               # Path status
```

The remaining paths for this connection were prepared and configured in the same manner that was adopted for the above two paths. It is worth noting that the configuration files must adhere to a tight structure, including comment-only lines. In [6], the researchers suggested that this be adjusted for the most widely used freestyle configuration files using keyword parsing.

V. MPT Measurements and Results

To examine and analyze the effect of path QoS on the throughput aggregation capability of the MPT network layer multipath communication library, more scenarios were implemented using the iPerf3 [21] real-time network performance measurement tool. It is a cross-platform, open-

TABLE I
THROUGHPUT OF ASYMMETRIC PATHS WITH DELAY APPLIED TO BOTH NETWORK INTERFACES OF THE SERVER

Delay Interface	0ms	10ms	20ms	30ms	40ms	50ms
eth1	9.9	9.8	9.79	9.77	9.72	9.39
eth2	94.8	94.7	94.7	94.8	94.8	94.7
tun0	103.5	98.61	88.71	78.73	66.16	52.65

TABLE II
THROUGHPUT OF ASYMMETRIC PATHS WITH DELAY APPLIED TO ONE NETWORK INTERFACE OF THE SERVER

Delay Interface	0ms	10ms	20ms	30ms	40ms	50ms
eth1	9.9	9.8	9.8	9.8	9.8	9.7
eth2	94.8	94.8	94.7	94.8	94.8	94.7
tun0	103.6	102	98.45	93.52	90.55	82.99

source client-server program that may be used to test the throughput between two hosts. We used the following style commands on the client side:

```
iperf3 -c 10.2.2.2 -t 30 -f M
```

This command ran a 30-sec experiment and returned the throughput in MB/sec units. The server, on the other hand, was launched with the following command line:

```
iperf3 -s -f M
```

We applied the additional server to be able to adjust various QoS metrics of the bypassing traffic using the *tc* tool of Linux. We experimented with different values of delay, packet loss, and different speeds. The MPT server program allocates the outgoing packets among the network paths according to their weights; in the asymmetric paths, we assigned each path a weight equal to its transmission speed except for the last experiment when we tested the effect of proper and improper weight settings.

A. Experiments with Network Delay

We generated various delays, where the *x* millisecond delay was set to 10ms, 20ms, 30ms, 40ms and 50ms.

```
tc qdisc add dev eth1 root netem delay xms
```

Table I shows the effect of delay on the throughput where the delay was added to both network interfaces of the server. (It means that the packets were delayed in both directions.) Analyzing the results shows that while the effect of the delay on the throughput of the path was minor (it was reduced from 9.9Mbps to 9.39Mbps), its effect on the tunnel was more significant, where the throughput reduced from 103.5Mbps (with no delay) to 52.65Mbps (with 50ms delay).

On the other hand, we added the delay on one of the two network interfaces of the server. The results in Table II show the effect of delay on the throughput. Analyzing the results shows a lower throughput effect on the delayed port (reduced from 9.9Mbps to 9.7Mbps) compared to the previous experiment when the delay was added to both ports. Additionally, the throughput effect on the tunnel (reduced from 103.6Mbps with no delay to 82.99Mbps with a 50ms delay) was also lower compared to the previous experiment.

TABLE IV
THROUGHPUT OF ASYMMETRIC PATHS WITH DIFFERENT PACKET LOSS RATES

Packet loss Interface	0 %	1%	2%	3%	4%	5%
eth1	9.8	9.43	9.33	8.7	7.7	4.6
eth2	94.8	94.8	94.8	94.8	94.7	94.8
tun0	103.5	24.5	13.9	9.02	6.1	4.1

B. Experiments with Transmission Speed Limit

We applied various transmission speed limitations, where *x* was set to 10Mbps, 20Mbps, …, and 100Mbps using Token Buffer Filter (TBF) to influence traffic speed. The data transmission speed was controlled by applying rate-limiting instructions to both network interfaces of the server using the following command:

```
tc qdisc add dev eno2 root tbf rate x latency 400ms
```

We always allocated the path weight equal to its transmission speed. Table III shows the effect of using asymmetric paths with different transmission speeds. Analyzing the results shows that the value of tunnel throughput is very close to the sum of the path throughputs. We can conclude that the aggregation is very efficient if the weight of the paths is equal to their speeds. Please refer to Section V.E for our experiments using weights that are different from the path speed.

C. Experiments with Packet Loss

We tested various packet loss cases as follows: the percentage of lost data x was set to 1%, 2%, 3%, 4% and 5%. The packet loss metric was added to both network interfaces of the server using the following command:

```
tc qdisc add dev eno2 root netem loss x
```

Table IV shows the effect of packet loss on the throughput. Analyzing the results shows that the effect of the packet loss on the throughput of the individual paths was negligible. However, the effect on the throughput of the tunnel was clearly obvious, where the throughput reduced from 103.5 Mbps (with no packet loss) to 4.1 Mbps (with 5% packet loss). This caused serious performance issues for the tunnel in MPT communication.

TABLE III
THROUGHPUT OF ASYMMETRIC PATHS WITH DIFFERENT TRANSMISSION SPEEDS

Speed Interface	10Mbps	20Mbps	30Mbps	40Mbps	50Mbps	60Mbps	70Mbps	80Mbps	90Mbps	100Mbps
eth1	9.84	19.9	29.9	39.9	49.8	59.7	69.5	78.9	88.6	94.8
eth2	94.7	94.7	94.7	94.7	94.7	94.7	94.7	94.7	94.7	94.8
tun0	103.4	112.7	121.9	132.2	140.3	149.6	159	168	177.2	186

TABLE V
JITTER OF SYMMETRIC AND ASYMMETRIC PATHS

Interfaces	Jitter (ms)	
	Symmetric	Asymmetric
eth1	0.104	0.132
eth2	0.111	0.118
tun0	0.179	0.158

D. Experiments with Jitter

We considered two successive packets that were sent to the traffic, $C_0$and C_1. For packet C_j , $j = 0{,}1$ and node $k = 1, \dots, n$, let $T_j^{in}(k)$ and $T_j^{out}(k)$ be the times of incoming and departure packets of C_j at node k, let $W_j(k)$ be the waiting time of C_j at node k, and finally let $\Delta_k = \left(W_1(k) - W_0(k)\right)$ be the variation of the inter-packet delay at node k. The jitter is defined as follows [22]:

$$J_{[1..n]}(T) = E\left[\,\left|\sum_{k=1}^{n}\left(W_1(k) - W_0(k)\right)\right|\,\right]=$$

$$= E\left[\,\left|\ \sum_{k=1}^{n}\Delta_k\ \right|\,\right] \qquad (1)$$

Consequently, the jitter is clarified as the predicted absolute value of the total packet delay fluctuations imposed by each node along the route from source to destination. As a lower jitter score indicates a more constant and dependable response time, it is safe to assume that a connection is good.

Higher jitter scores indicate more noticeable variations in reaction times [23], [24].

We tested various situations where 20 packets were sent during the second topology and in the case of symmetric and asymmetric paths from the source to the destination.

We calculated the round-trip times (RTT) of symmetric paths, representing the network latency that it takes for a request to go from the first node to the destination and back again. This time variation, expressed in milliseconds, affects the typical time of transmitting data packets when it is clear and large.

The jitter was calculated using equation (1). It was found that the variance in the jitter was good [25] because it was less than 30ms, as shown in Table V. The results proved the reliable operation of MPT multipath communication library in this situation because in both cases the jitter value was a small score.

E. Experiments with Various Path Weights

We have measured the throughput of the tunnel for different cases, where the path speeds were tested from 10Mbps to 100Mbps. For each path, we examined different weights from 10 to 100. The speed and weight of the second path was always kept constant at 100Mbps and 100, respectively (Fig. 3 shows the results). It needs to be noted that we also measured the throughputs of the individual paths. It was about 94.8Mbps for a 100Mbps link and 9.85Mbps for a 10Mbps link.

On the one hand, using proper weights (that is, the weight of the path is equal to the speed of the path) the throughput aggregation is nearly perfect. The throughput of the tunnel is close to the sum of the throughput of the paths. Let us see two extreme examples:

- When the first path had 100Mbps speed and 100 weight, the throughput was 186Mbps, nearly the sum of the throughputs of the two individual paths.
- When the first path had 10Mbps speed and 10 weight, the throughput was 103.4Mbps, nearly the sum of the throughput of the two individual paths.

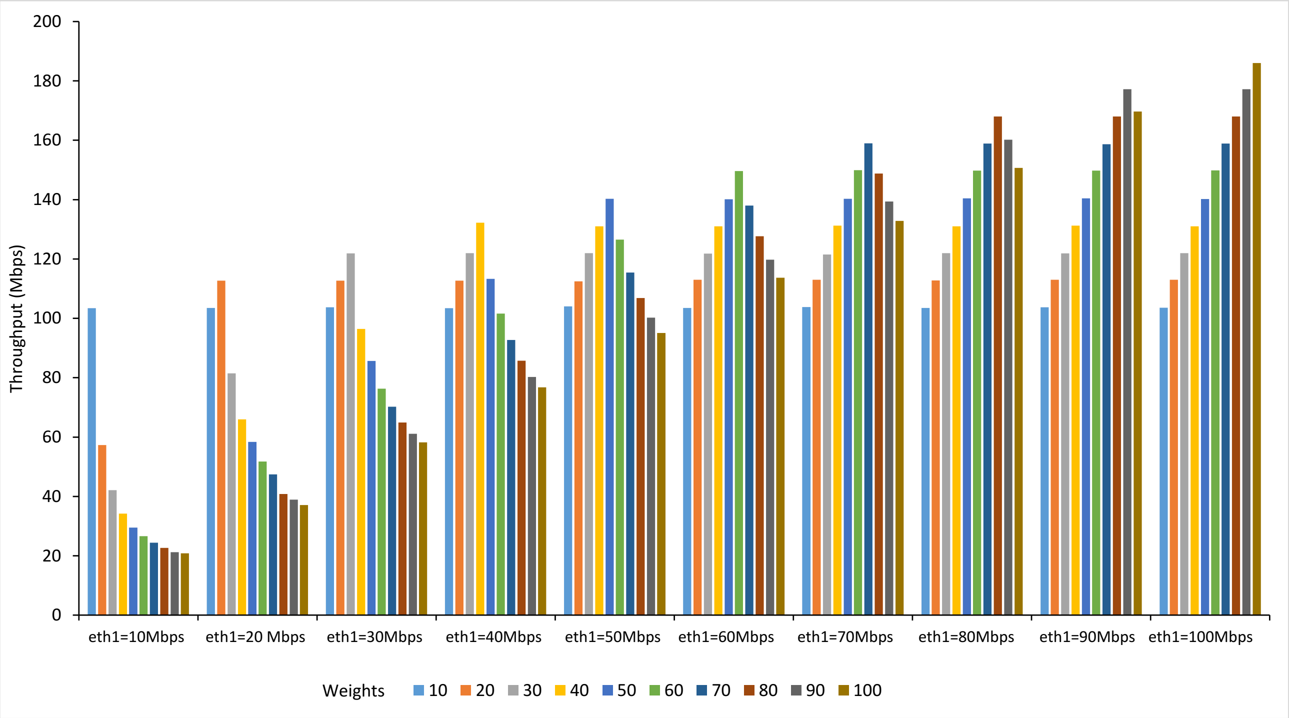


Fig. 3. The tunnel throughput as a function of different transmission speeds and weights for path 1.

On the other hand, any improper weight setting deteriorates the throughput aggregation capability of MPT. Let us see two extreme examples:

- When the first paths had 100Mbps speed and 10 weight, the throughput was 103.6Mbps, that is, the first path could contribute to the throughput only as if it were a 10Mbps path.
- When the first path had 10Mbps speed and 100 weight, the throughput was 20.8Mbps, that is, the second path could contribute to the throughput only as if it were also a 10Mbps path.

In other words, if equal weights are used for asymmetric paths, the faster link can contribute to the throughput as much as the slower link.

VI. Conclusion

We have tested the channel aggregation capability of the MPT library, which provides a network layer multipath solution based on GRE-in-UDP between two hosts with the possibility of using any transport layer protocol (TCP or UDP). Our test system enabled us to experiment by changing various QoS metrics (latency, transmission speed, packet loss rate, and jitter) and examine how their different values affect the throughput aggregation capability of the MPT network layer multipath communication library. We found that the distribution of the outgoing packets among the links according to their weights makes the throughput of the tunnel close to the sum of the throughput of the two paths. However, improper weights, as well as increasing delay and frame loss rate of one of the paths, may cause a significant deterioration of the throughput of the tunnel.

Acknowledgement

The authors thank John Kowalchuk, Széchenyi István University, for the English language proofreading of the manuscript.

References

[1] Almási, B., Lencse, G., and Szilágyi, S., “Investigating the multipath extension of the GRE in UDP technology,” *Comput. Commun.*, vol. 103, pp. 29–38, 2017. DOI: 10.1016/j.comcom.2017.02.002

[2] Ford, A., Raiciu, C., Handley, M., and Bonaventure, O., “TCP extensions for multipath operation with multiple addresses”, IETF, Jan. 2013, RFC 6824.

[3] Jabbar, N. and Lencse, G., “An Overview of the multipath technologies, their importance and types,” *Proceedings of The Technical University of Sofia*, 72(1), pp. 21–28, 2022. DOI: 10.47978/TUS.2022.72.01.004

[4] Fejes, F., “MPT – multi-path tunnel”, precompiled version can be downloaded from: http://github.com/spyff/mpt, 2019.

[5] Jabbar, N. and Lencse, G., “Measurement and analysis of MPT multipath throughput in wire channels,” *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, pp. 1–5, IEEE, 2022. DOI: 10.1109/ICECCME55909.2022.9987956

[6] Lencse, G. and Kovács, Á., “Advanced measurements of the aggregation capability of the MPT network layer multipath communication library,” *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, vol. 4, no. 2, pp. 41–48, 2015. DOI: 10.11601/ijates.v4i2.112

[7] Szilágyi, S., Fejes, F., and Katona, R., “Throughput performance comparison of MPT-GRE and MPTCP in the Fast Ethernet IPv4/IPv6 environment,” *Journal of Telecommunications and Information Technology*, vol. 2, pp. 53–59, 2018. DOI: 10.26636/jtit.2018.122817

[8] Szilágyi, S., Bordán, I., Harangi, L., and Kiss, B., “Throughput performance comparison of MPT-GRE and MPTCP in the gigabit Ethernet IPv4/IPv6 environment,” *J. Electra. Electron.* Eng., vol. 12, no. 1, pp. 57–60, 2019.

[9] Lencse, G. and Kovács, Á., “Testing the channel aggregation capability of the MPT multipath communication library”, *World Symposium on Computer Networks and Information Security 2014 (WSCNIS 2014)*, Hammamet, Tunisia, Paper ID: 1569946547, 2014.

[10] Gál, Z., Almási, B., Dabóczi, T., Vida, R., Oniga, S., Baran, S., & Farkas, I., “Internet of things: application areas and research results of the FIRST project”, *Infocommunications Journal*, vol. 6, no. 3, pp. 37–44, 2014.

[11] Szilágyi, S. and Bordán, I., “Throughput performance measurement of the MPT-GRE multipath technology in emulated WAN Environment,” *CEUR Workshop Proc.*, vol. 2874, pp. 187–195, 2021.

[12] Szilágyi, S. and Bordán, I., “Investigating the through put performance of the MPT-GRE network layer multipath library in emulated WAN environment,” *Acta Technica Jaurinensis*, vol. 15, no. 1, 2022. DOI: 10.14513/actatechjaur.00639

[13] Almási, B. and Szilágyi, S., “Investigating the performance of the MPT multipath communication library in IPv4 and IPv6,” *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, vol. 5, no. 1, pp. 53–60, 2016. DOI: 10.11601/ijates.v5i1.148

[14] Kovács Á., “Comparing the aggregation capability of the MPT communications library and multipath TCP”, *2016 7th IEEE International Conference on Cognitive Infocommunications (CogInfoCom)*, pp. 157–162, 2016. DOI: 10.1109/CogInfoCom.2016.7804542

[15] Kovács Á., “Evaluation of the Aggregation Capability of the MPT Network Layer Multipath Communication Library and Multipath TCP”, *Acta Polytechnica Hungarica*, vol. 16, no. 6, pp. 129–147. DOI: 10.12700/APH.16.6.2019.6.9

[16] Szilágyi, S., Bordán, I., Harangi, L., and Kiss, B., “Throughput performance analysis of the multipath communication technologies for the cloud,” *Journal of Electrical and Electronics Engineering*, vol. 12, no. 2, pp. 69–72, 2019

[17] Gao, K., Xu, C., Qin, J., Yang, S., Zhong, L., and Muntean, G., “QoS-driven path selection for MPTCP: A scalable SDN-assisted approach,” *2019 IEEE Wireless Communications and Networking Conference (WCNC)* pp. 1–6, IEEE, 2019. DOI: 10.1109/WCNC.2019.8885585

[18] De Coninck, Q., and Bonaventure. O., “Multipath QUIC: Design and Evaluation,” *In Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies (CoNEXT '17)*. Association for Computing Machinery, New York, NY, USA, pp. 160–166. DOI: 10.1145/3143361.3143370

[19] Bulgarella, F., Cociglio, M., Fioccola, G., Marchetto, G., and Sisto, R., “Performance measurements of QUIC communications,” *In Proceedings of the Applied Networking Research Workshop (ANRW '19)*. Association for Computing Machinery, New York, NY, USA, pp. 8–14. DOI: 10.1145/3340301.3341127

[20] “Cisco Catalyst 2960 Series Switches.” Cisco. URL https://www.cisco.com/c/en/us/support/switches/catalyst-2960-series-switches/series.html.

[21] Mortimer, M., “Iperf3 documentation,” 2018. https://buildmedia.readthedocs.org/media/pdf/iperf3-python/latest/iperf3-python.pdf

[22] Brun, O., Bockstal, C., and Garcia, J. M., “A simple formula for end-to-end jitter estimation in packet-switching networks,” *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*, pp. 14–19, IEEE, 2006. DOI: 10.1109/ICNICONSMCL.2006.34

[23] Castro, M., Márquez, L., and Márquez, J., "A comparative analysis of QoS parameters measurement applying packet scheduling algorithms on Cisco 2800 Router with Static Routing," *2020 6th International Conference on Science in Information Technology (ICSITech)*, pp. 23–28, IEEE, 2020. DOI: 10.1109/ICSITech49800.2020.9392032

[24] Al-Shaikhli, A., Esmailpour, A., and Nasser, N., "Quality of service interworking over heterogeneous networks in 5G," *2016 IEEE international conference on communications (ICC)*, pp. 1–6, IEEE, 2016. DOI: 10.1109/ICC.2016.7510913

[25] Armitage, G., and Stewart, L., "Limitations of using real-world, public servers to estimate jitter tolerance of first-person shooter games," *Proceedings of the 2004 ACM SIGCHI International Conference on Advances in computer entertainment technology*, pp. 257–262, 2004. DOI: 10.1145/1067343.1067377

Naseer Al-Imareen (received his MSc in Computer Science at the Informatics Institute for Graduate Studies of Baghdad (Iraq) in 2019.
He has worked for the Department of computer science, Al-Qadisiyah University in Iraq since 2008. He taught computer networks, data structure, operating systems, and web design. Now, he is a PhD student at Széchenyi István university of Győr, Hungary. The area of his research includes the performance analysis of computer networks and investigation of quality of service.

Gábor Lencse received his M.Sc. and Ph.D. degrees in computer science from the Budapest University of Technology and Economics, Budapest, Hungary in 1994 and 2001, respectively.
He works for the Department of Telecommunications, Széchenyi István University, Győr, Hungary since 1997. He is now a professor. He is also a part time Fellow at the Department of Networked Senior Research Systems and Services, Budapest University of Technology and Economics since 2005. His research interests include the performance and security analysis of IPv6 transition technologies.

Ultra Wideband-based wireless synchronization of IEEE 1588 clocks

Gergely Hollósi, and István Moldován

Abstract—**Time-Sensitive Networking (TSN) requires clock synchronization superior to the well-known Network Time Protocol (NTP). The IEEE 802.1AS-2020 used for synchronization in TSN networks is based on the IEEE 1588-2019 standard (also known as Precision Time Protocol, PTP) defines methods and tools to perform sub-microsecond time synchronization over vari- ous communication channels. However, the IEEE 1588 implementation is commonly used with wired communication protocols, although there are use cases that could gain an advantage from a wireless solution. This paper investigates the possibility of PTP clock synchronization through wireless Ultra Wideband (UWB) communication. UWB excels where other wireless technologies are lacking: it provides high accuracy timestamping even if multipath propagation is present. The method is evaluated using commercial, well-accessible cheap hardware, resulting in the order of 10-nanosecond accuracy. The paper also highlights the main error components and requirements for improving wireless PTP synchronization.**

Index Terms—**IEEE 1588, UWB, PTP, TSN, clock synchronization.**

I. Introduction

Precise and accurate synchronization is gaining more and more attention in actual industrial internet-of-things (IIoT) and a couple of different use-cases, including real-time applications like nuclear fusion control, mobile communication, substation automation, and, modern manufacturing plant [1], [2]. The well-known Network Time Protocol (NTP) was designed to perform time transfer in IT services, and its accuracy is in the millisecond range. However, new services require sub-millisecond accuracy, e.g., microsecond or, in some cases, nanosecond accuracy [2], [3]. The IEEE 1588-2019 standard [4] (commonly known as the Precision Time Protocol – PTP) addresses the topic of sub-microsecond accurate clock synchronization over a communication network. In most cases, these accurate clock synchronization solutions are implemented on a wired network with PTP. There are many wireless implementations based on GPS synchronization, which are also capable of sub-microsecond clock synchronization, but they have significant limitations for indoor applications. Therefore, wired PTP solutions are favored for indoor clock synchronization applications. Still, there are advantages of a wireless clock synchronization solution in an indoor environment for validation and wireless master clock purposes. The industrial standard to validate clock synchronization accuracy in PTP networks is based on PPS (Pulse Per Second) signals. During the validation, the PPS signal of the clock of the synchronized device can be compared to the PPS signal of a reference clock, from which the synchronization accuracy can be measured. For a grand master reference, GPS is widely applied, however, it is prevalent that GPS cannot be an option in an indoor environment, while the wired network's PPS signal transmission requires additional cabling and network configuration. Such challenges open the path for wireless PTP validation where there is no need for additional cabling and offer a flexible solution. Besides validation, wireless PTP can be utilized as a master clock to eliminate non-transparent PTP devices from the PTP network, also there is no need for cabling; existing network devices do not have to be replaced and it can be significantly cheaper compared to wired PTP system implementations.

Present paper proposes a method to synchronize local PTP clocks by means of wireless UWB communication. While synchronizing UWB clocks is a widely studied topic, using UWB communication for synchronization of PTP enabled clocks of Ethernet devices is a rarely researched area. The main advantage of the presented method is that the PTP clocks then readily can be used as master clocks in a PTP network.

The paper is structured as follows: The related works present the core concepts of IEEE 1588 including its application areas, wired and wireless PTP implementations and the introduction of the UWB technology. Besides the general methodology, there are many specific implementation challenges, which are presented in a separate section. The evaluation section shows the results of the UWB-based PTP clocks' synchronization errors and describes the origins of these errors.

II. Related works

The PTP standard provides tools to synchronize a so-called slave clock to a master clock. Here, only the end-to-end solution is presented, as follows. The standard uses two essential messages to achieve end-to-end synchronization (see Fig. 1), a *Sync* message and a *Delay_Req* message. The *Sync* message is sent by the master, and the master notes the transmission (TX) timestamp (t_1) of the message. The slave device receives the message and saves the receive (RX) timestamp (t_2) of the message. In case of one-step implementation, the TX timestamp is embedded in the *Sync* message, while for two-step implementation an auxiliary message (*Follow_Up*) is used to send the TX timestamp to the slave. While the clock drift (the frequency difference) can be derived from the

The authors are with the Department of Telecommunications and Media Informatics, Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Budapest, Hungary.
(e-mail: hollosi.gergely@vik.bme.hu)

DOI: 10.36244/ICJ.2023.2.4

Sync message, an additional *Delay_Req* message is required to estimate the clock offset. The *Delay_Req* is sent by the slave at t_3 and received by master at t_4, which is sent back to the slave in an auxiliary message *Delay_Resp*. From the recorded timestamps, the clock offset and clock drift can be calculated.

To achieve micro- or nanosecond accuracy, software-only solutions are insufficient, thus hardware-aided methods are preferred. Hardware-aided methods make it possible to precisely record the TX and RX timestamps for packets transmitted to or received from the network; however, the synchronization algorithm can be implemented in software. Moreover, there is the White Rabbit project – included in IEEE 1588-2019 – where sub-nanosecond accuracy can also be achieved on a specialized network. White Rabbit is a project delivering to create an Ethernet-based network with low-latency, deterministic packet delivery and network-wide, transparent, high-accuracy timing distribution. The White Rabbit Network is based on Ethernet (IEEE 802.3), Synchronous Ethernet (SyncE) and PTP standards. The measured PTP performance demonstrates sub-nanosecond accuracy over a 5km fiber optic link with a precision below 10 ps [3].

Accurate clock synchronization and PTP's main application area is in the industrial domain, especially in Time-Sensitive Networking (TSN). TSN is a set of standards under development by the Time-Sensitive Networking task group of the IEEE 802.1 working group. Time-Sensitive Networking Task Group specifies TSN functionalities as a set of standards that provide deterministic services through IEEE 802 networks to enable bounded low packet loss, guaranteed packet delivery, bounded low latency and low packet delay variation. TSN targets a variety of particular aspects, among them timing and synchronization aspects. Synchronization is an essential building block to meet these requirements, and IEEE 802.1AS-2020 standard [5] defines a PTP profile to use in TSN networks.

Even though wired solutions are the main direction of PTP implementations, there are existing solutions and research in the wireless PTP domain. Óscar et al. [1] proposes a timestamping method for time synchronization over WLAN standard conditions. The paper presents several simulations using the IEEE 802.11n physical layer and four wireless time-dispersive and time-variant channel models. They have also performed validation experiments using an 802.11g modem implemented over a high-performance Software Defined Radio hardware platform. Inaki et al. [6] presents an IEEE 802.1AS clock synchronization performance evaluation of an integrated wired-wireless TSN architecture. Wireless TSN is expected to be integrated with Ethernet TSN to create large-scale wired–wireless TSN networks. The paper presents two hardware architectures to enable clock synchronization distribution among the network domains. Another Wireless PTP implementation is presented in [7]. This paper evaluates the performance of the over-the-air time synchronization mechanism, which has been proposed in 3GPP Release 16. The paper analyses the accuracy of time synchronization through the boundary clock approach in the presence of clock drift and different air-interface timing errors related to reference time indication. The paper also investigates the frequency and scalability aspects of over-the-air time synchronization. The performance evaluation reveals the conditions required for accuracy of 1μs or below in TSN time synchronization.

In case of IEEE 802.11 (commonly known as WiFi) the software based PTP solutions are capable of reaching time synchronization error in the order of 10 microseconds using wireless links [8], [9]. However, more precise synchronization can be achieved using the WiFi receiver information. Since IEEE 802.11-2006 standard, the protocol supports the fine timing measurement (FTM) for ranging purposes, which can be used to precise time-of-flight measurement [10]. The IEEE 802.1AS standard [5] also mentions the WiFi as the possibly media-dependent layer, however, available implementations are lagging behind.

There are a couple of explicit hardware solutions or circuits to help the implementation of the PTP protocol for Ethernet-based (IEEE 802.3) networks. However, wireless products – while theoretically capable of – do not provide timestamping features or hide the information which is needed to calculate accurate RX and TX timestamps. Furthermore, the propagation characteristics of the radio channel – especially in non-line-of-sight situations – generates jitter in receive timestamps [11]. Fortunately, Ultra Wideband (UWB) technology is perfectly suitable for timestamp reception and transmission of packets since indoor localization requires sub-nanosecond accuracy to provide location in centimeter precision. UWB is applied in various use-cases [12]–[14], but its main application area is indoor, centimeter-based localization using ranging techniques. UWB technology is applied also in time synchronization and synthonization use-cases [15]–[17], mainly for localization purposes (e.g. in time-difference-of-arrival systems). Marcelo et al. [18] achieves 5-ns RMS results in a UWB network, while the Wicsync solution reports errors below 3 nanoseconds [19]. However, all the solutions synchronizes the clocks in the UWB clock domain which avoids the need for clock domain change. UWB applies very short pulses, which help to estimate the channel impulse response (CIR) to extract the first component arrived, hence providing precise timestamps for the first (and hopefully the line-of-sight) component. The IEEE 802.14.5 standard [20] specifies the ranging counter as the clock for timestamping events, which has a resolution of around 15 picoseconds; however, the timestamping accuracy is in the order of nanoseconds.

III. Methods

Our goal is to design a device pair capable of providing accurate synchronization using UWB communication. There are two target use-cases as shown in Fig. 2:

- wireless synchronization between master and slave PTP devices and
- wireless PPS signal transmitter.

The first one aims to provide means to synchronize a local PTP master clock to a remote grand master clock using UWB communication, which can be applied in situations e.g. where

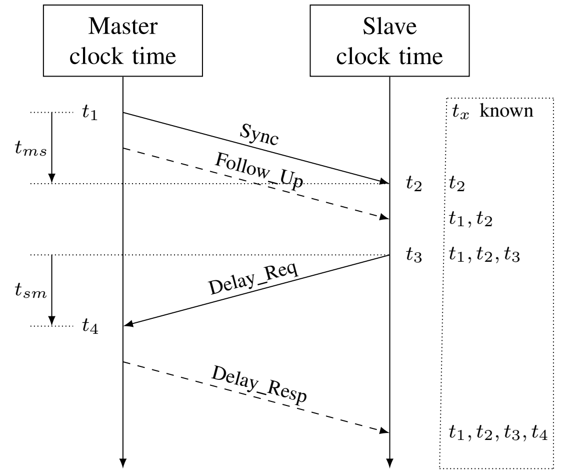
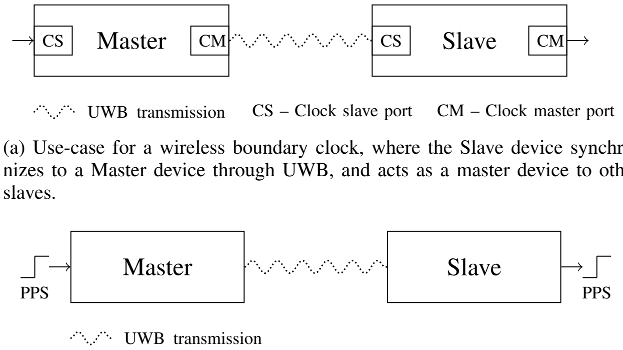


Fig. 1. Basic PTP message exchange [4]



(a) Use-case for a wireless boundary clock, where the Slave device synchronizes to a Master device through UWB, and acts as a master device to other slaves.

(b) Wireless PPS signal transmitter.

Fig. 2. The target use-cases for the UWB based PTP synchronization.

wiring would be hard and expensive between two subnetworks, or there are no transparent clocks between the subnetworks. In this initial version we are focused on the second use-case where the aim is to transmit a PPS signal from the master to the slave device, e.g. for diagnostic purposes to check the synchronization between remote devices without transmitting the PPS signal through wire.

In our scenario, the master device assumed the PTP master role, in order to synchronize the slave clock to the master.

Naturally, we use the high precision timestamping feature of the UWB device to accurately timestamp the PTP messages on the UWB radio link. However, this time instead of the physical distance, the delay is calculated.

To calculate the offset value from the PTP master, the master-to-slave and the slave-to-master offset need to be defined (see Fig. 1):

$$\begin{aligned} d_{\mathrm{m2s}} &= t_1 - t_2 \\ d_{\mathrm{s2m}} &= t_3 - t_4 \end{aligned} \tag{1}$$

From this, the offset from the master can be calculated:

$$\Delta t = d_{\mathrm{m2s}} - d_{\mathrm{prop}} = d_{\mathrm{m2s}} - \frac{d_{\mathrm{m2s}} + d_{\mathrm{s2m}}}{2} \tag{2}$$

, where d_{prop} is the propagation delay. However, this calculation requires the TX and RX events to be timestamped by the PTP clock.

A. Switching local clock domain between SoCs

The main issue regarding the synchronization of PTP clocks using UWB communication is the different clock domains of the UWB transmitter and the PTP clock. Note, that clock domain in this section means the different local clock speeds of the SoC and the UWB transmitter, and not the clock domain concept of PTP! Fig. 3 shows a typical UWB transmitter solution with its clock domains, where the UWB transmitter is controlled by a general SoC (System-on-a-Chip). While UWB communication typically requires a quality clock signal (i.e. UWB is very sensitive to the phase noise), SoC microcontrollers are satisfied with cheap oscillators. To synchronize the PTP clock, the timestamp of RX and TX events needs to be timestamped in the PTP clock domain. The question is, if the exact timestamp of some event is known in the clock domain of the UWB transmitter, how the timestamp of the same event can be calculated in the clock domain of the PTP clock?

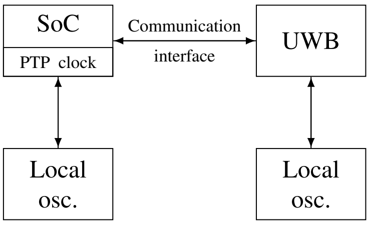


Fig. 3. Typical ultra wide-band hardware solution using different clock domains on the UWB transmitter and the SoC

Having two ideal clocks in different clock domains, the general clock model can be written for both clocks:

$$C^{\mathrm{SoC}} = \int_0^t f^{\mathrm{SoC}}(t)\, dt + o^{\mathrm{SoC}} \tag{3a}$$

$$C^{\mathrm{UWB}} = \int_0^t f^{\mathrm{UWB}}(t)\, dt + o^{\mathrm{UWB}} \tag{3b}$$

Here C is the actual clock counter value, $f(t)$ is the actual frequency, o is the offset of the clock and t is the time. Using crystal oscillators or even TCXOs, it is straightforward that the frequency drift between f^{SoC} and f^{UWB} accumulates very fast. One solution is to use expensive OCXO oscillators with low frequency error (i.e. 1 ppb), however, it is easier to use the same clock for the SoC and the UWB transmitter, i.e. $f^{\mathrm{SoC}}(t) = f^{\mathrm{UWB}}(t)$. In this case, subtracting Eq. 3b from Eq. 3a:

$$C^{\mathrm{SoC}} = C^{\mathrm{UWB}} + (o^{\mathrm{SoC}} - o^{\mathrm{UWB}}) = C^{\mathrm{UWB}} + \Delta o \tag{4}$$

, where Δo is the offset between the SoC and the UWB chip clocks.

However, even with common clock source the offsets in each clock domain cannot be controlled, since the PLLs (Phased Locked Loop) and other circuits make the clock

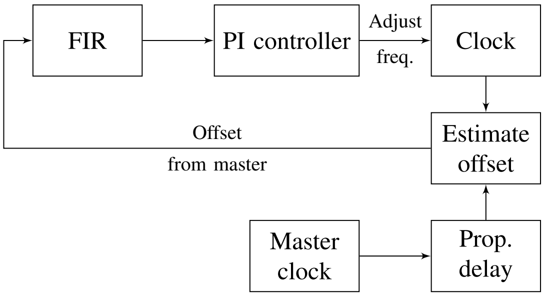


Fig. 4. The clock servo algorithm used to synchronize the PTP clock. To eliminate clock offset and drift, a PI controller is applied.

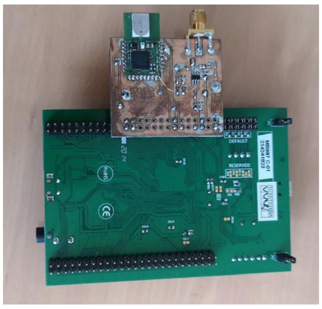


Fig. 5. The evaluation device is based on the STM32F407 evaluation board, and extended by a user-made board containing the DWM1000 module and the clock circuits with an optional SMA connector for the external clock signal.

initialization somewhat stochastic, so Δo can change at each reset. Denote Δo_m the offset at the master and Δo_s the offset at the slave. Define

$$\begin{aligned} t_1 &= C_1^{\mathrm{UWB}} + \Delta o_m \\ t_2 &= C_2^{\mathrm{UWB}} + \Delta o_s \\ t_3 &= C_3^{\mathrm{UWB}} + \Delta o_s \\ t_4 &= C_4^{\mathrm{UWB}} + \Delta o_m \end{aligned} \tag{5}$$

Combine Eq. 5 and Eq. 2, which yields

$$\begin{aligned} \Delta t = C_1^{\mathrm{UWB}} - C_2^{\mathrm{UWB}} + \Delta o_m - \Delta o_s - \\ - \frac{C_1^{\mathrm{UWB}} - C_2^{\mathrm{UWB}} + C_3^{\mathrm{UWB}} - C_4^{\mathrm{UWB}}}{2} \end{aligned} \tag{6}$$

Unfortunately, the difference $\Delta o_m - \Delta o_s$ is unknown and dependent on the initial offset of the clock, which is mainly random. Ideally, Δo_m should equal Δo_s, and there shall be some process providing constant Δo offsets. To achive this, some kind of synchronization facility needs to be provided by the UWB transmitter, e.g. DW1000 chip is able to reset the internal timebase triggered by an external pulse. A concrete example is presented in Section IV; however, the exact method of synchronization depends on the actual hardware capabilities used in the implementation.

B. Clock servo algorithm

For adjusting the PTP clock, a simple PI controller is applied (see Fig. 4.). There are a couple of other, more sophisticated solutions to implement the clock servo algorithm, but for the goals of this paper, the simple PI controller is well-suited since the errors stay direct enough to be evaluated from the viewpoint of timestamping.

The controller itself is driven by the offset from the master error signal (Δt), and passed through a FIR filter, which smooths the random errors of timestamp measurement. The PI controller outputs the control signal, which is used to tune the frequency of the PTP clock.

IV. IMPLEMENTATION

The implementation is based on a STM32F407 SoC, which is a powerful, widely used ARM Cortex M4-based device used in embedded systems. The chip has an Ethernet MAC with a built-in frequency tunable PTP clock, which is able to timestamp RX and TX events on the MAC layer. The UWB communication is provided by the well-known Qorvo DW1000 chip, which has excellent timestamping and external synchronization capabilities. The evaluation devices are designed by the authors, and can be seen in Fig. 5.

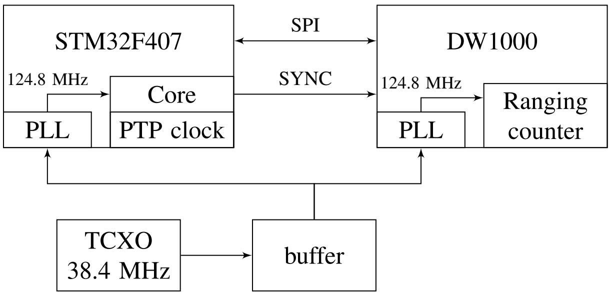


Fig. 6. The synchronization circuit for evaluating the clock synchronization algorithm. The SoC (STM32F407) and DW1000 UWB transmitter are communication through an SPI interface, and the clock synchronization is performed by the Sync signal. The ranging counter and the SoC system clock (and also the PTP clock) are running on 124.8 MHz.

Fig. 6 shows the connections between the components. The clock is generated by a 38.4 MHz thermal-controlled oscillator (TCXO) with a very low phase noise (-132 dBc/Hz at 1 kHz). The clock is distributed between the components by a PL133 clock distributor IC, which also provides low additive phase noise (in the order of femtoseconds). The DW1000 chip uses a PLL to generate the 124.8 MHz signal to drive the ranging counter. The ranging counter is 40 bits wide, providing a resolution of 15 picoseconds. However, the actual timestamping happens on the 124.8 MHz system clock (i.e. the last 9 bits are zeros), and the chip uses a special algorithm based on the channel impulse response to fine-tune the timestamp [21]. While the STM32F407 SoC can operate up to 168 MHz, to simplify implementation the STM32F407 SoC is also programmed to generate a $f_{\mathrm{SYS}} = 124.8$ MHz signal, and the PTP clock and also the Cortex core are driven by this clock.

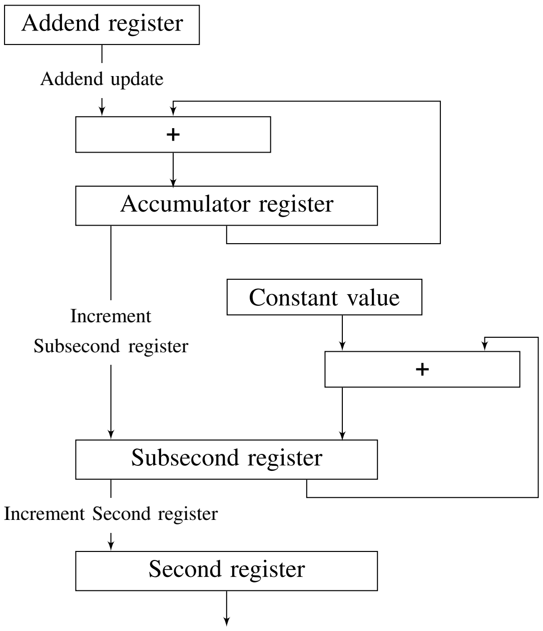


Fig. 7. The operation of the PTP clock. The PTP clock consists of a second and a subsecond register. The subsecond is incremented by a constant when the accumulator register is overflown. [22]

A. The hardware PTP clock

The hardware PTP clock (PHC – PTP Hardware Clock) consists of a 32-bit wide second register and a 31-bit wide subsecond register, allowing a resolution of 0.46 nanoseconds [22]. While the PTP clock is driven by the 124.8 MHz clock, the counter is virtually running somewhat slower. The frequency of the counter can be tuned by a so-called addend register (C_{addend}) shown in Fig. 7, which is added to the accumulator register at each clock cycle, effectively changing the clock frequency as

$$f_{\text{PTP}} = \xi \cdot f_{\text{SYS}} \cdot \tau \quad \xi = \frac{C_{\text{ADDEND}}}{2^{32}} \quad \tau = \frac{C_{\text{SS}}}{2^{31}} \tag{7}$$

, where C_{SS} is the value of the 8-bit subsecond register, τ is the resolution of the PTP clock and ξ is the frequency tune coefficient.

Changing the addend register, the clock frequency changes. To select the correct values for the addend and the subsecond register, one should compromise the resolution of the PTP clock and the limits of the clock frequency tuning. While the former provides better accuracy, the latter limits the control signal from the PI controller.

B. Synchronization with the DW1000 chip

The main issue in synchronization is that the packet receive and transmit time instants shall be known by the PTP clock. Typically, the PTP clock is integrated in the hardware that receives and transmits the packets. Also, the DW1000 UWB chip provides timestamps using his own counter (with his own offset Δo), however, the clock of the DW1000 chip cannot be tuned, thus it is not suitable to use as a PTP clock. To synchronize a PTP clock outside of the DW1000 clock domain, external synchronization facilities shall be used. External synchronization is implemented by a special SYNC signal in the DW1000 chip. There are two modes used: one-shot transmit synchronization mode (OSTS) and the one-shot timebase reset (OSTR).

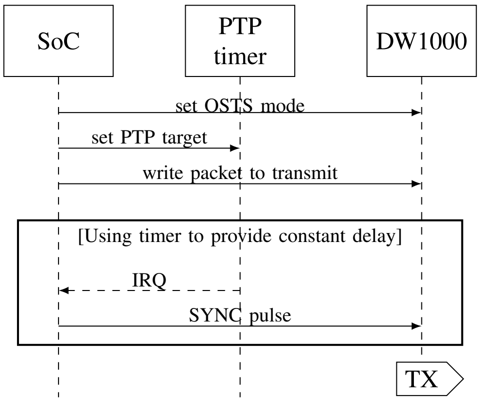


Fig. 8. The method of TX synchronization. The transmission starts after the SYNC pulse with a constant delay.

One shot timebase reset mode allows a reset to be applied to the timebase counter used for timestamping in DW1000 at a deterministic and predictable time relative to a synchronisation event (i.e. the SYNC pin). The DW1000 chip will reset the counter at a repeatable time to typically less than 100ps variation. Besides OSTR mode, one-shot transmit synchronization mode provides for the transmission of a frame at a well-defined time (typically 12 ps) relative to the assertion of the SYNC pin of the DW1000 chip. To learn more of the mechanism of OSTS and OSTR mode, the DW1000 user manual has a detailed description [21].

1) Transmission synchronization: For scheduled transmission, OSTS mode is used. For transmitting a packet at a specified moment in the future, the PTP clock target is set to give an interrupt (see Fig. 8). However, interrupts on Cortex M4 are not ensured to be real-time, so it introduces a jitter of a couple of clock cycles. To avoid the jitter, the PTP interrupt triggers a timer, which constructs a fixed-sized SYNC pulse in constant time. At the rising edge of the SYNC pulse, the DW1000 is guaranteed to start transmission in a fixed time delay. Notice that the transmission timestamp can be included in the message, so one-step method can be used which does not need to send a *Follow_Up* message.

2) Receive synchronization: Receive synchronization has to provide constant Δo offset (see Section III-A). The DW1000 chip is able to reset its timebase against a rising edge of the SYNC signal, using the external synchronization mode OSTR. When setting the SYNC signal, the PTP clock shall be read and stored as t_{sync} (see Fig. 9). In a Cortex M4 processor, the two 32-bit registers of the PTP clock and the GPIO change cannot be performed simultaneously; however, it can be done

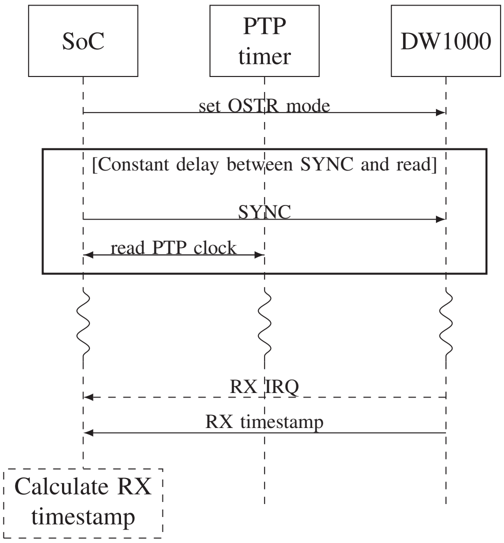


Fig. 9. The method of RX synchronization. The transmission starts after the SYNC pulse with a constant delay.

with a constant delay with disabled interrupts.

Later on, at reception, the DW1000 timestamp can be read out, and the PTP timestamp for the receive event can be calculated as

$$t_{\text{PTP}} = t_{\text{SYNC}} + \frac{C_{\text{DW}}}{2^9} \cdot \xi \cdot f_{\text{SYS}} \cdot \tau \tag{8}$$

, where C_{DW} is the 40 bit DW1000 timestamp.

C. Timestamping errors

In the implementation, there are a couple of potential error or jitter sources.

1) PTP clock resolution: One of the most basic jitter source is the resolution and frequency of the PTP clock. The limited resolution (see Eq. 7) of the PTP clock results in a classical sampling noise; however, the situation is worse as the frequency tuning by the addend register deviates from the sampling points. Increasing the effective frequency of the PTP clock results in a decrement in the sampling noise.

2) Wireless propagation: The stochastic behavior of wireless propagation results in timestamping errors, i.e. the first component that arrived is wrongly detected and timestamped. To avoid this issue, UWB devices observe the channel impulse response to refine the timestamp, acquiring subnanosecond accuracy of timestamping. However, pure NLOS (non line-of-sight) propagation can add higher timestamp offset, which is hard to detect.

3) Clock domain synchronization error: The main source of error results from the clock domain switch between the SoC and the UWB transmitter. The SYNC signal of the DW1000 chip is sampled at the rising edge of the 38.4 MHz clock; however, SoC runs on a faster clock, 124.8 MHz. The SoC toggle the SYNC signal on its own clock, which can result in some jitter since SYNC signals at different rising edges of the SoC clock sampled at the same rising edge of the DW CLK (see Fig. 10). This error can introduce around 26 nanoseconds of jitter or uncertainty in timestamping, due to the 38.4 MHz sampling clock.

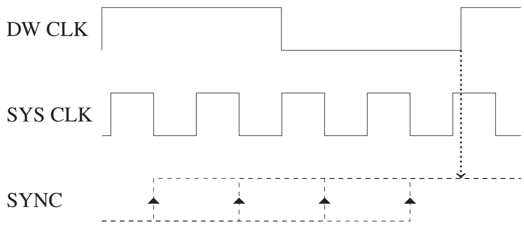


Fig. 10. Jitter resulting from clock domain change. The SYNC signal is sampled at the rising edge of the DW clock, but driven by the SYS clock.

TABLE I
THE SETTINGS USED FOR EVALUATION

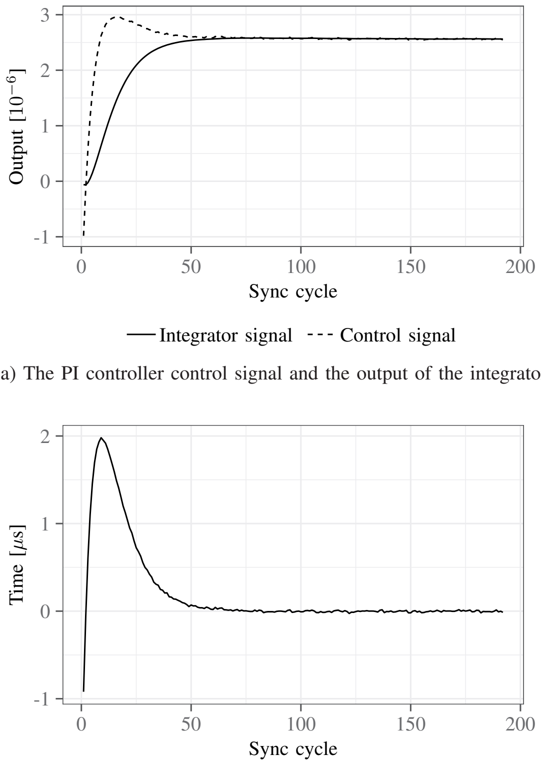
Subsecond update	0x14
Addend	0xDC41363A
Sync period	500 ms
SYSCLK	124.8 MHz
K_i (PI)	15
K_p (PI)	1
FIR	[0.5,0.5]
UWB channel	5
UWB bitrate	850 kbps
UWB PRF	64 MHz
UWB preamble syms	1024

V. EVALUATION

The evaluation is based on the implemented synchronization method presented in Section IV. For evaluation, two devices were used, one is a free-running master device, and the other one is the slave device synchronizing to the master device. The setting of the arrangement is summarized in Table I.

After a cold start, the PI controller starts to converge to the synchronous state, as shown in Fig. 11. The figure shows that the error signal's steady state converges to zero in the order of nanoseconds, and the control signal for the PTP clock converges to a steady state. The control signal has a small overshoot, and the convergence happens in 70-80 sync cycles corresponding to 35-40 seconds. The parameters of the PI controller were selected for the system to be stable with a high integrator coefficient. The high integrator coefficient helps to avoid the overreaction resulting from timestamping and clock domain change errors. However, the paper do not target the design method of the optimal controller for transient behaviour, only concentrates on the steady state.

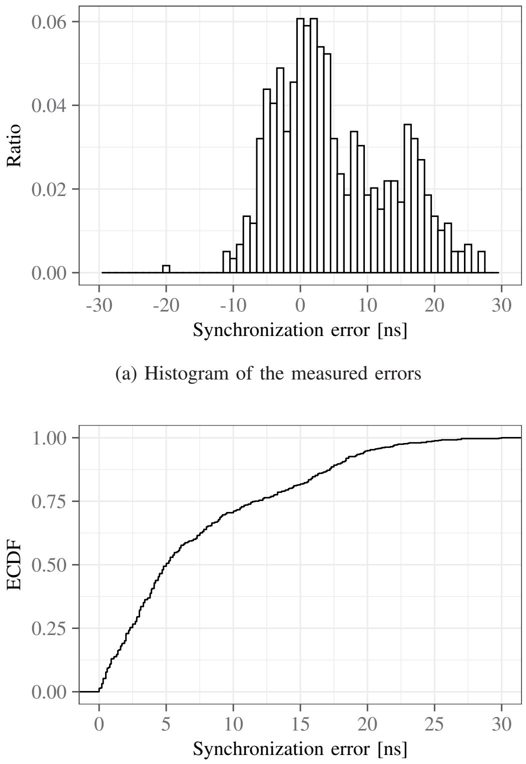
After reaching the steady state, 1000 measurements were made by a DSO-X 3054A oscilloscope, using the Pulse Delay Measurement function to analyze and record the delay between the PPS signals of the master and slave PTP clock (see Fig 12). The result can be seen in Fig. 13 as a histogram. It is clearly seen that the error between the two PPS signals does not exceed 30 nanoseconds in absolute value; however, the distribution is skewed, and there are less negative errors than positive errors. 90 percent of the absolute errors are below



(a) The PI controller control signal and the output of the integrator

(b) The error signal of the PI controller

Fig. 11. The error signal and the output of the PI controller of the clock servo. The time axis shows the synchronization cycles, where one cycle is 500 ms. It can be clearly seen, that the error signal is in the order of nanoseconds.



(a) Histogram of the measured errors

(b) The empirical cumulative distribution plot of the absolute error

Fig. 13. Distribution of the error measured between the two PPS signals. The histogram is based on 1000 sync cycle after the controller has locked.

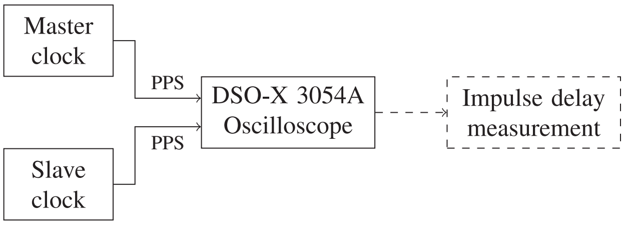


Fig. 12. The measurement method of the clock synchronization error between the master and slave devices.

20 nanoseconds, while 70 percent of the absolute errors are below 10 nanoseconds.

The skewness of the distribution assumes that the timestamping error is asymmetric, i.e. it is not exactly the same in the case of master-to-slave and slave-to-master. The errors are likely to originate from a couple of sources presented before:

1) The error resulting from clock domain change.
2) The PTP clock resolution.
3) Multipath propagation.

It is worth noticing that the magnitude of the error can be explained by the clock domain change error in itself and is well below the requirements of an industrial profile TSN network (i.e. 250ns).

VI. Conclusions

The paper investigates the feasibility of PTP clock synchronization using the wireless Ultra Wideband technology, which provides an accurate timestamping feature for packet transmission and reception. Both the methodology and the implementation-specific issues are presented. The results show that the synchronization accuracy is in the order 10 nanoseconds. This clock synchronization accuracy is on the same scale as the commercially available wired solutions. It can be concluded that – even in its initial form – the presented UWB implementation can be an excellent solution for an accurate wireless PTP master clock synchronization or as a validation method for clock synchronization due to its low cost and wireless properties. However, for the validation of synchronization accuracy and precision, the presented solution is useful only in PTP wireless environments or in PTP networks with PTP unaware devices, since the resolution is the same as the accuracy of the state-of-the-art methods. As a bonus, localization is also provided as the original use case for UWB.

The main causes of the synchronization error are also presented, anticipating the possibility of further improving the accuracy of the synchronization. Specifically, the clock domain switch error has the same magnitude as the overall synchronization error, thus estimating the constant delay at the clock domain switch the synchronization accuracy can be drastically improved.

Regarding future work, the synchronization error of the master and slave device can be further reduced with fine tuning of PI controller or with the implementation of a more sophisticated solution such as Kalman-filtering. Another possible future research direction would be the evaluation and measurements of the different LOS and NLOS scenarios and the characteristics of the distance between the master and slave device. Furthermore, as the UWB technology has significant limitations beyond a certain distance, there is some initial research on a multi-hop UWB PTP system. Such a system can provide clock synchronization on the order of 10 ns over many times the UWB radio range. However, in this case, the synchronization errors are accumulated, offering an exciting research topic.

References

[1] O. Seijo, J. A. López-Fernández, H.-P. Bernhard, and I. Val, "Enhanced Timestamping Method for Subnanosecond Time Synchronization in IEEE 802.11 Over WLAN Standard Conditions," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 5792–5805, 2020, **doi**: 10.1109/TII.2019.2959200.

[2] Z. Idrees, J. Granados, Y. Sun, S. Latif, L. Gong, Z. Zou, and L. Zheng, "IEEE 1588 for Clock Synchronization in Industrial IoT and Related Applications: A Review on Contributing Technologies, Protocols and Enhancement Methodologies," *IEEE Access*, vol. 8, pp. 155 660–155 678, 2020, **doi**: 10.1109/ACCESS.2020.3013669.

[3] M. Lipiński, T. Włostowski, J. Serrano, and P. Alvarez, "White rabbit: a PTP application for robust sub-nanosecond synchronization," in *2011 IEEE International Symposium on Precision Clock Synchronization for Measurement, Control and Communication*, 2011, pp. 25–30, **doi**: 10.1109/ISPCS.2011.6070148.

[4] "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems," *IEEE Std 1588- 2019 (Revision of IEEE Std 1588-2008)*, pp. 1–499, 2020, **doi**: 10.1109/IEEESTD.2020.9120376.

[5] "IEEE Standard for Local and Metropolitan Area Networks–Timing and Synchronization for Time-Sensitive Applications," *IEEE Std 802.1AS-2020 (Revision of IEEE Std 802.1AS-2011)*, pp. 1–421, 2020, **doi**: 10.1109/IEEESTD.2020.9121845.

[6] I. Val, O. Seijo, R. Torrego, and A. Astarloa, "IEEE 802.1AS Clock Synchronization Performance Evaluation of an Integrated Wired–Wireless TSN Architecture," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, pp. 2986–2999, 2022, **doi**: 10.1109/TII.2021.3106568.

[7] H. Shi, A. Aijaz, and N. Jiang, "Evaluating the performance of over-the-air time synchronization for 5g and tsn integration," in *2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, 2021, pp. 1–6, **doi**: 10.1109/BlackSea-Com52164.2021.9527833.

[8] T. Adame, M. Carrascosa-Zamacois, and B. Bellalta, "Time- Sensitive Networking in IEEE 802.11be: On the Way to Low-Latency WiFi 7," *Sensors*, vol. 21, no. 15, 2021. [Online]. Available: https://www.mdpi.com/1424-8220/21/15/4954. **doi**: 10.3390/s21154954

[9] J. Haxhibeqiri, X. Jiao, M. Aslam, I. Moerman, and J. Hoebeke, "Enabling TSN over IEEE 802.11: Low-overhead Time Synchronization for Wi-Fi Clients," in *2021 22nd IEEE International Conference on Industrial Technology (ICIT)*, vol. 1, 2021, pp. 1068–1073, **doi**: 10.1109/ICIT46573.2021.9453686.

[10] "IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*, pp. 1–3534, 2016, **doi**: 10.1109/IEEESTD.2016.7786995.

[11] G. Hollósi, "Distribution of ultra wideband (UWB) receive timestamps in dense indoor environment based on the Saleh-Valenzuela channel model," in *2022 14th International Conference on Communications (COMM)*, 2022, pp. 1–5, **doi**: 10.1109/COMM54429.2022.9817167.

[12] A. Jiménez and F. Seco, "Finding objects using uwb or ble localization technology: A museum-like use case," in *2017 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2017, pp. 1–8, **doi**: 10.1109/IPIN.2017.8115865.

[13] W. Shule, C. M. Almansa, J. P. Queralta, Z. Zou, and T. Westerlund, "UWB-Based Localization for Multi-UAV Systems and Collaborative Heterogeneous Multi-Robot Systems," *Procedia Computer Science*, vol. 175, pp. 357–364, 2020, mobiSPC. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050920317324. **doi**: 10.1016/j.procs.2020.07.051

[14] M. Drobczyk, C. Strowik, and C. Philpot, "A Wireless Communication and Positioning Experiment for the ISS Based on IR-UWB," in *2017 IEEE Wireless Communications and Networking Conference (WCNC)*, 2017, pp. 1–6, **doi**: 10.1109/WCNC.2017.7925487.

[15] S. Rinaldi, A. Musatti, A. Depari, P. Ferrari, A. Flammini, and E. Sisinni, "An Experimental Characterization of Chain of PLLs for Wired Clock Synchronization of UWB Anchors for Indoor Location," in *2022 IEEE International Instrumentation and Measurement Technology Conference (I2MTC)*, 2022, pp. 1–6, **doi**: 10.1109/I2MTC48687.2022.9806698.

[16] R. Zou, N. Wu, Z. Qu, and J. Chen, "Design and Implementation of a High-precision Wireless Clock Synchronization System Based on UWB," in *2022 4th International Conference on Intelligent Control, Measurement and Signal Processing (ICMSP)*, 2022, pp. 1094–1099, **doi**: 10.1109/ICMSP55950.2022.9859065.

[17] P. Ferrari, P. Bellagente, A. Depari, A. Flammini, M. Pasetti, S. Rinaldi, and E. Sisinni, "Resilient time synchronization opportunistically exploiting uwb rtls infrastructure," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–10, 2022, **doi**: 10.1109/TIM.2021.3132354.

[18] M. Segura, S. Niranjayan, H. Hashemi, and A. F. Molisch, "Experimental demonstration of nanosecond-accuracy wireless network synchronization," in *2015 IEEE International Conference on Communications (ICC)*, 2015, pp. 6205–6210, **doi**: 10.1109/ICC.2015.7249312.

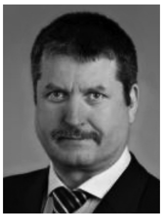
[19] B. Xue, Z. Li, P. Lei, Y. Wang, and X. Zou, "Wicsync: A wireless multi-node clock synchronization solution based on optimized UWB two-way clock synchronization protocol," *Measurement*, vol. 183, p. 109760, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S026322412100717X. **doi**: 10.1016/j.measurement.2021.109760

[20] "IEEE standard for low-rate wireless networks," *IEEE Std 802.15.4-2020 (Revision of IEEE Std 802.15.4-2015)*, pp. 1–800, 2020, **doi**: 10.1109/IEEESTD.2020.9144691.

[21] D. Ltd., DW1000 User Manual, *"How To use, configure and program the DW1000 UWB transmitter"*, Qorvo, 2017.

[22] ST, *Reference manual, STM32F405/415, STM32F407/417, STM32F427/437 and STM32F429/439 advanced Arm-based 32-bit MCUs*, 2021.

Gergely Hollósi is a researcher at Dept. of Telecommunications and Media Informatics (TMIT) of Budapest University of Technology and Economics (BME). Gergely received his M.Sc. in the Budapest University of Technology and Economics (BME) in 2009. He is actively working and researching on computer vision, image processing, machine learning algorithms and indoor localization systems.



István Moldován is a Research Fellow at the Budapest University of Technology and Economics in the Department of Telecommunications and Media Informatics. In 1996, he received an M.Sc. degree in Automation and Industrial Informatics from the Technical University of Tirgu-Mures, Romania. His research interests include network management, embedded systems, simulation and performance evaluation of computer networks. He is lecturing on communication networks.

An SDN controller-based framework for anomaly detection using a GAN ensemble algorithm

Dubem Ezeh, *Student Member, IEEE*, and J. de Oliveira, *Member, IEEE*

***Abstract*—Of recent, a handful of machine learning techniques have been proposed to handle the task of intrusion detection with algorithms taking charge; these algorithms learn, from traffic flow examples, to distinguish between benign and anomalous network events. In this paper, we explore the use of a Generative Adversarial Network (GAN) ensemble to detect anomalies in a Software-Defined Networking (SDN) environment using the Global Environment for Network Innovations (GENI) testbed over geographically separated instances. A controller-based framework is proposed, comprising several components across the detection chain. A bespoke dataset is generated, addressing three of the most popular contemporary network attacks and using an SDN perspective. Evaluation results show great potential for detecting a wide array of anomalies.**

***Index Terms*—Software-Defined Networking, network anomaly detection, GAN ensemble, machine learning, DDoS.**

I. Introduction

In this paper, we propose the use of a GAN ensemble algorithm to detect network anomalies by understanding the distribution of normal network behaviour. in the context of Software Defined Networks (SDNs), where a controller executes the algorithm and can take action upon detecting an anomaly. Network anomaly detection has been extensive researched by academia and industry, and many methods have been proposed; from middleboxes (e.g., Intrusion Detection Systems) to other traditional rule-based tools (e.g., Snort). Machine learning has become the natural choice for anomaly detection, specially given the dynamic nature of the network attacks that are prominent today.

Ensemble learning is a machine learning technique that combines several base models in order to produce one optimal predictive model, usually by taking a (weighted) vote of the predictions of the base learners. Such models have been shown to perform better than each of their base learners [1], [2]. Although ensemble models have been proposed recently in the context of anomaly detection in traditional networks [3], our work uses a GAN ensemble approach in the context of an SDN environment to detect current and future threats. We envision a controller-based framework that comprises various co-operating systems representing each aspect of the detection chain. For validation, we used both existing popular datasets (CAIDA, UNSW-NB) and also created a new dataset by running experiments on the GENI research testbed [4], with instances deployed over geographically-separated zones. Our dataset contains three of the most popular contemporary network attacks. Evaluation results show an edge over other one-class as well as multi-class classification algorithms and a potential for detecting a wide array of new anomalies.

The contributions of this paper include:

- Proposing an SDN Controller framework to deploy a GAN ensemble approach for network anomaly detection;
- Generation of a new dataset that addresses three of the most popular contemporary network attacks;
- Evaluation of the proposed framework using publicly available datasets as well as the newly created dataset;
- Evaluating the proposed framework's performance using a real testbed with geographically-separated nodes.

Throughout this paper, we will refer to an *abnormal* network flow as one that involves any of the intrusion exploits included in the datasets used. The rest of this paper is organized as follows. In Section II, we highlight previous contributions aimed at solving the anomaly detection problem and their shortcomings. We present in Section III, background information on the machine learning model utilized in this work. The major components of our proposed framework, together with the datasets used to validate proposal are detailed in Section IV. We present our experimental results in Section V, while Section VI contains our conclusions and thoughts on future work.

II. Related work

Anomaly detection has become a mainstay feature in computer networks as not all users utilize network resources for benign purposes. There are many types of network anomaly detection systems and this section will look at related work in these broad areas: signature-based and anomaly-based Network Intrusion Detection Systems (NIDS), machine-learning-based approaches, semi-supervised learning approaches, Generative Adversarial Networks (GANs) and ensembles.

In [5], NIDS have been classified, based on their detection approach as either signature-based (SIDS) or anomaly-based (AIDS) detection systems, and have been used extensively in many network deployments across the globe. The SIDS [6], [7], [8] are popular for efficiently detecting known attacks, but need to be updated constantly to handle new signatures, and thus fair poorly against unknown attacks. The AIDS approach [9], [10], [11] covers statistics-based, knowledge-based and machine learning-based solutions; these techniques require initial training but tend to fair better against new attacks. Of the three, machine learning-based solutions have witnessed immense proliferation and attention due to an improvement in computational capabilities, particularly in the area of Graphics Processing Units (GPUs), which speed up the training process of very complex machine learning models.

The authors are with the Department of Electrical and Computer Engineering, Drexel University, Philadelphia, PA, USA. (e-mail: jco24@drexel.edu)

DOI: 10.36244/ICJ.2023.2.5

Machine learning algorithms can be grouped into four main categories, depending on how much information is known to the model a priori, during training: supervised, semi-supervised, unsupervised and reinforcement learning algorithms, with the supervised and unsupervised learning models being the two most common machine learning techniques used for anomaly detection in SDNs [12].

Supervised learning algorithms [13], [14] use labelled inputs and outputs for training, after which new inputs are used for testing. In [15], a CART-based Decision Tree algorithm was utilized for detecting anomalous traffic in the CICIDS2017 dataset; it was set up as a simulation for an SDN-oriented IoT network with detection being centralized at the controller.

Semi-supervised learning algorithms [16], [17], [18] use both labeled data (usually expensive and difficult to obtain) and unlabeled data (usually cheaper to obtain). These one-class classifiers are advantageous because they can, through different techniques, build boundaries around normal data so that anomalous events are easy to detect. The One-Class Support Vector Machine (OCSVM) algorithm was used in [19], [20] to detect novelty (another term for anomalies) in Internet of Things (IoT) devices; the memory and computation requirements of the OCSVM, which increase with the size of the training dataset, make it a less desired option for anomaly detection [21]. Isolation Forest [22] and Local Outlier Factor [23] are some other one-class classifiers that have also been used in the past for anomaly detection.

Unsupervised learning algorithms [24], [25], [26] are supplied inputs without labels, with the aim of grouping observations based on some metric of similarity between them. Clustering and data aggregation are the most popular unsupervised techniques in use today.

GANs are, originally, unsupervised, and deep-learning-based; they are used for generative modelling and involve two components: a generator and a discriminator, that work together to learn the patterns of a training dataset so that new examples can be generated which look very similar to examples in the training set. Because of their generative and discriminative properties, GANs have been employed to learn patterns of normal data so that they can easily detect anomalous data, thus adapting to anomaly detection solutions. MADGAN, a GAN variant, was used in [27] to detect early onset of brain anomalies, like Alzheimer's disease, mild cognitive impairment and brain metastases. Like MADGAN, several other proposals [28], [29] have been put forward to perform anomaly detection in the computer vision space.

Ensemble models are machine learning models that are built on the backs of two or more base models which may be of the same type, or may be heterogeneous, like in [30]. Ensembles offer the benefits of improved robustness and performance over their base models, and have been used to win different machine learning competitions [31]. In [32] an ensemble model built from multiple Efficient GAN-Based Anomaly Detection (EGBAD) models [33] was proposed; each generator in a base model was configured to learn from all the discriminators in the ensemble and vice-versa. The focus here was mostly on image datasets and computer vision applications.

In this paper, we draw inspiration from [32], [34] to propose the use of an ensemble algorithm, built upon homogeneous base EGBAD models, to properly detect today's SDN-oriented network anomalies, especially those of the highly pervasive DDoS type. We utilize two unique datasets for our experiments: a bespoke dataset, curated from an SDN topology built on the GENI research testbed [4] with instances deployed over geographically-separated zones (instagenis), and data from the UNSWB and CAIDA, all rolled into one. While other classifiers and network anomaly detectors require all classes of attack to be present during training, our GAN-based one-class classifier learns to represent only the normal space so as to detect when any attack is encountered since said attack would fall outside the boundary of normality; it also leverages the benefits of ensemble learning to yield a robust anomaly detector.

III. Background

This section describes the ensemble-based algorithms used for detection. This model was first proposed in [33], primarily to help detect anomalies in the computer vision space and was therefore adapted to our purpose.

A. EGBAD model

A conventional GAN model is made from a Generator network, that tries to perfect the art of synthesizing data samples that fit the distribution of actual training samples; and a Discriminator network, that tries to discern whether a given sample is from the Generator or from the actual dataset. There are many variations of the GAN model ([35], [36], [37], [38]) with some more suited for computer vision exploits than others. In the EGBAD model [33], there is a choice between a conventional GAN and Bidirectional GAN (BiGAN) architecture. The latter performs better on tabular data type, to which the GENI-SDN and the CAIDA-UNSWB datasets belong. In the BiGAN architecture, the generator component is actually made up of an encoder and a decoder, such that the decoder output is what we use, together with real samples, to train our discriminator to distinguish between samples.

B. Ensemble

The idea behind an ensemble model is to build upon the strengths of other base machine learning models [39].

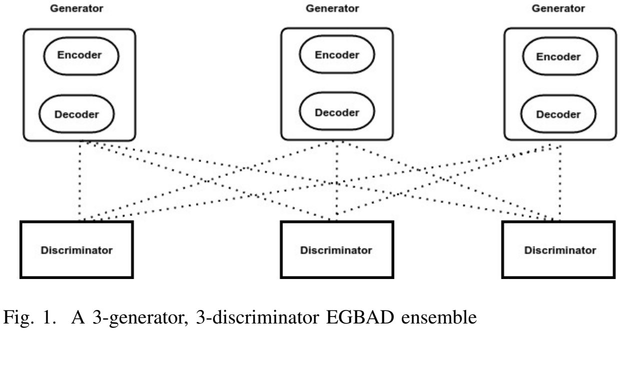


Fig. 1. A 3-generator, 3-discriminator EGBAD ensemble

Algorithm 1 EGBAD Ensemble from [32]

```
Input: Training set $X = \{x_i\}_{i=1}^N$
Output: Trained generators $\{G_e(\cdot;\phi_i), G_d(\cdot;\psi_i)\}_{i=1}^I$ and discriminators $\{D(\cdot;\gamma_j)\}_{j=1}^J$
Initialize parameters for $(\phi_i, \psi_i)_{i=1}^I$ and $(\gamma_j)_{j=1}^J$
$t \leftarrow 0$
while the objective not converge and $t <$ max_iter do
    Sample $i$ from $\{1, \ldots, I\}$ and $j$ from $\{1, \ldots, J\}$
    Sample a minibatch $X^t$ from $X$
    Compute the adversarial loss $L_a^{(ij)}$
    Update $D(\cdot;\gamma_j) : \gamma_j \leftarrow \gamma_j + \nabla_{\gamma_j} L_a^{(ij)}$
    $\mathcal{L}^{(ij)} = \alpha_1 L_a^{(ij)} + \alpha_2 L_r^{(i)} + \alpha_3 L_d^{(ij)} + \alpha_4 L_e^{(i)}$
    Update $G_e(\cdot;\phi_i) : \phi_i \leftarrow \phi_i - \nabla_{\phi_i} \mathcal{L}^{(ij)}$
    Update $G_d(\cdot;\psi_i) : \psi_i \leftarrow \psi_i - \nabla_{\psi_i} \mathcal{L}^{(ij)}$
    $t \leftarrow t + 1$
end while
```

In this paper, there are three similar base models, each built using the BiGAN-based EGBAD algorithm for anomaly detection. Each generator network gets feedback from multiple discriminators while a discriminator receives samples from multiple generators, much like a meshed network (see Fig. 1). An anomaly score is taken from the average of anomaly scores computed for all generator-discriminator pairs; a higher anomaly score points to the sample falling outside the distribution of normality, while a lower anomaly score points to a sample that is normal. This interaction between the base models is what gives the ensemble the upper hand.

The anomaly detection problem is therefore solved in Algorithm 1, according to the implementation in [32]. Each generator, G_i, is characterized by an encoder, $G_e(\cdot;\phi_i)$ and a decoder, $G_d(\cdot;\psi_i)$. The encoder maps a given sample, x, to a latent vector, z, while the decoder computes a reconstruction, x' of the sample from z. The Discriminator on the other hand, takes a sample from the decoder and predicts the probability of the sample being from the actual sample set, X, instead of from the encoder-decoder.

IV. Proposed Framework and Experimental Setup

This section describes the implementation of our testbed, the proposed SDN controller-based framework for detection, and the datasets used to validate the efficacy of our solution.

A. GENI and SDN

The GENI [4] testbed is a very important tool for performing networking experiments and research. By harnessing Network Function Virtualization (NFV), GENI users are able to reserve and obtain geographically-separated compute resources within the United States, including layer 2 networks, protocols of their choice in layer 3 and above, and custom operating systems best suited to their research demands.

Fig. 2 shows the topology used to produce our GENI-SDN dataset. It comprises the following components:

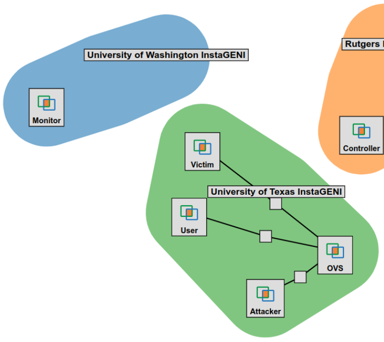

University of Washington InstaGENI
Monitor
Rutgers InstaGENI
Controller
Victim
University of Texas InstaGENI
User
OVS
Attacker

Fig. 2. Topology of experiment setup using GENI

1) SDN Controller: The controller oversees all traffic policies associated with the experiments and was deployed at Rutgers University (New Jersey). The Pox controller module (Fangtooth variant) was installed on top of a compute instance running the Ubuntu 18.04.6 LTS (Bionic Beaver) operating system.

2) OVS Switch and Associated Nodes: An Open vSwitch (OVS) was deployed at the University of Texas (Texas), together with three nodes: *Attacker*, *User* and *Victim*, all on the same local area network governed by the OVS. This switch was then linked to the remote controller for all traffic policies (done by setting the set-fail-mode to secure).

3) Monitor: This node was deployed at the University of Washington (Washington) to remotely listen for all traffic traversing the various ports of the OVS switch in Texas. To achieve this, a Generic Routing Encapsulation (GRE) tunnel was created between the monitor node and the OVS switch, and a Pox component was initiated from the controller to allow traffic duplication to said tunnel. The operating system of choice for this node and the other nodes on the LAN is Kali Linux as it is best suited for cybersecurity research.

We use three separate sites to demonstrate how, even when in different networks, packets can still be forwarded to a remote node for analyses/anomaly detection in "real-time". A simpler testbed could be setup with two sites, and with a remote controller acting as the monitoring node.

B. Proposed Framework

We show our proposed controller-based anomaly detection framework in Fig. 3 where multiple dataplane devices connect to the controller via the Southbound API, and are configured to forward traffic traces to the controller at regular intervals for analysis. The Northbound API is utilized to forward any observed anomalies to the network administrators in a timely fashion. The frequency of updates to the controller via the southbound interface would be a function of both Service Level Agreement (SLA) demands and prevailing network conditions. The controller would be the repository for the trained detection model, as well as copies of traffic traces that are analysed for potential threats.

Fig. 4 shows a basic process pipeline for anomaly detection within the controller. The controller serves as a repository for

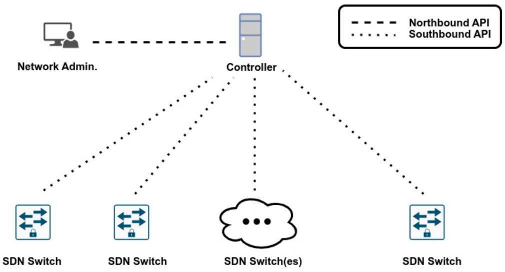


Fig. 3. Overview of controller-based anomaly detection framework

packet traces, obtained at intervals and containing information about events on the network. These traces are usually stored in *filename.pcap.gz* format. The controller would be responsible for pre-processing the traces into a machine-learning-readable format (usually *filename.csv*) with string, categorical and ordinal values properly encoded prior to training a model.

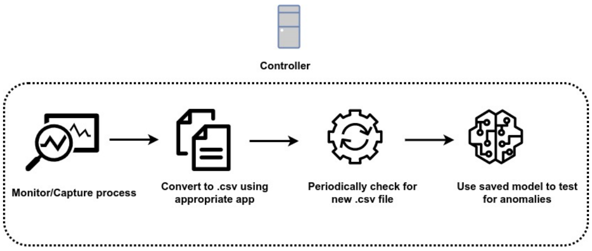

Controller
Monitor/Capture process
Convert to .csv using appropriate app
Periodically check for new .csv file
Use saved model to test for anomalies

Fig. 4. Anomaly detection pipeline within controller

A detection model is trained (saved in *model.h5* format) and used to test incoming data for classification. Such a setup could process packet traces in short time intervals (e.g., five-minute intervals) to detect, and nip in the bud, nefarious actions within the network. From time to time, depending on the performance of the saved model, a re-training exercise might be scheduled to allow for a system that keeps up with changes in network behavior. In our experiments, a five-minute packet capture was used as a test case: a 28MB traffic trace was captured, pre-processed, encoded and tested. Roughly 1 second was used to extract information from the pcap file, encoding took 5 seconds to execute, and testing took 5.5 seconds with the computer used in the study, described in Table II. In all, a five-minute interval worked well in our testing, allowing for prompt testing of traces.

C. Datasets

1) GENI-SDN Dataset: The highly ranked KDD dataset was produced at a time when DDoS attacks and SDN technology had not become widespread. In order to properly validate the ensemble in view of current network trends, we produced a bespoke dataset by capturing network traffic at various intervals between the 28th of May, 2021, and the 17th of June 2021. To generate normal traffic, we used the *Iperf* application [40], running a server instance on the victim node and client instances on the other nodes directly connected to the OVS switch. Next, we describe how we created the other types of traffic.

Denial of Service (DoS): This type of attack attempts to flood a computer that provides a service in such a way that the server becomes unable to attend to the requests of legitimate clients. For the DoS attack, we run a simple HTTP server on the victim node. The attacker node uses the *Hping3* application [41] in flood-mode, in a bid to make the victim unavailable to legitimate users.

Distributed Denial of Service (DDoS): In DDoS, multiple attacking nodes combine their efforts to overwhelm a server and make it unavailable. DDoS traffic was generated using the Python-based open source tool, *Pyloris* [42], which works by spawning multiple threads (as specified by the user) to emulate the bots in a botnet that execute a DDoS exploit.

Enumeration: This type of attack is passive in that there is no action at this stage to overwhelm a server. The aim is to perform reconnaissance on a network and its associated resources to find out how many hosts are available on a network, the IP address layout, what services are listening on what open ports, what operating system is running on what host(s), etc. While it may be the most subtle of the attacks, information gleaned from this stage can be used for very harmful attacks subsequently. To implement this attack, we used the *Nmap* tool [43] to probe for different types of information about the network. It contains a total of 20 hours of network traffic traces stored on the remote monitor node. These traces were then pruned to extract a total of 32 features and 4 classes of network flow, including *Normal, DDoS, DoS* and *enumeration*. We limited the scope of our attacks since our experiments were run over an active testbed serving other researchers as well. The overall dataset contains over $1,000,000$ observations covering the aforementioned network classes and distributed in the fashion seen in Fig. IV-C1. A combination of *AWK* [44], *Bash* [45], *TCPdump* [46] and *ARGUS* [47] commands were used to generate the GENI dataset. The protocol distribution is 71.23% TCP, 28.59% UDP and 0.18% other.

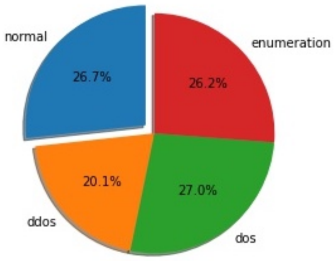


Fig. 5. Distribution of samples in the GENI-SDN dataset

2) CAIDA-UNSW Dataset: In order to properly validate our proposal, we utilized two datasets that covered diverse network anomalies - the UNSW-NB 15 Dataset [48] and the CAIDA DDoS Dataset [49].

UNSW-NB 15 Dataset: This dataset was created to assist researchers with credible data for network anomaly experiments. Initially in its raw form as hundreds of gigabytes of packet captures, the dataset was pruned to extract a total of 49 features and 9 classes of network flow, including *Fuzzers, Analysis, Backdoors, DoS Exploits, Generic, Reconnaissance, Shellcode* and *Worms*. The overall dataset contains about $2,540,048$ observations covering the aforementioned network classes. DDoS anomalies were not included in the experiments that yielded this dataset.

CAIDA Dataset: The CAIDA DDoS dataset contains tens of gigabytes of compressed packet captures which together cover approximately one hour of anonymized network traffic traces from a DDoS attack. All non-attack traffic have been removed from the get-go and traces anonymized using CryptoPAn prefix-preserving anonymization [49].

After obtaining the relevant packet traces from the two datasets and processing them to usable formats, the two were then merged to create a new dataset with a total of 10 network classes - all of the earlier 9 and an additional 'DDoS' class. This new dataset helps guarantee that a working model can at least detect normal and anomalous (including of the DDoS type) network flows to a great degree of accuracy.

Feature Selection: Many models, especially those based on regression slopes and intercepts, will estimate parameters for every included feature. Because of this, the presence of non-informative features can add uncertainty to predictions and reduce the overall effectiveness of the model [50]. Issues relating to over-fitting and computational complexity can become accentuated when redundant dataset features are used to train models. With these in mind, and considering the sizes of the datasets, we had to employ three feature-selection algorithms to remove non-informative or redundant predictors from the dataset, namely the *ANOVA, Chi-Squared* and *Mutual Information* algorithms. These were carefully selected since they work well with mixed data types (numerical, categorical and ordinal) and are better suited for classification modeling problems. The features eventually picked for the experiments are seen in Table I.

TABLE I
SELECTED FEATURES AND THEIR DESCRIPTIONS

Feature	Description
Proto	The upper protocol used in the transaction
State	The state and its dependent protocol
Dur	Record total duration
SrcBytes	Source to destination transaction bytes
DstBytes	Destination to source transaction bytes
SrcLoss	Source packets retransmitted or dropped
DstLoss	Destination packets retransmitted or dropped
SrcLoad	Source bits per second
DstLoad	Destination bits per second
SrcPkts	Source-to-destination packet count
DstPkts	Destination-to-source packet count
sMeanPktSz	Mean of the flow packet size transmitted by the source
dMeanPktSz	Mean of the flow packet size transmitted by the destination
TcpRtt	Tcp connection setup RTT, sum of synack and ackdat
SynAck	TCP connection setup time, the time between the SYN and the SYN_ACK packets.
AckDat	TCP connection setup time, the time between the SYN_ACK and the ACK packets

V. EXPERIMENTAL RESULTS

Our experimental results will be in two parts, addressing the two datasets used. Details of the environmental setup for the pre-processing and model training/testing stages are provided in Table II. The compute resources used for training and testing the algorithms mentioned in this paper were supplied by Chameleon Cloud [51], a configurable experimental environment for large-scale edge to cloud research.

The hyperparameters in Table III were used for training the ensemble model. To build an accurate but efficient ensemble model, we tried various combinations of generator and discriminator values and plotted the Receiver Operating Characteristic (ROC) curve for each scenario; it is a plot of the false positive rate $\frac{FalsePositives}{FalsePositives+TrueNegatives}$, or false alarm rate, against the true positive rate $\frac{TruePositives}{TruePositives+FalseNegatives}$ (or hit rate). The motive behind training the model on only benign observations is for such a system to be able to detect a wide range of network anomalies, including those not present in the datasets, as shown in [52].

TABLE II
ENVIRONMENTAL DETAILS

Number of flows	498136
CPU	AMD EPYC 7763 3.1GHz * 64 cores
Memory (RAM)	256GB
GPU	AMD Instinct MI100 (32GB) * 2

TABLE III
HYPERPARAMETERS USED FOR ENSEMBLE TRAINING

Parameter	Value
GAN type	BiGAN
Learning rate	0.00002
Number of GPUs	2
Latent dimension (encoder)	32
Training set	80% of all normal samples in the dataset
Number of generators	5
Number of Discriminators	5

As depicted in Fig. 6, we noticed no significant increase in performance beyond 5 generators and 5 discriminators, so we use this number for all our experiments.

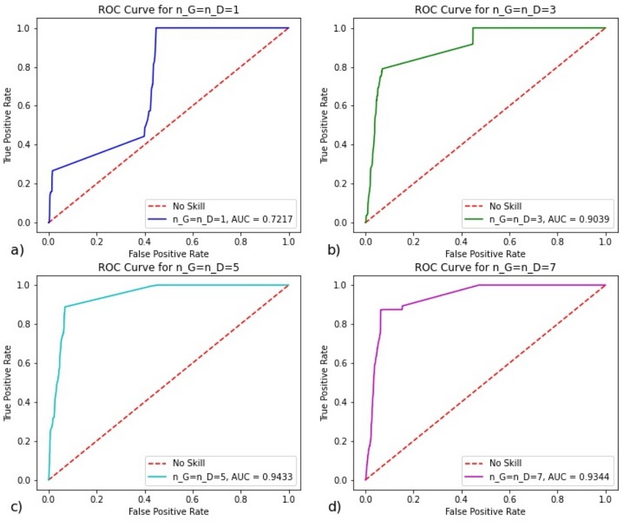


Fig. 6. ROC curve plots for ensembles built using: (a) 1 generator, 1 discriminator (b) 3 generators and 3 discriminators (c) 5 generators and 5 discriminators (d) 7 generators and 7 discriminators (based on the CAIDA-UNSWB dataset)

A. Benchmark Models and Performance Metrics

The Scikit-Learn [53] and Pytorch libraries played an integral role in the building and testing of the anomaly detector. To evaluate like-for-like algorithms, we restricted our comparisons to the following one-class models:

- Local outlier Factor (LoF): This algorithm works by computing the local density deviation of a given sample with respect to its neighbors.
- Isolation Forest (IsoF): This algorithm is an ensemble model that isolates anomalies by using binary trees instead of trying to profile normal samples.
- Minimum Covariance Determinant (MCD): This algorithm works by finding those samples in a set whose covariance matrix has the lowest determinant.

The performance metrics described in Table IV were used in our evaluation.

TABLE IV
METRICS FOR EVALUATING MODEL PERFORMANCE

Metric	Description
Precision	The fraction of the total amount of relevant instances that were actually retrieved
Recall	The fraction of relevant instances among the retrieved instances
F-1 score	The harmonic mean of precision and recall
AUROC	A measure of the model's ability to discriminate between normal and anomalous traffic
Accuracy	the ratio of correctly predicted data points to the number of all the data points

TABLE V
DETECTION PERFORMANCE FOR DIFFERENT MODELS ON THE GENI-SDN DATASET IN A TWO-CLASS SCENARIO

	accuracy	precision	recall	f1-score
EGBAD ensemble	**0.995**	**0.999**	**0.994**	**0.997**
LoF	0.989	0.998	0.989	0.994
IsoF	0.834	0.997	0.792	0.884
MCD	0.756	0.814	0.899	0.855

TABLE VI
AUROC RESULTS FOR DIFFERENT MODELS ON THE GENI-SDN DATASET USING RESPECTIVE ATTACK TYPES

	DDoS	DoS	Enumeration	Average
EGBAD ensemble	**0.999**	**0.994**	**0.999**	**0.997**
LoF	0.989	0.998	0.989	0.992
IsoF	0.834	0.997	0.792	0.874
MCD	0.756	0.814	0.899	0.823

B. GENI-SDN Results

Five BiGAN-based EGBAD models were used to train the ensemble model. Using a batch size of 1024 to fetch samples for training and a size of 32 for the latent vector, our ensemble model was able to perform remarkably when compared to other classifiers, as seen in Table V; recall values and precision for the ensemble outperform the other one-class learning algorithms used in our experiments. The plots in Fig. 7 show the AUROC performance for the various one-class models under observation and again, we observe that the EGBAD plot shows the largest area under the curve, implying a large percentage of True Positives and a low percentage of False Positives.

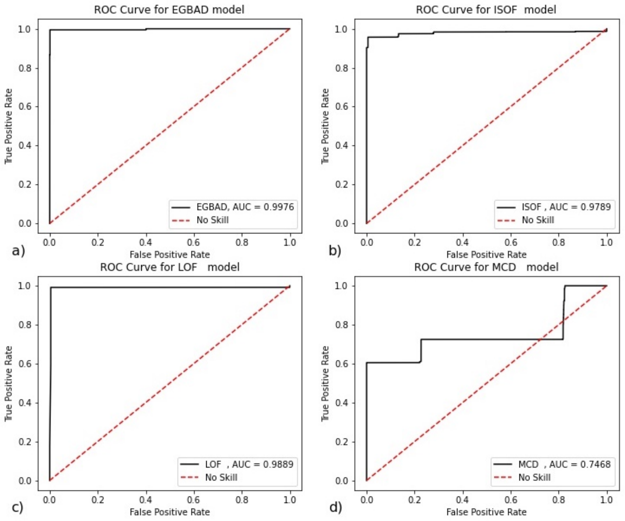


Fig. 7. ROC curve plots based for the: (a) EGBAD (b) ISOF (c) LOF (d) MCD one-class anomaly detectors based on the GENI dataset

In Table VI, we compare the AUROC results for the different models under observation using the respective attack types; we notice that the EGBAD ensemble model performs better per instance and collectively on average.

The two-class confusion matrix shown in Fig. 8 corroborates the 99.5% classification accuracy of our model, with only 0.030% of the overall testset (or 0.0015% of the anomalous part of the testset) being incorrectly classified as benign.

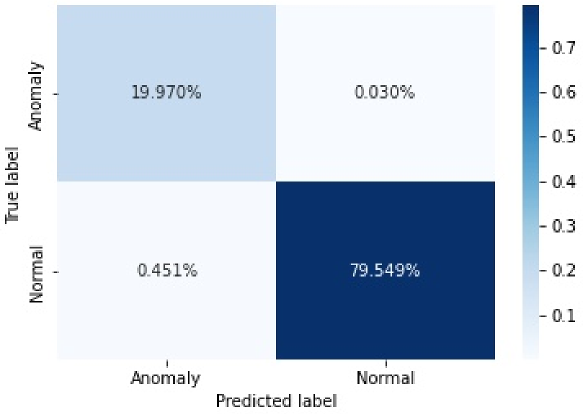


Fig. 8. Two-class confusion matrix based on GENI-SDN dataset

C. CAIDA-UNSWB Results

Like in the GENI case, a 5x5 ensemble model was used here, comprising five generators and five discriminators, all learning from each other. The composite dataset used here had more observation samples and overall attack classes, providing more variety with which to benchmark our proposed solution. We see in Table VII that our EGBAD ensemble records a 90% score in detection accuracy, with the next best model scoring a distant 83% in detection accuracy. The same is observed for the other metrics except the recall score in which the Local Outlier Factor model performs marginally better. A tight race is also observed in the AUROC performance (see Fig. 9) where the Isolation Forest model, also an ensemble, wins it at 94%, but only narrowly.

TABLE VII
DETECTION PERFORMANCE FOR DIFFERENT MODELS ON THE CAIDA-UNSWB DATASET

	accuracy	precision	recall	f1-score
EGBAD ensemble	**0.905**	**0.973**	0.973	**0.944**
LoF	0.806	0.808	**0.993**	0.891
IsoF	0.833	0.833	0.989	0.904
MCD	0.738	0.798	0.900	0.846

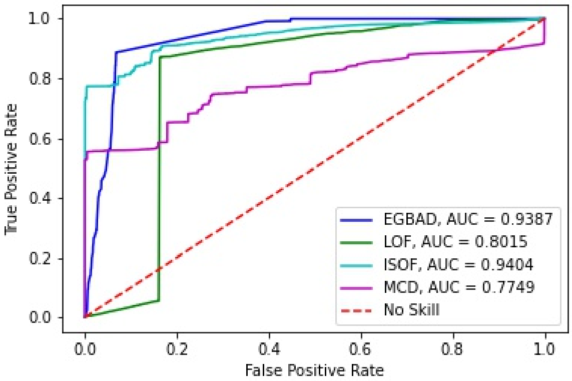


Fig. 9. AUROC results for the different models based on the CAIDA-UNSWB dataset

VI. CONCLUSIONS AND FUTURE WORK

To be able to properly detect anomalies in software-defined networks, we proposed a controller-based detection framework, including an ensemble learning technique, built on five diverse base EGBAD learners. We curated a bespoke SDN-based dataset and performed experiments in various anomaly detection scenarios, entailing a scenario with four classes (normal, DDoS, DoS and enumeration), as well as a binary-class scenario (normal and anomalous). The ensemble model showed consistently better detection performance numbers than its base learners, as well as when compared against other established one-class anomaly-detection algorithms. Similar behaviors were observed when the EGBAD model was applied to the CAIDA-UNSWB dataset even though it more observations and more attack classes than the GENI-SDN dataset. In terms of future work, we are working on a more robust dataset with even more attack classes; this would allow for an ensemble model that can accurately identify even more types of network anomalies when they occur. This presents the opportunity to create datasets from a purely SDN perspective. We also plan to test a multiple-controller-based framework that exploits a distributed approach to anomaly detection with the added benefits of resilience and redundancy.In summary, we observed an average detection accuracy above 90% over the two datasets when collapsed to just two classes (normal and abnormal). This demonstrates the potential for GAN-based algorithms to be used for network anomaly detection after training a robust discriminator network on what normal network events look like. Because this is an offline detector, training is done once, and without any impact on active network functions, as is testing with new data. The datasets and associated codes will be made available on our Github page accordingly.

ACKNOWLEDGMENT

Results presented in this paper were obtained using the Chameleon and GENI testbeds supported by the National Science Foundation.

REFERENCES

[1] D. Ezeh, "On packet classification using a decision-tree ensemble," in *Proceedings of the Student Workshop*, ser. CoNEXT'20. New York, NY, USA: Association for Computing Machinery, 2020, p. 17–18. [Online]. Available: DOI: 10.1145/3426746.3434054

[2] R. Polikar, "Ensemble based systems in decision making," *IEEE Circuits and Systems Magazine*, vol. 6, no. 3, pp. 21–45, 2006. [Online]. Available: DOI: 10.1109/MCAS.2006.1688199

[3] A. Mahfouz, A. Abuhussein, D. Venugopal, and S. Shiva, "Ensemble classifiers for network intrusion detection using a novel network attack dataset," *Future Internet*, vol. 12, no. 11, 2020. [Online]. Available: https://www.mdpi.com/1999-5903/12/11/180

[4] M. Berman, J. S. Chase, L. Landweber, A. Nakao, M. Ott, D. Raychaudhuri, R. Ricci, and I. Seskar, "Geni: A federated testbed for innovative network experiments," *Computer Networks*, vol. 61, pp. 5–23, 2014, special issue on Future Internet Testbeds - Part I. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128613004507

[5] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecur.*, vol. 2, p. 20, 2019.

[6] A. Altaher, "An improved android malware detection scheme based on an evolving hybrid neuro-fuzzy classifier (ehnfc) and permission-based features," *Neural Computing and Applications*, vol. 28, pp. 4147–4157, 2016.

[7] A. H. Hamamoto, L. F. Carvalho, L. D. H. Sampaio, T. Abrão, and M. L. Proença, "Network anomaly detection system using genetic algorithm and fuzzy logic," *Expert Systems with Applications*, vol. 92, pp. 390–402, 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S095741741730619X

[8] S. Elhag, A. Fernández, S. Alshomrani, and F. Herrera, "Evolutionary fuzzy systems: A case study for intrusion detection systems," *Studies in Computational Intelligence*, 2018.

[9] W.-C. Lin, S.-W. Ke, and C.-F. Tsai, "Cann: An intrusion detection system based on combining cluster centers and nearest neighbors," *Knowl. Based Syst.*, vol. 78, pp. 13–21, 2015.

[10] A. P. Meshram and C. Haas, "Anomaly detection in industrial networks using machine learning: A roadmap," in *ML4CPS*, 2016.

[11] S. Elhag, A. Fernández, A. Bawakid, S. Alshomrani, and F. Herrera, "On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems," *Expert Syst. Appl.*, vol. 42, pp. 193–202, 2015.

[12] J. feng Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, C. meng Wang, and Y. Liu, "A survey of machine learning techniques applied to software defined networking (sdn): Research issues and challenges," *IEEE Communications Surveys & Tutorials*, vol. 21, pp. 393–430, 2019.

[13] S. Alhaidari and M. Zohdy, "Network anomaly detection using two-dimensional hidden markov model based viterbi algorithm," in *2019 IEEE International Conference On Artificial Intelligence Testing (AITest)*, 2019, pp. 17–18.

[14] T. Kim, S. C. Suh, H. Kim, J. Kim, and J. Kim, “An encoding technique for cnn-based network anomaly detection,” in *2018 IEEE International Conference on Big Data (Big Data)*, 2018, pp. 2960–2965.

[15] P. Amangele, M. J. Reed, M. Al-Naday, N. Thomos, and M. Nowak, “Hierarchical machine learning for iot anomaly detection in sdn,” in *2019 International Conference on Information Technologies (InfoTech)*, 2019, pp. 1–4.

[16] A. Kumagai, T. Iwata, and Y. Fujiwara, “Semi-supervised anomaly detection on attributed graphs,” *2021 International Joint Conference on Neural Networks (IJCNN)*, pp. 1–8, 2021.

[17] L. Ruff, R. A. Vandermeulen, N. Görnitz, A. Binder, E. Müller, K. Müller, and M. Kloft, “Deep semi-supervised anomaly detection,” in *8th International Conference on Learning Representations, ICLR 2020, Addis Ababa, Ethiopia, April 26-30, 2020*. OpenReview.net, 2020. [Online]. Available: https://openreview.net/forum?id=HkgH0TEYwH

[18] M. E. Villa-Pérez, M. A. Álvarez Carmona, O. Loyola-González, M. A. Medina-Pérez, J. C. Velazco-Rossell, and K.-K. R. Choo, “Semi-supervised anomaly detection algorithms: A comparative summary and future research directions,” *Know.-Based Syst.*, vol. 218, no. C, apr 2021. [Online]. Available: **DOI**: 10.1016/j.knosys.2021.106878

[19] A. Shorman, H. Faris, and I. Aljarah, “Unsupervised intelligent system based on one class support vector machine and grey wolf optimization for iot botnet detection,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, 07 2020.

[20] I. Razzak, K. Zafar, M. Imran, and G. Xu, “Randomized nonlinear one-class support vector machines with bounded loss function to detect of outliers for large scale iot data,” *Future Generation Computer Systems*, vol. 112, 06 2020.

[21] K. Yang, S. Kpotufe, and N. Feamster, “An efficient one-class svm for anomaly detection in the internet of things,” *ArXiv*, vol. abs/2104.11146, 2021.

[22] H. Xiang, J. Wang, K. Ramamohanarao, Z. Salcic, W. Dou, and X. Zhang, “Isolation forest based anomaly detection framework on non-iid data,” *IEEE Intelligent Systems*, vol. 36, no. 3, pp. 31–40, 2021.

[23] N. Paulauskas and F. Bagdonas, “Local outlier factor use for the network flow anomaly detection,” *Security and Communication Networks*, vol. 8, 08 2015.

[24] A. Vikram and Mohana, “Anomaly detection in network traffic using unsupervised machine learning approach,” *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, pp. 476–479, 2020.

[25] T. Li, Z. Wang, S. Liu, and W.-Y. Lin, “Deep unsupervised anomaly detection,” in *2021 IEEE Winter Conference on Applications of Computer Vision (WACV)*, 2021, pp. 3635–3644.

[26] A. Allahdadi and R. Morla, “Anomaly detection and modeling in 802.11 wireless networks,” *J. Netw. Syst. Manag.*, vol. 27, no. 1, pp. 3–38, 2019. [Online]. Available: **DOI**: 10.1007/s10922-018-9455-2

[27] C. Han, L. Rundo, K. Murao, T. Noguchi, Y. Shimahara, Z. Milacski, S. Koshino, E. Sala, H. Nakayama, and S. Satoh, “Madgan: unsupervised medical anomaly detection gan using multiple adjacent brain mri slice reconstruction,” *BMC Bioinformatics*, vol. 22, p. 31, 04 2021.

[28] T. Schlegl, P. Seeböck, S. Waldstein, U. Schmidt-Erfurth, and G. Langs, “Unsupervised anomaly detection with generative adversarial networks to guide marker discovery,” 03 2017, pp. 146–157.

[29] Q. Yang and X. Li, “Bigan: Lncrna-disease association prediction based on bidirectional generative adversarial network,” *BMC Bioinformatics*, vol. 22, no. 1, p. 357, Jun 2021. [Online]. Available: **DOI**: 10.1186/s12859-021-04273-7

[30] Y. Zhong, W. Chen, Z. Wang, Y. Chen, K. Wang, Y. Li, X. Yin, X. Shi, J. Yang, and K. Li, “Helad: A novel network anomaly detection model based on heterogeneous ensemble learning,” *Comput. Netw.*, vol. 169, no. C, mar 2020. [Online]. Available: **DOI**: 10.1016/j.comnet.2019.107049

[31] G. Seni and I. John F. Elder, “Ensemble methods in data mining: Improving accuracy through combining predictions,” in *Ensemble Methods in Data Mining*, 2010.

[32] X. Han, X. Chen, and L.-P. Liu, “Gan ensemble for anomaly detection,” 2020.

[33] H. Zenati, C. S. Foo, B. Lecouat, G. Manek, and V. R. Chandrasekhar, “Efficient gan-based anomaly detection,” 2019.

[34] P. Lin, K. Ye, and C.-Z. Xu, *Dynamic Network Anomaly Detection System by Using Deep Learning Techniques*, 06 2019, pp. 161–176.

[35] A. Brock, J. Donahue, and K. Simonyan, “Large scale gan training for high fidelity natural image synthesis,” 2018. [Online]. Available: https://arxiv.org/abs/1809.11096

[36] M. Mirza and S. Osindero, “Conditional generative adversarial nets,” 2014. [Online]. Available: https://arxiv.org/abs/1411.1784

[37] H. Zhang, T. Xu, H. Li, S. Zhang, X. Wang, X. Huang, and D. Metaxas, “Stackgan: Text to photo-realistic image synthesis with stacked generative adversarial networks,” 2016. [Online]. Available: https://arxiv.org/abs/1612.03242

[38] M. Arjovsky, S. Chintala, and L. Bottou, “Wasserstein gan,” 2017. [Online]. Available: https://arxiv.org/abs/1701.07875

[39] A. Geron, *Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow: concepts, tools, and techniques to build intelligent systems*, second edition. ed. Sebastopol, CA: O’Reilly Media, 2019.

[40] Iperf, “Iperf, https://iperf.fr/,” 2021, last Accessed: Nov., 1.

[41] Hping, “Hping, http://hping.org/,” 2021, last Accessed: Nov., 1.

[42] Pyloris, “Pyloris, https://github.com/darkerego/pyloris,” 2021, last Accessed: Nov., 1.

[43] Nmap, “Nmap, https://nmap.org,” 2021, last Accessed: Nov., 1.

[44] AWK, “Awk manual, https://www.gnu.org/software/gawk/manual/gawk.html,” 2021, last Accessed: Nov., 1.

[45] BASH, “Bourne again shell, https://www.gnu.org/software/bash/,” 2021, last Accessed: Nov., 1.

[46] TCPdump, “Tcpdump, https://tcpdump.org/,” 2021, last Accessed: Nov., 1.

[47] ARGUS, “Argus, https://openargus.org/,” 2021, last Accessed: Nov., 1.

[48] N. Moustafa and J. Slay, “Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set),” in *2015 Military Communications and Information Systems Conference (MilCIS)*, 2015, pp. 1–6. [Online]. Available: **DOI**: 10.1109/MilCIS.2015.7348942

[49] CAIDA, “Caida ddos dataset, https://www.caida.org/data/passive/ddos-20070804_dataset.xml,” 2021, last Accessed: Nov., 1.

[50] M. Kuhn, *Applied predictive modeling*. New York: Springer, 2013. [Online]. Available: **DOI**: 10.1007/978-1-4614-6849-3

[51] K. Keahey, J. Anderson, Z. Zhen, P. Riteau, P. Ruth, D. Stanzione, M. Cevik, J. Colleran, H. S. Gunawi, C. Hammock, J. Mambretti, A. Barnes, F. Halbach, A. Rocha, and J. Stubbs, “Lessons learned from the chameleon testbed,” in *Proceedings of the 2020 USENIX Annual Technical Conference (USENIX ATC ’20)*. USENIX Association, July 2020.

[52] D. Ezeh, “Exploring advanced machine learning solutions for traffic classification, anomaly detection, and adaptive data transmission in software defined networks,” Ph.D. dissertation, Drexel University, 2023.

[53] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, “Scikit-learn: Machine learning in Python,” *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011. [Online]. Available: **DOI**: 10.48550/arXiv.1201.0490

Dubem A. Ezeh received his B.Eng degree in Electrical Engineering from Ahmadu Bello University, Nigeria, in 2009, his MS degree in Telecommunications Engineering from Staffforsdshire University, UK, in 2012, and is currently pursuing a PhD degree in Computer Engineering from Drexel University, USA. His research interests include Software-Defined Networks, Traffic Engineering, Network Security and Machine Learning Applications in Computer Networks.

Jaudelice de Oliveira is an Associate Professor in the Department of Electrical and Computer Engineering (ECE) at Drexel University. She earned her B.S.E.E. degree from Federal University of Ceara, Ceara, Brazil, M.S.E.E. from the State University of Campinas, São Paulo, Brazil, and her Ph.D. degree in ECE from the Georgia Institute of Technology. Currently, her research interests include Software Defined Networks, Smart Grid and IoT. She is a Member of the IEEE and Senior Member of the ACM.

Performance Analysis of Encryption Capabilities of ARM-based Single Board Microcomputers

Sandor R. Repas

***Abstract*—In the few years since the Raspberry Pi was released in 2012, countless microcomputers based on the ARM architecture have been introduced. Their small size, high performance relative to their power consumption, and the ability to run the popular Linux operating system make them ideal for a wide range of tasks. Information security is an area of particular importance. Different encryption and encoding algorithms play an important role in almost all areas of information security. However, these algorithms are very computationally intensive, so it is important to investigate which microcomputers can be used for these tasks, and under which trade-offs.**

The performance of ten different microcomputers is investigated and presented for the application of common symmetric and public-key encryption and decryption, digest creation and message authentication protocols, such as RSA, AES, HMAC, MD5, SHA.

Reliable encryption requires the generation of reliable (pseudo)random numbers (Cryptographically Secure Random Numbers, CSRN), and microcomputers based on ARM SoCs usually have hardware implemented (pseudo)random number generators. The applicability of the random number generators of different microcomputers are investigated and presented; test methods are described, and recommendations are made.

***Index Terms*—ARM; encryption; performance; security; random numbers**

I. Introduction

As semiconductor technologies continue to evolve, microprocessors and microcontrollers have emerged that can be produced at ever lower cost and with ever lower power consumption, and offer ever higher performance. As the degree of integration has increased, it has become possible to produce integrated circuits that incorporate both the microprocessor and the additional circuitry (e.g. memory, graphics, and USB controllers.). These chips (System on a Chip, SoC) are used to build the increasingly popular smart phones, and the popularity of smart handsets is accelerating the development of these circuits. Increasingly powerful SoCs have also enabled the emergence of Single Board Computers (SBCs), the best known of which is the ARM architecture-based [1] Raspberry Pi [2] with a 700 MHz single-core processor and 256 MB of memory, released in 2012. Thanks to rapid development, SBCs with eight cores and 2GB of memory are now available [3].

Today information security plays an increasingly important role, with encryption, decryption, digital signatures and signature verification being of high importance. However, encryption operations are mathematical operations with a very high computational demand. With the proliferation of increasingly powerful yet cost-effective SBCs, an important question is what encryption capabilities SBCs have, and thus how effectively they can be applied in the field of information security.

In the following, we present in detail our methods used to investigate the encryption capabilities of SBCs, as well as the results.

II. Summary of the Current Research Results

Many papers have been published on Raspberry Pi and other SBCs, but none of them have explicitly investigated their encryption capabilities.

In [4], the authors present, among other results, their solution for the Raspberry Pi to create a secure TFTP (Secure Trivial File Transfer Protocol) to ensure the security of remote updates.

Researchers have investigated the performance of BeagleBone Black [5], BeagleBone, and Raspberry Pi SBCs using LMbench [6], and their proprietary application (CoAP, Constrained Application Protocol) to measure performance on constrained devices [7]. They concluded that the SBCs were less than half the speed of a modern computer, and the BeagleBone Black had the lowest latency of the three devices. Their important conclusion is that for IoT (Internet of Things) applications, faster and more expensive external memory has significantly less impact on the performance of an SBC than the type of the processor. In addition, running the graphical interface did not have a significant impact on performance.

In two papers, researchers presented results of memory and processor performance tests on four different ARM platforms in [8] and [9]. Their measurements were also compared to Intel Atom [10] processors, which produced similar results, but with significantly lower power consumption on ARM SoC-based

S. R. Repas is with the Department of Telecommunications, Széchenyi István University, Győr, Hungary (e-mail: repas.sandor@sze.hu).

DOI: 10.36244/ICJ.2023.2.6

TABLE I
The Most Important Parameters of the Selected SBCs

Model	CPU architecture	SoC type	CPU cores (pcs)	CPU freq. (GHz)	RAM size (GB)
Banana Pi	Cortex A7	AllWinner A20	2	1	1
Banana Pi M2	Cortex A7	AllWinner A31s	4	1	1
BeagleBone Black	Cortex A8	TI AM3359	1	1	0.5
ODROID-C1	Cortex A5	Amlogic S805	4	1.5	1
ODROID-U3	Cortex A9	Samsung Exynos 4412	4	1.7	2
ODROID-XU3 Lite	Cortex A15+A7	Samsung Exynos 5422	4+4	1.8+1.3	2
Orange Pi Mini	Cortex A7	AllWinner A20	2	1	1
Orange Pi Plus	Cortex A7	AllWinner H3	4	1.6	1
Raspberry Pi Model B+	1176JZ(F)-S	Broadcom BCM2835	1	0.7	0.5
Raspberry Pi 2 Model B+	Cortex A7	Broadcom BCM2836	4	0.9	1

devices. The authors also point out that this may change in the future.

Using BeagleBoard and PandaBoard [11], researchers investigated the potential of using ARM SoC-based devices in HPC (High Performance Computing) applications [12], with a focus on computing performance and power consumption. The authors concluded that due to the high power consumption of devices that are redundant for HPC applications (e.g. USB, HDMI, VGA, etc.), SBCs based on generic SoCs are not well suited for HPC designs.

In [13], the authors investigated six different types of SBCs from several aspects, with the aim of finding out the performance of a heterogeneous cluster built from different SBCs in discrete-time simulations performed in parallel as described in [14] and [15]. Their important result is that multicore performance should be the primary consideration in the calculations.

These publications do not investigate the performance of SBCs during encryption operations; therefore, it is necessary to develop methods for measuring this and to perform the tests.

III. Test Methods

The devices chosen for the performance tests and the test methods applied are described below.

A. *Selection of Devices*

In selecting the SBCs, the primarily following criteria were considered:

- The Raspberry Pi is a must due to its pervasiveness, as it greatly increases the usability of the results.
- It is important to measure as many different SoCs as possible, thus providing a comprehensive picture for comparing each SoC.
- Include in the tests two SBCs from different manufacturers, based on the same SoC. This should help to find out how much of the performance depends on the SoC and how much on the external components (e.g. memory) used with the SoC.
- At least one SBC based on a SoC using the Big-Little [16] architecture will be investigated. In this way, the advantages and disadvantages of such an SoC will be identified.

Table I shows the main parameters of the selected SBCs. (The datasheets for each SoC were not always made available by the manufacturers, so I could not include some parameters, such as cache size.)

B. *Test Environment for the Encryption Performance Measurements*

Linux was installed on all SBC devices to perform the tests. If the manufacturer provides or recommends a Linux version for the device, that version was used. In all cases, we tried to make only the most necessary changes, avoiding any modifications that could affect performance. The only exception to this was disabling the launch of the graphical interface on all devices so that it did not affect the measurement results.

To perform the measurements, we needed to implement the network shown in Fig. 1. The measurement process was started from the laptop at the top of the figure and its progress could also be monitored from there. The server on the left of the figure controlled the measurement, and collected and pre-processed the data. The ten SBCs tested are shown at the bottom of the figure. To ensure comparability, all measurements were also performed on the Sun Sunfire X2100 M2 computer on the right side of the figure, which contained an Opteron 1222 dual core CPU and 4 pieces of 2GB DDR2-5300 ECC RAM modules.

IV. Measurements and Results

To ensure accurate results, the measurements were automated using bash shell scripts. Each measurement was repeated 16 times, of which only the results of the last 11 times

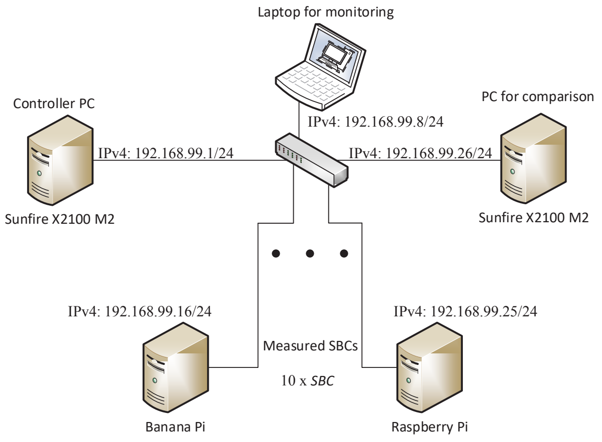


Fig. 1. Topology of the test network for the measurements

were processed. This avoided the influence of the storage system's speed during the measurements (by using cache). The openssl program was used for the measurements. Where it is applicable, measurements were also made using one and then all cores. The measurements were also performed on the Sunfire X2100 M2 computer, making comparison easier.

In order to avoid errors, the results were collected in text files, pre-processed using awk scripts and then evaluated.

In the following, the measurement results will be described and then evaluated in detail.

A. Symmetric Key Encryption

Today's most widely used symmetric key encryption is the Advanced Encryption Standard (AES) using the Rijndael algorithm [17]. It is also used with 128, 192 and 256-bit-long keys. Its use is very widespread. Its performance in file encryption has been investigated in Cipher Block Chaining (CBC) mode, which greatly increases the protection against algorithmic attacks.

The measurements were performed using the openssl speed command, with all three key lengths, 8k block size, on 1 and then with multiple threads. The use of multiple threads allowed the simultaneous use of multiple CPU cores.

1) Single Thread Results

The average values of the speed results obtained in the runs is shown in Table II, while the standard deviations are shown in Table III. The averages are visualized for better comparison in Fig. 2.

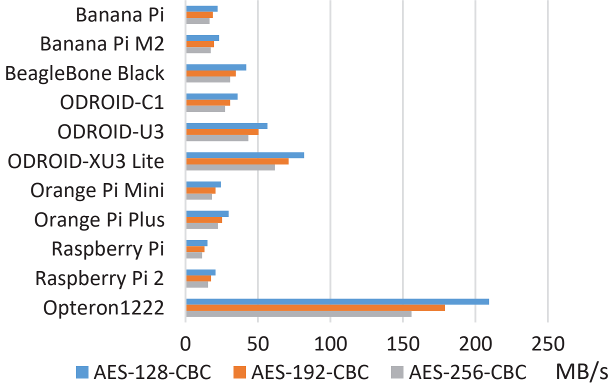


Fig. 2. Average speed values of AES-CBC encryption (MB/s), 1 thread, 8k block

The first column of Table II shows the type of SBC tested. The second column is the average of the amount of data encrypted per second in MB when using 128-bit key length AES CBC (AES-128-CBC). The third column contains the average of the data volume encoded per second using AES-192-CBC, and the last column contains the average of the data volume encoded per second using AES-256-CBC. The corresponding columns in Table III contain the standard deviation values for the calculated mean values.

2) Discussion of the Results

The analysis of the values shows that:

- Odroid-XU3 Lite is the fastest, Odroid-U3 is the second, and BeagleBone Black is the third one.
- The Raspberry Pi is the slowest.
- The two SBCs based on the same SoC produced different results (Banana Pi and Orange Pi Mini), but the difference is only around 10%.
- The standard deviation values are low compared to the average values, so the measured values are stable for the devices tested.
- The performance of each SBC relative to the other is not significantly affected by the key length used for encoding.
- Even the speed of the fastest SBC is a fraction of that of the Opteron 1222-based system (e.g. for AES-128-CBC: 209.5/81.85=2.56).

3) Multi-thread Results

Multi-threaded runs have been used to test SBCs based on SoCs that contain multiple processor cores. In each case, the measurement was performed on as many threads as the processor has in the given SoC, so that all cores participated in the coding and the aggregate performance could be measured. In the case of Odroid-XU3 Lite using the Big-Little architecture, the measurement was also performed using 4 threads due to the different core speeds. To present the results, we have chosen the AES-256-CBC encoding values, which are shown in Table IV.

The second column shows how many threads were used for each measurement. The third column shows the average amount of the encoded data from the last 11 measurements. The data in the fourth column has already been presented for the single

TABLE II
AVERAGE SPEED VALUES OF AES-CBC ENCRYPTION (MB/S), SINGLE THREAD, 8K BLOCK

Model	AES-128	AES-192	AES-256
Banana Pi	22.06	18.88	16.60
Banana Pi M2	23.15	19.74	17.49
BeagleBone Black	41.85	34.70	30.82
ODROID-C1	35.95	30.86	27.26
ODROID-U3	56.59	50.44	43.27
ODROID-XU3 Lite	81.85	71.05	61.77
Orange Pi Mini	24.45	20.81	18.33
Orange Pi Plus	29.72	25.32	22.29
Raspberry Pi Model B+	15.06	13.04	11.50
Raspberry Pi 2 Model B+	20.62	17.58	15.59
Opteron 1222	209.50	179.08	156.01

TABLE III
STANDARD DEVIATION OF SPEED VALUES OF AES-CBC ENCRYPTION (MB/S), SINGLE THREAD, 8K BLOCK

Model	AES-128	AES-192	AES-256
Banana Pi	0.04	0.03	0.03
Banana Pi M2	0.07	0.04	0.04
BeagleBone Black	0.08	0.06	0.05
ODROID-C1	0.20	0.16	0.14
ODROID-U3	0.48	0.42	0.37
ODROID-XU3 Lite	0.07	0.01	0.03
Orange Pi Mini	0.04	0.08	0.05
Orange Pi Plus	0.03	0.00	0.00
Raspberry Pi Model B+	0.00	0.00	0.00
Raspberry Pi 2 Model B+	0.01	0.03	0.01
Opteron 1222	0.13	0.09	0.07

TABLE IV
AVERAGE SPEED VALUES OF AES-256-CBC ENCRYPTION (MB/S), MULTIPLE THREADS, 8K BLOCK

Model	Thr.	AES-256 *x* threads (MB/s)	AES-256 1 thread (MB/s)	Rel. acc.	Std. dev.
Banana Pi	2	33.22	16.60	2.00	0.02
Banana Pi M2	4	69.96	17.49	4.00	0.02
ODROID-C1	4	109.57	27.26	4.02	0.04
ODROID-U3	4	88.43	43.27	2.04	7.38
ODROID-XU3 L.	4	195.01	61.77	3.16	1.01
ODROID-XU3 L.	8	276.21	61.77	4.47	2.20
Orange Pi Mini	2	36.36	18.33	1.98	0.01
Orange Pi Plus	4	46.55	22.29	2.09	6.40
Raspberry Pi 2	4	62.31	15.59	4.00	0.01
Opteron 1222	2	310.88	156.01	1.99	0.32

thread measurement, it is only presented again here for ease of reference.

The relative acceleration in column 5 is the ratio of the average speeds in the fourth and third columns. The last column contains the standard deviation values for the third column.

4) *Discussion of the Results*

The analysis of the values shows that:

- Odroid-XU3 Lite is the fastest, Odroid-C1 is the second and Odroid-U3 is the third.
- The Odroid-U3 and Orange Pi Plus produce large standard deviations. The measured performance is not constant, shows large fluctuations and the system behavior can only be estimated imprecisely.
- Among devices with low standard deviation, the fastest SBCs are Odroid-XU3 Lite, Odroid-C1, Banana Pi M2 and Raspberry Pi 2.
- The relative acceleration is almost equal to the number of cores used, except for the two devices with high standard deviation and the Big-Little architecture Odroid-XU3 Lite. By increasing the number of cores, a linearly proportional acceleration is obtained.
- The performance of the fastest SBC (Odroid-XU3 Lite with 8 threads) now approaches that of the Opteron 1222 system.

5) *Message Digest and Authentication*

- The use of hash function and message authentication code is also essential to ensure secure communication. They are generally used to ensure integrity and detect tampering. The analyzed protocols and some of their characteristics:
- MD5
  - 128 bit-long digest
  - Not secure, but used for compatibility reasons.
- SHA1
  - 160 bit-long digest
  - No longer recommended
  - Widespread, widely known and used.
- SHA256
  - 256 bit-long digest
  - Recommended for use.
- SHA512
  - 512 bit long digest
  - Not always recommended due to its slowness.
- HMAC
  - MD5-based message authenticator
  - Keyed-Hash Message Authentication Code

6) *Single Thread Results*

The average values of the results obtained in the runs is shown in Table V, while the standard deviations are shown in Table VI. The averages are visualized for better comparison in Fig. 3.

The structure of the table is very similar to the one used for the previous tables, so it is not explained in detail.

7) *Discussion of the Results*

The analysis of the values shows that:

- The fastest is Odroid-XU3 Lite, the second is Odroid-U3.
- The slowest is Raspberry Pi.
- The two SBCs based on the same SoC produced different results (Banana Pi and Orange Pi Mini), but again the difference is only around 10%.
- The standard deviation values are low compared to the average values, so the measured values are stable for the devices tested.
- The relative performance of each SBC is not necessarily the same for different tasks (e.g. Odroid-C1 and BeagleBone Black MD5: 118.71/102.88=1.15, while for SHA1: 73.62/77.57=0.95).
- Even the speed of the fastest SBC is a fraction of that of the Opteron 1222-based system (e.g. for MD5: 562.56/240.15=2.34, while for SHA512: 290.29/95.70=3.03).

TABLE V
AVERAGE SPEED VALUES OF DIGEST AND MESSAGE AUTHENTICATION (MB/S), SINGLE THREAD, 8K BLOCK

Model	MD5	SHA 1	SHA 256	SHA 512	HMAC
Banana Pi	82.49	44.29	26.01	22.35	82.62
Banana Pi M2	82.96	46.30	27.93	14.12	82.83
BeagleBone Black	102.88	77.57	56.30	37.88	104.70
ODROID-C1	118.71	73.62	43.43	36.66	118.88
ODROID-U3	200.43	118.47	69.70	59.88	200.17
ODROID-XU3 L.	240.15	158.88	91.43	95.70	242.87
Orange Pi Mini	91.53	48.22	28.33	24.41	91.90
Orange Pi Plus	111.43	58.67	34.52	29.69	111.98
Raspberry Pi	51.92	29.12	18.79	9.11	53.15
Raspberry Pi 2	73.77	41.19	24.84	12.56	73.65
Opteron 1222	562.56	430.60	186.18	290.29	562.81

TABLE VI
STANDARD DEVIATION OF SPEED VALUES OF DIGEST AND MESSAGE AUTHENTICATION (MB/S), SINGLE THREAD, 8K BLOCK

Model	MD5	SHA 1	SHA 256	SHA 512	HMAC
Banana Pi	0.23	0.11	0.05	0.02	0.16
Banana Pi M2	0.13	0.11	0.04	0.03	0.17
BeagleBone Black	0.08	0.10	0.09	0.07	0.15
ODROID-C1	0.72	0.37	0.23	0.19	0.69
ODROID-U3	2.05	1.21	0.68	0.54	1.80
ODROID-XU3 L.	0.18	0.25	0.14	0.08	0.20
Orange Pi Mini	0.53	0.47	0.05	0.02	0.20
Orange Pi Plus	0.03	0.01	0.00	0.00	0.08
Raspberry Pi	0.10	0.01	0.03	0.00	0.03
Raspberry Pi 2	0.08	0.03	0.06	0.01	0.15
Opteron 1222	1.11	0.17	0.85	0.08	0.71

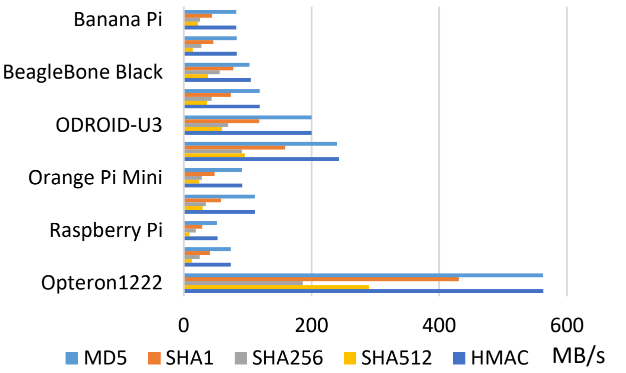


Fig. 3. Average speed values of digest and message authentication (MB/s), single thread, 8k block

TABLE VII
AVERAGE SPEED VALUES OF SHA256 MESSAGE DIGEST CREATION (MB/S), MULTIPLE THREADS, 8K BLOCK

Model	Thr.	SHA256 *x* threads (MB/s)	SHA256 1 thread (MB/s)	Rel. acc.	Std. dev.
Banana Pi	2	52.04	26.01	2.00	0.08
Banana Pi M2	4	111.79	27.93	4.00	0.13
ODROID-C1	4	174.79	43.43	4.02	0.21
ODROID-U3	4	260.81	69.70	3.74	112.01
ODROID-XU3 L.	4	317.19	91.43	3.47	6.99
ODROID-XU3 L.	8	442.94	91.43	4.84	31.49
Orange Pi Mini	2	56.32	28.33	1.99	0.13
Orange Pi Plus	4	72.00	34.52	2.09	32.10
Raspberry Pi 2	4	99.54	24.84	4.01	0.09
Opteron 1222	2	370.94	186.18	1.99	1.72

TABLE VIII
AVERAGE EXECUTION TIMES OF 100 PIECES OF ENCRYPTION AND DECRYPTION BY RSA ALGORITHM (IN SECONDS) – LOWER IS BETTER!

Model	2048 bit encr.	2048 bit decr.	4096 bit encr.	4096 bit decr.
Banana Pi	2.71	7.89	3.14	38.54
Banana Pi M2	2.43	7.07	2.82	34.42
BeagleBone Black	3.03	7.68	3.42	34.58
ODROID-C1	1.74	5.05	2.02	24.56
ODROID-U3	1.10	3.30	1.28	16.12
ODROID-XU3 L.	1.18	2.73	1.31	11.41
Orange Pi Mini	2.88	7.62	3.28	35.33
Orange Pi Plus	2.22	6.16	2.55	29.27
Raspberry Pi	6.63	15.19	7.36	64.64
Raspberry Pi 2	2.93	8.15	3.37	38.84
Opteron 1222	0.50	0.74	0.52	1.89

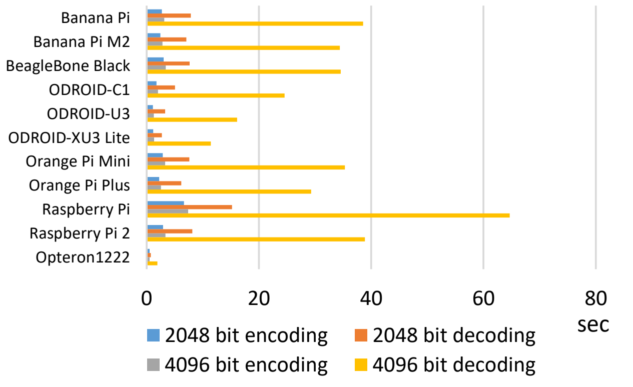


Fig. 4. Average execution times of 100 pieces of encryption and decryption by RSA algorithm (in seconds) – Lower is better!

8) Multi-thread Results

To present the results, we have chosen the SHA256 digest generation, which are shown in Table VII. The structure of the table is the same as in Table IV.

9) Discussion of the Results

The analysis of the values shows that:

- Odroid-XU3 Lite is the fastest, Odroid-U3 is the second, and Odroid-C1 is the third.
- The Odroid-XU3 Lite, Odroid-U3 and Orange Pi Plus produce large standard deviations (The ratio of speed to standard deviation for devices Odroid-U3 and Orange Pi Plus are almost identical). The measured performance is not constant, shows significant fluctuations and the system behavior is not predictable.
- Among devices with low standard deviation, the fastest SBCs are Odroid-C1, Banana Pi M2 and Raspberry Pi 2.
- The relative acceleration is almost equal to the number of cores used, except for the three devices with high standard deviation. By increasing the number of cores, a linearly proportional acceleration is obtained.

B. Public key Cryptography

Public key cryptography is generally used for the encrypted transmission of symmetric keys, and the creation of digital signatures. The methods currently in use are extremely computationally intensive and slow, so they are usually used in combination with symmetric encryption for transmitting large amounts of data. The most widely used RSA encryption, developed by Ron Rivest, Adi Shamir and Leonard Adleman, was investigated with 2048 and 4096 bit long keys, as the minimum key length currently recommended for adequate security is 2048 bits.

1) RSA Encryption Results

In the RSA encryption, the same randomly generated file was encrypted and decrypted with the same key pair for each SBC. To test the performance of encryption using the 2048-bit key, one 1920-bit file was encrypted or decrypted 100 times in each measurement cycle for the 2048-bit key, and a 4000-bit file for the 4096-bit key (RSA is only able to encrypt data to a maximum amount equal to the key size, minus padding and header data.). The results of the test are presented in Table VIII and graphically displayed in Fig. 4.

2) Discussion of the Results

The analysis of the values shows that:

- Odroid-U3 is the fastest for encoding, Odroid-XU3 Lite is the second, while for decoding, the order is reversed. Odroid-C1 is the third one in all cases.
- The slowest is the Raspberry Pi.
- The two SBCs based on the same SoC produced different results (Banana Pi and Orange Pi Mini), with the Banana Pi being faster in the encoding operation and the Orange Pi Mini in the decoding operation. In all cases, the differences were below 10% for the two SoCs.
- The relative performance of each SBC to the other is not necessarily the same for the different tasks.

- Even the speed of the fastest SBC is a fraction of that of the Opteron 1222-based system (e.g. for 4096-bit key length decoding: 11.41/1.89=6.04).

C. Random Number Generation

Random numbers and their generation play a key role in cryptography. Without the right random numbers, secure encryption cannot be done. Generating true random numbers (TRNs) with computers is almost impossible. There are several algorithms for generating pseudo random numbers (PRN), which are recommended for different purposes. Some are explicitly not recommended for encryption tasks, while others are suitable (e.g. Dual_EC_DRBG).

According to the available information, (almost) all ARM-based SoCs under investigation have some kind of hardware random number generator (HWRNG). The following information has been extracted from publicly available documentation:

- Amlogic S805: Built-in LSFR Random number generator.
- TI AM3359: Crypto Hardware Accelerators (AES, SHA, PKA, RNG).
- Allwinner A20: 160-bit hardware PRNG with 192-bit seed.
- Allwinner A31: 160-bit hardware PRNG with 192-bit seed.
- Allwinner H3: 160-bits hardware PRNG with 175-bits seed. 256-bits TRNG.
- Samsung Exynos 5422: Hardware Crypto Accelerators: AES, DES/3DES, ARC4, SHA-1/SHA-256/MD5/HMAC/PRNG, TRNG, PKA, and Secure Key Manager.

The two SoCs produced by Broadcom also contain some form of HWRNG, but no documentation has been found.

1) Support

HWRNG is not well documented for any of the SoCs examined. Only partial information could be found.

A common Linux driver for all Allwinner SoCs HWRNG is produced, but at the time of testing it was not yet working reliably.

No information could be found for Samsung SoCs.

The HWRNG of the TI AM3359 SoC is supported in the new kernels, however the Linux released for the BeagleBone Black does not yet have this kernel.

The Amlogic S805 in Odroid-C1 is supported.

The two Broadcom SoCs found in the Raspberry Pi SBCs are also supported.

2) Tests

a) Entropy

Due to the shortcomings of the documentation, we were only able to examine the quality of the random numbers to a limited extent: we only performed statistical analysis on the (pseudo)random numbers generated by the SBCs. The most commonly used tools for statistical analysis and their latest versions are the following:

- Diehard [18]
- Dieharder 3.31.1 [19]
- NIST Special Publication 800-22rev1a 2.1.2 [20]
- Ent [21]
- rngtest [22]
- TestU01 1.2.3 [23]
- Practically Random 0.94 [24]

To perform the tests, 10GB of (pseudo)random numbers were generated and analyzed. The results of the analyses are summarized in Table IX.

TABLE IX
RESULTS OF THE STATISTICAL ANALYSIS OF THE GENERATED RANDOM NUMBERS

Model	Dieharder	Ent X^2 distribution	NIST 800-22
ODROID-C1	Passed	suspect (98,71%)	1 error
Raspberry Pi	1 weak (bitstream)	Ok (59,7%)	Success
Raspberry Pi 2	1 weak (rank 32x32)	almost suspect (90,83%)	1 error

TABLE X
THE SPEED VALUES OF THE HARDWARE RANDOM NUMBER GENERATORS

Model	Speed
ODROID-C1	7.3MB/s
Raspberry Pi	105kB/s
Raspberry Pi 2	147kB/s

The results show that none of the random numbers generated by the systems can be used for encryption. However, the Linux kernel is prepared to use multiple sources for random number generation, so the weakness of one source is not necessarily a problem, but the use of HWRNG can speed up random number generation. It is also important to note that the lack of proper documentation (hence knowledge of how the SoC HWRNG works) is also a drawback for its use in encryption applications.

b) Visual Analysis

Rather just for interest, we also visually examined the quality of the random numbers produced. Fig. 5. shows the images created from the generated random numbers in 256 by 256 grids of (24 bit) RGB values. A close inspection of the figures does not reveal any anomalous repetition or shape.

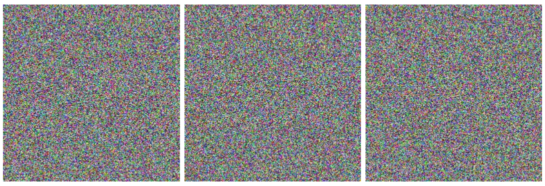


Fig. 5. Images created from random numbers generated by Odroid-C1, Raspberry Pi, and Raspberry Pi 2

c) Speed

Table X shows the speed of random number generation using the HWRNG for the three SBCs under study.

V. CONCLUSIONS

The results show that even the slowest SBC has sufficient performance to perform the encryption task required in a normal application. For more specialized applications with higher amount of encrypted traffic, the characteristics of each SBC need to be taken into account.

If only one processor core can be used efficiently due to the application, then the BeagleBone Black is recommended rather than Raspberry Pi Model B+ (While it is worth noting that the Odroid-XU3 Lite produces the highest speed with single thread in almost all cases.).

The use of Odroid-XU3 Lite, Odroid-U3 and Orange Pi Plus should be avoided due to their performance fluctuation under heavy load. Further investigation is required to determine the reasons.

Due to its performance and predictable, stable operation, we recommend using Odroid-C1 for encryption applications (moreover, its HWRNG is the fastest among the devices tested). For its speed, the Bana Pi M2 is also a good choice. For its coverage, and thus support and awareness, the Raspberry Pi 2 is recommended.

The HWRNGs we tested do not provide reassuring entropy, but we found the fewest problems with Raspberry Pi.

Different memory speeds of SBCs based on the same SoCs do not significantly affect the performance of the SBC.

VI. SUMMARY AND FURTHER RESEARCH

Based on the results, SBCs are cost-effective, energy-efficient devices that are well suited for information security applications.

Further measurements of encryption capabilities (e.g. HTTPS, SCP, SFTP, IPsec) need to be developed and performed to determine their potential applications. The performance of network transmissions is an important area to be investigated.

Finally, it is important to investigate the virtualization capabilities of each SBC, as well as its compatibility with other operating systems in the security domain. (e.g. OpenBSD, FreeBSD.)

ACKNOWLEDGMENT

We thank HunNet-Média Ltd. for providing us with the single-board computers for the studies, thus contributing to the publication.

REFERENCES

[1] https://www.arm.com/

[2] Raspberry Pi Foundation, https://www.raspberrypi.org/

[3] ODROID-XU3 Lite, https://www.hardkernel.com/shop/odroid-xu3-lite/

[4] M. A. M. Isa et al., "A Series of Secret Keys in a Key Distribution Protocol," in *Transactions on Engineering Technologies, London*, UK, 2-4 July 2014, pp. 615–628. DOI: 10.1007/978-94-017-9804-4_43

[5] BeagleBone Black, https://beagleboard.org/black

[6] LMbench - Tools for Performance Analysis, http://lmbench.sourceforge.net/

[7] C. P. Kruger and G. P. Hancke, "Benchmarking Internet of things devices," in *Proc. 2014 12th IEEE International Conference on Industrial Informatics (INDIN)*, Porto Alegre, Brazil, 27-30 July 2014, pp. 611–616. DOI: 10.1109/INDIN.2014.6945583

[8] R. G. Reed et al., "A CPU benchmarking characterization of ARM based processors," *Computer Research and Modeling*, vol. 7, issue 3, pp. 581–586. 2015. DOI: 10.20537/2076-7633-2015-7-3-505-509

[9] G. T. Wrigley, R. G. Reed, B. Mellado, "Memory benchmarking characterisation of ARM-based SoCs," *Computer Research and Modeling*, vol. 7, issue 3, pp. 607–613. 2015. DOI: 10.20537/2076-7633-2015-7-3-607-613

[10] Intel Atom processor, https://www.intel.com/content/www/us/en/products/details/processors/atom.html

[11] https://hu.mouser.com/new/pandaboardorg/pandaboardES/

[12] E. L. Padoinetal., "Evaluating Performance and Energy on ARM-based Clusters for High Performance Computing," in *Proc. 2012 41st International Conference on Parallel Processing Workshops*, Pittsburgh, USA, 10-13. September 2012, pp. 165–172. DOI: 10.1109/ICPPW.2012.21

[13] G. Lencse and S. Répás, "Method for Benchmarking Single Board Computers for Building a Mini Supercomputer for Simulation of Telecommunication Systems," in *Proc. 2015 38th International Conference on Telecommunications and Signal Processing (TSP)*, Prague, Czech Republic, 9-11 July 2015, pp. 246–251. DOI: 10.1109/TSP.2015.7296261

[14] G. Lencse, I. Derka, L. Muka, "Towards the Efficient Simulation of Telecommunication Systems in Heterogeneous Distributed Execution Environments," in *Proc. 2013 36th International Conference on Telecommunications and Signal Processing (TSP)*, Rome, Italy, 2-4 July 2013, pp. 304–310. DOI: 10.1109/TSP.2013.6613941

[15] G. Lencse and I. Derka, "Measuring the Efficiency of Parallel Discrete Event Simulation in Heterogeneous Execution Environments", *Acta Technica Jaurinensis*, vol. 9. no. 1. pp. 42–53, DOI: 10.14513/actatechjaur.v9.n1.394

[16] H. D. Cho, K. Chung, T. Kim, "Benefits of the big. LITTLE Architecture", TechOnline, https://www.techonline.com/tech-papers/benefits-of-the-big-little-architecture/

[17] Announcing the ADVANCED ENCRYPTION STANDARD (AES), Federal Information Processing Standards Publication 197, National Institute of Standards and Technology, November 26, 2001. Available: https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.197.pdf

[18] The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness, https://web.archive.org/web/20160125103112/ http://stat.fsu.edu/pub/diehard/

[19] Dieharder: A Random Number Test Suite, https://webhome.phy.duke.edu/~rgb/General/dieharder.php

[20] A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, https://csrc.nist.gov/publications/detail/sp/800-22/rev-1a/final, DOI: 10.6028/NIST.SP.800-22r1a

[21] ENT A Pseudorandom Number Sequence Test Program, https://www.fourmilab.ch/random/

[22] rng-tools, https://github.com/nhorman/rng-tools

[23] TestU01, http://simul.iro.umontreal.ca/testu01/tu01.html

[24] PractRand, https://github.com/MartyMacGyver/PractRand

Sandor R. Repas received his BA in Business Management University Hungary in 2009, BSc in Electrical Engineering from the Óbuda University in 2011, MSc in Electrical Engineering from the Széchenyi István University in Administration and from the Corvinus of Budapest, Budapest 2013 and MSc in Defence C3 System Manager from National University of Public Service in 2017. He received his PhD in computer science from the Széchenyi István University in 2018.

He is an Associate Professor at the Széchenyi István University, Győr Hungary. The main field of his research is the IPv6 implementation technologies. His other favorite topics are computer networking and information security. He has several certificates from Microsoft, Cisco, ISACA and other vendors.

A game theoretic framework for controlling the behavior of a content seeking to be popular on social networking sites

Khadija Touya, Hamid Garmani, Mohamed Baslam, Rachid El Ayachi, and Mostafa Jourhmane

***Abstract*—Over the years, people are becoming more dependent on Online Social Networks, through whom they constitute various sorts of relationships. Furthermore, such areas present spaces of interaction among users; they send more messages and posts showing domains they are interested in to guarantee the level of their popularity. This popularity depends on its own rate, the number of comments the posted topic gets but; also on the cost a user has to pay to accomplish his task on this network. However, the selfish behavior of those subscribers is the root cause of competition over popularity among those users. In this paper, we aim to control the behavior of a social networks users who try their best to increase their popularity in a competitive manner. We formulate this competition as a non-cooperative game. We propose an efficient game theoretical model to solve this competition and find a situation of equilibrium for the said game.**

***Index Terms*—Social network, game theory, popularity, utility function, content, publishing distribution, number of comments, price of anarchy, Nash equilibrium, best response.**

I. Introduction

Generally, social network users who have a specific type of relationship try to maintain these relational links; but they also seek to achieve a particular place within the network they use. Moreover, by posting content that guarantees a good reputation within the social network, each user looks to maximize his profit in terms of popularity so he becomes more popular, then he will attract more users to interact with him and precisely make them react to content he publishes on his own news feed, on the pages and the walls of the groups of his network. As users reveal self-promotions in their target to reach their objectives, many competitions are happening between those users; each one seeks to maximize his profit. One of these competitions is the conflict over popularity. Indeed, to have a good level of popularity, users think about publishing more content to be on the top of a timeline. This selfish behavior causes competition between published content.

Thus, popularity on social networks has become a topic of interest for researchers who want to establish analyses and studies regarding these areas of interaction [1], [2], [3], [4], [5], [6], [7], [8].

Currently, various works are done in this field and many approaches are proposed to predict, optimize and estimate popularity in online social networks [9], [10], [11]. Thus, in [12], Reiffers-Masson et al. worked on solving the popularity optimization problem. They presented an approach based on flow control. Firstly, the authors developed a mathematical model of popularity, then they proved the equivalence of the popularity maximization problem with a pseudo concave optimization problem, and finally, they provided an algorithm converging to the optimal solution. In [13], authors presented a game-theoretic approach to model the competition for the popularity of contents in social networks; thus, they formulated the interaction between contents in the form of a non-cooperative game where they took into consideration the rate as the main parameter, but the price and the cost of creating the content also influence the utility function. This analysis is based on the work done by Altman in [14], where the author treated a competitive situation about popularity among service providers, he modeled this competition as a non-cooperative game and considered the creation of content by service providers and the use of the acceleration method; this tool ensuring the evolution of the content's popularity in an increasing way.

In this context, the game theory seems to be the most effective tool to solve this kind of competition; it is an approach that offers new perspectives and mechanisms beyond what classical technics could do.

In this work, we focus on solving the popularity competition problem, formulating it as a non-cooperative game where the players are the content published on the social network walls. We model the game, prove the existence and uniqueness of the Nash equilibrium and then propose an efficient algorithm to learn the equilibrium point.

To achieve the goal of our theoretical approach, we organized the rest of this paper as follows: in section II, we propose the model of the non-cooperative game between contents shared by selfish and competitive information providers, and then present an efficient analysis employing technics from algorithmic game theory, in particular, the best response algorithm ensuring fast convergence to the Nash equilibrium. In section III, we present some results illustrating the proposed theoretical approach. Finally, we close our study with a general conclusion in section IV.

The authors are with the TIAD Laboratory, Computer Science Department, Faculty of Sciences and Techniques, Sultan Moulay Slimane University, Beni Mellal, Morocco (e-mail: {ouya.khadija, garmani.hamid}@gmail.com)

DOI: 10.36244/ICJ.2023.2.7

II. Problem modelisation

In this section, we formulate the interaction between selfish information providers (IPs), sharing content or posting messages, as a non-cooperative game between the contents shared on social network walls.

To set up our model, we consider a game that describes a social network with N contents (players). For each content, there is an appropriate strategy to guarantee the maximization of its popularity. This maximization is achieved taking into consideration strategies of other contents.
Let λ_i be the publishing distribution of content i, γ_i the price it must pay to be published.
And α_i the number of comments it will acquire and β_i the price to pay for getting a comment.

We analyze the set game, starting with the development of the utility function, then proving the existence and the uniqueness of the Nash equilibrium, and ending with the best response algorithm that guarantees convergence to the equilibrium situation, already noticed.

Utility model

We consider that contents shared within a social network are actors who do their best to improve their results in terms of popularity within this structure of interactions.

$G = [\mathscr{N}, \{\Lambda_i, \Theta_i\}, \{U_i\ (.)\}]$ denotes the non-cooperative game of publishing distribution and number of acquired comments, $\mathscr{N}$ is the set of contents, Λ_i, Θ_i is the set of strategies appropriate to the publishing distribution of content i and the comments it has accumulated, $\Lambda_i = [0, \lambda_i^{max}]$, $\Theta_i = [0, \alpha_i^{max}]$ and $U_i(.\ )$ is its utility function which he seeks to maximize by choosing the best strategy.

There is a tie between the publishing distribution, acquiring comments, and the popularity of the specific content published on the walls of social networks. Therefore, the utility function, of each content looking to gain popularity, depends on its revenue both in terms of the publishing distribution and in terms the number of comments it requires within the social network it propagates. But also, on the prices, it has to be distributed and to achieve a comment. Formally, the objective function of content i is defined as follows:

$$U_i(\lambda, \alpha, t) = P_0 + p_{ip}(t) \times \sum_j \lambda_j + p_{ic}(t) \times \sum_j \alpha_j - \gamma_i \lambda_i^2 - \beta_i \alpha_i^2 \tag{1}$$

Where :

The first term P_0 is a positive constant ensuring non-negative popularity. The second term, $p_{ip}(t) \times \sum_j \lambda_j$, is the impact of other contents' publishing distribution on the revenue of the content i in terms of the publishing distribution. The third term, $p_{ic}(t) \times \sum_j \alpha_j$, denotes the impact of the number of comments other agents accumulate on the revenue of the content i concerning the number of acquired comments. The fourth term, $i\lambda_i^2$, is the cost the content i has to be distributed and the last one, $\beta_i \alpha_i^2$, is the cost the same content has to pay to acquire a comment.

Following the work made in [12], arrivals are considered Poisson Point Processes. Therefore, both $p_{ip}\,(t)$ and $p_{ic}\,(t)$ follow an exponential distribution with rates, respectively, λ_i and α_i. Then the two parameters are expressed as follows:

$p_{ip}\,(t) = \int_0^T \lambda_i e^{-\lambda_i t}\ dt$ is the probability for the content i to be distributed.

$p_{ic}\,(t) = \int_0^T \alpha_i e^{-\alpha_i t}\ dt$ is the probability for the content i to acquire a comment.

When T tends to infinity, the probabilities are calculated as shown below:

$$p_{ip}\,(t) = \int_0^\infty \lambda_i e^{-\lambda_i t}\ dt\ = [-e^{-\lambda_i t}]_0^\infty\ = 1$$

$$p_{ic}\,(t) = \int_0^\infty \alpha_i e^{-\alpha_i t}\ dt\ = [-e^{-\alpha_i t}]_0^\infty\ = 1$$

Based on these results, we describe the utility function using the following formula:

$$U_i(\lambda, \alpha) = P_0 + \sum_j \lambda_j + \sum_j \alpha_j - \gamma_i \lambda_i^2 - \beta_i \alpha_i^2 \tag{2}$$

III. Game analysis

Given that the competition between contents is becoming more popular, the natural solution of this non-cooperative game will be allowed by the Nash equilibrium, which is considered to be a strategic profile such that no content can unilaterally increase its revenue. Using the tools of concave game theory, we prove the existence and the uniqueness of the Nash equilibrium point as presented in [15]. We assume that a non-cooperative game G is concave if the utility functions of all players are strictly concave with respect to their corresponding strategies [15].

According to [15], a Nash equilibrium exists for a concave game if the space of joint strategies is compact and convex, and the utility function that a given player seeks to maximize is concave with respect to his own strategy and continuous at any point in the space of strategies through the understudy system.

Let φ be the weighted sum of utility functions with non-negative weights, it is defined by the following formula:

$$\varphi = \sum_{i=1} x_i U_i \tag{3}$$

To ensure the uniqueness of the Nash equilibrium, φ must be diagonally strictly concave. Where, the concept of strict diagonal concavity means that the control an individual content has over its utility function is greater than the control that others have over it. Thus, the uniqueness of the existing equilibrium is demonstrated using the pseudo-gradient of the weighted sum of utility functions discussed in [15].

A. Publishing distribution game

The game G of publishing distribution is defined for fixed values $\alpha_i \in \Theta_i$ such as: $G(\alpha) = [\mathscr{N}, \{\Lambda_i\}, \{U_i(., \alpha)\}]$

Definition 1: Publishing distributions' vector $\lambda^* = (\lambda_1^*, ..., \lambda_N^*)$ is a Nash equilibrium if for each $i \in \{1, ..., N\}$,

$$U_i\left(\lambda_i^*, \lambda_{-i}^*\right) = \max_{\lambda_i \in \Lambda_i} U_i(\lambda_i, \lambda_{-i}^*) \tag{4}$$

In other words, the definition 1 shows, clearly, that by reaching the equilibrium point, no source could obtain a benefit by changing its strategy unilaterally (individually).

Theorem 1: For the game $G(\alpha)$ which is concave, the Nash equilibrium exists and it is unique.

Proof 1: To prove the existence of the equilibrium point, we mention that the strategy space of each content Λ_i is defined by all frequencies in the closed interval bounded by the minimum and maximum frequencies. Thus, the joint strategy space Λ_i is non-empty, convex, and compact. Moreover, the utility functions are concave with respect to λs as shown by the second derivative test:

$$\frac{\partial^2 U_i(\lambda,\alpha)}{\partial^2\lambda_i} = -2\gamma_i < 0 \qquad (5)$$

Having reached the negativity of the second derivative, we focus on the proof of the uniqueness of the equilibrium situation. Following [15], we define the weighted sum of the users' utility functions as follows:

$$\varphi\left(\lambda,x\right) = \sum_{i=1}^{N} x_i U_i(\lambda_i,\lambda_{-i}) \qquad (6)$$

The pseudo-gradient of the equation (6) is given by :

$$g(\lambda,x) = \left[x_1\nabla U_1(\lambda_1,\lambda_{-1}),\ \ \ldots.\ \ ,x_N\nabla U_N\left(\lambda_N,\lambda_{-N}\right)\right]^T$$

Thus, the Jacobian matrix J of the pseudo-gradient is expressed as follows:

$$J = \begin{pmatrix} x_1\frac{\partial^2 U_1}{\partial\lambda_1^2} & \cdots & x_1\frac{\partial^2 U_1}{\partial\lambda_1\partial\lambda_N} \\ \vdots & \ddots & \vdots \\ x_N\frac{\partial^2 U_N}{\partial\lambda_N\partial\lambda_1} & \cdots & x_N\frac{\partial^2 U_N}{\partial\lambda_N^2} \end{pmatrix}$$

$$J = \begin{pmatrix} -2x_1\gamma_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & -2x_N\gamma_N \end{pmatrix}$$

The found matrix J is a diagonal matrix with negative diagonal elements, so we can say that J is negatively defined. Similarly, $[J + J^T]$ is negatively defined, and according to [15], the weighted sum of utility functions is diagonally strictly concave. Thus, the game $G(\alpha)$ admits a unique Nash equilibrium.■

B. Number of acquired comments game

The game G of the number of acquired comments is defined for fixed values $\lambda_i \in \Lambda_i$ such as: $G(\lambda) = [\mathscr{N}, \{\Theta_i\}, \{U_i(\lambda,.)\}]$

Definition 2: The number of acquired comments' vector $\alpha^* = (\alpha_1^*, ..., \alpha_N^*)$ is a Nash equilibrium if for each $i \in \{1, ..., N\}$,

$$U_i\left(\alpha_i^*,\alpha_{-i}^*\right) = \max_{\alpha_i\in\Theta_i} U_i(\alpha_i^*,\alpha_{-i}^*) \qquad (7)$$

As it is already mentioned (in definition 1), the definition 2 allows to conclude that also no content (player) has the advantage to change its strategy individually, as it is already noted in the last part reserved to the game of publishing distribution of contents.

Theorem 2: For the game $G(\lambda)$ which is concave, Nash equilibrium existes and it is unique.

Proof 2: Calculating the second derivative of the utility function with respect to the number of comments, we find that :

$$\frac{\partial^2 U_i(\lambda,\alpha)}{\partial\alpha_i^2} = -2\beta_i < 0 \qquad (8)$$

Ensuring the existence of the Nash equilibrium, we turn to the proof of its uniqueness. Following [15], we define the weighted sum of users' utility functions as follows:

$$\varphi\left(\alpha,x\right) = \sum_{i=1}^{N} x_i U_i(\alpha_i,\alpha_{-i}) \qquad (9)$$

The pseudo-gradient of the equation (9) is given by :

$$g(\alpha,x) = \left[x_1\nabla U_1(\alpha_1,\alpha_{-1}),\ \ \ldots.\ \ ,x_N\nabla U_N\left(\alpha_N,\alpha_{-N}\right)\right]^T$$

Thus, the Jacobian matrix J of the pseudo-gradient is expressed as follows:

$$J = \begin{pmatrix} x_1\frac{\partial^2 U_1}{\partial\alpha_1^2} & \cdots & x_1\frac{\partial^2 U_1}{\partial\alpha\partial\alpha_N} \\ \vdots & \ddots & \vdots \\ x_N\frac{\partial^2 U_N}{\partial\alpha_N\partial\alpha_1} & \cdots & x_N\frac{\partial^2 U_N}{\partial\alpha_N^2} \end{pmatrix}$$

$$J = \begin{pmatrix} -2x_1\beta_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & -2x_N\beta_N \end{pmatrix}$$

The found matrix J is a diagonal matrix with negative diagonal elements, so we allowed to say that J is negatively defined. Similarly, $[J + J^T]$ is negatively defined, and according to [15], the weighted sum of utility functions is diagonally strictly concave. Thus, the game $G(\lambda)$ admits a unique Nash equilibrium. ■

C. Learning the Nash equilibrium

The above sections show that the Nash equilibrium exists and it is unique. Indeed, we will develop a distributed algorithm that converges to the Nash equilibrium of the publishing distribution set and the number of acquired comments. The algorithm 1 details the work done to learn the Nash equilibrium.

Algorithm 1 Best Response Algorithm

```
1: Initialization of publishing distribution and number of acquired comments vectors $\lambda$ and $\alpha$, randomly;
2: For each content $i \in \mathscr{N}$, at the iteration $t$ :
       $a)\quad \lambda_i(t+1) = \underset{\lambda_i \in \Lambda_i]}{\text{argmax}} \left(U_i(\lambda_i, \lambda_{-i})\right).$
       $b)\quad \alpha_i(t+1) = \underset{\alpha_i \in \Theta_i]}{\text{argmax}} \left(U_i(\alpha_i, \alpha_{-i})\right).$
3: IF $\forall i \in \mathscr{N}$,
   $|\lambda_i(t+1) - \lambda_i(t)| < \epsilon$ and $|\alpha_i(t+1) - \alpha_i(t)| < \epsilon$, STOP.
4: ELSE, $t \leftarrow t+1$ and go back to step (2)
```

D. Price of anarchy

The price of Anarchy was introduced by Koutsoupias and Papadimitriou, in their work [16]. Then the book [17] developed central ideas of it, but also multiple kinds of works have been produced around this concept. Furthermore, the work established by Roughgarden and Tardos [18] made this main measure of loss of equilibrias efficiency more popular. In fact, they employed the price of anarchy in atomic and nonatomic congestion games. Moreover, PoA has also appeared for facilitating a location in [17] and for creating a network in [19]. Thereby, the price of anarchy is considered to be a tool for resolving the issue of multiple equilibriums adopting a worst-case approach. This approach defines that loss as the worst-case ratio comparing the global efficiency measure at an outcome, to the optimal value of that efficiency measure. In a noncooperative game, the price of anarchy is defined as the ratio between the worst utility function value of equilibrium and the one of an optimal outcome. According to [20], the inefficiency caused by the players self-promotion is measured as the quotient between the social welfare, that Maille and Tuffin presented as the sum of the utilities of all providers in the system) in [21], obtained at the Nash equilibrium and the maximum value of the social welfare, as shown in (10).

$$\begin{cases} PoA_\lambda = \frac{\min W_{NE}(\lambda)}{\max W(\lambda)} \\ PoA_\alpha = \frac{\min W_{NE}(\alpha)}{\max W(\alpha)} \end{cases} \tag{10}$$

Where:

$$\begin{cases} \max W(\lambda) = \max_\lambda \sum_{i=1}^{N} U_i(\lambda) \\ \max W(\alpha) = \max_\alpha \sum_{i=1}^{N} U_i(\alpha) \end{cases}$$

is a system presenting the social welfare function for each parameter,
and

$$\begin{cases} W_{NE}(\lambda) = \sum_{i=1}^{N} U_i(\lambda^*) \\ W_{NE}(\alpha) = \sum_{i=1}^{N} U_i(\alpha^*) \end{cases}$$

is a system presenting the sum of utilities of all contents at a frequency Nash equilibrium and a number of acquired comments Nash equilibrium.

IV. NUMERICAL INVESTIGATIONS

We propose to numerically study the interaction game between the contents on the walls and the news feeds of a social network, taking into account the previous expressions of the utilities. To illustrate our work and show how to take advantage of our theoretical analysis, we perform the numerical part considering the best response algorithm and the expression of the utility function of each content.

To do so, we consider a system with two contents; two players seeking to maximize their respective revenues. Each content varies its own decision parameters - publishing distribution and the number of comments it receives - taking into account those of its opponent.

Taking into account the expression of the utility function given by the equation (2), we start with the graphical representation of this function, in the case of the publishing distribution game on the one hand and the number of comments game on the other hand.

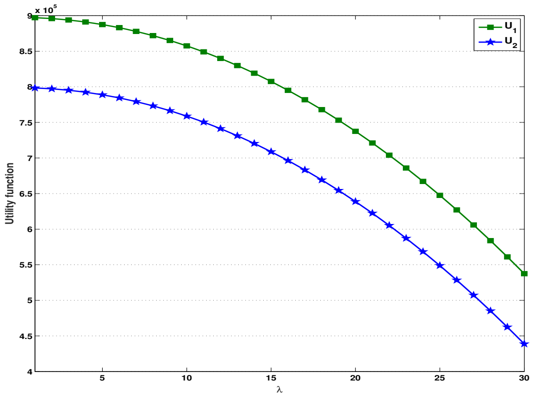


Fig. 1: Publishing distribution game: Utility function with respect to λ.

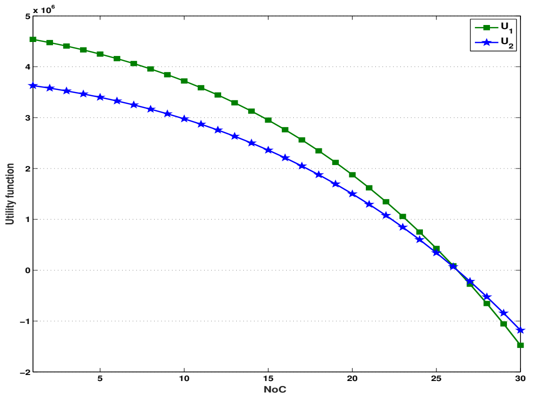


Fig. 2: Number of acquired comments game: Utility function with respect to Noc.

Figures 1 and 2 present the evolution of the utility functions of the contents as a function of the two parameters; the publishing frequency and the number of acquired comments. We notice that the plotted curves reveal the concavity of the function for all the values of the decision parameters already mentioned (λ and NoC). Therefore, the Nash equilibrium for both cases exists and it is also unique.

Concerning the learning of the Nash equilibrium of publishing frequency and also of the number of comments, we use the best response algorithm (algorithm 1) .

Figures 3 and 4 illustrate the convergence to the Nash equilibrium of posting frequency and to the Nash equilibrium of number of comments acquired. We remark that this convergence is ensured after a few rounds (almost 5 iterations are sufficient to reach the Nash equilibrium), which means that the learning speed of the Nash equilibrium is relatively high. These numerically completed investigations reinforce, then, the results that we have already proved theoretically.

We move on to study the impact of the publishing price and the comment acquisition price on the performance of the treated system.

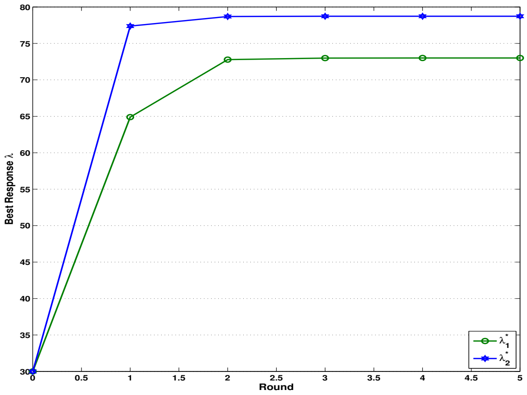


Fig. 3: Publishing frequency game: Convergence to the Nash equilibrium of λ.

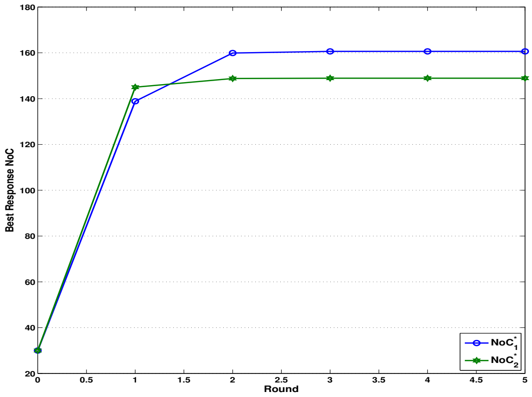


Fig. 4: Number of acquired comments game: Convergence to the Nash equilibrium of NoC.

Figures 5 and 6 describe the impact of the publishing price on the Nash equilibrium utility function and publishing distribution. With increasing values of the price of publishing content on the timelines of a social network γ, the equilibrium utility functions and publishing frequencies decrease. While when the price is low, the publishing frequencies and utility functions are higher. As a result, increasing the publishing price γ leads to the adoption of a content publishing frequency which is lower.

On the other hand, the price of obtaining a comment has a large influence on the values of the utility functions but also on the number of acquired comments (NoC) at the equilibrium.

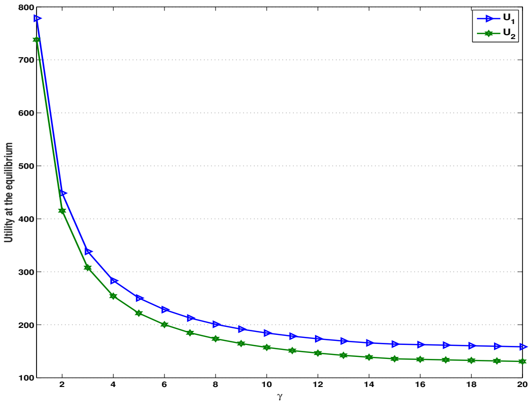


Fig. 5: Publishing distribution game: Impact of the price γ on the utility function at the equilibrium.

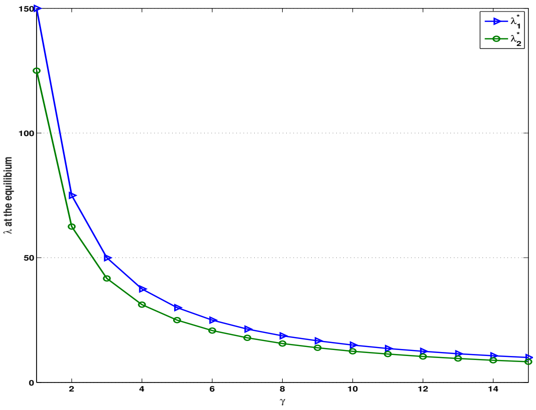


Fig. 6: Publishing distribution game: Impact of the price γ on the publishing distribution at the equilibrium.

The curves, in Figures 7 and 8, illustrate the impact of the price of acquiring a comment, respectively, on the utility function and the number of acquired comments of both of contents (players) at Nash equilibrium. According to the graphs, increasing the price of obtaining a comment β leads to the decrease of the values at Nash equilibrium concerning the utility function and the number of aquired comments. So, with a low price of getting a comment, the number of comments obtained and the utility function at the Nash equilibrium have higher values for both players which encourages the contents to look for acquiring more comments. Whereas, for a very high price, the contents concur to weaken the number of acquired comments.

To measure the efficiency of the Nash equilibrium, in our study, we propose to analyze the evolution of the price of anarchy as a function of the prices γ and β.

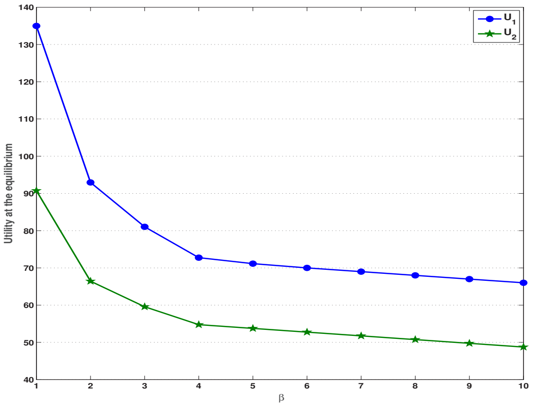


Fig. 7: NoC game : Impact of the price β on the utility function at the equilibrium.

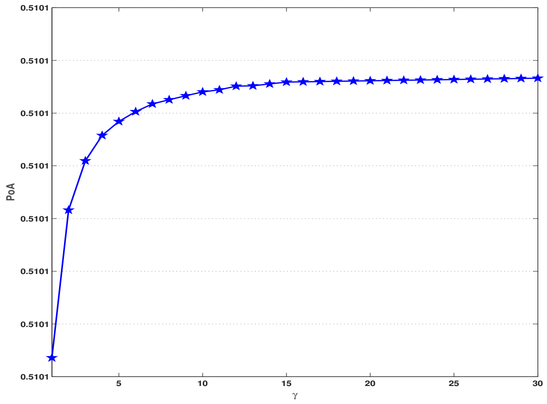


Fig. 9: Publishing game: Price of anarchy with respect to the price γ.

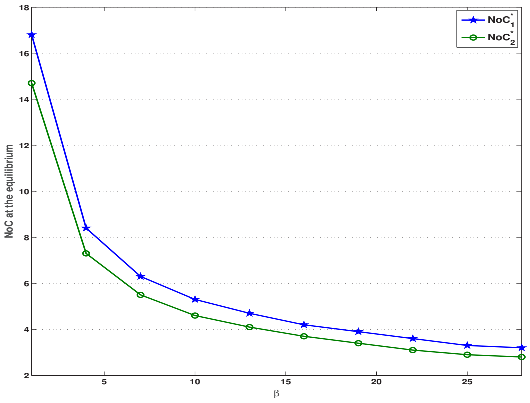


Fig. 8: NoC game : Impact of the price β on the NoC at the equilibrium.

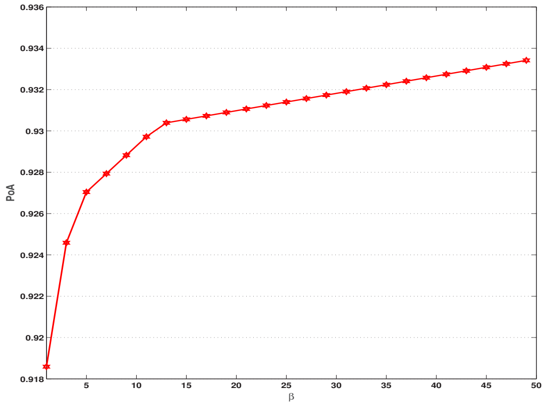


Fig. 10: NoC game: Price of anarchy with respect to the price β.

The impact of prices (publishing price and comment acquisition price) on the efficiency of the studied system is represented in Figures 9 and 10. The two curves reveal that the PoA increases with respect to the publishing price (comment acquisition price). For a publishing price and a comment acquisition price which are low, PoA is low. Subsequently, players behave in a highly selfish and individual manner to maximize their gain in terms of popularity. However, by increasing prices, the PoA increases and thus the players move, in their decision making, towards the Nash equilibrium strategies of publishing frequency and strategies of number of acquired comments. Thus, the Nash equilibrium is fair and socially efficient in both cases.

V. Conclusion

In this paper, we proposed a theoretical approach using game theory to model the interactions between contents posted on social network news feeds as players through a class of two-parameter Nash equilibrium models. The model is based on a simple function describing the behavior of the contents. In fact, we took into account the characteristics of the content itself (its publishing frequency and the number of comments it receives), but also those of other contents sharing the same structure. We proved the existence and the uniqueness of the Nash equilibrium point and developed the distributed best response algorithm that allows to learn this equilibrium point in a finite number of iterations. In short, the numerically obtained results validate the work established to study user reactions; they can be extended to general considerations on networks. In this context, the existence and the uniqueness of the Nash equilibrium, in the proposed approach, help us to confirm the stability within the under study social network. Since the progression of popularity is considered as a primordial step that cannot be ignored in order to see one's web visibility explode, information providers employ it to dominate social networks they are subscribed to. Then maximize their profit while communicating through the network.

References

[1] B. Ribeiro and C. Faloutsos, “Modeling Website Popularity Competition in the Attention-Activity Marketplace,” *arXiv:1403.0600 [physics]*, Mar. 2014, **doi**: 10.1145/2684822.2685312.

[2] A. Matakos and A. Gionis, “Tell me something my friends do not know: Diversity maximization in social networks,” *arXiv:1811.10354 [cs]*, 2018 **doi**: 10.1109/ICDM.2018.00048.

[3] Y. Ma, J. He, and Q. Yu, “Modeling on social popularity and achievement: A case study on table tennis,” *Physica A: Statistical Mechanics and its Applications*, vol. 524, pp. 235–245, 2019, **doi**: 10.1016/j.physa.2019.04.007.

[4] S. Dhamal, W. Ben-Ameur, T. Chahed, and E. Altman, “A two phase investment game for competitive opinion dynamics in social networks,” *Information Processing & Management*, vol. 57, no. 2, p. 102064, 2020, **doi**: 10.1016/j.ipm.2019.102064.

[5] K. Touya, M. Baslam, R. El Ayachi, and M. Jourhmane, “A Game theoretic approach for competition over visibility in social networks,” *Bulletin of Electrical Engineering and Informatics*, vol. 8, no. 2, pp. 674–682, 2019, **doi**: 10.11591/eei.v8i2.728.

[6] X. Li, I. Kawachi, O. M. Buxton, S. Haneuse, and J.-P. Onnela, “Social network analysis of group position, popularity, and sleep behaviors among us adolescents,” *Social Science and Medicine*, vol. 232, pp. 417–426, 2019, **doi**: 10.1016/j.socscimed.2019.05.026.

[7] Q. Cao, H. Shen, J. Gao, B. Wei, and X. Cheng, “Popularity prediction on social platforms with coupled graph neural networks,” in *Proceedings of the 13th international conference on web search and data mining,* 2020, pp. 70–78, **doi**: 10.1145/3336191.3371834.

[8] S. C. Montgomery, M. Donnelly, P. Bhatnagar, A. Carlin, F. Kee, and R. F. Hunter, “Peer social network processes and adolescent health behaviors: A systematic review,” *Preventive medicine*, vol. 130, p. 105900, 2020, **doi**: 10.1016/j.ypmed.2019.105900.

[9] K. Lerman and T. Hogg, “Using a Model of Social Dynamics to Predict Popularity of News,” *arXiv:1004.5354 [cs]*, Apr. 2010, **doi**: 10.1145/1772690.1772754.

[10] Z. Bao, Y. Liu, Z. Zhang, H. Liu, and J. Cheng, “Predicting popularity via a generative model with adaptive peeking window,” *Physica A: Statistical Mechanics and its Applications*, vol. 522, pp. 54–68, May 2019, **doi**: 10.1016/j.physa.2019.01.132.

[11] D. Wu, B. Liu, Q. Yang, and R. Wang, “Social-aware cooperative caching mechanism in mobile social networks,” *Journal of Network and Computer Applications*, vol. 149, p. 102457, 2020, **doi**: 10.1016/j.jnca.2019.102457.

[12] A. R. Masson, Y. Hayel, E. Altman, and G. Martel, “A Generalized Fractional Program for Maximizing Content Popularity in Online Social Networks,” in *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. Barcelona: IEEE, Aug. 2018, pp. 869–872, **doi**: 10.1109/ASONAM.2018.8508480.

[13] S. Hafidi, M. Baslam, and R. E. Ayachi, “Analysis of Competition Fronting the Popularity of Content in Social Networks,” vol. 6, no. 2, pp. 86–94, 2017, **doi**: 10.11591/ijict.v6i2.pp86-94, number: 2.

[14] E. Altman, “A semi-dynamic model for competition over popularity and over advertisement space in social networks,” in *Proceedings of the 6th International Conference on Performance Evaluation Methodologies and Tools*. Cargse, France: IEEE, 2012, **doi**: 10.4108/valuetools.2012.250334.

[15] J. B. Rosen, “Existence and Uniqueness of Equilibrium Points for Concave N-Person Games,” *Econometrica*, vol. 33, no. 3, p. 520, 1965, **doi**: 10.2307/1911749.

[16] E. Koutsoupias and C. Papadimitriou, “Worst-case equilibria,” *Computer science review*, vol. 3, no. 2, pp. 65–69, 2009, **doi**: 10.1016/j.cosrev.2009.04.003.

[17] A. Vetta, “Nash equilibria in competitive societies, with applications to facility location, traffic routing and auctions,” pp. 416–425, 2002, **doi**: 10.1109/sfcs.2002.1181966.

[18] T. Roughgarden and . Tardos, “How bad is selfish routing?” *Journal of the ACM (JACM)*, vol. 49, no. 2, pp. 236–259, 2002, **doi**: 10.1145/506147.506153.

[19] E. Anshelevich, A. Dasgupta, E. Tardos, and T. Wexler, “Near-optimal network design with selfish agents,” pp. 511–520, 2003, **doi**: 10.1145/780542.780617.

[20] L. Guijarro, V. Pla, J. Vidal, and J. Martinez-Bauset, “Analysis of price competition under peering and transit agreements in internet service provision to peer-to-peer users,” in *IEEE Consumer Communications and Networking Conference (CCNC2011), Las Vegas, Nevada USA*, 2011, pp. 9–12, **doi**: 10.1109/ccnc.2011.5766356.

[21] P. Maill and B. Tuffin, “Analysis of price competition in a slotted resource allocation game,” pp. 888–896, 2008, **doi**: 10.1109/infocom.2007.141.

Khadija Touya received her Ph.D. degree in 2022 from the Faculty of Sciences and Techniques, Sultan Moulay Slimane University, Morocco. Her research interests include network economics, network security, applications of game theory in social networks, wireless networks, and radio resource management.

Hamid Garmani is a Professor of computer science in the Faculty of Sciences and Techniques, Sultan Moulay Slimane University, Morocco. His research interests include network economics, network security, applications of game theory in wireless networks, and radio resource management.

Mohamed Baslam is a Professor of computer science in the Faculty of Sciences and Techniques, Sultan Moulay Slimane University, Morocco. His current research interests include performance evaluation and optimization of networks based on game-theoretic and queuing models, applications in communication/transportation and social networks, such as wireless flexible networks, bio-inspired and selforganizing networks, and economic models of the Internet and yield management.

Rachid El Ayachi is a Professor of computer science in the Faculty of Sciences and Techniques, Sultan Moulay Slimane University, Morocco. His research interests include image processing, machine learning, natural language processing, Network Engineering Games, social networks and neutrality issues.

Mostafa Jourhmane is a professor of mathematics and computer science in the Faculty of Sciences and Techniques, Sultan Moulay Slimane University, Morocco. His research interests include Numerical analysis, classification, image processing, neural networks, big data, Network Engineering Games, social networks and their control and the analysis through game theoretical models of network and neutrality issues.

Call for Papers

International Workshop on
Analytics for Service and Application Management
AnServApp 2023

Niagara Falls, Canada, 30 October - 2 November 2023
Co-located with CNSM 2023
http://www.cnsm-conf.org/2023/workshop_AnServApp.html

With enterprise organizations generating petabytes of data each day, their use of, and reliance on data analytics to provide contextual insight into their operations is imperative for improving the implementation, management and delivery of services and applications. Approaches such as predictive data analytics, data mining, machine learning and deep learning are promising mechanisms to harness this immense stream of service and application data to meet the needs of an organization. The main goal of **AnServApp** is to present research and work-in-progress results in the area of data analytics, machine learning and cognitive science for service and application management.

Topics of interest include but are not limited to:

- AI/ML powered ticket resolution
- Application Management Services (AMS)
- AI/ML/DL powered ticket resolution
- Event log analysis
- Network and service security
- Knowledge management
- Predictive maintenance
- Asset tracking and provisioning
- Workload optimization
- Sentiment analysis
- Social media
- Lower carbon foot print applications / services / systems
- Smart cities and smart transportation services / systems
- Social media apps / services / systems
- Smart education services / systems
- Edge, fog, cloud services / systems
- Sustainability and resilience of applications / services / systems

Paper Submission Guidelines: Authors are invited to submit original contributions that have not been published or submitted for publication elsewhere. Papers should be prepared using the IEEE 2-column conference style and are limited to 7 pages including references.

Papers must be submitted electronically in PDF format through EDAS using this link.

In addition to regular papers, short papers describing late-breaking advances and work-in-progress reports from ongoing research are also welcomed. These should also be in IEEE 2-column format between 2 to 4 pages in length.

Workshop Co-chairs:

- Nur Zincir-Heywood, Dalhousie University, Canada
- Khurram Aziz, Dalhousie University, Canada
- Pal Varga, Budapest University of Technology and Economics, Hungary

Important Dates:

Paper Submission:	8 August 2023
Acceptance Notification:	25 August 2023
Camera Ready Submission:	8 September 2023

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

https://journals.ieeeauthorcenter.ieee.org/
Then click: "IEEE Author Tools for Journals"
- "Article Templates"
- "Templates for Transactions".

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
g) Document Object Identifier (DOI)

[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. DOI: 10.1109/TEI.1984.298778

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 following portal address:

https://www.ojs.hte.hu/infocommunications_journal/about/submissions

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

Editor-in-Chief: Pál Varga – pvarga@tmit.bme.hu

Associate Editor-in-Chief:
Rolland Vida – vida@tmit.bme.hu
László Bacsárdi – bacsardi@hit.bme.hu

2024 IEEE Network Operations and Management Symposium (NOMS 2024)

6-10 May 2024 Seoul, Korea

Towards intelligent, reliable, and sustainable network and service management

• • • Call for Papers • • •

IEEE Network Operations and Management Symposium (NOMS 2024) will be held May 6-10, 2024 in Seoul, Korea. First organized in 1988, NOMS 2024 follows the 36 years tradition of NOMS and IM as the primary IEEE Communications Society's forum for technical exchange on network and service operations and management, focusing on research, development, integration, standards, service provisioning, and user communities. The theme of NOMS 2024 is "*Towards intelligent, reliable, and sustainable network and service management*." NOMS 2024 will offer various types of sessions, including keynotes, technical, experience, poster, panel, tutorial and PhD dissertation. High quality is assured through a well-qualified Technical Program Committee (TPC) and stringent peer review of paper submissions. Papers can be submitted as full or short technical session papers, experience session papers, and dissertation papers. In addition, we invite proposals for demonstrations, exhibitions, panels, tutorials, and workshops. Please be advised that NOMS 2024 will be an in-person only event, and virtual presentation or attendance will not be available.

Topics of Interest

Authors are invited to submit papers that fall into or are related to the following topics of interest:

Network Management

- IP Networks
- Wireless and Cellular Networks
- Optical Networks
- Virtual Networks
- Home Networks
- Access Networks
- Fog and Edge Networks
- Wide Area Networks
- Enterprise and Campus Networks
- Data Center Networks
- Industrial Networks
- Vehicular Networks
- IoT and Sensor Networks
- Information-Centric Networks
- 5G network and Beyond (6G)

Service Management

- Multimedia Services
- Content Delivery Services
- Cloud Computing Services
- Internet Connectivity and Internet Access Services
- Internet of Things Services
- Security Services
- Context-Aware Services
- Information Technology Services
- Service Assurance

Business Management

- Economic Aspects
- Multi-Stakeholder Aspects
- Service Level Agreements
- Lifecycle Aspects
- Process and Workflow Aspects
- Legal Perspective
- Regulatory Perspective
- Privacy Aspects
- Organizational Aspects

Functional Areas

- Fault Management
- Configuration Management
- Accounting Management
- Performance Management
- Security Management

Management Paradigms

- Centralized Management
- Hierarchical Management
- Distributed Management
- Federated Management
- Autonomic and Cognitive Management
- Policy- and Intent-Based Management
- Model-Driven Management
- Pro-active Management
- Energy-aware Management
- QoE-Centric Management

Technologies

- Communication Protocols
- Middleware
- Overlay Networks
- Peer-to-Peer Networks
- Cloud Computing and Cloud Storage
- Data, Information, and Semantic Models
- Information Visualization
- Software-Defined Networking
- Network Function Virtualization
- Orchestration
- Operations and Business Support Systems
- Control and Data Plane Programmability
- Distributed Ledger Technology
- Digital Twin

Methods

- Mathematical Logic and Automated Reasoning
- Optimization Theories
- Control Theory
- Probability Theory, Stochastic Processes, and Queuing Theory
- Artificial Intelligence and Machine Learning
- Evolutionary Algorithms
- Economic Theory and Game Theory
- Monitoring and Measurements
- Data Mining and (Big) Data Analysis
- Computer Simulation Experiments
- Testbed Experimentation and Field Trials
- Software Engineering Methodologies

Paper submission guidelines

Authors are invited to submit original contributions written in English that have not been published or submitted for publication elsewhere. Technical papers must be formatted using the IEEE 2-column format and not exceed 8 pages (excluding references) for full paper submissions or not exceed 4 pages (excluding references) for short paper submissions. All papers should be submitted through JEMS at https://jems3.sbc.org.br/noms2024.

All submitted papers will be peer-reviewed. Accepted and presented papers will be published in the conference proceedings and submitted to IEEE Xplore. Authors of the best accepted papers will be invited to submit extended versions of their papers to a fast-tracked, special issue of Wiley's International Journal of Network Management (IJNM).

Important Dates:

- Paper Submission Deadline: Sep. 29, 2023
- Notification of Acceptance: Dec. 22, 2023
- Final Camera Ready: Feb. 2, 2024

General Chair:

- James Won-Ki Hong, POSTECH, Korea

TPC Co-Chairs:

- Baek-Young Choi, UMKC, USA
- Roberto Riggio, Università Politecnica delle Marche, Italy
- Myung-Sup Kim, Korea University, Korea

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: **FERENC VÁGUJHELYI** • *elnok@hte.hu*
Secretary-General: **ISTVÁN MARADI** • *istvan.maradi@gmail.com*
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*