Infocommunications Journal

A PUBLICATION OF THE SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS (HTE)

June 2021 Volume XIII Number 2 ISSN 2061-2079

MESSAGE FROM THE EDITOR-IN-CHIEF

SELECTED INVITED PAPERS

CALL FOR PAPERS / PARTICIPATION

ADDITIONAL

Technically Co-Sponsored by

IEEE ComSoc™
IEEE Communications Society

hte

IEEE
HUNGARY SECTION

Indexing information

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

Infocommunications Journal

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

Supporters

FERENC VÁGUJHELYI – president, Scientific Association for Infocommunications (HTE)

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, Fax: +36 1 463 3108
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

www.infocommunications.hu

Recent Advances in Communication System Management, Security and Performance

Pal Varga

SINCE its first issue just over a decade ago Infocommunications Journal authors, readers, and especially the Editorial Board have wished to witness the journal ranking improve. Due to the sometimes exhaustive review process, the quality of the papers is high – but still, the wide acceptance of our journal got delayed. This has recently changed, and the Infocommunications Journal got ranked into the Q3 quartile in both of its domains, namely in Computer Science and in Electrical and Electronic Engineering – and it is getting closer to receiving an impact factor > 1. Climbing up one quartile and receiving an impact factor is a great recognition; our authors' work keeps getting more visible and cited widely. Let us all keep up the excellent work and – on behalf of the Editorial Board – let me thank you, dear authors and reviewers, that our journal has passed this milestone.

The current issue of the journal features six papers; all are openly accessible already. The current issue features recent advances in the domain of quantum random number generators, satellite quantum repeaters, stateless NAT64 testing, noise suppression in power line communication, risk management for cyber-physical system of systems, as well as 5G performance evaluation. This set of papers highlight some of the advances in communication system management, security, and performance. Let us have a brief overview of the papers in this issue.

In his paper, Gábor Lencse provides an evaluation – especially for accuracy – of Siitperf, the first free software for testing the Stateless IP/ICMP Transition (SIIT) part of the RFC 8219, which is discussing benchmarking methodologies of IPv6 transition technologies. Siitperf implements throughput, frame loss rate, latency, and packet delay variation tests. The evaluation finds that the reliability of its results mainly depends on the accuracy of the timing of the Siitperf tool. The importance of such evaluation and calibration reports lies within their proof as they strengthen trust towards the methods and tools. Validation and verification equipment always have to prove themselves – that the results they provide are accurate –, and this article offers exactly those proofs.

In their recent work, Botond L. Márton, Dóra Istenes and László Bacsárdi investigate the quality of quantum based random number generators (QRNGs). After presenting the general concept of QRNGs, and two of their methods for random number generation, they introduce selected tests for determining the quality of the generated random numbers. Further, they present the idea of extractors, their place in the lifecycle of QRNGs, and eight examples of the extractors. They examined the effect of different extractors on two QRNG outputs and found that by choosing the right extractor for the task, the quality of the generated random numbers can be improved.

Satellite-based quantum repeaters are key for long-range QKD (quantum key distribution), as well as in point-to-point communication. András Mihály and László Bacsárdi evaluated the QKD capabilities of quantum repeaters in a satellite-based network, along with selected types of noises. They examined the effects of various noises on the quantum memory of quantum repeaters and their impacts on the quantum bit error rate. They found that for future satellite networks, one of the most crucial noises is the quantum dephasing noise, and in the future, we should prioritize minimizing it.

Wei Zhang et al. present an enhanced, multi-step method for impulsive noise suppression for Power Line Communication (PLC). Their method is based on wavelet dimensioning (WD) and independent component analysis (ICA). The denoising effect of the new WD-PowerICA algorithm overperforms other, compared ICA algorithms in separating noise from the useful signal, although the current paper merely analyzed the correlation index, so BER will follow as future work.

Cyber-Physical Systems of Systems (CPSoS) are complex, so as the risk factors associated with them. George Matta et al. apply threat modeling for the security analysis of CPSoS in their paper, covering risk management and threat identification, as well. After describing their integrated risk management process, they report their experience of using a risk management framework to identify the most critical security vulnerabilities in CPSoS in the railway sector and show the broader impact on the domain of safety and security management.

In his paper, John Baghous evaluates the performance of a current 5G system regarding its throughput in non-line of sight scenarios, utilizing Massive-MIMO, applying a cluster delay channel model. As expected, it is found that the throughput has improved with the use of Massive MIMO technology – the detailed results of the preliminary experience with various antenna scenarios are exciting, indeed.

Pal Varga received his Ph.D. degree from the Budapest University of Technology and Economics, Hungary. He is currently an Associate Professor at the Budapest University of Technology and Economics and also the Director at AITIA International Inc. 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 of the Sensors (MDPI) and Electronics (MDPI) journals, and the Editor-in-Chief of the Infocommunications Journal.

Checking the Accuracy of Siitperf

Gábor Lencse

Abstract— **Siitperf is the world's first free software RFC 8219 compliant SIIT (Stateless IP/ICMP Translation, also called as Stateless NAT64) tester, which implements throughput, frame loss rate, latency and packet delay variation tests. In this paper, we show that the reliability of its results mainly depends on the accuracy of the timing of its frame sender algorithm. We also investigate the effect of Ethernet flow control on the measurement results. Siitperf is calibrated by the comparison of its results with that of a commercial network performance tester, when both of them are used for determining the throughput of the IPv4 routing of the Linux kernel.**

Index Terms—**accuracy, network benchmarking tools, calibration, frame loss rate, latency, network performance measurement, siitperf, throughput.**

I. Introduction

RFC 8219 [1] has defined a benchmarking methodology for the high number of *IPv6 transition technologies* [2] by classifying them into a small number of categories and defining benchmarking procedures for each category. As far as we know, our **`siitperf`** [3] is the world's first free software RFC 8219 compliant SIIT (Stateless IP/ICMP Translation) [4] (also called stateless NAT64) tester, written in C++ using DPDK (Data Plane Development Kit) [5] available from GitHub [6]. Being a measurement tool, the accuracy of **`siitperf`** is a key issue, which we examine in this paper. To that end, first, we give a short introduction to RFC 8219 and **`siitperf`** only up to the measure necessary to understand the rest of this paper. Then, we define our error model by overviewing the most important factors that could cause unreliable measurement results. Next, we examine the effect of Ethernet flow control on the measurement results. After that, we measure the throughput of the same DUT (Device Under Test) using a commercial network performance tester and **`siitperf`** and compare their results. Finally, we discuss our results and disclose our plans for further research.

II. A Short Introduction to RFC 8219 and Siitperf

In order to provide the reader with the necessary background information for the understanding of the rest of this paper, we give a short overview of RFC 8219 and **`siitperf`.**

A. Summary of RFC 8219 in a Nutshell

RFC 8219 has defined a benchmarking methodology for IPv6 transition technologies aiming to facilitate their performance measurement in an objective way producing reasonable and comparable results. To that end, it has defined *measurement setups*, *measurement procedures*, and several parameters such as standard frame sizes, duration of the tests, etc. To be able to deal with the high number of different IPv6 transition technologies, they were classified into the following categories: *dual stack*, *single translation*, *double translation* and *encapsulation* technologies, and the members of each category may be handled together.

RFC 8219 recommends the *Single DUT test setup* shown in Fig. 1 for the performance evaluation of the single translation technologies, where SIIT belongs to. Here, the *Tester* device benchmarks the *DUT* (Device Under Test). Although the arrows would imply unidirectional traffic, testing with bidirectional traffic is required by RFC 8219 and testing with unidirectional traffic is optional. Of course, both X and Y in IPvX and IPvY are from the set of {4, 6}. Naturally, if we are talking about SIIT, then it implies that X≠Y.

From among the measurement procedures, we summarize only those that are implemented by **`siitperf`**.

Throughput is defined as the highest (constant) frame rate at which the DUT can forward all frames without frame loss. Although its measurement procedure has special wording, in practice, the throughput is determined by a binary search. There are further conditions, e.g. core measurements of the binary search should last at least for 60 seconds and the tester should continue on receiving for 2 more seconds after finishing frame sending so that all residual (buffered) frames may arrive safely.

The *frame loss rate* measurement procedure measures the frame loss rate at some specific frame rates starting from the maximum frame rate for the media and decreasing the frame rate in steps not higher than the 10% of the maximum frame rate. Measurements may be finished after two consecutive 0% frame loss results.

```
         +--------------------+
         |                    |
+--------|IPvX   Tester   IPvY|<-------+
|        |                    |        |
|        +--------------------+        |
|                                      |
|        +--------------------+        |
|        |                    |        |
+------->|IPvX     DUT    IPvY|--------+
         |                    |
         +--------------------+
```

Fig. 1. Single DUT test setup [1].

Submitted: March 21, 2021, revised April 15.

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

DOI: 10.36244/ICJ.2021.2.1

Both the *latency* and the *packet delay variation* measurements are to be performed at the frame rate determined by the throughput test. The latency measurement has to tag at least 500 frames, the latencies of which are measured using sending and receiving timestamps, and the final results are the typical latency (the median of the latency values) and the worst case latency (the 99.9th percentile of the latency values). Packet delay variation measurement first determines the one way delay of every single frame, then it calculates the 99.9th percentile and the minimum of the one way delay values, and finally, their difference is the packet delay variation.

For an easy to follow introduction to RFC 8219, please refer to the slides of our IIJ Lab seminar presentation in Tokyo in 2017 [7].

On the one hand, we are not aware of any other RFC 8219 compliant benchmarking tools for network interconnect devices than our **`siitperf`**. On the other hand, RFC 8219 has taken several benchmarking procedures from the more than 20 years old RFC 2544 [8]. Several RFC 2544 compliant hardware and software Testers are listed in [9]. Further network benchmarking tools are collected and compared in [10].

B. *Summary of siitperf in a Nutshell*

We give a short overview of **`siitperf`** on the basis of our open access paper [3], in which all the details can be found. Our aim was to design and implement a high performance and also flexible research tool. To that end, **`siitperf`** is a collection of binaries and shell scripts. The core measurements are performed by one of three binaries, which are executed multiple times by one of four shell scripts. The binaries perform the sending and receiving of certain IPv4 or IPv6 frames[1] at a pre-defined constant frame rate according to the test setup shown in Fig. 1. We note that **`siitperf`** allows X=Y, that is, it can also be used for benchmarking an IPv4 or IPv6 router. The shell scripts call the binaries supplying them with the proper command line parameters for the given core measurement.

The first two of the supported benchmarking procedures (*throughput* and *frame loss rate*) require only the above mentioned sending of test frames at a constant rate and counting of the received test frames, thus the core measurement of both procedures is the same. The difference is that throughput measurement requires to find the highest rate at which the DUT can forward all the frames without loss, whereas the frame loss rate measurement requires to perform the core measurement at various frame rates to determine the frame loss rate at those specific frame rates. The core measurement of both tests is implemented in the **`siitperf-tp`** binary and the two different benchmarking procedures are performed by two different shell scripts.

The *latency* benchmarking procedure requires that timestamps are stored immediately *after* sending and receiving of tagged frames. The latency for each tagged frame is calculated as the difference of the receiving and sending timestamps of the given frame. The latency benchmarking procedure is implemented by **`siitperf-lat`**, which is an extension of **`siitperf-tp`**.

From our point of view, the *packet delay variation* benchmarking procedure is similar to the latency benchmarking procedure, but it requires timestamping of every single frame. The packet delay variation benchmarking procedure is implemented by **`siitperf-pdv`**, which is also an extension of **`siitperf-tp`**.

The binaries are implemented in C++ using DPDK to achieve high enough performance. We used an object oriented design: the **`Throughput`** class served as a base class for the **`Latency`** and **`Pdv`** classes.

Internally, **`siitperf`** uses *TSC* (Time Stamp Counter) for time measurements, which is a very accurate and computationally inexpensive solution (it is a CPU register, which can be read by a single CPU instruction: **`RDTSC`** [11]).

To achieve as high performance as possible, all test frames used by **`siitperf-tp`** and **`siitperf-lat`** are pre-generated (including the tagged frames). The test frames of **`siitperf-pdv`** are prepared right before sending by modifying a set of pre-generated frames: their individual identifiers and checksums are rewritten.

Regarding our error model, it is important that the sending and receiving of the frames are implemented by sender and receiver functions, which are executed as threads by the CPU cores specified by the user in the configuration file.

III. Our Error Model

A. *Accuracy of the Timing of Frame Sending*

There is an excellent paper that examines the accuracy of the timing of different software packet generators [12]. It points out that the *inter-sending time of the packets is rather imprecise* at demanding frame rates, if pure software methods are used. It also mentions the *buffering of the frames by the NIC* (Network Interface Card) among the root causes of this phenomenon, what we have also experienced and reported: our experience was that when a packet was reported by the DPDK function as "sent", it was still in the buffer of the NIC [3]. Unfortunately, this buffering completely discredits any investigation based on using timestamps stored at the sending of the frames: even if we store timestamps both before and after the sending of a frame, we may not be sure, when the frame was actually sent.

Imprecise timing may come from various root causes. At demanding frame rates, one of them is that our contemporary CPUs use several solutions to increase their performance including caching, branch prediction, etc. and they usually provide their optimum performance only after the first execution (or after the first few executions) of the core of the packet sending cycle, thus the first (few) longer than required inter-sending time(s) is/are followed by shorter ones to compensate the latency. This compensation depends on the

[1] more precisely: Ethernet frames containing IPv4 or IPv6 packets

timing algorithm of the sender function. For example, the original implementation of **dns64perf++** used a sophisticated algorithm that intended to distribute the compensation of such initial latency for the rest of the measurement time [13]. Unfortunately, the compensation algorithm did not work well and thus the sending rate was somewhat lower than required from the beginning of the measurement for a long time, and it was significantly higher than required at the end [14]. Therefore, we have replaced the timing algorithm with a simpler one that promptly compensates the latency [14]. We followed the same approach in **siitperf**, thus it sends the test frame (if it can), when its time has arrived, with no respect to what has happened before [3]. Therefore, **siitperf** very likely produces micro burst(s) at rates close to the upper limit of its sending performance.

Unfortunately, we did not have a NetFPGA device used by the authors of [12], therefore, we decided to check, how the imprecise timing of **siitperf** influences its measurement results. Our error model is that traffic with not exact inter-arrival time may have the following influence on the throughput test results:

1. The median decreases, because the imprecise timing causes sometimes overload and thus frame loss at lower rates than the throughput rate with precise timing.
2. The dispersion of the results increases, because some random events (like interrupts) influence each execution of the test differently.

The actual frame loss caused by the imprecise timing may also depend on a further parameter, namely, if Ethernet flow control (IEEE 802.3x) is used or not, because flow control may "iron out" the random peaks of the frame sending rate caused by imprecise timing.

Therefore, first, we test how the presence or absence of flow control influences the results. This phenomenon is interesting by itself, and the results of this comparison proved to be very important due to the limitations of our next examination.

Then, we benchmark the same DUT with both a calibrated tester and **siitperf** so that we can see the difference. The fact that **siitperf** is able to perform pure IPv4 or IPv6 benchmarking tests, allowed us to use an RFC 2544 [8] compliant legacy tester. This solution has also its limitations: although RFC 8219 has taken the throughput and frame loss rate tests verbatim from RFC 2544, the latency test has been redefined (it requires at least 500 tagged frames instead of a single one) and packet delay variation measurement is a completely new one. Thus they cannot be validated by an RFC 2544 tester.

We note that even if we can directly check the accuracy of frame sending of **siitperf-tp** only, we expect that the accuracy of frame sending of the other two programs is not worse, either. As for **siitperf-lat**, the relatively low number of tagged frames, which are distributed evenly, cannot make any significant effect. As for **siitperf-pdv**, the setting of their individual identifier and checksum requires some time, and thus there is non-zero lower bound for their inter-frame time, at least in theory. We note that it guarantees nothing in practice due to the fact of NIC buffering: back-to-back frames (that is frames with minimum inter-frame gap) may still occur.

B. *Consideration of Other Errors*

Unlike the sender function that sends frames individually, the receiver function may receive multiple frames together to ensure high performance. This can surely not cause any problem with the throughput and frame loss rate measurements, because the frames are only counted. The receiving timestamps of latency and packed delay variation tests may be influenced, but they are also influenced by buffering even if they are taken out from the receive buffer individually.

The sending and receiving timestamps are subject to further errors due to the fact that interrupts may occur between the sending/receiving of the frames and taking the timestamp by the execution of the RDTSC machine code instruction. This is a kind of error we cannot measure. As for latency measurements, one possible mitigation can be, if the user sets the number of time stamps to be used to a significantly higher value than the required minimum 500 (**siitperf** supports up to 50,000) and thus the calculation of the 99.9th percentile removes the errors, if they are rare enough. This mitigation automatically applies for packet delay variation tests, as all frames are time stamped.

Although it is the responsibility of the user to specify the four cores that execute the sending and receiving threads so that they belong to the same physical CPU as the main core (used for starting the program), **siitperf** does some sanity checks if the TSC-s of the four CPU cores are synchronized with that of the main core. Otherwise the TSC values specified for starting and stopping the experiment as well as the differences of the timestamps of the corresponding senders and receivers would be invalid.

We believe that all other errors including the conversions between (milli)seconds and TSC, the counting of the sent and received frames, the calculations with the timestamps, etc. are subject to general software testing and verification procedures.

IV. INVESTIGATION OF THE EFFECT OF ETHERNET FLOW CONTROL

To be able to investigate, how the presence or the absence of the Ethernet flow control influences the results, we needed a test system that is free from any other effects that may make our results noisy. Based on our SIIT benchmarking experience [15], we have chosen to reuse a previously built tests system, which was build up by two identical Dell PowerEdge C6220 servers in the NICT StarBED, Japan. The very same system was also used for benchmarking the extension of **siitperf** with the ability of using random source and destination port numbers [16] as required by RFC 4814 [17].

We have taken the following description of the test system from that paper [16].

"The servers were equipped with two 2GHz Intel Xeon E5-2650 CPUs having 8 cores each, 128GB 1333MHz DDR3 RAM and Intel 10G dual port X520 Ethernet network adapters.

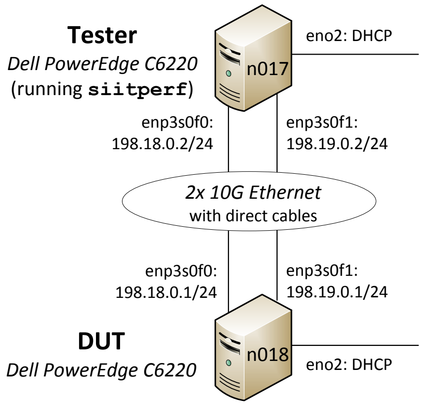


Fig. 2. Measurement setup for IPv4 Linux kernel routing: throughput tests with and without Ethernet flow control.

The Debian Linux operating system was updated to version 9.13 on all computers. The Linux kernel version was: 4.9.0-4-amd64. The DPDK version was 16.11.11-1+deb9u2." [16]

The "varport" branch of **siitperf** was used, its latest commit was bfddb5f on Aug 23, 2020. (Since then, the varport branch was merged into the master branch.)

We expected that the difference between the results with and without Ethernet flow control depends on the frame rate and we also wanted to test this hypothesis.

To achieve high enough frame rates, first, we benchmarked IPv4 kernel routing using random source and destination port numbers as we did in [16]. The topology of the test system is shown in Fig. 2. The CPU clock rate was set to fixed 2GHz on both computers and hyperthreading was switched off (using the same BIOS settings as specified in the appendix of [18]). All cores of the second CPU of the DUT were switched off using the **maxcpus=8** kernel parameter to avoid NUMA issues (please refer to [15] for a detailed explanation).

As for frames sizes, we used 64, 128 and 256 bytes from among the standard frame sizes recommended by RFC 8219, because the throughput of the DUT was limited by the performance of the DUT with these frame sizes, whereas throughput was limited by the maximum frame rate of the 10G Ethernet for all higher standard frame sizes.

Technical note: **siitperf** interprets the specified frame size values for IPv6 frames and uses 20 bytes less for IPv4 frames, therefore we always set 20 bytes higher values. This is important, if someone would like to repeat our experiments.

As required by RFC 8219, we used bidirectional traffic and 60s long tests at each step of the binary search. The *Error*[2] parameter of the binary search was set to 1. The throughput tests were performed 20 times and the median, minimum and maximum values of the 20 results were calculated. In addition to that, we have also calculated another value to express the consistent or scattered nature of the results, which we named *dispersion* and defined as follows:

$$Dispersion = \frac{max - min}{median} \cdot 100\% \qquad (1)$$

The results are shown it Table I. We note that commercial Testers like the one we used in the next section, usually report the number of *all* frames per second (including frames in both directions), but **siitperf** reports the number of frames per second *per direction*. Thus the number of *all* frames per second forwarded by the Linux kernel was the double of the numbers shown in Table I.

Let us compare the results with and without flow control for each frame size individually. As for 64-byte frames, the median throughput with flow control (3,432,658fps) is about 0.6% higher than the median throughput without flow control (3,411,322fps). The lack of flow control has also significantly increased the dispersion of the results (from 0.6% to 1.28%). As for 128-byte frames, the median throughput with flow control (3,352,378fps) is only about 0.2% higher than the median throughput without flow control (3,444,630fps). Finally, with 256-byte frames, the median throughput with flow control (3,153,894fps) is only about 0.03% higher than the median throughput without flow control (3,152,872fps). We can observe that the difference between the median of the results with and without flow control definitely decreases with the increase of the frame size.

We are satisfied with the results in the sense that the 3.4Mfps is more than the half of the 6.3Mfps maximum frame rate **siitperf** can achieve on the given hardware [16] and our results with and without Ethernet flow control are quite close to each other (even the largest difference is below 1%).

To be able to test the effect of the Ethernet flow control at a significantly lower frame rate using the very same test system, we used fixed port numbers. In this case, the packet processing at the DUT was not hashed to all 8 active CPU cores of the DUT, but only two CPU cores were used[3] (one core per direction). This time we performed the throughput measurements using all standard frame sizes, as throughput was always lower than the theoretical maximum value for the media at the given frame size. Our results with flow control are shown in Table II. As we expected, the dispersion of the results is lower than 1% for all frame rates. The median throughput slightly decreases, when we increase the frame size from 64 bytes (885,643fps) through 128 bytes (878,256fps) to 256 bytes (857,575fps). There is significant decrease at 512 bytes (779,410fps) and median throughput remains constant (within measurement error) at all higher frame sizes. The investigation of the decrease of the median at 512 bytes is beyond the scope of our current paper, we just mention that it can also be observed in Fig. 3 of [15].

[2] Error means that the binary search may stop, when: *upper_limit – lower_limit ≤ Error*.

[3] We could observe only the load caused by software interrupts.

TABLE I.
IPv4 Linux kernel routing performance **with and without flow control**, Dell PowerEdge C6220 servers, fixed 2GHz CPU clock rate, 8 active CPU cores, RFC 4814 **random port numbers**

mode	*with flow control*			*without flow control*		
frame size	***64 bytes***	***128 bytes***	***256 bytes***	***64 bytes***	***128 bytes***	***256 bytes***
median (fps)	3,432,658	3,352,378	3,153,894	3,411,322	3,344,630	3,152,872
min (fps)	3,420,774	3,347,624	3,145,506	3,374,999	3,312,499	3,140,624
max (fps)	3,441,407	3,359,921	3,158,448	3,418,731	3,351,578	3,164,064
disp. (%)	0.60	0.37	0.41	1.28	1.17	0.74

TABLE II
IPv4 Linux kernel routing performance **with flow control**, Dell PowerEdge C6220 servers, fixed 2GHz CPU clock rate, 8 active CPU cores, but only two of them are used due to **fixed port numbers**

frame size	*64 B*	*128 B*	*256 B*	*512 B*	*768 B*	*1024 B*	*1280 B*	*1518 B*
med (fps)	885,643	878,256	857,575	779,410	779,503	779,982	779,194	779,035
min (fps)	882,811	874,006	855,467	775,389	777,326	777,342	777,828	777,342
max (fps)	887,696	880,860	859,631	781,746	781,861	781,251	780,274	779,663
disp. (%)	0.55	0.78	0.49	0.82	0.58	0.50	0.31	0.30

TABLE III
IPv4 Linux kernel routing performance **without flow control**, Dell PowerEdge C6220 servers, fixed 2GHz CPU clock rate, 8 active CPU cores, but only two of them are used due to **fixed port numbers**

frame size	*64 B*	*128 B*	*256 B*	*512 B*	*768 B*	*1024 B*	*1280 B*	*1518 B*
med (fps)	880,381	875,126	850,740	778,295	778,861	778,535	779,078	779,069
min (fps)	826,610	742,186	749,999	757,807	765,624	734,374	749,693	749,968
max (fps)	883,850	876,617	853,763	780,274	780,274	779,790	780,518	779,420
disp. (%)	6.50	15.36	12.20	2.89	1.88	5.83	3.96	3.78

Our results without flow control are shown in Table III. The difference of the median throughput between the results with flow control (885,643fps) and without flow control (880,381fps) is about 0.6% at 64 bytes frame size. Although this difference decreases to 0.36% at 128 bytes, but it is about 0.8% at 256 bytes frame size. Thus the increase of the frames size was not enough to make the difference diminish. For the following three standard frame sizes, this difference is about: 0.14%, 0.08%, 0.2%, and for the last two frame sizes, the difference is deliberately less than measurement error. Unfortunately, the dispersion of the results of the measurements without flow control is rather high: it exceeds 15% at 128 bytes frame size. At this point, we cannot tell whether this high dispersion is caused by the improper timing of **`siitperf`** or by the nature of the DUT.

V. Calibration with a Standard Tester

We have built two test systems to determine the IPv4 routing performance of the same DUT, which was a Sun Fire X4150 server with two Quad Core 2.83GHz Intel Xeon E5440 CPUs, four 2GB 667MHz DDR2 SDRAM modules and four Gigabit Ethernet ports. Debian 9.11 GNU/Linux operating system with 4.9.0-5-amd64 kernel was installed on it. The clock frequency of all 8 CPU cores was set to fixed 2.833GHz using the **`cpufreq-set`** command of the **`cpufrequtils`** package.

A. Reference Measurement

To provide reference, the throughput of IPv4 Linux kernel routing was measured using a commercial Anritsu MP1590B Network Performance Tester. It had a four port Anritsu MU210212A 10/100/1000M Ethernet Module, and we used Port1 and Port2 of the module. The measurement setup is shown in Fig. 3.

As RFC 8219 has somewhat extended the standard frame sizes to be used for benchmarking originally defined in RFC 2544, we have chosen custom frame sizes and defined the following frame sizes: 64, 128, 256, 512, 768,1024, 1280, 1518.

As required by RFC 8219, bidirectional traffic was used and full 60s length trials were executed and the “Loss Tolerance” parameter was set to 0%.

The Anritsu tester has a parameter called “Resolution”, which can be specified as the percentage of maximum frame rate of the media. Its smallest possible value is 0.01. As the theoretical maximum frame rate for Gigabit Ethernet with 64 byte frame size is 1,488,095, this setting means that the

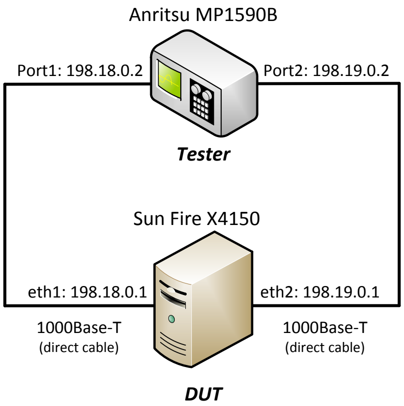


Fig. 3. Measurement setup for IPv4 Linux kernel routing: reference throughput test with a commercial Tester.

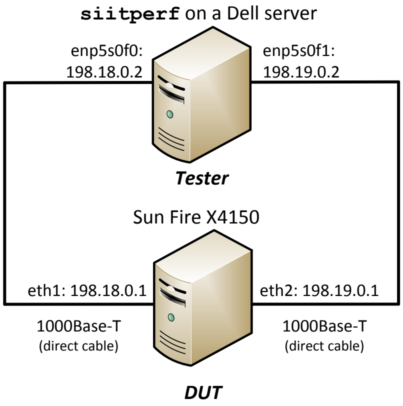


Fig. 4. Measurement setup for IPv4 Linux kernel routing: throughput test with **siitperf**.

resolution (or with other words *error*) of the binary search was about 149fps (calculated as: 1,488,095/10,000).

We note that the Anritsu tester does not perform a binary search, if the test at the "Maximum Frame Rate" is successful. We set the value of this parameter to 100%.

By default, flow control was not enabled on the Anritsu tester. When we enabled flow control, the Anritsu tester became practically unusable for throughput measurements, because it qualified all tests as successful, even if they lasted much longer than 60s. Thus, we could use this tester for meaningful measurements only, when flow control was disabled.

B. Measurements with Siitperf

The parameters of the DUT were the same as in the previous case, but this time the Tester was a Dell PowerEdge R620 server with two six core 2GHz Intel Xeon E5-2620 CPUs, two 16GB 1600MHz DDR3 SDRAM modules and with an additional Intel I350-T4 Ethernet Server Adapter (needed for DPDK). Debian 9.11 GNU/Linux operating system with 4.9.0-11-amd64 kernel was installed on it. The version of DPDK was 16.11.9-1+deb9u2. As **siitperf** does not have version numbers yet, we can identify its version with its latest commit number 05247a1 on Jul 1, 2020. This time, we used the master branch.

The measurement setup is shown in Fig. 4. We used the same standard frame sizes mentioned before.

As required by RFC 8219, bidirectional traffic was used and full 60s length trials were executed, and the "Error" of the binary search was set to 1.

We note that as the **binary-rate-alg.sh** script distributed with **siitperf** supports only tests for a single pre-set frame size, with a single pre-set upper bound, we have added a **for** cycle to the script with the appropriate frame sizes and the following upper bounds for the consecutive standard frame sizes: 1,500,000 850,000 460,000 240,000 160,000 120,000 100,000 82,000. They are wilfully somewhat higher than the theoretical maximum frame rates for the media with the given frame size, because we wanted to test and demonstrate how **siitperf** behaves, when the maximum frame rate for the media is achieved by the DUT. Our script performed the binary search for all standard fame sizes starting in the interval of 0 (as lower bound) and the above mentioned upper bound values.

Unlike with the Antritsu Tester, the log file of the DUT showed that flow control was enabled on the interfaces used for testing (Flow Control: Rx/Tx). We tried to switch off flow control using the same command as with the 10G Ethernet interfaces (**ethtool -A *interface* rx off tx off**), which has been executed without any error message, however flow control remained enabled.

C. Results

The Anritsu Tester reported the results in a form of a graph, which we include in Fig. 5 to facilitate an easy overview of the results. Except for the first two frame sizes, the throughput achieved its theoretical maximum value. However, this reporting format covers some very important details by displaying only the average value of the measurement results. Therefore, we processed the detailed result file and calculated the median, minimum, and maximum of the 20 throughput results for each frame size. Please see our results in Table IV. We note that the Anritsu Tester reported the number of *all*

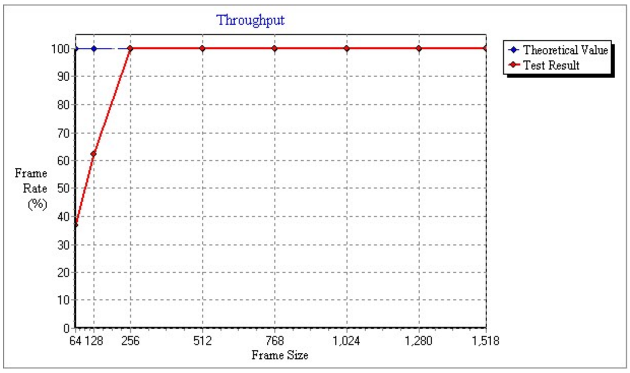


Fig. 5. IPv4 Linux kernel routing performance of the Sun server: reported by the Anritsu Tester with no flow control

TABLE IV
IPv4 LINUX KERNEL ROUTING PERFORMANCE OF THE SUN SERVER: MEASURED BY THE ANRITSU TESTER WITHOUT FLOW CONTROL

frame size	*64 B*	*128 B*	*256 B*	*512 B*	*768 B*	*1024 B*	*1280 B*	*1518 B*
med (fps)	548,958	526,351	452,899	234,962	158,629	119,732	96,154	81,274
min (fps)	511,310	522,720	452,853	234,962	158,629	119,732	96,154	81,274
max (fps)	553,720	529,561	452,899	234,962	158,629	119,732	96,154	81,274
disp. (%)	7.73	1.30	0.01	0.00	0.00	0.00	0.00	0.00

TABLE V
IPv4 LINUX KERNEL ROUTING PERFORMANCE OF THE SUN SERVER: MEASURED BY **SIITPERF** WITH FLOW CONTROL

frame size	*64 B*	*128 B*	*256 B*	*512 B*	*768 B*	*1024 B*	*1280 B*	*1518 B*
med (fps)	549,297	522,413	452,930	234,986	158,652	119,752	96,173	81,294
min (fps)	547,850	521,285	452,926	234,986	158,650	119,752	96,173	81,294
max (fps)	550,782	524,610	452,960	234,990	158,667	119,767	96,178	81,301
disp. (%)	0.53	0.64	0.01	0.00	0.01	0.01	0.01	0.01

frames per second (including frames in both directions), but we divided the results by two to report the number of frames per second *per direction*. We did so to show values comparable with the theoretical maximum frame rates given in Appendix A.1 of RFC 5180 [19].

One of the most conspicuous things in the table is the high dispersion of the results at 64-byte frame size. It is caused by a single outlier. We have investigated the case in the measurement log file, and we found that 8 frames were missing during that step of the binary search when the target rate was 34.37%. Of course, it meant that the test failed. After that, all tests were successful and thus the final result was 34.36%. This single outlier does not influence the median, but it is reflected by the minimum and, therefore, in the dispersion, too.

As for the results at 128-byte frame size, the minimum and the maximum are nearly symmetrical around the median.

As for the results at 256-byte frame size, a single test failed at 100% due to the loss of a few frames, therefore, binary search was performed, which finished at 99.99%. All other tests passed at 100% and thus no binary search was performed.

No binary search was performed at any higher frame sizes, this is why their minimum and maximum values are equal with their medians.

The results of the throughput measurements with **siitperf** are shown in Table V. The dispersion of the results is always below 1%, and it is practically 0 upwards from 256 bytes frame size, as the maximum frame rate for the media has limited the throughput. As the upper limit was set higher than the theoretical maximum frame rate for the media, **siitperf** executed binary search and it measured slightly higher values. It was possible for at least two reasons:

- As Appendix A.1 of RFC 5180 states: “Ethernet's maximum frame rates are subject to variances due to clock slop. The listed rates are theoretical maximums, and actual tests should account for a +/- 100 ppm tolerance.”
- The “TOLERANCE” parameter of **siitperf** was set to 1.00001, which means that 0.001% more time is allowed for sending.

There are two throughput values that were limited by the CPU performance: throughput measured with 64 bytes and 128 bytes frame sizes. The differences of the results of the two test systems are 0.06% and 0.75%, which we consider good and acceptable, respectively.

VI. DISCUSSION AND PLANS FOR FUTURE RESEARCH

Our conditions for calibrating **siitperf** with a standard tester were far from ideal. We cannot tell the maximum frame rate, at which the CPU of the Dell PowerEdge R620 server would be able to generate frames, but it is very likely several million frames per second, thus the measured throughput around 550,000 fps was not at all close to it. The technical issue that we could use the Anritsu tester only without flow control, whereas we could use **siitperf** only with flow control (in the Gigabit Ethernet environment) makes the comparison of their results more difficult.

We plan to purchase a NetFPGA device like the one used by the authors of [12] and examine the inter-frame time of the traffic generated by **siitperf**.

We also plan to test the accuracy of **siitperf** in a 10GBase-T environment with a Spirent SPT-N4U Tester used out of courtesy for the measurements of [20].

VII. CONCLUSION

We have carefully examined, what kind of factors may distort the measurement results of **siitperf**, and we set up an error model.

We have compared the results of **siitperf** used with and without Ethernet flow control in a 10GBase-T environment, and we found that the deviation of the results was always below 1%.

We have calibrated **siitperf** with a commercial Tester in a Gigabit Ethernet environment, and we found that the deviation of the results was below 1%.

We conclude that it is necessary to calibrate **`siitperf`** also in a 10GBase-T environment and we plan to do so.

Acknowledgements

The measurements for the investigation of the effect of Ethernet flow control were carried out by remotely using the resources of NICT StarBED, 2-12 Asahidai, Nomi-City, Ishikawa 923-1211, Japan. The author would like to thank Shuuhei Takimoto for the possibility to use StarBED, as well as to Satoru Gonno and Miku Takuma for their help and advice in StarBED usage related issues.

The author thanks the National Media and Infocommunications Authority (NMHH) of Hungary for lending us the Anritsu MP1590B Network Performance Tester. The author thanks István Pilisi, NMHH, for his support how to use the device.

The author thanks István Pilisi and Alexandru Moise for reading and commenting the manuscript.

References

[1] M. Georgescu, L. Pislaru, G. Lencse, “Benchmarking methodology for IPv6 transition technologies”, IETF RFC 8219, 2017. doi: 10.17487/rfc8219

[2] G. Lencse and Y. Kadobayashi, “Comprehensive survey of IPv6 transition technologies: A subjective classification for security analysis”, *IEICE Transactions on Communications*, vol. E102-B, no 10, pp. 2021–2035. doi: 10.1587/transcom.2018ebr0002

[3] G. Lencse, “Design and implementation of a software tester for benchmarking stateless NAT64 gateways”, *IEICE Transactions on Communications*, vol. E104-B, no. 2, pp. 128-140. doi: 10.1587/transcom.2019ebn0010

[4] C. Bao, X. Li, et al., IP/ICMP translation algorithm, IETF RFC 7915, doi: 10.17487/rfc7915

[5] D. Scholz, “A look at Intel’s dataplane development kit”, *Proc. Seminars Future Internet (FI) and Innovative Internet Technologies and Mobile Communications (IITM)*, Munich, 2014, pp. 115–122. doi: 10.2313/NET-2014-08-1_15

[6] G. Lencse, Siitperf: An RFC 8219 compliant SIIT (stateless NAT64) tester, free software under GPLv3 license, [Online] Available: https://github.com/lencsegabor/siitperf

[7] G. Lencse, Benchmarking methodology for IPv6 transition technologies, IIJ Lab seminar, Tokyo, Oct. 10, 2017. [Online] Available: https://seminar-materials.iijlab.net/iijlab-seminar/iijlab-seminar-20171010.pdf

[8] S. Bradner, J. McQuaid, Benchmarking methodology for network interconnect devices, IETF RFC 2544, 1999. doi: 10.17487/rfc2544

[9] D. Raumer, S. Gallenmüller, et al., “Revisiting Benchmarking Methodology for Interconnect Devices”, *Proc. 2016 Applied Networking Research Workshop (ANRW’16)*, Berlin, 2016. doi: 10.1145/2959424.2959430

[10] K. Velásquez and E. Gamess, “A survey of network benchmark tools”, in: *Machine Learning and Systems Engineering*, Springer, Dordrecht, 2010, pp. 465–480. doi: 10.1007/978-90-481-9419-3_36

[11] Intel, Intel 64 and IA-32 Architectures Software Developer’s Manual, Volume 2B: Instruction Set Reference, M-U, Order Number: 253667-060US, 2016. [Online] Available: https://www.intel.com/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-vol-2b-manual.pdf

[12] P. Emmerich, S. Gallenmüller, et al., Mind the gap - A comparison of software packet generators, *Proc. 2017 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS)*, Beijing, China, 2017. doi: 10.1109/ancs.2017.32

[13] G. Lencse, D. Bakai, “Design and implementation of a test program for benchmarking DNS64 servers”, *IEICE Transactions on Communications*, vol. E100-B, no. 6, pp. 948–954. doi: 10.1587/transcom.2016EBN0007

[14] G. Lencse and A. Pivoda, “Checking and increasing the accuracy of the dns64perf++ measurement tool for benchmarking DNS64 servers”, *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, vol. 7, no 1, pp. 10–16. doi: 10.11601/ijates.v7i1.255

[15] G. Lencse, K. Shima, “Performance Analysis of SIIT Implementations: Testing and Improving the Methodology”, *Computer Communications*, vol. 156, no. 1, pp. 54–67. doi: 10.1016/j.comcom.2020.03.034

[16] G. Lencse, “Adding RFC 4814 random port feature to siitperf: Design, implementation and performance estimation”, *International Journal of Advances in Telecommunications, Electrotechnics, Signals and Systems*, vol. 9, no. 3, pp. 18–26. doi: 10.11601/ijates.v9i3.291

[17] D. Newman, T. Player, “Hash and stuffing: Overlooked factors in network device benchmarking”, IETF RFC 4814, 2008. doi: 10.17487/RFC4814

[18] G. Lencse and Y. Kadobayashi, “Benchmarking DNS64 Implementations: Theory and Practice”, *Computer Communications*, vol. 127, no. 1, pp. 61–74. doi: 10.1016/j.comcom.2018.05.005

[19] C. Popoviciu, A. Hamza, et al., “IPv6 benchmarking methodology for network interconnect devices”, IETF RFC 5180, 2008. doi: 10.17487/rfc5180

[20] G. Lencse, “Benchmarking Stateless NAT64 Implementations with a Standard Tester”, *Telecommunication Systems*, vol. 75, no. 3, pp. 245–257. doi: 10.1007/s11235-020-00681-x

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

He has been working full time for the Department of Telecommunications, Széchenyi István University, Győr, Hungary since 1997. Now, he is a Professor. He has been working part time for the Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, Hungary as a Senior Research Fellow since 2005. The main area of his research is the performance and security analysis of IPv6 transition technologies. He is a co-author of RFC 8219.

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

Enhancing the operational efficiency of quantum random number generators

Botond L. Márton, Dóra Istenes and László Bacsárdi, *Member, IEEE*

Abstract— **Random numbers are of vital importance in today's world and used for example in many cryptographical protocols to secure the communication over the internet. The generators producing these numbers are Pseudo Random Number Generators (PRNGs) or True Random Number Generators (TRNGs). A subclass of TRNGs are the Quantum based Random Number Generators (QRNGs) whose generation processes are based on quantum phenomena. However, the achievable quality of the numbers generated from a practical implementation can differ from the theoretically possible. To ease this negative effect post-processing can be used, which contains the use of extractors. They extract as much entropy as possible from the original source and produce a new output with better properties. The quality and the different properties of a given output can be measured with the help of statistical tests. In our work we examined the effect of different extractors on two QRNG outputs and found that with the right extractor we can improve their quality.**

Index Terms—**random numbers, statistical testing, quantum communication, QRNG**

I. Introduction

Quantum technologies are developing at a rapid speed in the modern world and they vastly differ from their classical counterparts. They offer new approaches for communication, cryptography or algorithm design. From an algorithmic standpoint they propose new and in many cases faster algorithms (for example Shor's algorithm for prime factoring or in the area of resource distribution [1]) which can utilize the unique phenomena present only in the world of quantum mechanics[2][3]. Two of the most developed technologies in the field are QRNGs and QKD (Quantum Key Distribution). QKD is mostly used as a building block in cryptographic solutions. One of these is the one-time pad encryption scheme, where parties use a different, unique random key for the encryption of each message. This is a mathematically proven secure method, with only one weakness, sharing the keys. QKD patches this weakness by providing a safe way to share the keys between the parties [4].

The application of random numbers ranges from dice simulators to cryptographic systems and mathematical simulations [5]. These various usages require different traits from the generators. High bitrate, quality, and safety are among the attributes the different applications expect.

Quantum generators make ideal outputs for most requirements, but their main quality is generating truly random numbers due to an underlying quantum phenomenon. Even so, they have their flaws, which mainly come from the limits of our physical tools.

The field of QRNGs is becoming more popular as some of the generators are already available on the commercial market (one of which is briefly introduced in Section II.A), see [6] for more. At the same time the field of randomness extraction also had interesting results. Ma et al investigated the effect of a Trevisian and Toeplitz extractor on a QRNG in [7]. In our work, we applied the Toeplitz extractor as well but the QRNG they used is based on a different generation mechanism. Qi and Bing tested a generator based on amplified spontaneous emission [8]. One of the QRNGs we worked with is also based on amplified spontaneous emission, but they used a different setup. In [9] Zhang, Xiao-Guang, et al presented a generator based on laser phase fluctuations, where they used a pipeline based solution with a Toeplitz extractor to achieve real-time processing. In our work we used the Toeplitz extractor, but the real-time operation was not one of our goals, therefore our implementation differs. Shakhovoy, Roman, et al. introduced a QRNG which works without the need for post-processing [10]. In current work we focused on investigation of QRNG, but another important question is the comparison of efficiency between QRNGs and PRNGs which was investigated by Martínez, Aldo C., et al in [11].

In our work we concentrated on two QRNGs, which were built at Budapest University of Technology and Economics (BME)[16]. Prior to our work, the generators were only tested without post-processing. In this paper, we present how extractors can improve the quality of two outputs from these generators. We implemented the extractors in Python, examined their applicability and their yielded results.

This article is structured as follows. In Section II we will introduce two popular generation methods used in QRNGs (on which the tested generators are based on) then we will show how can we measure the quality of random numbers and what is an extractor. After that in Section III we will present what we found during our testing, while Section IV contains our conclusion.

The authors are with the Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, H-1117 Hungary.
E-mail: martonboti@gmail.com, idooori@gmail.com, bacsardi@hit.bme.hu.

The work was supported by the National Research Development and Innovation Office of Hungary (Project No. 2017-1.2.1-NKP-2017-00001). L. Bacsárdi thanks the support of the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

DOI: 10.36244/ICJ.2021.2.2

II. RANDOM NUMBER GENERATORS

A. Generation methods

PRNGs generate a stream based on a mathematical algorithm and a starting point, the so-called seed. Although this makes it easy to generate numbers in high quantity, it also makes the output deterministic, and in turn prone to exploitation. Within possession of its algorithm and seed, which may be acquired through inspecting the output, the PRNGs upcoming outputs become easily predictable. This makes it highly unsafe to use them in applications with a high-security requirement, such as lottery or cryptographic solutions [12].

For TRNGs their entropy source comes from inherently random events, like radioactive decay, atmospheric noise or quantum mechanical events. Their set up is much more complex than the PRNGs, and their generation speed is also slower, but due to the high unpredictability of their source, their output is adequate for high-security uses.

QRNGs provide non-deterministic outputs in great quantities in a short time. and they are one of the most actively developed quantum computing technologies.

The two main producers of commercially available QRNG chips are ID Quantique (IDQ) and Quantum Numbers Corp (QNC). Both companies produce state of the art QRNG chips although the smallest commercial one belongs to IDQ, the Quantis QRNG chip. It contains a LED light source that emits random number of photons which are captured and counted by an image sensor, providing a set of easily accessible raw numbers. It also has a self-verification process, where if it detects any failure it starts an automatic recovery procedure instantly and notifies the user [13].

B. Photon detection interval

Many types of optical QRNGs exist. A portion of them rely on a beam splitters and different amount of detectors. These tools can contribute greatly to the bias of a generator. In theory there are ideal equipments but in truth, perfect tools do not exist. Even a single detector's quantum efficiency is not 100% but using multiple detectors raises the problem of the two detectors differences [14].

The photon detection interval generator uses only one detector, as to mitigate the bias.

The distribution of the time between two detections is exponential with a probability density function $\lambda e^{-\lambda t}$ where λ is the expected number of photons detected in a unit of time.

The time values are compared in pairs. For t_1, t_2 time values the generator returns 0 if $t_1 > t_2$ and 1 in case of $t_2 > t_1$. We restart the clock at each detection to eliminate correlation between the data. The time values of course have a certain amount of accuracy which makes equal values more probable. To overcome this issue we discard equal values [6].

C. Amplified Spontaneous Emission

To achieve long ranges in fiber communication optical amplification is used. The basis for this technique is stimulated emission. During stimulated emission when a particle in excited state interacts with an incoming photon, the excited particle drops to a lower energy level emitting a new photon, whose properties are the same as the ones which started the process. For stimulated emission to be dominant over absorption, population inversion must be present. This means that there are more particles in excited state than in lower energy state. However, if stimulated emission is possible for a particle, than so is spontaneous emission, during which an excited particle randomly drops to a lower energy level while emitting a new photon with random properties. This photon then can cause stimulated emission thus creating amplified spontaneous emission, ASE. In an optical system this phenomenon is considered noise which fortunately can be measured, therefore it can be used as a basis for random number generation. During generation if there is no incoming signal in the amplifier, ASE will be the dominant interaction. Then the optical power can be sampled, giving statistically independent random variables. [6][15][16]

D. Measuring the randomness

As we saw earlier, there are many ways to build a random number generator. But we need to determine the quality of the numbers (or the bits) which are coming out of the machine. The first problem is that we have to measure how random the output is. This means that we need to define what randomness is. This is a hard task, because we cannot tell certainly whether a given finite sequence of bits is random or not. In most cases we have to settle for a more practical solution. Instead of declaring that the output of a generator is truly random with absolute certainty, we will say that the output is closer to a true random source then a given limit. Therefore we can only say with a given probability, that the measured output is random or not, but if this probability is high enough, this approach is good for most usages.

The tests we can use on a generator (or the output of this generator) can range from the very simple to the more complex; but they have a common property: they require a finite number of bits. This means that firstly the length of the bit sequence is important. The longer the sequence is the better the precision of the tests. Secondly, this means that we can never look at the whole output of a generator, only a part of it and we have to make a decision based on this part. It is therefore possible that the generator will fail the same test that it passed earlier, because on the second run the new output will be different. To give an example of a simple test one can think about a truly random source, e.g. the uniform distribution. It puts out a 1 or a 0 bit with equal probability (50%), so if one looks at a longer and longer sequence from this source, one will find out the number of 1s and 0s is approaching the same number. This can be interpreted as a test: we count the 1 and 0 bits in the output of the generator and compare them to each other.

The main goal of these tests is to measure the randomness of the sequence which cannot be made with certainty as it was stated earlier, that's the reason why these tests are statistical tests. They take a statistical property (for example the number of 1s and 0s as mentioned above) and based on this result and a previously given criterion (for example: how far can the number of 1s and 0s differ from each other) can declare whether the sequence passed or not. Most of the tests fall under the statistical hypothesis test category. In the hypothesis test we want to accept or reject the null-hypothesis (H_0). During the testing of a random number generator the null-hypothesis is that the generator is producing random numbers. The other hypothesis in the test is called the alternative hypothesis (H_a). H_a is the opposite of H_0: it says that the generator isn't producing truly random numbers. The next step is to calculate a distribution function with the help of a probabilistic value (most of the time these are well known probabilistic values) while assuming that the null-hypothesis is true. After this we select a significance level (α) on this distribution. Generally, this is a very small value. In the RNG testing α tends to be around 1%. Lastly, we calculate the statistical value which the given test measures and compare it to the significance level. If it is below α, we reject the null-hypothesis and accept the alternative. If it is above it, we accept the null-hypothesis and reject the alternative. Based on our decision and the reality we have four possible outcomes. If we accepted the null-hypothesis and it is in fact true, we chose correctly (this has a probability of 1-α). It is the same if we rejected it and it was false in reality (the probability of this outcome is 1-β). The other two outcomes are called Type I and Type II error. The Type I error occurs when we rejected H_0, but it was true. This outcome has a probability of α and is called false positive. The Type II error is when we accept H_0, but it was false. It has a probability of β and is called false negative. Out of these two the Type I is more acceptable and with a good decision on the value of α we can fine tune it. In this case we falsely brand the RNG as "not random" in the test. But with the help of other tests we can still state at the end that it is in fact "random". The Type II error is harder to manage, because here a "not random" source passed the test it should not have. To lower the probability of the Type II error we have to choose an acceptable value for α and for the length of the sequence. The above mentioned information can also be interpreted as a so called p-value. The p-value is between 0 and 1 and it is the probability of getting results at least as extreme as the ones observed, given that the null-hypothesis is correct. In other words it is a metric showing how strong our evidences supporting the null-hypothesis are. To use the p-value we compare it to α and if it is below it we reject H_0. It is important to note here that α is used as a lower and 1- α is used as an upper bound and the p-values obtained throughout the test should follow a uniform distribution as well.

When we want to measure the randomness of a given bit sequence one test can only look at one property of the sequence. Therefore we need multiple tests which we can use and we need them to be different (in the sense that they are testing different properties). To solve the issue certain test were grouped together into a so-called test suite. Some of the suites are defined by standards, other are organized by various people.

An example for a standardized test suite is the NIST STS (National Institution of Standards and Technology Statistical Test Suite) [17] which consist of 15 different test and used widely in the world. Another test is the Diehard [18] and it is extended version the Dieharder [19] which are maintained by a community. The Dieharder suite consists of around 100 tests (it includes the NIST STS as well) which cover a large range of complexity. One of these test is the 32x32 binary rank test. This test takes 32 32-bit integer and builds a 32-by-32 matrix of 1s and 0s. Then it calculates the rank of this matrix and goes on for the next 32 number. Ranks less than or equal to 29 are rare, therefore they are treated as one rank. A Chi-squared test [20] is performed on the ranks 32, 31, 30, and ≤ 29,checking the uniformity of these rank groups.

One important question regarding these tests is when to use them. Using the tests must be part of the creation process of the generator. It is important during this time to run selected tests which might point to possible flaws in the design. After the generator is complete or when it is used in a real system monitoring the randomness of the output is vital for the underlying system which is using the numbers from the generator and for the maintenance of the generator as well. These tests can be used in real-time [21]. The NIST published several recommendations on which tests to use in which part of the generators lifecycle [22].

E. Extractors

With the help of the statistical tests we mentioned in the previous section we can measure the quality of the numbers produced by a generator while we are building it. This helps us to see how far are we in the development. If we are not satisfied with the results, we can try to make the construction better with for example a new layout or with the help of more precise components. But there is point where we cannot improve the system further just by fine tuning because the physical implementation of an RNG cannot be 100% efficient or the physical phenomenon which the generator is based on hasn't got a high enough entropy. This means that we have to find another way to improve the quality of the generated numbers which comes after the generation phase. This is the post-processing, where we aim to improve the original output of the generator by making a new with better properties.

During post-processing we use extractor functions or algorithms. Their main goal is to extract as much entropy from the original source as possible and to create a new output whose entropy is as close to the original source as possible and has a better quality [23]. Previously we mentioned that a good random number generator is close to a truly random source or indistinguishable from it. Now we will define what this means. The distance of two random variable can be written as:

$$d(X,Y) = \max_{a \in A} |P_X(a) - P_Y(a)|$$

where X and Y are random variables of the same sample space A. If we think about our generator and a truly random source as a random variable can modify the definition to this:

$$d(X, U) = \max_{a \in A} |P_X(a) - P_U(a)| \leq \varepsilon.$$

In this inequality X is random variable (our generator), U is a random variable representing the uniform distribution (a truly random source) and ε is an upper bound for the distance. If X satisfies this inequality we say that X is ε uniform.

The next step is to measure the entropy of the source, because the main objective of the extractors is to extract as much entropy as possible and we need a way to compare the new output to the old one. There are different ways to measure the entropy for example the Shannon entropy but in the case of extractors the min-entropy is the mostly used version.

The definition of the min-entropy is the following:

$$H_\infty(X) = \min_x \left\{ \log\left(\frac{1}{P(X=x)}\right) \right\}$$

where log is the base 2 logarithm and X is a random variable. With the help of this definition we can calculate the minimum entropy for the source if we want an ε-uniform bit sequence with length m. For the uniform distribution the probability of all possible outcome is 2^{-m}. This means that the min-entropy is m and this is the value we want to reach (or get close to it).

We can distinguish different extractors. The first group is the deterministic extractors. These extractors use a source denoted with C, a min-entropy, an input with a length of n and have an output with length k and of course they are ε-uniform. Because they are deterministic the output only depends on the input, this means that for the same input they will produce the same output.

The second group is the so-called seeded extractors. They have the same properties as the deterministic extractors, but they also have a seed with length d. The seed is used as an initialization vector just like with a hash function for example. During the creation of the new output these extractors are using seed as well as the input. This means that the same input won't result in the same output (of course if the seed is the same it will). The seed has to be a random sequence because only then will it provide the desired effect of altering the output in a hard to reverse way. But producing a long random sequence could be a hard task, therefore we want to minimize the length of seed while at same time maximize the possible length of the output.

In our testing we chose and implemented 8 extractor algorithms. The extractors we picked cover a wide range of different properties. We have simple ones, which manipulate the bits with logical operators to produce the output. But we also have more complex algorithms, which use techniques that are widely used in cryptography for example. Now we would like to introduce some of these extractors.

1) The XOR Operator as an Extractor

The XOR logical operator is one of the most used operator in computer science ranging from RAID technology to cryptography but it can also be used as a very simple extractor [24].

The XOR operator can be used effectively to lower the bias of the source but only if the bits are independent. The easiest way to use this extractor is to go over the original output of the generator and use the XOR on the bits in pairs. This means that the new output will have half the length of the original one. We can go further an use the XOR n times always using the new output as the input for the next XOR. Doing so will lower the length of the generated output at the end $1/(n+1)$ times the original.

Although this extractor is very simple, can lower the bias of the source and can be quickly computed, it is not used, because the independency of the output bits cannot be guaranteed every time and it has a heavy effect on the length of the output (therefore the possible bitrate of the generator).

2) The Von Neumann Extractor

The Von Neumann extractor was created by John Von Neumann and it is the first extractor to be created [25]. Because it is the first extractor its main aim is to eliminate the bias of the source (like the XOR).

The operation of the algorithm is very simple, but just like at the XOR it is important that the bits are independent. It takes two bits as input and based on the values of these two it produces one or no bit. If the two bits are equal it discards the two bits. If they different it will give out the first one as the output. For a uniform source the new output will have the quarter of the length of the original.

The Von Neumann extractor has the same problems as the XOR. Although it is easy to use and it can eliminate the bias, it has a heavy toll on the length of the output.

3) Other variants of the Von Neumann extractor

Since the Von Neumann extractor was the first extractor, many have modified its operation. The two main problems the original design had are that it discards to many bits of the original bitstream and only has 2 bit long input. To overcome these issues the iterating [26] and the N bit Von Neuman extractors have been created [27][28].

In the case of the Iterating Von Neumann the original extractor is used as a building block. The discarded bits are reused as new input, but before this they are modified with different operators. For the N bit Von Neumann extractor the original design was extended in such a way that the length of the input can be longer than two bits.

4) H Function

The H function was created by Markus Dichtl [29] and just like the previous algorithms this extractor can also be simply implemented with logical gates, but compared to them it can achieve better result (as we will see in the tests).

It takes 16 bits as an input and gives out 8 bits as output and presumes that the bits are independent. In this area it is similar to the XOR. The algorithm works in the following way: We take the input bits and make two groups. The first is a_1 which is the first 8 bit, the second is a_2 which is the next 8 bit. The output of the algorithm is

$$H(a_1, a_2) = \left(a_1 \text{ XOR rotate\_left}(a_1, 1)\right) \mathit{XOR}\ a_2.$$

Where rotate_left(a_1,1) means rotating the a_1 to the left with 1 step by taking the leftmost bit and putting it in the rightmost position.

Although the H function produces a new sequence with half the length of the original one, it can better reduce the bias compared to the XOR operator. It can be implemented simply with logic gates and it is very efficient to use.

5) Hash Function As Extractors

Hash functions were not designed with the intent to be used as extractors but today they can be used as extractor algorithms for example during key derivation in cryptography [30].

A deterministic function which takes an m bit length input and gives out an n bit length output have to have specific properties to be called a hash function. These include collision resistance, the avalanche effect, one-way property etc. The properties of a hash function make it a good choice for extraction. The output values are uniformly distributed and one bit difference between two inputs result in a bigger difference between the outputs. Other than that the length of the output can be the same as the input therefore the bitrate of the generator does not change. The physical implementation of a hash function can be achieved with good efficiency because there are specific hardware components which are designed for the fast computation of specific hash functions.

One of these hash functions is the Toeplitz hashing [31], where a Toeplitz matrix is used during extraction where the input bits (divided into smaller groups) as a vector is multiplied with this matrix.

6) Using S-boxes as extractors

Substitution boxes (S-boxes) are mostly used in symmetric key encryption algorithms. For example they are used in the Data Encryption Standard (DES) [32]. They take an *m* long bits of input and give out bits of *n* length, substituting the input for the output. As their main goal in encryption systems is to increase confusion, they can be used as extractors [33].

III. TESTING THE GENERATORS AND THE EXTRACTORS

Our main objective during the testing was to find out how can the different extractors improve the quality of the original outputs from the generator. During the testing of the two generators we firstly implemented the extractors we previously introduced. For running the test we used the Dieharder test suite which we introduced in the previous chapter. This test suite has a command line program which can be used on Linux based operating systems and provides a variety of possible arguments which can be given to the test [34].

In the implementation phase we decided that for the N bit Von Neumann extractor we will implement the N=4 case and for the iterative Von Neuman extractor we use 2 iteration. For the extractor which uses the Toeplitz matrix we generated Toeplitz matrix with the help of a PRNG. For the S-boxes we used the one which can be found in DES. For the hash function we chose the SHA-256.

After we implemented the extractors we had to choose the tests we wanted to run. We chose 19 test from the Dieharder test suite from which 16 was part of the Dierharder and 3 was part of the NIST STS. We only chose this subset of the Dierharder tests, because the generators were already tested with the NIST STS in previously published paper [21] and our main goal was to demonstrate the effect of the extractors on the original output. Therefore the results we will be presenting in the following subsections cannot be taken as a thorough statistical test of the generators.

After we chose the tests we set up the testing environment. We gathered data from the two generators. In case of the generator which is based on the arrival times of photons the size of the data was bigger. After this we ran the tests on the original output as well as the new ones which were produced by the 8 implemented extractor. We summarized the result in tables. In the rows we can see the tests, in the columns we can see the name of the tested outputs. If the generator PASSED the given test we can see the p-value it has achieved, if it failed it we can see an “F”.

A. Testing the ASE generator

The first generator we tested was the ASE generator. First of all we have to note that during the creation of the original output we deliberately introduced oversampling into the creation process. This resulted in a higher bitrate, but as we will see it heavily effected the quality of the numbers.

Table 1 shows the results of the original output as well as 4 simple extractors. We can see the effect of the oversampling. The original output could only pass 1 test out of 19. The simple extractors could slightly improve the quality, only 1 or 2 more tests were successful with their help. This correlates with the previously mentioned information about these extractors.

Table 2 shows the results of the 4 more complex extractors. As we can see they performed much better compared to the previous ones. The *H* function performed really good considering it is simple construction and the hash function could almost eliminate all the failed tests. During the testing of this generator, we found that if there is a problem in the creation process (here, for example oversampling) with the help of extractors we cannot eliminate it perfectly, but we can mitigate the effect it has on the quality of the numbers. This is important, because there could be an underlying system which uses the number created by the generator and it requires a high bitrate. If we can only provide the desired bitrate with oversampling then the extractors could help us meet some of the quality requirements.

B. Testing The Generator Based On The Arrival Times Of Photons

The second generator we tested was the one which is based on the arrival times of photons.

Table 3 shows the results of the original and the 4 simple extractors. We can see that the original output achieved a good result, only 2 out 19 tests failed. The explanation for the 2 failed test is the minimal inaccuracy of the hardware components in the generator (for example the photon sensor). The extractors couldn’t improve the quality of the output to a perfect case but the XOR for example only failed 1 test. Table 4 shows the results for the second group of extractors. As we can see they performed better. The *H* function and the hash function were able to achieve a perfect result, eliminating the 2 failed test in the original one. The other 2 extractor achieved good results as well. We can conclude from the testing of this generator that with the help of extractors we can eliminate the negative effects the physical implementation introduces to the system.

IV. CONCLUSION

In our paper we presented the concept of QRNGs and also briefly presented two of techniques which are used in these generators during the creation of the numbers. We introduced selected tests which can be used to determine the quality of the generated numbers on a probabilistic basis. After this we presented the idea of extractors and showed where they fit into in the lifecycle of the generator.

We have presented 8 extractors, together with their operation and listed some of their strengths and weaknesses. In the last part of our paper we concentrated on these 8 extractors and their effect on the quality of the outputs produced by two QRNGs. We ran several statistical tests to determine how the extractors effect the properties of the numbers and presented the outcome of these tests on both generators. After we performed the tests we concluded that post-processing can be utilized to enhance the output of the generators, but we have to select the right extractors as not all of them can perform equally. While there are ones which can greatly increase the number of passed tests, they can also decrease the possible output speed of the generator. Another important property we found was that in case of a miscalibration during the generation process inside the generator the extractors can to a certain degree mitigate the negative effects. The chosen tests do not cover all the aspects which are needed for a deep statistical testing of the complete post-processing with these extractors, therefore as a future improvement it can be studied.

TABLE I
THE RESULTS FOR THE GENERATOR BASED ON AMPLIFIED SPONTANEOUS EMISSION PART 1.

Name of the test	**H function**	**S-box**	**Toeplitz-matrix**	**SHA256**
diehard_birthdays	0.946	0.136	F	F
diehard_operm	50.187	0.359	F	0.414
diehard_rank_32x32	0.467	0.101	F	0.861
diehard_rank_6x8	0.419	F	F	0.497
diehard_bitstream	F	F	F	0.822
diehard_opso	F	F	F	0.231
diehard_oqso	0.010	F	F	F
diehard_dna	0.035	F	F	0.382
diehard_count_1s_str	F	F	F	0.361
diehard_count_1s_byt	0.196	F	F	0.406
diehard_parking_lot	0.061	F	F	0.011
diehard_2dsphere	0.872	F	F	0.564
diehard_3dsphere	0.844	0.097	F	0.823
diehard_squeeze	F	F	F	0.954
diehard_runs	F	0.475	0.522	0.198
diehard_craps	F	F	F	F
sts_monobit	F	F	F	0.062
sts_runs	F	F	F	0.322
sts_serial	F	F	F	0.563

TABLE II
THE RESULTS FOR THE GENERATOR BASED ON AMPLIFIED SPONTANEOUS EMISSION PART 2.

Name of the test	Original	XOR	Von Neumann	Iterating Von Neumann	4 bit Von Neumann
diehard_birthdays	F	F	F	F	F
diehard_operm5	F	0.080	F	F	0.078
diehard_rank_32x32	0.565	0.042	0.036	0.479	0.215
diehard_rank_6x8	F	F	F	F	F
diehard_bitstream	F	F	F	F	F
diehard_opso	F	F	F	F	F
diehard_oqso	F	F	F	F	F
diehard_dna	F	F	F	F	F
diehard_count_1s_str	F	F	F	F	F
diehard_count_1s_byt	F	F	F	F	F
diehard_parking_lot	F	F	F	F	F
diehard_2dsphere	F	F	F	F	F
diehard_3dsphere	F	F	F	F	F
diehard_squeeze	F	F	F	F	F
diehard_runs	F	0.631	0.767	0.363	0.617
diehard_craps	F	F	F	F	F
sts_monobit	F	F	F	F	F
sts_runs	F	F	F	F	F
sts_serial	F	F	F	F	F

TABLE III
THE RESULTS FOR THE GENERATOR BASED ON THE ARRIVAL TIMES OF PHOTONS PART 1.

Name of the test	Original	XOR	Von Neumann	Iterating Von Neumann	4 bit Von Neumann
diehard_birthdays	0.564	0.810	0.536	0.100	0.853
diehard_operm5	0.952	0.163	0.066	0.463	0.360
diehard_rank_32x32	0.313	0.948	0.576	0.327	0.917
diehard_rank_6x8	0.121	0.817	0.606	0.884	F
diehard_bitstream	0.305	0.121	0.524	0.297	F
diehard_opso	F	0.448	0.227	0.068	F
diehard_oqso	0.927	0.691	0.987	0.134	F
diehard_dna	0.549	0.602	0.972	0.533	F
diehard_count_1s_str	0.927	0.976	0.935	0.540	F
diehard_count_1s_byt	0.941	0.875	0.674	0.821	F
diehard_parking_lot	0.863	0.100	0.273	0.012	F
diehard_2dsphere	0.576	0.336	0.754	F	F
diehard_3dsphere	0.574	0.982	0.575	0.031	0.246
diehard_squeeze	0.114	0.498	0.043	0.013	F
diehard_runs	0.176	0.805	0.684	0.284	0.419
diehard_craps	0.307	0.711	F	0.737	F
sts_monobit	0.360	F	0.762	0.249	F
sts_runs	F	0.892	F	F	F
sts_serial	0.570	0.459	0.548	0.453	F

TABLE IV
THE RESULTS FOR THE GENERATOR BASED ON THE ARRIVAL TIMES OF PHOTONS PART 2

Name of the test	H function	S-box	Toeplitz-matrix	SHA256
diehard_birthdays	0.307	0.732	0.991	0.065
diehard_operm5	0.359	0.912	0.336	0.241
diehard_rank_32x32	0.243	0.383	0.313	0.007
diehard_rank_6x8	0.304	F	0.121	0.438
diehard_bitstream	0.115	F	0.145	0.120
diehard_opso	0.880	F	0.219	0.354
diehard_oqso	0.858	F	0.524	0.412
diehard_dna	0.482	0.351	0.368	0.734
diehard_count_1s_str	0.575	F	0.280	0.578
diehard_count_1s_byt	0.037	F	0.520	0.280
diehard_parking_lot	0.547	0.109	0.576	0.818
diehard_2dsphere	0.784	0.126	0.304	0.792
diehard_3dsphere	0.877	0.524	0.565	0.501
diehard_squeeze	0.905	F	0.348	0.274
diehard_runs	0.780	0.555	0.463	0.518
diehard_craps	0.644	0.392	0.733	0.384
sts_monobit	0.898	0.041	0.403	0.989
sts_runs	0.632	F	F	0.520
sts_serial	0.576	F	0.468	0.565

REFERENCES

[1] Sara El Gaily, Sándor Imre, “Quantum Optimization of Resource Distribution Management for Multi-Task, Multi-Subtasks”, Infocommunications Journal, Vol. XI, No 4, December 2019, pp. 47-53. DOI: 10.36244/ICJ.2019.4.7

[2] Sandor Imre, Laszlo Gyongyosi. “Advanced quantum communications: an engineering approach”, Wiley, 2012, ISBN: 978-1-118-00236-0, DOI: 10.1002/9781118337462

[3] Laszlo Gyongyosi, Sandor Imre, Hung Viet Nguyen: “A Survey on Quantum Channel Capacities”, IEEE [11] Communications Surveys and Tutorials, IEEE, DOI: 10.1109/COMST.2017.2786748, 2018.

[4] Laszlo Gyongyosi, Laszlo Bacsardi and Sandor Imre, “A Survey on Quantum Key Distribution”, Infocommunications Journal, Vol. XI, No 2, June 2019, pp. 14-21. DOI: 10.36244/ICJ.2019.2.2

[5] Mario Stipcevic, “Quantum random number generators and their applications in cryptography”, Proc. SPIE 8375, Advanced Photon Counting Techniques VI, 837504 (2012); DOI: 10.1117/12.919920

[6] Herrero-Collantes, Miguel, and Juan Carlos Garcia- Escartin, “Quantum random number generators.” Reviews of Modern Physics 89.1 (2017), DOI: 10.1103/revmodphys.89.015004

[7] Ma, Xiongfeng, et al. “Post-processing for quantum random-number generators: Entropy evaluation and randomness extraction.” Physical Review A 87.6 (2013), DOI: 10.1103/physreva.87.062327.

[8] Qi, Bing. "True randomness from an incoherent source." Review of Scientific Instruments 88.11 (2017), DOI: 10.1063/1.4986048

[9] Zhang, Xiao-Guang, et al. "Note: Fully integrated 3.2 Gbps quantum random number generator with real-time extraction." Review of Scientific Instruments 87.7 (2016), DOI: 10.1063/1.4958663

[10] Shakhovoy, Roman, et al. "Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator." Optics express 28.5 (2020), DOI: 10.1364/oe.380156

[11] Martínez, Aldo C., et al. "Advanced statistical testing of quantum random number generators." Entropy 20.11 (2018), DOI: 10.3390/e20110886

[12] Kelsey, John, et al. “Cryptanalytic attacks on pseudorandom number generators.” International workshop on fast software encryption. Springer, Berlin, Heidelberg, (1998) DOI: 10.1007/3-540-69710-1_12

[13] Gras, Gaëtan, et al. “Quantum entropy model of an integrated QRNG chip.” (2020) arXiv preprint arXiv:2011.14129

[14] Michael A. Wayne, Evan R. Jeffrey, Gleb M. Akselrod and Paul G. Kwiat: “Photon arrival time quantum random number generation”, Journal of Modern Optics Vol. 56, No. 4, 20 February 2009, 516–522, DOI: 10.1080/09500340802553244

[15] Jie Yang, Fan Fan, Jinlu Liu, Qi Su, Yang Li, Wei Huang, and Bingjie Xu, “Randomness Quantification for Quantum Random Number Generation Based on Detection of Amplified Spontaneous Emission Noise” Quantum Science and Technology, Vol. VI, No. 1, 2020, DOI: 10.1088/2058-9565/abbd80

[16] Ádám Marosits, Ágoston Schranz and Eszter Udvary, “Amplified spontaneous emission based quantum random number generator”, Infocommunications Journal, Vol. XII, No 2, July 2020, pp. 12-17. DOI: 10.36244/ICJ.2020.2.2

[17] “NIST SP 800-22: Documentation and Software” https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software, (Last visit: 23 Feb 2021).

[18] G. Marsaglia, “The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness”. Florida State University. 1995. archived on 2016-01-25.” https://web.archive.org/web/20160125103112/http:/stat.fsu.edu/pub/diehard/.sdfsdf

[19] Robert G. Brown. “Robert G. Brown's General Tools Page”, https://webhome.phy.duke.edu/~rgb/General/dieharder.php, (Last visit: 23 Feb 2021.)

[20] NIST/SEMATECH e-Handbook of Statistical Methods, “Chi-Square Goodness-of-Fit Test” https://itl.nist.gov/div898/handbook/eda/section3/eda35f.htm (Last visit: 14 May 2021)

[21] Balazs Solymos, Laszlo Bacsardi, “Real-time Processing System for a Quantum Random Number Generator”, Infocommunications Journal, Vol. XII, No 1, March 2020, pp. 53-59. DOI: 10.36244/ICJ.2020.1.8

[22] “SP 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation,” https://csrc.nist.gov/publications/detail/sp/800-90b/final, (Last visit: 23 Feb 2021)

[23] Salil P. Vadhan, “Pseudorandomness”, Foundations and Trends in Theoretical Computer Science: Vol. 7: No. 1–3, 2012, pp. 1-336.

[24] R. B. Davies, “Exclusive OR (XOR) and hardware random number generators”, Tech. Rep., 2002. [Online], Available: http://www.robertnz.net/pdf/xor2.pdf (Last visit: 23 Feb 2021)

[25] John Von Neumann, “Various techniques used in connection with random digits”, National Bureau of Standards Applied Math Series 12, pp. 36–38., 1951

[26] Y. Peres, “Iterating Von Neumann’s Procedure for Extracting Random Bits”, Ann. Statist., pp. 590–597., 1992, DOI: 10.1214/aos/1176348543

[27] P. Elias, “The efficient construction of an unbiased random sequence” Ann. Math.Statist., pp. 865–870., 1972, DOI: 10.1214/aoms/1177692552

[28] Ruilin Zhang, Sijia Chen, Chao Wan, Hirofumi Shinohara, “High-Throughput Von Neumann Post- Processing for Random Number Generator”, 201850 International Symposium on VLSI Design Automation and Test (VLSI-DAT), pp.1-4, 2018, DOI: 10.1109/vlsi-dat.2018.8373253

[29] Markus Dichtl, “Bad and Good Ways of Post-Processing Biased Physical Random Numbers” 14th International Workshop, FSE2007, Luxembourg, Luxembourg, March 26-28, 2007, DOI: 10.1007/978-3-540-74619-5_9

[30] Wegman, Mark N., and J. Lawrence Carter, “New hash functions and their use in authentication and set equality.” Journal of computer and system sciences 22.3 (1981): 265-279., DOI: 10.1016/0022-0000(81)90033-7

[31] Krawczyk H., “New Hash Functions for Message Authentication.”, Advances in Cryptology, EUROCRYPT (1995) Lecture Notes in Computer Science, vol 921. Springer, Berlin, Heidelberg. DOI: 10.1007/3-540-49264-X_24

[32] “Data Encryption Standard (DES)” https://csrc.nist.gov/publications/detail/fips/46/3/archive/1999-10-25 (Last visit: 23 Feb 2021)

[33] AVAROĞLU, ERDİNÇ, and Taner Tuncer. “A novel S-box-based post-processing method for true random number generation.” Turkish Journal of Electrical Engineering & Computer Sciences 28.1 (2020): 288- 301., DOI: 10.3906/elk-1906-194

[34] “dieharder - Linux man page” https://linux.die.net/man/1/dieharder (Last visit: 23 Feb 2021)

Botond L. Márton received his B.Sc. degree in computer engineering from Budapest University of Technology and Economics (BME) in early 2021. He is currently pursuing his M.Sc. at BME. Currently he is involved in a quantum key distribution project at the university. His research interests are quantum computing and quantum communications.

Dóra Istenes received her B.Sc. degree in the beginning of 2021 in Computer Science Engineering from the Budapest University of Technology and Economics (BME). She started her M.Sc. studies at BME in the same year. Her current research interests are quantum computing and communications.

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 corresponding 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 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.

Effects of selected noises on the quantum memory of satellite based quantum repeaters

András Mihály and László Bacsárdi, *Member, IEEE*

***Abstract*— Quantum repeaters are a key part of long-range free-space quantum key distribution. They allow us to circumvent the negative effects of the no-cloning theorem. Quantum repeaters are also a key point in point-to-point communication since otherwise, a direct line of sight would be necessary. In our simulation, we examined the QKD capabilities of quantum repeaters in a satellite-based network, along with selected types of noises.**

***Index Terms*—QKD, Quantum memory, amplitude damping, dephasing noise, depolarizing noise, quantum communications**

I. INTRODUCTION

RSA-based public-key cryptography is a part of our everyday life. It's used by banks, websites, and every other entity that wants to ensure its communications are secure on the web. But with the advancement of quantum computers and thanks to Shor's algorithm [1], the time when public-key-based encryptions will be broken is at our doorstep. By utilizing quantum computing, we can not only break today's most used encryptions, but we can also speed up the problem-solving for various problems. Using Groover's algorithm, we can find a record in unordered data in $\sqrt{N}$ time [2], or even extreme values [3]. By utilizing quantum computing we can solve problems like multi-user detection [3] or optimal resource distribution [4]. Quantum key distribution (QKD) is a subpart of quantum communication that can not only alleviate these problems thanks to the symmetric key-based encryption it's enabling, but (if used right) is virtually unbreakable. One problem with QKD using systems is the no-cloning theorem, which entails that we cannot copy a quantum bit.

This problem can be mitigated with the use of entanglement swapping quantum repeaters. To perform this task, we use the side effect of the Bell state measurement (BSM), which we detail later in the paper in section IV. But for these operations, quantum repeaters use two critical elements: quantum logic gates and quantum memories. Which are both affected by various noises.

Today's research is mostly connected to quantum satellites that use only one in their simulation, for example, the Chinese Micius [5], the Canadian QEYSSat [6], or the European QKDSat [7]. In our research, we simulated not a single satellite but a network of quantum satellites.

In our simulation of satellite networks composed of multiple quantum repeaters, the repeaters were simulated with varying amplitude damping, depolarizing, and dephasing noises affecting quantum memory. Our goal was to identify which noise types could be the most damping for a future quantum satellite network. So that we know what types of noise reductions are crucial for quantum memories. We also simulated multiple network setups, from real-world point-to-point (eg. Budapest-Moscow) to varying node-to-node distance and node cardinality.

The structure of the paper is as follows: in Section II. we detail the current state of quantum key distribution. After that, we present the available selection of quantum network simulators. In Section IV. we discuss the use of satellite-based quantum repeaters and their edge over fiber-based networks. Then, we present our simulation and its architecture on the module level. In Section VI, we present our findings on the effects of various noise on the error rate.

II. QUANTUM KEY DISTRIBUTION TODAY

QKD despite, being a relatively new technology, already has multiple uses. One of the most important applications of quantum technology is quantum cryptography. Using quantum key distribution protocols like BB84 [8] or E91 [9], we can create secure sources of communication with the combination of one-time padding and symmetric-key encryption.

Quantum protocols are versatile, for example we can take the aforementioned protocols E91 and BB84. While the protocol developed by Charles and Gilles in 84 (hence the name) uses the quantum randomness of the photon polarization for its algorithm. On the other hand, in the development of the E91 QKD protocol Artur used quantum entanglement as means to generate secure key bits. There are also variations of protocols, for example, SARG04 [10] is derived from the BB84 QKD protocol but made for weak laser pulses instead of single photons. Today when we are talking about quantum-key distribution medium, we can consider two different platforms for quantum key distribution medium.

Fiber-based QKD: using fiber, we have a controllable medium at the cost of forcing the network to only used the established links. To date, there have been multiple experiments utilizing fiber-based QKD. To name a few: the first quantum key distribution over 48 km distance in Los Alamos [11] or the first quantum key distribution using a commercial fiber network in china [12].

Free-Space QKD: using free-space communicational channel (either terrestrial or satellite-based), we gain the ability

The authors are with the Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, H-1117, Hungary.
E-mail: andras.mihaly.1998@gmail.com, bacsardi@hit.bme.hu.

This research was supported by the Ministry of Innovation and Technology and the National Research, Development and Innovation Office within the Quantum Information National Laboratory of Hungary. L. Bacsárdi thanks the support of the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

DOI: 10.36244/ICJ.2021.2.3

to change established links and gain even lower the error rate originating from the medium by using satellites to relay our quantum bits. Until nowadays, there have been multiple experiments regarding the use of satellites in quantum key distribution. The first satellite-relayed intercontinental quantum network between Viena and Beijing [13], and the first entanglement-based quantum key distribution using a satellite at the altitude of 1,200 km [14], are one of these.

With the evolution of quantum satellites and communication, the dependency on different types of optical communications became to play an important role in free-space and satellite communications [15] [16] .

A detailed explanation of QKD is out of scope for this paper, but an in-depth survey can be found in [17].

III. Quantum Satellite Networks

As shown in Section II, using fiber as our primary medium for QKD can lower the number of possible connections. Using satellite-based quantum repeater networks has multiple advantages over the aforementioned fiber-based counterpart. Using a single satellite can already increase our coverage area depending on the elevation of the said satellite. The only negative drawback is the increase in latency since no information can travel faster than light. To negate this, we used an array of satellites at lower (500 km) altitudes. But since we are using a multitude of quantum repeaters, the errors that arose from different noises can increase along with the increased number of nodes or increased distance.

It is important to note that in this paper we don't use the error rate generated by the different types of aerial turbulences. A paper detailing the various effects of atmospheric turbulence and earth-satellite degree can be found in [18].

In our simulation, for the satellite positions, we used the data gathered from the Starlink satellite network. The use of Starlink satellites was self-evident since they mostly operate in low earth orbits and are working in large groups for increased coverage.

A quantum satellite repeater network would not only allow secure point-to-point communication, but they also would be able to create a secure network for communication, that uses QKD for encryption. In this paper, we analyze the effects of 3 types of noises (dephasing, depolarizing, and amplitude damping) on the quantum memory of quantum repeaters. Using various simulations, we simulated networks along with various noise rate combinations and routes, with differing node-to-node distance and node cardinality.

IV. Quantum simulators

In our research, we tried multiple quantum network simulators before ending up with NetSquid. The three main simulators that we tried are Simulaqron [19], Squanch [20] and Netsquid [21].

Simulaqron is developed by QuTech and provides an application-level simulation of quantum networks. Since our simulation needed low-level simulation capabilities, we did not choose this one.

Squanch although provides an almost hardware-level simulation, didn't have the capability to also work on a higher level as Netsquid.

Finally, our search stopped with Netsquid which is also being developed at QuTech and provided us with all the needed features, from programable quantum processors to massive networks with multiple nodes.

V. Our setup

A. Overview of our simulator

The simulator uses the Netsquid framework and the quantum repeater example as a base. The simulator can be divided into four sub-modules as it is illustrated in Fig 1

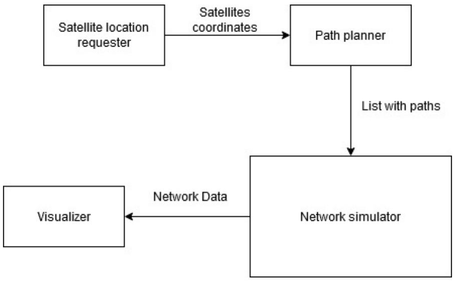


Figure 1. The architecture of the simulator

Satellite location requester: using N2YO.com's API [22], this module requests the location of all STARLINK satellites for the next N seconds ($N < 300$)

Path planner: using Dijkstra's algorithm, the module calculates the optimal route between two terrestrial nodes.

Network simulator: simulates the quantum entanglement exchange beside varying noises.

Visualizer: using the output data from the network simulator module, depicts the change in quantum bit error rate (QBER). The node architecture setup follows the Fig. 1. A quantum source supplies entangled quantum bits to the local and next-in-line node's quantum processor. Using that, the quantum processor executes the Bell state measurement swapping the entanglement between quantum bits. The simulator runs multiple times with varying levels of amplitude damping, dephasing, and depolarizing noise. The chance to depolarize calculated using the following formula:

$$P_{depolarization} = 1 - exp(-\text{delay[ns]} * \text{depolarization rate [Hz]} * 10^{-9}) \tag{1}$$

For dephasing, the chance to occur is is calculated with the following formula:

$$P_{dephasing} = 1 - exp(\text{-delay[ns]} * \text{dephasing rate [Hz]} * 10^{-9}) \tag{2}$$

In the case of amplitude damping, instead of probability, the formula gives us the damping parameter γ.

$$\gamma = 1 - exp(\text{-delay[ns]} \ * \ \text{amplitude damping} \ * 10^{-9}) \tag{3}$$

γ is used in the following quantum operation:

$$e(p) = \sum_i E_i p E^\dagger \tag{4}$$

Where E_i is substituted with the corresponding matrix from the equations found in 5, 6, 7 and 8

$$E_0 = \sqrt{p}\begin{bmatrix}1 & 0\\ 0 & \sqrt{1-\gamma}\end{bmatrix} \tag{5}$$

$$E_1 = \sqrt{p}\begin{bmatrix}0 & \sqrt{\gamma}\\ 0 & 0\end{bmatrix} \tag{6}$$

$$E_2 = \sqrt{1-p}\begin{bmatrix}\sqrt{1-\gamma} & 0\\ 0 & 1\end{bmatrix} \tag{7}$$

$$E_3 = \sqrt{1-p}\begin{bmatrix}0 & 0\\ \sqrt{\gamma} & 0\end{bmatrix} \tag{8}$$

B. Overview of our topology

In our simulation, the topology we used was a linear one. As seen in Figure 2, the nodes have two crucial elements:

The quantum CPU is responsible for the execution of BSM on the qubits got from the two inputs (Quantum input 0, Quantum Input 1). The quantum source function is the generation of entangled quantum bits, one for the local quantum CPU and the other for the next node.

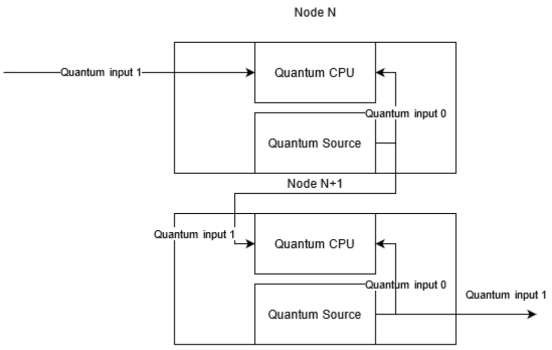


Figure 2. The simulated topology

C. Quantum repeater composition

Quantum repeaters [23] are the key to quantum communication over long distances. The repeaters utilize the consequence of Bell state measurement, which is swapping entanglements. For instance, we have two entangled quantum bit pairs, namely $Q_{11} - Q_{12}$ and $Q_{21} - Q_{22}$. After applying BSM on Q_{11} and Q_{22}, we get two new entangled pairs: $Q_{11} - Q_{22}$ and $Q_{12} - Q_{21}$, as observed, a quantum entanglement generates between $Q_{12} - Q_{21}$ without the need for physical contact. With BSM, we can generate entangled quantum bits over large distances[23]. In our simulation, we generated entanglement between two terrestrial nodes by using quantum repeaters mounted on satellites. For the quantum entanglement swapping, we also require quantum memory, in this paper, we focused on how various quantum memory noises affect the quantum bit error rate.

VI. Results

In our paper, we made three types of simulations:

Budapest-Moscow: the simulation was made with real data from satellites over the region, simulating a network of quantum repeaters.

Iterative increase of the distance: this simulation was made specifically to examine the effects of increasing distances on QBER.

Iterative increase of the number of nodes: the simulation was made to test the effects of increasing the number of nodes on QBER.

A. Budapest-Moscow trajectory

The simulation produced interesting results: the different types of noises yielded different values of QBER with the same distance. To validate these claims, we created the other two simulation variants.

As in the next section, we can see. The increase in the distance affected the QBER differently depending on the type of noise. For example, in the case of depolarizing noise, the error rate stayed well under 0.5 for most of the simulations.

B. Iterative increase of distance

In this simulation, we examined the effects of distance increases on the QBER for the sake of the experiment the number of nodes stayed at a constant value of 5. As expected and seen in Fig. 3, 4, and 5 the error rate increased along with the distances. At the maximum distance of 12200 km, almost all noise rates produced a QBER of 0.5, with the sharpest increase along the dephasing rate. The first time each noise combination reached the QBER value of 0.5 is visible in the aforementioned figures. The distance values for each iteration can be using equation 9:

$$D_i = 2800 + i * 600 \text{ and for every i} \equiv 1 \bmod 4 \rightarrow +200 \tag{9}$$

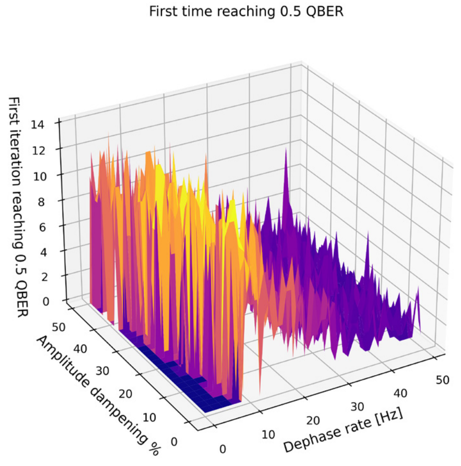


Figure 3. The first iteration of the simulation that reached a QBER of 0.5 with dephasing and amplitude damping noises. The exact distance can be calculated by using the equation 9.

The figure 3 details the first time an iteration reached the error rate of 0.5 for each noise combination. On the Z-axis, we can see the iteration on a scale from 0 to 14, and on the X and Y axes, we can see the error rates. As previously mentioned, and seen in figure 3, in the case of distance, the most crucial element is the dephasing noise, which reached the QBER of 0.5 as soon as the second iteration.

C. *Iterative increase of the number of nodes*

In the case of iterative node volume increase, we can see that in the case of this simulation, had a similar effect on the QBER as the iterative increase in distance, which we can see in Fig. 6, 7, and 8. The slight variation that we can observe on the figures is thanks to the variability of the simulator. The number of hops for each iteration is available in Table I. Looking at the aforementioned figures, we can discover the same pattern as in the one with an iterative increase in distances.

Table I
TABLE CONTAINING THE NUMBER OF HOPS FOR EACH ITERATION OF THE SIMULATOR

Iteration:	0	1	2	3	4	5	6	7	8
Hops:	5	6	7	7	8	9	9	10	11
Iteration:	9	10	11	12	13	14			
Hops:	11	12	13	13	14	15			

VII. Conclusion

In this paper, we presented the effects of various noises on the quantum memory of quantum repeaters and their impacts on the quantum bit error rate. We could see that from the amplitude damping, dephasing, and depolarizing trio, the most susceptible to the increase due to distance and node number was the dephasing noise (as seen in Sections VI. B. and VI. C). In the end, we can conclude that for future satellite networks, one of the most crucial noises is the quantum dephasing noise, and in the future, we should prioritize minimizing it.

In this paper, we only examined one element of the quantum repeaters with one type of error model. In the future, we would like to rerun the simulation with different error models to test the correlation between the iterative distance and node number increases mentioned before in Section V. C.

Another angle for future research is to introduce new variables in our simulation. The two models we would like to use to expand our simulation are aerial turbulences and quantum gates.

Appendix
A. Figures

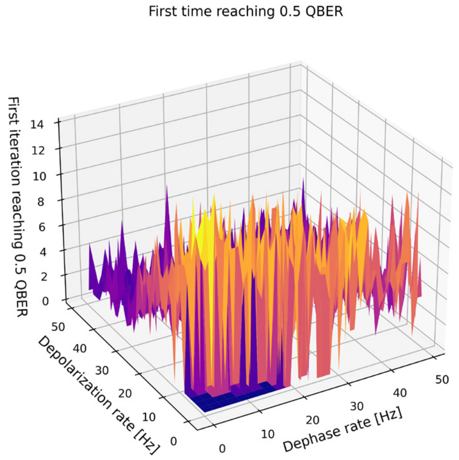


Figure 4. The first iteration of the simulation that reached a QBER of 0.5 with dephasing and depolarizing noises. The exact distance can be calculated by using the equation 9.

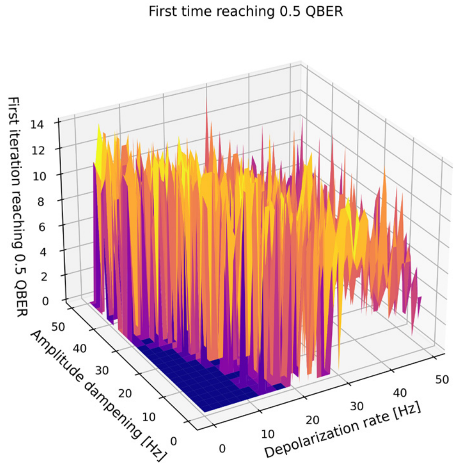


Figure 5. The first iteration of the simulation that reached a QBER of 0.5 with depolarizing and amplitude damping noises.The exact distance can be calculated by using the equation 9.

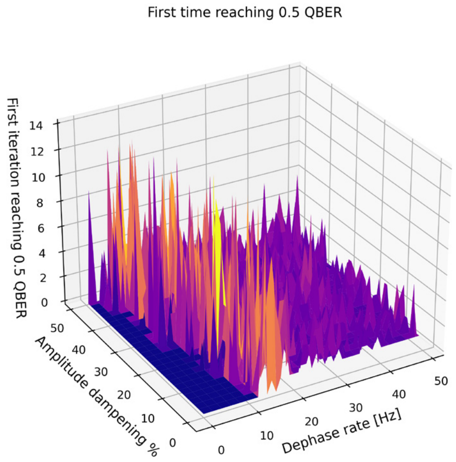


Figure 6. The first iteration of the simulation that reached a QBER of 0.5 with dephasing and amplitude damping noises. With varying hops and a constant distance of 6200. The number of hops can be seen in the table I.

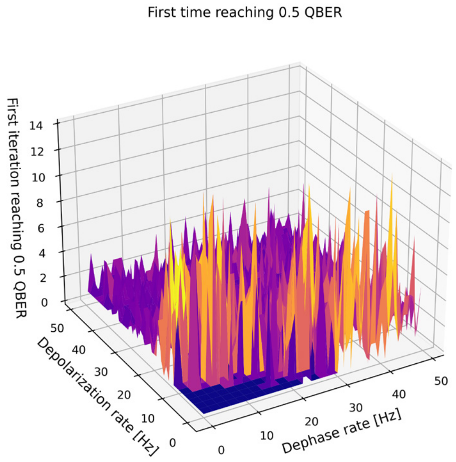


Figure 7. The first iteration of the simulation that reached a QBER of 0.5 with dephasing and depolarizing noises. With varying hops and a constant distance of 6200. The number of hops can be seen in the table I.

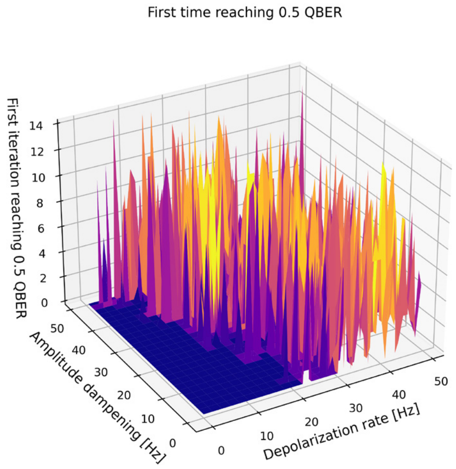


Figure 8. The first iteration of the simulation that reached a QBER of 0.5 with depolarizing and amplitude damping noises. With varying hops and a constant distance of 6200. The number of hops can be seen in the table I.

Acknowledgement

L. Bacsárdi thanks the support of the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

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 Schrödinger’s equation to the quantum 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 Application 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] Shengkai Liao et al. “Satellite-Relayed Intercontinental Quantum Network.” In: *Physical review letters* 120 3 (2018), p. 030501. doi: 10.1103/PhysRevLett.120.030501.

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

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

[8] Charles H. Bennett and Gilles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *Theoretical Computer Science 560* (Dec. 2014), pp. 7–11. ISSN: 0304-3975. doi: 10.1016/j.tcs.2014.05.025.

[9] Artur Ekert. “Ekert, A. K.: Quantum Cryptography Based on Bell’s Theorem. Phys. Rev. Lett. 67(6), 661”. In: *Physical review letters* 67 (Sept. 1991), pp. 661–663. doi: 10.1103/PhysRevLett.67.661.

[10] Cyril Branciard et al. “Security of two quantum cryptography protocols using the same four qubit states”. In: *Phys. Rev. A* 72 (3 Sept. 2005), p. 032301. doi: 10.1103/PhysRevA.72.032301.

[11] Richard J. Hughes, George L. Morgan, and C. Glen Peterson. “Quantum key distribution over a 48 km optical fibre network”. In: *Journal of Modern Optics* 47.2-3 (2000), pp. 533–547. doi: 10.1080/09500340008244058.

[12] Yichen Zhang et al. “Continuous-variable QKD over 50 km commercial fiber”. In: *Quantum Science and Technology* 4.3 (May 2019), p. 035006. doi: 10.1088/2058-9565/ab19d1.

[13] C. S. N. Koushik et al. “A Literature Review on Quantum Experiments at Space Scale—QUESS Satellite”. In: *Innovations in Electronics and Communication Engineering*. Ed. by H. S. Saini et al. Singapore: Springer Singapore, 2020, pp. 13–25. doi: 10.1007/978-981-15-3172-9_2.

[14] Juan Yin et al. “Entanglement-based secure quantum cryptography over 1,120 kilometres”. In: *Nature* 582 (June 2020), pp. 1–5. doi: 10.1038/s41586-020-2401-y.

[15] Andrea Farkasvolgyi and Istvan Frigyes. “Optical transfer in space communication”. In: *Infocommunications Journal* 10 (Sept. 2018), pp. 9–13. doi: 10.36244/ICJ.2018.3.2.

[16] Eszter Udvary. “Visible Light Communication Survey”. In: *Infocommunications journal* (Jan. 2019), pp. 22–31. doi: 10.36244/ICJ.2019.2.3.

[17] Laszlo Gyongyosi, Laszlo Bacsardi, and Sandor Imre. “A Survey on Quantum Key Distribution”. In: *Infocommunications journal* (Jan. 2019), pp. 14–21. doi: 10.36244/ICJ.2019.2.2.

[18] Mate Galambos and Laszlo Bacsardi. “Comparing Calculated and Measured Losses in a Satellite-Earth Quantum Channel”. In: *Infocommunications Journal* 10 (Sept. 2018), pp. 14–19. doi: 10.36244/ICJ.2018.3.3.

[19] A. Dahlberg and S. Wehner. “SimulaQron - A simulator for developing quantum internet software”. In: *ArXiv/abs/1712.08032* (2017).

[20] Ben Bartlett. “A distributed simulation framework for quantum networks and channels”. In: *arXiv:1808.07047* (2018).

[21] Tim Coopmans et al. “NetSquid, a discrete-event simulation platform for quantum networks”. In: *arXiv* preprint *arXiv:2010.12535* (2020).

[22] *N2YO.com API, N2yo.com, 2021. [Online].*
Available: https://www.n2yo.com/api/. [Accessed: 02-Feb-2021].

[23] Sandor Imre and Laszlo Gyongyosi. *Advanced quantum communications: an engineering approach.* Wiley-Blackwell, 2013.

András Mihály studied at Göllner Mária Regional Waldorf secondary school, received his BSc degree, and started his MSc education in 2021 in Computer Engineering from the Budapest University of Technology and Economics (BME). In 2020 he reached 3rd place in the local Scientific student conference. Currently, he is pursuing research in the quantum field.

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 corresponding 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 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.

An Enhanced Impulsive Noise Suppression Method Based on Wavelet Denoising and ICA for Power Line Communication

Wei Zhang, Zhongqiang Luo, Xingzhong Xiong, and Kai Deng

***Abstract*—Aiming at the problem of noise suppression in power lines, traditional noise suppression methods need to know prior knowledge and other defects. In this paper, blind source separation methods that do not need prior knowledge are selected. In the case of low signal-to-noise ratio, the basic independent component analysis algorithm has poor denoising effect. Therefore, this paper proposes a joint independent component analysis algorithm based on Wavelet denoising and Power independent component analysis (WD-PowerICA). In this work, firstly, the pseudo observation signal is constructed by weighted processing, and the blind separation model of single channel is transformed into a multi-channel determined model. Then, the proposed WD-PowerICA algorithm is used to separate noise and source signals. Finally, the simulation results demonstrate that the proposed algorithm in this paper can effectively separate noise and source signal under low SNR. At the same time, the stronger the α pulse noise is, the closer the WD-PowerICA separated signal is to the source signal. The proposed algorithm is better than the state of the art PowerICA algorithm.**

***Index Terms*—Impulse noise, Blind source separation, Power line communication, Independent component analysis, Orthogonal frequency division multiplexing.**

I. INTRODUCTION

POWER grid is the largest, most popular and most reliable power supply carrier. Power line communication(PLC) technology is a new technology that utilizes widely existing power lines for communication and has received increasing attention [1]. The research on power line carrier communication technology is mainly carried out from three aspects, namely signal attenuation characteristics, impedance characteristics and noise characteristics [2-3]. Among them, noise interference is one of the most important factors affecting the success rate of power line carrier communication. The noise in power line carrier communication is far more complicated than that in other dedicated communication lines. It is found that power line noise can be divided into five types of noise: colored background noise, narrowband noise, periodic impulse noise asynchronous to power frequency, and period synchronized with power frequency, impulse noise and asynchronous impulse noise. Most of the literature classifies the first three as background noise, the latter two being called impulse noise. Impulse noise is the main detrimental cause of affecting communication quality [4]. Therefore, it is necessary to take effective measures to solve impulse noise for power line stable and reliable communication.

So far, scholars around the world have done a lot of research on noise removal of PLC systems based on OFDM signals. In [5-6] provide time-domain elimination methods for impulse noise in PLC, including limiting, zeroing, and a combination of the two. These methods are so simple and can also improve the performance of the system to a certain extent. However, the optimal threshold calculation of these algorithms is very difficult. Therefore, in practice, it is often set by experience, which not only limits the performance of this type of method but also destroys the orthogonality between OFDM subcarriers [7]. To solve the problem of inter-carrier interference caused by blanking, an iterative interference cancellation method is proposed [8], but this method has a slower convergence rate. A method for eliminating impulse noise combined with equalization in the frequency domain is proposed [9], the method reconstructs noise by estimating the time domain position, amplitude and phase of the occurrence of impulse noise, and the implementation process is very complicated. The compressive sensing method needs to meet the following constraints: the number of impulse signals in an OFDM symbol cannot exceed the minimum threshold of the number of Fourier transform points and the number of empty subcarriers [10], due to the random of the impulse noise signal itself, the above constraints limit the use of this method. In [11], based on the sparse Bayesian learning method, according to the decision regression detection, the impulse noise signal is reconstructed and then eliminated. However, when reconstructing the impulse noise signal, it is necessary to know the state information of impulse noise and Gaussian noise, and the calculation complexity is high, which is difficult to deal with in the actual system. In [12], a fractional low order independent component analysis algorithm based on negative entropy is proposed to remove mixed noise. This algorithm can protect the pure signal in the mixed signal, and does not need the characteristic parameter of noise. However, the separation

This work was supported by National Natural Science Foundations of China (No. 61201266), Scientific research projects of Yibin University (No. 2021PY20)

Wei Zhang and Kai Deng are with Yibin University, Yibin 644000, China (Corresponding author: 991728174@qq.com).

Zhongqiang Luo and Xingzhong Xiong are with Artificial Intelligence Key Laboratory of Sichuan Province, Sichuan University of Science and Engineering, Yibin 644000, China.

DOI: 10.36244/ICJ.2021.2.4

effect of this algorithm is terrible, and it is not good at low signal-to-noise ratio(SNR).

Through the research analysis of previous scholars, we know that some existing methods have certain limitations. Due to the complexity and variability of power channels, the advanced algorithm of blind source separation, i.e. power iterative independent component analysis algorithm(PowerICA), is still selected in this project, which can achieve fast and stable separation of mixed signals [13]. But this algorithm is not ideal at low SNR. Therefore, this study combines wavelet denoising and power iterative independent component analysis algorithm to denoise (WD-PowerICA). The simulation results show that the de-noising effect is very good. At the same time, it makes up for the disadvantage of power iteration algorithm in low SNR denoising performance, so that we can receive the required signals stably and reliably.

The rest of the paper is structured as follows: In section II, we construct the model of the PLC system and the model of signal as well as problem formulation; In section III, the basic principles of FastICA, PowerICA, WD-PowerICA are illustrated; The simulation results and brief analysis are presented in Section IV; Section V summarizes the experimental results and gives the next research ideas.

II. Signal Model and Problem Formulation

Random impulse noise is mainly caused by the switch of household appliances and lightning in natural phenomena. This kind of noise is characterized by strong randomness, short duration, large energy, uncertain pulse interval and pulse width, and serious interference to power line communication. Some researchers model the noise of PLC as Middleton Class A model [14]. Literature [15] points out that Middleton Class A model cannot accurately describe the noise in PLC channels. Through the actual measurement of the background noise and pulse noise of PLC system, a noise model that obeys α stable distribution is proposed [16]. The actual measured values in reference [17] show that as a special case of α stable distribution, symmetric alpha stable (SαS) distribution not only includes the case of Gaussian distribution (i.e. characteristic factor α=2), but also can reflect the pulse characteristics of background noise, which is full of generalized central limit theorem [18]. The probability density function of α stable distribution has no uniform expression, and is generally described by its characteristic function. In [19], it can be expressed as follow:

$$\varphi(t) = \exp(jpt - \gamma|t|^{\alpha}\left[1 + j\beta sgn(t)\omega(t,\alpha)\right]) \tag{1}$$

Where

$$\omega(t,\alpha) = \begin{cases} \tan\dfrac{\alpha\pi}{2}, \alpha \neq 1 \\ \dfrac{2}{\pi}\log|t|, \alpha = 1 \end{cases} \tag{2}$$

Among them $\alpha \in (0,2]$, is the characteristic index, which determines the degree of pulse characteristics of the distribution. The smaller the α value is, the more significant the pulse characteristics are. When α=2, the characteristic function formula is the same as that of the Gaussian distribution with the mean value of a and variance of $2\delta^2$, that is, the Gaussian distribution is a special case of the α stable distribution; $-1 < \beta < 1$ is the symmetric parameter, $\beta = 0$ is the symmetric distribution; γ is the dispersion coefficient, which is a measure of the dispersion degree of samples relative to the mean value, similar to the variance in the Gaussian distribution; $p \in (-\infty, +\infty)$ is the position parameter. For SαS distribution, if $0 < \alpha \le 1$, p represents the median value; if $1 < \alpha \le 2$, p is the mean value.

The indoor single phase power line consists of three wires: phase wire(P), neutral wire(N), protection earth wire (PE). It can provide multiple feeding and receiving ports for the communication system: P-N, P-PE, and N-PE. The voltage difference between two power lines can be called a port, like an antenna in a wireless network, these PLC ports can be used as communication ports for signal transmission and reception, but they need to meet Kirchhoff's rule. Therefore, the transmitter can only use two antennas [20], the model of PLC system is shown in Figure 1.

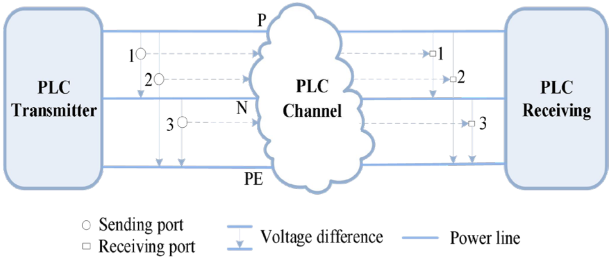


Fig. 1. PLC channel model

In the process of signal transmission, the channel model of the system is equipped with 2 feeding ports and 2 receiving ports(2×2). Assume that both Gaussian noise and impulse noise exist at the same time. The noise model of receiving mixed signal can be expressed as follows:

$$\boldsymbol{X} = \begin{bmatrix} a_{11} \, a_{12} \\ a_{21} \, a_{22} \end{bmatrix} \begin{bmatrix} \boldsymbol{s} \\ \boldsymbol{v} \end{bmatrix} + \boldsymbol{n} \tag{3}$$

where $\boldsymbol{X}$ is an observation signal, $\boldsymbol{s}$ is OFDM source signal, $\boldsymbol{v}$ is impulse noise subject to stable distribution, $\boldsymbol{n}$ is Gaussian noise, a_{ij} is equivalent to complex channel influence factor. $\boldsymbol{s}, \boldsymbol{v}$ are the system input signal, $\boldsymbol{n}$ is PLC channel random generation. Due to the advantages of blind separation [21], we don't need to estimate the channel influence factor and synchronization parameter. It is significant to use the blind adaptive separation algorithm to achieve noise cancellation in low SNR.

III. Blind Separation Algorithm based on WD-PowerICA

BSS is a kind of adaptive signal processing, which is used to retrieve multi-channel mixed original signals transmitted from multiple point sources. Because the source signal and the mixed channel are unknown, it is called blind source separation. The task of BSS is to recover the original sources from their linear instantaneous mixing only dependent on the statistical independent sources. The ICA analysis is the main method to solve the problem of blind source separation. Its properties depend on the independence criterion and optimization algorithm. Non-Gaussian is a common criterion for ICA. According to the generalized central limit theorem, the non-Gaussian criterion can be used as the cost function to maximize the non-Gaussian to achieve the purpose of extracting independent sources. The ICA linear mixed model can be expressed as [13]:

$$\boldsymbol{X} = \boldsymbol{AS} + \boldsymbol{n} \tag{4}$$

Where $\boldsymbol{X} = \left[x_1 \quad x_2 \quad \cdots \quad x_M\right]^{\mathrm{T}}$ represents observation signal, $\boldsymbol{A}$ is a $M \times N$ unknowing mixed matrix, $\boldsymbol{S} = \left[s_1 \quad s_2 \quad \cdots \quad s_N\right]^{\mathrm{T}}$ represents the system input signal. According to the ICA principle, The model of received noise signal in this paper is shown in equation (3), the noise signal blind source separation model is shown in figure 2.

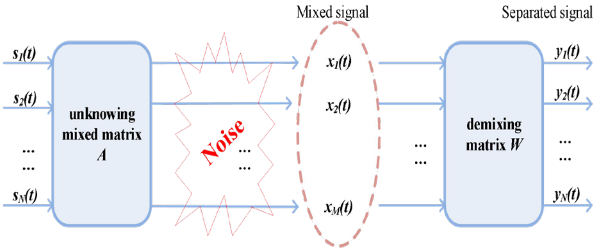


Fig. 2. Noisy blind source separation model

A. FastICA Algorithm

Fast independent component analysis(FastICA) is an iterative estimation method based on information theory and principle. It is an estimation algorithm based on negative entropy maximization, negentropy is obtained from differential entropy and defined as [22]:

$$J(\boldsymbol{Y}) = H(\boldsymbol{Y}_{Gauss}) - H(\boldsymbol{Y}) \tag{5}$$

where $\boldsymbol{Y}_{Gauss}$ and $\boldsymbol{Y}$ are the random variables with the same covariance And the expression of the differential entropy $H(\boldsymbol{Y})$:

$$H(\boldsymbol{Y}) = -\int P_Y(\xi) \log P_Y(\xi) d\xi \tag{6}$$

FastICA is an iterative calculation process. The rule it learns is to explore the direction which gains the maximum degree of non-Gaussian in terms of the equation . The FastICA algorithm finds the demixing matrix by iteration objective function:

$$J(\boldsymbol{y}) \approx c\left[E\{G(\boldsymbol{y})\} - E\{G(\boldsymbol{\upsilon})\}\right]^2 \tag{7}$$

c is a positive constant and υ is a random variable of the Gaussian with zero mean and unit variance, G is a non-quadratic function. Since OFDM signal is sub-Gaussian, G can be expressed as:

$$G(\boldsymbol{u}) = \frac{1}{a}\log_2 \cosh(a\boldsymbol{u}), G^{'}(\boldsymbol{u}) = \tanh(a\boldsymbol{u}) \tag{8}$$

Where $a \in [1,2]$.

Due to $\boldsymbol{y} = \boldsymbol{w}^{\mathrm{T}}\boldsymbol{X}$, equation (7) can be written as:

$$J_G(\boldsymbol{W}) \propto \left\{E\left[G\left(\boldsymbol{w}^T\boldsymbol{X}\right)\right] - E\left[G\left(\boldsymbol{\upsilon}\right)\right]\right\}^2 \tag{9}$$

The maximum $J_G(\boldsymbol{W})$ is converted to finding the maximum value of the separation matrix $\boldsymbol{W}$. FastICA estimator maximizes the Lagrangian.

$$\mathcal{L}(\boldsymbol{w};\lambda) = \left|\mathbb{E}\left[G\left(\boldsymbol{w}^T\boldsymbol{X}\right)\right]\right| - \frac{\lambda}{2}\left(\boldsymbol{w}^T\boldsymbol{w} - 1\right) \tag{10}$$

Here, λ is the Lagrange multiplier. Due to the local optimum of (10), the following equations hold

$$F(\boldsymbol{w}) = \mathrm{m}(\boldsymbol{w}) \text{-} \lambda(\boldsymbol{w})\boldsymbol{w} \text{=} 0 \tag{11}$$

where $\mathrm{m}(\boldsymbol{w}) \text{=} \mathbb{E}\left[g(\boldsymbol{w}^{\mathrm{T}}\boldsymbol{X})\boldsymbol{X}\right]$ and $\lambda(\boldsymbol{w}) = \boldsymbol{w}^T m$ can be obtained by multiplying w^T from the left on both sides of equation (11), $\lambda(\boldsymbol{w})$ is treated as a constant that does not depend on w . the one-unit fixed point FastICA algorithm is used as an approximate Newton-Raphson iterative update. The iteration of FastICA can be further expressed as:

$$\boldsymbol{w} \leftarrow \frac{\mathrm{m}(\boldsymbol{w}) - \beta(\boldsymbol{w})\boldsymbol{w}}{\left\|\mathrm{m}(\boldsymbol{w}) - \beta(\boldsymbol{w})\boldsymbol{w}\right\|} \tag{12}$$

until convergence, $\beta(\boldsymbol{w}) = \mathbb{E}\left[g^{'}(\boldsymbol{w}^{\mathrm{T}}\boldsymbol{X})\right] \in \mathbb{R}$ is a scalar multiplier, $g = G^{'}$.

B. WD-PowerICA Algorithm

Use either SI (MKS) or CGS as primary units. (SI units are strongly encouraged.) English units may be used as secondary units (in parentheses). This applies to papers in data storage**.** For example, write "15 Gb/cm^2 (100 Gb/in^2)." An exception is when English units are used as identifiers in trade, such as "3½-in disk drive." Avoid combining SI and CGS units, such as current in amperes and magnetic field in oersteds. This often leads to confusion because equations do not balance dimensionally. If you must use mixed units, clearly state the units for each quantity in an equation.

Wavelet analysis consists of breaking up a signal into scaled and shifted versions of the original signal or mother wavelet. Wavelets are family of functions constructed from translations and dilations of a single function, they are defined by:

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right), a \neq 0 \tag{13}$$

Where $\psi_{a,b}(t)$ is called daughter wavelet, $\psi(t)$ is called mother wavelet, the parameter a is the scaling parameter or scale, and it measures the degree of compression, the parameter b is the shift parameter which determines the time location of the wavelet [23].

Shahab Basiri et al. propose a novel power iteration algorithm for FastICA, which is numerically more stable than the original FastICA algorithm, when the sample size is not orders of magnitudes larger than the dimension [24]. The algorithm does not require using unnecessary assumptions, the Lagrangian multiplier is not treated as a constant and an ad-hoc approximation is not used for Jacobian matrix in the NR update, the method can be run on parallel computing nodes, which drastically reduces the computational time. Therefore, FastICA as a further expression of the PI method:

$$\boldsymbol{w} \leftarrow \frac{\left[\mathrm{H}(\boldsymbol{w})\text{-}\beta(\boldsymbol{w})\mathrm{I}\right]\boldsymbol{w}}{\left\|\left[\mathrm{H}(\boldsymbol{w})\text{-}\beta(\boldsymbol{w})\mathrm{I}\right]\boldsymbol{w}\right\|} \tag{14}$$

Where $\mathrm{H}(\boldsymbol{w})=\mathbb{E}\left[\frac{g(\boldsymbol{w}^{\mathrm{T}}\boldsymbol{X})}{\boldsymbol{w}^{\mathrm{T}}\boldsymbol{X}}\boldsymbol{X}\boldsymbol{X}^{\mathrm{T}}\right]\in\mathbb{R}^{d\times d}$ is positive definite for all conventional ICA nonlinearities.

Following the previous work [13], this article studies the separation effect of the PowerICA algorithm under low signal-to-noise ratio conditions. Simulation experiments verify that the separation effect is not ideal. Therefore, under the condition of low SNR, this time the wavelet denoising is used to preprocess the mixed signal, the signals $\boldsymbol{X}^{'}(t)$ processed by wavelet transform is:

$$\begin{aligned}\boldsymbol{X}^{'}(t)=\langle\boldsymbol{X}(t),\psi_{a,b}(t)\rangle&=\int_{-\infty}^{\infty}\boldsymbol{X}(t)\psi_{a,b}^{*}(t)dt\\&=\int_{-\infty}^{\infty}(\boldsymbol{AS}(t)+\boldsymbol{N}(t))\psi_{a,b}^{*}(t)dt\end{aligned} \tag{15}$$

After preprocessing the mixed signals using wavelet denoising and then it is separated by PowerICA. Experimental simulations verify that the combination of the two algorithms(ie, WD-PowerICA) can achieve stable and efficient separation [25]. The specific steps are:

1. After receiving the entire observation signal, remove the cyclic prefix from the OFDM signal, and then perform the fast Fourier transform.

2. Apply wavelet denoising to preprocess the observation signals with random weights.

3. Perform PowerICA processing on the N sub-carriers to estimate the MIMO channel of the N sub-carriers.

4. Use interpolation to obtain channel estimates for the remaining subcarriers.

The processing flow chart is illustrated in Figure 3.

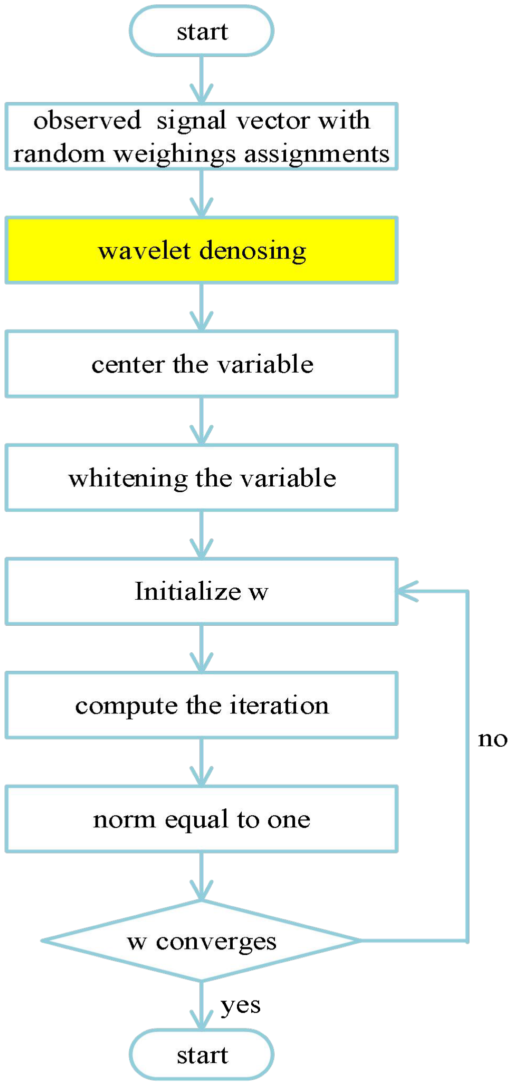


Fig. 3. Flowchart of WD-PowerICA

Next, the computational cost of the WD-PowerICA Algorithm will be analyzed simply, $\boldsymbol{X}=\boldsymbol{AS}+\boldsymbol{n}$ takes *O(MN)* operations.Therefore, the computational cost is described as,

$$O(total)=iterations\times(O(MN)) \tag{16}$$

From above analysis, although the computational steps of the proposed algorithm are relatively complex, the computational complexity remains unchanged. However, the WD-PowerICA algorithm is very important to improve the performance of power line communication in the case of low SNR.

IV. Simulation Analysis and Discussion

To demonstrate the effectiveness of the proposed WD-PowerICA algorithm based blind source separation for power line communication system at low SNR, we conduct simulation experiments to evaluate the performance. In the experiment, the signal noise model is shown in section Ⅱ. The useful signal s is the OFDM signal, and v is the impulse noise, they are seen as two input source signals, the carrier frequency is 1000 and sample frequency is 2000, and the SNR of input signal is 8dB, and the number of sample points is 500 when $\alpha = 0.8, \beta = 0, \gamma = 1, \lambda = 0$, the original input signals are shown in Figure 4.

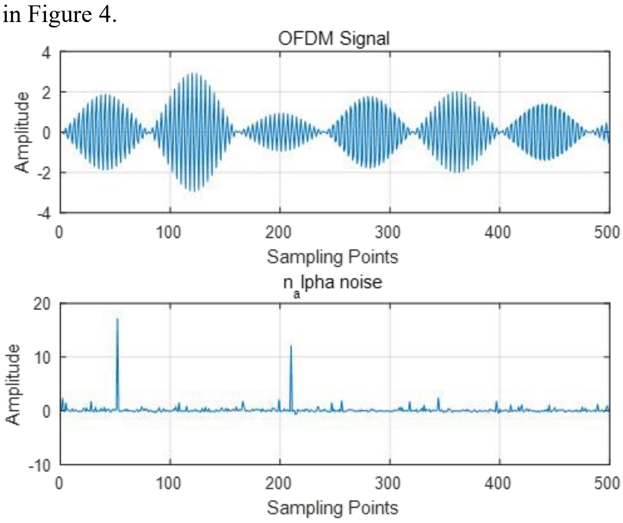


Fig. 4. The original input signals

To generate the two random mixed observation signals, the two random number couples used as mixing weighing assignment vectors are multiplied respectively with the original input signals , and the observation signals are shown Figure 5.

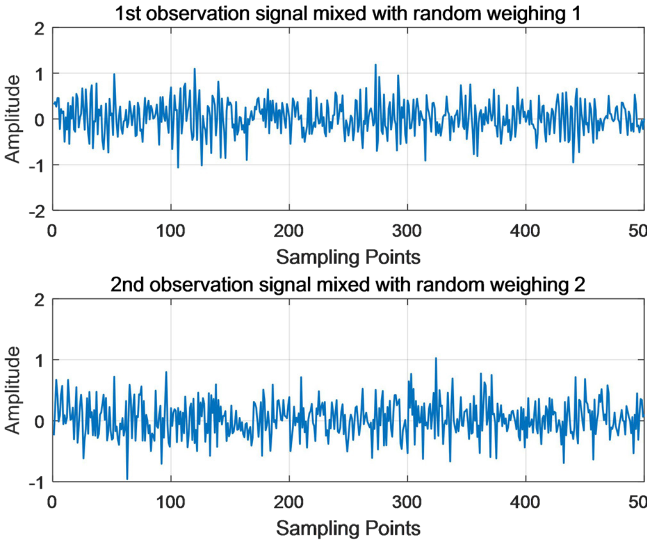
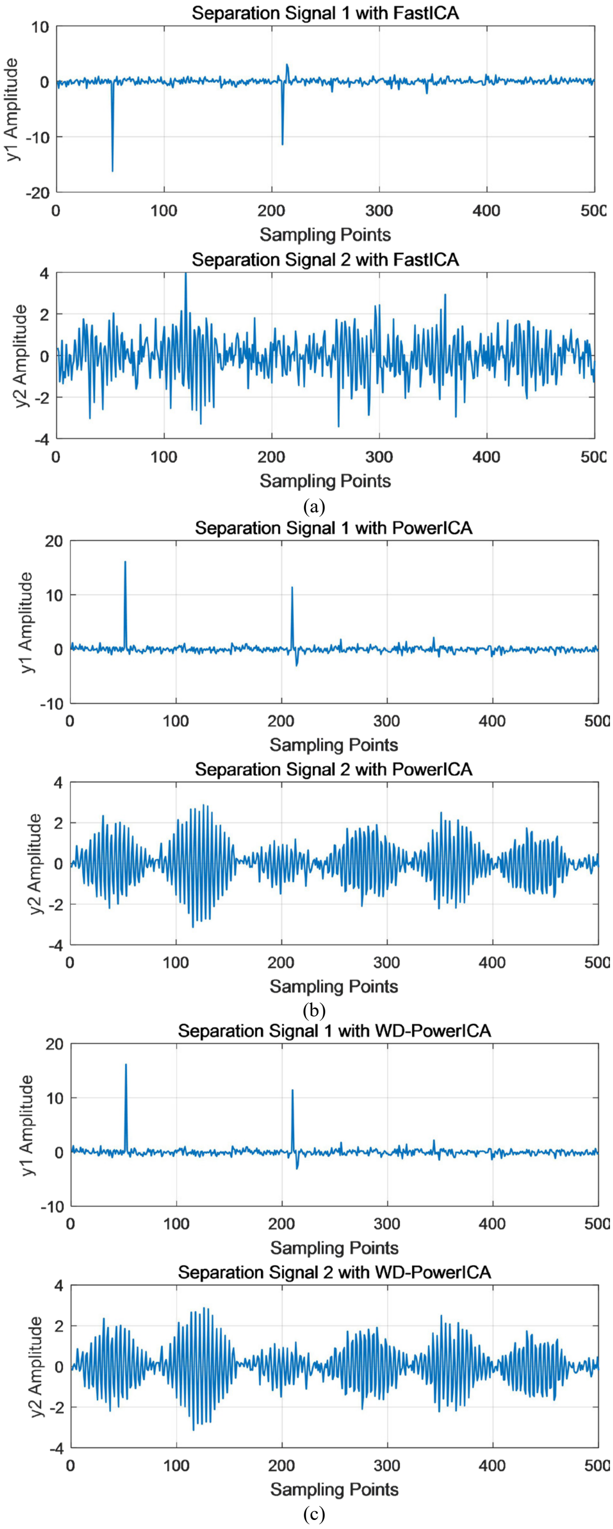


Fig. 5. Observation signals

ICA algorithm is based on the statistical characteristics of signals to maximize the independence between signals, so as to achieve the purpose of estimating the source signal. Compared with Gaussian white noise and OFDM signals, the α-stable distribution noise is the strongest. Therefore, the impulse noise can be extracted first. By FastICA, PowerICA and WD-PowerICA, the separation results are shown in (a), (b) and (c) of Figure 6.



(a)

(b)

(c)

Fig. 6. Algorithm separation result: (a) FastICA algorithm separation; (b) PowerICA algorithm separation; (c) WD-PowerICA algorithm separation.

In the simulation experiment, other conditions remain unchanged, only the SNR is changed, and the separation effect of the three algorithms is shown in Figure 7. Through the experimental simulation, the algorithm in this paper is obviously superior to the other two algorithms, especially in the case of low signal-to-noise ratio.

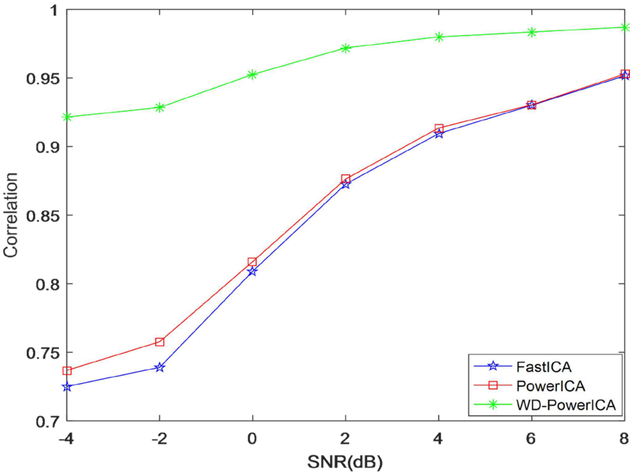


Fig. 7. Separation result of changing SNR

Due to $\alpha \in (0,2]$, the larger α, the stronger Gauss, changing the value describing the Gaussian strength of impulse noise, the experimental results are as shown in Figure 8. When the input signal is very non-Gaussian, the algorithm in this paper has a better separation effect. However, When $\alpha > 1.1$ approximately, WD-PowerICA algorithm performance is significantly reduced, This is my next problem to be solved.

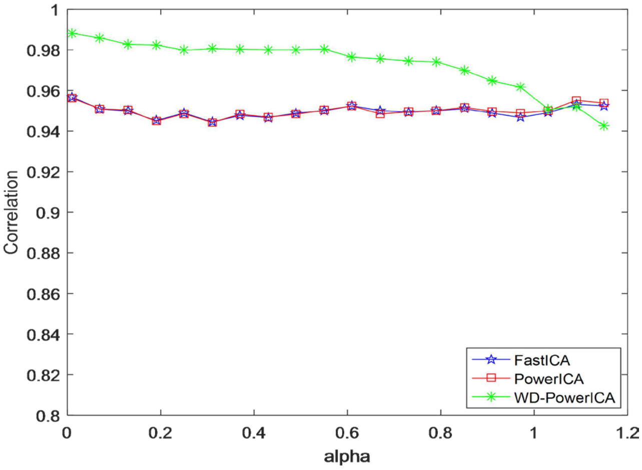


Fig. 8. Separation result of changing

V. Conclusions

This paper studies the denoising method of power line communication in low signal-to-noise ratio. Aiming at the situation that the denoising effect of PowerICA algorithm is not ideal in low signal-to-noise ratio, combined with the advantages of wavelet denoising algorithm, a joint denoising method combining wavelet and PowerICA algorithm is proposed. The WD-PowerICA denoising effect is obviously improved, and the effective separation of noise and useful signal is realized. However, due to the limited time, this paper only analyzes the correlation index. Next, we will study the BER and other performance indicators.

References

[1] Baig S., Asif H. M., Umer T., et al.: 'High data rate discrete wavelet transform-based PLC-VLC design for 5G communication systems'. IEEE Access, 2018, 6, pp. 52490-52499.

[2] Songnong L., Xiaorui H., Ke Z., et al.: 'Measurement and research on attenuation characteristics of low voltage power line communication channel'. Power Line System Protection and Control, 2018, 46, (4), pp. 99-106.

[3] Ying C., Xiaosheng L., Dianguo X.: 'Game analysis and optimization of communication network performance for low voltage power line'. Automation of Electric Power Systems, 2018, 42, (11), pp. 122-128. DOI: 10.7500/ AEPS20170807005.

[4] Hui Z., Wenbing L., Xiongwen Z., et al.: 'Noise modeling for power line communication channel using the LS-SVM and wavelet neural networks'. Transactions of China Electrotechnical Society, 2018, 33, (16), pp. 3879-3888.

[5] Juwono F. H., Guo Q., Huang D., et al.: 'Deep clipping for impulsive noise mitigation in OFDM-based power-line communications'. IEEE Transactions on Power Delivery, 2014, 29, (3), pp. 1335-1343.

[6] Papilaya V .N., Vinck A.J.H.: 'Investigation on a new combined impulsive noise mitigation scheme for OFDM transmission'. International Symposium on Power Line Communications and Its Applications, Johannesburg, South Africa, March, 2013, pp. 86-91.

[7] Darsena D., Gelli G., Melito F., et al.: 'ICI-free equalization in OFDM systems with blanking preprocessing at the receiver for impulsive noise mitigation'. IEEE Signal Processing Letters, 2015, 22, (9), pp. 1321-1325.

[8] Yih C. H.: 'Iterative interference cancellation for OFDM signals with blanking nonlinearity in impulsive noise channels'. IEEE Signal Processing Letters, 2012, 19, (3), pp. 147-150.

[9] Ando H., Nakamura A., Ohno K., et al.: 'A study on channel estimation under class A impulsive PLC channel'. International Symposium on Power Line Communications and Its Applications, Johannesburg, South Africa, March, 2013, pp. 69-70.

[10] Mehboob A., Li Z., Khangosstar J.: 'Adaptive impulsive noise mitigation using multi mode compressive sensing for powerline communications'. International Symposium on Power Line Communications and Its Applications, Beijing, China, March, 2012, pp. 368-373.

[11] Lin J., Nassar M., Evans B. L.: 'Impulsive noise mitigation in powerline communications using sparse Bayesian learing'. IEEE Journal on Selected Areas in Communications, 2013, 31, (7), pp. 1172-1183.

[12] Qiu T. S., Li B., Zha D. F.: 'Elimination of pulse-noise from mixed-noise based on fractional lower order ICA'. Journal on Communications, 2011, 32, (9), pp. 77-81.

[13] Wei Z., Zhongqiang L., Xingzhong X.: 'Impulse Noise Suppression Based on Power Iterative ICA in Power Line Communication'. International Journal of Electronics and Telecommunications, 2019, 64, (4), pp. 651-656.

[14] Middleton D.: 'Statistical-physical models of electromagnetic interference'. IEEE Transactions on Electromagnetic Compatibility, 1977, EMC-19, (3), pp. 106-127. DOI: 10.1109/TEMC.1977.303527.

[15] Andreadou N., Pavlidou F. N.: 'Modeling the noise on the OFDM power-line communications system'. IEEE Transactions on Power Delivery, 2010, 25, (1), pp. 150-157. DOI: 10.1109/TPWRD.2009.2035295.

[16] Tran T. H., Do D. D., Huynh T. H.: 'PLC impulsive noise in industrial zone: Measurementand characterization'. International Journal of Computer and Electrical Engineering, 2013, 5, (1), pp. 48-51. DOI: 10.7763/IJCEE.2013.V5.660.

[17] Laguna-Sanchez G., Lopez-Guerrero M.: 'On the use of alpha-stable distributions in noise modeling for PLC'. IEEE Transactions on Power Delivery, 2015, 30, (4), pp. 1863-1870. DOI: 10.1109/TPWRD.2015.2390134.

[18] Mahmood A., Chitre M.: 'Optimal and near-optimal detection in bursty impulsive noise'. IEEE Journal of Oceanic Engineering, 2017, 42, (3), pp. 639-653. DOI: 10.1109/JOE.2016.2603790.

[19] Shao M., Nikias C. L.: 'Signal processing with fractional lower order moments: stable processes and their applications'. Proceedings of the IEEE, 1993, 81, (7), pp. 986-1010.

[20] Berger L. T., Schwager A., Pagani P., et al.: 'MIMO Power Line Communications: Narrow and Broadband Standards, EMC, and Advanced Processing'. (CRC Press, 2014, 1st edn.), pp.5-43.

[21] Zhongqiang L., Chengjie L., Lidong Z.: 'A Comprehensive Survey on Blind Source Separation for Wireless Adaptive Processing: Principles, Perspectives, Challenges and New Research Directions'. IEEE Access 2018, 6, pp. 66685-66708.

[22] Chengjie L., Lidong Z., Zhongqiang L.: 'Underdetermined Blind Source Separation of Adjacent Satellite Interference Based on Sparseness'. China Communications, 2017, 14, (2), pp. 140-149.

[23] Karanpreet Kaur. Disceret Wavelet Transform based OFDM System using Convolutional Encoding. Master thesis. Patiala: Thapar university; 2014, pp. 58-63.

[24] Basiri S., Ollila E., Koivunen V.: 'Alternative Derivation of FastICA With Novel Power Iteration Algorithm'. IEEE Signal Processing Letters, 2017, 24, (9), pp. 1378-1382.

[25] Abdel-Hamid G., Samir R.: 'Blind Channel Estimation Using Wavelet Denoising of Independent Component Analysis for LTE'. Indonesian Journal of Electrical Engineering and Computer Science, 2016, 17, (1), pp.126-137.

Wei Zhang received the B.S. and M.S. degrees in communication engineering and pattern recognition and intelligent systems from Sichuan University of Science and Engineering(SUSE), Zigong, China, in 2017 and 2020, respectively. Since Sep. 2020, she has been with Yibin University, Her research contain Blind Source Separation, intelligent Signal Processing and Artificial Intelligence.

Zhongqiang Luo received the B.S. and M.S. degrees in communication engineering and pattern recognition and intelligent systems from Sichuan University of Science and Engineering, Zigong, China, in 2009 and 2012, respectively. He received the Ph.D. degree in communication and information systems from University of Electronic Science and Technology of China (UESTC), in 2016. Since 2017, he has been with the Sichuan University of Science and Engineering, where he is currently a lecturer. From December 2018-December 2019, he is a visiting scholar with Department of Computer Science and Electrical Engineering in University of Maryland Baltimore County (UMBC). His research interests include machine learning, blind source separation, signal processing for wireless communication system and intelligent signal processing.

Xingzhong Xiong received the B.S. degrees in communication engineering from Sichuan University of Science and Engineering, Zigong, China, in 1996. He received the M.S and Ph.D. degrees in communication and information system from University of Electronic Science and Technology of China (UESTC), in 2006 and 2009, respectively. In 2012, he completed a research assignment from the Postdoctoral Station of Electronic Science and Technology at the UESTC. He is currently a professor at the School of Automation and Electronic Information, Sichuan University of Science and Engineering. His research interests include wireless and mobile communications technologies, intelligent signal processing, Internet of Things technologies, and very large-scale integration (VLSI) designs.

Kai Deng received the B.S., M.S. and Ph.D. degrees in communications and information systems from University of Electronic Science and Technology of China(UESTC), Chengdu, China, in 2002, 2005 and 2009, respectively. He is currently with Faculty of Intelligent Manufacturing, Yibin University, Yibin, China. His research interests mainly include signal processing in wireless communications.

Risk Management and Standard Compliance for Cyber-Physical Systems of Systems

George Matta[1], Sebastian Chlup[2], Abdelkader Magdy Shaaban[3], Christoph Schmittner[4],
Andreas Pinzenöhler[5], Elke Szalai[6] and Markus Tauber[7]

***Abstract*— The Internet of Things (IoT) and cloud technologies are increasingly implemented in the form of Cyber-Physical Systems of Systems (CPSoS) for the railway sector. In order to satisfy the security requirements of Cyber-Physical Systems (CPS), domain- specific risk identification and assessment procedures have been developed. Threat modelling is one of the most commonly used methods for threat identification for the security analysis of CPSoS and is capable of targeting various domains. This paper reports our experience of using a risk management framework to identify the most critical security vulnerabilities in CPSoS in the domain and shows the broader impact this work can have on the domain of safety and security management. Moreover, we emphasize the application of common analytical methods for cyber-security based on international industry standards to identify the most vulnerable assets. These will be applied to a meta-model for automated railway systems in the concept phase to support the development and deployment of these systems. Furthermore, it is the first step to create a secure and standard complaint system by design.**

I. Introduction

Cyber-physical systems (CPS) in the railway industry are increasingly being developed using IoT and cloud services, employing generic commercial-off-the-shelf (COTS) components and heterogeneous communication protocols, which raises the potential for cyber-attacks. The challenge is that cyber attacks on critical infrastructure in the rail domain are increasing in intensity. This will raise concerns about employee safety, potential security risks including the loss of sensitive information, reputational damage, financial loss and faulty decisions. Moreover, IBM statistics show that the railway industry is impacted by numerous types of cyber attacks: SQLi (SQL Injection), DDoS (Distributed Denial of Service), malware, brute force, tampering, phishing, etc [1]. For instance, Danish Railways reported that hackers perpetrated a massive DDoS attack on the Danish State Railways (DSB) in May 2018 that crippled part of its operations, including ticketing systems and communications infrastructure [2]. Therefore, we will perform a comprehensive safety and security analysis, taking into account the wireless communication used in networked and autonomous rail vehicles and modern management systems that enable communication between such CPS. In order to provide the required and appropriate mitigation measures, we have considered the risk management process, which is responsible for identifying, analysing and assessing potential threats and their mitigation such as ISO 27001 and NIST SP 800-30 [3], [4] investigated in order to enable appropriate planning [5]. In order to satisfy risk management demands for a CPSoS we adopt a methodology focused on system assets, to identify potential threats affecting the system. This requires system awareness to identify the most critical assets [6]. However, security breaches are tolerated more easily if a company can prove that the system under consideration was vulnerable despite being compliant with an international security standard [7], [8]. Therefore, we will use the existing guidelines and recommendations of IEC 62443-3-3 [9] to investigate the system's compliance to be developed. The system's configuration reflects the level of compliance. This is based on the security controls given by the standard recommendation. In our use case, we show the analysis of communication channels between different system components. For this purpose, we employ an IoT framework as a Separation Kernel (e.g. Arrowhead [10], [11]) to provide an additional abstraction layer to handle the registration, authentication, authorisation and encryption between system components.

We discuss our experience concerning the most vulnerable components of the use case, "a CPSoS in the railway domain," in a cyber-attack event. Moreover, we identify and assess potential threats and present samples related to STRIDE categories. In addition, we investigate the categorisation of potential threats to the system and most vulnerable components. Furthermore, for each threat identified, we discuss how the appropriate security controls extracted from IEC 62443-3-3 can be used as countermeasures to mitigate them. The paper is organized as follows; Section II presents state of the art on model-based approaches for security analysis, security risk assessment methods for connected vehicle systems, and analysis of information flow security CPS. Section III describes the case study and presents the risk management framework. Section IV discusses major challenges and concludes the risk

[1] Forschung Burgenland Eisenstadt, Austria
[2,3,4] Austrian Institute of Technology Vienna, Austria
[5] IQSOFT Vienna, Austria
[6] FH Burgenland Eisenstadt, Austria
[7] Research Studios Austria Vienna, Austria
[1] E-mail: george.matta@forschung-burgenland.at
[2] E-mail: sebastian.chlup@ait.ac.at
[3] E-mail: abdelkader.shaaban@ait.ac.at
[4] E-mail: christoph.schmittner@ait.ac.at
[5] E-mail: andreas.pinzenoehler@iqsoft.com
[6] E-mail: elke.szalai@fh-burgenland.at
[7] E-mail: markus.tauber@researchstudio.at

DOI: 10.36244/ICJ.2021.2.5

management process results. The road-map of our approach is discussed in Section V.

II. RELATED WORK

State of the art research has revealed several model-based approaches to manage risks posed to a system. Multiple security analysis methods based on threat modelling utilising data-flow diagrams were analysed for the CPS domain. Although they have in common that they are model-based, they employ different review methods to assess security risks for networked, autonomous vehicles. Strobl et al. analysed threats and vulnerabilities of connected vehicles, for which system assets and data flows were specified to perform safety analysis. A risk assessment of the threats and vulnerabilities potentially targeting this system was carried out. This resulted in a threat and vulnerability catalogue [12].

Ma and Schmittner [6] introduce guidelines for the implementation of threat models. They propose using a threat modelling approach specified in the ”SAE J3061” guidebook [13] to identify threats and vulnerabilities. Hamad and Pervelakis have revised several existing threat modelling approaches and their potential adaption in the automotive sector. This has resulted in a hybrid threat model called SAVTA, which combines several techniques developed for the automotive industry. By identifying potential attackers and targets, an abstract model is created to achieve a holistic model. Hamad and Pervelakis concluded that effective protection measures for threat prevention, countering threats have to be permanently complemented [14].

Sheehan et al. [15] investigated the Bayesian Network (BN) cyber-risk classification model for its ability to classify the risk of vulnerabilities of a Connected and Autonomous Vehicle (CAV) GPS. The purpose was to provide vehicle manufacturers with a method to analyse CAV risk based on known systems vulnerabilities. Moreover, they used the Common Vulnerabilities Scoring System (CVSS) as a standardised framework to assess cyber threats in a CAV.

In addition, Schmittner et al. [16] show how threat modelling for railway safety analysis might be conducted during a development life-cycle based on IEC 62443. In their approach, they have proposed the identification of threats in addition to the IEC 62443-4-2 [17] security standard for Industrial Automation and Control Systems (IACS). Another approach is proposed by Shaaban et al. [18] for utilizing the concept of the IEC 62443 on the component level instead of the system level. By splitting, e.g. storage, processing units and interfaces into independent zones, different criticality levels can be assigned to these zones. This enables the mitigation of possible security risks with the help of a gap analysis for the different zones. Consequently, an application can be split into smaller portions where one part may handle communication between zones, or with other components while another zone may represent the safety-critical part of the CPS of Systems.

Additionally, in the autonomous railway vehicle requires safety measures to be applied. Therefore, besides cybersecurity, the system that will be developed depends on functional safety [19] as well as safety of the intended functionality (SotIF) [20]. Functional Safety focuses on reducing risks within a technological system to avoid malfunctions and to ensure proper operation [21]. However, functional safety does not include topics such as risks that emerge due to insufficient performance of the respective component and, consequently, safety of the intended functionality should be considered, which deals with risks caused by performance issues [21]. A sensor system not detecting obstacles due to insufficient performance may lead to a disaster. Therefore, one of our goals is to apply SotIF to the autonomous railway vehicle and in a broader sense to the railway sector which currently mainly deals with functional safety.

A management process is specified in NIST SP 800-12 rev.1 [22] for developing a set of security policies, which derives security rules from security objectives is recommended. This process analyses the need for **C**onfidentiality, **I**ntegrity, and **A**vailability (CIA) to represent a security goal. In the system concept description, components, assets and cybersecurity properties are specified as part of the system development phase. Attackers could apply different malicious activities against the system to exploit existing security vulnerabilities within components and their corresponding assets. Therefore, a potential threat targeting a vulnerability in the system also affects the CIA's security measures.

III. CONCEPT AND FRAMEWORK

In our project's context, we aim to create a system architecture model and a component catalogue for an existing interlocking system. It aims at developing ”Railway Operations as a Service” (ROaaS) as the basis of a fully autonomous CPSoS. As the existing interlocking system is already Safety Integrity Level (SIL) certified, the original underlying system architecture shall remain untouched to avoid the necessity of re-certification.

Therefore, we propose integrating a risk management process within this research to identify, assess, and treat existing cyber risks. We will focus on communication topics, such as the integration of external systems and devices in particular.

In fact, we chose this risk management process approach because of the costs involved in designing and implementing secure CPS, and there are no reliable statistics on the cost differences between average day-to-day system development on the one hand and security-conscious development on the other. Anecdotal evidence suggests that security-conscious systems are more expensive [23].

In this work, we develop a secure railway system architecture. In order to represent the system model, we chose the Systems Modeling Language (SysML). SysML is a common modelling language often used by systems engineers, as discussed in [24]. SysML facilitates implementing all changes in our proposed system model in the design phase of CPSoS.

We defined use cases targeting the intended operation of the autonomous railway system. Moreover, we selected one of these use cases presented in subsection III-A. Subsequently, the required components, communication channels, and security assumptions are defined based on threat modelling.

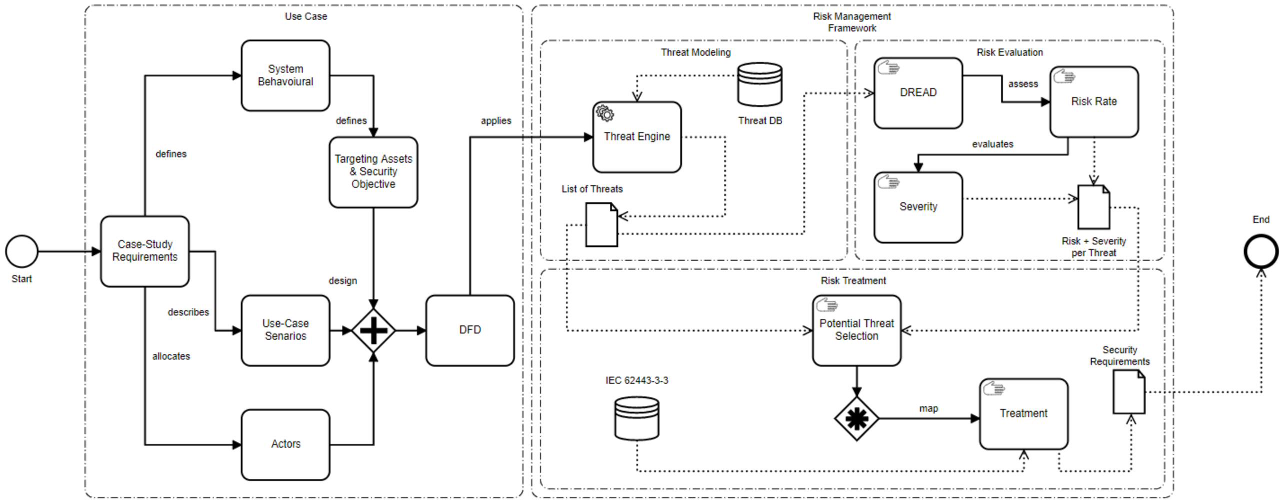


Fig. 1. Risk Management Process Model

Section III-B discusses the analysis process of identifying potential threats in the given system model. According to the identified threats, the risk evaluation process is conducted to rate each threat and define the appropriate risk level, as considered in Section III-C. Once risks have been assessed, security requirements targeting potential threats were selected based on IEC 62443-3-3, as explained in Section III-D. An illustration of this process is given in Fig. 1.

A. Specification of the Use Case

We focused on communication topics to further develop an existing industrial interlocking into a digital interlocking system and manage autonomously operating railway vehicles on secondary, less frequently used railway lines, such as the secure integration of external systems and devices in particular, e.g. COTS. Additional focus is given to their implementation impact on risks and threats.
Therefore, this work utilises an IoT framework as Separation Kernel (e.g., Arrowhead [10], [11]), which adds a layer of abstraction to build a chain of trust in such an SoS for secure communication. Moreover, the IoT framework architecture aims to enable the creation of local automation clouds that provide local real-time performance, security, inseparability, and scalability through multi-cloud interaction. Through this, it is feasible to manage various systems and, consequently, this approach is not limited to one specific interlocking system. On the contrary, by registering with the IoT framework, multiple systems can be controlled without manual configuration. Furthermore, autonomous vehicles can be mounted or unregistered on the fly. We have defined the system behavioural and actuators through the case study requirement and the already existing interlocking system. So we could identify the targeting assets and the security objectives and created the use case diagrams. All these steps enabled the creation of the Dataflow diagram (DFD). A use case diagram of the backbone of this system - the Separation Kernel as shown in fig. 2.

We identified four scenarios relevant for the coordination of such a system:

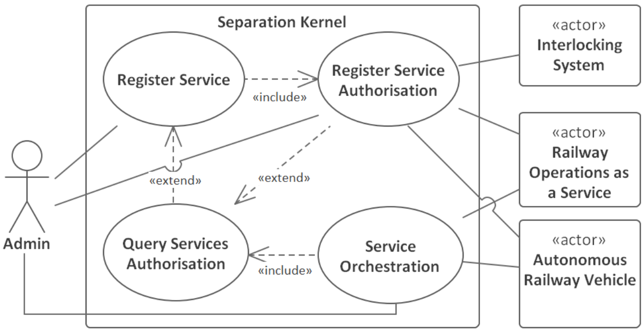

Separation Kernel
Register Service
«include»
Register Service Authorisation
«actor» Interlocking System
«actor» Railway Operations as a Service
«actor» Autonomous Railway Vehicle
«extend»
«extend»
Admin
Query Services Authorisation
«include»
Service Orchestration

Fig. 2. Use Case: System Enquiry Coordination by Separation Kernel

1) **Register Service**: Registers the service systems in the IoT framework (ROaaS, Interlocking system, Autonomous Railway Vehicles)
2) **Register Service Authorisation**: Authorisation privileges are granted and allocated by the administrator of the registered systems
3) **Query Services Authorisation**: Validates the orchestration service requests: actor identification and authorisation, origin and destination of the request
4) **Service Orchestration**: Manages requests from the registered service systems

B. Threat Modelling

The DFD in fig. 3 illustrates a portion of the communication channels between the Separation Kernel and the several system components. The Separation Kernel serves as the communication gateway for registration, authentication, authorisation within the IoT framework and handles data encryption between system components. According to the use case described in section A, the interactions between the several system assets are as follows:

1) Request: Registration, Authentication, Authorisation; from Interlocking System, ROaaS, Autonomous Railway Vehicles to Separation Kernel

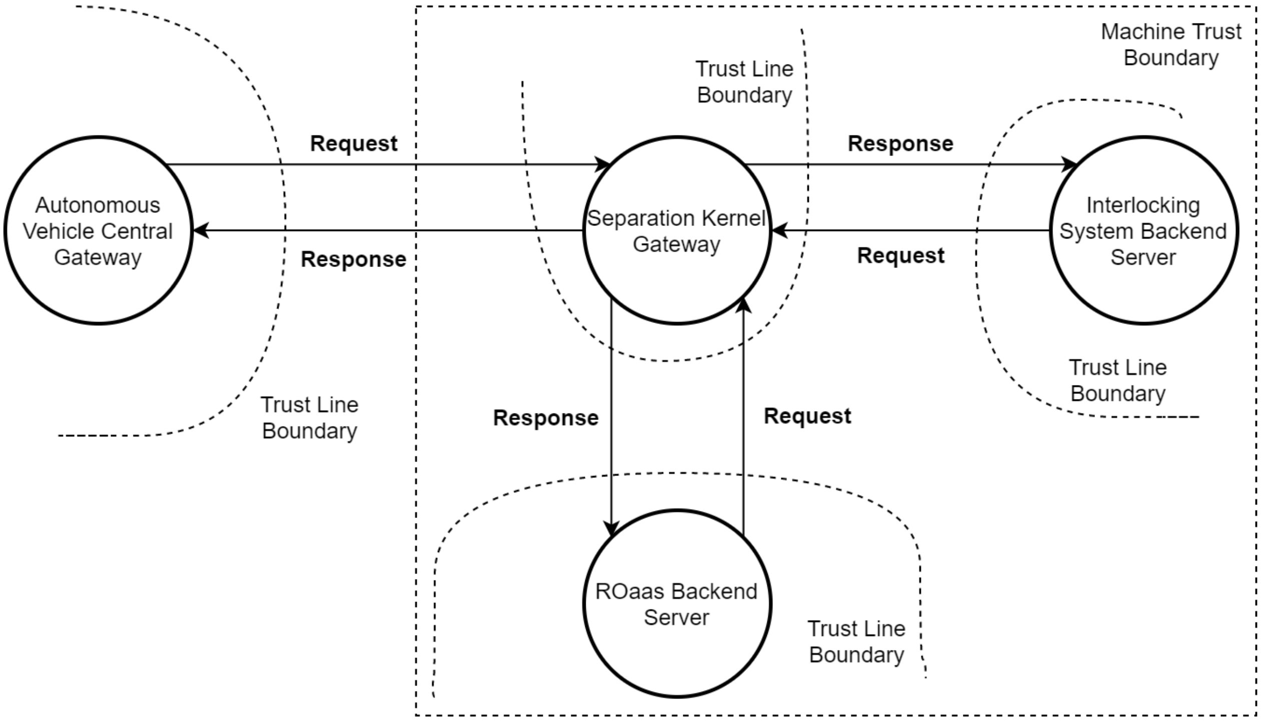


Fig. 3. DFD: Asset System Component Identifiable Data

2) Request: Stored system component identifiable data; from Interlocking System back-end server to database, ROaaS back-end server to database
3) Responses: Confirm Registration, Authentication, Authorisation; from Separation Kernel to each Autonomous Vehicle, ROaaS, and Interlocking System

Based on our DFD, we performed threat analysis using the Microsoft Threat Modelling Tool [1]. According to the threat analysis, there are 31 threats identified in the given diagram, as shown in Table I. These threats are classified based on the STRIDE model [25] categories.

TABLE I
THE IDENTIFIED THREATS COLLECTION CLASSIFIED ACCORDING TO THE STRIDE MODEL AND CIA^3 OBJECTIVES

Threat Category	No. of Threats	Security Objectives (CIA^3)
Tampering	11	Integrity
Elevation of Privilege	8	Authorization
Spoofing	5	Authentication
Information Disclosure	3	Confidentiality
Denial of Service	2	Availability
Repudiation	2	Auditing

The table summarizes the rate of all identified threats and their classifications using the STRIDE model. Each category of threat violates a specific security property (e.g., spoofing violates authentication, tampering violates integrity, repudiation violates non-repudiation, information disclosure violates confidentiality, denial of service violates availability, and elevation of privilege violates authorization). Accordingly, we use CIA^3 [14] as an extended version of the CIA according to the violations of security properties. CIA^3 establishes six categories, as follows:

- Confidentiality - protect confidential data from unauthorized access
- Integrity - ensuring that data remains unchanged
- Availability - ensuring the access to an asset
- Authentication - ensuring that an entity is who it claims to be
- Authorization - ensuring that only entities with permissions can conduct certain actions
- Auditing - Ensuring the traceability of actions

As shown in table I, the most common identified threats are considered in the integrity area for the asset system component identifiable data. In addition, we have investigated which threats may be allocated to the system components by analysing the in- and out-data flows for each component. As a result, the most affected component by 21 identified threats is the autonomous rail vehicle.

C. Risk Evaluation

The risk evaluation process comes into account of this work to assess each identified threat's risk rate. We propose using the DREAD model to analyse the risk for conducting a qualitative risk analysis to assess, compare, and prioritise the severity of risk posed by each potential threat. DREAD represents a method to determine the impact of potential threats based on five foundational aspects: **D**amage Potential, **R**eproducibility, **E**xploitability, **A**ffected Users, and **D**etectability.

[1] https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling

According to the DREAD scoring system [26] and classification, the assessment is carried out in terms of a particular threat's criticality. The result reflects the criticality of a particular threat to the system.

For scoring, threats are classified as **high** (3), **medium** (2) and **low** (1). The points per category are awarded on the assumption that the attack has been started successfully. The formula for calculating the overall risk rate is as follows [26]:

$$Risk\ Rate = D + R + E + A + D$$

- **Damage Potential**: What damage will be caused if the threat occurs?
- **Reproducibility**: How easily can the attack be repeated?
- **Exploitability**: How much effort is required to trigger an attack?
- **Affected Users**: How many users are approximately affected?
- **Detectability**: How easily can the exploit be found?

Table II illustrates threats that impact the most critical system component, which we identified as the autonomous railway vehicle. These findings are based on communication between the autonomous railway vehicle and the Separation Kernel and are categorized based on CIA3 objectives and DREAD scores. Although the Separation Kernel, as shown in fig. 3 may appear to be the most critical system component, as it is the central element and has the most inbound and outbound data flows. However, in terms of component interfaces and increased security target allocation, the autonomous railway vehicle is exposed to far more threats; in fact, the autonomous railway vehicle communication is transmitted wirelessly. Furthermore, there are physical interfaces that are cumbersome to secure sufficiently. Consequently, we conclude that security threats targeting critical cyber-physical systems also affect safety. Therefore, a safety and security analysis should be performed in a well-coordinated manner.

Afterwards, a set of security requirements needs to be selected to mitigate risk emanated from the above potential threats. The next section discusses the mapping approach for addressing these threats by selecting a set of security requirements for each threat.

D. Risk Treatment Based on IEC 62443-3-3

This section presents the mapping process between the previously discussed potential threats and a set of security requirements for addressing these system security issues. The IEC 62443-3-3 is applied to create a set of security requirements against existing security threats. IEC 62443-3-3 defines four security levels for each security requirement to define the minimum and maximum security capability of each security requirement against potential threats. The standard classifies security requirements into seven groups called foundational requirements (FR), as discussed in [9]. These FRs are defined as:

- Identification and Authentication Control (IAC)
- Use Control (UC)
- System Integrity (SI)
- Data Confidentiality (DC)
- Restricted Data Flow (RDF)
- Timely Response to Events (TRE)
- Resource Availability (RA)

In order to reach a security goal, we need to map between a Security Level (SL) and relevant FRs for selecting appropriate security requirements to address system design security issues, as discussed in [27], [28].

However, we have investigated how FRs could be mapped to the CIA^3 objectives and threat categories in the Risk management processes. In Table III shows the rough mapping of the FRs. In this example, we map the previously identified threats with appropriate security requirements for addressing security issues in the system design. Fig. 4 depicts a mapping of security requirements with potential threats.

The figure illustrates some of the selected security requirements according to the IEC 62443-3-3, for addressing potential threats. Each threat needs at least one appropriate security requirement for addressing its malicious behaviours. In this example, we select one security requirement for each threat according to its FR and SL. According to the DREAD risk rate, as described in Table II, we define the SL of security requirements for addressing a particular security issue. Furthermore, according to these ratings, we propose using SL = 3 and SL = 4 for each selected security requirement concerning the FR to achieve the primary goal.

CPSoS include many cyber components communicating with physical ones through different communication protocols over a network. An attacker could exploit security vulner-

TABLE II
LIST OF THREATS WITH THE HIGHEST RISK RATE PER CIA^3 CATEGORY

CIA^3 Objective	Threats	
Authentication	Title	Spoofing on vehicle gateway
	Description	Spoof autonomous vehicle central gateway with a fake one
	Category	Spoofing
	Risk Rate	11
	Severity	Medium
Confidentiality	Title	Access to confidential data
	Description	Gain access to confidential data through SQL Injection
	Category	Information Disclosure
	Risk Rate	15
	Severity	High
Integrity	Title	SQL Injection
	Description	Compromise confidential data by performing SQL injection
	Category	Tampering
	Risk Rate	15
	Severity	High
Availability	Title	Network Flooding
	Description	Deny actions on gateway due to flooding of network
	Category	Denial of Service
	Risk Rate	11
	Severity	Medium
Authorization	Title	Unauthorized access to device
	Description	Gain unauthorized access to privileged features on autonomous vehicle central gateway
	Category	Elevation of Privilege
	Risk Rate	11
	Severity	Medium
Auditing	Title	Removing attack footprints
	Description	Deny a malicious act and remove the attack footprints leading to repudiation issues
	Category	Repudiation
	Risk Rate	13
	Severity	High

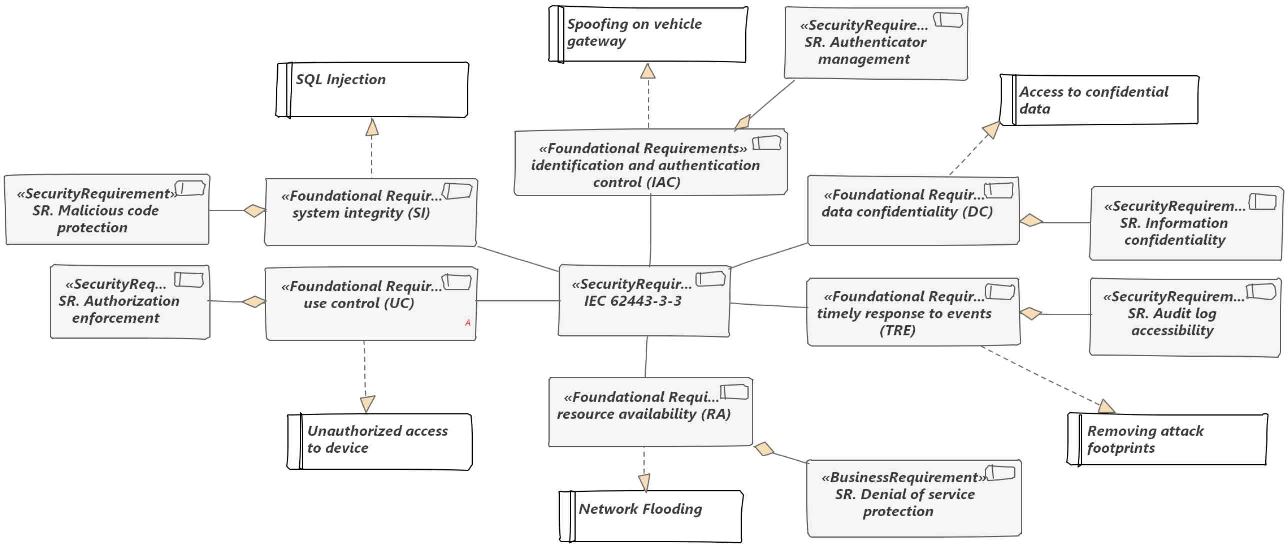

Spoofing on vehicle gateway
«SecurityRequire... SR. Authenticator management
SQL Injection
Access to confidential data
«Foundational Requirements» identification and authentication control (IAC)
«SecurityRequirement» SR. Malicious code protection
«Foundational Requir... system integrity (SI)
«Foundational Requir... data confidentiality (DC)
«SecurityRequirem... SR. Information confidentiality
«SecurityReq... SR. Authorization enforcement
«Foundational Requir... use control (UC)
«SecurityRequir... IEC 62443-3-3
«Foundational Requir... timely response to events (TRE)
«SecurityRequirem... SR. Audit log accessibility
«Foundational Requi... resource availability (RA)
Unauthorized access to device
Removing attack footprints
«BusinessRequirement» SR. Denial of service protection
Network Flooding

Fig. 4. IEC 62443 System Requirements Mapping with the Highest Risk Rated Threats from Table II

TABLE III
MAPPING IEC 62443-3-3 FOUNDATIONAL SECURITY REQUIREMENT ACCORDING TO CIA^3 AND THREAT CATEGORY

IEC 62443-3-3 FR	CIA³ Objectives	Threat Category
IAC	Authentication	Spoofing
SI	Integrity	Tampering
TRE	Auditing	Repudiation
DC	Confidentiality	Information Disclosure
RA	Availability	Denial of Service
UC	Authorization	Elevation of Privilege
RDF	System Segmentation	

abilities in the system's design, which leads to a different level of negative consequences in terms of safety, reliability, availability and maintainability. Furthermore, cybersecurity in railways protects data and critical units managing functional safety. Therefore, security requirements play an essential role in creating a new feature or updating existing ones for solving security issues [29]. It is essential to understand security issues to address them by an appropriate set of security requirements sufficiently.

E. Safety-Security Interaction

Current standards focus on procedural aspects of safe and secure system development and leave much room for interpretation in terms of the technical characteristics of the solution being assessed. Individual, bespoke solutions increase both the documentation effort and associated assessment costs. Generic, secure system architecture will reduce costs due to its proven and standardized security features. This will be a welcome contribution to the competitiveness of the railway sector in the future.

However, safety and security can usually not be treated independently. Thus insufficient security measures may affect the safety of such a system. This becomes evident when considering the "adversarial attack" on tesla cars [30] in the automotive domain regarding autonomous vehicles and the disruption of railway signals in 2011 [31]. The active threat landscape in the railway domain [16], [32], [33] and the high impact of safety and security issues are defined as a trade-off between security and functional safety. Safety of the intended functionality will be made, and cyber-security measures potentially affecting safety shall be analyzed in detail.

IV. DISCUSSION AND CONCLUSION

Risk management for Cyber-Physical Systems of Systems is and will remain a major challenge. As multiple components have to be examined at the same time, risks can be of various origins and, therefore, differ in their impact. However, threat modelling is a practical approach in order to identify threats in the security analysis of CPSoS in the railway sector. While the adoption of IEC 62443-3-3 was an important step, there are still many open issues that need to be addressed (e.g. the way risks are measured is a highly contested factor). In terms of assessing the likelihood and impact of a threat, most common approaches (e.g. NIST SP800-30, ISO/IEC 27001) use qualitative measures. The advantage is simplicity, risk appetite and measurement of risk. Whereas, the disadvantage of the qualitative approach is its subjectivity and imprecision. As a result, various techniques involving probabilistic models have been proposed to solve these issues (e.g. OCTAVE, CVSS). However, the complexity of the analysis and the costly estimation of the probability of the threat event occurring, as well as, the impact value provide insufficient measures during the concept phase, as there is not enough data available. These aspects have made the application of a qualitative analysis in the form of DREAD beneficial to this work.

We have shown that threat modelling is a useful and efficient threat identification method for IoT framework communication. Moreover, based on our security analysis in Table 1, we have classified the identified threats into STRIDE categories and CIA^3 security objectives to show the highest impact. We identified the most frequently identified threats are identified in the area of integrity for the system Component identifiable data. In parallel, we have investigated which threats can be attributed to the system components by Analysing the data flow for each component. As result is that the component most affected by 21 identified threats is the autonomous rail vehicle. Table I displays that the tampering category suffers from 11 potential threats, indicating that the integrity attribute is violated the most. Similarly, we see that the attack vectors with the highest risk rate in Table II also fall in this area. We can conclude that the most vulnerable component is the autonomous vehicle and that special attention should be given to integrity and authorisation as a security objective.

V. Future Work

From a socio-technical perspective, research on trust and user vulnerability of the automated system is essential. For this, interviews with system users on security issues will be conducted to develop a concept of a hypothetical archetype of real users (persona) that can be imagined as a real person (name, age, personal habits, hobbies, emotions) which serves to express a certain user behaviour. In the next steps, the persona model and Roberta will allow us to make general deductions that will help us to describe attackers, threats to humans and machines, and also on humans and machines, at a general level. In the future, with this basis, it will be possible to have a model that makes it possible to discuss safety and security aspects comprehensively, independent of the current concrete project and occasion. Use cases depending on the product or application can be extended by these aspects in the modeling with the help of the Persona-Roberta model.

As a result, the interaction between the persona and the CPSoS might be depicted in the safety and security analysis. To evaluate its protection needs and risks and threats to the persona as a system component. Through this, multiple requirements and layers in the risk management processes can be analysed in-depth with socio-technical questions and targeted answers to design more efficient processes. Based on this, we will work on a novel approach that could allow us to integrate social aspects into the safety and security analysis to optimise resources in terms of effort and expenses.

In addition, we aim to integrate the ThreatGet tool [21] for the threat modeling process to define all existing security issues on the component and the asset level of the railway system design. Therefore, we will investigate an ontology-based reasoning approach for linking detected threats to an appropriate set of security requirements.

Acknowledgment

This work is supported by the Austrian Research Promotion Agency (FFG) and the fundings for BESTE-AB (contract no. 871551) from the ”Mobility of the Future” Programme, as well as BMK and BMDW.

References

[1] R. Kour, M. Aljumaili, R. Karim, and P. Tretten, “emaintenance in railways: Issues and challenges in cybersecurity,” *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, vol. 233, no. 10, pp. 1012–1022, 2019.

[2] P. Paganini, “Massive DDoS attack hit the Danish state rail operator DSB,” May 2018. [Online]. Available: https://securityaffairs.co/wordpress/72530/hacking/rail-operator-dsb-ddos.html

[3] G. Disterer, “Iso/iec 27000, 27001 and 27002 for information security management,” 2013.

[4] E. Aroms et al., “Nist special publication 800-30 risk management guide for information technology systems,” 2012.

[5] S. Radack, “Managing information security risk: organization, mission and information system view,” National Institute of Standards and Technology, Tech. Rep., 2011.

[6] Z. Ma and C. Schmittner, “Threat modeling for automotive security analysis,” *Advanced Science and Technology Letters*, vol. 139, pp. 333– 339, 2016.

[7] A. Bicaku, C. Schmittner, M. Tauber, and J. Delsing, “Monitoring industry 4.0 applications for security and safety standard compliance,” in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 2018, pp. 749–754.

[8] A. Bicaku, C. Schmittner, P. Rottmann, M. Tauber, and J. Delsing, “Security Safety and Organizational Standard Compliance in Cyber Physical Systems,” *Infocommunications Journal*, vol. XI, p. 2, Mar. 2019.

[9] International Electrotechnical Commission, “IEC 62443-3-3: Industrial communication networks – network and system security – part 3-3: System security requirements and security levels,” 2013.

[10] A. Bicaku, S. Maksuti, C. Hegedűs, M. Tauber, J. Delsing, and J. Eliasson, “Interacting with the arrowhead local cloud: On-boarding procedure,” in *2018 IEEE industrial cyber-physical systems (ICPS)*. IEEE, 2018, pp. 743–748.

[11] D. Kozma and P. Varga, “Supporting Digital Supply Chains by IoT Frameworks: Collaboration, Control, Combination,” *Infocommunications Journal*, pp. 22–32, Dec. 2020.

[12] S. Strobl, D. Hofbauer, C. Schmittner, S. Maksuti, M. Tauber, and J. Delsing, “Connected cars—threats, vulnerabilities and their impact,” in *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. IEEE, 2018, pp. 375–380.

[13] SAE, “Cybersecurity guidebook for cyber-physical vehicle systems j3061_201601,” https://www.sae.org/standards/content/j3061_201601/, (accessed on: March 12, 2021).

[14] M. Hamad and V. Prevelakis, “Savta: A hybrid vehicular threat model: Overview and case study,” *Information*, vol. 11, no. 5, p. 273, 2020.

[15] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, “Connected and autonomous vehicles: A cyber-risk classification framework,” *Transportation research part A: policy and practice*, vol. 124, pp. 523–536, 2019.

[16] C. Schmittner, P. Tummeltshammer, D. Hofbauer, A. M. Shaaban, M. Meidlinger, M. Tauber, A. Bonitz, R. Hametner, and M. Brandstetter, “Threat modeling in the railway domain,” in *International Conference on Reliability, Safety, and Security of Railway Systems*. Springer, 2019, pp. 261–271.

[17] International Electrotechnical Commission et al., “Iec 62443-4-2: 2019, security for industrial automation and control systems-part 4-2: Technical security requirements for iacs components,” 2019.

[18] A. M. Shaaban, E. Kristen, and C. Schmittner, “Application of IEC 62443 for IoT Components,” in *Computer Safety, Reliability, and Security*, ser. Lecture Notes in Computer Science, B. Gallina, A. Skavhaug, E. Schoitsch, and F. Bitsch, Eds. Cham: Springer International Publishing, 2018, pp. 214–223.

[19] ISO/TC 22/SC 32, ISO 26262 *Road vehicles - Functional safety*. ISO - International Standardization Organization, 2018.

[20] ——, ISO/PAS 21448 *Road vehicles — Safety of the intended functionality*. ISO - International Standardization Organization, 2019.

[21] C. Schmittner, S. Chlup, A. Fellner, G. Macher, and E. Brenner, “Threat-Get: Threat modeling based approach for automated and connected vehicle systems,” in *AmE 2020 - Automotive meets Electronics; 11th GMM-Symposium*, Mar. 2020, pp. 1–3.

[22] S. NIST, "800-12 rev. 1(2017),"*An Introduction to Information Security*, 2019.

[23] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," *Computers & Security*, vol. 53, pp. 65–78, 2015.

[24] G. Bakirtzis, B. T. Carter, C. R. Elks, and C. H. Fleming, "A model-based approach to security analysis for cyber-physical systems," in *2018 Annual IEEE International Systems conference (SysCon)*. IEEE, 2018, pp. 1–8.

[25] A. Shostack, *Threat modeling: designing for security*. Indianapolis, IN: Wiley, 2014, oCLC: 855043351.

[26] J. Meier, *Improving web application security: threats and countermeasures*. Microsoft press, 2003.

[27] A. M. Shaaban, T. Gruber, and C. Schmittner, "Ontology-based security tool for critical cyber-physical systems," in *Proceedings of the 23rd International Systems and Software Product Line Conference-Volume B*, 2019, pp. 207–210.

[28] B. Glas, J. Gramm, and P. Vembar, "Towards an information security framework for the automotive domain." *Automotive-Safety & Security 2014*, 2015.

[29] OWASP, "C1: Define security requirements," https://owasp.org/www-project-proactive-controls/v3/en/c1-security-requirements, 2018, (Accessed January 19, 2021).

[30] K. Hao, "Hackers trick a Tesla into veering into the wrong lane," Apr. 2020. [Online]. Available: https://www.technologyreview.com/2019/04/01/65915/hackers-trick-teslas-autopilot-into-veering-towards-oncoming-traffic/

[31] K. Zetter, "Hackers Breached Railway Network, Disrupted Service," Wired, Jan. 2012. [Online]. Available: https://www.wired.com/2012/01/railyway-hack/

[32] N. Ralston, "Preventing railway cyber attack," https://www.cyberbit.com/blog/ot-security/railway-cyber-attack/ 2019, (Accessed January 19, 2021).

[33] C. H. News, "Cyber incidents affecting railways - a threat to customer data," https://cyware.com/news/cyber-incidents-affecting-railways-a-threat-to-customer-data-a8d25ccc, 2020, (Accessed January 19, 2021).

George Matta BSc. received his Bachelor degree in IT Infrastructure Management in 2021 at the University of Applied Sciences Burgenland. In parallel to his studies he worked from 2019 until 2021 as a researcher at the research center Forschung Burgenland in the research field " Cloud and Cyber-Physical Systems Security ". His research activity include cybersecurity engineering, mainly in CPSoS secure communication and security requirements management processes driven by security standardizations (e.g., ISA/IEC 62443-series, ISO/IEC27000-series).

Sebastian Chlup MSc received his master's degree in computer science in 2020 at the University of Vienna. He has been working for the AIT Austrian Institute of Technology GmbH for more than 5 years in the department of Safety and Security. His main activities include cybersecurity engineering, developing a threat modeling tool and leading a national project in the railway domain.

BSc. MSc. Abdelkader Magdy Shaaban received his master's degree in computer engineering from the Arab Academy for Science, Technology and Maritime Transport in Alexandria, Egypt. Currently, he is a PhD candidate at the faculty of computer science at the University of Vienna and working at the AIT Austrian Institute of Technology. His research interests are in cybersecurity engineering, mainly in IoT and the automotive domain. He focuses on threat analysis and security requirements management processes driven by security standardizations (e.g., ISA/IEC 62443-series, ISO 21434, IEEE 1686, and ISO/IEC 27000-series).

Christoph Schmittner Received his M.Sc. in System and Software Engineering at the University of Applied Sciences Regensburg in 2013. His main research area is safety and security co-engineering. He works on safety, security analysis and co-analysis methods, connected and safety-critical / fault & intrusion tolerant system architectures, functional safety and cybersecurity standards and interdependence of safety and security in critical systems. He is a member of the Austrian mirror committees for ISO/TC 22 Road vehicles and IEC TC 56 Dependability and designated Austrian expert in corresponding international standardization groups (IEC 61508, IEC 62443 ISO 26262 and ISO/SAE 21434), member of TC65/WG20 "Industrial-process measurement, control and automation– Framework to bridge the requirements for safety and security", TC65/AHG2 "Reliability of Automation Devices and Systems" and TC65/AHG3 "Smart Manufacturing Framework and System Architecture" and coordinating the Austrian contribution to the development of ISO/SAE 21434 "road vehicles – cybersecurity engineering".

Dr Andreas Pinzenöhler is head of innovation management and new technologies at Austrian software company IQSOFT. He graduated in "Social and Economic Sciences" at Vienna University of Economics and Business. Already his Ph.D. thesis focused on implementation of open standards in combination with model driven development methodologies. After serving as university assistant at the beginning of his career he still fulfills teaching duties giving lectures on business process modeling at his alma mater. As a senior consultant at IQSOFT, more recently he focuses on process and technology consulting for infrastructure projects. He is actively participating in international standardization activities. He contributed to the UIC RailTopo model which provides a robust fundament for the development of joint vocabularies both for rail infrastructure and rail operations. Since 2017 as member of the IFC Rail Technical Services team he made substantial contributions to the infrastructure extension of the upcoming IFC 4.3 specification. IFC is the most successful open BIM standard.

DI Elke Szalai MA works as university lecturer and research associate at the University of Applied Sciences Burgenland. Current research and teaching focus: Technology&Society, SDGs, gender and diversity aspects as well as creative techniques in technology design.

Markus Tauber He works as Chief Scientific Officer at Research Studios Austria Forschungsgesellschaft mbH. Between 2015 until 2021, he worked as FH-Professor for the University of Applied Sciences Burgenland, where he held the position: director of the MSc program "Cloud Computing Engineering" and led the research center "Cloud and Cyber-Physical Systems Security". From 2012 until 2015, he coordinated the "High Assurance Cloud" research topic at the Austrian Institute of Technology (AIT) part of AIT's ICT-Security Program. Amongst the coordinator of the FP7 Project "Secure Cloud other activities, he was computing for CRitical infrastructure IT" - (www.seccrit.eu) and involved in the ARTEMIS Project Arrowhead. From 2004 to 2012, he was working at the University of St Andrews (UK), where he worked as a researcher on various topics in the area of network and distributed systems and was awarded a PhD in Computer Science for which he was working on "Autonomic Management in Distributed Storage Systems".

5G system throughput performance evaluation using Massive-MIMO technology with Cluster Delay Line channel model and non-line of sight scenarios

John Baghous

Abstract— **The fourth-generation system for mobile cellular communications (4G) has achieved great developments. The main problem here is that, with the passage of time and technical development, the need for new applications and services has emerged, and thus we need a new system that supports these matters in addition to the problems and limitations. One of the main challenges that the 4G system suffers from is the ability to support a larger number of devices, low latency, working in real time, provide greater capacity, in addition to providing a high data rate (bit rate) – hence 4G stands unable to support many new applications. This is what made researchers aspire to overcome these problems or reduce their impact to the maximum extent and this is what we expect to achieve in the new generation system (5G). In this research, a presentation was made of the 5G system regarding with one of its most important techniques (Massive MIMO technology), clarification of some concepts related to the study such as throughput and NLOS (Non-Line of Sight), as well as the channel model used. The results of the experiments were presented with the discussion.**

Index Terms—**(5G mobile networks), Massive MIMO technology, 5G channel models, NLOS scenario, 5G Throughput**

I. Introduction

Although wireless cellular technologies have been upgraded to the fourth generation, it still suffers from some problems, as it is unable to meet the requirements of many new use-cases. For example, the 4G network cannot handle massive mobile broadband requirements, and it is difficult to achieve Device-to-Device communication anywhere. It is also unable to support HD video transmission, high-quality audio, augmented reality, virtual reality and other services, so the 4G system has left some important unresolved problems, such as limited bandwidth, unlimited peripheral increase, limited data rate and more [1]. Therefore, new-generation wireless networks must be optimized to meet the demands of increasing data rate, improving capacity, reducing latency and improving quality of service. With the increasing demand from users, the 4G network will be extended (and then maybe replaced) by the 5G network with the help of some advanced technologies such as Massive MIMO, Device-to-Device communication, millimeter waves connections, beam division multiple access and others [2]. The goals of the 5G cellular communication system are to achieve an end-user data rate 10 to 100 times higher and this is the key here, as it ranges from 1 to 10 Gbps in dense urban environments. The 5G network may also support higher endpoint density: 5 to 10 times the connected devices in a given area. The energy efficiency in low-power dense machine communications need to improve more than ten times, so it is necessary to introduce new technologies in 5G system to achieve this matter [3]. The Massive MIMO technology attracted great interest in previous years and was considered one of the most promising and most important (radio-related) technologies in the 5G system by applying a large amount of antennas at the base station that can support many users in the same time frequency domain. It also possesses potential advantages for increasing the efficiency, improving the frequency spectrum, and facing channel fading [3, 4].

II. Methods and Experiments

Although mathematical, programming and simulation methods were used in the research behind this paper, but because of the inability to carry out experiments and take practical measurements on the ground, this was sufficed. After verifying the correctness and accuracy of the implementation and based on the mathematical comparison between the results obtained in the simulation and the equations used, this report was written in a summary.

Computers and appropriate software were used to obtain the results. I conducted a performance evaluation of the 5G system based on a series of comparisons to ascertain the extent of practical investigation of some theoretical issues.

In order to complete the work on this paper, I recommend that realistic measurements be made to compare them with my resulting standardized results to reach results that benefit workers in this field.

III. The Fifth Generation of Mobile Wireless Cellular Communications

The 4G cellular mobile technology has been published and gradual improvements are being made to it, but it has almost reached a state of maturity, so it is necessary to go to the new

John Baghous is with Faculty of Engineering, Damascus University (e-mail: john0baghous@gmail.com).

DOI: 10.36244/ICJ.2021.2.6

generation [5]. The 5G is the name of the new generation of mobile cellular wireless communications. As expected, this new system will provide high speeds ranging between 10 and 100 Gbps in the future. Moreover, this considered one of the most important strength foundations of this system. In addition to enough capacity that greater than previously and low delay, where the delay time that was provided by 4G system ranges between 40 and 60 ms, whereas in 5G the delay time will be between 1 and 10 ms. One of the main technologies that will be used in this system are Massive MIMO, that will have many benefits such as achieving an increase in capacity and throughput, Device-to-Device (D2D) communication, millimeter wave technology and some multi-access technologies such as Beam Division Multiple Access (BDMA).

It also plans to connect all equipment and terminals to the network to obtain what is called Internet of Things (IoT) and after that we are expected to become Internet for everything. Also, some of the connected terminals may need large amounts of data while others need small packets of them. Therefore, the bandwidth of this can be allocated adaptively, including improving the overall capacity of the system. Among the requirements and challenges of the 5G system are power efficiency, high reliability and availability, large capacity and low delay, given that the system deals with a high bit rate.

There is a major problem related to how to reduce the delay time and to support applications and provide services we need a delay of less than 1 ms [2]. The 5G network will not be a single system that relies on a single Radio Access Technology (RAT) similar to previous generations. Further, it is believed that the 5G network is a "network of networks". That is a heterogeneous system that includes a variety of radio interfaces and protocols frequency bands, access nodes, and different types of networks. This means that the 5G system will not be a single system that replaces the previous 4G system, but rather will combine all of the above and what is new. So, one of the main challenges will be the smooth integration between everything old and new [6].

The requirements for this system are expected to be met by the new spectrum that reaches the millimeter wavelength bands and use of the wide channel bandwidth available in the millimeter bands. Although the demand for data is increasing significantly, the usage patterns of this system are not only limited to the pattern of mobile broadband use, but it is expected to support a variety of usage scenarios classified into three broad categories [7]:

- Enhanced mobile broadband (eMBB)
- Ultra-reliable and low latency communications (URLLC)
- Massive machine type communications (mMTC)

In order to understand the engineering challenges facing this system concretely, and plan to meet them, it is necessary first defining their requirements, but it must be emphasized that it is not necessary to meet all these elements at one time, as different applications will put different requirements on performance. The following elements are the system's major requirements in each major dimension that must be met in certain situations: data rate, delay, power and cost, density [5].

The need for a higher data rate in all areas is receiving one of the greatest interests and this is discussed in this paper. Our view is that the improvements in 5G system will be achieved through combined gains in three categories [5]:

A. Increase density greatly to improve the spectral efficiency of the area and increase the number of active nodes within one area and frequency.
B. Increase the bandwidth, mainly by moving towards the wide spectrum and its capabilities, and also by making better use of the unlicensed spectrum of Wi-Fi in the 5 GHz range to obtain a larger frequency spectrum.
C. Increase spectral efficiency, primarily by advancing the MIMO rank, to achieve a higher throughput per channel and per node.

Using wider frequency range between certain number of nodes will not necessarily increase the achievable bandwidth. Other ideas not included in the above categories such as managing frequency interference through cooperation of base stations may contribute to the improvements, but the increase in capacity should come from the ideas in the above categories. One of the new things in the system is the issue of millimeter waves, whose range is between 30 and 300 GHz, with wavelengths ranging from 1 to 10 mm. This field of millimeter wave spectrum has not been used for a long time because, until recently, it was considered unsuitable for mobile communications due to its rather subtle and complex propagation characteristics, including high path loss, atmospheric and rain absorption, low diffraction around obstructions and weak penetration through various objects, due to strong phase noise. However, with progress and technical development, work is in progress to solve most of the cost and other related problems [5].

IV. THE MASSIVE MIMO TECHNOLOGY

The Multi-user Multiple-Input Multiple-Output (MIMO) technology provides significant advantages over traditional Point-to-Point MIMO technology [15] as it offers improvements in several aspects: increasing the data rate, enhancing reliability, improving power efficiency, reducing interference [8].

Due to the wide use of multimedia application services such as voice, writing, pictures, videos, Internet access, etc. In recent years, the demand for the rapid transmission of information and the reliability of communications through wireless communication systems has increased greatly, and to overcome these limitations we are going to use multiple antennas at the same time in transmission and reception. Transmission systems take advantage of the spatial dimension in order to transmit information. This technology is called Massive MIMO or Wide Field MIMO as it allows us to improve the throughput and performance of wireless links [9, 16]. This technology provides significant support to the system through the use of a large number of antennas with a time-dividing process. Multiple antennas help to focus power in consistently smaller areas to provide significant improvements in throughput, low latency, and radiated power efficiency [6]. Whereas the expected throughput depends on the propagation environment which provides orthogonal channels converging to the user terminals [8].

In MIMO technology, communication takes place in two ways: spatial diversity and spatial multiplexing. In spatial diversity, the same data travels over different paths and the data are received by multiple antennas and processed. Using this technology, we can improve the reliability of the link. The other technique is spatial multicast, where the data is divided into small parts and each part is transmitted through a different path and thus the transmission speed is increased at the expense of less reliability [2].

The MIMO system generally consists of a number of transmitting (M) and receiving (N) antennas and the communication channel through which the signal passes. Thus, the general equation for this technique is given by the equation (1) [2]:

$$Y = H.X + W \ (1)$$

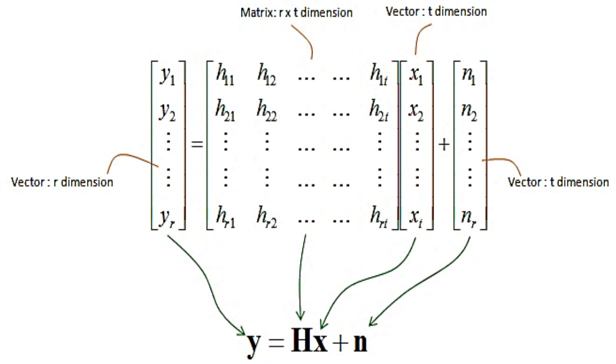

Matrix: r x t dimension
Vector : t dimension
Vector : r dimension
Vector : t dimension
y_1
y_2
y_r
h_{11} h_{12} … … h_{1t}
h_{21} h_{22} … … h_{2t}
h_{r1} h_{r2} … … h_{rt}
x_1
x_2
x_t
n_1
n_2
n_r
$\mathbf{y} = \mathbf{Hx} + \mathbf{n}$

Fig. 1. A Massive MIMO equation.

Where: Y=N×1 receiver matrix, H=N×M channel matrix, X=M×1 transmitter matrix and W is the noise. This is illustrated in Figure 1.

We have two scenarios for these networks, internal and external. For the external, the user terminal will communicate with the antennas distributed at the cell site, while the internal will be in cooperation with Wi-Fi technology, optical communications, and millimeter wave technology [2]. Figure 2 shows the Massive MIMO technology in a downlink condition.

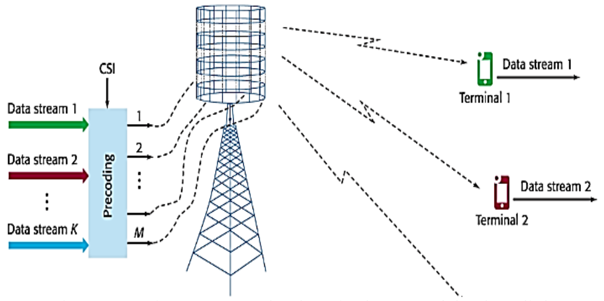


Fig. 2. Massive MIMO technology in the case of the downlink.

V. The Importance of Improving the Throughput

There are two basic facts: firstly, the demand for wireless productivity will always increase and secondly: the amount of available electromagnetic frequency spectrum will not increase. Taking into consideration that wireless communications are radically different from optical fiber communications, as more fibers can always be manufactured and put in place, and there is no doubt that any future optical demand will always be met. In contrast, there is no easy solution to wireless throughput [10]. The throughput is generally given to a given area by equation (2) [11]:

$$Area\ throughput\ \left(\frac{bps}{km^2}\right) = BW\ (Hz) \times Cell\ density\ \left(\frac{cells}{km^2}\right) \times$$
$$Spectral\ efficiency\ \left(\frac{\frac{bps}{Hz}}{cell}\right) (2)$$

Our basic wireless problem arises in the physical layer of how to reliably and uniformly provide increased overall wireless throughput across a given region [10].

The previous simple relationship, equation (2) shows that there are three main components that can be improved to achieve higher throughput [11, 10]:

1. More bandwidth can be allocated to 5G services.
2. The network can be condensed by adding more cells with access points operating independently.
3. The efficiency of data transmission (per cell and for a specified range of bandwidth) can also be improved and the use of multiple antennas at both the transmitting and receiving ends.

In this paper, Throughput has been calculated based on the bit rate equation of the 5G system shown in equation (3) [14]:

$$\text{Data Rate (Mbps)} =$$
$$10^{-6} \sum_{j=1}^{J} \left(\begin{array}{c} v_{Layers}^{(j)} \cdot Q_m^{(j)} . f^{(j)} . R_{max} \cdot \frac{N_{PRB}^{BW(j),u} .12}{T_s^u} \cdot \\ (1 - OH^{(j)}) \end{array} \right) (3)$$

where J is the number of aggregated component carriers in a band or band combination; R_{max}=948/1024; $v_{layers}^{(j)}$ is the maximum number of layers; $Q_m^{(j)}$ is the maximum modulation order and takes the following values (2 for QPSK, 4 for 16-QAM, 6 for 64-QAM, 8 for 256-QAM); $f^{(j)}$ is the scaling factor, the scaling factor can take the values 1, 0.8, 0.75, and 0.4. μ is the numerology (as defined in 3GPP TS 38.211) and can takes values from 0 to 5. T_S^{μ} is the average OFDM symbol duration in a subframe for numerology. $N_{PRB}^{BW(j),\mu}$ is the maximum RB allocation in bandwidth. $BW^{(j)}$ with numerology μ where $BW^{(j)}$ is the UE supported maximum bandwidth. $OH^{(j)}$ is the overhead and takes the following values:

- FR1 frequency range: DL: 0.14; UL: 0.08
- FR2 frequency range: DL: 0.18; UL: 0.1

VI. CHANNEL MODEL AND PROPAGATION SCENARIO

The Cluster Delay Line (CDL) channel model consists of a number of independent groups of delayed beams wherein each group contains a number of multiple path components that have the same known delay values but differ in departure angles and arrival angles. The beam angle difference may be different from the base station with respect to the mobile terminal and the displacement angles are Laplacian represented for each beam [12]. The CDL model takes into account all factors that affect the signal through the communication channel, in addition to the characteristics of the transmitting and receiving antennas. (Massive MIMO technology in this case.) In addition to the multi-path signal, where in the real environment, the received signal usually consists of a direct path and many paths, these paths differ in number and depend on the interaction between the electromagnetic wave and surrounding obstacles [12][13]. The signal obtained at the receiver (the receiving antenna) corresponds to the sum of these waves that reach the receiver with different delays [12]. In some environments, such as indoor, the Line-of-Sight (LOS) may not always be available. In this case, the Non-Line-of-Sight (NLOS) pathways allow communication as the signal in this case gets phase and amplitude changes. Figure 3. illustrates the concept of multipath propagation as well as the main propagation phenomena encountered [12].

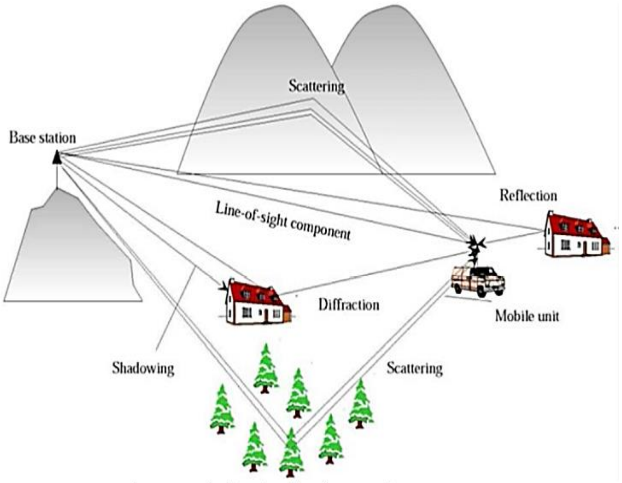


Fig. 3. The multipath propagation scenario.

This model was presented as one of the 5G models that were presented in 3GPP TR 38.901 version 14.0.0 Release [13]. As it supports a frequency range between 0.5 and 100 GHz and supports channel bandwidth up to 2 GHz, the propagation scenarios related to the NLOS are divided into 3 types, namely CDL-A, CDL-B and CDL-C [13]. We have shown that there are differences between the three models in terms of usage scenario [13]. All information such as formulas and tables can be found in [13].

TABLE I
PARAMETERS USED DURING SIMULATION

Parameter	Value
Code Rate	1/2
Modulation	16QAM
Subcarrier spacing (kHz)	30
Resource block	30
Layers	2
Number of sending frames	5
The number of transmitting antennas	8, 16, 32, 64, 128, 256
The number of receiving antennas	2, 4, 8, 16
Channel models	CDL-A. B. C
Parameter	value
Code Rate	1/2
Modulation	16QAM
Subcarrier spacing (kHz)	30
Resource block	30

VII. IMPLEMENTATION AND RESULTS

Specific parameters were used during the simulation process, which are shown in Table 1.

VIII. PRELIMINARY EXPERIMENTS

Here we will change the number of transmitting antennas (Tx) related to Massive MIMO technology to the following values: 8, 16, 32, 64, 128, 256 and keep the number of receiving antennas (Rx) equal to (2) and measure the extent to which this change affects the throughput performance. These experiments in three scenarios for the channel model used CDL-A, B, C will take a relationship between the system throughput and Signal-to-Noise (SNR) value and compare the results. In case CDL-A, we have Figure 4, in case CDL-B, we have Figure 5, and in case CDL-C, we have Figure 6.

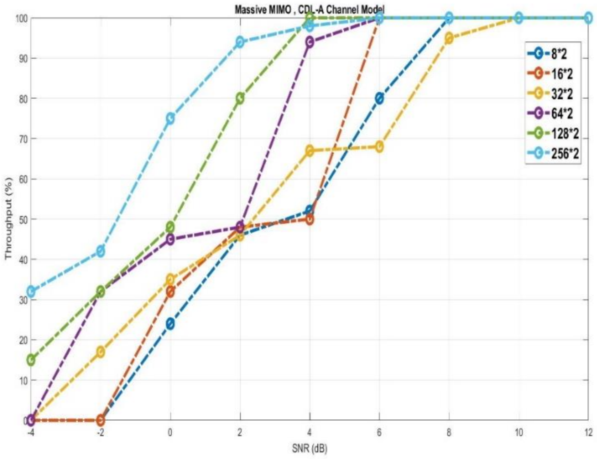


Fig. 4. System throughput with a number of antennas (8, 16, 32, 64, 128 and 256×2) with (CDL-A) channel model.

We will divide the notes and discussion on the previous figures into two parts: the first relates to Massive MIMO technology and the second relates to the channel model used.

With regard to the technology used, the increase in the number of transmit antennas array led to improved performance and consequently improved QOS for users. Technically, it can be said that increasing the number of transmit antennas array number contributed to an increase in the number of bits arrive to receiver, including an increase in the bit rate as this process contributes to improving the spectral efficiency of the system, that is, the number of transmitted bits/Hz.

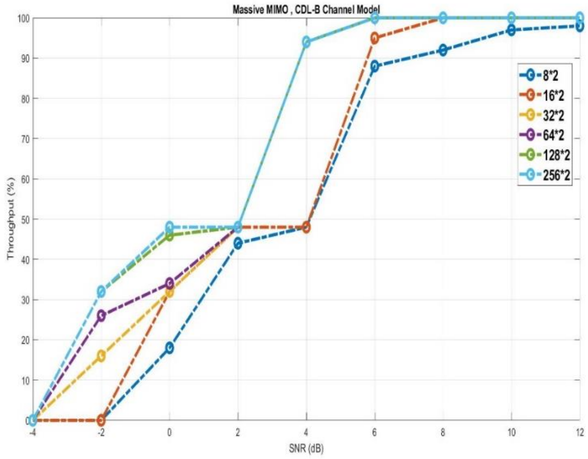


Fig. 5. System throughput with a number of antennas (8, 16, 32, 64, 128 and 256×2) with (CDL-B) channel model.

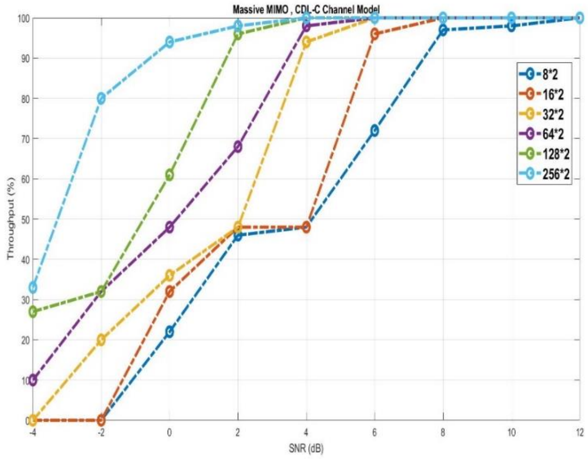


Fig. 6. System throughput with a number of antennas (8, 16, 32, 64, 128 and 256×2) with (CDL-C) channel model.

As for the channel models used, we notice from the previous figures that, the better performance of the system was in the case of the CDL-C model, then CDL-A, then CDL-B. As in case of the CDL-C model, the effect of increasing the number of antennas was very clear with the curves, while this clarity decreased in the CDL-A model and decreased further in the CDL-B model.

In general, the advantage of this technique is to obtain higher system throughput at lower SNR values, that is, to obtain good performance under difficult ambient conditions and big noise.

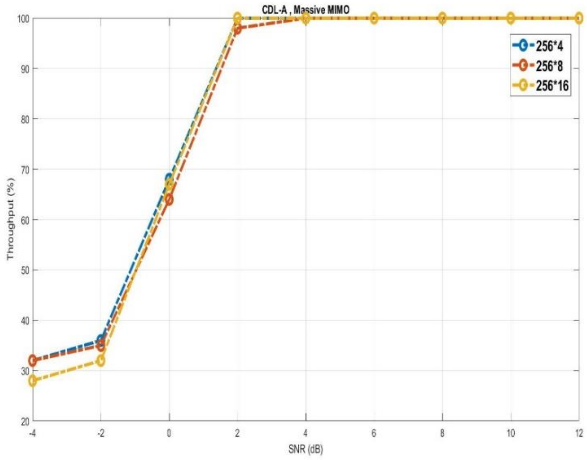


Fig. 7. System throughput with a number of antennas (256×4, 256×8, 256×16) with (CDL-A) channel model.

IX. Increasing the Receiver Antennas Number

In this section, the simulation process is presented to increase the number of receiving antennas while the number of transmitting antennas remains constant with the effect of that on throughput, the amount of bits reached to the user.

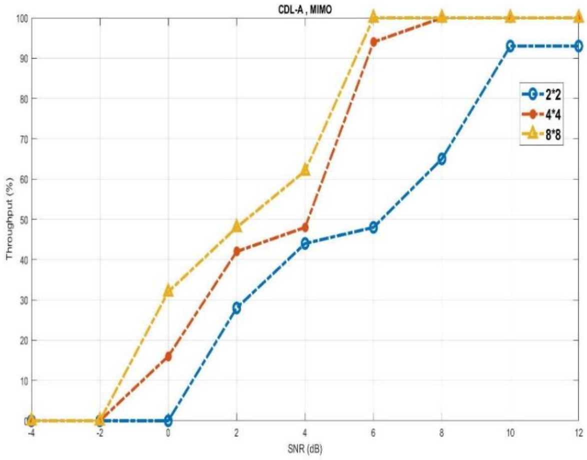


Fig. 8. System throughput with a number of antennas (2×2, 4×4, 8×8) with (CDL-C) channel model.

As we see in Figure 7, The effect of increasing the number of receiving antennas did not appear clearly and it may appear if we raise the number to greater values up to 256, and this matter requires an advanced computer with high and modern capabilities and may take a longer time to implement the operation with the increase in the number of antennas.

X. System Performance when Using MIMO

In this section, the case of using normal MIMO is presented as we see in Figure 8, which the number of antennas is low and not dense as in the case of the latest technology of MIMO. When comparing this figure with the other previous figures we note that the throughput was non-existent at low SNR values. In addition, the throughput did not reach the upper limit only with an increase in the SNR ratio to high limits unlike cases in which the number of antennas was more.

XI. Discussion

The previously shown simulations can be divided into three types. In the first case, we demonstrated the effect of increasing the number of transmitting antennas with the constant number of receiving antennas on the system's throughput performance. As is evident, the increase in the number of antennas leads to improved performance by obtaining higher throughput at a lower SNR value. This is a very important improvement because with the increase in the throughput, the spectral efficiency also increases and thus we will have an improvement in the system performance.

In the second case, we increased the number of receiving antennas under the scenario of the CDL-A channel model as an example, and the case showed a convergence in the performance of the throughput curves.

In the third case, we experimented with the use of MIMO technology with fewer antennas at both ends of the communication, in the case of using the CDL-C channel model as an example. In addition, we noticed a clear difference in throughput between this case and the case of Massive MIMO technology. We obtained higher throughput rates in the case of Massive MIMO compared to MIMO case.

XII. Conclusion and Future Work

We notice from the previous results that the throughput of the system has improved with the use of Massive MIMO technology. Further, with the improvement of throughput, we will obtain higher values of bit rate at lower SNR values, and we will obtain an improvement in the spectral efficiency. Accordingly, we notice an improvement in the performance of the studied system, and from it, this modern technology will leave its effective impact on the ground and improve the user experience.

In the future, we are looking forward to conduct further experiments on 5G system, in addition to study other parameters and technologies related to this system, and we are looking forward to develop in this regard.

References

[1] Ni, Shanjin. "The Key Technologies in Physical Layer of 5G Wireless Communications". Research Gate. 2017.

[2] Hussain, S. S., Yaseen, S. M., & Barman, K. "An Overview of Massive MIMO System in 5G". International Science Press, IJCTA, 2016. pp. 4957.

[3] Zheng, K., Leung, V. C., Yang, L. L., & Chatzimisios, P. "Guest Editorial Special Issue on 5G Wireless Systems with Massive MIMO". *IEEE Systems Journal*, vol.11, n. 1, 4-6. 2017. DOI: 10.1109/JSYST.2017.2651338.

[4] Liang, W., Wang, Y., Li, B., Wang, W., Sheng, J., Han, Y. & Kishiyama, Y.. "Ultra-high-Throughput Massive MIMO field-trial over radio computing architecture with peak spectrum efficiency of 79.82 bps/Hz". In 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) (pp. 1-7). *IEEE*. 2017, October. DOI: 10.1109/PIMRC.2017.8292309.

[5] Andrews, J. G., Buzzi, S., Choi, W., Hanly, S. V., Lozano, A., Soong, A. C., & Zhang, J. C." What will 5G be?" *IEEE Journal on selected areas in communications*, vol. 32, n. 6, 1065-1082. 2014. DOI: 10.1109/JSAC.2014.2328098

[6] Chávez-Santiago, R., Szydełko, M., Kliks, A., Foukalas, F., Haddad, Y., Nolan, K. E. & Balasingham, I. "5G: The convergence of wireless communications". *Wireless Personal Communications*, vol. 83, n. 3, 1617- 1642. 2015. DOI: 10.1007/s11277-015-2467-2.

[7] Shafi, M., Molisch, A. F., Smith, P. J., Haustein, T., Zhu, P., De Silva, P., Tufvesson, F., Benjebbour, A. & Wunder, G. "5G: A tutorial overview of standards, trials, challenges, deployment, and practice". *IEEE journal on selected areas in communications*, vol. 35, n. 6, 1201-1221. 2017. DOI: 10.1109/JSAC.2017.2692307.

[8] Larsson, E. G., Edfors, O., Tufvesson, F., & Marzetta, T. L. "Massive MIMO for next generation wireless systems". *IEEE communications magazine*, vol. 52, n. 2, 186-195. 2014. DOI: 10.1109/MCOM.2014.6736761.

[9] Riadi, A., Boulouird, M., & Hassani, M. M. R. "An Overview of Massive-MIMO in 5G Wireless Communications". In *Colloque International TELECOM* (pp. 10-12). 2017, May.

[10] Marzetta, T. L. "Massive MIMO: an introduction". *Bell Labs Technical Journal*, vol. 20, 11-22. 2015. DOI: 10.15325/BLTJ.2015.2407793.

[11] Ed. Wei Xiang, Kan Zheng, Xuemin (Sherman) Shen, "Part of: 5G Mobile Communications", pp. 77-116. ISBN: 978-3-319-34206-1. 2017. DOI: 10.1007/978-3-319-34208-5_4.

[12] Belhabib, M. "Investigation on radio channel over the air emulation by multi-probe setup" (*Doctoral dissertation, Université Rennes 1*). 2017.

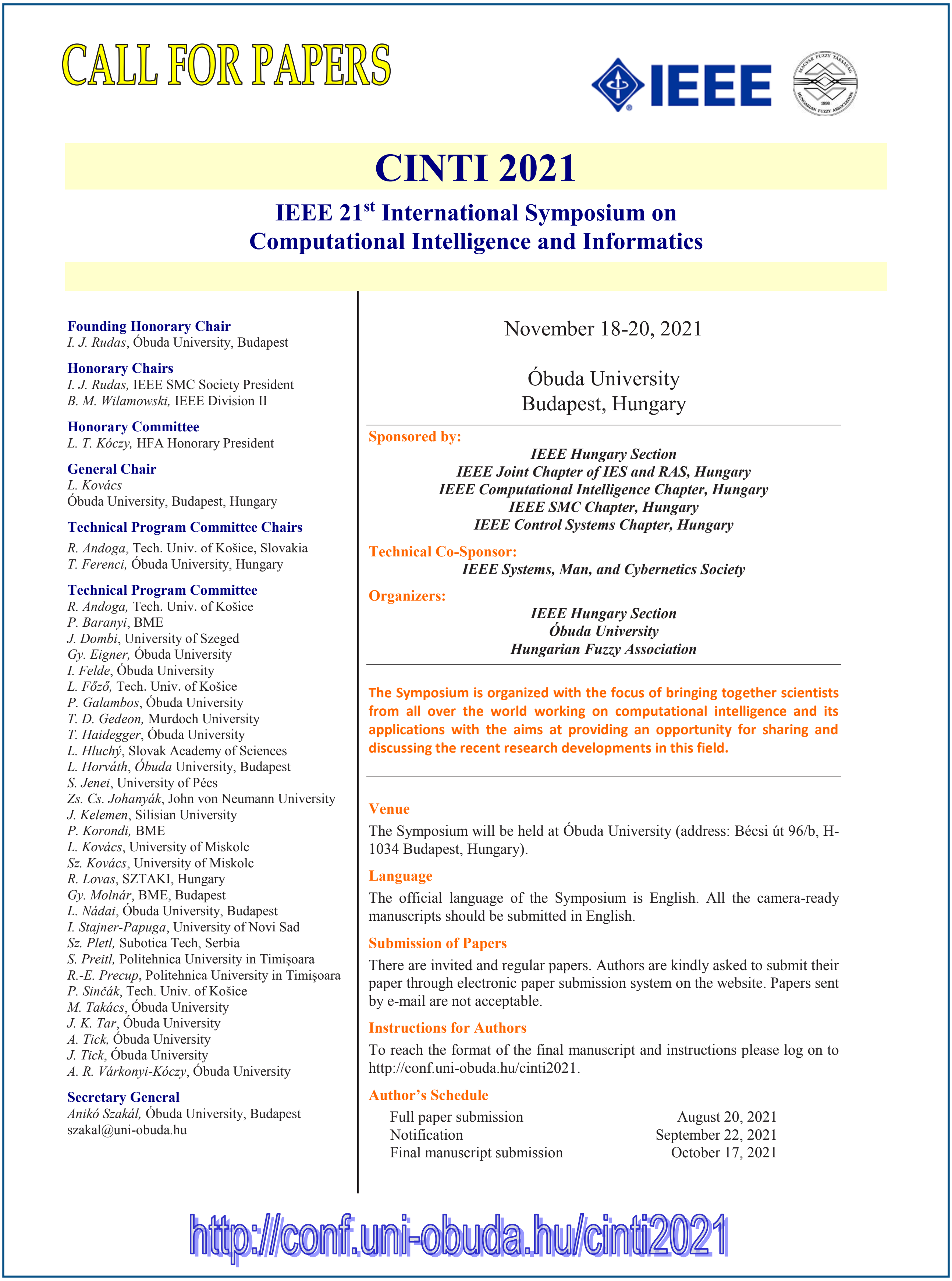
[13] 3GPP TR, "5G; Study on channel model for frequencies from 0.5 to 100 GHz", *ETSI*, 3GPP TR 38.901 version 14.0.0 Release. 2017.

[14] 3GPP TR, "5G-NR-User Equipment (UE) radio access capabilities", *ETSI*, 3GPP TS 38.306 version 15.3.0 Release 1.2018.

[15] Ladvánszky, J. "Detection of 2x2 MIMO signals". *INFOCOMMUNICATIONS JOURNAL*, vol. 12, n. 3, 24-30. 2020. DOI: 10.36244/ICJ.2020.3.4

[16] Csathó, B. T., Horváth, B. P., & Horváth, P. Modeling the near-field of extremely large aperture arrays in massive MIMO systems. *INFOCOMMUNICATIONS JOURNAL*, vol. 12, n. 3, 39-46. 2020. DOI: 10.36244/ICJ.2020.3.6.

John Baghous obtained license degree in Telecommunication and electronic Engineering, master degree in Advanced Telecommunication Engineering, from Faculty of Engineering, Damascus University, lecturer at the university. Interested in all types of telecommunication systems especially mobile (4G, 5G ...etc.), wireless, WLAN, Wi-Fi, Li-Fi. Bluetooth etc.



CALL FOR PAPERS

CINTI 2021

IEEE 21st International Symposium on Computational Intelligence and Informatics

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

Honorary Chairs
I. J. Rudas, IEEE SMC Society President
B. M. Wilamowski, IEEE Division II

Honorary Committee
L. T. Kóczy, HFA Honorary President

General Chair
L. Kovács
Óbuda University, Budapest, Hungary

Technical Program Committee Chairs
R. Andoga, Tech. Univ. of Košice, Slovakia
T. Ferenci, Óbuda University, Hungary

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

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

November 18-20, 2021

Óbuda University
Budapest, Hungary

Sponsored by:

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

Technical Co-Sponsor:

IEEE Systems, Man, and Cybernetics Society

Organizers:

IEEE Hungary Section
Óbuda University
Hungarian Fuzzy Association

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

Venue

The Symposium will be held at Óbuda University (address: Bécsi út 96/b, H-1034 Budapest, Hungary).

Language

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

Submission of Papers

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

Instructions for Authors

To reach the format of the final manuscript and instructions please log on to http://conf.uni-obuda.hu/cinti2021.

Author's Schedule

Full paper submission	August 20, 2021
Notification	September 22, 2021
Final manuscript submission	October 17, 2021

http://conf.uni-obuda.hu/cinti2021

IEEE/IFIP Network Operations and Management Symposium

25-29 April 2022 // Budapest, Hungary

IEEE | IEEE ComSoc IEEE Communications Society

CALL FOR PAPERS

The 18th IEEE/IFIP Network Operations and Management Symposium (NOMS 2022) will be held on 25-29 April 2022 in Budapest, Hungary. Held in even-numbered years since 1988, NOMS 2022 will follow the 34 years tradition of NOMS and IM as the primary IEEE Communications Society's forum for technical exchange on management of information and communication technology focusing on research, development, integration, standards, service provisioning, and user communities. The theme of NOMS 2022 is Management in the Age of Softwarization and Artificial Intelligence. It aims to capture recent results, emerging approaches and technical solutions for dealing with the management of Fixed and Mobile Networks and Services, Clouds, and Vertical Eco-Systems (e.g., smart cities and smart transportations). NOMS 2022 will offer various types of sessions: keynotes, technical, experience, demo, tutorial, poster, panel, and dissertation. Topics of interest include, but are not limited to, the following:

Management of 6G Networks and Network 2030

- Softwarization and management for extreme performance networking, such as very low latency and ultra-high peak data rate
- APIs, multi-domain orchestration, interoperability methods and algorithms for the softwarized networks and management in 6G
- Softwarization and management of the deterministic networks, of the high-precision networks
- Softwarization and management of the converged infrastructures: integration of data spaces with compute cloud networks and connectivity networks
- Methods/algorithms/APIs for control and management of addressing and routing for Network 2030
- Precision telemetry, Management of multi-domain services in 6G
- High-Precision networking services using Fog and Edge Computing
- Service assurance for precision micro services
- In-network service level optimization; predictable KPIs and QoS
- Management of Data Spaces, Management of Meta-data, Management of Data Identity
- Transition scenarios from existing networks to network 2030

Management of Smart Vertical Systems in the Industry 4.0 Era

- Smart Cities, Smart Grid, Smart Homes, Smart Environment, Smart Manufacturing, Smart Energy
- Internet of Things (IoT)
- 5G& 6G networking practices and principles
- Social Networks
- Cyber-Physical Systems including techniques supported with Augmented Reality, Virtual Reality, Mixed Reality, Physical vs. Digital Twins
- Applications and case studies

Artificial Intelligence Techniques for Network and Service Management

- Management with AI
- Artificial Neural Networks
- Machine Learning & Deep Learning
- Big Data & Data Mining
- Mobile Agents
- AI vs. legacy optimization methods in management

Management of Softwarised Networks, Software-Defined Networking, Network Function Virtualization, Service Function Chaining

- Network virtualization
- Control plane programmability
- Cloud Network (data, control, management planes) programmability
- Methods and frameworks enabling customized functions on data packets and processes to program the header of the packets
- Cloud Network Slicing in 5G & 6G
- Management & Orchestration (MANO)
- Service Function Chaining
- Protocols, languages, and frameworks
- Open-source networking
- Cloud-native networking
- Case studies and practical deployments

Management Functions and Practical Approaches

- FCAPS: Fault, Configuration, Accounting, Performance and Security Management
- Cybersystems, Security and Reliability in Network Softwarization and Management
- Green operation & management
- Billing & Accounting
- Service Assurance
- Service Fulfillment
- Service Level Management

Network Management & Operational Experience

- Ad-hoc networks
- Automotive and Vehicular networks
- Broadband access networks
- Cognitive Radio networks
- e-Maintenance
- Future Internet
- Heterogeneous networks
- Home networks
- M2M networks
- OSS/BSS development
- Overlay networks
- Personal area networks
- Sensor networks
- Wireless and mobile networks

Service Management

- Business management
- Clouds
- Data center management
- Data service management
- Hosting
- Infrastructure as a Service, Management as a Service, Platform as a Service, Software as a Service
- IT service management
- Managed service provisioning
- Multimedia service management
- OTT service management
- Virtualized infrastructure management
- Security Management
- Intrusion detection, intrusion prevention, intrusion response
- Network security
- Security for peer-to-peer and overlay networks
- Security for smart X and large systems and critical infrastructures
- Privacy and anonymity
- Vulnerability management
- Early warning

Modelling, Measurement and Performance Analysis

- Performance measurements and evaluation, monitoring, data analytics, validation and debugging for network management and softwarized networks, digital twinning
- Network and service qualities, performance, reliability, scalability, elasticity, resilience, sustainability, maintainability, safety, and security with guarantees
- Protocols and methods for delivery of high precision services with Key Performance Indicators (KPIs) guarantee
- Profiling and performance evaluation of softwarized network functions/components
- Debugging of softwarized networks
- High precision networking, precision telemetry, management of cyber-networking systems supporting physical/digital twins

Methodologies for Network Operations and Management

- Management and operation of high-precision networks and services
- Control theory
- Markov Chains and management
- Data collection and aggregation
- Digital twining
- Design and simulation
- Economic/finance theories
- Experimental approaches
- Optimization theory
- Probability and stochastic processes, queuing theory
- Risk management
- Software engineering methodologies Visualization
- Management approaches for Quantum Networking

Management Approaches, Resources and Functions

- Management architectures, Softwarized network architectures/ Infrastructures
- Networking, Edge cloud-native networking,Time-Sensitive Networking and IP convergence, Deterministic Networking, IoT-Edge-Cloud Network Continuum
- End-to-end and multi-domain softwarized networks, multi-domain management, green operations and management, management of energy-efficient networks and datacenters
- Network and cloud network operating systems facilities, resource abstraction, connectors and adaptation, capability and operation exposure, network functions, cloud-native functions
- Dynamic migration of network functions, interfaces, deployment and integration with software-based control, management, and orchestration
- Resource allocation mechanisms for deterministic data transmission and networking
- Microservices, serverless computing, secured containers infrastructure and new software paradigms for managing and operating network functions
- Standard frameworks and systems
- Integrated management
- Autonomic and self-management
- Blockchain Networking
- Zero-Configuration Networking, Closed-loop operations, Self-Driving Networking, Intent-based Management, Smart Networks, Zero-Trust Networking
- Best practices and management standards
- Centralized management
- Distributed management
- Organizational aspects
- Policy-based management
- Process-oriented management
- IT service management (ITSM)
- Process engineering and frameworks (ITIL, CobIT, RiskIT, ValIT)

Management Efforts for Pandemics and Crisis Situations (COVID-19)

- Contact and Activity Tracing
- Network/Service Management Support
- Network Measurements
- Network Adaptation

Case Studies, Testbeds and Practical Experiences

IMPORTANT DATES

Paper Submission Deadline: 20 September 2021
Notification of Acceptance: 17 December 2021
Camera-Ready Submission: 14 January 2022

GENERAL CO-CHAIRS

Pal Varga (Budapest University of Technology and Economics, Hungary)
Lisandro Zambenedetti Granville (UFRGS, Brazil)

TECHNICAL PROGRAM COMMITTEE CO-CHAIRS

Alex Galis (UCL, UK)
Istvan Godor (Ericsson, Hungary)
Michele Nogueira (UFMG, Brazil)

For more information, please visit http://noms2022.ieee-noms.org

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

IEEE International Conference on Communications

16-20 May 2022 // Seoul, Korea

Intelligent Connectivity for Smart World

CALL FOR PAPERS AND PROPOSALS

The 2022 **IEEE International Conference on Communications** (ICC) will be held in the world famous Gangnam district which is the most vibrant part of the city of Seoul, Korea, from 16 to 20 May 2022. Themed "Intelligent Connectivity for Smart World," this flagship conference of the IEEE Communications Society will feature a comprehensive high-quality technical program including 13 symposia and a variety of tutorials and workshops. IEEE ICC 2022 will also include an attractive industry program aimed at practitioners, with keynotes and panels from prominent research, industry and government leaders, business and industry panels, and technological exhibits.

TECHNICAL SYMPOSIA

- IoT & Sensor Networks
- Cognitive Radio & AI-Enabled Networks
- Communication & Information System Security
- Communication QoS, Reliability, & Modeling
- Communication Software & Multimedia
- Communication Theory
- Green Communication Systems & Networks
- Mobile & Wireless Networks
- Next-Generation Networking & Internet
- Optical Networks & Systems
- Signal Processing for Communications
- Wireless Communications
- Selected Areas in Communications
  - *Big Data*
  - *Cloud Computing, Networking and Storage*
  - *e-Health*
  - *Molecular, Biological and Multi-Scale Communications*
  - *Satellite & Space Communications*
  - *Smart Grid Communications*
  - *Social Networks*
  - *Machine Learning for Communications*
  - *Backhaul/Fronthaul Networking and Communications*
  - *Aerial Communications*
  - *Quantum Communications & Computing*
  - *Full-Duplex Communications*

INDUSTRY FORUMS AND EXHIBITION PROGRAM

Proposals are sought for forums, panels, presentations and demos, specifically related to issues facing the broader communications and networking industries.

TUTORIALS

Proposals are invited for half- or full-day tutorials in all communication and networking topics.

WORKSHOPS

Proposals are invited for half- or full-day workshops in all communication and networking topics.

icc2022.ieee-icc.org

IMPORTANT DATES

Paper Submission
11 October 2021

Tutorial Proposals
4 October 2021

Acceptance Notification
18 January 2022

Workshop Proposals
2 August 2021

Camera-Ready
15 February 2022

Industry Forum Proposals
13 December 2021

ORGANIZING COMMITTEE

General Chair
Dong In Kim (Sungkyunkwan University, Korea)

General Co-Chair
Seung Chan Bang (ETRI, Korea)

General Vice Chair
Yoan Shin (KICS, Korea)

Technical Program Chair
Ekram Hossain (University of Manitoba, Canada)

Technical Program Co-Chairs
Inkyu Lee (Korea University, Korea)
Petar Popovski (Aalborg University, Denmark)

Workshop Co-Chairs
Wan Choi (Seoul National University, Korea)
Bruno Clerckx (Imperial College London, UK)
Erik G. Larsson (Linköping University, Sweden)

Tutorials Co-Chairs
Byonghyo Shim (Seoul National University, Korea)
Rath Vannithamby (Intel, USA)
Rui Zhang (National University of Singapore, Singapore)

Industry Forums and Exhibition Chair
James Won-Ki Hong (POSTECH, Korea)

Industry Forums and Exhibition Co-Chairs
Sunghyun Choi (Samsung Electronics, Korea)
Byoung-Hoon Kim (LG Electronics, Korea)
Anthony C. K. Soong (Futurewei Technologies, USA)

IEEE ComSoc®
IEEE Communications Society
IEEE

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*