Infocommunications Journal

A PUBLICATION OF THE SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS (HTE)

December 2022 Volume XIV Number 4 ISSN 2061-2079

MESSAGE FROM THE EDITOR-IN-CHIEF

Recent advances on high performance computing, mobile networking, and security ..... *Pal Varga* 1

Our reviewers in 2022 2

PAPERS FROM OPEN CALL

A New Gateway Selection Algorithm Based on Multi-Objective Integer Programming and Reinforcement Learning ..... *Hasanain Alabbas, and Árpád Huszák* 4

Evaluation of the HoloLens for Medical Applications Using 5G-connected Mobile Devices ..... *György Wersényi* 11

DITIS: A Distributed Tiered Storage Simulator. ..... *Edson Ramiro Lucas Filho, Lambros Odysseos, Yang Lun, Fu Kebo, and Herodotos Herodotou* 18

FiLiP: A File Lifecycle-based Profiler for hierarchical storage ..... *Adrian Khelili, Sophie Robert, and Soraya Zertal* 26

Saving Bit-flips through Smart Overwrites in NVRAM ..... *Arockia David Roy Kulandai, and Thomas Schwarz* 34

Exact Outage Analysis for Non-regenerative Secure Cooperation Against Double-tap Eavesdropping ..... *Kotha Venugopalachary, Deepak Mishra, and Ravikant Saini* 42

BER-Aware Backscattering Design for Energy Maximization at RFID Passive Tag. ..... *Amus Chee Yuen Goay, Deepak Mishra, and Aruna Seneviratne* 49

LoRa Positioning in Verification of Location Data's Credibility ..... *Anna Strzoda, Rafał Marjasz, and Krzysztof Grochla* 56

Using Dynamic Programming to Optimize Cellular Networks Modeled as Graphical Games ..... *Artur Popławski, and Szymon Szott* 62

Review of Some Recent European Cybersecurity Research and Innovation Projects ..... *Mehmet Ufuk Çağlayan* 70

A Fine-grained Dynamic Access Control Method for Power IoT Based on Kformer ..... *Rixuan Qiu, Xue Xue, Mingliang Chen, Jinkun Zheng, Sitong Jing, and Yuancheng Li* 79

CALL FOR PAPER / PARTICIPATION

ICC 2023 / IEEE International Conference on Communications IEEE ICC 2023, Roma, Italy 86

IEEE HPSR 2023 / IEEE International Conference on High Performance Switching and Routing IEEE HPSR 2023, Albuquerque, NM, USA 87

IECON 2023 / 49th Annual Conference of the IEEE Industrial Electronics Society IECON IEEE IES 2023, Singapore 89

ADDITIONAL

Guidelines for our Authors 88

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

Recent advances on high performance computing, mobile networking, and security

Pal Varga

WE have reached the end of this turbulent year of 2022. In terms of scientific achievements, it was a successful one for our community: the journal never received so many – close to 150 – individual submissions within a calendar year before. This is certainly due to three factors. The first reason is, of course, the continuously and visibly improving journal metrics. Second, the two calls for special issue papers: on Internet of Digital & Cognitive Realities and on Tech-Augmented Legal Environment. Third, the activities of the Editorial Board, which helped a lot in attracting great papers. As the Infocommunications Journal is listed in the Web of Science: Emerging Sources Citation Index, we became eligible for an official Impact Factor calculated by Clarivate, already for the year 2022 – the actual value will be announced in June 2023. We are very positive that this value will be very attractive, and its announcement in June provides our Journal even better visibility than we have now.

Let us have a brief overview of the articles included in the last issue of the Infocommunications Journal for the year 2022.

In the first paper of this issue, H. Alabbas and Á. Huszák propose a novel gateway selection algorithm for vehicular networks in urban areas. Their method consists of two phases: at first it identifies the best available gateways using multiobjective integer programming, after which it selects the most suitable gateway for the given vehicular nodes, by using reinforcement learning.

Augmented Reality and related technologies are in the focus of attention for many application domains – including healthcare. In his paper, György Wersényi investigates the usability of the HoloLens device for medical applications. He evaluates the HoloLens usage, especially regarding latency and throughput, and finds that at this stage, it is very useful for education, training, or teleassistance, but not yet reliable enough for latency-sensitive tasks.

In their paper, Edson Ramiro Lucas Filho and his coauthors present a comprehensive simulator for distributed and tiered file-based storage system, DITIS. It is able to accurately simulate the distributed file system behaviors, taking into account the performance characteristics of each node. This understanding of the underlying behavior and effects of these systems brings multiple benefits to users – as shown here.

Regarding profiling hierarchical storage, A. Khelili, S. Robert and S. Zertal present FiLiP, which provides statistics and metrics for better understanding the performance behind application file access and file movements across hierarchical storage. The authors highlight the feasibility of FiLiP by demonstrating its results on various I/O-intensive highperformance computing applications.

Adding to hardware performance tweaks, A.D.R. Kulandai and T. Schwarz present a new strategy on how to select memory locations for overwrites that result in a lower number of bit-flips. They apply this method on non-volatile random access memories (NVRAMs), and calculate the expected bitflip savings for the new strategy, so they can determine rules for finding the best candidate memory locations.

In their paper, K. Venugopalachary, D. Mishra and R. Saini investigate the exact and secrecy outage possibilities of aamplify-and-forward cooperative communication systems while passive external monitoring (or eavesdropping) is present. As a result, the authors provide the close-form expressions for probabilities of secrecy outage and secrecy intercept, which are then validated through simulations.

The problem of output load power maximization with optimal load impedances selection for RFID tags is in the focus of the study by A.C.Y. Goay, D. Mishra and A. Seneviratne. They investigate this topic for BER-aware backscatter communication, where the tag uses binary ASK. The proposed design provides a gain of cca. 16%, which is a significant argument in favor of utilizing this method.

Zooming out to communication systems, A. Strzoda, R. Marjasz and K. Grochla evaluate LoRa localization capabilities and data credibility. They found that although trilateration has limited accuracy, the LoRa measurement can still be very well used for evaluating the credibility of the location information.

In their paper, Artur Poplawski and Szymon Szott represent certain cellular network models as graphical games, and use dynamic programming for optimizing it. They demonstrate the idea through the game on interference in the radio access network, and verify the feasibility through simulations.

A review of current activities in European cybersecurity research and innovation is presented by Mehmet Ufuk Caglayan Among others, it specifically reviews the projects NEMESYS, SDK4ED, KONFIDO, GHOST, SerIoT, IoTAC and their sidelobe research and innovation initiatives.

As the closing paper of this issue, Rixuan Qiu and his coauthors propose a Kformer-based fine-grained dynamic access control method to automate authorization management tasks. The presented experimental results show that KFormer is feasible for the tasks, stable, and has high accuracy.

With this overview, we wish you a great turn of 2022/23, with pleasant reads of the papers of the current issue.

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

Our reviewers in 2022

The quality of a research journal depends largely on its reviewing process and, first of all, on the professional service of its reviewers. It is my pleasure to publish the list of our reviewers of 20 countries from 4 continents in 2022 and would like to express my gratitude to them for their devoted work.

Your Editor-in-Chief

Alija Pasic
BME, Hungary

Dániel Kozma
BME, Hungary

Attila Frankó
AITIA International Inc., BME, Hungary

Pal Varga
BME, Hungary

Gusztáv Adamis
BME, Hungary

Ruba Almahasneh
BME, Hungary

Sara Alouf
University of Paris Saclay, France

Mohammed Salah Al-Radhi
BME, Hungary

Jonatha Anselmi
INRIA, France

László Bacsárdi
BME, Hungary

Simonetta Balsamo
University of Venice Ca' Foscari, Italy

Máté Bancsics
BME, Hungary

József Barta
Ericsson, Hungary

Gilles Bernot
University of Nice Cote d'Azur, France

Gergely Biczók
BME, Hungary

József Bíró
BME, Hungary

Ulf Bodin
Lulea University of Technology, Sweden

György Bognár
BME, Hungary

Jalil Boukhobza
ENSTA-Bretagne, France

Ashima Chawla
Athlone Institute of Technology, Ireland

Tibor Csöndes
Ericsson, Hungary

László Csurgai-Horváth
BME, Hungary

Tadeusz Czachorski
Instititute of Theoretical and Applied Informatics, Polish Academy of Sciences, Poland

Márton Czermann
BME, Hungary

Tien Van Do
BME, Hungary

Taha Elwi
Al-Ma'moon University College, Iraq

Hiroyuki Endo
National Institute of ICT, Japan

Károly Farkas
BME, Hungary

Andrea Farkasvölgyi
BME, Hungary

Hassan Farran
BME, Hungary

Tibor Fegyó
BME, Hungary

Bruno Gaujal
INRIA, France

Erol Gelenbe
Instititute of Theoretical and Applied Informatics, Polish Academy of Sciences, Poland

László Gönczy
BME, Hungary

Krysztof Grochla
Instititute of Theoretical and Applied Informatics, Polish Academy of Sciences, Poland

András Gulyás
BME, Hungary

Gábor Háden
ELKH TTK, Hungary

Csaba Hegedűs
AVAYA, Hungary

Attila Hilt
Nokia Networks, Hungary

Gergely László Hollósi
BME, Hungary

Benny van Houdt
University of Antwerp, Belgium

Bálint Horváth
BME, Hungary

Péter Horváth
BME, Hungary

Martin Husák
Masaryk University, Czech Republic

Árpád Huszák
BME, Hungary

Ilias Iliadis
IBM Research, Switzerland

Miren Illarramendi
Mondragon University, Spain

Sándor Imre
BME, Hungary

Gábor Járó
Nokia Networks, Hungary

Rainer Keller
Hochschule Esslingen, Germany

Benedek Kovács
Ericsson, Hungary

György Kovács
Lulea University of Technology, Sweden

László Kovács
AITIA International Inc., Hungary

Andrey Koucheryavy
St. Petersburg State University of Telecommunications, Russia

Árpád László
Makara BME, Hungary

János Lázár
OTP Bank, Hungary

Gábor Lencse
BME, Hungary

Gábor Magyar
BME, Hungary

Silia Maksuti
UNIQUA AG, Austria

Markosz Maliosz
BME, Hungary

Ali Raheem Mandeel
BME, Hungary

Vashek Matyas
Masaryk University, Czech Republic

Ferenc Mogyorósi
BME, Hungary

István Moldován
BME, Hungary

Sándor Molnár
BME, Hungary

Róbert Moni
Continental AG, BME, Hungary

Albert Mráz
Magyar Telekom, Hungary

Attila Mátyás Nagy
BME, Hungary

Lajos Nagy
BME, Hungary

Gábor Németh
BME, Hungary

Krisztián Németh
BME, Hungary

Bence Oláh
BME, Hungary

Péter Orosz
BME, Hungary

Lydia Ait Ouchegou
National Institute of Standards and Technology (NIST), USA

Géza Paksy
Magyar Telekom, BME, Hungary

Dávid Papp
BME, Hungary

Adrián Pekár
BME, Hungary

Nihal Pekergin
University of Paris-Est, France

Sándor Plósz
Heriot-Watt University, UK

Zoltán Pödör
ELTE, Hungary

S. Ramesh
SRM Valliammai Engineering College, India

Rama Rao
SRM Institute of S.T., India

Sándor Répás
Széchenyi István Egyetem, Hungary

Zoltán Rózsa
SZTAKI, Hungary

Gerardo Rubino
IRISA, France

Slavisa Sarafijanovic
IBM Research, Switzerland

Gyula Sallai
BME, Hungary

Christoph Schmittner
Austrian Institute of Technology, Austria

Karl Sigman
Columbia University, USA

Tamás Skopkó
BME, Hungary

Balázs Sonkoly
BME, Hungary

Gábor Soós
Magyar Telekom, BME, Hungary

Péter Soproni
BME, Hungary

Burkhard Stiller
University of Zürich, Switzerland

Sree Vattaparambil Sudarsan
Lulea University of Technology, Sweden

Géza Szabó
Ericsson Research, Hungary

Márk Szalay
BME, Hungary

Szabolcs Szilágyi
University of Debrecen, Hungary

Ákos Szlávecz
BME, Hungary

Gábor Szűcs
BME, Hungary

Markus Tauber
Research Studios, Austria

Miklós Telek
BME, Hungary

Lászkó Tóth
SZTE, Hungary

Tamás Tóthfalusi
BME, Hungary

Eszter Udvary
BME, Hungary

Péter Vári
NMHH, Hungary

Balázs Vass
BME, Hungary

Rolland Vida
BME, Hungary

Zoltán Vincze
Nokia Bell Labs, Hungary

Jinsong Wu
University of Chile, Chile

Csaba Zainkó
BME, Hungary

Engin Zeydan
CTTC, Spain

Albert Zomaya
University of Sydney, Australia

Zoltán Zsóka
BME, Hungary

Thomas Zwick
Karlsruhe Institute of Technology, Germany

A New Gateway Selection Algorithm Based on Multi-Objective Integer Programming and Reinforcement Learning

Hasanain Alabbas, and Árpád Huszák

Abstract—**Connecting vehicles to the infrastructure and benefiting from the services provided by the network is one of the main objectives to increase safety and provide well-being for passengers. Providing such services requires finding suitable gateways to connect the source vehicles to the infrastructure. The major feature of using gateways is to decrease the load of the network infrastructure resources so that each gateway is responsible for a group of vehicles. Unfortunately, the implementation of this goal is facing many challenges, including the highly dynamic topology of VANETs, which causes network instability, and the deployment of applications with high bandwidth demand that can cause network congestion, particularly in urban areas with a high-density vehicle. This work introduces a novel gateway selection algorithm for vehicular networks in urban areas, consisting of two phases. The first phase identifies the best gateways among the deployed vehicles using multi-objective integer programming. While in the second phase, reinforcement learning is employed to select a suitable gateway for any vehicular node in need to access the VANET infrastructure. The proposed model is evaluated and compared to other existing solutions. The obtained results show the efficiency of the proposed system in identifying and selecting the gateways.**

Index Terms—**VANET, gateway selection, multi-objective integer programming, reinforcement learning.**

I. INTRODUCTION

THE Vehicular Ad Hoc Networks (VANETs) represent the vital nerve of the Intelligent Transportation System (ITS) as the research, and industrial communities have become increasingly interested in developing VANETs [1]. In general, VANET's infrastructure consists of vehicles equipped with a communication device and Road Side Units (RSUs), which are fixed communication units located near intersections or distributed on the side of the roads [2], [3]. The communication in the VANET environment is divided into two types, namely: Vehicle-to-Vehicles (V2V), which allows the vehicles to communicate directly, and Vehicle-to-Infrastructure (V2I), in which the vehicles are able to make contact with the infrastructure like routers, base stations, and RSUs [4], [2]. The main drive for V2I development is providing the drivers with the necessary information and assistance to increase safety and decrease accidents, as well as providing Internet access for entertainment [5], [6]. However, with the increasing growth of greedy Internet applications, providing the Internet connectivity for vehicular users has become an urgent need, especially in urban areas. As a consequence, new concepts have emerged dedicated to this purpose, like Urban Vehicular Ad Hoc Network (UVANET), which deals with non-safety applications (Internet service, media sharing, and data sharing) [7]. Providing the Internet for vehicles requires finding a suitable gateway. Unfortunately, the implementation of this goal is facing many challenges. The applications with high bandwidth demand can cause network congestion, particularly in urban areas with a high density of vehicles. In addition, the VANET environment is characterized as a high dynamic environment because of the high speed of vehicles that connect or disconnect to the network very frequently, causing unstable network connections [8].

Gateway selection strategies often rely on inquiry and solicitation messages sent and received between the vehicular nodes (VNs) to find a suitable gateway [8]. These kinds of messages overwhelm the networks and can cause broadcast storm problems and overhead when the number of nodes increases [9]. Investing in cloud computing and making it compatible with ITS, provides a valuable opportunity to benefit from cloud computing resources utilized by VANET services [10], [11]. This union produced a new paradigm called Vehicular Cloud (VC) [12] [13]. VC presents many services like network information collection, traffic control optimization, and congestion detection [12]. Because of the massive services and features provided by VC, we will use it to build our gateway selection model, so we can reduce the impact of overhead in the network. The gateways aim to provide the Internet for vehicles that need it. The identified gateways are employed to connect the source vehicles to the infrastructure. The major feature of using the gateways is to decrease the load of network infrastructure resources. Each gateway is responsible for a group of vehicles by handling and multiplexing the traffic amount of the group to send them to the infrastructure. It should be noted; our proposed system is the extension of our previous work entitled "Reinforcement Learning based Gateway Selection in VANETs" . In the previous work, we assumed that the public transport buses are equipped with Internet access and can serve as mobile gateways (MGs) [13]. We used reinforcement learning to select the best gateway for each vehicle that needs Internet access. We are now expanding the scope of our work to include defining the gateways instead of assuming them, and this

Hasanain Alabbas is with the Department of Networked Systems and Services, Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Hungary, and Computer Center Department, Al-Qasim Green University, E-mail: hasanain@hit.bme.hu

Árpád Huszák is with the Department of Networked Systems and Services, Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, and ELKH-BME, Cloud Applications Research Group, Hungary, E-mail: huszak@hit.bme.hu

DOI: 10.36244/ICJ.2022.4.1

leads us to find a mechanism to identify the gateways. Our proposed model now consists of two phases instead of one phase. For the first phase, we utilized the Multi-Objective Integer Programming (MO-IP) to define the best gateways in terms of speed, distance from the base station and geographical distribution. In the second phase, we adopted reinforcement learning to find the best gateway for client vehicles.

II. Related Works

Providing a stable connection to VANET infrastructure is a considerable challenge because of the highly dynamic environment. In [14], the authors proposed a gateway selection strategy to access the information and retrieve the data from the cloud by using epidemic spread routing (ESR). The content accessibility preference (CAP) model has been used to confine the greedy behavior of ESR and minimize the data access delay. In [15], a fuzzy multi-metric qos-balancing gateway selection algorithm (FQGwS) was proposed to provide stable communication and increase the link connectivity duration between the vehicles and LTE infrastructure. The LTE Advanced eNodeBs are employed as fixed gateways. The communication between vehicles and the LTE infrastructure is directly or via a relay gateway. The fuzzy logic is adopted to select the best gateways based on a blend of metrics like signal strength, resources occupation, connection lifetime, and QoS traffic classes. However, this kind of solution uses the reactive approach where vehicles exchange messages to discover an appropriate gateway, thus causing a high amount of overhead. The authors [16] proposed a routing strategy to provide Internet access for vehicles by selecting a suitable mobile gateway. The study utilized the vehicle's characteristics (speed, direction, position) to determine the best mobile gateway. On the other hand, it calculates the trust parameter to determine if the connection is reliable and secure or not. Driss et al. [17] proposed a gateway selection algorithm based on heterogeneous VANET and 4G LTE cellular networks. The study considered that the vehicles fitted with 4G LTE and IEEE 802.11p-based-VANETs interfaces are potential mobile gateways. These possible gateways can provide a reliable connection with the 4G LTE cellular networks to ordinary vehicles. The study took into account several factors for the selection of the mobile gateways, such as signal strength, vehicles' movement, and path length.

However, even though these kinds of solutions show good results in terms of packet delivery when applied in a highway scenario, they are not suitable in urban scenarios. The proactive and reactive strategies used in these algorithms can decrease the throughput when the vehicle numbers increase. Moreover, there is no optimization in the selection procedure.

In [18], the authors suggested a new gateway selection system by using multi-objective optimization to address the issues generated by the previous studies. The system takes into consideration two contradicting objectives. The first objective aims to maximize the number of connected vehicles while the second one aims to minimize the overload of the gateways.

We present a novel model to identify and select the mobile gateways using Multi-Objective Integer Programming (MO-IP) and Reinforcement Learning (RL) in urban scenarios.

III. System Model

Our system model is a hybrid network architecture composed of a VANET, VANET's infrastructure (4G/5G base station, RSU), and Vehicular Cloud (VC). We assume all vehicles in VANET are equipped with an On-Board Unit (OBU). So that they can communicate with each other and with the infrastructure, as stated in Figure 1. We propose a

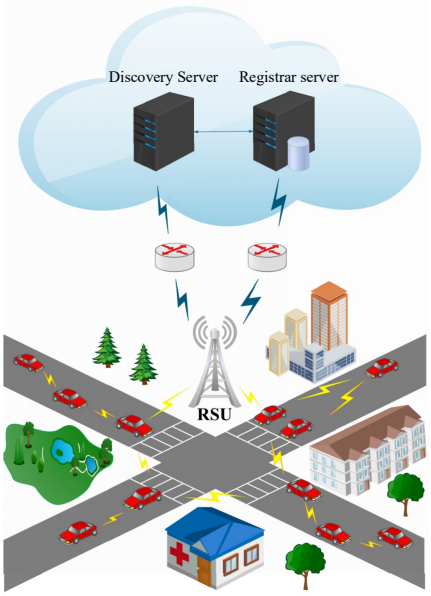


Fig. 1: System architecture.

centralized gateway selection system that aims to identify the gateways and allocate them to vehicles needing of Internet access. Unlike the decentralized strategies in literature, the centralized mechanism reduces the overload situation when there are many nodes in the network.

Our proposed system is based on the VC, which consists of two servers, namely Registrar and Discovery servers. The Registrar Server accumulates the necessary information about vehicles movements and the infrastructure network. It calculates the Link Connectivity Duration (LCD) between them. On the other hand, the proposed system is integrated into the discovery server. Our proposed algorithm is an extension of our previous study [13]. In the previous work, we assumed that the gateways are public transport buses connected directly to the Internet. Based on this assumption, we used reinforcement learning to discover a suitable gateway for source vehicles. In our current work, we aim to make our algorithm more general and comprehensive. The development and expansion is the use of a mechanism to identify the gateways instead of assuming their existence. Therefore, our proposed system consists of two phases:

1) Gateways Identification: we use Integer Programming (IP) to identify the gateways.
2) Gateway Selection: we adopt reinforcement learning to allocate a suitable gateway for ordinary vehicles.

A. Gateways Identification Phase

In this phase, we propose an algorithm seeking the gateways based on different objectives. These objectives ensure that the gateways are close to the infrastructure with lowest relative speed and the highest number of neighbors.

Despite the good results achieved by reinforcement learning to select the best gateways in the previous study compared to MOO, it cannot be applied to the gateway identification phase. In the gateway identification phase, all gateways must be determined by a single decision. Since each gateway has its own criteria for identifying it, the final outcome of the reward function becomes too complex and as a result, the agent becomes confused and unable to learn.

Regarding the run-time complexity, IP is considered NP-complete and can be affected by the number of variables and constraints while RL agent should be trained in a simulated environment. Once the neural network is set up, the decision is very fast.

The MO-IP technique is employed to optimize the gateways discovery. It aims to find optimal solution based on different objectives. The main challenge faced by this type of optimization is finding a compromise solution among Pareto optimal solutions. Pareto optimal solution refers to a non-dominated solution, which means none of objective functions can be improved without making the other objective values degrade. In the rest of this subsection, we formulate the gateways discovery problem. VANET consists of a set of vehicular nodes (VNs), which is represented by $\mathcal{VN}$ and a set of Base Stations (BSs), which is represented by the $\mathcal{BS}$. The distance between a VN $i \in \mathcal{VN}$ and a BS $j \in \mathcal{BS}$ is represented by d_{ij}, while the distance between VNs is denoted by $d_{i_1 i_2}$ where $i_1 \in \mathcal{VN}$ and $i_2 \in \mathcal{VN}$. Let $\mathcal{V}_i$ denotes the velocity of the VN i. $\mathcal{D}_i$ is the direction of a VN i and Nie_i is the number of neighbors located under the VN i range. $\mathcal{U}(\mathcal{VN})$ denotes a binary vector where $\mathcal{U}(i)$ = 1 if the VN i is selected as a gateway, else $\mathcal{U}(i)$ = 0. The relationship between VNs and BSs is represented through the binary matrix $\mathcal{X}(\mathcal{VN},\mathcal{BS})$. If and only if the VN i is selected as a Gateway (GW) to the BS j, then $\mathcal{X}(i,j)$ = 1, otherwise $\mathcal{X}(i,j)$ = 0. The binary symmetric matrix $\mathcal{Y}(\mathcal{VN},\mathcal{VN})$ is defined, if and only if $i_1 \in \mathcal{VN}$ and $i_2 \in \mathcal{VN}$ are Gateways, then $y(i_1,i_2)$ = 1, otherwise $y(i_1,i_2)$ = 0. The gateway identification problem is expressed by the integer program as follow.

$$f = \alpha \sum_{j=1}^{M}\sum_{i=1}^{N} d_{ij}\mathcal{X}(i,j) - \beta \sum_{j=1}^{M}\sum_{i=1}^{N} \mathcal{V}_i \mathcal{X}(i,j) - \gamma \sum_{j=1}^{M}\sum_{i=1}^{N} Nie_i \mathcal{X}(i,j) \quad (1a)$$

Subject to

$$\forall i \in \mathcal{VN}, \forall j \in \mathcal{BS}, d_{ij}\mathcal{X}(i,j) \leq r \quad (1b)$$

$$\forall i \in \mathcal{VN}, \sum_{i \in \mathcal{VN}} \mathcal{U}(i) \leq \mathcal{N} \quad (1c)$$

$$\forall i \in \mathcal{VN}, \forall j \in \mathcal{BS}, \sum_{j \in \mathcal{BS}} \mathcal{X}(i,j) = \mathcal{U}(i) \quad (1d)$$

$$(100 - d_{i_1 i_2})\mathcal{U}(i_1)\mathcal{U}(i_2) \leq \mathcal{M}\mathcal{Y}(i_1,i_2) \quad (1e)$$

$$(45 - |\mathcal{D}i_1 - \mathcal{D}i_2|)\mathcal{U}(i_1)\mathcal{U}(i_2) \leq \mathcal{M}(1 - \mathcal{Y}(i_1,i_2)) \quad (1f)$$

$$\forall i_1 \in \mathcal{VN}, \forall i_2 \in \mathcal{VN}, \mathcal{Y}(i_1,i_2) = \mathcal{Y}(i_2,i_1) \quad (1g)$$

$$\forall i \in \mathcal{VN}, \forall j \in \mathcal{BS}, \mathcal{X}(i,j) \in \{0,1\} \quad (1h)$$

$$\forall i \in \mathcal{VN}, \mathcal{U}(i) \in \{0,1\} \quad (1i)$$

$$\forall i_1 \in \mathcal{VN}, \forall i_2 \in \mathcal{VN}, \mathcal{Y}(i_1,i_2) \in \{0,1\} \quad (1j)$$

The integer programming model consists of three objective functions. The first objective aims to find a GW having the minimum distance with the BS. The second one is used to find a GW with the highest number of neighbors, while the third one aims to identify the lowest speed VN as a GW. Therefore, the utility function (1a). α, β, and γ are the objectives weights so that $\alpha + \beta + \gamma = 1$. The set of constraints are explained as follow:

- Constraint (1b) is used to ensures that VN i, if selected as a GW to a BS j then the distance between i and j must not exceed the range r.
- Constraint (1c) is used to restrict the number of GWs, where $\mathcal{N}$ is the number of the GWs.
- Constraint (1d) is used to ensure that every GW is connected to only one BS.
- Constraint (1e) and constraint (1f) represent if-then constraint which ensure that if the difference in direction between GW i_1 and GW i_2 is less than 45, then the distance between them must be greater than 100 m. $\mathcal{M}$ is a large number enough to bound the difference. These two constraints ensure that the GWs moving in the same direction are not concentrated in a certain area more than the others.
- Constraint (1g) is used to ensure that the matrix $\mathcal{Y}$ is symmetric.
- Constraints (1h), (1i), and (1j) are integrality constraints.

B. Reinforcement Learning

Reinforcement Learning (RL) is an area of machine learning inspired by human interaction with the environment to learn skills. The main parts of the RL system are the agent and the environment. RL is modeled by a Markov decision process. The concepts (state (S), action (A), reward (R)) represent the

interaction of the agent with its environment. At each time (t), the agent senses the environment state (s_t) and takes action (a_t) from the set of available actions causing a state transition to a new state (s_{t+1}). The agent obtains a reward (r_t) that indicates whether the decision taken is correct or not.

The mapping between the action (a) and the state (s) is denoted by the policy $\pi(a, s)$. The policy $\pi(a, s)$ reflects the behavior of agent during sensing its environment.

The agent seeks the optimal policy $\pi^*(a, s)$ by maximizing accumulated discounted reward for each $s \in S$ and $a \in A$ expressed in Equation (3):

$$\pi^*(a \mid s) = \arg\max_{\pi(a|s)} \sum_{t=t_0}^{t_{end}} \gamma^{t-t_0} r_t \tag{2}$$

where $\gamma \in (0, 1)$ is the discount factor and t is the time horizon. Policy optimization algorithms can be categorized into two groups which are value-based algorithms and policy-based algorithms. Although the policy-based algorithms have better convergence and are more convenient for large action spaces but they have some shortcomings. Proximal Policy Optimization (PPO) [19] combines the value-based and policy-based features by using two neural networks called actor-critic. The first one, named $actor$, takes the state (s) as entries and outputs the policy $\pi(a, s)$, while the second one, named $critic$, optimizes $V(s)$ that measures the goodness of the action (a). PPO uses the advantage function $A(s, a)$ to reduce the estimation variance.

PPO uses the Trust Region Policy Optimization(TRPO) strategy to ensure that the new updated policy never goes far away from the old policy, making it more stable and reliable. For these reasons, we adopt PPO algorithm in our proposed gateway allocation phase, namely RL-agent.

C. Gateway Allocation Phase

After electing a specific set of VNs to be gateways to the infrastructure in the first phase, the second phase is concerned with assigning an appropriate GW to each VN that needs access to the Internet or infrastructure network services. RL mechanism is adapted to achieve this goal. Three main parts must be accurately identified to enable the RL agent to sense the VANET environment and make the right decision: state, action, and reward.

1) Definition of Observation State: The state (s) will be created for each VN i that needs access to the infrastructure network and looks for a connection to a suitable GW j. It represents the relationship between the VN and all the identified GWs in terms of geographical location, speed, and available bandwidth. The state is expressed by the entries as follow:

$$X = \begin{bmatrix} Lo_{i1} & Lat_{i1} & V_{i1} & \theta_{i1} & C_1 \\ Lo_{i2} & Lat_{i2} & V_{i2} & \theta_{i2} & C_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ Lo_{ij} & Lat_{ij} & V_{ij} & \theta_{ij} & C_j \end{bmatrix} \tag{3}$$

- Lo_{ij}, Lat_{ij}, V_{ij}, and θ_{ij} represent the difference in longitude, latitude, velocity, and direction between VN i and GW j, respectively.
- C_j denotes the available capacity of a GW j.

Since the relationship of the VN to each MG is represented by five parameters $S = (Lo, Lat, V, \theta, C)$, the total number of entries to represent the state is $|S| \cdot |GW|$,where $|S|$ is the number of parameters used to describe a state, while $|GW|$ is the number of MGs.

2) Definition of Agent Action and Rewards: The action space represents all possible actions. Since the agent's action is to assign an appropriate GW to each VN trying to reach the infrastructure, the action space represents all GWs. Action $a = \{a_1 a_2 a_3 \dots a_n\}$, where a_1 represents the selection of GW_1 and a_n stands for the selection of GW_n. The reward function is assigned based on two metrics: the first one is the link connectivity duration between the VN and GW, whereas the second one is the GW capacity. The first metric motivates the agent to find a GW with the highest LCD for each VN, while the second one aims to reduce the VNs connected to the same GW. Multi-Objective Reinforcement Learning (MORL) is adapted to set the reward function by finding a compromise between the objectives. The reward function is expressed as:

$$R = w_1 \cdot lcd_{ij} + w_2 \cdot C_j \tag{4}$$

where lcd_{ij} denotes the link connectivity duration value between VN i and MG j, while C_j represents the available GW j capacity. Parameters w_1 and w_2 take values between 0 and 1 depending on the importance of the objectives so that w_1 + w_2 = 1. The reward value is positive when the action is valid otherwise, the reward is negative. The positive reward ranges in value between 0 and 20, while the negative reward is (-4). The negative reward is applied in two cases:

1) The GW allocated to a VN is out of its coverage range.
2) The allocated GW does not have enough traffic amount.

As mentioned above, the reward value was adopted after training the agent several times with different reward values because the assumed value showed a faster response from the agent to learn.

3) Agent parameters: The GW allocation system depends mainly on the dataset collected by the registrar server. The dataset consists of a huge number of snapshots collected from the VANET environment. The process of adding a snapshot to the dataset takes place after defining the GWs in the first phase. The snapshot is divided into a number of entries so that the number of entries in each snapshot is equal to the number of VNs. Each entry represents the relationship between each VN with all the GWs in terms of the Cartesian coordinates, speed, LCD, and the available bandwidth for each GW. PPO is employed to maximize the GWs selection return. The reward r is a multi-objective reward in which the agent tends to find a GW for a VN with the maximum LCD and minimum number of VNs connected to it. The dataset is employed to train the RL agent.

IV. RESULTS

The simulation results are presented to show the efficiency of our proposed algorithm. Simulations are implemented by combining Python programming language, Urban Mobility simulator (SUMO), and Open Street Map (OSM). SUMO is used to simulate the vehicles' mobility [20], while OSM is used to extract real-world map data, which makes the simulation more realistic [21]. Gurobi Optimizer is executed to solve the MO-IP problem used in the gateway identification phase [22], while Baseline3 library is used to implement the RL problem used in gateway allocation phase [23]. The entire simulation parameters are listed in Table I.

TABLE I
SIMULATION PARAMETERS.

Parameters	Setting
Simulation area	1500 m X 1500 m
Transmission Range	500 m
Vehicles speed	0-20 m/s
Vehicles Number	120-200

The nature of the roads in urban areas in terms of the spread of intersections, speed limitation, and traffic jams makes them more challenging than the highway environment. It can be considered a true measure of algorithms performance. The number of VNs deployed in the simulation network is 120-220. The MO-IP algorithm used in the gateways identification phase is evaluated and compared with the Fuzzy Multi-metric QoS-balancing Gateway Selection Algorithm (FQGwS) [15] which uses Received Signal Strength (RSS) metric between the VNs and the infrastructure to discover the potential gateways candidates. Three metrics have been used for the performance evaluation in which metric 1 represents the number of GWs' neighbors, metric 2 represents the velocity of GWs, and metric 3 represents the connection lifetime duration between GWs and VANET's infrastructure. Figure 2 which represents the relationship between metric 1 and metric 2 shows that our proposed algorithm has a good trade-off compared to FQGwS algorithm by finding GWs with low speed and a high number of neighbors. On the other hand, Figure 3 which represents the relationship between metric 1 and metric 3 shows our proposed algorithm has better results in terms of choosing GWs with the lowest speed in comparison with FQGwS, but for the connection lifetime metric, the results are approximately similar. In Figure 4, the 3D diagram is depicted, which combines all the metrics. It should be noted, the results plotted in these figures are collected from 10 times of executions for different scenarios.

In the gateway allocation phase, Reinforcement Learning agent (RL-agent) performance is evaluated based on the number of connected VNs and the VNs distribution among GWs. All approaches are simulated and executed under the same conditions. Each scenario is executed and evaluated multiple times so that each point in the plot shows the mean of 10 executions with a variance representing the error in the error-bar plots. Two case studies are applied to make sure our algorithm is efficient under different conditions so that the GWs are either with a bandwidth limitation constraint or without.

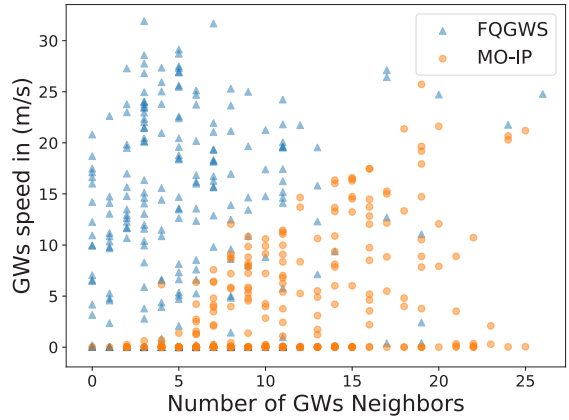


Fig. 2: Number of GWs neighbors.

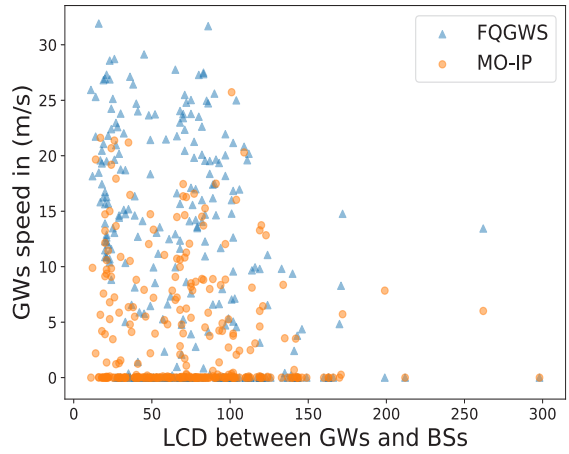


Fig. 3: connection lifetime between GWs and BSs.

The bandwidth constraint limits number of VNs per GW. We set the GW capacity number to 10. Figure 6 and 5 show that the RL-agent has better performance in increasing the number of connected VNs in comparison with FQGwS and DIS-based algorithms. Without bandwidth limitation constraint, RL-agent causes inequality and a wide variation in the distribution of VNs over the MGs, as shown in Figure 7. Figure 8 shows that the RL-agent is not affected by capacity constraint, and it has a higher efficiency in distributing VNs compared to other solutions.

Finally, the connection lifetime between VNs and the infrastructure is evaluated. The connection lifetime is the minimum of $(CON_{VN2GW}, CON_{GW2BS})$ where CON_{VN2GW} represents the connection lifetime between the VN and the GW and CON_{GW2BS} denotes the connection lifetime between the GWs and the infrastructure. In figure 9, the connection lifetime rate of the proposed algorithm (GWS-MORL) is higher than in case of other algorithms. It is also not affected by the limitation constraint of GWs capacity when the number of vehicles increases, unlike the other algorithms in which the connection lifetime rate decreases, as presented in figure 10.

V. CONCLUSION

In this paper, a new gateway selection algorithm based

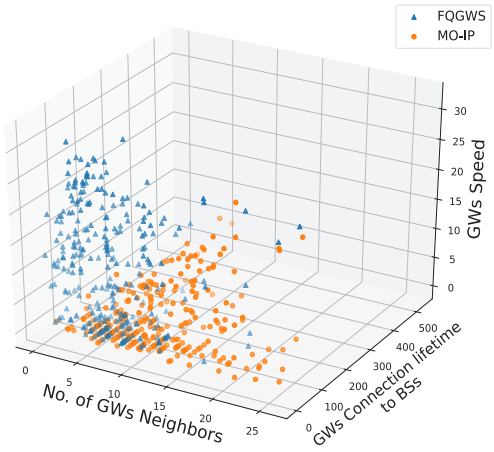


Fig. 4: Projection of metric 1, metric 2, and metric 3.

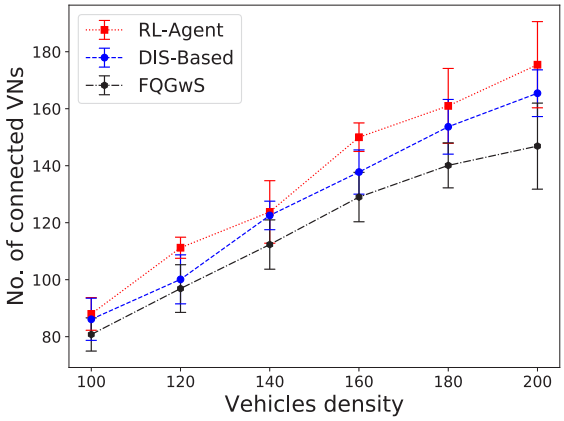


Fig. 5: Number of VNs connected to GWs.

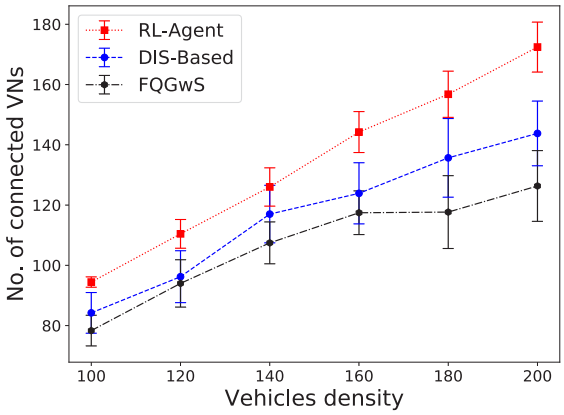


Fig. 6: Number of VNs connected to limited bandwidth GWs.

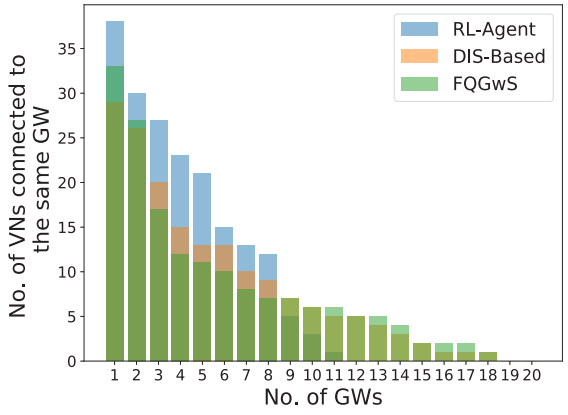


Fig. 7: VNs distribution among GWs.

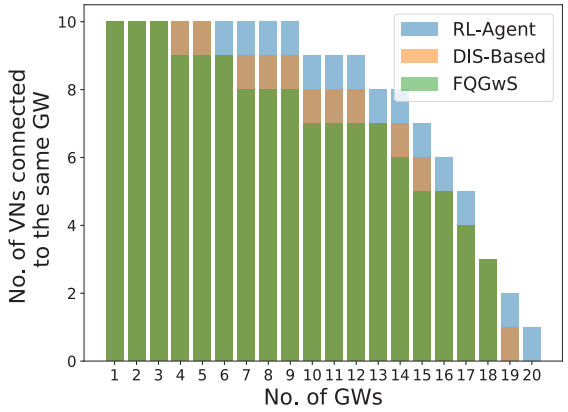


Fig. 8: VNs distribution among limited bandwidth GWs.

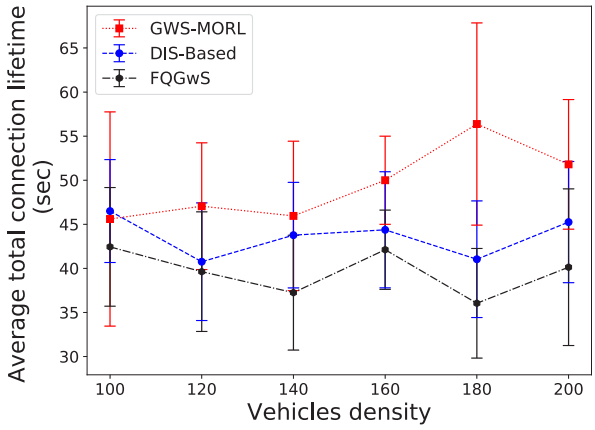


Fig. 9: VNs distribution among GWs.

on multi-objective integer programming and reinforcement learning is presented. The proposed system is a central algorithm assisted by vehicular cloud. System architecture consists of two phases. In the first phase, multi-objective Integer programming is used to elect the best gateways depending on their speed, direction, and proximity to the base stations. The reinforcement learning technique is employed in the second phase to allocate one of elected gateways for each vehicle in need of the infrastructure services. Two agents are created based on the objectives' preferences. Compared with the existing mobile gateway selection algorithms, the simulation results show that the proposed approach is effective in terms of increasing the number of connected vehicles, distributing the vehicular nodes among gateways, and increasing the connection lifetime between the source vehicles and the infrastructure.

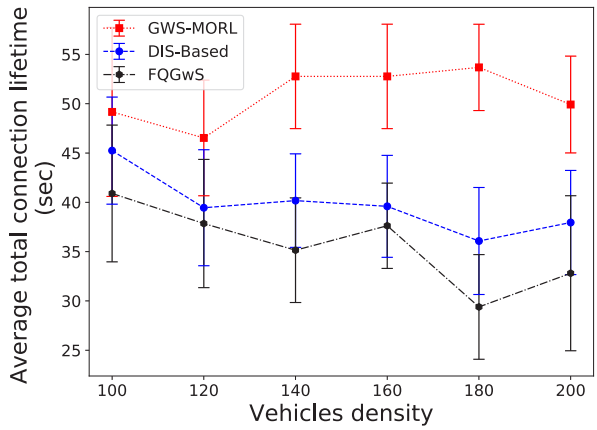


Fig. 10: VNs distribution among limited bandwidth GWs.

REFERENCES

[1] M. Lee and T. Atkison, "Vanet applications: Past, present, and future," *Vehicular Communications*, vol. 28, p. 100310, 2021, DOI: 10.1016/j.vehcom.2020.100310.

[2] J. Jeong, Y. Shen, T. Oh, S. Céspedes, N. Benamar, M. Wetterwald, and J. Härri, "A comprehensive survey on vehicular networks for smart roads: A focus on ip-based approaches," *Vehicular Communications*, vol. 29, p. 100334, 2021, DOI: 10.1016/j.vehcom.2021.100334.

[3] H. Alabbas and Á. Huszák, "Camvc: Stable clustering algorithm for efficient multi-hop vehicular communication on highways," in *2020 43rd International Conference on Telecommunications and Signal Processing (TSP)*. IEEE, 2020, pp. 149–152, DOI: 10.1109/TSP49548.2020.9163488.

[4] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. A. Mini, and A. A. Loureiro, "Data communication in vanets: Protocols, applications and challenges," *Ad Hoc Networks*, vol. 44, pp. 90–103, 2016, DOI: 10.1016/j.adhoc.2016.02.017.

[5] H. Hejazi and L. Bokor, "A survey on the use-cases and deployment efforts toward converged internet of things (iot) and vehicle-to-everything (v2x) environments," *Acta Technica Jaurinensis*, 2021, DOI: 10.14513/actatechjaur.00627.

[6] D. A. Mahmood and G. Horváth, "Analysis of the message propagation speed in vanet with disconnected rsus," *Mathematics*, vol. 8, no. 5, p. 782, 2020, DOI: 10.3390/math8050782.

[7] S. Bhoi, P. Khilar, M. Singh, R. Sahoo, and R. Swain, "A routing protocol for urban vehicular ad hoc networks to support non-safety applications," *Digital Communications and Networks*, vol. 4, no. 3, pp. 189–199, 2018, DOI: 10.1016/j.dcan.2017.08.003.

[8] M. Alawi, E. Sundararajan, R. Alsaqour, and M. Ismail, "Gateway selection techniques in heterogeneous vehicular network: Review and challenges," in *2017 6th International Conference on Electrical Engineering and Informatics (ICEEI)*. IEEE, 2017, pp. 1–6, DOI: 10.1109/ICEEI.2017.8312425.

[9] H. Shahwani, S. A. Shah, M. Ashraf, M. Akram, J. P. Jeong, and J. Shin, "A comprehensive survey on data dissemination in vehicular ad hoc networks," *Vehicular Communications*, p. 100420, 2021, DOI: 10.1016/j.vehcom.2021.100420.

[10] Y.-W. Lin, J.-M. Shen, and H.-C. Weng, "Gateway discovery in vanet cloud," in *2011 IEEE international conference on high performance computing and communications*. IEEE, 2011, pp. 951–954, DOI: 10.1109/HPCC.2011.138.

[11] R. Hussain, J. Son, H. Eun, S. Kim, and H. Oh, "Rethinking vehicular communications: Merging vanet with cloud computing," in *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*. IEEE, 2012, pp. 606–609, DOI: 10.1109/CloudCom.2012.6427481.

[12] S. Bitam, A. Mellouk, and S. Zeadally, "Vanet-cloud: a generic cloud computing model for vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 22, no. 1, pp. 96–102, 2015, DOI: 10.1109/MWC.2015.7054724.

[13] H. Alabbas and Á. Huszák, "Reinforcement learning based gateway selection in vanets," *International journal of electrical and computer engineering systems*, vol. 13, no. 3, pp. 195–202, 2022.

[14] A. Tolba, "Content accessibility preference approach for improving service optimality in internet of vehicles," *Computer Networks*, vol. 152, pp. 78–86, 2019, DOI: 10.1016/j.comnet.2019.01.038.

[15] G. El Mouna Zhioua, N. Tabbane, H. Labiod, and S. Tabbane, "A fuzzy multi-metric qos-balancing gateway selection algorithm in a clustered vanet to lte advanced hybrid cellular network," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 2, pp. 804–817, 2014, DOI: 10.1109/TVT.2014.2323693.

[16] B. Sharef, R. Alsaqour, M. Alawi, M. Abdelhaq, and E. Sundararajan, "Robust and trust dynamic mobile gateway selection in heterogeneous vanet-umts network," *Vehicular communications*, vol. 12, pp. 75–87, 2018, DOI: 10.1016/j.vehcom.2018.02.002.

[17] D. Abada, A. Massaq, A. Boulouz, and M. B. Salah, "An adaptive vehicular relay and gateway selection scheme for connecting vanets to internet," *Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks: Emerging Technologies for Connected and Smart Vehicles*, vol. 242, p. 149, 2019.

[18] S. Retal and A. Idrissi, "A multi-objective optimization system for mobile gateways selection in vehicular ad-hoc networks," *Computers & Electrical Engineering*, vol. 73, pp. 289–303, 2019.

[19] J. Schulman, F. Wolski, P. Dhariwal, A. Radford, and O. Klimov, "*Proximal policy optimization algorithms*," arXiv preprint arXiv:1707.06347, 2017.

[20] P. A. Lopez, M. Behrisch, L. Bieker-Walz, J. Erdmann, Y.-P. Flötteröd, R. Hilbrich, L. Lücken, J. Rummel, P. Wagner, and E. Wießner, "Microscopic traffic simulation using sumo," in *The 21st IEEE International Conference on Intelligent Transportation Systems*. IEEE, 2018. [Online]. Available: https://elib.dlr.de/124092/

[21] OpenStreetMap contributors, "Planet dump retrieved from https://planet.osm.org ," https://www.openstreetmap.org , 2017.

[22] Gurobi Optimization, LLC, "Gurobi Optimizer Reference Manual," http://www.gurobi.com, 2021.

[23] A. Raffin, A. Hill, M. Ernestus, A. Gleave, A. Kanervisto, and N. Dormann, "Stable baselines3," https://github.com/DLR-RM/stable-baselines3, 2019.

[24] R. S. Sutton and A. G. Barto, *Reinforcement learning: An introduction*. *MIT press*, 2018.

[25] H. Dong, H. Dong, Z. Ding, S. Zhang, and Chang, *Deep Reinforcement Learning*. Springer, 2020.

[26] C. Liu, X. Xu, and D. Hu, "Multiobjective reinforcement learning: A comprehensive overview," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 45, no. 3, pp. 385–398, 2014, DOI: 10.1109/TSMC.2014.2358639.

Hasanain Alabbas received his MSc. in Computer Engineering from Al-Nahrain University, Iraq in 2014 and received BSc. from University of Technology, Iraq in 2007. He is currently a PhD student in the Department of Networked System and Services at Budapest University of Technology and Economics, Hungary. His current research interests are in the area of vehicular networks, routing protocols and clustering algorithms.

Árpád Huszák received his M.Sc. degree in 2003 as an Electrical Engineer from the Budapest University of Technology and Economics (BUTE) at the Department of Telecommunications (Dept. of Networked Systems and Services since 2013). He received Ph.D. degree in electrical and computer engineering in 2010. Currently he is with the Department of Networked Systems and Services as assistant professor, but he also joined the Mobile Innovation Center Hungary (MIK). He is member of the IEEE and HTE. Recently, he has been involved in many European (FP6-IST, FP7-ICT, EIT and Celtic) and domestic projects. His research interests focus on network protocols, mobile computing and machine learning.

Evaluation of the HoloLens for Medical Applications Using 5G-connected Mobile Devices

György Wersényi

Abstract—**The updated range of models of smart glasses has expanded the availability of augmented reality (AR) technology in a way that opens them up to several applications. The first prototypes have been replaced by new models and vendors offer off-the-shelf solutions. E-health and medical applications have been in focus from the start. Furthermore, the roll-out of 5G technology would enable almost real-time, high-speed and low- latency communication, which would expand the potential uses and ideas. This paper gives a short overview of the current state, focusing on medical applications using smart glasses. The HoloLens glasses were evaluated regarding latency and data rates by using WiFi and the 5G campus network of the university. Results show that the HoloLens may be used in education, training and teleassistance; however, assisting latency-sensitive tasks that require a reliable network connection, ergonomic design, and privacy issues still remain a problem.**

Index Terms—**5G, HoloLens, Telemedicine, Augmented Reality, Smart glasses**

I. INTRODUCTION

Google presented their AR smart glasses in 2014, where computer generated information (text or graphics) could be superimposed on physical objects in the field of view. This application was considered a human computer interaction (HCI) issue that focused on the multimodal interaction methods and problems (i.e., touch, touchless and hand-held), and design challenges of input and information manipulation. Touch input can be further divided into on-device and on-body, while touchless input can be classified into hands-free and freehand [1]. The user interface plays a significant role in usability, and thus, in the adaptation of new technology [2].

Technology assisted solutions for healthcare ecosystems could address patient-specific needs, but adaptation to it requires time, especially from the patient side [3]–[5]. A 2016 study revealed the importance of different drivers for acceptance, such as usability, functional benefits, branding/fashion issues, individual differences, social norms, and privacy concerns [6], [7]. Results showed that the greater concern is of other people's privacy rather than their own.

A. Clinical Applications

The main goals of introducing smart glasses in clinical applications are: improving patient care, increasing efficiency, and decreasing healthcare costs [8], [9]. Web-connected smart glasses can present data, record images, and videos that are accompanied by audio communication. A 2015 article reviewed 71 cases using smart glasses in health care, highlighting their limitations [10]. The first applications included hands-free documentation; telemedicine meetings and diagnostics; live broadcasting (educational purposes); electronic record storage; and updates. Qualitative evaluation of applications is needed after adjusting to the special needs of the subsections of medicine. Further problems need to be addressed, such as social interactions, physiological and psychological problems, and legal issues [11]. Communication with the patients is a key driver of passive trust in technology and of trust in caregivers [12], [13].

In neurology, smart glasses were tested during ward rounds on 103 neurocritical care patients. Both human supervision and telepresence assistance were available. In 90% of the cases, excellent overall reliability was observed. There was a wide user acceptance and high satisfaction rate for virtual ward rounds [14].

Another study investigated the applicability and accuracy of smart glasses for an AR-based neurosurgical navigation. 3D MRI computer graphics were projected on to the smart glasses, using markers, which allowed for accurate navigation. The test involved two patients with brain tumors located on the surface of the brain. Hands-free neuronavigation inside the operative field was maintained and computer graphics of brain tumors were clearly visualized during surgery [15].

In anatomic pathology the HoloLens was tested for virtual annotation during autopsies, viewing 3D various pathology specimens, navigating slide images, telepathology, as well as real-time pathology-radiology correlation [16]. Residents performing autopsies were remotely instructed. The device was found to be comfortable to wear, easy to use, it provided sufficient computing power, and supported high-resolution imaging.

The HoloLens was compared to a mobile handheld tablet used in anatomy education of medical students. Both methods were beneficial; however, in the case of HoloLens, 25% more subjects reported dizziness [17]. In general, AR/VR-based head-mounted device technology was seen as a key solution in the future in medical education [18].

Another study evaluated the HoloLens as a potential alternative to conventional monitors in endoscopic surgery and minimally invasive surgery. Performance by novice surgeons was improved. The device was widely accepted as a surgical visual aid, specifically as a feasible alternative to the conventional setups with the possibility of aligning the surgeon's visual-motor axis [19].

Promotion of the integration of VR, AR and MR is im-

Széchenyi István University, Győr, Hungary;
E-mail: wersenyi@sze.hu

DOI: 10.36244/ICJ.2022.4.2

portant for comprehensive rehabilitation training, as well as concise extremity rehabilitation and telemedicine (i.e., training of motor skills, individual training programs with automated correction mechanisms) [5].

Furthermore, patient safety in intensive care units may be enhanced by smart glasses. Based on interviews, smart glasses can enhance current monitoring and routines, but not replace human supervision [20], [21].

Integrating data of patients, such as information of the patient in the health care system and devices connected to the patient, can be successful using fast and reliable automated patient recognition based on face recognition using the cameras of smart glasses [22]. Smart glasses can be used to assist visually impaired in their mobility tasks, especially for obstacle detection above waist level [23]. Infrared and position sensors together with noise filters and an Android app resulted in 93% sensitivity and 95% specificity. However, there is a problem with the ergonomic design, which is of great importance, as they need to wear the device for an extended period.

Simulator sickness or cybersickness is a common problem using VR and AR simulators [24]–[26]. It is due to distorted sensation, where the information from the visual modality (often supported by the hearing modality) differs from those of the body (body posture, movement in alignment with vision). It is more common in the case of fully immersive VR scenarios, but can also happen during augmented and mixed realities using head mounted devices.

B. 5G

5G technology offers low latency, high data rate and a large number of connected devices (IoT) in mobile communications and opens new business opportunities [27]. Medical applications can be latency-sensitive, where response times as low as 1 ms are required to create real-time communication. Seeking health care services, getting individual diagnosis and treatment, and avoiding imbalanced resource management (logistics) open the way to new services and applications [5], [28]–[30].

Surgical training and telesurgery (as a future perspective) are the most important areas where low-latency is a prerequisite [31]–[33]. Nevertheless, real telesurgery is still underdeveloped due to lack of confidence from both the patient and surgeon side. Furthermore, during teleoperation, an expert surgeon must be present on-site in the operating room in case of an emergency, this raises the question of whether this is procedure is really necessary or not, as it requires two surgeons to do the job of the one that is present.

Robotic-assisted surgery can be the technological solution to bridge the gap between traditional surgery and future telesurgery (i.e., DaVinci, Hugo RAS System, Fig. 1) [34], [35]. Minimally invasive surgery can be brought to more patients with increased safety, if high operational costs can be reduced [36]. The main advantage is here to have flexible arms during operation compared to the rigid manipulators used today (i.e., in laparoscopy) [37]. On the other hand, the feeling of touch and depth perception is lost. Laparoscopes provide depth perception by looking at a 2D screen and moving the arms back and forth, thus maintaining the eye-hand coordination. 3D imaging techniques, implementation of deep learning procedures, augmented reality, and the development of force feedback robots can lead the way to resolve these problems [38]–[41].

Fig. 1. The DaVinci model Generation 4. It contains a surgeon console for HD images in 3D, a patient cart for the instruments and a vision cart for communication [34]

5G also contributes to the development of related fields in personal medicine, such as big data, artificial intelligence, smart decision making, and diagnosis assistance. The risks of a communication breakdown, and drop in instantaneous data speed or latency have to be solved in order to have a reliable system. Network slicing can help enhance safety, optimize QoS and network load for health care solutions [42], [43].

This is especially true in sparsely inhabited rural areas, which face challenges that can partly be assisted or even solved using e-health solutions based on 5G networks. The full potential of 5G can be exploited for AR solutions as well [44]–[47].

Although not a direct medical approach, multiple HoloLens devices were used for communication with an Unmanned Aerial Vehicle (UAV) that provided multiple video streaming. This allowed the user to switch among multiple perspectives that were provided by the UAVs. A 5G connection was used to compensate for the range limit of the flying device (thus independent of a WiFi connection) [48]. Using drones in the transportation of medicine, medical equipment, samples and supplies can contribute to e-health services. The HoloLens can be also used with mobile devices that share a 5G internet connection [49]–[51]. 5G edge computing enables the distribution of computation-intensive AR tasks to edge servers through 5G networks, thus, increasing quality in latency-sensitive tasks.

An alternative solution to AR glasses is that human supervision can be broadened, simplified or even replaced by automated supervision of patients in rehabilitation. In this case, a device for home usage is installed and connected to the internet (XBox 360 Kinect), which has a camera that records the patient movements, and via automatic analysis, feedback and instructions are given for corrections. Applications can be

Fig. 2. First generation Microsoft HoloLens

Fig. 3. System block diagram. The HoloLens communicates via 2.4 GHz WiFi with a 5G enabled cellphone. Both cellphone and remote device (tablet) connect to the same 5G base station.

developed to meet individual needs of patients and the elderly or for treatment of certain diseases, such as stroke, MS and Parkinson's, where extensive movements would be restricted by smart glasses [52]–[56].

II. Setup and Results

The HoloLens is supported by the Dynamics 365 Remote Assist application, originally developed for Teams. It can be downloaded and installed on the Android platform. The glasses run on a Windows 10 operating system, both the glasses and remote device(s) have to install the application, and be connected to the internet. The real-time video captured by the camera of the HoloLens is streamed to the remote device and simultaneously it is displayed as an overlay in the HoloLens. Both users can edit the video, e.g., by placing pointers, drawings, and text information on it; additionally the communication is enhanced by bidirectional audio connection. The picture of the camera of the remote device cannot be shared and displayed on the HoloLens. Figure 2 shows the first generation HoloLens device.

In our test of the HoloLens, we first set up the connectivity of the devices using the university public indoor WiFi. For measuring the uplink and downlink speed, as well as the response time (ping), a "speedtest" was used in a browser window [57]. Both devices ran the Remote Access application for shared communication. A call can be only initialized from the HoloLens to the tablet, at which point the picture of the HoloLens will be streamed and displayed. Figure 3 shows the system setup in a simplified form in the case of a 5G-based connection. Both devices were connected to the same base station and communication involved the non-stand alone core network.

Using WiFi, the tablet had a 7 ms latency, 92-95 Mbps download, 69-75 Mbps upload speed compared to the HoloLens that had a 16-18 ms latency, 54-62 Mbps upload speed, and 38-41 Mbps download speed (these were measured based on ten measurements). During an established connection between the devices, the speedtest reported 14-17 ms ping, 50-55 Mbps download and most importantly 8-40 Mbps upload rate from the HoloLens side.

Connection	Environment		Remote Device (tablet)	HoloLens
indoor Wi-Fi	without Remote Assist	ping (ms)	7	16-1
		download (Mbps)	92-95	54-62
		upload (Mbps)	69-75	38-41
	with Remote Assist	ping (ms)	7-10	14-17
		download (Mbps)	89-96	50-55
		upload (Mbps)	59-71	8-40
campus 5G	without Remote Assist	ping (ms)	17-25	30-70
		download (Mbps)	800-1020	35-70
		upload (Mbps)	112-125	5-8
	with Remote Assist	ping (ms)	15-26	32-68
		download (Mbps)	810-950	33-69
		upload (Mbps)	101-121	6-8

Fig. 4. Measurement results (max-min values) based on ten measurements for latency, download and upload speeds. The tablet connected to the 5G network directly. The HoloLens connected to the 5G network via the cellphone's 5G module.

Moving outside the buildings, the campus 5G network was used to repeat the tests. A cellphone shared the internet connection with the HoloLens, and the same tablet served as the remote device. Both connected to the same base station operated by a national service provider. The HoloLens used the 2.4 GHz WiFi to connect to the cellphone. The tablet delivered ping results of 17-25 ms, 800-1000 Mbps download and 125 Mbps upload speed. However, the HoloLens had 30-70 ms ping, 35-70 Mbps download and only 5-8 Mbps upload speed independent of being connected or disconnected via Remote Assist (again, based on ten measurements).

Figure 4 shows a summary of the measurement results. Furthermore, a subjective evaluation was made with nine individuals after 30-minute test runs. Five surgeons and four physiotherapists experimented with the device and reported on ergonomics, usability and potential uses in their field of interest.

III. Discussion

A. Latency and Data Speed

A ping, in regard to software, measures the latency time of a round-trip of messages sent from the source to a destination computer and back. Latency issues are clearly problematic in the case of HoloLens if low-latency is required. WiFi outperformed 5G not just in the actual ping measurements, but the difference was clearly detectable by the users experiencing perceptible lags between glasses and the remote device. Results of 30-70 ms from the HoloLens side seem to be far from the promised values of 5G (as low as 1 ms). A limiting factor is the HoloLens itself; newer models may deliver better results. Using the 5G network, there was no significant difference is latency and speed rates with or without running the Remote Assist application.

Although the remote device connected to the 5G base station performed well both in download and upload speed,

the HoloLens upload data rate of several Mbps would be insufficient for applications that have high data rate video streams.

Testing in an outdoor scenario on a sunny day, the HoloLens was almost unusable with very limited picture visibility. This can be also problematic for other devices as well, and also true for bright indoor environments, i.e., in an operating room.

B. Ergonomics

The glasses were tested by subjects of the target group, mostly for ergonomics and comfort. Even when individually adjusted to the head, users were not satisfied with the comfort: the device is quite large and heavy (580 grams), the nose strip is uncomfortable, after head movements it has to be replaced, and tilting of the head can cause it to slip off of the nose and head. Test persons did not support the idea of using it in the operating rooms or while making extended, large-scale movements. However, the subjects stated that in the future they would be interested in testing the device for training and educational purposes. Additionally, six out of the nine subjects reported simulator sickness and mild dizziness.

The HoloLens and its wireless control device can be charged via the micro USB port. After a full charge, about 2 hours of operation is guaranteed, but users did not prefer sessions longer than 20-30 minutes.

C. Other Models

Other vendors also offer solutions. First of all, the follow-up model of the HoloLens, called HoloLens 2 offers a Research Mode, API and methods to access the raw sensor data using open-source tools [58], [59]. Furthermore, using the USB-C connector, an external 5G device can be connected for a direct 5G connection. Size and weight are almost the same, but balance is shifted for a more comfortable wear, the visor can be flipped and regular glasses can be worn inside the helmet. Some additional functionality improvements were added, such as eye-tracking, HD video, two-hands and gesture tracking, and an increase in the field-of-view from 30 to 52 degrees.

Google Glass Enterprise Edition 2 is the latest update from the company running on the Android platform [60]. It is lightweight, only 46 grams without frames (glass pod and titanium band). To mirror the device or remotely operate it, any standard Android 8.1-compatible casting application, i.e., *Vysor* or *scrcpy* can be used. WiFi is the basic connection and there is no information about a direct 5G connection. Due to its special design and light-weight, it can be worn as long as you would a normal set of glasses, so they are much more comfortable than the HoloLens. If the user is already wearing regular glasses or safety frames, the needed parts are detachable and can be attached to them. However, the small display in front of the left eye results in the eye constantly focusing on it, causing the user to suffer from eye strain after some time. It is comfortable if the user only needs the small screen once in a while. This can be a limitation in use and can lead to ”after-effects” after finishing the procedure. It does not have a controller or hand-tracking, only a touchpad-like part of the frame (speech-command apps should be developed for the system).

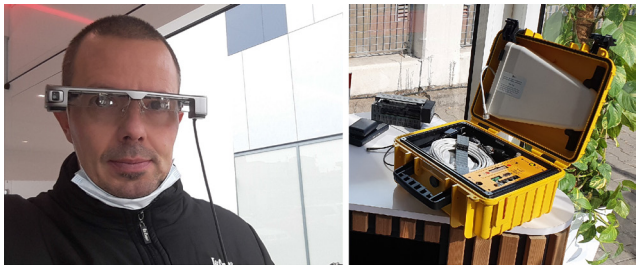


Fig. 5. AR Remote Trouble Shooting case with Epson’s Moverio glasses

The Epson Moverio family offers different glasses for different applications [61]. Headsets are always tethered to a controller and the battery is separated from the headset; both of these features allow for comfort and to keep the weight low. Although this has two displays that show the same image in order to avoid conflicting images between the two eyes, this may cause fatigue. Some models offer SIM connectivity. There is a stand-alone Android Smart Glass model where apps can be installed directly to the controller. Another model includes an interface box to display content from an existing external device to the glasses. Using the Moverio, Huawei presented the AR Remote Trouble Shooting assistance system that enables untrained mechanics to operate complex systems easily (Fig. 5). The system contains a 5G antenna set in an integrated case as an all-in-one solution. A recent survey analyzed 82 publications in the field of logistics and supply chain management. Potential benefits were identified for the latter include visualization, interaction, user convenience, and navigation. For logistics, technical, organizational, and ergonomic considerations were the most important aspects [62].

In an experiment on solving logistic tasks, the Altered Vuxiz glasses were tested for comfort. Even though the ”side weighted” arrangement was the most comfortable, participants still found the device uncomfortable [63].

In manufacturing engineering, the Technological Readiness Level (TRL) of some of the components is still low (displays of TRL7 and the tracking part of TRL5) [64]. Acceptance in engineering tasks and medical applications is relatively low, mostly due to ergonomics. Users can find updated information about current virtual and augmented headsets in the online database called VRcompare [65].

D. SDK and API

HoloLens comes with a pre-installed operating system and the Remote Assist application can be used as an off-the-shelf solution in various cases. However, Microsoft offers lots of documents for HoloLens developers as well [66], [67]. There is no separate SDK for Windows Mixed Reality development. The Visual Studio with the Windows 10 SDK can be used instead. Tutorials are available for starting simple projects and also for users with no technological background.

Windows 10 is required to install Unity Personal as the engine. Optionally, Vuforia Augmented Reality Support can be added, if users want to use markers on real-world objects with the HoloLens. Furthermore, Visual Studio can be installed with the option "Game Development with Unity". The Mixed Reality Toolkit for Unity is a collection of scripts and components to accelerate development. The HoloLens should be in Developer Mode, but if there is no device on hand, the HoloLens can be emulated as well.

Unity is a real-time development platform with runtime code written in C++ and development scripting in C Sharp. The open source Unreal Engine 4.25 can be also used for development in C++ with full HoloLens support [68]. Optimized SDK for other models such as the Moverio and Vuzix smart glasses can be downloaded and installed based on Wikitude's JavaScript API [67]. Google Glass needs Android Studio and Android SDK 8.1 (API 27) to develop applications. All models offer open-source development environments.

E. Applications in Telemedicine and Telerehabilitation

Telerehabilitation, as part of telemedicine, has been among the first areas of applications for smart glasses. Supervision of stroke patients, children and elderly persons with disabilities, subjects that have sleep disorders or neurocognitive problems, as well as remote assistance and consultation for physical therapist has opened the way for the first tests and implementation [69]–[74].

Smart glasses and VR devices offer immersive experience and entertainment. Gamification or serious gaming can be an entertaining way of maintaining motivation during execution of tasks [75]–[77]. Especially children and patients needing sustained rehabilitation process can benefit from such technology. Connected simulations and virtual realities in sport, training or while exercising can enhance the experience and maintain motivation.

Legal and ethical considerations are of great importance, as telerehabilitation solutions usually assume a patient is supervised from a distance, where the patient may not see the other end of the connection, specifically who is watching, or even recording [78]. The environment can be intimate, where supervising personnel observe the patient getting undressed, sleeping or doing physical activities. Trust, together with data and personal security, is and will be a key factor in accepting this technology.

IV. CONCLUSIONS

This paper presented results about the evaluation of the Microsoft HoloLens glasses with a focus on possible medical applications. Using 5G mobile network connection and handheld devices, latency and uplink/downlink speed were measured between the device and remote supervision. Results showed that latency-sensitive tasks are still problematic, where response time is critical and connection breakdowns are not acceptable (e.g., telesurgery). Furthermore, privacy issues and design considerations have to be addressed in order to increase acceptance by the medical personnel, patients, and society. Nevertheless, AR/MR solutions based on smart glasses are suitable for extending telemedicine services in remote consultation and assistance. Furthermore, this technology could be used in medical education and training (e.g., autopsy, anatomy, neurology, stroke treatment). Some headset models are lighter in weight and have a more ergonomic design, which allow for longer use. 5G will offer speed, reduced latency and increased throughput for medical IoT solutions, real-time audio and video streaming, but connected devices have to be fitted in order to utilize all possibilities. The communication module of smart glasses can be enhanced with SIM-slots and 5G antennas along with WiFi terminals. Future work includes exploring further application areas, especially in telemedicine, nursing, rehabilitation, and home care. Currently, an updated measurement setup is being tested using CT and MRI scans of real patients that are displayed, manipulated (rotation, zooming) with an external controller and validated by radiologist. Different wireless solutions will be tested for latency and data rates. Furthermore, other areas, i.e., telemaintenance, e-learning, e-commerce (marketing) and tourism offer additional possibilities for smart glasses [79]–[84]. Involvement and testing of other AR glasses need to be explored in the future.

Acknowledgements

The research was supported by the NKFIH from the project 'Research on the health application of artificial intelligence, digital imaging, employment and material technology developments by linking the scientific results of Széchenyi István University and Semmelweis University' under grant number TKP2021-EGA-21.

REFERENCES

[1] L.-H. Lee and P. Hui, "Interaction methods for smart glasses: A survey," *IEEE access*, vol. 6, pp. 28 712–28 732, 2018. DOI: 10.1109/ACCESS.2018.2831081

[2] A. E. Ok, N. A. Basoglu, and T. Daim, "Exploring the design factors of smart glasses," in *2015 Portland international conference on management of engineering and technology (PICMET)*. IEEE, 2015. pp. 1657–1664. DOI: 10.1109/PICMET.2015.7273236

[3] S. Anwar and R. Prasad, "Framework for future telemedicine planning and infrastructure using 5G technology," *Wireless Personal Communications*, vol. 100, no. 1, pp. 193–208, 2018. DOI: 10.1007/s11277-018-5622-8

[4] W. Tian, "Exploration and prospect of 5G application in telemedicine," *Zhonghua wai ke za zhi [Chinese Journal of Surgery]*, vol. 58, no. 1, pp. 1–4, 2020. DOI: 10.3760/cma.j.issn.0529-5815.2020.01.001

[5] D. Li, "5G and intelligence medicine—how the next generation of wireless technology will reconstruct healthcare?" *Precision clinical medicine*, vol. 2, no. 4, pp. 205–208, 2019. DOI: 10.1093/pcmedi/pbz020

[6] P. A. Rauschnabel and Y. K. Ro, "Augmented reality smart glasses: An investigation of technology acceptance drivers," *International Journal of Technology Marketing*, vol. 11, no. 2, pp. 123–148, 2016. DOI: 10.1504/IJTMKT.2016.075690

[7] P. A. Rauschnabel, J. He, and Y. K. Ro, "Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks," *Journal of Business Research*, vol. 92, pp. 374–384, 2018. DOI: 10.1016/j.jbusres.2018.08.008

[8] N. A. Basoglu, M. Goken, M. Dabic, D. Ozdemir Gungor, and T. U. Daim, "Exploring adoption of augmented reality smart glasses: Applications in the medical industry," *Front. Eng.*, vol. 5, no. 2, pp. 167–181, 2018. DOI: 10.15302/J-FEM-2018056

[9] S. Park, S. Bokijonov, and Y. Choi, "Review of Microsoft HoloLens applications over the past five years," *Applied Sciences*, vol. 11, no. 16, p. 7259, 2021. DOI: 10.3390/app11167259

[10] S. Mitrasinovic, E. Camacho, N. Trivedi, J. Logan, C. Campbell, R. Zilinyi, B. Lieber, E. Bruce, B. Taylor, D. Martineau et al., "Clinical and surgical applications of smart glasses," *Technology and Health Care*, vol. 23, no. 4, pp. 381–401, 2015. **DOI**: 10.3233/THC-150910

[11] B. L. Due, "The future of smart glasses: An essay about challenges and possibilities with smart glasses," *Working Papers on Interaction and Communication*, vol. 1, no. 2, pp. 1–21, 2014.

[12] K. Klinker, J. Obermaier, and M. Wiesche, "Conceptualizing passive trust: the case of smart glasses in healthcare," in *European Conference on Information Systems*, 2019.

[13] K. Klinker, M. Wiesche, and H. Krcmar, "Smart glasses in health care: A patient trust perspective," in *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 2020. **DOI**: 10.24251/HICSS.2020.435

[14] T. Munusamy, R. Karuppiah, N. F. A. Bahuri, S. Sockalingam, C. Y. Cham, and V. Waran, "Telemedicine via smart glasses in critical care of the neurosurgical patient—COVID-19 pandemic preparedness and response in neurosurgery," *World neurosurgery*, vol. 145, pp. e53–e60, 2021. **DOI**: 10.1016/j.wneu.2020.09.076

[15] K. Maruyama, E. Watanabe, T. Kin, K. Saito, A. Kumakiri, A. Noguchi, M. Nagane, and Y. Shiokawa, "Smart glasses for neurosurgical navigation by augmented reality," *Operative Neurosurgery*, vol. 15, no. 5, pp. 551–556, 2018. **DOI**: 10.1093/ons/opx279

[16] M. G. Hanna, I. Ahmed, J. Nine, S. Prajapati, and L. Pantanowitz, "Augmented reality technology using Microsoft HoloLens in anatomic pathology," *Archives of pathology & laboratory medicine*, vol. 142, no. 5, pp. 638–644, 2018. **DOI**: 10.5858/arpa.2017-0189-OA

[17] C. Moro, C. Phelps, P. Redmond, and Z. Stromberga, "HoloLens and mobile augmented reality in medical and health science education: A randomised controlled trial," *British Journal of Educational Technology*, vol. 52, no. 2, pp. 680–694, 2021. **DOI**: 10.1111/bjet.13049

[18] S. Barteit, L. Lanfermann, T. Bärnighausen, F. Neuhann, C. Beiersmann et al., "Augmented, mixed, and virtual reality-based head-mounted devices for medical education: systematic review," *JMIR serious games*, vol. 9, no. 3, p. e29080, 2021. **DOI**: 10.2196/29080

[19] H. F. Al Janabi, A. Aydin, S. Palaneer, N. Macchione, A. Al-Jabir, M. S. Khan, P. Dasgupta, and K. Ahmed, "Effectiveness of the HoloLens mixed-reality headset in minimally invasive surgery: a simulation-based feasibility study," *Surgical Endoscopy*, vol. 34, no. 3, pp. 1143–1149, 2020. **DOI**: 10.1007/s00464-019-06862-3

[20] C. Romare, U. Hass, and L. Skär, "Healthcare professionals' views of smart glasses in intensive care: A qualitative study," *Intensive and Critical Care Nursing*, vol. 45, pp. 66–71, 2018. **DOI**: 10.1016/j.iccn.2017.11.006

[21] C. Romare, L. Skäretal., "Smart glasses for caring situations in complex care environments: scoping review," *JMIR mHealth and uHealth*, vol. 8, no. 4, p. e16055, 2020. **DOI**: 10.2196/16055

[22] J. Ruminski, M. Smiatacz, A. Bujnowski, A. Andrushevich, M. Biallas, and R. Kistler, "Interactions with recognized patients using smart glasses," in *8th Int. Conf. on Human System Interaction (HSI)*. IEEE, 2015. pp. 187–194. **DOI**: 10.1109/HSI.2015.7170664

[23] M. M. da Silva, L. S. Chaves, C. A. F. Júnior, C. S. D. Guerra, S. R. L. Fernandes, P. A. C. Aguilar, I. T. Monteiro, and A. L. Sampaio, "Wearable device in the form of glasses to assist the visually impaired in detecting obstacles," in *Proceedings of the XX Brazilian Symposium on Human Factors in Computing Systems*, 2021. pp. 1–11. **DOI**: 10.1145/3472301.3484376

[24] E. Chang, H. T. Kim, and B. Yoo, "Virtual reality sickness: a review of causes and measurements," *International Journal of Human–Computer Interaction*, vol. 36, no. 17, pp. 1658–1682, 2020. **DOI**: 10.1080/10447318.2020.1778351

[25] K. Stanney, B. D. Lawson, B. Rokers, M. Dennison, C. Fidopiastis, T. Stoffregen, S. Weech, and J. M. Fulvio, "Identifying Causes of and Solutions for Cybersickness in Immersive Technology: Reformulation of a Research and Development Agenda," *International Journal of Human–Computer Interaction*, vol. 36, no. 19, pp. 1783–1803, 2020. **DOI**: 10.1080/10447318.2020.1828535

[26] A. Vovk, F. Wild, W. Guest, and T. Kuula, "Simulator sickness in augmented reality training using the Microsoft HoloLens," in *Proceedings of the 2018 CHI conference on human factors in computing systems*, 2018. pp. 1–9. **DOI**: 10.1145/3173574.3173783

[27] G. Soós, D. Ficzere, T. Seres, S. Veress, and I. Németh, "Business opportunities and evaluation of non-public 5g cellular networks–a survey," *Infocommunications Journal*, vol. 12, no. 3, pp. 31–38, 2020. **DOI**: 10.36244/ICJ.2020.3.5

[28] C. Gjellebæk, A. Svensson, C. Bjørkquist, N. Fladeby, and K. Grundén, "Management challenges for future digitalization of healthcare services," *Futures*, vol. 124, p. 102636, 2020. **DOI**: 10.1016/j.futures.2020.102636

[29] E. Liu, E. Effiok, and J. Hitchcock, "Survey on health care applications in 5G networks," *IET Communications*, vol. 14, no. 7, pp. 1073–1080, 2020. **DOI**: 10.1049/iet-com.2019.0813Citations

[30] F. Qiu, "Hospital archives intelligent management system based on 5G network and internet of things system," *Microprocessors and Microsystems*, vol. 80, p. 103564, 2021. **DOI**: 10.1016/j.micpro.2020.103564

[31] M. Sugimoto, "CloudXR (Extended Reality: Virtual Reality, Augmented Reality, Mixed Reality) and 5G Mobile Communication System for Medical Image-Guided Holographic Surgery and Telemedicine," in *Multidisciplinary Comp. Anatomy*. Springer, 2022, pp. 381–387.

[32] P. J. Choi, R. J. Oskouian, and R. S. Tubbs, "Telesurgery: past, present, and future," *Cureus*, vol. 10, no. 5, 2018. **DOI**: 10.7759/cureus.2716

[33] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Tactile-internet-based telesurgery system for healthcare 4.0: An architecture, research challenges, and future directions," *IEEE Network*, vol. 33, no. 6, pp. 22–29, 2019. **DOI**: 10.1109/MNET.001.1900063

[34] "Robotic-assisted surgery – Da Vinci Generation 4," https://www.davincisurgery.com/da-vinci-systems/about-da-vinci-systems, 2022.

[35] "A new era in robotic-assisted surgery," https://www.medtronic.com/covidien/en-gb/robotic-assisted-surgery/hugo-ras-system.html/, 2022.

[36] G. I. Barbash, "New technology and healthcare costs–the case of robot-assisted surgery," *The New England journal of medicine*, vol. 363, no. 8, p. 701, 2010. **DOI**: 10.1056/NEJMp1006602

[37] N. Enayati, E. De Momi, and G. Ferrigno, "Haptics in robot-assisted surgery: Challenges and benefits," *IEEE reviews in biomedical engineering*, vol. 9, pp. 49–65, 2016. **DOI**: 10.1109/RBME.2016.2538080

[38] L. Qian, J. Y. Wu, S. P. Di Maio, N. Navab, and P. Kazanzides, "A review of augmented reality in robotic-assisted surgery," *IEEE Transactions on Medical Robotics and Bionics*, vol. 2, no. 1, pp. 1–16, 2019. **DOI**: 10.1109/TMRB.2019.2957061

[39] A. A. Shvets, A. Rakhlin, A. A. Kalinin, and V. I. Iglovikov, "Automatic instrument segmentation in robot-assisted surgery using deep learning," in *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*. IEEE, 2018. pp. 624–628. **DOI**: 10.48550/arXiv.1803.01207

[40] N. Haouchine, W. Kuang, S. Cotin, and M. Yip, "Vision-based force feedback estimation for robot-assisted surgery using instrument-constrained biomechanical three-dimensional maps," *IEEE Robotics and Automation Letters*, vol. 3, no. 3, pp. 2160–2165, 2018. **DOI**: 10.1109/LRA.2018.2810948

[41] I. El Rassi and J.-M. El Rassi, "A review of haptic feed-back in tele-operated robotic surgery," *Journal of medical engineering & technology*, vol. 44, no. 5, pp. 247–254, 2020. **DOI**: 10.1080/03091902.2020.1772391

[42] P. I. Tebe, J. Li, Y. Yang, F. Xie, Y. Huang, W. Tian, and G. Wen, "Dynamic 5G Network Slicing for Telemedicine Systems," in *2021 IEEE 6th International Conference on Signal and Image Processing (ICSIP)*. IEEE, 2021. pp. 931–936. **DOI**: 10.1109/ICSIP52628.2021.9688742

[43] K. Mebarkia and Z. Zsóka, "Qos impacts of slice traffic limitation," *Infocommunications Journal*, vol. 13, no. 3, pp. 24–32, 2021. **DOI**: 10.36244/ICJ.2021.3.3

[44] A. Y. Ding and M. Janssen, "Opportunities for applications using 5G networks: Requirements, challenges, and outlook," in *Proceedings of the Seventh International Conference on Telecommunications and Remote Sensing*, 2018. pp. 27–34. **DOI**: 10.1145/3278161.3278166

[45] D. González Morín, P. Pérez, and A. García-Armada, "Toward the distributed implementation of immersive augmented reality architectures on 5G networks," *IEEE Communications Magazine*, vol. 60, no. 2, pp. 46–52, 2022. **DOI**: 10.1109/MCOM.001.2100225

[46] N. Amuomo, "The Evolution of GSM Technologies into 5G and the Imminent Emergence of Transformative Telemedicine Applications: A Review," *East African Journal of Information Technology*, vol. 2, no. 1, pp. 8–16, 2020. **DOI**: 10.37284/eajit.2.1.131

[47] A. Ahad, M. Tahir, M. Aman Sheikh, K. I. Ahmed, A. Mughees, and A. Numani, "Technologies trend towards 5g network for smart health-care using iot: A review," *Sensors*, vol. 20, no. 14, p. 4047, 2020. **DOI**: 10.3390/s20144047

[48] D. E. Widiyanti and S. Y. Shin, "Multi-UAV Multi-HoloLens streaming System," Korean Institute of Communications and Information Sciences, vol. 2020, pp. 424–425, 2020.

[49] J. Cao, X. Liu, X. Su, S. Tarkoma, and P. Hui, "Context-Aware Augmented Reality with 5G Edge," in *2021 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2021, pp. 1–6. DOI: 10.1109/GLOBECOM46510.2021.9685498

[50] A. Vidal-Balea, O. Blanco-Novoa, I. Picallo-Guembe, M. Celaya-Echarri, P. Fraga-Lamas, P. Lopez-Iturri, L. Azpilicueta, F. Falcone, and T. M. Fernández-Caramés, "Analysis, design and practical validation of an augmented reality teaching system based on Microsoft HoloLens 2 and edge computing," in *Engineering Proceedings, vol. 2. Multidisciplinary Digital Pub. Inst.*, 2020., p. 52. DOI: 10.3390/ecsa-7-08210

[51] J. Cao and X. Su, "5G Edge Computing Enhanced Mobile Augmented Reality," in *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*. IEEE, 2021. pp. 416–417. DOI: 10.1109/PerComWorkshops51409.2021.9431024

[52] J. Tollar, F. Nagy, M. Moizs, B. E. Tóth, L. M. Sanders, and T. Hortobágyi, "Diverse Exercises Similarly Reduce Older Adults' Mobility Limitations," Medicine and science in sports and exercise, vol. 51, no. 9, pp. 1809–1816, 2019. DOI: 10.1249/MSS.0000000000002001

[53] L. R. Tovar, J. E. Sierra, C. P. Flórez, and M. B. Barreto, "Functional Telerehabilitation System in Interactive Virtual Environments and Biomedical Technologies," *Utopía y praxis latinoamericana: revista internacional de filosofía iberoamericana y teoría social*, no. 11, pp. 195–203, 2020. DOI: 10.5281/zenodo.4278348

[54] "FysioGaming Expands Rehabilitation Options with Kinect Games," https://www.fitness-gaming.com/news/health-and-rehab/fysiogaming-expands-rehabilitation-options-with-kinect-games.html, 2014.

[55] B. Milosevic, A. Leardini, and E. Farella, "Kinect and wearable inertial sensors for motor rehabilitation programs at home: state of the art and an experimental comparison," *BioMedical Engineering OnLine*, vol. 19, no. 1, pp. 1–26, 2020. DOI: 10.1186/s12938-020-00762-7

[56] S. Sekimoto, G. Oyama, S. Chiba, M. Nuermaimaiti, F. Sasaki, and N. Hattori, "Holomedicine: Proof of the concept of interactive three-dimensional telemedicine," Movement Disorders, vol. 35, no. 10, pp. 1719–1720, 2020. DOI: 10.1002/mds.28249

[57] "Speedtest," https://www.speedtest.net/, 2022.

[58] "Microsoft," https://www.microsoft.com/en-us/hololens/hardware, 2022.

[59] D. Ungureanu, F. Bogo, S. Galliani, P. Sama, X. Duan, C. Meekhof, J. Stühmer, T. J. Cashman, B. Tekin, J. L. Schönberger et al., "Hololens 2 research mode as a tool for computer vision research," arXiv preprint arXiv:2008.11239, 2020. DOI: 10.48550/arXiv.2008.11239

[60] "Google," https://www.google.com/glass/tech-specs/, 2022.

[61] "Epson Moverio," https://moverio.epson.com/, 2022.

[62] A. Rejeb, J. G. Keogh, G. K. Leong, and H. Treiblmaier, "Potentials and challenges of augmented reality smart glasses in logistics and supply chain management: a systematic literature review," *International Journal of Production Research*, vol. 59, no. 12, pp. 3747–3776, 2021. DOI: 10.1080/00207543.2021.1876942

[63] E. Smith, L. Strawderman, H. Chander, B. K. Smith et al., "A comfort analysis of using smart glasses during picking" and putting" tasks," *International Journal of Industrial Ergonomics*, vol. 83, p. 103133, 2021. DOI: 10.1016/j.ergon.2021.103133

[64] O. Danielsson, M. Holm, and A. Syberfeldt, "Augmented reality smart glasses in industrial assembly: Current status and future challenges," *Journal of Industrial Information Integration*, vol. 20, p. 100175, 2020. DOI: 10.1016/j.jii.2020.100175

[65] "VR Compare Homepage," https://vr-compare.com/, 2022.

[66] "Microsoft HoloLens," https://docs.microsoft.com/en-us/hololens/, 2022.

[48] A. I. Hussein and W. B. Kuhn, "Bandpass ΣΔ Modulator Employing Undersampling of RF Signals for Wireless Communication," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 47, no. 7, pp. 614–620, 2000. DOI: 10.1109/82.850420

[67] "Wikitude," https://www.wikitude.com/download-wikitude-sdk-for-hololens/, 2020.

[68] "Unreal Engine," https://docs.unrealengine.com/4.27/en-US/SharingAndReleasing/XRDevelopment/AR/ARPlatforms/HoloLens/, 2020.

[69] M. Agostini, L. Moja, R. Banzi, V. Pistotti, P. Tonin, A. Venneri, and A. Turolla, "Telerehabilitation and recovery of motor function: a systematic review and meta-analysis," *Journal of telemedicine and telecare*, vol. 21, no. 4, pp. 202–213, 2015. DOI: 10.1177/1357633X15572201

[70] C. F. D. Leochico, A. I. Espiritu, S. D. Ignacio, and J. A. P. Mojica, "Challenges to the emergence of telerehabilitation in a developing country: a systematic review," *Frontiers in neurology*, p. 1007, 2020. DOI: 10.3389/fneur.2020.01007

[71] H. I. Sarsak, "Telerehabilitation services: a successful paradigm for occupational therapy clinical services," *Int Phys Med Rehabil J*, vol. 5, no. 2, pp. 93–98, 2020. DOI: 10.15406/ipmrj.2020.05.00237

[72] M. Waller and C. Stotler, "Telemedicine: a primer," *Current allergy and asthma reports*, vol. 18, no. 10, pp. 1–9, 2018. DOI: 10.1007/s11882-018-0808-4

[73] P. Seron, M.-J. Oliveros, R. Gutierrez-Arias, R. Fuentes-Aspe, R. C. Torres-Castro, C. Merino-Osorio, P. Nahuelhual, J. Inostroza, Y. Jalil, R. Solano et al., "Effectiveness of telerehabilitation in physical therapy: A rapid overview," *Physical therapy*, vol. 101, no. 6, p. pzab053, 2021. DOI: 10.1093/ptj/pzab053

[74] L. Suso-Martí, R. La Touche, A. Herranz-Gómez, S. Angulo-Díaz-Parreño, A. Paris-Alemany, and F. Cuenca-Martínez, "Effectiveness of telerehabilitation in physical therapist practice: An umbrella and mapping review with meta–meta-analysis," *Physical therapy*, vol. 101, no. 5, p. pzab075, 2021. DOI: 10.1093/ptj/pzab075

[75] R. S. Alsawaier, "The effect of gamification on motivation and engagement," *The International Journal of Information and Learning Technology*, 2018. DOI: 10.1108/IJILT-02-2017-0009

[76] Y.-k. Chou, *Actionable gamification: Beyond points, badges, and leader-boards*. Packt Publishing Ltd, 2019.

[77] M. Sailer and L. Homner, "The gamification of learning: A meta-analysis," *Educational Psychology Review*, vol. 32, no. 1, pp. 77–112, 2020. DOI: 10.1007/s10648-019-09498-w

[78] B. G. Fields, "Regulatory, legal, and ethical considerations of telemedicine," *Sleep Medicine Clinics*, vol. 15, no. 3, pp. 409–416, 2020. DOI: 10.1016/j.jsmc.2020.06.004

[79] D. Kim and Y. Choi, "Applications of smart glasses in applied sciences: A systematic review," *Applied Sciences*, vol. 11, no. 11, p. 4956, 2021. DOI: 10.3390/app11114956

[80] G. Molnár and D. Sik, "Smart devices, smart environments, smart students-a review on educational opportunities in virtual and augmented reality learning environments," in *2019 10th IEEE International Conference on Cognitive Infocommunications (CogInfoCom)*. IEEE, 2019. pp. 495–498. DOI: 10.1109/CogInfoCom47531.2019.9089984

[81] D.-I. D. Han, M. C. Tom Dieck, and T. Jung, "Augmented Reality Smart Glasses (ARSG) visitor adoption in cultural tourism," *Leisure Studies*, vol. 38, no. 5, pp. 618–633, 2019. DOI: 10.1080/02614367.2019.1604790

[82] E. Litvak and T. Kuflik, "Enhancing cultural heritage outdoor experience with augmented-reality smart glasses," *Personal and ubiquitous computing*, vol. 24, no. 6, pp. 873–886, 2020. DOI: 10.1007/s00779-020-01366-7

[83] R. Iacoviello and D. Zappia, "HoloCities: a shared reality application for collaborative tourism," in *IOP Conference Series: Materials Science and Engineering*, vol. 949. IOP Publishing, 2020, pp. 12–36. DOI: 10.1088/1757-899X/949/1/012036

[84] S. Verde, M. Marcon, S. Milani, and S. Tubaro, "Advanced Assistive Maintenance Based on Augmented Reality and 5G Networking," *Sensors*, vol. 20, no. 24, p. 7157, 2020. DOI: 10.3390/s20247157

György Wersényi was born in 1975 in Győr, Hungary. He received his MSc degree in electrical engineering from the Technical University of Budapest in 1998 and PhD degree from the Brandenburg Technical University in Cottbus, Germany. Since 2002 he has been member of the Department of Telecommunications at the Széchenyi István University in Győr. From 2020 to 2022 he was the dean of Faculty of Mechanical Engineering, Informatics and Electrical Engineering, as well as the scientific president of the Digital Development Center at the university. Currently, he is a full professor, member of the European Acoustics Association (EAA) and the Audio Engineering Society (AES). His research focus is on acoustic measurements, virtual and augmented reality solutions, sonification, cognitive infocommunications, and assistive technologies.

DITIS: A Distributed Tiered Storage Simulator

Edson Ramiro Lucas Filho[1], Lambros Odysseos[1], Yang Lun[2], Fu Kebo[2], and Herodotos Herodotou, *IEEE* [1,*]

***Abstract*—This paper presents DITIS, a simulator for distributed and tiered file-based storage systems. In particular, DITIS can model a distributed storage system with up to three levels of storage tiers and up to three additional levels of caches. Each tier and cache can be configured with different number and type of storage media devices (e.g., HDD, SSD, NVRAM, DRAM), each with their own performance characteristics. The simulator utilizes the provided characteristics in fine-grained performance cost models (which are distinct for each device type) in order to compute the duration time of each I/O request processed on each tier. At the same time, DITIS simulates the overall flow of requests through the different layers and storage nodes of the system using numerous pluggable policies that control every aspect of execution, ranging from request routing and data redundancy to cache and tiering strategies. For performing the simulation, DITIS adapts an extended version of the Actor Model, during which key components of the system exchange asynchronous messages with each other, much like a real distributed multi-threaded system. The ability to simulate the execution of a workload in such an accurate and realistic way brings multiple benefits for its users, since DITIS can be used to better understand the behavior of the underlying file system as well as evaluate different storage setups and policies.**

***Index Terms*—Storage Simulator, Distributed Data Storage, Tiered Storage, Performance Cost Models**

I. INTRODUCTION

THE inclusion of multiple storage and caching tiers consisting of multiple HDD, SSD, NVRAM, and DRAM devices (among others) are common in modern data storage systems, but require the development of new data management policies for controlling the flow, placement, and migration of data across the tiers. At the same time, it is hard to evaluate the impact of the tiers and their policies across different workloads as that would require constantly modifying and redeploying the storage system. Hence, the development and testing of such policies can quickly become a very cumbersome and time-consuming process. From the end-users' perspective, it becomes exceedingly difficult to (i) identify whether their workloads will execute efficiently on a particular multi-tiered system configuration, or (ii) select the best system configuration that will satisfy their requirements.

DITIS is a new distributed tiered storage simulator that can be used to address the aforementioned challenges by enabling its users to accurately simulate I/O flows and data storage operations for given workloads and system configurations. In particular, DITIS is able to represent a set of distributed nodes containing multiple storage tiers with different storage media and performance characteristics, as well as multiple levels of caches. DITIS processes a workload trace and simulates the execution of file system operations, which are guided by numerous data flow, caching, and tiering policies, while maintaining all metadata information and several statistics. As a result, developers can use DITIS to narrow down the design spaces, evaluate design trade-offs, test different setups and policies, and reduce prototyping efforts, while end users can use it to better understand the system's behavior and identify the system configuration that best satisfies their requirements.

Even though DITIS is a discrete-event simulator (i.e., it models operations as a discrete sequence of events), it does not follow the typical event-oriented or process-oriented models. Instead, DITIS adapts the **actor model** as a basic design principle [1]. As such, each key component is an actor that maintains its own private state, processes messages received from other actors, and sends messages to other actors. This enables the seemingly concurrent computation of actors that interact only through direct asynchronous message passing. In DITIS adaptation, all outgoing messages are associated with a simulated (virtual) time of submission, based on which DITIS schedules message delivery. The use of the actor model and other crucial design decisions resulted in a simulator that is:

- **Configurable:** With over 100 configuration parameters, DITIS can simulate a large variety of different system setups and scenarios. For example, a user can configure a system with multiple storage nodes, with up to 3 different persistent storage tiers, and up to 3 additional levels of caches, along with the performance characteristics of the storage media.
- **Extensible:** All key decisions made by a storage system are modelled as policies that can be replaced for changing the behavior of the system and the simulation. Currently, there are 39 policies that control every aspect of execution, including the routing of requests, data flow management, caching, tiering, and performance modeling.
- **Accurate:** DITIS utilizes fine-grained performance cost models at the level of individual storage devices and network data transfers while modeling (and costing) the flow of messages between the different system components.

Section II presents the design of DITIS. Section III presents the flow management of I/O requests. Section IV presents the device-specific performance cost models. Section V presents the experimental evaluation of DITIS. Section VI presents the related work. Finally, Section VII concludes the paper.

II. DESIGN AND ARCHITECTURE

This section presents the design and architecture of DITIS.

[1] E. R. Lucas Filho, L. Odysseos, and H. Herodotou are with Cyprus University of Technology, Cyprus (e-mail: edson.lucas@cut.ac.cy, lambros.odysseos@cut.ac.cy, herodotos.herodotou@cut.ac.cy)

[2] Y. Lun and F. Kebo are with Huawei Technologies Co., Ltd., China (e- mail: yanglun12@huawei.com, fukebo@huawei.com).

* Corresponding author.

DOI: 10.36244/ICJ.2022.4.3

A. Simulation Input

DITIS requires two input files for simulating a workload execution on a storage system. The first one is an *input workload trace* (in CSV) with each line corresponding to one file request to be processed by the storage system. A file request consists of (1) the process id of the application that submitted the request, (2) the submission epoch timestamp (in microseconds), (3) the file operation (open, close, read, write, or delete), (4) the name for the file to be accessed, (5) the offset of the file (in bytes) when reading from or writing to a file, (6) the length containing the amount of data to be processed (in bytes), (7) the current file size, and (8) the original duration of the operation (in microseconds). The original duration is ignored by the simulator but having it facilitates its comparison with the simulated duration time.

The second input is a *configuration file*, which defines the storage system and its behavior. DITIS is a very flexible and extensible simulator, and its configuration allows users to adapt the simulated storage system in many ways. For instance, users can resize internal components of the storage system (e.g., set 3 nodes, 10 SSDs per node), specify their performance characteristics (e.g., disk IOPS, RPM), as well as determine which combination of policies to use during the simulation.

B. Components

Figure 1 depicts the overall architecture and key components of DITIS, inspired by modern hybrid storage systems such as Huawei OceanStor series. Next, we present the description of each component.

Workload Level: The *Trace Parser* is responsible for parsing requests from the input trace, validating them, and preparing them to be processed by DITIS as trace events. The Trace Parser is used by the Workload Initializer and the Workload Replay to process the input trace. The *Workload Initializer* is responsible for creating an initial state for the storage system before the trace is executed. For example, it can create files that are read by the trace but not created by the trace, place files in specific layers, populate caches, or execute any other action required. The *Workload Replay* is a policy that dictates the order and timing for replaying the trace of file requests based on the submission timestamps. The Workload Replay creates a new Application for each distinct process id it encounters and a message for every file request. This message is then sent to its corresponding Application for processing. Each *Application* represents a different client application outside the storage system that submits file requests to the storage system.

Access Layer: The Access Layer defines the interface of the storage system for client Applications. It holds a set of *Access Modules*, and an *Application Connector*, which is responsible for balancing incoming Application connections to the available Access Modules. An Access Module represents either the storage system's client running on the Application node or an access component of the storage system running on a storage node. The Access Module receives and processes file requests from Applications, and has three main components: the *Dataflow Manager*, which determines when and how to process or forward a file request based on the *Dataflow Policies*; the *Metadata Manager Cache* that manages the information about the files stored in the system and accessed by this Access module; and the *Cache Manager* that manages the data stored in the *L0 DRAM Data Cache* using the *L0 Cache Policies*, which are responsible for admitting, evicting, or prefetching data to/from the L0 Data Cache.

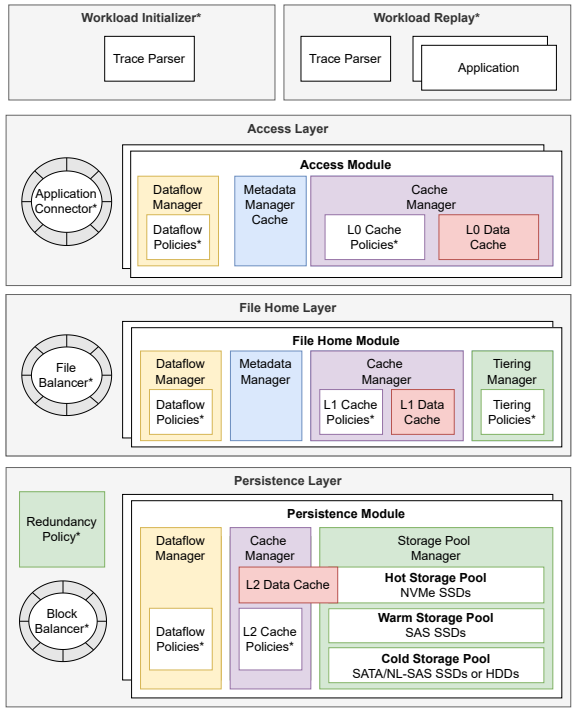


Fig. 1: The architecture of DITIS. Components marked with a * are pluggable policies.

File Home Layer: The File Home Layer holds the *File Balancer* and a list of *File Home Modules*, one for each storage node of the system. The File Balancer distributes files across the File Home Modules based on full file paths, and the File Home Modules maintain the file system namespace and process the file requests forwarded by the Access Layer. The File Home Module consists of the *Dataflow Manager* and its *Dataflow Policies*; the *Metadata Manager* that manages the metadata information about the files stored in the system; the *Cache Manager* that hosts the *L1 NVRAM Data Cache* and the *L1 Data Policies*; and the *Tiering Manager* that manages the *Tiering Policies*, which decide when to place, migrate, and delete files from the storage tiers in the Persistence Layer.

Persistence Layer: The Persistence Layer models the underlying storage capabilities of the storage system. It holds the *Redundancy Policy* that determines how to create and distribute redundancy blocks (e.g., using Erasure Coding, replication, or per-node RAID); the *Block Balancer* that distributes blocks across the Persistence Modules; and the *Persistence Modules* (one per node) that process block requests forwarded by the Access and File Home Layers as well as store data blocks on the different storage pools that form the storage tiers. The Persistence Module has three main components: the *Dataflow Manager* with its *Dataflow Policies*; the *Cache Manager* that

```
// initialize storage
storage.initialize()
// Process events scheduled in the queue
lastTraceTime ← -1;
while lastTraceTime != INF or queue.hasPendingMessages() do
  if !queue.hasPendingMessages() or lastTraceTime <
  ↪  queue.getNextMessageTime() then
    // Get a new trace item and generate a new message
    lastTraceTime ← workloadReplay.processNextTraceItem()
  else
    // Process the next available message
    queue.processNextMessage()
  end
end
```

Algorithm 1: Main simulation control loop.

hosts the *L2 Data Cache* in the hot tier and manages the *L2 Data Policies*; and the *Storage Pool Manager*, which manages the storage pools consisting for storage medias (e.g., HDDs, SSDs) organized in up to three tiers (Hot, Warm, and/or Cold).

C. Simulation Model

DITIS employs a modified version of the *Actor Model* for simulating a distributed data storage system. In DITIS, the Workload Replay, the Applications, the Access Modules, the File Home Modules, and the Persistence Modules are modeled as *actors*. Actors are only responsible for maintaining their own private state, making local decisions, and exchanging messages to communicate with each other. In the original Actor Model, every actor can concurrently send messages to other actors, create new actors, and react on a message basis asynchronously. There is no ordered sequence that needs to be followed, and these actions can be executed in parallel. In DITIS, however, instead of exchanging messages directly to each other, DITIS implements a *global simulation message queue*. This is a priority queue, where the timestamp of messages is the priority token. Thus, actors exchange messages by writing and reading to and from the simulation queue. The messages are then delivered based on the timestamp of each message to simulate the passing of time in an orderly fashion.

Another difference from the original actor model is that, in DITIS, actors are allowed to perform concurrent actions respecting the simulation time. DITIS implements a *Simulation Clock* that maintains the simulation time. The timestamps of exchanged messages are set based on the Simulation Clock and the duration time of the request processing. The requests hold the duration time, which accounts for the simulated time taken to process the request. Each time some processing is taking place, the processing is calculated based on some performance cost model and added to the duration time.

This enables a fine grained modeling of the various actions that take place during processing, such as exchanging data over the network, accessing a cache, accessing one or more disks in parallel, etc. The simulated duration at various points is added to the Simulation Clock to specify the time the next message needs to be delivered. The scheduling of messages from the simulation queue then respects the execution flow of the simulated storage system and accounts for all processing taken at different parts of the system.

Algorithm 1 presents the main simulation control loop of DITIS. First, the storage is initialized by the Workload Initializer policy. Then, if the simulation queue does not have any pending message to be processed, it will schedule a new trace event in the queue. Processing the next trace event means that the Workload Replay will create a new message based on the next trace event and queue it to be processed by its application. A new trace event is also scheduled if there is a gap between the last trace event and the next message in the queue to ensure that messages in the trace are scheduled correctly before other pending messages in the queue. Otherwise, if the system has messages in the queue, DITIS will process the next message in the queue, which also sets the current simulation time.

D. Simulation Output

During the simulation, DITIS will generate an *output trace*. This is a trace with the same sequence of requests given in the input trace but contain the simulated duration time instead. The output trace is written as the file requests are finished but following the correct order of submission. DITIS also generates a *report* containing a wealth of information regarding the simulated execution of the workload trace. In particular, it contains information and statistics about the input trace, for the storage initialization, for each storage layer, and for each application, including the number of bytes read and written by the file requests, the number of files opened, closed, written, and read, the number of requests processed, the cache hit ratio, the throughput, and much more.

III. Request Flow Management and Routing

During a simulation, the I/O requests originate from applications, traverse the appropriate layers of the storage system in order to be served, and then are returned to the applications. This section presents the request routing model and the key flow of requests in DITIS.

A. Three-level Request Routing

DITIS has three levels of routing used to distribute requests across storage layers and nodes due to semantic differences. The first level routes requests from Application to Access modules and is implemented by the *Application Connector*. The first time an Application is ready to submit a request to the file system, the Application Connector is invoked to connect a specific Access Module with the Application. The default policy connects an Application to an Access Module in a Round Robin fashion, simulating the presence of a basic load balancer at the top of the file system. DITIS also supports a Client Mode policy that connects each Application to its own private Access Module, which runs on the same (compute) node as the Application. This enables DITIS to simulate a scenario where each application has its own local data cache and showcases another aspect of DITIS's flexibility.

The second level routes requests to the appropriate File Home Modules based on file semantics and is implemented by the *File Balancer*. When an Access Module submits a file

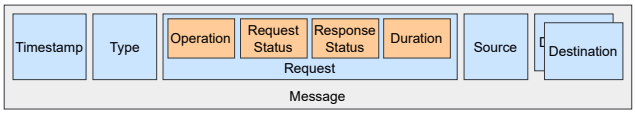


Fig. 2: Simulator message attributes.

request to the File Home Layer, the File Balancer is used to find the File Home Module hosting the required file so that the request is correctly routed there. The current policy uses hashing based on file path to determine the appropriate File Home Module but more complex approaches such as consistent hashing or distributed hash table are easily supported.

The last level routes requests to the appropriate Persistence Modules based on block semantics and is implemented by the *Block Balancer*. When an Access or File Home Module sends a block request to a Persistence Module, the Block Balancer is used for determining the Persistence Module that is responsible for managing that particular block. The default policy also employs hashing based on the block id but more advanced routing strategies are also easy to support.

B. General Request Flow

During a simulation, the trace events in the input trace are converted into I/O *requests*. Currently, a request can be a *file*, a *standard stream* (e.g., stdout), or a special *device* (e.g., to CD-ROM) request. Only file requests are sent and served by the simulated storage system. Every request holds the *type of operation* (open, close, read, write, or delete), the *request status* (pending, in-progress, or completed), the *response status* after request completion (success or fail); and the *duration time* taken to process the request. Requests are encapsulated in *messages*, in order to be sent from one component to another based on the actor model. Figure 2 depicts the message attributes, including the request. A message consists of a *timestamp*, referring to the simulated submission time; a *type* that distinguishes whether the message should be sent forward to the next destination or backward to the previous source; the *source* component that is sending the message; and the list of *destination* components that received the messages in order. The list of destination components forms the lineage of the request and is used for returning the message back through the components that initiated or forwarded the request.

Figure 3 depicts the general request flow starting from the Workload Replay, which creates and passes requests to the appropriate Applications (based on the request's PID in the input trace), and continuing through the components of the simulator. Access Modules receive messages from Applications containing file requests. Each Access Module extracts the request and forwards it to the Data Flow Manager. The Data Flow Manager processes the request according to its Data Flow Policies, which determine how the processing interacts with the Cache Manager and the Metadata Manager, and decide if the request can be completed or not. In the former case, a response message is send back to the Application. Otherwise, either file requests are sent to appropriate File Home Modules or block requests to appropriate Persistence

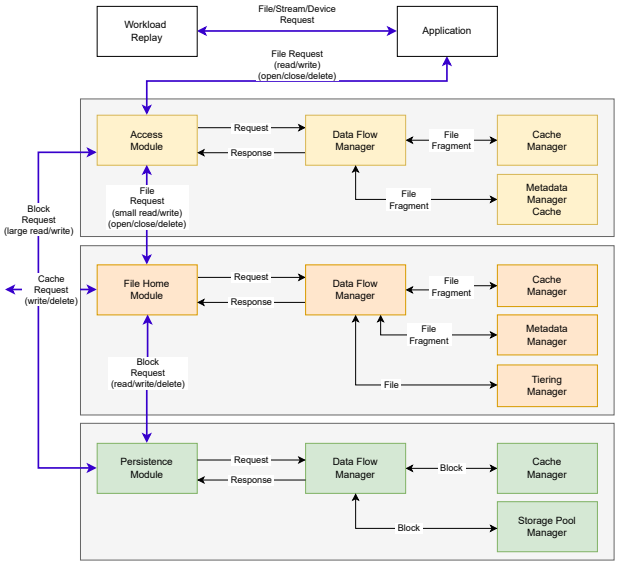


Fig. 3: Request Exchange.

Modules. The request flow in the File Home is analogous to the Access Module. The only additional component is the Tiering Manager, that invokes its Tiering Policies to decide how to place, migrate, or delete files among the storage tiers. Request processing in a File Home Module may result in cache mirroring requests to other File Home Modules or block requests to Persistence Modules. Finally, the Persistence Modules receive block requests from the Access and File Home Modules and processes them in a similar manner.

Messages exchanged among the modules can either be *synchronous* or *asynchronous*, depending on the simulated operation. Synchronous messages create chains of requests for which the successor requests need to be completed before the predecessor requests are completed. For example, if a file read request cannot be completed by the cache of the File Home Module, then synchronous block read requests are sent to appropriate Persistence Modules. Asynchronous messages contain requests that can execute independently from other requests. For example, when a fixed size of data is accumulated on a File Home cache, asynchronous block write requests are sent to Persistent modules for persisting that data.

C. Read/Write Request Flow

We present the key read and write operations simulated in the File Home Module by the default read and write policies. The data flow policies in the other modules are similar.

File Home Module read: The read policy receives a request containing a file name, an offset, and a data length. It checks with the Metadata Manager if the file exists and is open. If not, the request is returned with fail status. Then, the Cache Manager is invoked to check if the fragment is in the cache. If the cache contains the entire fragment, the fragment is read from the cache. The Data Flow Manager adds the read time to the request duration, marks the request as completed, and returns it to the source Access module. If the cache contains

only some parts of the file fragments, those parts are read and the missing file fragments are computed. If the cache does not contain the fragment, then the entire fragment is considered missing. The read policy asks the Metadata Manager for the location of the blocks storing the missing fragments. Then, it creates a child block request for each block, and sends them to the Persistence layer in a synchronous manner. When the child requests are received back, their fragments are offered to the cache. The Cache Manager decides whether to cache the fragments or not based on an admission policy. After receiving all child requests, the Data Flow Manager adds the time of the slowest request to the read duration time of the original request (since child requests were executed in parallel and any potential interactions are accounted for in the lower layers), sets it as completed, and returns to the appropriate Access module.

File Home Module write: The received write request contains a file name, an offset, and a data length. First, it checks with the Metadata Manager whether the file exists and is open. If not, the request is returned with fail status. Note that a new file is created and opened during an open request. The fragment is written directly to the File Home Cache and then mirrored to other File Home Modules (to other storage nodes) according to a data mirroring policy. The times to write to the cache and to mirror to other nodes are both accounted for in the duration of the request. If the insertion of new file fragments into the cache caused other fragments to be evicted, and if those fragments were dirty (i.e., they are not stored in the Persistence layer), then the dirty evicted fragments are sent to the Persistence layer as block requests in a synchronous manner. New file fragments that are added into the cache are aggregated into larger data blocks before they are flushed to the Persistence layer. If enough data has been aggregated for flushing, then that data is sent to the Persistence layer. These operations are managed by a flushing policy that decides when and which data to flush. For example, if erasure coding is used, the flushing policy will wait until a full stripe of data is formed before flushing it. The original request is considered completed when all synchronous child requests return from the Persistence layer (if any). The Data Flow Manager adds to the original duration the write time of the slowest request and returns to the originating Access module.

IV. PERFORMANCE COST MODELING

This section presents the current cost models used to simulate the performance of storage media types and network. The cost models are pluggable, and hence, can be easily replaced.

A. HDD Modeling

A Hard Disk Drive (HDD) is a non-volatile data storage device that consists of an *arm*, a *platter*, a *spindle*, a *read and write head*, and an *interface*. In order to serve I/O requests, in a simplified description, the *arm* moves to find the right track and the *spindle* spins the *platter* to set it to the right sector. Then, the *read and write head* transfers data to or from the *platter*. The data is received from or sent to the interface, and the I/O request is completed [2].

Modeling the performance of HDD devices require accounting for the delays of every internal action. First, moving the arm accounts for the *seek* time. Manufacturers generally report the average seek time $\bar{t}_{seek} = s$ as a constant. Yet, if this parameter is not given, estimations present that this value is approximately one-third of the full seek time [2]. In short, $\bar{t}_{seek} = n^3/3$, where n is the number of tracks.

Rotating the platters to position the head to the right sector accounts for the *rotation* time. The average rotational time $\bar{t}_{rotation}$ is derived directly from the disk rotation speed, which is given by manufacturers as Rotations Per Minute (RPM). Thus, the rotation time for a disk with r RPM is given by:

$$\bar{t}_{rotation} = \frac{60}{r} \cdot \frac{1}{2} \cdot 10^6 \tag{1}$$

where $60/r$ is the time (in seconds) to execute one single rotation, the $1/2$ is included because, on average, a request will require a half rotation [2], and we multiply by 10^6 to convert to microseconds. The data being accessed might be contiguous to the previous data, and consequently, the seek and rotation times would be lower. Our model can differentiate random from sequential operations.

Finally, transferring data accounts for the *transfer* time. The average transfer time $\bar{t}_{transfer}$ depends on the amount of data transferred over the peak transfer rate. In particular, $\bar{t}_{transfer}$ in microseconds is calculated as:

$$\bar{t}_{transfer} = \frac{\lceil \frac{k}{p} \rceil \cdot p}{m} \cdot 10^6 \tag{2}$$

where, m is the maximum transfer rate of the disk in MB/sec, p is the minimum amount of data in a single transfer (and equals the disk page size), and k is the amount of data requested.

Thus, the total duration time for a single **random request** is the sum of the seek, rotation, and transfer times. For sequential I/O requests, there will be no seek and rotation costs.

Disks also maintain a queue of outstanding requests that need to wait for some time while the disk is serving other requests. If the disk is idle when the request arrives, the wait time is zero. Otherwise, the wait time equals the time left for processing the currently active request plus the duration times of all outstanding requests in the disk queue. DITIS computes the wait time by (i) maintaining the virtual completion time of the last request that arrived at the disk, and (ii) subtracting the virtual completion time from the current virtual time if the current request arrives before the last completion time.

B. SSD Modeling

A solid-state drive (SDD) device, in a simplified manner, consists of an *I/O controller*, a *flash array*, a *data register*, and a *cache register*. The I/O controller receives requests for reading or writing data, which is stored in the flash array. The data register acts as data buffer for the flash array, and the cache register acts as a buffer for the I/O requests. A read request involves decoding the I/O request, reading data from the flash array to the data register, then transferring data from the data register to the I/O bus. When reading multiple pages, it will first transfer data to the data register, then to the cache register, which will finally transfer the data to the I/O bus [3].

Consider t_{rr} as the total duration time for reading a single random page. Then:

$$t_{rr} = t_{cmd} + t_{read} + t_{trans} \tag{3}$$

where t_{cmd} is the time to decode the I/O request, t_{read} is the time to read a page from the flash array, and t_{trans} is the time to transfer a page from the data register or cache register to the I/O bus. For sequential read requests, there will be only one single I/O request, but multiple transfers from the data register to the data cache and I/O bus. The following equation generalizes the average time to read n bytes of data:

$$\bar{t}_n = \bar{t}_{acc} + \frac{\lceil \frac{n}{p_{size}} \rceil \cdot p_{size}}{m} \tag{4}$$

where t_{acc} is the average access time (accounting for decoding and reading the first page), p_{size} is the page size, and m is the maximum data transfer rate.

Similar to HDDs, SSDs also maintain a queue of outstanding requests. The simulator computes the wait time of each arriving request in the same manner as for HDDs.

C. DRAM/NVRAM Modeling

A memory address consists of a *bank*, a *row*, and a *column*. Multiple DRAM commands are required to access a particular location. The duration of internal steps required to serve a request is counted in clock cycles. Accessing a specific location requires that an entire row from a specific bank to be *activated*. After the activation, any location within the row can be read or written [4], [5]. DRAM manufacturers provide the number of clock cycles required to perform these internal actions. The constant t_{cl} is the number of clock cycles between receiving a request and having the data ready; t_{rp} is a minimum number of cycles to open a new row; and t_{ras} is the amount of cycles that a row must be open to write data.

Considering f to be the DRAM frequency, n to be the number of bytes to be accessed, r the size of a row in bytes, m_r the maximum read transfer rate, and t_r the time to execute a read request, then:

$$t_r(n) = \frac{\lceil \frac{n}{r} \rceil \cdot r}{m_r}, \text{ where } m_r = \frac{f \cdot r}{t_{cl}} \tag{5}$$

Similarly, the time to execute a write request t_w for n bytes can also be expressed using:

$$t_w(n) = \frac{\lceil \frac{n}{r} \rceil \cdot r}{m_w}, \text{ where } m_w = \frac{f \cdot r}{t_{cl} + t_{rp} + t_{ras}} \tag{6}$$

D. Network Modeling

A model developed by Mathis et al. [6] predicts network bandwidth for a sustained TCP connection subjected to moderate packet losses, including losses caused by network congestion. According to this model, the maximum network bandwidth bw is measure by:

$$bw = \frac{MSS}{RTT} \cdot \frac{C}{\sqrt{p}} \tag{7}$$

where MSS is the Maximum Segment Size, i.e., the amount of data in bytes that a computer can receive in a single TCP segment; RTT is the Round Trip Time, i.e., the time a packet takes to go to a destination and return; C is a constant of proportionality; and p is a random packet loss at constant probability. The bw value represents the maximum throughput in a channel. Thus, the time to transfer n bytes end-to-end is:

$$t_n = \frac{n}{bw} \tag{8}$$

When multiple clients are actively using the network concurrently, the network bandwidth is split evenly between the clients. The simulator keeps track of the active network connections a and adjusts the model to compute the transfer of n bytes accordingly:

$$t_n = \frac{n \cdot a}{bw} \tag{9}$$

V. EXPERIMENTAL EVALUATION

In this section, we present the evaluation of DITIS. All experiments were executed on a machine with i7-7500U CPU @ 2.70GHz, 12 GB of RAM, and OpenJDK 17.0.3. The simulator was developed with Java v17, and Maven v3.8 is used for automating the process of building the project. At the moment, the simulator consists of 25 packages, 12 enumeration types, 31 interfaces, 9 abstract classes, and 140 classes, totaling over 10700 lines of code.

We evaluate DITIS by simulating eight traces derived from production workloads provided by Huawei Technologies Inc. To evaluate the simulation accuracy, we compare the real and simulated times of each request present in the traces, and report the *Mean Absolute Percentage Error* (*MAPE*). The details of each trace are presented in Table I, including the number of file requests per trace, the ratio of read and write operations, the number of random and sequential (read/write) operations, as well as the corresponding MAPE. As it can be seen, the traces exhibit a wide-spectrum of behavior ranging from read-heavy to write-heavy, with different mixes of sequential versus random read/write requests. Note that we consider sequential requests those that operate over consecutive file fragments through a sequential time frame. In our evaluation, DITIS simulates each input trace with a different storage configuration (which we cannot reveal due to privacy considerations), as each trace was originally executed with a different setup. Since open and close requests are straightforward operations, we focus our evaluation on read and write requests.

DITIS is able to accurately simulate write and read requests in most cases. The MAPE metric ranges from 0.06 up to 0.26 in 7 out of 8 traces for write requests, with an outlier of 0.96 for trace 5. Note that up to 70% of trace 5 amounts to read requests, which were simulated with a MAPE of 0.27. Read request simulations exhibited a slightly worse MAPE ranging from 0.07 to 0.93. Figure 5 presents the real and simulated execution times for the write requests of trace 4. DITIS is able to correctly follow the execution trends of the real workload along with all the spikes, albeit with lower magnitude for

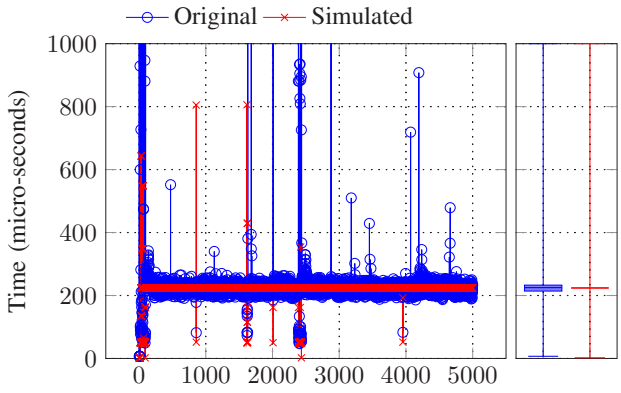


Fig. 4: Real and simulated execution times (raw values and distributions) for read requests for trace 2.

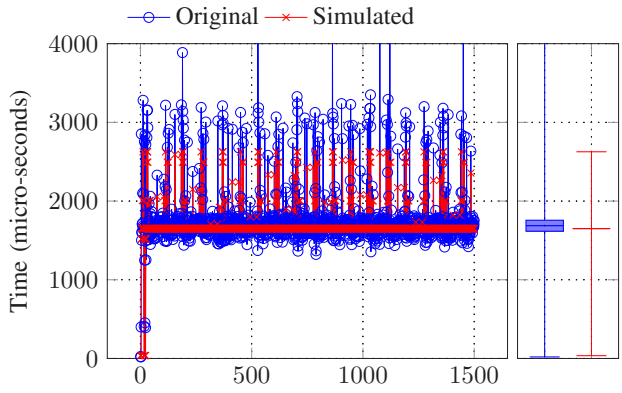


Fig. 5: Real and simulated execution times (raw values and distributions) for write requests for trace 4.

TABLE I
REQUEST DISTRIBUTION AND SIMULATION ERROR PER TRACE.

		Ratio (%)		Sequential		Random		MAPE	
	Requests	Read	Write	Read	Write	Read	Write	Read	Write
1	3106	100.0	0.0	3022	0	84	0	0.34	-
2	5528	99.7	0.3	5342	9	171	6	0.07	0.31
3	49883	0.2	99.8	101	49770	12	0	0.75	0.21
4	16118	89.6	10.4	3388	1544	11047	139	0.70	0.06
5	71496	68.3	31.7	48767	22630	92	7	0.27	0.96
6	47823	85.4	14.6	10562	0	30263	6998	0.92	0.13
7	54473	96.1	3.9	8633	1573	43713	554	0.92	0.13
8	1483669	99.3	0.7	1285	10053	1472181	150	0.93	0.26

TABLE II
DITIS RUN TIMES (IN SECONDS) AND INTERESTING STATISTICS DURING INITIALIZATION AND SIMULATION.

	Initialization			Simulation				
	Files Created	Bytes Written	Run Time	Write Requests	Bytes Written	Read Requests	Bytes Read	Run Time
1	56	35.2M	0.14	0	0.0	3106	11.99M	0.13
2	21	14.9G	1.50	15	109.9M	5513	6.7G	0.36
3	12	809.2K	0.16	49770	376.1M	113	817.2K	23.22
4	3136	526.7K	4.98	1683	7.0G	14435	3.8G	1.11
5	10	707.2M	0.37	22637	707.4M	48859	708.3M	55.30
6	3299	635.7M	5.38	6998	37.8G	40825	3.1G	3.87
7	3138	51.7M	5.00	2127	8.7G	52346	2.6G	1.92
8	857778	6.6G	13.84	10203	465.7K	1473466	11.3G	18.61

the bigger spikes. Similarly, Figure 4 presents the real and simulated times for the read requests for trace 2. While DITIS is able to correctly simulate most of the trace, there are a few outliers present in the trace that are missed by DITIS. These differences (observed mainly for read requests) are due to the different policies that move file fragments through the data storage with different approaches (e.g., policies related to cache, tiers, data placement during initialization), or delays that are not yet modeled by DITIS such as different levels of network contention within the distributed storage. For example, some read requests in DITIS were served from a cache, whereas they were probably served by the persistence storage in the real system (based on their duration). It is a complex task to precisely simulate and replay the various data management and caching decisions in the presence of several policies that works together and influences each other. Yet, DITIS is able to follow the overall trend of the real execution times as well as accurately match the average execution times.

Next, we evaluate the efficiency of DITIS during both the initialization phase and the trace simulation. The corresponding run times are shown in Table II along with statistics that explain DITIS' run times. The Workload Initializer (recall Section II-B) is responsible for creating an initial state for the storage system, such as creating files that existed prior to the beginning of the trace. The time needed for initialization is proportional to (i) the number of files created since DITIS maintains metadata for each file, and (ii) the file size since DITIS distributes file data into blocks that are stored across the storage media, and maintains metadata for each block, much like like a real storage system does. Even when hundreds of thousand of files are created and GBs of data are written, this part of the simulation executes within a few seconds.

Simulating a trace with DITIS is also very efficient and completes within seconds as shown in Table II. The simulation time depends heavily on both the number of write requests and bytes written in the trace for the same reasons explained above. The simulation time is also proportional to the number of read requests but is not affected much by the the number of bytes read. Finally, simulation time can also be affected by other, non-obvious factors, such as the order of requests (as it can impact cache policies), the size of requests (as it can impact data flow policies), as well as configuration parameters (such as the number of disks or disk block size). Nonetheless, DITIS is able to simulate large traces both efficiently and accurately.

VI. RELATED WORK

There are several efforts to simulate multi-tiered data storage systems. MDCSim [7] is a multi-tier data center simulation framework that supports a three-tier architecture, whereas OGSSim [8] enables users to explore the design space of storage systems by supporting various combinations of tiers and volumes. StorageSim [9] enable users to define up to three storage tiers with their performance profiles, while it provides pluggable data placement policies to analyze their impact in the storage's performance. All aforementioned simulators focus on single-node storage systems. EEffSim [10] supports pluggable data placement policies and aims to study the impact of data placement on energy efficiency for distributed (but single-tier) storage systems. Both PFSsim [11] and HPIS3 [12]

focus on simulating Parallel File Systems in High Performance Computing (HPC) centers, but HPIS3 also supports HDD/SSD hybrid systems. NCAR MSS [13] simulates storage drives and software components to explore the design space for cache on data storage systems. SANgo [14] employs reinforcement learning to explore the stability of data storage systems by adjusting the modeled hardware and introducing failures.

In contrast to the related work, DITIS is extremely versatile and extensible. DITIS implements a series of policies that govern all decisions related to cache, tiers, request processing flow, data redundancy, load balance, as well as other options and configurations, like storage device arrangement, number of nodes, threshold values, and enabling/disabling tiers.

VII. CONCLUSION

DITIS is a comprehensive storage simulator that is able to simulate the execution of file system requests on a distributed storage system with multiple levels of tiers and caches. Each tier and cache can be configured with different types of storage media devices, each with their own performance characteristics. The simulator will utilize the provided characteristics in fine-grained performance cost models (which are distinct for each device type) in order to compute the duration time of each request processed on each tier. At the same time, DITIS will accurately simulate the overall flow of requests through the different layers and storage nodes of the system using numerous pluggable policies that control every aspect of execution, ranging from request routing and data redundancy to cache and tiering strategies. The ability to simulate the execution of a workload in such an accurate and realistic way brings multiple benefits for its users, since DITIS can be used to better understand the behavior of the underlying file system as well as evaluate different storage setups and policies.

REFERENCES

[1] G. A. Agha, I. A. Mason, S. F. Smith, and C. L. Talcott, "A Foundation for Actor Computation," *J. Funct. Program.*, vol. 7, no. 1, p. 1–72, jan 1997. [Online]. Available: DOI: 10.1017/S095679689700261X

[2] R. H. Arpaci-Dusseau and A. C. Arpaci-Dusseau, *Operating Systems: Three Easy Pieces*. North Charleston, SC, USA: CreateSpace Independent Publishing Platform, 2018.

[3] K. El Maghraoui, G. Kandiraju, J. Jann, and P. Pattnaik, "Modeling and Simulating Flash based Solid-state Disks for Operating Systems," in *WOSP/SIPEW '10*. ACM Press, 2010, p. 15. [Online]. Available: DOI: 10.1145/1712605.1712611

[4] J. H. Ahn, M. Erez, and W. J. Dally, "The Design Space of Data-parallel Memory Systems," in *Proc. of the 2006 ACM/IEEE Conference on Supercomputing (SC)*. ACM Press, 2006, p. 80. [Online]. Available: DOI: 10.1145/1188455.1188540

[5] A. Hansson, N. Agarwal, A. Kolli, T. Wenisch, and A. N. Udipi, "Simulating DRAM Controllers for Future System Architecture Exploration," *IEEE ISPASS*, pp. 201–210, 2014. [Online]. Available: DOI: 10.1109/ISPASS.2014.6844484

[6] M. Mathis, J. Semke, J. Mahdavi, and T. Ott, "The Macroscopic Behavior of the TCP Congestion Avoidance Algorithm," *Computer Communication Review*, vol. 27, no. 3, pp. 67–82, 1997. [Online]. Available: DOI: 10.1145/263932.264023

[7] S.-H. Lim, B. Sharma, G. Nam, E. K. Kim, and C. R. Das, "MDCSim: A Multi-tier Data Center Simulation Platform," in *IEEE Intl. Conf. on Cluster Computing and Workshops. IEEE*, 2009, pp. 1–9. [Online]. Available: DOI: 10.1109/CLUSTR.2009.5289159

[8] S. Gougeaud, S. Zertal, J. C. Lafoucriere, and P. Deniel, "A Generic and Open Simulation Tool for Large Multi-Tiered Hierarchical Storage Systems," *Simulation Series*, vol. 48, no. 8, pp. 91–98, 2016. [Online]. Available: DOI: 10.1109/SPECTS.2016.7570515

[9] C. San-Lucas and C. L. Abad, "Towards a Fast Multi-tier Storage System Simulator," *IEEE ETCM*, pp. 1–5, 2016. [Online]. Available: DOI: 10.1109/ETCM.2016.7750836

[10] R. Prabhakar, E. Kruus, G. Lu, and C. Ungureanu, "EEffSim: A Discrete Event Simulator for Energy Efficiency in Large-scale Storage Systems," *IEEE Intl. Conf. on Energy Aware Computing (ICEAC)*, 2011. [Online]. Available: DOI: 10.1109/ICEAC.2011.6136682

[11] Y. Liu, R. Figueiredo, Y. Xu, and M. Zhao, "On the Design and Implementation of a Simulator for Parallel File System Research," *IEEE Symposium on MSST*, pp. 0–4, 2013. [Online]. Available: DOI: 10.1109/MSST.2013.6558438

[12] B. Feng, N. Liu, S. He, and X. H. Sun, "HPIS3: Towards a High-performance Simulator for Hybrid Parallel I/O and Storage Systems," *Proc. of the 9th Parallel Data Storage Workshop*, pp. 37–42, 2014. [Online]. Available: DOI: 10.1109/PDSW.2014.12

[13] B. Anderson, "Mass Storage System Performance Prediction using a Trace-driven Simulator," *IEEE Symposium on MSST*, pp. 297–306, 2005. [Online]. Available: DOI: 10.1109/MSST.2005.19

[14] K. Arzymatov, A. Sapronov, V. Belavin, L. Gremyachikh, M. Karpov et al., "SANgo: A Storage Infrastructure Simulator with Reinforcement Learning Support," *PeerJ Computer Science*, vol. 2020, no. 5, pp. 1–16, 2020. [Online]. Available: DOI: 10.7717/peerj-cs.271

Edson Ramiro Lucas Filho is a post-doctoral researcher at the Data Intensive Computing Research Lab, Cyprus Univ. of Technology. He received his Ph.D. from the Federal University of Paraná, Brazil, in June 2020. He held positions as a post-doctoral researcher at the Scalable Database Systems group, Univ. of Passau, Germany, and as a Software Engineer R&D at the Interdisciplinary Centre for Security, Reliability and Trust, Univ. of Luxembourg.

Lambros Odysseos acquired his M.Sc. in Data Science and Engineering (2019) and his B.Sc. in Computer Engineering and Informatics (2017) from Cyprus Univ. of Technology (CUT) both with first student in class award. He worked as a research associate at CUT for 3 years and his research interests include data analytics and visualizations, smart data processing, Internet of Things, and machine learning. Currently, he works as an IT officer at CUT.

Yang Lun is an algorithm engineer in Huawei Data Storage Product Line. He received his Ph.D. in Mathematics and completed his undergraduate studies in Electrical Engineering from Beihang University in 2020 and 2014, respectively. He was a visiting student scholar in Energy Resource Engineering at Stanford University from 2018-2019. His research interests are in storage system algorithms.

Fu Kebo is an algorithm engineer in Huawei Data Storage Product Line. His research interests include data placement and intelligent storage algorithms.

Herodotos Herodotou is an Assistant Professor at the Cyprus Univ. of Technology leading the Data Intensive Computing Research Lab. He received his Ph.D. in Computer Science from Duke University in May 2012. His Ph.D. work received the ACM SIGMOD Jim Gray Doctoral Dissertation Award Honorable Mention. Prior, he held research positions at Microsoft Research, Yahoo! Labs, and Aster Data. His research interests are in large-scale data processing, storage, and database systems.

FiLiP: A File Lifecycle-based Profiler for hierarchical storage

Adrian Khelili, Sophie Robert and Soraya Zertal

Abstract—**The increasing gap between computing speed and storage latency leads to possible I/O bottlenecks on massively parallel computers. To mitigate this issue, hierarchical storage provides multi-tiered configurations where each tier has its own physical characteristics and associated performance. Selecting the most appropriate file placement policy on this multi-tiered storage is difficult and there is to our knowledge no tool that systematically provides statistics and metrics for optimal file policy selection. In this paper, we present FiLiP (File Lifecycle Profiler), a software which provides statistics and metrics for a better understanding of file access by applications and the consequences on file movements across hierarchical storage. After the description of FiLiP's main features and architecture, we highlight the usefulness of our tool using three I/O intensive simulation HPC applications: NEMO, S3DIO and NAMD and a three-tiered burst buffer.**

Index Terms—**I/O, File lifecycle, Profiling, Burst Buffer, Hierarchical storage, HPC**

I. INTRODUCTION

On modern High Performance Computing (HPC) systems, important efforts are put in improving massively parallel computations and communication between compute nodes in order to deliver a higher performance. However, the huge gap between the computing capacity and the storage system latency leads to I/O bottlenecks, and a similar effort has to be made on the I/O and storage systems as a response to the large amount of data generated, manipulated, shared and transferred by modern applications. Recent computer architectures provide hierarchical storage systems with different tiers [28], each with its own physical characteristics based on the device technology and its associated performance metrics, such as latency or throughput [8]. Because of the performance disparity between these tiers, a good file placement is required in order to make the most out of the performance of each one and improve applications performance. Understanding the storage hierarchy behavior, along with the file access performed by the application, is thus key to adapt the data placement to the application's access profile.

Such a file data placement policy can be considered effective when it increases the performance of the system by placing hot files in the best performing tiers and cold files in the worst performing tiers, so that the files with the highest probability of being read are quickly available to the application [8]. To distinguish between these two access and achieve an efficient data placement, the first step is to perform a thorough profiling of the application and its files manipulation, to characterize file re-use throughout the application's lifetime. From these observations, an optimal file placement policy can then be designed and selected. However, selecting the best policy is often a complicated task, as the literature is rich of different strategies: Random, LRU and LFU in their basic versions [13] [16] or optimized ones [10] [24], methods using tuning as ARC [21], methods introducing additional history information as LIRS [15] or methods combining tiering and caching [30]. Novel approaches attempting cache management using statistics of past requests [12] or through machine learning techniques as in [14] [31] [11] [4] have proven successful, by focusing on I/O patterns detection to predict which block should be loaded into the different cache tiers at a given time.

Among all these different approaches, the selection of the optimal placement should rely on objective criteria and metrics describing the placement, such as the cache hits and cache miss rates, file re-use rate, file lifecycles…To our knowledge, none of these metrics have been systematically included into an I/O profiler and correlated with the behavior of the application at the file level for selecting an optimal file placement, as the literature mainly focuses on the application level. We believe that combining the profiling at the file level with the description of file movements through hierarchical and heterogeneous storage tiers fills this literature gaps, and we suggest in this paper a new tool called FiLiP (**Fi**le **Li**fecycle **P**rofiler) to provide data analysis at the file level, by allowing the visualization of operations performed on the file by the application, and systematically including statistics quantifying the quality of file placement policies in the hierarchical storage.

This paper is structured as follow. We present in section II the related works and point out the novelty of FiLiP compared to existing profiling software. In section III, we describe FiLiP's main features. Section IV presents its utilisation within three different HPC applications running on hierarchical storage, and present an analysis of their file-level manipulation that can only be done using our new suggested software. In section V, we conclude the paper by providing some insight on some works we are currently inquiring.

Adrian Khelili: Atos BDS R&D Data Management Li-PaRAD, UPSaclay-UVSQ, France. (E-mail: adrian.khelili@atos.net)

Sophie Robert: Atos BDS R&D Data Management Echirolles, France. (E-mail: sophie.robert@atos.net)

Soraya Zertal: Li-PaRAD, UPSaclay-UVSQ Guyancourt, France. (E-mail: soraya.zertal@uvsq.fr)

DOI: 10.36244/ICJ.2022.4.4

age, and present an analysis of their file-level manipulation that can only be done using our new suggested software. In section V, we conclude the paper by providing some insight on some works we are currently inquiring.

II. RELATED WORKS

Profiling has been used in different areas and at different levels from the top of the software stack to the hardware level. This technique has proven its efficiency and accuracy to investigate any component and understand its behavior when submitted to various execution conditions. The literature is rich of many profiling tools dedicated to power and energy, computing, memory and storage hierarchies. For example, in the energy and power domain to understand energy consumption by providing a suite of statistics [17] [26] and experimental methodology [29]. When it comes to tasks placement, synchronization and communication, monitoring and profiling tools such as [9] [25] for MPI and MapReduce allow to understand applications running on massively parallel architectures. At the memory hierarchy level, profiling guides heap management [22] and improve the suitability of mapping parallel applications [7].

At the storage hierarchy level, several I/O profilers exist and aim to understand applications I/Os such as IOPIN [18] and IOPRO [19]. Their principal utility is to identify I/O bottlenecks and thus better exploit the system potential. One of the most popular I/O profiler is Darshan [5] : a characterization tool developed at Argonne National Lab and designed to capture an accurate picture of the I/O behavior of an application to help developers tune their application parameters by measuring the effect of a parameter set on execution time. Rather than capturing a complete trace of each I/O, Darshan characterizes the job by recording global statistics, such as counters for POSIX operations and their timestamps, cumulative bytes read and written, for a compact representation in memory. A similar profiling tool is Atos IO Instrumention tool (IOI) [2] with a web interface delivering a maximum of information to users by providing statistics as time series describing a wide range of I/O related statistics.

All these profilers are application-oriented and thus have only one perspective when profiling and analyzing the system. We propose through FiLiP the possibility to investigate and analyze the system from the file perspective, by providing the novel features that:

- **Enables profiling at the file-level**: FiLiP provides the possibility to characterize the I/O behavior of an application at the file level for a thorough understanding of file lifecycles and data movements through hierarchical storage. It displays metrics at the application level as well, such as hit/miss rates, total reads, writes, to provide a higher level description of the application's I/O behavior.
- **Provides a standardized interface**: FiLiP relies on a suggested standardized format for description of file movement between the storage hierarchy tiers that can be implemented with any monitoring system.
- **Evaluates the quality of a destaging policy**: Given a destaging policy described through this standardized format, FiLiP evaluates its quality through relevant statistics. It acts then as a performance evaluation tool for new tiers-management strategies.

III. FEATURES AND ARCHITECTURE

A. Definitions and notations

We define the following terms that will be referred to throughout the rest of the paper:

- **Storage tiers**: n storage tiers, ordered hierarchically depending on their access latency (for example, $tier_1$ = RAM, $tier_2$ = NVMe, $tier_3$ = HDD). We will denote $tier_n$ the tier at level n.
- **File lifecycles**: a temporal series of operation performed on the file $(o_t)_{1 \leq t \leq T}$, with o_t an operation in the POSIX set {READ, WRITE, OPEN, CLOSE}.
- **File placement policy**: a temporal series describing the data movement from and to a storage tier (m_{ij}) with i the source tier and j the target one.

B. Main features

FiLiP gives the user an easy to access Web interface, providing:

- **A general understanding of the file manipulation behavior of the application**: Visualization of general statistics on the file behavior during the application's execution, as can be seen in figure 4.
- **The visualization of file lifecycles**: Visualization of file lifecycles to observe how the application manipulates its different files during their lifespans through POSIX operations, as can be seen in figure 4.
- **The visualization of file placement policies**: Files movements are correlated with the file lifecycles to assess the impact of file accesses on moves across the hierarchical storage. File placement policies can also be characterized through generic statistics for proper evaluation as depicted in figure 1 and described in section III-C.
- **The visualization of operations per file**: These statistics are displayed as a table that contains for each accessed file the number of *read*, *write*, *open*, and *close* operations, as well as the volume of data manipulated per file for each of read and write operations in Gb.
- **Visualisation of tiers usage**: FiLiP's provide the usage percentage for each tier, at each moment of the application execution. The fill rate of the tiers are displayed as a time series, that offers a global view about fluctuations in tiers usage during the execution.

C. Evaluation metrics

As displayed in figure 1, FiLiP's main menu provides the following metrics to evaluate the quality of file placement policies:

- **Cache hits from tiers**: For every tier available in the storage hierarchy, the software provides the number of

Listing 1: Example of file lifecycle declaration

```
"file_name": [
    {
    "timestamp": "xxx",
    "type": "OPEN"
    }
]
```

Listing 2: Example of file policy

```
"file_name": [
    {
    "timestamp": "xxx",
    "from": "tier_1"
    "to": "tier_2"
    }
]
```

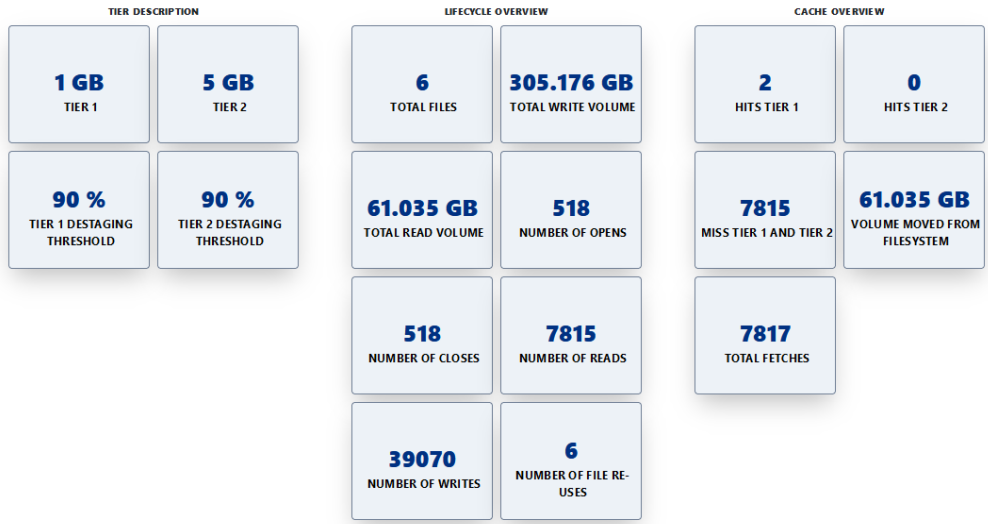


Fig. 1: Example of main menu general statistics for S3DIO application.

hits. This metric allows us to assess a policy's ability to place hot files in the most suitable tier (the one delivering the best performance) and place files less likely to be accessed often in slower tiers.

- **Total fetches**: This is an additional information on total fetches to put the previous metrics in context. It corresponds to the sum of the fetches from each tier.
- **File re-use**: This metric allows us to determine the relevance of a file-level policy for a given application. For example, an application which does not re-use many files will not benefit from a file-level policy and vice-versa for applications with high file re-use.

D. Expected input format

To provide a generic API and to accommodate a wide variety of monitoring systems, we define a standard interface of files to use for our tool. Three different files are required as input for such a visualization :

- **File lifecycles**: File that contains all the operations for each file used by the application. The expected format is presented in listings 1.
- **Data movements**: File that describes data movements between the different tiers. The expected format is presented in listings 2.
- **Storage tiers metadata**: Metadata file that contains the size of the tiers and the maximum memory size allowed for the application use. Optionally, the threshold used for triggering the cache eviction can be specified.

Any file respecting this standard can be imported and visualized through the Web interface.

E. Architecture and implementation choices

The architecture of FiLiP is available in figure 2. The first step is the extraction of the raw data describing the file lifecycles, the memory movements and the storage tiers metadata. This data is then given to the file-extractor module that produces JSON files with the format described in listings 1 and 2. Once these files are created, they are given to the front-end interface that renders the profiling information for the application. This front-end interface communicates through a REST HTTP API that returns for each visualization the required data.

The Web front-end is developed using the reactive javascript framework *Vue.js* [3] and the visualization components developed using the *D3.js* library. All computations rely on a REST API, developed using the Python framework FastAPI [1].

TABLE II
FILE MANIPULATION BEHAVIOR FOR THE THREE CASE STUDIES

Application	Total files	File re-used	Number of read	Number of write	Number of open	Number of close
NEMO	56	22	1600	9904	106	106
S3DIO	6	6	6274	31365	38	38
NAMD	14	10	1346	3959	244	244

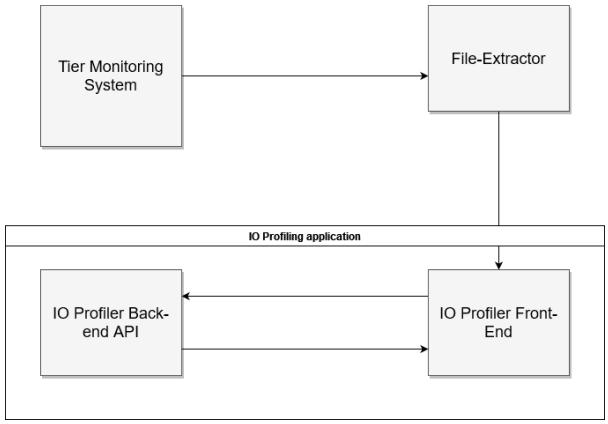


Fig. 2: FiLiP's architecture

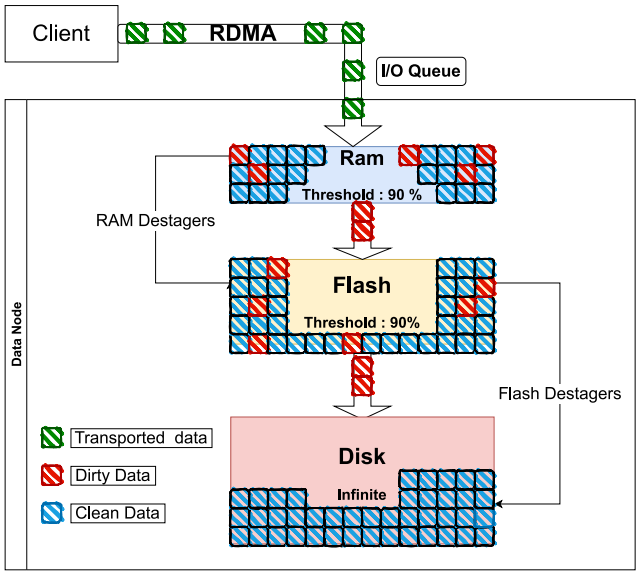


Fig. 3: Schematic representation of the burst buffer

IV. CASE STUDIES

To highlight the usefulness of FiLiP, we test it on a three levels hierarchical storage (RAM, NVMe, HDD). The RAM and NVMe are deployed as a data node, also called *burst buffer* [20] [27] [6], a fast intermediate layer located between the compute nodes and the end storage. A monitoring system is deployed on the burst buffer to capture file transfers through the storage hierarchy and observe the I/O flow between the different layers, as displayed in figure 3. When data comes to a cache level, the data has not yet been flushed to the underlying tier and is labeled as dirty. As soon as it is flushed, it is flagged as clean and can be evicted from the cache level.

To show the usefulness of FiLiP on production use-cases, we select two scientific applications and a popular I/O benchmark: NEMO [**?**], NAMD [23] and S3DIO [**?**] which implements the I/O kernel of the S3D HPC application. Because of their many parallel accesses and their high file re-use rate, these applications are relevant to show the usefulness of FiLiP and representative of the behavior of I/O intensive HPC applications. All of these applications are run on the *burt buffer* using different tiers size, to display the impact of the tier size on file movements and consequently application's performance, that can only be detected through FiLiP.

A. Experimentation scenarios and hardware

Each applications has been selected for its specific and representative behavior of sub-classes of HPC applications. Indeed, NEMO generates a large number of files and exhibits a high degree of file manipulation and re-use, S3DIO is an I/O intensive application generating a low number of files, and NAMD is very sensitive to hardware variation due to large I/O bursts. Table I summarizes the file manipulation characteristics of these three applications.

Each application is run using FiLiP according to three scenarios with a fixed combination of the available space on tiers 1 (RAM) and 2 (NVMe), and an infinite size for tier 3 (HDD) as detailed on table II. The variation in size of the different tiers shows how FiLiP can help to understand the reasons behind file movements and policy efficiency when hardware parameters or cache policy are subject to change.

TABLE II
TIER SIZE FOR EACH SCENARIO

Scenario	RAM Size	NVME Size
1	1 GiB	5GiB
2	32GiB	500 GiB
3	100 GiB	1024 GiB

Table III gathers the hit rates for the two first tiers and the miss rate when data is neither in the first tier nor in the second. We have chosen scenarios that show the difference of hit rates for the applications when we change the size of the fastest tier. So we can study the evolution of the hit rate when we present new cache movement policies in further works.

The eviction policy used in the three scenarios is *Least Recently Used* (LRU) cache management policy [16], parameterized to be triggered when a threshold of 90% of the physical capacity is reached. When this limit is reached, the dirty data is evicted from the filled cache level.

Every applications are run on a single node, with 134GiB memory, an AMD EPYC 7H12 processor with 64 cores. The data node RAM is a DDR4 and the SSD is an NVMe. The HDD storage bay relies on the Lustre filesystem.

TABLE III
COMPARISON OF FILE MOVEMENTS STATISTICS PER AP- PLICATION AND SCENARIOS

		RAM hit rate	Flash hit rate	Miss
Sc 1	NAMD	13.39 %	10 %	76%
	NEMO	99%	0%	1%
	S3DIO	0.1%	0%	99.9%
Sc 2	NAMD	27%	0%	73%
	NEMO	99%	0%	1%
	S3DIO	0.1%	0 %	99.9%
Sc 3	NAMD	27%	0%	73%
	NEMO	99%	0%	1%
	S3DIO	0.1%	0%	99.9%

B. NEMO

NEMO [**?**] (*Nucleus for European Modeling of the Ocean*) is a state-of-the-art modeling framework for research activities in ocean and climate sciences. It is characterized by a significant file re-use, highlighting the importance of a custom file placement policy in the hierarchical storage to keep the most accessed files in the most efficient tier.

a) Application configuration: For our experiment, we use the GYRE configuration, which simulates the seasonal cycle of a double-gyre box model, and which is often used for I/O benchmarking purpose as it is very simple to increase grid resolution and does not require any input file. In our case, the grid resolution is set to 5 and the number of MPI processes to 32 to increase the I/O activity.

b) Characterization of file lifecycle behavior: For this configuration, the application generates a total of 56 files, that are opened and closed 106 times, to realize 9904 writes, and 1600 reads. Over the 32 manipulated files, 10 are re-used which represent a ratio of 32%. Regardless of the used scenario, we observe in table III a hit rate of 99% for the first tier, as the whole dataset fits in tier 1. The misses are due to the cold accesses performed at the beginning of the application's execution, corresponding to the first access of these files on the filesystem before moving them to the highest performing tier.
The lifecycle behavior of NEMO, displayed in figure 4a, shows that the application concentrates its writes mainly on output files, such as `ocean.output` and `output.namelist.dyn`, performing several checkpoints within the application's lifetime. The configuration file `namelist_cfg` is often re-used as well, this time through read-only accesses, accessed at different moments during the application execution. Files corresponding to the checkpointing of the simulation grid (such as `GYRE_*` files) or describing the state of the mesh grid (such as `mesh_mask_*` files) are accessed more sporadically for computation purposes, and always within a short timespan.

c) Consequences on file placement policy: Despite its very high hit rate in this configuration, this application illustrates the need for a file lifecycle-based policy to manage file placement, especially if considered in a setting generating a higher volume of data. As we can see from figure 4a, results files, recognizable by the `*output*` regexp in their filenames, such as `output.namlist.dyn` and `ocean.output`, are moved frequently between the tiers, while a policy based on access frequency could have kept these files in the highest performing tiers until the end of the application execution.
On the other hand, checkpointing files (such as `GYRE_*` files) are only accessed for the duration of the checkpoint, and should be evicted directly as soon as written in the last tier to free some memory. As we can see from this example, this priority-based cache eviction policy, selected from the re-use rate, is not taken into account by the LRU policy available within the tested *burst buffer* setting and used for our experimentation. This leads to the eviction of data from the higher tier that can be re-used in the future, causing an increase of data access latency. This analysis on a file per file basis can only be done through tools like FiLiP.

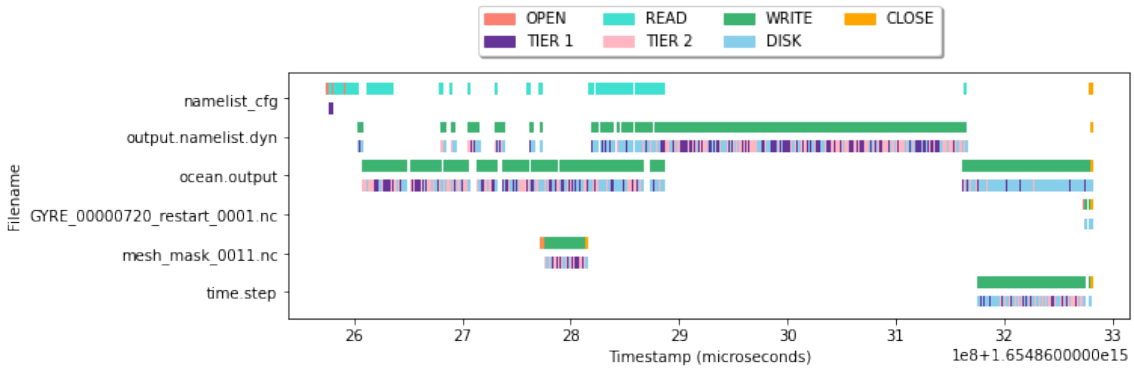
C. S3DIO

S3DIO is an I/O benchmarking application corresponding to the I/O kernel of the S3D application, a continuum scale first principles direct numerical chemical 3D-simulation code. It is an I/Os intensive application with the highest number of operations (6274 reads and 31365 writes) performed on only 6 files (against 56 for NEMO and 14 for NAMD), as can be read from table I. All its files are re-used which shows the interest of keeping them in the higher tiers for as long as possible, and will be a good case study for a further fine anticipated placement strategy of these files according to the time sequence of their re-use.

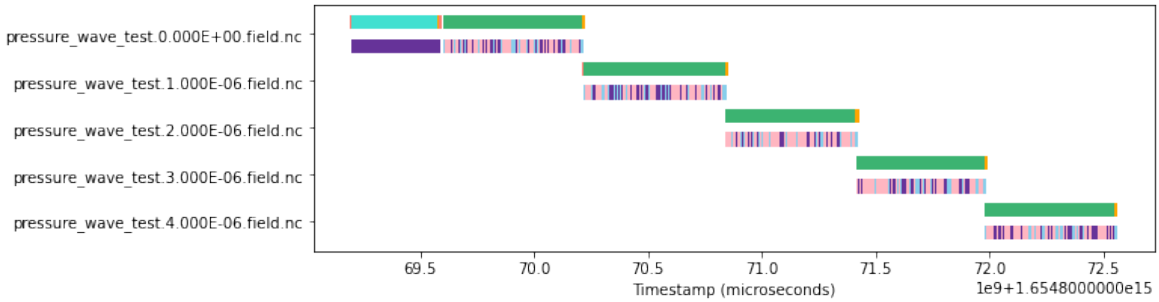
a) Application configuration: Each axis of the three dimensions were set to 800 in order to perform the computations on a large cube and increase the I/O activity of the application. For each of these dimensions, we use four MPI processes. We used a PnetCDF blocking API that allows users to first post multiple requests and later flush them altogether in order to achieve a better performance instead of a Nonblocking API. The restart parameter is set to true in order to reuse a previously written file and obtain more reads operations. The number of checkpoints, which corresponds to the number of output files as well, is set to 5 to obtain large I/Os bursts.

b) Characterization of file lifecycle behavior: The lifecycle behavior of the S3DIO application is representative of an I/O intensive application which puts each of its manipulated files under pressure during all the execution time. In the first scenario, we observe a negligible hit rate close to 0, despite high file re-use, because the accessed blocks of the files are changing all the time. We also observe that when the RAM fills up the data starts to be evicted to flash and the same phenomenon is observed from the flash to the disk. In the second scenario, the hit rate is still very low, even if the higher tiers size has have been increased due to a low blocks re-use. The third scenario leads to a slightly different behavior: the RAM (tier 1) size is large enough to contain all data, but the hit rate is still the same. As can be seen from figure 4b, we can observe that files corresponding to the grid description, characterized by their `*nc*` extension, are accessed successively in long sequences of writes, except for the first file `pressure_wave_test.0.000E+00.field.nc` corresponding to the re-use of the previously written result file.

(a) Nemo File lifecycles in the context of scenario 1



(b) S3DIO lifecycles in the context of scenario 1



(c) NAMD File lifecycles in the context of scenario 1

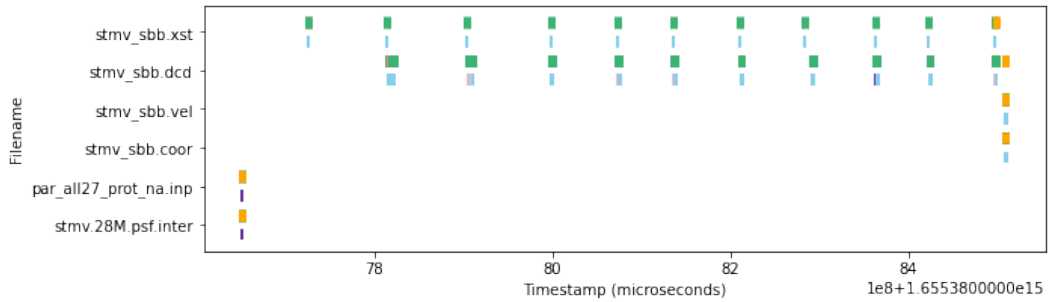


Fig. 4: Lifecycles of the tested case studies

c) Consequences on file placement policy: We can observe that the hit rate is very low because the cold access are the majority. Thus, although the data already read once are entirely in memory, the absence of a prefetch mechanism in the current implementation of the *burst buffer* causes the hit rate to remain very low. This could be improved by a lifecycle based policy that prefetches data from disk when the file is heavily re-used to predict future accesses.

D. NAMD

NAMD [23] is a parallel molecular dynamics code designed for high-performance simulation of large bio-molecular systems. It has the particularity of being very dependent on the storage hardware, due to its large I/O bursts, and is thus a good use-case for FiLiP.

a) Application configuration: For our experiment, we use the Satellite Tobacco Mosaic Virus (STMV-28M) configuration. This is a 3x3x3 replication of the original STMV dataset from the official NAMD site, containing roughly 28 million atoms. NAMD execution goes through 50 steps corresponding to the number of simulation time steps to achieve. Another parameter defines the number of steps after which a checkpoint is performed that is set to 5 to obtain ten checkpoints per run for a significant I/O activity.

b) Characterization of lifecycle behavior: This application has the highest number of file activation, with 244 open and close, and a partial but high file re-use rate, as 10 files are re-used out of the 14. The lifecycle behavior of this application provides several interesting file manipulation cases. We observe that NAMD makes I/Os on many files, each with a constant re-use rate. This results for each file in small sequences of (open-read/write-close) as we can see in figure 4c. We can observe also that the re-use rate is high due to a systematic succession of operations on each file since its

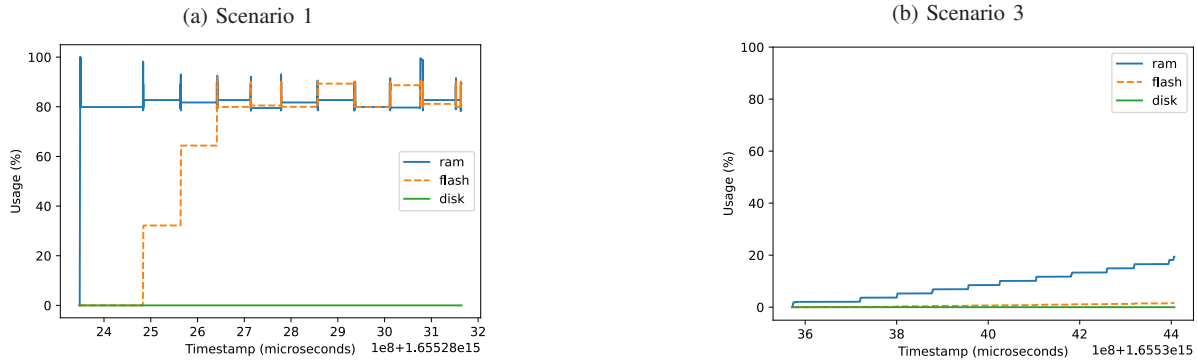


Fig. 5: Evolution of tiers fill for NAMD application

opening. NAMD handles a total of 14 files with a re-use ratio of 71%, that are opened and closed 46 times, for a total 1346 writes and 3959 reads. The application reads a total amount of 2.041 GB of data and gives different hit rates according to the different scenarios and the size of the hierarchical storage.

In the first scenario, we observe a hit rate of 13% because the RAM size is not big enough to contain all the data previously read. The 76% of miss rate corresponds to the first load of data from disk when it is read for the first time. An identical behavior is observed for the second and the third scenarios when all data fetched from disk fits in RAM and the miss rate is only due to first time cold accesses. All the data accessed a second time are already in the most performant tier.

Adding to that, we can observe that the input data, such as `stmv.28M.psf.inter` and `par_all27_prot_na.inp`, are accessed once at the start of the application and never re-used. Other files, such as checkpointing files like `stmv_sbb.xst` and `stmv_sbb.dcd` are heavely re-used.

c) Consequences on file placement policy: In the case of NAMD application, the hit rate can be increased by a data movement policy centered on the file lifecycles: a detection of the heavily re-used files would have outperformed the LRU. Similarly to S3DIO, the hit rate is low because of cold access and the absence of a prefetching mechanism. By using a predicting model that classifies input/output files we could evict this type of input files directly after their use. The checkpoint files are re-used and should be kept in RAM in priority while input ones should be evicted.

d) Impact of file placement on tiers usage: FiLiP also gives the possibility to visualize tiers filling over time. This feature helps us to understand when and why the tier eviction policy is triggered. In the case of our particular implementation of a *burst buffer*, the file movement policy fills in priority the fastest tier: tier 1, and tier2 is synchronized to the tier1 immediately such that it contains the same data.

Once they are removed from the most performant tier, they are still present in the second one and can only be evicted through a threshold based policy. As we can see from figure 5, every time the 90% threshold is reached, the data is evicted from the tier. This visualization allows us to determine how an application reaches the limits of the most efficient tiers.

In figure 5a, we can see that tiers 1 and 2 are very critical resources for the NAMD application. Indeed, when the tier usage threshold of 90% is reached, the data is evicted until another low threshold of 80% is reached. This data is evicted only when it is not dirty anymore, and an inefficient cache movement policy could stall the application while the data is awaiting eviction. In figure 5b, we present the evolution within scenario 3, where the higher tiers are large enough to contain the whole data, and therefore the eviction policy is never triggered. This confirms that an efficient file placement policy for hierarchical storage should necessarily take into account the size of the available storage, and especially for restricted resources. For NAMD application, the RAM hit rate goes from 27% in the case of a large RAM (scenario 3), as displayed in table III, to 13% in the case of smaller one (scenario 1).

V. Conclusion and Further Works

In this work, we have presented a file-based profiling tool called FiLiP to consider I/O from another perspective in the case of hierarchical storage, by giving the possibility to investigate file re-use properties present in HPC and scientific computing. This tool allows the understanding of how these files are used by the applications during their entire life cycle and the consequences of these re-use on the file movements through the hierarchical storage. Using FiLiP, we analyze and describe the file behavior of 3 different HPC applications: NEMO, S3DIO and NAMD, and give some interesting insights to better understand file manipulations and allow in the future a smarter file placement policies with reduced miss rates.

References

[1] Fastapi. https://fastapi.tiangolo.com/.

[2] IO Instrumentation. https://atos.net/wp-content/uploads/2018/07.

[3] Vue.js. https://vuejs.org/.

[4] A. ben Ameur, A. Araldo, and T. Chahed. Cache allocation in multi-tenant edge computing via on-line reinforcement learning. In *IEEE ICC*, 2022. DOI: 10.48550/arXiv.2201.09833. arXiv:2201.09833.

[5] P. Carns, K. Harms, W. Allcock, C. Bacon, S. Lang, R. Latham, and R. Ross. Understanding and improving computational science storage access through continuous characterization. *ACM Transactions on Storage*, 7:1–26, 2011. DOI: 10.1145/2027066.2027068.

[6] R. F. da Silva, S. Callaghan, and E. Deelman. On the use of burst buffers for accelerating data-intensive scientific workflows. In *Proceedings of the 12th Workshop on Workflows in Support of Large-Scale Science - WORKS* '17, pages 1–9. ACM Press, 2017. DOI: 10.1145/3150994.3151000.

[7] M. Diener, E. H.M. Cruz, L. L. Pilla, F. Dupros, and P. O. A. Navaux. Characterizing communication and page usage of parallel applications for thread and data mapping. *Performance Evaluation*, pages 18–36, 2015. DOI: 10.1016/j.peva.2015.03.001.

[8] F. R. Duro, J. G. Blas, and J. Carretero. A hierarchical parallel storage system based on distributed memory for large scale systems. In *Proceedings of the 20th European MPI Users' Group Meeting on - EuroMPI '13,* pages 139–140. ACM Press, 2013. DOI: 10.1145/2488551.2488598.

[9] B. Elis, D. Yang, O. Pearce, K. Mohror, and M. Schulz. QMPI: A next generation MPI profiling interface for modern HPC platforms. *Parallel Computing Journal*, 96, 2020. DOI: 10.1016/j.parco.2020.102635.

[10] Y. Han, R. Wang, and J. Wu. Random caching optimization in large-scale cache-enabled internet of things networks. *IEEE Transactions on Network Science and Engineering*, 7(1):385–397, 2020. DOI: 0.1109/TNSE.2019.2894033.

[11] M. Hashemi, K. Swersky, J. A. Smith, G. Ayers, H. Litz, J. Chang, C. Kozyrakis, and P. Ranganathan. *Learning Memory Access Patterns*. *Technical Report* arXiv:1803.02329, Cornell University, 2018. DOI: 10.48550/arXiv.1803.02329.

[12] G. Hasslinger and K. Ntougias. Evaluation of caching strategies based on access statistics of past requests. In *International Confernece on Measurement, Modelling and Evaluation of Computing Systems and Dependability and Fault tolerence*, 2014. DOI: 10.1007/978-3-319-05359-29.

[13] J. L. Hennessy and D. A. Patterson. *Computer Architecture: A Quantitative Approach*. Morgan Kaufmann, Amsterdam, 5th edition, 2012. ISBN: 978-0-12-383872-8.

[14] H. Herodotou and E. Kakoulli. Automating distributed tiered storage management in cluster computing. *Proceedings of the VLDB Endowment*, 13(1):43–56, 2019. DOI: 10.14778/3357377.3357381.

[15] S. Jiangand X. Zhang. LIRS: An Efficient Low Inter-reference Recency Set Replacement Policy to Improve Buffer Cache Performance. *ACM SIGMETRICS Performance Evaluation*, 30(1):31–42, 2002. DOI: 10.1145/511399.511340.

[16] R. Karedla, J. S. Love, and B. G. Wherry. Caching strategies to improve disk system performance. *Computer Journal*, 27(3):38–46, 1994. DOI: 10.1109/2.268884.

[17] G. Kestor, R. Gioiasa, D.J. Kerbyson, and A. Hoisie. Enabling accurate power profiling of HPC applications on exascale systems. In *proceedings of the 3rd International Workshop on Runtime and Operating Systems for Supercomputers*, number 4, pages 1–8, 2013. DOI: 10.1145/2491661.2481429.

[18] J. S. Kim. *Parallel I/O Profiling and Optimization in HPC Systems*. PhD thesis, Pennsylvania State University, 2014.

[19] J. S. Kim, Y. Zhang, S. W. Son, M. Kandemir, W k. Liao, R. Thakur, and A. Choudhary. IOPro: a parallel I/O profiling and visualization framework for high-performance storage systems. *supercomputing*, pages 840–870, 2015. DOI: 10.1007/s11227-014-1329-0.

[20] N. Liu, J. Cope, P. Carns, C. Carothers, R. Ross, G. Grider, A. Crume, and C. Maltzahn. On the role of burst buffers in leadership-class storage systems. In *IEEE 28th Symposium on Mass Storage Systems and Technologies (MSST)*, pages 1–11. IEEE, 2012. DOI: 10.1109/MSST.2012.6232369.

[21] N. Megiddo and D. S. Modha. ARC: A self-tuning, low over- head replacement cache. In *2nd USENIX Conference on File and Storage Technologies (FAST 03)*, pages 115–130, 2003. DOI: 10.5555/1090694.1090708.

[22] D-J Oh, Y. Moon, D. K. Ham, T. J. Ham, Y. Park, J. W. Lee, J. H. Ahn, and E. Lee. Maphea: A framework for lightweight memory hierarchy-aware profile-guided heap allocation. *ACM Transactions On Embedded Computing Systems*, 2022. DOI: 10.1145/3527853.

[23] J. C. Phillips, D. J. Hardy, J. D. C. Maia, J. E. Stone, J. V. Ribeiro, R. C. Bernardi, R. Buch, G. Fiorin, J. Henin, W. Jiang, R. McGreevy, M. C. R. Melo, B. K. Radak, R. D. Skeel, A. Singharoy, Y. Wang, B. Roux, A. Aksimentiev, Z. Luthey-Schulten, L. V. Kale, K. Schulten, C. Chipot, and E. Tajkhorshid. Scalable molecular dynamics on CPU and GPU architectures with NAMD. *Journal of Chemical Physics*, 2020. DOI: 10.1063/5.0014475.

[24] G. Quan, J. Tan, A. Eryilmaz, and N. B. shroff. A new flexible multi-flow LRU cache management paradigm for minimizing misses. In *proceedings of the ACM on Measurement and analysis of computing systems*, volume 3, pages 1–30, 2019. DOI: 10.1145/3341617.3326154.

[25] Md. W. Rahman, N. S. Islam, X. Lu, D. Shankar, and D. K. Panda. MR-Advisor: A comprehensive tuning, profiling, and prediction tool for mapreduce execution frameworks on hpc clusters. *Journal of Parallel and Distributed Computing*, 120:237–250, 2018. DOI: 10.1016/j.jpdc.2017.11.004.

[26] M. Rashti, G. Sabin, D. Vansickle, and B. Norris. WattProf: A flexible platform for fine-grained HPC power profiling. In *IEEE International Conference on Cluster Computing*, pages 698–705, 2015. DOI: 10.1109/CLUSTER.2015.121.

[27] M. Romanus, R. B. Ross, Robert, and M. Parashar. Challenges and Considerations for Utilizing Burst Buffers in High-Performance Computing. Technical Report arXiv:1509.05492, Cornell University, 2015. DOI: 10.48550/arXiv.1509.05492.

[28] W. Teng, B. Surendra, D. Bin, and T. Houjun. Univistor: Integrated hierarchical and distributed storage for hpc. *IEEE International Conference on Cluster Computing (CLUSTER)*, pages 134–144, 2018. DOI: 10.1109/CLUSTER.2018.00025.

[29] K. R. Vaddina, L. Lefevre, and A. C. Orgerie. Experimental workflow for energy and temperature profiling on hpc systems. In *IEEE Symposium on Computers and Communications*, pages 1–7, 2021. DOI: 10.1109/ISCC53001.2021.9631413.

[30] K. Wu, Z. Guo, G. Hu, K. Tu, R. Alagappan, R. Sen, K. Park, A. Arpaci-Dusseau, and R. Arpaci-Dusseau. The Storage Hierarchy is Not a Hierarchy: Optimizing Caching on Modern Storage Devices with Orthus. In *Usenix Conference on File ans Storage Technologies*, 2021.

[31] C. Zhong, M. C. Gursoy, and S. Velipasalar. A deep reinforcement learning-based framework for content caching. In *52nd Annual Conference on Information Sciences and Systems (CISS)*, pages 1–6, 2018. DOI: 10.1109/CISS.2018.8362276.

Adrian Khelili is a PhD Student at University of Paris Saclay and Atos R&D working on "Intelligent data placement on tiered storage. He has a mSc in computer science and is particularly interested in Data Science and its applications to complex systems.

Sophie Robert has a PhD in Computer Science on the application of black-box optimization method for the optimization of complex systems. She is a researcher at Atos R&D and her main research interest is the intelligent placement of files across hierarchical storage, and especially in the case of burst buffers.

Soraya Zertal is professor in computing science at university Paris Saclay and a member of the Architecture and Parallelism research group at Li-PaRAD lab. Her main research interests include parallel architectures and storage systems especially in HPC context, analytical modeling, simulation and adaptive/optimization strategies for data placement. She published several research articles, held a series of research grants and supervised Masters and PhDs students in the area.

Saving Bit-flips through Smart Overwrites in NVRAM

Arockia David Roy Kulandai, *Student Member, IEEE*, Thomas Schwarz, *Senior Member, IEEE*

***Abstract*—New generations of non-volatile random access memories will combine the best features of memory (access times, byte addressability) with the best features of storage (non-volatility, low costs per byte). Some, like PCM, have a limited endurance. All will only consume energy when accessed, but writes will use much more energy than reads. These characteristics put a cost on flipping bits in memory. Bit-flip aware data structures lower the number of bits flipped by not resetting fields to zero to indicate a deleted record but by using bit-maps. If given a choice of where to over-write data, they will select the location which results in a lower number of bit-flips. We calculate the expected bit-flip savings of this strategy and derive a rule to determine the number of the possible candidate locations.**

***Index Terms*—PCM endurance, NVRAM, Smart writes for PCM.**

I. INTRODUCTION

Processed information continues to grow exponentially [16]. The emergence of Non-Volatile RAM (NVRAM) technologies that combine the advantages of storage (non-volatility, low-costs, large size) and of memory (fast access times, byte-addressability) allow systems to combine the functions of memory and storage in a single layer. These types of NVRAMs do not use energy when their data is at rest. Writes typically use much more energy than reads. Some, like Phase Change Memory (PCM) have limited endurance for over-writes. (Their endurance is more than sufficient for use as main memory as long as the over-write load is decently distributed over a large memory. As memories in the Terabyte range are affordable, this is not a problem.) These behaviors put a premium on bit-flip avoiding behavior.

A large number of schemes to save bit-flips in hardware exists. Fundamental is *Data Comparison Write* (DCW) that eliminates redundant bit writes by first reading the word before writing it and only setting and resetting bits that need to be changed [18], [19]. On the software side, Bittman and colleagues [3], [4] observe that data structures can save considerably on the number of bit-flip operations. One ingredient of these bit-flip aware data structures is to try to overwrite new data with stale data of roughly the same type. Slight encoding can increase the effect for web-content [10] and for pointers [11]. Besides observing that storing pointers as the result of an exclusive-or with another pointer, Bittman *et al.* found that bit-flips can be saved if a data structure does not invalidate keys by zeroing them out but by using a bit to indicate whether a key entry exists or not. Unfortunately, they did not elaborate on this observation.

In this article, we investigate the amount of savings to be had by using an "is-valid" bit-array instead of using overwrites. We also follow up on another suggestion by Bittman, namely that selecting a candidate stale key among a set of keys can lead to additional savings. We therefore determine experimentally the number of bit-flips if we choose the best key among k to overwrite, with k varying from 2 to 10. We can then use these numbers to determine the best strategy for saving bit-flips. Because processors communicate with memory through several levels of cache, we investigate whether loading additional cache lines in order to find better candidates for overwrites is advantageous.

Our goal is to understand how the internal character of data interacts with bit-flip pressure, not to build a new data structure. The latter is the ultimate goal. We contribute to it by trying to understand the fundamental building blocks. As a consequence, our setup is not a complete data structure, but a test bed to answer the question how much better it is to keep stale data (marked as such by a valid-bit) as opposed to zeroing it out. For starters, zeroing out deleted keys has the advantage of preventing reading deleted keys so that we are protected against software faults.

In the following, we first describe our data structure. We then discuss the case of uniformly distributed random bit-strings. To start our experimental work, we first discuss the impact of encoding of non-Latin alphabets. We then present our results using a number of data sets, using different natural languages, and also a floating point key. We did not try out integer keys such as social security numbers or telephone numbers, as they were not available for privacy reasons. We then verify our data by a closer simulation using data from Amazon product reviews. We then calculate the optimal energy saving strategies.

II. SETUP

There are many data structures that implement a key-value store, with key-based operations of insert, delete, look-up, and update. The various types of B-trees also implement a range query (for a range of keys). The importance of B-tree can hardly be exaggerated.

In contrast to the B-tree in general, B-tree node implementation has received less interest [8]. Early on, the prefix B-tree used prefix and suffix compression to place more keys in a node and therefore achieve better performance [2], [14]. B-tree nodes that do not use key compression often

D. Roy and T. Schwarz are with the computer science department at Marquette University, Milwaukee, Wisconsin, USA.

E-mails: david.roy@sxca.edu.in and thomas.schwarz@marquette.edu.

DOI: 10.36244/ICJ.2022.4.5

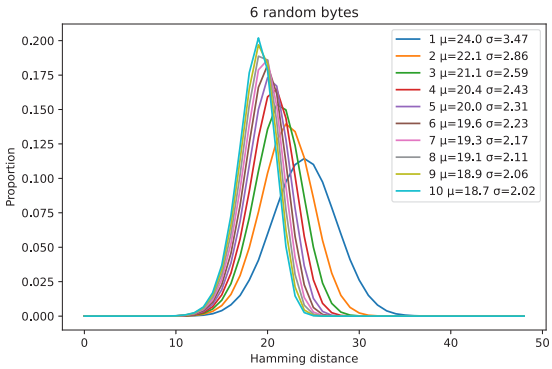


Fig. 1: Average number of bit-flips when overwriting a uniformly distributed, random 6B key. We select the key among k keys, $k = 1,2,...,10$.

place fixed-length keys in a contiguous array. Our results in what follows show that marking a key as invalid, and then overwriting it with a new key, results in bit-flip savings. Some node implementations will keep keys in order, which almost eliminates the chance to be able to select between two stale keys for overwrite. Other implementations already facilitate key insertions by using an auxiliary data structure to preserve the order. In this case, all of our experimental results tell us what bit-flip savings can be achieved. A thorough investigation of B-tree node structures, their interaction with caches, and their relations to bit-flip savings is left to the future. The clfB-tree [9] for example packs B-tree nodes into a cache line but does not consider bit-flips.

Key-value stores are of course not limited to B-trees and their derivatives. They can be based on hashing or other types of trees. In the context of NVRAM, we might store many sets of pairs of keys and pointers to records. Incidentally, the bit-flip aware manipulation of pointers is a different issue [11]. We now study in more detail the bit-flip behavior of the key portion of such a data structure. First, we consider the case of random keys, not because this is a frequent use case, but to set a base line.

III. The Random Case

We now study the expected number of bit-flips overwriting a fixed length key or overwriting the best of k candidate keys. This is a value that depends on the population of possible keys.

The simplest model for the keys is a string of random bits, where each bit is set with probability 50%. The Hamming distance between two such keys is binomially distributed with parameters n, the length of the key, and probability $p = 0.5$. The minimum Hamming distance between one such key and k other keys is the first order statistics of binomial distributions. If $\mathbb{B}(k;n,p)$ is the Cumulative Distribution Function (CDF) of the Binomial distribution with n and p, i.e.

$$\mathbb{B}(\nu;n,p) = \text{Prob}(X \leq \nu) = \sum_{i=0}^{\nu} \binom{n}{i} p^i (1-p)^{n-i}$$

TABLE I
Expected minimum of k normally distributed random values with mean $\mu = 24$ and standard deviation $\sigma = \sqrt{48/4}$ and exact numbers for a Binomial distribution with parameters $n = 48$ and $p = 0.5$.

k	Expected Value Normal Appr.	Expected Value Exact
1	24.0000	24.0000
2	22.0456	22.0507
3	21.0684	21.0760
4	20.4341	20.4442
5	19.9714	19.9838
6	19.6103	19.6250
7	19.3159	19.3328
8	19.0685	19.0875
9	18.8558	18.8767
10	18.6696	18.6925

then the CDF $\Phi(\nu)$ of the minimum out of k is given by

$$\begin{aligned} 1 - \Phi(\nu) &= \text{Prob}(\min(X_1, X_2, \ldots X_k) > \nu) \\ &= \prod_{i=1}^{k} \text{Prob}(X_i > \nu) \\ &= (1 - \mathbb{B}(\nu;n,p))^k. \end{aligned}$$

For reasonably small values, the exact formula can be evaluated. The binomial distribution can be approximated well with a normal distribution, but the order statistics for independently and identically distributed normal distribution only has a closed form even for the expectation for very small values of k [1].

We give the values of the expectation of the minimum of k normally distributed independent random variables with parameters $\mu = 0.5 \times 48$ and $\sigma = \sqrt{48 \times 0.5^2}$, i.e. where $n = 48$, which is the approximation for our experimental data in Table I.

Even in the random case, we save bit-flips by not zeroing out deleted keys. If we delete a key and then insert another one and if we use the valid-bit array, the valid-bit array itself has one bit set and reset (2 flips) and the expected costs of overwriting the key (of length 6B) is 24 flips. Zeroing out costs 24 bit-flips and overwriting costs also 24 bit-flips for a total of 48 bit-flips.

IV. Experimental Data

The efficiency of overwriting stale keys instead of zeroing out depends on the nature of the keys. We now gather experimental data on various data-sets. The most important class of keys that do not behave like random numbers are strings of characters. To avoid an anglo-centric view, we first discuss non-Latin alphabets. Unfortunately, our lack of knowledge of Chinese does not allow us to test for keys taken from this important language. We then use several data-sets with different types of keys in different languages to determine their bit-flip propensity. Finally, we use a different dataset to confirm the predictions based on our measurements for a closer simulation of a hypothetical data structure made up of key – pointer to record entries.

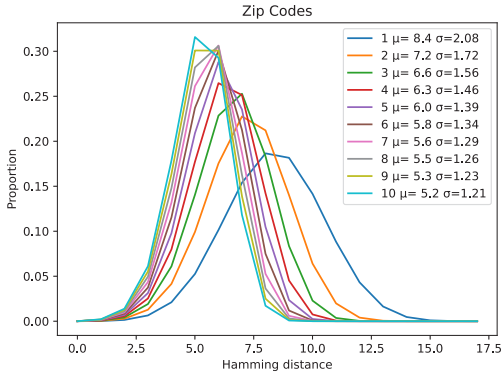


Fig. 2: Average number of bit-flips when overwriting a 4B zip code from the credit industry complaint data set.

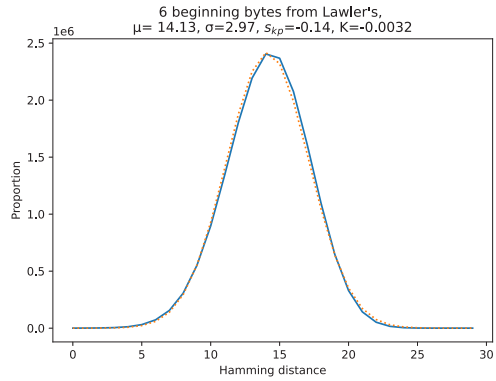


Fig. 3: Average number of bit-flips when overwriting a key in the Lawler corpus with another one and comparisonwith the normal distribution with the same mean and standard deviation.

A. Non-Latin Alphabets

At the byte level, encodings matter. Given its importance, we concentrate on keys encoded with utf-8, a version of Unicode very popular for web-documents. The utf-8 encoding is very efficient for English text, as the English character set is encoded just as the lower half of ASCII. For German, French, Spanish, or other languages using a Latin character set, the relatively infrequent letters with accents and Umlauts are stored in two bytes.

For non-Latin alphabets such as Tamil's Dravidian and Hindi's Devanagari script, utf-8 is not space efficient. Both scripts vary 7 bits encoded within three bytes for each character. In contrast, the less common utf-16 only uses two bytes for each Dravidian or Devanagari character. The *Standard Compression Scheme for Unicode* (SCSU) defined in the Unicode Technical Standard Nr. 6 uses *dynamically positioned windows* so that characters belonging to small scripts such as Devanagari can be encoded in a single byte [6], [7]. As an alternative to SCSU, Vijayalakshmi and Sasirekha propose to map the Tamil characters to the upper half of the ASCII encoding, i.e. between 0x80 and 0xff, characterized by the first bit being set [17]. While such a compression scheme uses space more efficiently, the costs of compression and decompression might mitigate against their use. If such a compression scheme is used, keys in Tamil or Hindi behave like keys in English or German. If instead utf-8 is used, the larger number of bytes to be read increases the read energy consumption, but in general, overwrites are close in efficiency to that of English text. Only the interference of punctuation marks, white spaces, or ASCII numerals cause alignment issues and generate more bit-flips and hence higher write energy use.

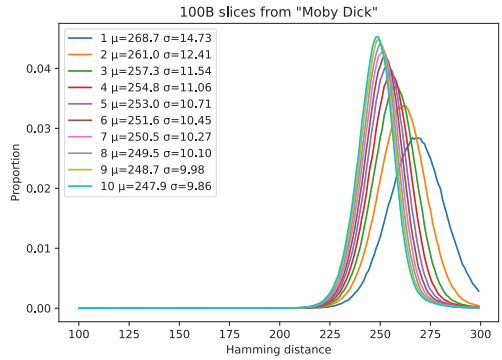


Fig. 4: Average number of bit-flips when overwriting a 100B slice with the best of a set of k, k = 1,2,...,10 randomly selected slices not containing the original slice.

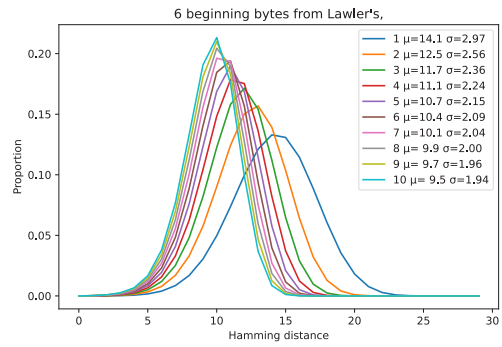


Fig. 5: Average number of bit-flips when overwriting a 6B key taken from the first 6 bytes of the words in Lawler's vocabulary list with the closest of k keys from the same source, where k varies k = 1,2,...,10.

B. Results

We used the following corpora for our experiments:
(1) The zip codes from a Kaggle dataset collected by A. Kumar on consumer complaints of financial products from the Consumer Financial Protection Bureau (CFPB) Open Tech site [12]. There are 26800 unique zip-codes, stored as integers in four bytes. Since the largest zip-code is 99999, which is in hexadecimal 0x1869f, only 17 bits are ever set.
(2) The novel "Moby Dick" from Project Gutenberg, downloaded as utf-8. We divided the novel into slices of 100 bytes each.

TABLE II
FREQUENCY OF BITS SET IN A BYTE

Bits	0	1	2	3	4	5	6	7	Total Bits Set	δ
Zip codes	0.44	0.33	0.33	0.34	0.34	0.34	0.32	0.28	2.12	2.12
Zip codes (last 16 b)	0.50	0.50	0.50	0.50	0.51	0.51	0.49	0.43	3.93	3.90
German	0.56	0.49	0.53	0.33	0.33	0.85	0.98	0.04	4.08	2.24
German (miniscules)	0.56	0.46	0.53	0.33	0.33	0.98	0.98	0.04	4.20	2.11
English (Moby Dick)	0.45	0.34	0.48	0.34	0.25	0.96	0.78	0.00	3.60	2.34
English (Lawler)	0.59	0.40	0.54	0.40	0.31	1.00	0.99	0.00	4.22	2.00
Tamil (Tirukkural)	0.28	0.48	0.52	0.51	0.14	0.85	0.33	1.00	4.12	2.37
Tamil (Agananuru)	0.28	0.47	0.52	0.51	0.14	0.85	0.33	1.00	4.10	2.45
Hindi (Bible)	0.22	0.14	0.48	0.18	0.12	0.91	0.33	0.90	3.28	1.65
Hindi (Ambedkar)	0.21	0.16	0.53	0.18	0.15	0.87	0.33	0.99	3.49	1.76
Earthquakes	0.41	0.42	0.41	0.38	0.40	0.42	0.60	0.39	3.44	3.25

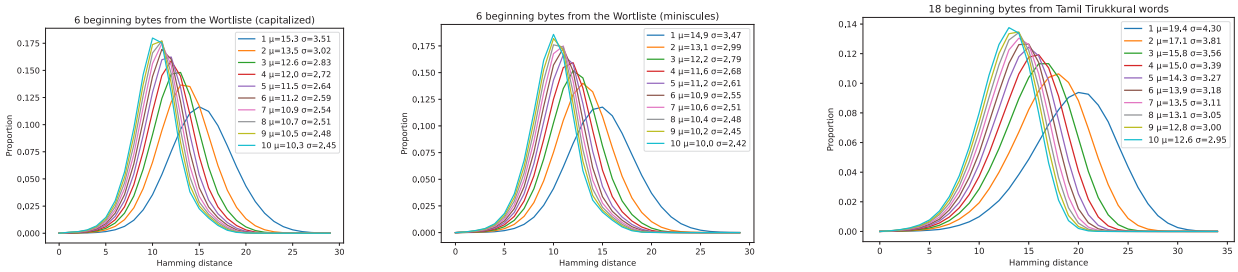


Fig. 6: Average number of bit-flips when overwriting a 6B key taken from the first 6 bytes of the words in Davidak's list with the closest of k keys from the same source, where the number k of candidates varies between 1 and 10. The graph on the left shows the results with upper case letters, the one in the middle with upper case letters converted to minuscules, and the one on the right from the Tirukkural.

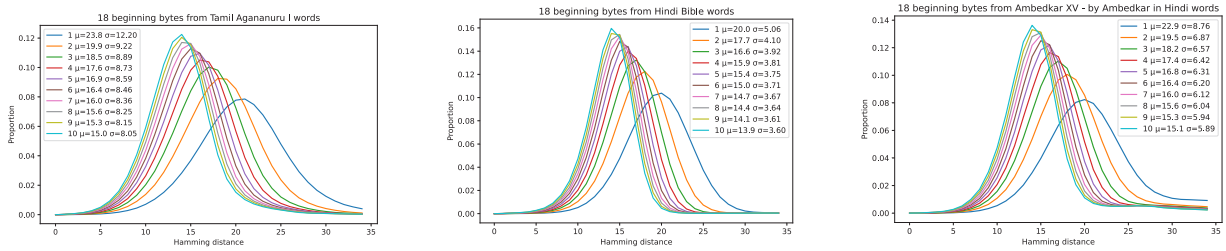


Fig. 7: Average number of bit-flips when overwriting a 6B key taken from the first 6 symbols (or 18B) from long words in Agananuru (left), a Hindi translation of the Old Testament (middle) and a volume of Dalit-leader B.R. Ambedkar (right).

(3) A list of English words by Lawler [13]. We used the first 6 bytes of each word at least this long.
(4) A word list *Wortliste* of German words collected by the pseudonymous Davidak [5]. We used the first 6 bytes of each word at least this long.
(5) The same list moving all capital letters to miniscules.
(6) A list of beginnings of words in Tamil. We used Tirukkural, the classic collection of poems from the 1st century by Thiruvalluvar in utf-8 format. We extracted the first six characters, i.e. first 18B, but ensured uniqueness.
(7) A similar list of beginning of words in Tamil from Agananuru, another poetry collection.
(8) A list of beginnings of words in Hindi. We used a translation of part of the Old Testament in the Bible.
(9) A similar list in Hindi taken from Volume 15 of Ambedkar's writings.
(10) Longitude and latitudes stored as floating point numbers from a list of major earth-quakes from 1974 to 2001. We mixed longitudes and latitudes and removed duplicate values from the list.

We use the zip codes as keys as an example where a "real-life" data-set has keys that are essentially random, where each bit is distributed with a Bernoulli distribution with parameter $p = 0.5$. A zip code stored as an integer uses two bytes and additionally the least significant bit of a third byte. As we can see from Figure 2, the frequency distributions closely resemble the one from Figure 1. Indeed, the means of the minima of k Binomial distributions with parameters $n = 17$ (corresponding to the 17 bits used for a zip code) and $p = 0.5$ are 8.5, 7.34541, 6.76812, 6.39478, 6.12341, 5.91242, 5.74099, 5.59733, 5.47414, and 5.36662 for $k = 1, \ldots, 10$.

Another example for this behavior would be keys derived from a good hash function such as MD5 or the SHA series.

We first calculated the bits set in each text corpus, Table II. The number for Latin alphabets is quite close, but still reflects differences. The numbers for the non-Latin alphabets are quite different. From these numbers alone, we can understand why overwriting text from one corpus with text from another corpus does not flip on average four bits per byte. Depending on the corpus, we can also define a most likely byte. Instead of replacing a deleted key with zero bytes, we could replace it with this most-likely byte. Unfortunately, this is somewhat dangerous, as the most likely byte is a normal letter, the character 'a' for German and English, and not special, like the zero byte. The last column of Table II gives the average distance δ of a byte in the corpus to the most-likely byte. Overwriting stale keys with a sequence of this most-likely byte costs 2δ bit-flips, resulting in strong savings compared to a policy of zeroing out stale keys. In the case of keys in a non-Latin alphabet, stored as a combination of bytes, we still advocate the use of a single most likely byte in order to avoid alignment problems such as those resulting from using (ASCII) digits or punctuations within the key, as the latter are encoded as a single byte.

Next, we calculate the expected number of bit-flips of overwriting with a new key, either a single, stale key or the closest (according to the Hamming distance) key of k candidate stale keys. We determined the Hamming distance between each key and the best of a sample of k candidate keys for a total of 300 samples per key. The results are given in Figures 5, 4, 6, and 7. The results look remarkably similar. Especially for $k = 1$, where we just overwrite a single key, the distribution looks remarkably similar. Figure 3 compares the value for the Lawler corpus with a normal approximation. (The Lawler distribution is discrete, and the normal approximation uses the difference between the CDF of the normal distribution at $i + 0.5$ and $i - 0.5$ as the discrete PDF, as is usual.) While optically, the approximation is very good, but skew and kurtosis are significantly different and as the χ^2 value is over $20,000$, the frequency distribution is definitely not normally distributed. When we look at the mean of order statistics (e.g. the minimum of k independently and identically distributed random variables,) then the difference also becomes obvious.

The numbers for the earthquake data set have peculiarities that we can ascribe to the nature of representations of floating point number. The curve for $k = 1$ is tri-modal and all other ones are bi-modal. Also, the decrease in the expected value μ_k of the bit-flips when selecting from k candidates is less pronounced. Despite these differences, the overall picture remains roughly the same.

The savings obtained by using more candidate keys for overwriting are remarkably similar. If the number of bit-flips has mean μ and a standard deviation of σ, then selecting the best of four candidate key fields (with previously deleted keys) lowers the expected number of bit-flips to $\mu - \sigma$. Moving to the best of ten candidate fields does not lower the expected number of bit-flips to $\mu - 2\sigma$.

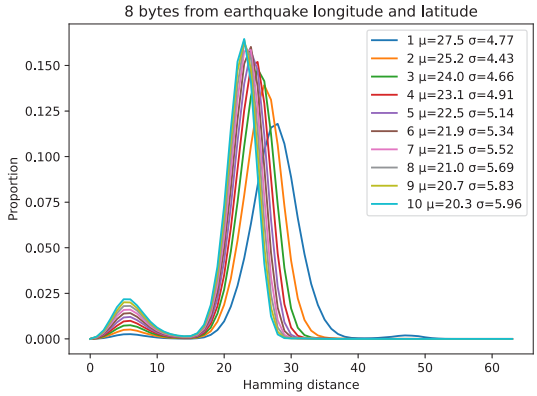


Fig. 8: Average number of bit-flips when overwriting a 8B key formed by a floating point number representing the longitude and latitude of epicenters of major earthquakes from 1970 to 2014. We select the best of k candidate keys, where k varies from 1 to 10.

C. Confirmation

In our fixed sized bucket of key – pointer to record data structure keys marked as deleted stay until they are overwritten. Therefore, an outlier from the population might stay much longer than expected. We call this the *persistent outlier* phenomenon. Basically, the set of candidate deleted keys is no longer random in such a bucket.

To test this, we use a data set downloaded from Kaggle [15] that contains product reviews. We used the 14B long Amazon user identifiers as our key stand-ins. When we simulated a single slot by overwriting the current user ID with the following user ID, we notice that there is a visible deviation from the normal bell-shaped frequency curve.

We then simulated the behavior of a small bucket with k keys. After filling up the bucket, all keys are deleted. A record with a certain key is inserted and in a short time deleted. When the key is inserted, we look for the nearest deleted key according to the Hamming distance. We calculated the number of bit-flips for this scenario going through all the user IDs. As we can see behavior does not quite match the previous data sets. The decrease in the mean of number of bit-flips is less pronounced.

A comparison with the minimum number of bit-flips when overwriting one of the candidates in a k-element set, Figure 9, bottom, does show some deviations. The calculated standard deviation of the bit-flip numbers σ is considerably and consistently smaller. On the other hand, the means are almost equal. Thus, the persistent outlier is not a problem, at least not for this data set.

V. Recommendations

We now combine our results to evaluate performance. We measure the expected costs for each strategy in multiples of the energy of one bit being written. For example, if the read energy is one tenth of the energy of a write, then writing 15 bits and reading 20 bits costs the energy spent to write to 17 bits.

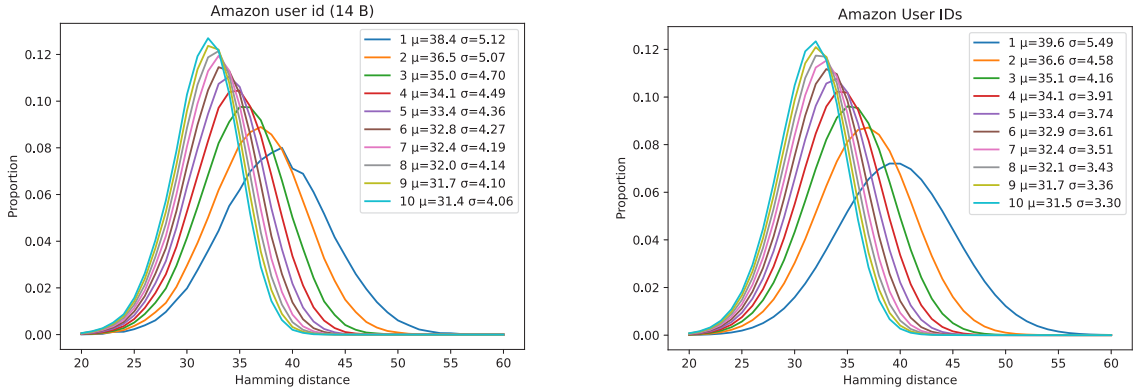


Fig. 9: Observed number of bit-flips for Amazon User IDs. The left shows the numbers when actually using the scheme, the right shows the numbers when using random elements.

We first consider the case where data on the NVRAM is accessed directly, without a cache. This might be the case for an embedded device. The costs for the zeroing strategy are simply twice the average number of bits set per byte times the size of the key. The costs for checking k candidate state keys to find the write victim to overwrite are 2 bits in the valid-bit field. The number of bits written is determined by the corresponding experimental value. We need to add to this the costs of reading $k-1$ candidates. The cost of reading the first is already included in the write costs as we are using read before write. If ρ is the ratio of read over write energies, then this adds $\rho \times (k-1)$ times the size of the key to our energy bill.

Figure 10 shows the energy costs for uniformly distributed random keys of length 4B. The zeroing strategy loses against the simple overwrite strategy. If reads take much less energy than writes, comparing a key to be inserted with up to five stale keys makes sense. As the read energy increases slightly, the number of comparisons goes down. Figure 11 gives the numbers for 6B keys derived from Lawler's word list, representing keys that are English strings. Here, zeroing is even less attractive. Depending on the costs of reads over writes, it makes sense to read up to four stale keys. Note in both cases that a more typical value for ρ is 0.15, so that the recommendation in both cases is to only select one stale key and over-write it.

Our argumentation breaks down, of course, if caching is used. Whenever we access a byte, we will cause a cache line's worth of data to be read. When the cache line is written back to NVRAM, only the bits that have changed are actually written, leading to the use of energy. To exploit the use of caching, our data structure needs to be cache-line aware. Presumably, the valid-bit array is part of the header of the bucket data structure, which will need to be read for every access. We can also assume that bucket data structures are cache-line aligned. Thus, each bucket will consist of a number of sub-buckets, each contained in a single cache-line.

If we want to insert a key, and there is at least one slot in the first sub-bucket, we have to decide whether we want to read more sub-buckets with open slots. When we do so, each sub-bucket accessed costs us read energy. As before, let us denote by rho the ratio of the energy costs of reading a bit over the energy costs of writing a bit. A typical cache-line has 64B or 512b. If we decide to load a sub-bucket of this size into cache, we have 512ρ costs. Denote the expected number of bits written after finding the best of k candidates, $1 \leq k$, with μ_k. Then on the other side of the ledger, if we have already located i stale data items and now decide on whether to read a sub-bucket with j stale data items, then reading the sub-bucket will save $\mu_i - \mu_{i+j}$ writes, but costs the equivalent of 512ρ bits written. Thus, we should read a sub-bucket if

$$\mu_i - \mu_{i+j} > 512\rho.$$

Since a typical value for ρ is $1/5$ or more for PCM, the costs savings have to be at least 100 bits written. A review of our experimental results suggests that savings of more than 1b per byte key length is unrealistic. In Figure 12, we illustrate this decision procedure. If i candidate keys are already read, we select the unread sub-bucket with the most number of keys. Assume that there are j keys in it. We then calculate the minimum number of the ratio of write energy per bit over read energy per bit (that is $1/\rho$) to save bitflips by reading the yet unread sub-bucket. Of course, if we read the beginning of the bucket and do not find a candidate for overwriting there, we will have to read a sub-bucket with a candidate. If there is no such sub-bucket, we will have to create an overflow page. The values for $1/\rho$ are almost exclusively quite high and all are higher than for currently proposed NVRAM technologies.

We give six examples in Figure 12, namely keys from Lawler's corpus, keys of 18B that behave like the keys in Lawler's corpus, keys of 18B that behave like the German word list, keys of 6B that taken from the capitalized version of the German word list, keys of 18B from the Hindi Ambedkar collection, and 18B keys from our first Tamil corpus. The

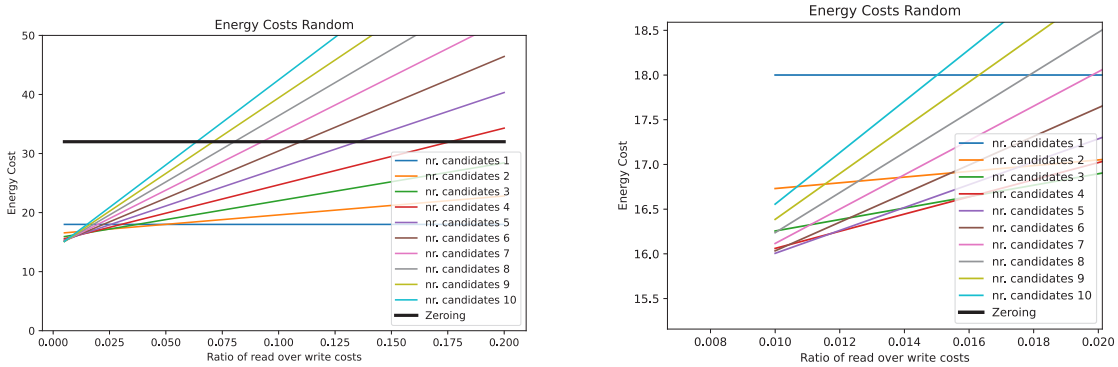


Fig. 10: Energy costs (in multiples of the energy of one bit written) using the Zeroing strategy and the best out of k overwrite strategy for random keys of length 4 bytes. The right is a blowup of the left figure.

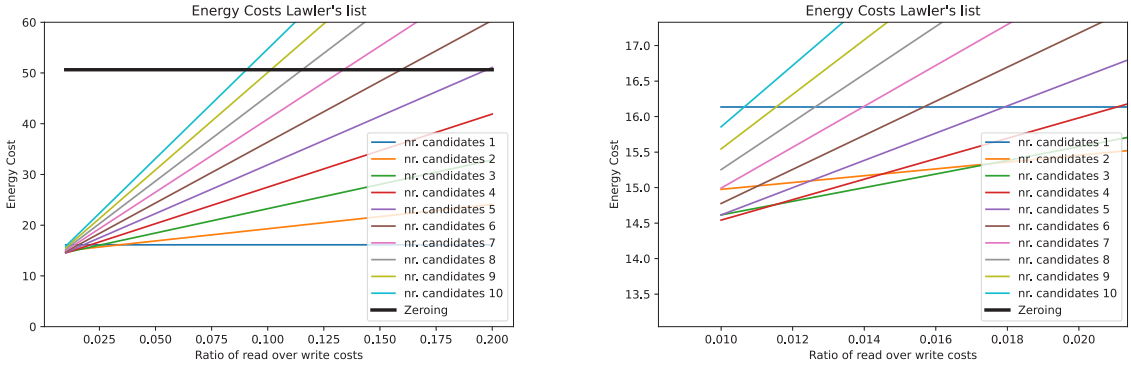


Fig. 11: Energy costs (in multiples of the energy of one bit written) using the Zeroing strategy and the best out of k overwrite strategy for 6B keys derived from Lawler's word list. The right is a blowup of the left figure.

minimum write energy needed to justify looking at another sub-bucket when one has already been located is at least 46. This happens for the German-like data set when we have one candidate and find a sub-bucket containing 4 stale keys. Even this amount is larger than for current and projected PCM memories. In all other cases, the discrepancy is much larger. We conclude from our experimental data that a cache aware algorithm trying to overwrite a stale key with a fresh, valid one should not access keys currently not in cache. Of course, this limits the bit-flip savings of such an algorithm.

VI. Conclusions

In this study, we investigated the bit-flip behavior of overwrites for typical keys. Our first take-away is instead of zeroing stale keys (or data in general), stale data should be marked and overwritten by new data. This confirms similar observations for pointers [11]. Alternatively, any key populations (such as words or names) have sufficient internal structure that zeroing out stale keys can be replaced by overwriting with the "most likely byte". Keys derived from texts in non-latin languages should be compressed. A cache length aware algorithm that is trying to overwrite a stale key should *not* load additional data into cache in order to find a better replacement. Overall, Bittman's observation and proposal have shown to be sound for a large variety of experimental data.

In general, the behavior of keys in our context is remarkably similar across different data sets. The observed distributions are very similar to a normal distribution and so are the order statistics. This gives us confidence in believing that the design of a bit-flip aware data structure will be valid across a wide range of key (and presumably data) populations.

We have not integrated these observations into the design of a bit-flip aware dictionary data structure. Neither did we investigate a bit-flip aware node structure for B-trees. This is left to future work.

References

[1] M. Ahsanullah, V. B. Nevzorov, and M. Shakil, *An introduction to order statistics*. Atlantis Press, 2013, DOI: 10.2991/978-94-91216-83-1.

[2] R. Bayer and K. Unterauer, "Prefix B-trees," *ACM Transactions on Database Systems (TODS)*, vol. 2, no. 1, pp. 11–26, 1977, DOI: 10.1145/320521.320530.

[3] D. Bittman, M. Gray, J. Raizes, S. Mukhopadhyay, M. Bryson, P. Alvaro, D. D. Long, and E. L. Miller, "Designing data structures to minimize bit flips on NVM," in *2018 IEEE 7th Non-Volatile Memory Systems and Applications Symposium (NVMSA)*. IEEE, 2018, pp. 85–90, DOI: 10.1109/NVMSA.2018.00022.

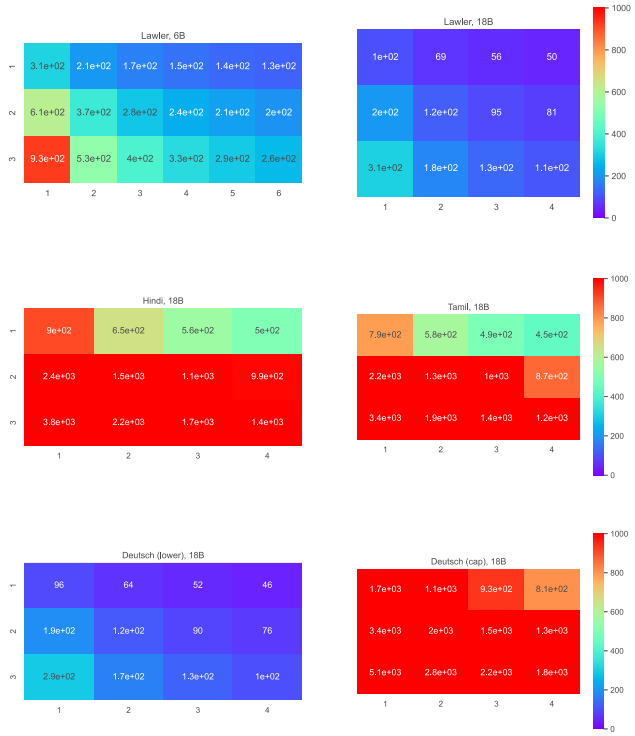


Fig. 12: Recommendations for reading a sub-bucket. The heatmap gives the minimum energy costs of writes over reads ($1/\rho$) making one read a sub-bucket. The x-axis gives the number of candidates in the new sub-bucket and the y-axis gives the number of candidates already available.

[4] D. Bittman, D. D. Long, P. Alvaro, and E. L. Miller, "Optimizing systems for byte-addressable NVRAM by reducing bit flipping," in *17th USENIX Conference on File and Storage Technologies*, 2019, pp. 17–30, https://dblp.org/db/conf/fast/fast2019.html#BittmanLAM19.

[5] Davidak, "Wortliste," 2016, accessed May 2022. [Online]. Available: github.com/davidak/wortliste

[6] D. Ewell, "A survey of unicode compression," 2004, www.unicode.org/notes/tn14/UnicodeCompression.pdf. [Online]. Available: https://www.unicode.org/notes/tn14/UnicodeCompression.pdf

[7] A. Gleave and C. Steinruecken, "Making compression algorithms for unicode text," 2017, arXiv:1701.04047.

[8] G. Graefe and H. Kuno, "Modern B-tree techniques," in *2011 IEEE 27th International Conference on Data Engineering*. IEEE, 2011, pp. 1370–1373, DOI: 10.1561/1900000028.

[9] W.-H. Kim, J. Seo, J. Kim, and B. Nam, "clfB-tree: Cache line friendly persistent B-tree for NVRAM," *ACM Transactions on Storage (TOS)*, vol. 14, no. 1, pp. 1–17, 2018, DOI: 10.1145/3129263.

[10] A. D. R. Kulandai and T. Schwarz, "Content-aware reduction of bitflips in phase change memory," *IEEE Letters of the Computer Society*, vol. 3, no. 2, pp. 58–61, 2020, DOI: 10.1109/LOCS.2020.3018401.

[11] ——, "Does XORing pointers save bitflips for NVRAM?" in *2021 29th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*. IEEE, 2021, pp. 1–6, DOI: 10.1109/MASCOTS53633.2021.9614290.

[12] A. Kumar, "Dataset: Consumer complaints: financial products, from the consumer complaint database maintained," 2020, accessed May 2022. [Online]. Available: www.kaggle.com/datasets/ashwinik/consumer-complaints-financial-products

[13] J. Lawler, "An English Word List," 1999, accessed May 2022. [Online]. Available: http://www-personal.umich.edu/~jlawler/wordlist.html

[14] D. Lomet, "The evolution of effective B-tree: Page organization and techniques: A personal account," *ACM SIGMOD Record*, vol. 30, no. 3, pp. 64–69, 2001, DOI: 10.1145/603867.603878.

[15] M. G. Jillani Soft Tech, "Amazon product reviews," 2022, Kaggle dataset, accessed May 2022. [Online]. Available: www.kaggle.com/datasets/jillanisofttech/amazon-product-reviews

[16] M. Nagy, J. Tapolcai, and G. Rétvári, "R3d3: A doubly opportunistic data structure for compressing and indexing massive data," *Infocommunications Journal*, vol. 11, no. 2, June 2019, DOI: 10.36244/ICJ.2019.2.7.

[17] B. Vijayalakshmi and N. Sasirekha, "Lossless text compression for Unicode Tamil documents," *ICTACT Journal on Soft Computing*, vol. 8, no. 2, pp. 1635–1640, 2018, DOI: 10.21917/ijsc.2017.0227.

[18] B.-D. Yang, J.-E. Lee, J.-S. Kim, J. Cho, S.-Y. Lee, and B.-G. Yu, "A low power phase-change random access memory using a data-comparison write scheme," in *2007 IEEE International Symposium on Circuits and Systems*. IEEE, 2007, pp. 3014–3017, DOI: 10.1109/ISCAS.2007.377981.

[19] P. Zhou, B. Zhao, J. Yang, and Y. Zhang, "Adurable and energy efficient main memory using phase change memory technology," in *Proceedings of the 36th International Symposium on Computer Architecture (ISCA'09)*, 2009, DOI: 10.1145/1555815.1555759.

Arockia David Roy Kulandai SJ David Roy is a Doctoral student of Computer Science at Marquette University, Milwaukee, WI, USA. Dr. Thomas Schwarz is his advisor. He has graduate degrees in Computer Applications and Philosophy. He was the Director of Xavier Institution of Computer Appli- cations (XICA) and Vice Principal of Department of Computer Sciences at St. Xavier's College (Autonomous), Ahmedabad, Gujarat, India from 2013 - 2018.

Thomas Schwarz SJ Dr. Thomas Schwarz has PhDs in Mathematics from Fern-Universität Hagen, Germany and Computer Science from University of California, San Diego. He is an associate professor in the department of computer science at Marquette University, Milwaukee, WI, USA and at Xavier Institute of Engineering, Mumbai, India. He is an adjunct professor at Santa Clara university, CA. He has taught at the Universidad Católica del Uruguay and at the Universidad Centro-Americana in El Salvador. He has over 125 publications to his credit and his research interest include Scalable Distributed Data Structures, Large Scale Storage Systems, High Availability, Erasure Correcting codes, security and Non-Volatile Memories.

Exact Outage Analysis for Non-regenerative Secure Cooperation Against Double-tap Eavesdropping

Kotha Venugopalachary, *Student Member, IEEE*, Deepak Mishra, *Member, IEEE*, and Ravikant Saini *Member, IEEE*

***Abstract*—This paper presents the secrecy performance analysis of an amplify-and-forward relay-assisted cooperative communication system in the presence of a passive external eavesdropper. In contrast to existing works that assume high signal-to-noise ratio (SNR) approximations, we have investigated exact and secrecy outage probabilities. Furthermore, we consider a more challenging scenario where the source may not be reachable to the intended user directly. But the eavesdropper can tap both the source link and the relay link. First of all, the outage probability is analyzed at the intended user as well as the eavesdropper. Next, defining the secrecy rate for the amplify-and-forward (AF) relaying system, the expression of the secrecy outage probability (SOP) and the secrecy intercept probability (SIP) have been derived, respectively. Noticing the complexity involved in the integration of SOP and SIP expressions, the closed-form expressions have been derived for asymptotic cases. Finally, the exact and asymptotic analysis has been verified by performing Monte-Carlo simulations. It is observed that the relay position should be closer to the source compared to the eavesdropper to achieve improved SOP.**

***Index Terms*—amplify-and-forward, physical layer security, secrecy rate, cooperative systems, secrecy outage probability.**

I. INTRODUCTION

Cooperative relaying in wireless communications has got extensive research interest as it helps in achieving fifth-generation (5G) objectives such as reliability, coverage area extension, and high data rate [1]–[6]. As the wireless channels are open in nature, the information transmission is prone to eavesdropping. With the enormous increase of online transactions and heterogeneity of connecting users, ensuring secrecy to the user's data is a challenging task. Securing information [7] from external eavesdroppers is a major concern for cooperative communication systems as well [1]. The physical layer security (PLS) has attracted the attention of researchers compared to the high-complex cryptography at higher levels (Application and Network) because it exploits the inherent characteristics of wireless channels [4], [8].

K. Venugopalachary is with the Department of Electrical Engineering at the Shiv Nadar University, Uttar Pradesh 201314, India (E-mail: vk227@snu.edu.in).

D. Mishra is with the School of Electrical Engineering and Telecommunications (EET) at the University of New South Wales (UNSW) Sydney, NSW 2052, Australia (E-mail: d.mishra@unsw.edu.au).

R. Saini is with Department of Electrical Engineering at the IIT Jammu, Jammu (J&K) 181221, India (E-mail: ravikant.saini@iitjammu.ac.in).

This work was partially supported by the Faculty Funded Postdoctoral Research Fellowship support of EET School at UNSW Sydney.

Corresponding author: D. Mishra.

A. Literature survey

Wireless PLS improvement using cooperative relaying schemes such as decode-and-forward (DF), amplify-and-forward (AF), randomize and forward (RF), and compress-and-forward (CF) have been investigated in [8]–[13]. Considering a jamming node, the PLS of cooperative NOMA in a severe scenario where there is no direct link from the source to far-destination while the direct link between the eavesdropper and source exists is investigated in [14]. Authors in [15] considered resource allocation in multi-carrier AF-relay systems under individual and sum power budget constraints to investigate the optimal secrecy rate. Authors in [16] have studied the analysis of secure beam forming and ergodic secrecy rate for AF relay networks and derived tight closed-form approximation for the ergodic secrecy rate for a large number of antennas. The secrecy outage probability (SOP) of relay and user (RU) selection in an AF system over Nakagamim fading channels is discussed in [17], and provided the asymptotic SOP expressions for maximal ratio combining (MRC) and selection combining techniques.

B. Motivation and Contributions

The DF relaying requires decoding capability at the relay node, which causes deployment costs. The cooperative jamming requires additional nodes and needs a generation of noise in the null space of the destination, causing more implementation and deployment costs. Whereas AF relaying simply amplifies the received signal using a power amplifier and retransmits, which is cost-effective and easy to deploy. Notifying the ease of deployment and the necessity of power-efficient low-cost implementation in the next-generation applications (like the internet of things (IoT) and their security), we are interested in studying the performance analysis of AF-relay assisted secure cooperative systems.

The secrecy performance analysis of AF systems with multiple relays and two hops under cochannel interference and correlated channels using optimal relay selection has been extensively investigated in [18], [19] without considering the dual-tapping of the eavesdropper. Considering full-duplex AF relaying, [20]–[22] have investigated the secrecy performance in terms of average secrecy rate and SOP. The PLS in AF relaying by considering direct links from the source to the destination and the eavesdropper has been investigated to a great extent [8], [23], [24]. Authors in [24] have considered the more general case of availability of direct links from source to both the destination and the eavesdropper and studied

DOI: 10.36244/ICJ.2022.4.6

the PLS over mixed Rayleigh and double-Rayleigh fading channels. In this paper, they have considered the maximal ratio combining at both the destination and the eavesdropper to get the advantage of diversity. The assumption of a direct link only to the eavesdropper, not to the main user, gives a more practical situation to achieve secrecy where the eavesdropper can get diversity and maybe stronger than the intended user's channel. *To the best of our knowledge, a more challenging scenario of a two-hop AF secure cooperative system where the source may not be reachable to the intended user directly, but the eavesdropper can tap both the source link and the relay link has not been studied yet*. In this paper, we consider the aforementioned system model to investigate the performance in terms of exact outage probability, exact secrecy outage probability (SOP), and secrecy intercept probability (SIP). The contributions of the paper are briefly summarised as follows.

- Initially, the outage probability analysis is performed individually at the intended user and at the eavesdropper.
- Defining secrecy rate for AF-relaying system, the SOP and the SIP expressions are provided in the integral form.
- We provide the closed-form expressions for SOP and SIP for asymptotic analysis.
- Finally, we validate our analysis by performing Monte-carlo simulations.

The remainder of the paper is divided into the following sections: Section II describes the system model and transmission protocol. The outage probability analysis of the intended user and the eavesdropper is analyzed individually in Section III. Section IV provides the SOP and the SIP analysis. The asymptotic analysis of SOP and SIP are detailed in Section V. Finally, Section VI shows the simulation results.

II. System Model

A. Topology

Consider a four-node wireless cooperative system consisting a source $\mathcal{S}$, a relay $\mathcal{R}$, a user $\mathcal{U}$ and an external eavesdropper $\mathcal{E}$ where all nodes are equipped with a single antenna. As shown in Fig. 1, $\mathcal{S}$ located at the origin, $(x_s, y_s) = (0, 0)$ of a two dimensional (2D) x-y plain, communicates with $\mathcal{U}$ located at $(x_d, y_d) = (d, 0)$ via $\mathcal{R}$. $\mathcal{E}$ is assumed to be located at (x_e, y_e) which tries to overhear the transmission from $\mathcal{S}$ to $\mathcal{R}$ and $\mathcal{R}$ to $\mathcal{U}$. As an essential scenario to examine in order to ensure security, it is assumed a direct link from $\mathcal{S}$ to $\mathcal{E}$ only and not to $\mathcal{U}$ while considering $\mathcal{R}$-to-$\mathcal{E}$ and $\mathcal{R}$-to-$\mathcal{U}$ links. We also assume the $\mathcal{S}$-to-$\mathcal{E}$ distance is greater than $\mathcal{S}$-to-$\mathcal{R}$. With path loss exponent α, the channels undergo large-scale fading.

B. Transmission Protocol and Channel Model

In the considered half-duplex relaying system, the transmission takes place in two phases [25]. In the first phase, the information is transmitted from $\mathcal{S}$ to $\mathcal{R}$, and in the second phase, $\mathcal{R}$ retransmits to $\mathcal{U}$ by amplifying the received signal with an amplification factor of β. Due to the broadcast nature of the transmission, $\mathcal{E}$ can overhear the information in both phases. Assuming P_s and P_r as transmit powers at $\mathcal{S}$ and $\mathcal{R}$ respectively, the received signals y_{1R} at $\mathcal{R}$ and y_{1E} at $\mathcal{E}$ from

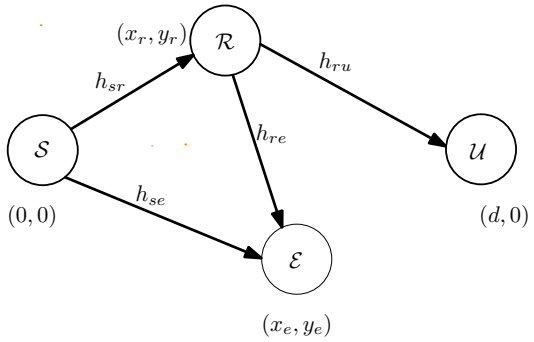


Fig. 1: Four-node AF secure cooperative system in 2D space.

$\mathcal{S}$ in first phase, and the received signals $y_{2\mathcal{U}}$ at $\mathcal{U}$ and $y_{2\mathcal{E}}$ at $\mathcal{E}$ from $\mathcal{R}$ in the second phase are:

$$y_{1\mathcal{R}} = h_{sr}\sqrt{P_s}x_1 + n_{1\mathcal{R}}, \quad y_{1\mathcal{E}} = h_{se}\sqrt{P_s}x_1 + n_{1\mathcal{E}}, \quad (1)$$

$$y_{2\mathcal{U}} = h_{ru}\sqrt{P_r}\beta x_1 + n_{2\mathcal{U}}, \; y_{2\mathcal{E}} = h_{re}\sqrt{P_r}\beta x_1 + n_{2\mathcal{E}}. \quad (2)$$

where h_{sr}, h_{se}, h_{ru} and h_{re} are the Rayleigh channel gain coefficients of $\mathcal{S}$-to-$\mathcal{R}$, $\mathcal{S}$-to-$\mathcal{E}$, $\mathcal{R}$-to-$\mathcal{U}$ and $\mathcal{R}$-to-$\mathcal{E}$ links respectively. $n_{1\mathcal{R}}$, $n_{1\mathcal{E}}$, $n_{2\mathcal{E}}$ $n_{2\mathcal{U}}$, represent mutually independent, Additive White Gaussian Noise (AWGN) with $N\left(0, \sigma^2\right)$ at $\mathcal{R}$, $\mathcal{E}$ in first and second phases and at $\mathcal{U}$ respectively. x_1 is unit power signal from $\mathcal{S}$ and $\beta = \frac{1}{\sqrt{P_s|h_{sr}|^2+\sigma^2}}$ is an amplification factor used at $\mathcal{R}$. At the eavesdropper, the signal received in two phases is combined using MRC.

III. Individual Outage Probability Analysis

In this section, defining the rate, closed-form expressions for outage probability at the main user and eavesdropper are derived.

1) Outage Analysis at the Intended User: As per the transmission protocol, the amplified signal is transmitted to the main user. Then, the achievable rate at $\mathcal{U}$ is given as [26]

$$R_{\mathcal{U}} = \frac{1}{2}\log\left(1 + \frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr} + \gamma_{ru} + 1}\right), \quad (3)$$

where γ_{sr}=$\frac{P_s|h_{sr}|^2}{d_{sr}^{\alpha}}$, γ_{ru}=$\frac{P_r|h_{rd}|^2}{d_{ru}^{\alpha}}$ are the signal to noise ratios (SNRs) over $\mathcal{S}$-to-$\mathcal{R}$ and $\mathcal{R}$-to-$\mathcal{U}$ links, and are exponentially distributed with means $\mu_1 = \frac{p_s}{d_{sr}^{\alpha}}$ and $\mu_2 = \frac{p_r}{d_{ru}^{\alpha}}$, respectively. The ratio, $\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1} = \gamma_{sru}$ is the effective SNR at the $\mathcal{U}$ under the AF relaying and its distribution is used to investigate the outage probability. The outage occurs when the $R_{\mathcal{U}}$ at $\mathcal{U}$ is less than a threshold rate r_u and its probability is called outage probability. The outage probability at the $\mathcal{U}$, $P_{out}^{\mathcal{U}}$ is

$$\begin{aligned} P_{out}^{\mathcal{U}} &= \Pr\left(\frac{1}{2}\log_2\left(1 + \frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr} + \gamma_{ru} + 1}\right) \le r_u\right) \\ &\overset{\rho_u=2^{2r_u}}{=} \Pr\left(1 + \frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr} + \gamma_{ru} + 1} \le \rho_u\right) \\ &= \Pr\left(\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr} + \gamma_{ru} + 1} \le \rho_u - 1\right) \\ &= F_{\gamma_{sru}}(\rho_u - 1), \end{aligned} \quad (4)$$

where $F_{\gamma_{sru}}$ is the cumulative distribution function (CDF) of the random variable (RV) $\gamma_{sru} = \frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1}$ which is a ratio

of product of RVs ($\gamma_{sr}\gamma_{ru}$) and sum of RVs ($\gamma_{sr}+\gamma_{ru}$). The CDF of the RV γ_{sru} is given as

$$F_{\gamma_{sru}}(\gamma) = 1 - 2\mathrm{e}^{-a_1\gamma}a_2\sqrt{\gamma(\gamma+1)}K_1(2a_2\sqrt{\gamma(\gamma+1)}),$$

where $a_1 = \mu_1+\mu_2$ and $a_2 = \sqrt{\mu_1\mu_2}$.

2) Outage Analysis at the Eavesdropper: When it comes to the transmission protocol, the $\mathcal{E}$ gets the signal two times, and then it uses MRC to merge the two versions of the signal. The rate that can be achieved at $\mathcal{E}$ is represented as

$$R_{\mathcal{E}} = \frac{1}{2}\log\left(1+\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}\right), \tag{5}$$

where $\gamma_{se} = \frac{P_s|h_{se}|^2}{d_{se}^{\alpha}}$ and $\gamma_{re} = \frac{P_r|h_{re}|^2}{d_{re}^{\alpha}}$ are the SNRs over the links $\mathcal{S}$-to-$\mathcal{E}$ and $\mathcal{R}$-to-$\mathcal{E}$, and are exponentially distributed with means $\lambda_1 = \frac{p_s}{d_{se}^{\alpha}}$ and $\lambda_2 = \frac{p_r}{d_{ru}^{\alpha}}$ respectively. Due to two copies of the received signal at $\mathcal{E}$: one from the $\mathcal{R}$ and another (2) from the $\mathcal{S}$, the effective SNR at the $\mathcal{E}$ by employing the MRC is given as $W = \gamma_{se} + \frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}$. The outage occurs at $\mathcal{E}$ if the $R_{\mathcal{E}}$ is less than a threshold rate r_e. The outage probability at the $\mathcal{E}$, $P_{out}^{\mathcal{E}}$ is given as

$$\begin{aligned}
P_{out}^{\mathcal{E}} &= \Pr\left(\frac{1}{2}\log\left(1+\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}\right)\le r_e\right)\\
&\overset{\rho_e=2^{2r_e}}{=} \Pr\left(\left(\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}\right)\le \rho_e-1\right)\\
&= \Pr(X+Z\le\rho_e-1) = \Pr(W\le\rho_e-1)\\
&= F_W(\rho_e-1),
\end{aligned} \tag{6}$$

where $W = X+Z$, $X = \gamma_{se}$ and $Z = \frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}$ with its CDF $F_W(w)$. The CDF of W is given as

$$\begin{aligned}
F_W(w) &= \int_{z=0}^{\infty}\int_{x=0}^{w-z} f_X(x)f_Z(z)dxdz\\
&= \int_{z=0}^{\infty} f_Z(z)F_X(w-z)dz\\
&= \int_{z=0}^{\infty}[2\mathrm{e}^{-b_1 z}[b_1b_2\sqrt{z(z+1)}K_1(2b_2\sqrt{z(z+1)})\\
&+ b_2^2(2z+1)K_0(2b_2\sqrt{z(z+1)})]](1-\mathrm{e}^{-\lambda_1(w-z)})dz\\
&= 1-2\mathrm{e}^{-\lambda_1 w}\int_{z=0}^{\infty}\mathrm{e}^{-(b_1-\lambda_1)z}\\
&\quad\Big[b_1b_2\sqrt{z(z+1)}K_1(2b_2\sqrt{z(z+1)})\\
&\quad+ b_2^2(2z+1)K_0(2b_2\sqrt{z(z+1)})\Big]dz,
\end{aligned} \tag{7}$$

where $b_1 = \mu_1+\lambda_2$ and $b_2 = \sqrt{\mu_1\lambda_2}$.

Using the CDF of W, the $P_{out}^{\mathcal{E}}$ is given as

$$\begin{aligned}
P_{out}^{\mathcal{E}} &= 1-2\mathrm{e}^{-\lambda_1(\rho_e-1)}\int_{z=0}^{\infty}\mathrm{e}^{-(b_1-\lambda_1)z}\\
&\quad\Big[b_1b_2\sqrt{z(z+1)}K_1(2b_2\sqrt{z(z+1)})\\
&\quad+ b_2^2(2z+1)K_0(2b_2\sqrt{z(z+1)})\Big]dz.
\end{aligned} \tag{8}$$

In the next section, by defining the secrecy rate for the considered AF relaying system where there is no direct link to the intended user while having a direct link along with the relay link to the eavesdropper, i.e., double tapping of an eavesdropper, we provide the detailed SOP analysis.

IV. Secrecy Outage Probability Analysis

A. Secrecy Rate Definition for Amplify-and-forward Relaying

The secrecy rate is the non-negative difference of the main and eavesdropper channels' rates, i.e. $R_s = [R_{\mathcal{U}} - R_{\mathcal{E}}]^+$. Hence, the secrecy rate for AF relaying is given as

$$R_s^{AF} = \left[\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1}}{1+\gamma_{se}+\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}}\right)\right]^+. \tag{9}$$

The secrecy rate equation in (9) is simplified by giving a proposition as (9) is more complicated to study the analyze.

Proposition 1: The upper bound of the secrecy rate (9) is

$$R_s^{AF} = \left[\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1}}{1+\gamma_{se}+\gamma_{re}}\right)\right]^+. \tag{10}$$

Proof: For any positive values of γ_{sr} and γ_{re}

$$\begin{aligned}
\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1} &\le \gamma_{sr}\\
\gamma_{sr}\gamma_{re} &\le (\gamma_{sr}+\gamma_{re}+1)\gamma_{sr}\\
0 &\le \gamma_{sr}(\gamma_{sr}+1).
\end{aligned} \tag{11}$$

Similarly, it can be observed that

$$\begin{aligned}
\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1} &\le \gamma_{re}\\
\gamma_{sr}\gamma_{re} &\le (\gamma_{sr}+\gamma_{re}+1)\gamma_{re}\\
0 &\le \gamma_{re}(\gamma_{re}+1).
\end{aligned} \tag{12}$$

Hence, $\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1} \le \min\{\gamma_{sr},\gamma_{re}\}$. As the relay location is assumed such that $d_{sr} < d_{re}$, $\gamma_{sr} > \gamma_{re}$. Hence, the maximum value of $\frac{\gamma_{sr}\gamma_{re}}{\gamma_{sr}+\gamma_{re}+1}$ is equal to γ_{re}. ■

B. Secrecy Outage Probability

The secrecy outage occurs when the R_s^{AF} is less than a threshold rate R_{th} and the corresponding probability is called secrecy outage probability (SOP). The SOP in AF relaying system is given as:

$$\begin{aligned}
P_{sop}^{AF} &= \Pr\left(R_s^{AF} < R_{th}\right)\\
&= \Pr\left(\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1}}{1+\gamma_{se}+\gamma_{re}}\right) < R_{th}\right)\\
&\overset{\rho=2^{2R_{th}}}{=} \Pr\left(\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1} < \rho(\gamma_{se}+\gamma_{re})+(\rho-1)\right)\\
&= \Pr(W_1-W_2<\rho-1)\\
&= \Pr(W<\rho-1) = F_W(\rho-1)\\
&= \int_{-\infty}^{\infty}\left[\int_{-\infty}^{w_2+\rho-1} f_{W_1}(w_1)f_{\rho W_2}(w_2)dw_1\right]dw_2\\
&= \int_{0}^{\infty} f_{W_2}(w_2)F_{W_1}(w_2+\rho-1)dw_2,
\end{aligned} \tag{13}$$

where W is the difference of two RVs $W_1 = \frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1}$ and $W_2 = \rho(\gamma_{se}+\gamma_{re})$. f_{W_2} is the PDF of W_2 and F_{W_1}, F_W are the CDFs of W_1, W respectively. The PDF f_{W_2} and the CDF F_{W_1} are obtained by using transformation of RVs [27], [28] :

$$f_{W_2} = \frac{\lambda_1\lambda_2}{|\rho|(\lambda_1-\lambda_2)}\left(\mathrm{e}^{-(\lambda_2 w_2/\rho)}-\mathrm{e}^{-(\lambda_1 w_2/\rho)}\right), \tag{14}$$

$$F_{W_1} = 1 - 2\mathrm{e}^{-(\mu_1+\mu_2)w_1}\sqrt{\mu_1\mu_2 w_1(w_1+1)} \\ K_1\left(2\sqrt{\mu_1\mu_2 w_1(w_1+1)}\right). \quad (15)$$

Hence, by substituting (15) in (13), we obtain P_{sop}^{AF} as:

$$P_{sop}^{AF} = \int_0^\infty \frac{\lambda_1\lambda_2}{|\rho|(\lambda_1-\lambda_2)}\left(\mathrm{e}^{-(\lambda_2 w_2/\rho)} - \mathrm{e}^{-(\lambda_1 w_2/\rho)}\right) \\ \Big[1 - 2\mathrm{e}^{-(\mu_1+\mu_2)(w_2+\rho-1)} \\ \sqrt{\mu_1\mu_2(w_2+\rho-1)(w_2+\rho)} \\ K_1\left(2\sqrt{\mu_1\mu_2(w_2+\rho-1)(w_2+\rho)}\right)\Big] dw_2. \quad (16)$$

C. Secrecy Intercept Probability

The secrecy intercept probability (SIP) is defined as the probability at which the secrecy rate is less than zero. The corresponding mathematical expression of the SIP is given as

$$\begin{aligned} P_{sip}^{AF} &= \Pr\left(\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1}}{1+\gamma_{se}+\gamma_{re}}\right) \le 0\right) \\ &= \Pr\left(\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}+1} \le (\gamma_{se}+\gamma_{re})\right) \\ &= \int_0^\infty \frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_2)}\left(\mathrm{e}^{-\lambda_2 w_2} - \mathrm{e}^{-\lambda_1 w_2}\right) \\ &\quad \Big[1 - 2\mathrm{e}^{-(\mu_1+\mu_2)w_2}\sqrt{\mu_1\mu_2 w_2(w_2+1)} \\ &\quad K_1\left(2\sqrt{\mu_1\mu_2 w_2(w_2+1)}\right)\Big] dw_2 \\ &= 1 - \frac{\lambda_1\lambda_2}{(\lambda_1-\lambda_2)}\int_0^\infty 2\sqrt{\mu_1\mu_2 w_2(w_2+1)} \\ &\quad \left(\mathrm{e}^{-(\mu_1+\mu_2+\lambda_2)w_2} - \mathrm{e}^{-(\mu_1+\mu_2+\lambda_1)w_2}\right) \\ &\quad K_1\left(2\sqrt{\mu_1\mu_2 w_2(w_2+1)}\right) dw_2. \quad (17) \end{aligned}$$

Since the modified Bessel function contains complex parameters, the integration in (16) and (17) are intractable. The next section presents the SOP and SIP for asymptotic regimes.

V. Asymptotic Secrecy Analysis Analysis

A. The Approximated Secrecy Outage Probability

By assuming that the end-to-end SNR of main channel is very stronger than the effective SNR over the eavesdropper channel, i.e., $\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}} >> (\gamma_{se}+\gamma_{re})$, the SOP is given as

$$\begin{aligned} \tilde{P}_{sop}^{AF} &= \Pr\left(\frac{1}{2}\log\left(\frac{\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}}}{\gamma_{se}+\gamma_{re}}\right) < R_{th}\right) \\ &\overset{\rho=2^{2R_{th}}}{=} \Pr\left(\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}} < \rho(\gamma_{se}+\gamma_{re})\right) \\ &= \Pr\left(Z_1 - Z_2 < 0\right) = F_Z(0) \\ &= 1 - \frac{2\lambda_1\lambda_2\sqrt{\mu_1\mu_2}}{\rho(\lambda_1-\lambda_2)}\int_0^\infty z_2 K_1\left(z_2\, 2\sqrt{\mu_1\mu_2}\right) \\ &\quad \left(\mathrm{e}^{-(\mu_1+\mu_2+\frac{\lambda_2}{\rho})z_2} - \mathrm{e}^{-(\mu_1+\mu_2+\frac{\lambda_1}{\rho})z_2}\right) dz_2. \quad (18) \end{aligned}$$

The closed form expression for $\tilde{P}_{sop}^{AF}$ in (18) can be obtained as (19), where $F\left(.,.;.;.\right)$ is the Gauss hypergeometric function (Table of integrals series and products [29]). In (19), $A_1 = \frac{\mu_1+\mu_2}{2} + \frac{\lambda_2}{\rho}$, $A_2 = \frac{\mu_1+\mu_2}{2} + \frac{\lambda_1}{\rho}$, and $B = \sqrt{\mu_1\mu_2}$.

B. Intercept probability for High SNR Regime

As the equation (17) involves the integration of a modified Bessel function of the second kind with difficult functional parameters, it is very difficult to obtain the closed-form expression for it. To relax the intractability of integration in (17), it is assumed that $\gamma_{sr}+\gamma_{ru} >> 1$. Hence, the secrecy rate equation in (10) reduces to the following equation

$$R_s^{AF} = \left[\frac{1}{2}\log_2\left(\frac{1+\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}}}{1+\gamma_{se}+\gamma_{re}}\right)\right]^+. \quad (20)$$

Now, the intercept probability is given as

$$\begin{aligned} \tilde{P}_{sip}^{AF} &= \Pr\left(\frac{1}{2}\log\left(\frac{1+\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}}}{1+\gamma_{se}+\gamma_{re}}\right) < 0\right) \\ &= \Pr\left(\frac{\gamma_{sr}\gamma_{ru}}{\gamma_{sr}+\gamma_{ru}} < (\gamma_{se}+\gamma_{re})\right) \\ &= \Pr\left(Z_1 - Z_2 < 0\right) = F_Z(0) \\ &= 1 - \frac{\lambda_1\lambda_2\sqrt{\mu_1\mu_2}}{(\lambda_1-\lambda_2)}\int_0^\infty z_2 K_1\left(z_2\sqrt{\mu_1\mu_2}\right) \\ &\quad \left(\mathrm{e}^{-(\frac{\mu_1+\mu_2}{2}+\lambda_2)z_2} - \mathrm{e}^{-(\frac{\mu_1+\mu_2}{2}+\lambda_1)z_2}\right) dz_2. \quad (21) \end{aligned}$$

The closed form expression is same as that of (19), where $A_1 = \frac{\mu_1+\mu_2}{2} + \lambda_2$, $A_2 = \frac{\mu_1+\mu_2}{2} + \lambda_1$, and $B = \sqrt{\mu_1\mu_2}$.

VI. Numerical Results

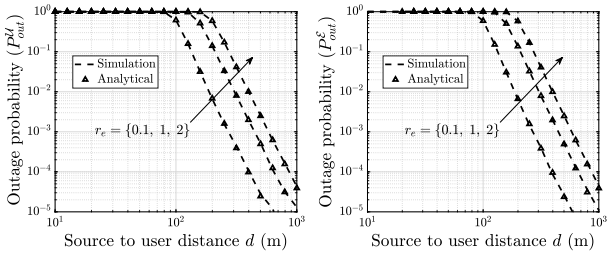
In this section, we validate the analytical expressions derived in Section III, Section IV and Section V. ***Default simulation parameters:*** Unless otherwise specified explicitly in figures, we set the default parameters that follow, the distance from source to the destination $d = 100$m, the total power $P_t = 40$dBm, the noise variance $\sigma^2 = -90$dBm and the path loss exponent $\alpha = 3$. The relay is located close to the source node with coordinates $(x_r,\ y_r) = (\frac{d}{10},\ \frac{d}{100})$ and the eavesdropper is located at $(x_e, y_e) = (\frac{d}{2},\ -2d)$ such that it is far from the source compared to the relay node. We perform 10^6 channel realizations to show the simulation results.

A. Validation of the Outage and Intercept Probability Analysis

In Fig. 2 (a) and Fig. 2 (b), we validate the outage analysis at the intended user and the eavesdropper respectively. Fig. 2 (a) shows the outage probability at the intended user derived in (4) and Fig. 2 (b) shows the outage probability at the intended user derived in (8), for different values of threshold rates $r_u = r_e = \{0.1,\ 1,\ 2\}$. It is observed from Fig. 2 that the outage probability improves with the reduction in threshold rates since the random nature of fading channel does not allow the channel to achieve significant rates.

Fig. 3 is plotted to show the validation of secrecy intercept probability. The intercept probability variation is drawn by changing the relay transmit power for different locations of eavesdropper such as $x_e = \frac{d}{2}$ and $y_e = \{\frac{x_e}{10}, x_e, 5x_e\}$. It is noted from the figure that the intercept probability increases as the distance between the eavesdropper and the source increase due to the leakage of information being more when the eavesdropper is closer to the source.

$$P_{so}^{AF} = 1 - \frac{64\lambda_1\lambda_2\mu_1\mu_2}{3(\lambda_1-\lambda_2)}\left[(A_1+B)^{-3}F\left(3,\frac{3}{2};\frac{5}{2};\frac{A_1-B}{A_1+B}\right) - (A_2+B)^{-3}F\left(3,\frac{3}{2};\frac{5}{2};\frac{A_2-B}{A_2+B}\right)\right]. \quad (19)$$



(a) (b)

Fig. 2: The outage probability analysis with the variation of relay position.

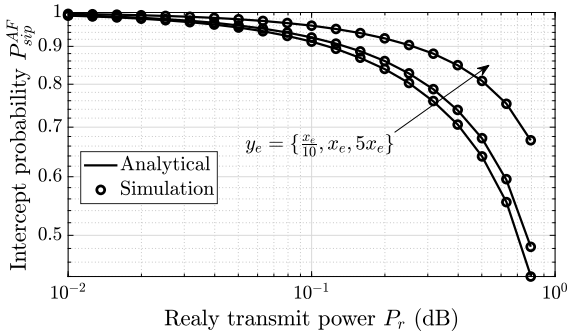


Fig. 3: Intercept performance with the variation of relay power

B. Verification of the Asymptotic and the Exact SOP

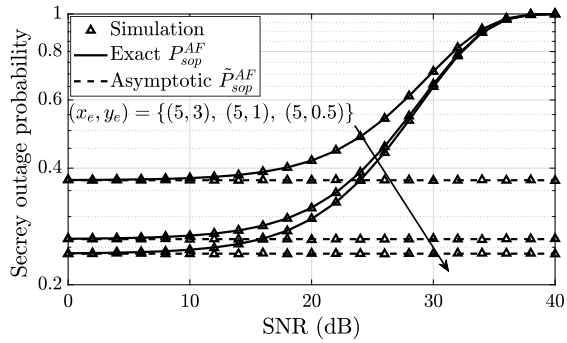


Fig. 4: Validation of exact SOP and the approximated SOP.

In Fig. 4, the performance variation of SOP in the exact and approximate regime of AF relaying has been analyzed and also verified the analysis by performing simulations. In the figure the exact SOP derived in (16) and the asymptotic SOP in (19) derived from (18) are shown by varying the SNR for various locations of eavesdropper $(x_e, y_e) = \{(5,\ 3), (5,\ 1), (5,\ 0.5)\}d$. In the figure, the eavesdropper coordinated are normalized w.r.t. the distance between $\mathcal{S}$ and $\mathcal{U}$. Fig. 4, also, validates the secrecy outage performance of the exact SOP in (16) and the approximated SOP in (19). It is noted that the SOP decreases as the eavesdropper moves away from the source. And also, it is verified that the exact and the approximated SOPs are the same at low SNRs.

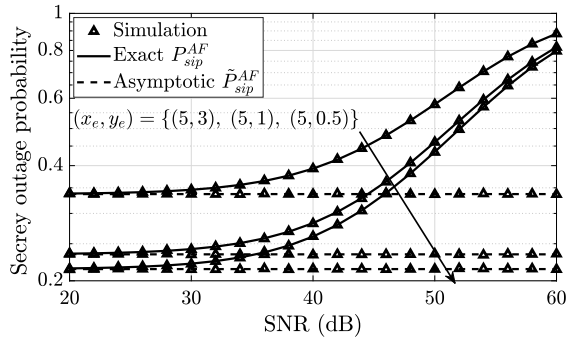
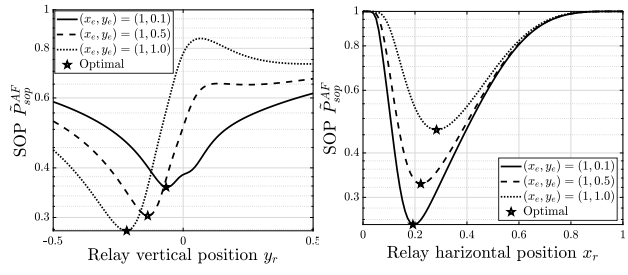


Fig. 5: Validation of intercept probability

In Fig. 5, the secrecy intercept probability is analyzed with the variation of SNR for different locations of the eavesdropper. The figure shows the validation of the exact secrecy intercept probability in (17) and the approximated SIP in (19) obtained from (21). It is noted that the analytical and the simulations exactly match each other. It is observed that the SIP is less as the eavesdropper is located farther from the source compared to the user relay node. And also, the asymptotic SIP is the same as the exact SIP at low SNRs.

C. Insights on Optimal Relay Location

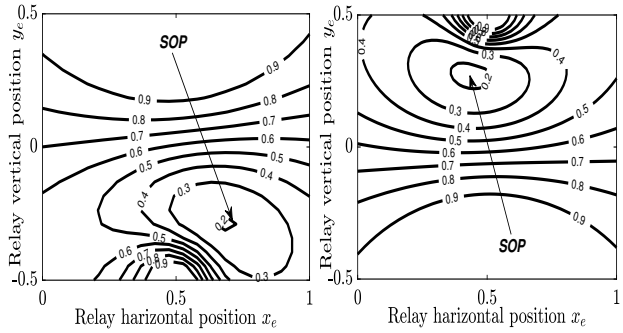


(a) (b)

Fig. 6: The SOP performance with the variation of R position.

We analyze the secrecy outage probability performance in Fig. 6 and provide the optimal secrecy outage probability. Fig. 6(a) gives the performance the SOP in (16) with the variation of horizontal relay position x_r and Fig. 6(b) gives the SOP with the variation of vertical relay position y_r for various locations of eavesdropper. It is observed that the optimal SOP improved as the $\mathcal{E}$ is away from the line of sight path from $\mathcal{S}$ to $\mathcal{U}$ while the relay is closer to the $\mathcal{S}$.

Fig.7 represents the optimal relay location to obtain the optimal. It shows the SOP variation with the relay position for various locations of eavesdropper $(x_e, y_e) = \{(\frac{D}{10}, \frac{3}{4}x_e), (\frac{D}{10}, \frac{1}{4}x_e)\}$. It is observed that the optimal relay placement is closer to the destination if the eavesdropper is located at $(\frac{D}{10}, \frac{3D}{40})$ and it should be placed near the midpoint of $\mathcal{S}$ and $\mathcal{U}$ when $\mathcal{E}$ is at $(\frac{D}{10}, \frac{D}{40})$ to get the best SOP performance.



(a) $x_e = \frac{d}{10}, y_e = \frac{3}{4}x_e$ (b) $x_e = \frac{d}{10}, y_e = \frac{1}{4}x_e$

Fig. 7: The optimal relay position for better SOP

VII. CONCLUSION

Outage analysis and secrecy outage analysis have been performed at the intended user as well as the eavesdropper in an AF relay-assisted cooperative system. To gain more analysis, an asymptotic scenario has been considered, and closed-form expressions for SOP and SIP have been derived. Numerical results validated the analytical formulation and showed the performance variation with the variation of SNR. Finally, key insights on relay location to obtain optimal SOP are given, which leads to an optimization problem.

REFERENCES

[1] F. Jameel, S. Wyne, G. Kaddoum, and T. Q. Duong, "A comprehensive survey on cooperative relaying and jamming strategies for physical layer security," *IEEE Commun. Surveys Tuts*, vol. 21, no. 3, pp. 2734–2771, 2019, DOI: 10.1109/COMST.2018.2865607.

[2] C. Cebrail, A.-O. Musaab, F. Mohammed, and A.-O. Wael, "Cooperative OSIC system to exploit the leakage power of MU-MIMO beamforming based on maximum SLR for 5G," *Infocommun. J.*, vol. 11, no. 3, pp. 13–20, 2019, DOI: 10.36244/ICJ.2019.3.3.

[3] L. J. Rodriguez, N. H. Tran, T. Q. Duong, T. Le-Ngoc, M. Elkashlan, and S. Shetty, "Physical layer security in wireless cooperative relay networks: state of the art and beyond," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 32–39, Dec. 2015,DOI: 10.1109/MCOM.2015.7355563.

[4] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: Theories, technologies, and challenges," *Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 347–376, Firstquarter 2017, DOI: 10.1109/COMST.2016.2598968.

[5] A. Fayad and T. Cinkler, "Cost-effective delay-constrained optical fron- thaul design for 5G and beyond," *Infocommun. J.*, vol. 14, no. 2, pp. 19–27, 2022, DOI: 10.36244/ICJ.2022.2.2.

[6] R. Saini and D. Mishra, "Chapter 4 - Privacy-aware physical layer security techniques for smart cities," in *Smart Cities Cybersecurity and Privacy*, D. B. Rawat and K. Z. Ghafoor, Eds. Elsevier, 2019, pp. 39–56, DOI: 10.1016/B978-0-12-815032-0.00004-4.

[7] H. Garmani, D. Ait Omar, M. El Amrani, M. Baslam, and M. Jourhmane, "Joint beacon power and beacon rate control based on game theoretic approach in vehicular Ad Hoc networks," *Infocommun. J.*, vol. 13, no. 1, pp. 58–67, 2021, DOI: 10.36244/ICJ.2021.1.7.

[8] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Signal Process.*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010, DOI: 10.1109/TSP.2009.2038412.

[9] R. Saini, D. Mishra, and V. Kotha, "Power allocation and relay placement for secrecy outage minimization over DF relayed system," in *2021 IEEE 18th Annual Consumer Commun. Networking Conf. (CCNC)*, 2021, pp. 1–4, DOI: 10.1109/CCNC49032.2021.9369642.

[10] K. Venugopalachary, D. Mishra, R. Saini, and V. Chakka, "Optimizing secrecy performance of trusted RF relay against external eavesdropping," in *2019 IEEE Global Commun. Conf. (GLOBECOM)*, 2019, pp. 1–6, DOI: 10.1109/GLOBECOM38437.2019.9013579.

[11] S. Thapar, D. Mishra, and R. Saini, "Novel outage-aware NOMA protocol for secrecy fairness maximization among untrusted users," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13259–13272, 2020, DOI: 10.1109/TVT.2020.3022560.

[12] I. Amin, D. Mishra, R. Saini, and S. Aïssa, "QoS-aware secrecy rate maximization in untrusted NOMA with trusted relay," *IEEE Commun. Lett.*, vol. 26, no. 1, pp. 31–34, 2022, DOI: 10.1109/LCOMM.2021.3124902.

[13] P. K. Hota, S. Thapar, D. Mishra, R. Saini, and A. Dubey, "Ergodic performance of downlink untrusted NOMA system with imperfect SIC," *IEEE Commun.* Lett., vol. 26, no. 1, pp. 23–26, 2022, DOI: 10.1109/LCOMM.2021.3126746.

[14] K. Cao, B. Wang, H. Ding, F. Gong, H. Hu, J. Tian, and T. Cheng, "Energy harvesting jammer enabled secure communication for cooperative NOMA systems," in *2020 Int. Conf. Wireless Commun. Signal Process. (WCSP)*, 2020, pp. 801–806, DOI: 10.1109/WCSP49889.2020.9299881.

[15] A. Jindal and R. Bose, "Resource allocation in secure multicarrier AF relay system under individual power constraints," *IEEE Trans. Veh. Technol.*, vol. 66, no. 6, pp. 5070–5085, June 2017, DOI: 10.1109/TVT.2016.2623747.

[16] O. Waqar, H. Tabassum, and R. Adve, "Secure beamforming and ergodic secrecy rate analysis for amplify-and-forward relay networks with wireless powered jammer," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3908–3913, 2021, DOI: 10.1109/TVT.2021.3063341.

[17] D. Lee,"Secrecy analysis of relay-users election in AS-AF systems over nakagami fading channels," *IEEE Trans. Veh. Technol.,* vol. 70, no. 3, pp. 2378–2388, 2021, DOI: 10.1109/TVT.2021.3058262.

[18] L. Fan, X. Lei, N. Yang, T. Q. Duong, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying with cochannel interference," *IEEE J. Sel. Topics Signal Process.*, vol. 10, no. 8, pp. 1494–1505, 2016, DOI: 10.1109/JSTSP.2016.2607692.

[19] L. Fan, R. Zhao, F. Gong, N. Yang, and G. K. Karagiannidis, "Secure multiple amplify-and-forward relaying over correlated fading channels," *IEEE Trans. Commun.*, vol. 65, no. 7, pp. 2811–2820, 2017, DOI: 10.1109/TCOMM.2017.2691712.

[20] S. Han, J. Li, W. Meng, M. Guizani, and S. Sun, "Challenges of physical layer security in a satellite-terrestrial network," *IEEE Network*, pp. 1–7, 2022, DOI: 10.1109/MNET.103.2000636.

[21] L. Qing, H. Guangyao, and F. Xiaomei, "Physical layer security in multi-hop AF relay network based on compressed sensing," *IEEE Commun. Lett.*, vol. 22, no. 9, pp. 1882–1885, 2018, DOI: 10.1109/LCOMM.2018.2853101.

[22] M. Marzban, A. El Shafie, A. Sultan, and N. Al-Dhahir, "Securing full-duplex amplify-and-forward relay-aided communications through processing-time optimization," *IEEE Trans. Veh. Technol.*, pp. 1–1, 2022, https://doi.org/10.1109/TVT.2022.3163376.

[23] A. H. A. El-Malek and S. A. Zummo, "Cooperative cognitive radio model for enhancing physical layer security in two-path amplify-and-forward relaying networks," in *Proc. IEEE GLOBECOM*, 2015, pp. 1–6, DOI: 10.1109/GLOCOM.2015.7417778.

[24] A. Pandey and S. Yadav, "Physical layer security in cooperative AF relaying networks with direct links over mixed rayleigh and double-rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 67, no. 11, pp. 10 615–10 630, 2018, DOI: 10.1109/TVT.2018.2866590.

[25] K. Venugopalachary, D. Mishra, R. Saini, and V. Chakka, "Secrecy-aware jointly optimal transmit power budget sharing and trusted DF relay placement," in *2019 IEEE Wireless Commun. Networking Conf. Workshop (WCNCW)*, 2019, pp. 1–6, DOI: 10.1109/WCNCW.2019.8902623.

[26] K. R. Liu, A. K. Sadek, W. Su, and A. Kwasinski, Cooperative communications and networking. Cambridge university press, 2009.

[27] A. Papoulis and S. U. Pillai, Probability, Random Variables, and Stochastic Processes, 4th ed. Boston: McGraw Hill, 2002.

[28] B. Barua, H. Q. Ngo, and H. Shin, "On the SEP of cooperative diversity with opportunistic relaying," *IEEE Commun. Lett.*, vol. 12, no. 10, pp. 727–729, Oct. 2008, DOI: 10.1109/LCOMM.2008.080915.

[29] I. S. Gradshteyn and I. M. Ryzhik, Table of integrals, series, and products, 7th ed. Academic Press, Amsterdam, 2007.

Kotha Venugopalachary (Student Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Nalla Malla Reddy Engineering College, affiliated with Jawaharlal Nehru Technological University (JNTU), Hyderabad, India, in 2013, the M.Tech. degree in Computational Engineering from the Rajiv Gandi University of Knowledge and Technologies, Andrapradesh, India in 2016, and currently doing Ph.D. on the topic of physical layer security in wireless cooperative systems in the department of electrical engineering, Shiv Nadar University, Uttar Pradesh, India, since 2017. His research interests include wireless communication (cooperative systems), resource allocation, physical layer security, and Graph signal processing.

Deepak Mishra (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Guru Gobind Singh Indraprastha University, New Delhi, India, in 2012, and the Ph.D. degree in electrical engineering from the Indian Institutes of Technology Delhi, New Delhi, in 2017. He has been a Senior Research Associate with the School of Electrical Engineering and Telecommunications, University of New South Wales Sydney, Australia, since August 2019. Before that, he was a Postdoctoral Researcher with the Department of Electrical Engineering (ISY), Linköping University, Linköping, Sweden, from August 2017 to July 2019. He has also been a Visiting Researcher with the Northeastern University, Boston, MA, USA, University of Rochester, Rochester, NY, USA, Huawei Technologies, Paris, France, and Southwest Jiaotong University, Chengdu, China.

His current research interests include energy harvesting cooperative communication networks, massive MIMO, backscattering, physical layer security, as well as signal processing and energy optimization schemes for the uninterrupted operation of wireless networks. He was a recipient of the IBM Ph.D. Fellowship Award in 2016, the Raman Charpak Fellowship Award in 2017, and the Endeavour Research Fellowship Award in 2018. He was selected as an Exemplary Reviewer of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS in 2017 and 2018, IEEE WIRELESS COMMUNICATIONS LETTERS in 2019, and IEEE TRANSACTIONS ON COMMUNICATIONS in 2019 and 2020.

Ravikant Saini (Member, IEEE) received the B.Tech. degree in Electronics and Communication Engineering and M.Tech. degree in Communication Systems from the Indian Institute of Technology Roorkee, India, in 2001 and 2005, respectively. He has received the Ph.D. degree from the Indian Institute of Technology Delhi, India, in 2017. From 2005 to 2009 he worked as a Senior Software Engineer with Aricent Technology, Gurgaon, India. From 2009 to 2011 he worked as an Assistant Professor in Shobhit University, Meerut, India. He is currently an Assistant Professor in the Department of Electrical Engineering, IIT Jammu, Jammu, India. His research interests include wireless communication, resource allocation, and physical layer security.

BER-Aware Backscattering Design for Energy Maximization at RFID Passive Tag

Amus Chee Yuen Goay, *Student Member, IEEE*, Deepak Mishra, *Member, IEEE*, and Aruna Seneviratne, *Member, IEEE*

***Abstract*—The radio frequency identification (RFID) passive tag is a wireless communication device with high energy sustainability, such that it uses the incident radio frequency (RF) signal to backscatter its information. This paper investigates the output load power maximization with optimal load impedances selection in the backscatter communication (BackCom) network. The considered BackCom system comprises a reader broadcasting an unmodulated carrier to the passive tag in the downlink. The tag backscatters its information signal to the reader with binary amplitude-shift keying (BASK) modulation in the uplink. We formulated an average output load power maximization problem by jointly optimizing the reflection coefficients while satisfying the minimum bit error rate (BER) requirement and tag sensitivity constraint. To simplify the problem, we transform the BER constraint to the modulation index constraint and reduce the 4 variables problem to 2 variables convex optimization problem. Using the Karush-Kuhn-Tucker (KKT) conditions, we design an algorithm to obtain the closed-form expression for the global optimal reflection coefficients that maximize the output load power. The simulation results provide insight into the impact of the information bit probability, tag sensitivity constraint, and BER on the achievable average load power. An overall gain of around 16% signifies the utility of our proposed design.**

***Index Terms*—Backscattering, RFID, Passive Tag, ASK, Energy Maximization, BER, Optimization.**

I. INTRODUCTION

RAdio Frequency Identification (RFID) device is a wireless communication tag that transmits information when activated by an interrogation pulse from a dedicated RFID interrogator. The first RFID passive tag was invented in the 1970s by Mario Cardullo but did not gain attention from the world. With the advent of the Internet of Things (IoT), RFID technology gained lots of interest and significant development. RFID and wireless sensor networks (WSNs) are the two main technologies being used and are becoming the two pillars of IoT [1]. RFID technology has played an important role in complementing the limitations of WSNs in IoT, specifically in manufacturing cost and energy source supplement of sensor nodes. The wireless sensor nodes will no longer require any active radio frequency (RF) component and have low power consumption, which all benefit from integrating the backscattering technique of RFID. However, the low energy efficiency in RFID far-field applications is still a major bottleneck to overcome [2]–[4].

A. C. Y. Goay, D. Mishra and A. Seneviratne are with the School of Electrical Engineering and Telecommunications, University of New South Wales, Sydney, NSW 2052, Australia (E-mail: a.goay@student.unsw.edu.au, d.mishra@unsw.edu.au, a.seneviratne@unsw.edu.au).

Corresponding author: A. C. Y. Goay

DOI: 10.36244/ICJ.2022.4.7

A. State-of-the-Art

In a backscatter communication (BackCom) system, a transmitter broadcasts a RF signal to power the passive RFID tag. The tag is a data carrier device designed to backscatter its information to the reader when interrogated, known as the wireless information transfer (WIT) [5]. In general, the passive tag generates information by load modulation, which switches the output loads to modulate and 'reflect' the incoming signal into a backscattered signal [6]. The 2 prominent load modulation schemes are amplitude-shift keying (ASK) and phase-shift keying (PSK) [7].

The RFID tag performance can be characterized by the data transmission rate, tag-to-reader transmission range, output load power, and bit error rate (BER) [8], [9]. The output load power depends on the connected output load in the load modulation scheme. The tag transfers the maximum load power with a perfectly matched output load, whereas the load power decreases with the mismatching degree. Since the tag performance is highly load-dependent [10], [11], existing research has revealed that load selection plays a huge role in the BackCom system. In [9], Muralter et al. have shown that the maximum transmission range varies significantly with the different output loads. Another work demonstrated simple rules for load selection to achieve a long transmission range, with one load in perfectly matched condition and another load greatly mismatched [12], [13]. Besides, in [11], Bletsas et al. illustrated the load selection policy for minimizing BER for ASK and PSK modulations without considering tag power sensitivity.

On the other hand, De Vita et al. proposed an output load selection with an equal mismatch in both states [7], which is different from [11]–[13]. In [14], Karthaus et al. investigated the load impedance selections exploited in [7], [11], [12], and showed the power efficiency varies with modulation depth.

Here it maybe also noted that recently there has been increasing focus on using multiple antennas at the reader and emitter [15]–[17] to exploit beamforming gains for overcoming the shortcomings of BackCom. However, this paper aims at enhancing the performance of single antenna reader aided RFID-based BackCom systems by optimally designing the underlying reflection coefficients at the tag.

B. Motivation and Contributions

The BackCom system has poor efficiency in far-field applications because the harvested output energy decreases dramatically over longer distances [18]. Therefore, the utility of the tag can be significantly improved by maximizing the

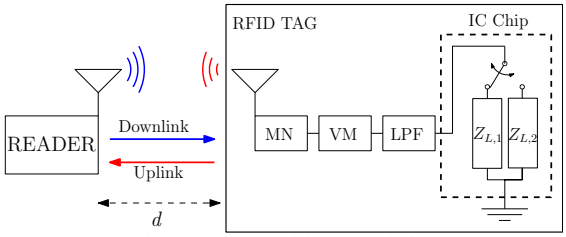


Fig. 1: BackCom system and its transmission protocol.

of the tag can be significantly improved by maximizing the output load power. Thus, allowing the tag to perform more on-board tasks and suit more applications. Unlike existing works considering equal probability for bits '0' and '1' during transmission, we determine the maximum average load power with unequal information bits probability for binary ASK (BASK) modulation scheme.

Besides, authors in [7], [11]–[14] have stated different load selections without finding the optimal value for enhancing the tag performance. *To the best of our knowledge, the average load power maximization with optimal load impedance selection under the BER and energy constraints has not been investigated yet.* This work will act as a benchmark whose results can be extended for other modulation schemes like M-ary ASK and PSK in the future.

The key contribution of this work is three-fold. 1) We formulated an RFID tag output load power maximization problem by jointly optimizing the reflection coefficients while considering the BER and tag sensitivity constraints. 2) We transformed the original 4-variable problem into a reduced optimization 2-variable convex problem. Then, we proposed an algorithm to determine the closed-form expression for the global optimal solution with the Karush-Kuhn-Tucker (KKT) conditions. 3)Simulation results are presented to quantify the maximum average load power for different applications under the varying value of the key system parameters. Here, we provided the design insight on the optimal value of the load impedances and verified the utility of the proposed optimal design by determining the achievable gain over the benchmark gain.

II. System Description

A. System Model and Transmission Protocol

Fig.1 shows a monostatic BackCom system with one reader and one passive RFID tag separated by distance d in a free-space transmission medium. As a dedicated power source, the reader stably broadcasts an unmodulated RF carrier with constant power P_t to the passive tag in the downlink. Then, the tag transmits the backscattered signal to the reader in the uplink. The passive tag comprises a receiver antenna, matching network (MN), voltage multiplier (VM), low-pass filter (LPF), and an integrated circuit (IC) chip[1] [18]. When a sinusoidal electromagnetic (EM) wave is presented, the tags will transfer the power of the EM wave into DC power and deliver it to power the IC chip. Once the IC chip is activated, it generates the information signals by switching between 2 output loads $(Z_{L,1}, Z_{L,2})$. These loads are selected depending on the modulation scheme, in which we consider the BASK in this paper. Therefore, we set the information bits '0' and '1' are generated when the output load impedances are $Z_{L,1}$ and $Z_{L,2}$, respectively. Also, we consider that the passive tag operates with the minimum scattering antenna.

[1]In the latest research, the traditional RFID tag integrated with sensing electronics, transforming it into a sensing and computational platform, has been studied for IoT applications. The tag with sensing capability is called computational RFID (CRFID), which has higher power consumption during operation [1].

B. RFID Tag Load Power Analysis

As we aim to maximize the average load power transfer to the tag, we first study the key parameters. According to Kurokawa [19], the power wave reflection coefficient is defined as the ratio of the reflected power wave to the total incident power wave. This paper denotes Γ_i as the power wave reflection coefficient, for $i \in \{1,2\}$ represent when the tag connects to $Z_{L,1}$ and $Z_{L,2}$, respectively. The Γ_i is given by [19]:

$$\Gamma_i \triangleq \frac{Z_{L,i} - \bar{Z}_A}{Z_{L,i} + Z_A}, \quad \forall i = \{1,2\}, \tag{1}$$

where $Z_A = R_A + jX_A$ is the antenna impedance, $\bar{Z}_A$ is the conjugate of Z_A, and $Z_{L,i} = R_{L,i} + jX_{L,i}$ [19]. The $R_{L,i}$ and R_A are the output load resistance and antenna resistance, respectively, whereas $X_{L,i}$ and X_A are the output load reactance and antenna reactance. To simplify the design optimization without the loss of generality, we consider the normalized load impedance $Z_{n,i} \triangleq R_{n,i} + jX_{n,i}$, and given that [12]:

$$R_{n,i} + jX_{n,i} \triangleq \frac{R_{L,i}}{R_A} + j\frac{X_{L,i} + X_A}{R_A}, \quad \forall i = \{1,2\}, \tag{2}$$

where $R_{n,i}$ is the normalized load resistance and $X_{n,i}$ is the normalized load reactance. Therefore, Γ_i can be expressed in $Z_{n,i}$ as below:

$$\begin{aligned}\Gamma_i &\triangleq \frac{Z_{n,i} - 1}{Z_{n,i} + 1} \\ &= \frac{R_{n,i}^2 + X_{n,i}^2 - 1 + j2X_{n,i}}{(R_{n,i}+1)^2 + X_{n,i}^2} \\ &= \Gamma_{a,i} + j\Gamma_{b,i}, \quad \forall i = \{1,2\},\end{aligned} \tag{3}$$

where $\Gamma_{a,i} \triangleq \frac{R_{n,i}^2 + X_{n,i}^2 - 1}{(R_{n,i}+1)^2 + X_{n,i}^2}$ and $\Gamma_{b,i} \triangleq \frac{2X_{n,i}}{(R_{n,i}+1)^2 + X_{n,i}^2}$.

The output load power $P_{L,i}$ delivered to the IC chip is given by [20]:

$$\begin{aligned}P_{L,i} &\triangleq P_a\left(1 - |\Gamma_i|^2\right) \\ &= P_a\left(1 - \Gamma_{a,i}^2 - \Gamma_{b,i}^2\right), \quad \forall i = \{1,2\},\end{aligned} \tag{4}$$

where $P_a \triangleq P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2$ is the maximum available power of $P_{L,i}$ [10]. The parameter P_t is the transmit power of the reader, G_t and G_r are the antenna gain of tag and reader, respectively, and λ is the wavelength of the RF carrier.

III. PERFORMANCE METRICS FOR BACKSCATTERING

In [8], [9], the authors elaborated the main factors that decide the maximum transmission range are load power, backscattered power, and BER. This paper considers the tag power sensitivity and the BER minimum requirement as the operation constraints to determine the optimal load impedances and the maximum average load power.

A. Tag Power Sensitivity

In the BackCom system, the tag remains in sleep mode and is only activated when enough power and a minimum threshold voltage are provided. Therefore, $P_{L,i}$ must be greater than the minimum load power threshold $P_{L,min}$, which is the sustainability requirement of the BackCom system. When $P_{L,i} < P_{L,min}$, the tag is not activated, and no information will be generated.

B. Bit Error Rate

The second factor that limits the tag performance is the BER, which is defined as the number of bits misidentified by the reader over the total number of transmitted bits at a given time interval [21]. The probability P_e is the ratio of bits in error to the total number of bits, which can be determined by the following equation [22]:

$$\begin{aligned} P_e &= \frac{1}{2}\text{erfc}\left(\frac{|V_1 - V_2|}{4\sqrt{2}\cdot\sigma}\right) \\ &= \frac{1}{2}\text{erfc}\left(\frac{|V_0|\cdot m}{2\sqrt{2}\cdot\sigma}\right), \end{aligned} \tag{5}$$

where V_i is the voltage applied to the reader's output load when the tag is connected to $Z_{L,i}$, and $V_i = V_0$ is when the tag is operated in perfectly matched condition $\left(Z_{L,i} = \bar{Z}_A\right)$. The inevitable additive white Gaussian noise n_r is assumed to have zero mean with $\mathbb{E}\{|n_r|^2\} \triangleq \sigma^2$.The modulation index m $(0 \leq m \leq 1)$ is the characteristic difference between the backscattered signal bits '0' and '1', and is defined as below [22]:

$$\begin{aligned} m &\triangleq \frac{|\Gamma_1 - \Gamma_2|}{2} \\ &= \frac{\sqrt{\left(\Gamma_{a,1} - \Gamma_{a,2}\right)^2 + \left(\Gamma_{b,1} - \Gamma_{b,2}\right)^2}}{2}, \end{aligned} \tag{6}$$

We set $\nu \triangleq \frac{|V_0|\cdot m}{2\sqrt{2}\cdot\sigma}$, and the complementary error function $\text{erfc}\,(\nu) = 1 - \text{erf}\,(\nu)$. Given that $\text{erf}\,(\nu)$ is the error function, this implies the higher the m, the lower the BER.

IV. PROBLEM DEFINITION

A. Optimization Formulation

When the tag is activated, it generates signal information with bits '0' and '1'. We denote p_1 and p_2 $(0 \leq p_1, p_2 \leq 1)$ as the occurrence probability of bits '0' and '1', respectively, with $p_1 + p_2 = 1$. In general, it is not necessary that the bits '0' and '1' have the same occurrence probability. Therefore, we consider p_1 and p_2 as application dependent constants, and the average load power $P_{L,avg}$ is given by:

$$P_{L,avg} \triangleq p_1 P_{L,1} + (1 - p_1)\, P_{L,2}, \tag{7}$$

Given the average load power $P_{L,avg}$ as a function of Γ_i, we are interested in determining the optimal reflection coefficient to maximize $P_{L,avg}$, subjecting to the following constraints. Constraint $C1$ defines the domain of the power reflection coefficient $|\Gamma_i| \leq 1$, whereas $C2$ and $C3$ include the boundary conditions for $\Gamma_{a,i}$ and $\Gamma_{b,i}$, respectively. To meet the minimum BER requirement, the passive tag must operate with a threshold m_{th} for the modulation index m as in constraint $C4$. Furthermore, constraint $C5$ refers to the minimum load power threshold $P_{L,min}$ that must be achieved at each state. Incorporating these constraints, we maximize the average load power $P_{L,avg}$, and the corresponding optimization problem $(P1)$ can be defined as:

$$\begin{aligned} (P1): &\max_{\mathbf{\Gamma}} \quad P_{L,avg} \\ \text{subject to } &C1: \Gamma_{a,i}^2 + \Gamma_{b,i}^2 \leq 1, \ \ \forall i = \{1,2\}, \\ &C2: \Gamma_{a,i} \in [-1,1], \ \ \forall i = \{1,2\}, \\ &C3: \Gamma_{b,i} \in [-1,1], \ \ \forall i = \{1,2\}, \\ &C4: \frac{\sqrt{\left(\Gamma_{a,1} - \Gamma_{a,2}\right)^2 + \left(\Gamma_{b,1} - \Gamma_{b,2}\right)^2}}{2} \geq m_{th}, \\ &C5: P_a\left(1 - \Gamma_{a,i}^2 - \Gamma_{b,i}^2\right) \geq P_{L,min}, \ \forall i = \{1,2\}. \end{aligned}$$

where $\mathbf{\Gamma} \triangleq [\Gamma_{a,1}, \Gamma_{a,2}, \Gamma_{b,1}, \Gamma_{b,2}]$.

Remark 1 *The IC chip will consume the power $P_{L,min}$ to generate the information signal, whereas the remaining power is delivered to a storage system. The total stored energy $E_{st} = (P_{L,avg} - P_{L,min})T$ over the operation period T is then used for the on-board task during the non-interrogating period. Therefore, the allowable on-board tasks depend on $P_{L,avg}$.*

The problem $(P1)$ is a 4-variable optimization problem, which is then reduced to a 2-variable problem with the following Lemmas.

Lemma 1 *The average load power is maximized when either $\Gamma_{a,i} = 0$ or $\Gamma_{b,i} = 0$.*

Proof *First, we set $\Gamma_{b,i}$ as a constant and we found that $\frac{\partial^2 P_{L,i}}{\partial \Gamma_{a,i}^2} = -2P_a$, which implies $P_{L,i}$ is a concave function in $\Gamma_{a,i}$. Therefore, for a given $\Gamma_{b,i}$, the maximum load power as obtained by solving $\frac{\partial P_{L,i}}{\partial \Gamma_{a,i}} = 0$ is $\Gamma_{a,i} = 0$. Likewise, we set $\Gamma_{a,i}$ as a constant and we found that $\frac{\partial^2 P_{L,i}}{\partial \Gamma_{b,i}^2} = -2P_a$, which implies $P_{L,i}$ is also a concave function in $\Gamma_{b,i}$. Similarly, for a given $\Gamma_{a,i}$, the maximum load power as obtained by solving $\frac{\partial P_{L,i}}{\partial \Gamma_{b,i}} = 0$ is $\Gamma_{b,i} = 0$. Hence, we proved Lemma 1.*

Lemma 2 *To ensure better receiver sensitivity at the reader while maximizing the average load power, we have to set $\Gamma_{b,i} = 0$ as compared to $\Gamma_{a,i} = 0$.*

Proof *Refer to Appendix A for the proof of Lemma 2.*

The following remark explains the practical use of Lemma 2 in the tag design.

Remark 2 *Since our BackCom system considers ASK modulation, the backscattered signal of the passive tag is designed to satisfy the phase-equality condition. Accordance to Lemma 2, we set $X_{n,i} = 0$, and $R_{n,i} = \frac{1+\Gamma_{a,i}}{1-\Gamma_{a,i}}$. The normalized load impedance plays a key parameter in the backscatter tag design [20].*

Using Lemma 2, and assuming $\Gamma_{a,1} \geq \Gamma_{a,2}$ without any loss of generality, we can reformulate the optimization problem $(P1)$ into $(P2)$ as defined below:

$$\begin{aligned} (P2): \max_{\Gamma_{a,1},\Gamma_{a,2}} \quad & P_{L,avg} \\ \text{subject to} \quad & C2, \\ & C6: \frac{\Gamma_{a,1}-\Gamma_{a,2}}{2} \geq m_{th}, \\ & C7: P_a\left(1-\Gamma_{a,i}^2\right) \geq P_{L,min}, \ \ \forall i = 1,2. \end{aligned}$$

V. Proposed Solution Methodology

A. Problem Feasibility and Convexity

Before solving problem $(P2)$, we discuss its feasibility condition with Lemma 3.

Lemma 3 *If problem $(P2)$ is feasible, $m_{th} \leq \sqrt{1-\frac{P_{L,min}}{P_a}}$ is always true.*

Proof *Refer to Appendix B for the proof of Lemma 3.*

Next, we discuss the convexity of problem $(P2)$ with Lemma 4.

Lemma 4 *The problem $(P2)$ is a convex problem.*

Proof *Refer to Appendix C for the proof of Lemma 4.*

B. Implementation Detail

We denote the maximum average load power for problem $(P2)$ as $P_{L,avg}^*$, and the underlying optimal solution as $\mathbf{\Gamma}^* = \left[\Gamma_{a,1}^*, \Gamma_{a,2}^*, \Gamma_{b,1}^* = 0, \Gamma_{b,2}^* = 0\right]$. Since $(P2)$ is a convex problem, we can claim that the Karush-Kuhn-Tucker (KKT) point gives the global optimal solution. The Lagrangian of $(P2)$ is:

$$\begin{aligned} \mathcal{L} = & -p_1 P_a\left(1-\Gamma_{a,1}^2\right) - (1-p_1) P_a\left(1-\Gamma_{a,2}^2\right) \\ & + \lambda_1\left(m_{th} - \frac{\Gamma_{a,1}-\Gamma_{a,2}}{2}\right) + \lambda_2\left(\Gamma_{a,1}^2 - 1 + \frac{P_{L,min}}{P_a}\right) \\ & + \lambda_3\left(\Gamma_{a,2}^2 - 1 + \frac{P_{L,min}}{P_a}\right), \end{aligned} \tag{8}$$

where λ_1 represents the Lagrange multipliers associated with $C6$, and λ_2, λ_3 correspond to $C7$ for $i \in \{1,2\}$, respectively. The KKT point can be found by solving the following equations.

$$\frac{\partial \mathcal{L}}{\partial \Gamma_{a,1}} = 2p_1 P_a \Gamma_{a,1} - \frac{1}{2}\lambda_1 + 2\lambda_2 \Gamma_{a,1} = 0, \tag{9}$$

$$\frac{\partial \mathcal{L}}{\partial \Gamma_{a,2}} = 2(1-p_1) P_a \Gamma_{a,2} + \frac{1}{2}\lambda_1 + 2\lambda_3 \Gamma_{a,2} = 0, \tag{10}$$

$$\lambda_1\left(m_{th} - \frac{\Gamma_{a,1}-\Gamma_{a,2}}{2}\right) = 0, \tag{11}$$

$$\lambda_2\left(\Gamma_{a,1}^2 - 1 + \frac{P_{L,min}}{P_a}\right) = 0, \tag{12}$$

$$\lambda_3\left(\Gamma_{a,2}^2 - 1 + \frac{P_{L,min}}{P_a}\right) = 0. \tag{13}$$

where (9) and (10) are the sub-gradient conditions, and (11),(12),(13) are the complementary slackness conditions. While solving (9) – (13), we obtain $\mathbf{\Gamma}^*$ in terms of the constant parameters, and thereby determine $P_{L,avg}^*$. Subsequently, we discuss the method to determine the KKT point in Lemma 5.

Lemma 5 *We can obtain the global optimal solution $\mathbf{\Gamma}^*$ by considering 3 cases, which are case (a) : $\lambda_1 \neq 0, \lambda_2 = \lambda_3 = 0$, case (b) : $\lambda_1, \lambda_2 \neq 0, \lambda_3 = 0$, and case (c) : $\lambda_1, \lambda_3 \neq 0, \lambda_2 = 0$.*

Proof *Since the objective function is decreasing with $\Gamma_{a,1}$ and $\Gamma_{a,2}$, the optimal solution without the constraints will have $\Gamma_{a,1} = \Gamma_{a,2} = 0$. However, constraint $C6$ requires a minimum separation between $\Gamma_{a,1}$ and $\Gamma_{a,2}$. Therefore constraint $C6$ is satisfied at equality, which implies λ_1 is always positive. It is noticed that λ_2 and λ_3 simultaneously greater than zero only when $m_{th} = \sqrt{1-\frac{P_{L,min}}{P_a}}$, which will obtain the same $\mathbf{\Gamma}^*$ at $\lambda_2 \neq 0$. Therefore, the optimal solution is given by either or both λ_2 and λ_3 are zero, while $\lambda_1 > 0$.*

Using Lemma 5, we proposed an algorithm to solve problem $(P2)$ and determine $\mathbf{\Gamma}^*$ and $P_{L,avg}^*$. We first consider case (a) and obtain the optimal solution by assuming it satisfied the boundary condition, denoted as $\Gamma_{a,i}^{(a)}$. Since λ_2 is associated with constraint $C7$, and $\Gamma_{a,1} \geq \Gamma_{a,2}$, the upper boundary condition will always satisfied when we set $\lambda_2 > 0$. Similarly, the lower boundary condition will always be satisfied when we set $\lambda_3 > 0$. Therefore, the global optimal solution is obtained from case (b) when $\Gamma_{a,1}^{(a)}$ is greater than the upper bound, and case (c) when $\Gamma_{a,2}^{(a)}$ is smaller than the lower bound. We summarize the problem $(P2)$ solving steps in Algorithm 1.

Algorithm 1 Optimal reflection coefficient design to maximize $P_{L,avg}$.

Input: p_1, m_{th}, $P_{L,min}$ and P_a

Output: $\Gamma_{a,1}^*$, $\Gamma_{a,2}^*$, $P_{L,avg}^*$

Set $\lambda_1 \neq 0, \lambda_2 = \lambda_3 = 0$,

$\Gamma_{a,1}^{(a)} = 2(1-p_1) m_{th}$, $\Gamma_{a,2}^{(a)} = -2p_1 m_{th}$

if $\Gamma_{a,1}^{(a)} > \sqrt{1-\frac{P_{L,min}}{P_a}}$ **then**

  Set $\lambda_1, \lambda_2 \neq 0, \lambda_3 = 0$,

  $\Gamma_{a,1}^* = \sqrt{1-\frac{P_{L,min}}{P_a}}$, $\Gamma_{a,2}^* = \sqrt{1-\frac{P_{L,min}}{P_a}} - 2m_{th}$

else if $\Gamma_{a,2}^{(a)} < -\sqrt{1-\frac{P_{L,min}}{P_a}}$ **then**

  Set $\lambda_1, \lambda_3 \neq 0, \lambda_2 = 0$,

  $\Gamma_{a,1}^* = -\sqrt{1-\frac{P_{L,min}}{P_a}} + 2m_{th}$, $\Gamma_{a,2}^* = -\sqrt{1-\frac{P_{L,min}}{P_a}}$

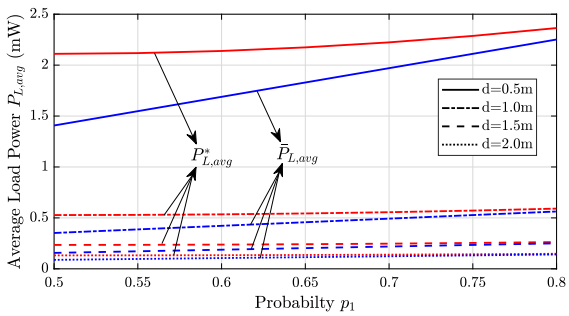


Fig. 2: Maximum average load power $P^*_{L,avg}$ for different probability p_1 with $m_{th} = 0.5$.

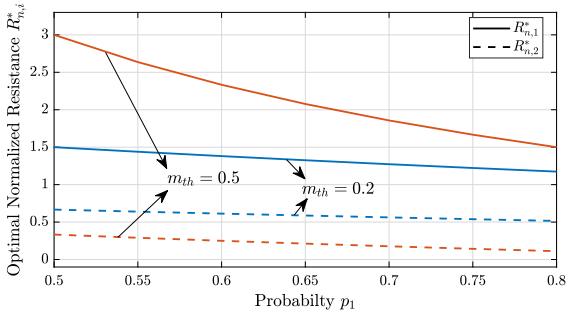


Fig. 3: Optimal normalized load resistance $R^*_{n,i}$ versus probability p_1 for $m_{th} = 0.2, 0.5$.

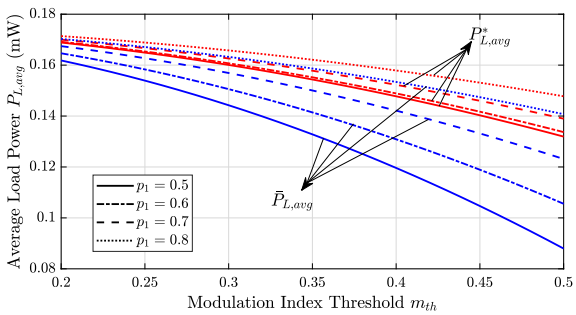


Fig. 4: Maximum average load power $P^*_{L,avg}$ for different m_{th}.

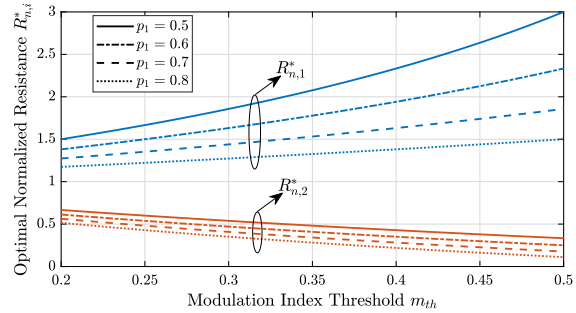


Fig. 5: Optimal normalized load resistance $R^*_{n,i}$ versus m_{th}.

else

$\Gamma^*_{a,1} = \Gamma^{(a)}_{a,1}, \Gamma^*_{a,2} = \Gamma^{(a)}_{a,2}$

end

$P^*_{L,avg} = p_1 P_a \left(1 - \left(\Gamma^*_{a,1}\right)^2\right) + (1 - p_1)\, P_a \left(1 - \left(\Gamma^*_{a,2}\right)^2\right)$

Algorithm 1 requires the system parameters p_1, m_{th}, $P_{L,min}$ and P_a as the input. After that, it generates decision making process subjected to the conditions derived from Lemma 5. Consequently, we obtain $\mathbf{\Gamma}^*$ along with the $P^*_{L,avg}$.

VI. Results and Discussion

We numerically demonstrate the performance of the optimal results obtained from problem $(P2)$. Unless otherwise stated, we set $P_t = 1$W with RF $f = 900$MHz, $\lambda = \frac{1}{3}$m, $G_t = G_r = 1$, $P_{L,min} = 10^{-4.9}$W, and $m_{th} = 0.5$. We consider the tag design in [11]–[13] as the benchmark to highlight the merits of our optimal design. Hence, we denote $\bar{P}_{L,avg}$ as the average load power of the benchmark result, with the underlying load impedances $\bar{Z}_{n,1} = 1$ and $\bar{Z}_{n,2} = \frac{1+2m_{th}}{1-2m_{th}}$ correspond to bits '0' and '1'.

A. Impact of Probability p_1 on the Optimal Average Load Power $P^*_{L,avg}$

Here, we investigate the relationship between probability p_1 and $P^*_{L,avg}$ with $m_{th} = 0.5$. Specifically, we plot the maximum average load power $P^*_{L,avg}$ for different values of p_1 and transmission distance d.

In Fig. 2, we notice that the $P^*_{L,avg}$ is greater than $\bar{P}_{L,avg}$ for $d = 0.5, 1.0, 1.5, 2.0$ m. The proposed optimal maximum load power achieves an average gain of 22.6% over the benchmark. However, the gain decreases with p_1 because the benchmark result has the highest allowable average load power when $p_1 = 1$, and the increases in p_1 will approach this outcome. Hence, as p_1 increases, the optimal load impedances $Z^*_{n,1}$ and $Z^*_{n,2}$ will approach the benchmark load selection (see Fig. 3), resulting in $P^*_{L,avg}$ approaching $\bar{P}_{L,avg}$. Besides, we observe that $P^*_{L,avg}$ is increased with p_1. This is because $P^*_{L,1}$ increases, whereas $P^*_{L,2}$ decreases with p_1, resulting in greater $P^*_{L,avg}$. It is also noticed that $P^*_{L,avg}$ increases at a shorter transmission distance d because the output load power is inversely proportional to d.

Fig.3 gives insight into the optimal load impedance $Z^*_{n,i} = R^*_{n,i} + jX^*_{n,i}$ for different p_1. As the output power is maximum when $R_{n,i} = 1$, we observed that $R^*_{n,1}$ approaches 1 as p_1 increases, whereas $R^*_{n,2}$ approaches 0 to meet the BER requirement. Furthermore, as proved in Lemma 2, $X^*_{n,1} = X^*_{n,2} = 0$. We also noticed that $Z^*_{n,i}$ does not vary with d because the transmission range is not the optimal reflection coefficient variable.

B. Impact of m_{th} on Optimal Average Load Power $P^*_{L,avg}$

The value of m_{th} varies in different applications, which depends on the BER requirement. Therefore, we study the maximum average load power $P^*_{L,avg}$ for different modulation index thresholds m_{th} at $d = 2$m. Fig.4 shows $P^*_{L,avg}$ versus m_{th} for $p_1 = 0.5, 0.6, 0.7$ and 0.8, where the optimal normalized load impedance $Z^*_{n,i}$ is depicted in Fig.5. Likewise, we observed that $P^*_{L,avg} > \bar{P}_{L,avg}$. The average gain achieved by the proposed optimal result over the benchmark is 9.9%. It is also noticed that $P^*_{L,avg}$ decreases with m_{th} due to a greater mismatch degree between the backscattered signals, as shown in Fig.5.

VII. CONCLUSION

This paper aimed to maximize the average load power of the RFID passive tag with the optimal reflection coefficients while meeting the tag sensitivity and BER constraints. We transformed the original 4 variables problem into 2 variables convex optimization problem, and obtained the closed-form expression for the global optimal reflection coefficients. The simulation results have shown that the information bits probability and modulation index can significantly impact the maximum average load power. Besides, we found that the average load power with the optimal load impedances provided an average gain of 16.3% over the benchmark.

APPENDIX A
PROOF OF LEMMA 2

In the BackCom system, there is a minimum power requirement for the backscattered signal to ensure the reader can successfully identify the signal. The backscattered power $P_{s,i}$ when the tag connected to $Z_{L,i}$ is given by [23]:

$$\begin{aligned} P_{s,i} &\triangleq P_a G_r |1-\Gamma_i|^2 \\ &= P_a G_r \left[(1-\Gamma_{a,i})^2 + \Gamma_{b,i}^2 \right], \quad \forall i = \{1,2\}, \end{aligned} \tag{14}$$

Now, we compare the 2 considered cases, where the first case assumed the reflection coefficient $\Gamma_{a,i}^{(1)} \neq 0, \Gamma_{b,i}^{(1)} = 0$, with the load power and backscattered power denoted as $P_{L,i}^{(1)}$ and $P_{s,i}^{(1)}$, respectively. The second case assumed the reflection coefficient $\Gamma_{a,i}^{(2)} = 0, \Gamma_{b,i}^{(2)} \neq 0$, with the load power and backscattered power denoted as $P_{L,i}^{(2)}$ and $P_{s,i}^{(2)}$, respectively. Then, we express the backscattered power in terms of load power as below:

$$P_{s,i}^{(1)} = P_a G_r \left(2 - \frac{P_{L,i}^{(1)}}{P_a} + 2\sqrt{1 - \frac{P_{L,i}^{(1)}}{P_a}} \right), \forall i = \{1,2\}, \tag{15}$$

$$P_{s,i}^{(2)} = P_a G_r \left(2 - \frac{P_{L,i}^{(2)}}{P_a} \right), \quad \forall i = \{1,2\}. \tag{16}$$

If we select the load impedance that gives $P_{L,i}^{(1)} = P_{L,i}^{(2)}$, we can clearly observed that $P_{s,i}^{(1)}$ is always greater than $P_{s,i}^{(2)}$. Hence, we proved Lemma 2.

APPENDIX B
PROOF OF LEMMA 3

Since $P_{L,min} \leq P_a$, constraint $C2$ will always satisfy when constraint $C7$ is satisfied in problem $(P2)$. Hence, from $C7$, we obtain the boundary condition for $\Gamma_{a,i}$ as below:

$$-\sqrt{1 - \frac{P_{L,min}}{P_a}} \leq \Gamma_{a,i} \leq \sqrt{1 - \frac{P_{L,min}}{P_a}} \tag{17}$$

As we consider $\Gamma_{a,1} \geq \Gamma_{a,2}$, the range of $(\Gamma_{a,1} - \Gamma_{a,2})$ from (17) is given by:

$$0 \leq (\Gamma_{a,1} - \Gamma_{a,2}) \leq 2\sqrt{1 - \frac{P_{L,min}}{P_a}} \tag{18}$$

Then, we rearrange constraint $C6$ of problem $(P2)$, and obtain the boundary condition for $(\Gamma_{a,1} - \Gamma_{a,2})$ as below:

$$\Gamma_{a,1} - \Gamma_{a,2} \geq 2m_{th} \tag{19}$$

While combining (18) and (19), we obtain:

$$m_{th} \leq \frac{\Gamma_{a,1} - \Gamma_{a,2}}{2} \leq \sqrt{1 - \frac{P_{L,min}}{P_a}} \tag{20}$$

Subsequently, we observe $m_{th} \leq \sqrt{1 - \frac{P_{L,min}}{P_a}}$ as the feasible condition to obtain a possible optimal solution when solving problem $(P2)$. Hence, we proved Lemma 3.

APPENDIX C
PROOF OF LEMMA 4

We determine the Hessian matrix of problem $(P2)$ objective function, which is given as [24]:

$$\begin{aligned} \mathbb{H} &= \begin{bmatrix} \frac{\partial^2 P_{L,avg}}{\partial \Gamma_{a,1}^2} & \frac{\partial^2 P_{L,avg}}{\partial \Gamma_{a,1} \partial \Gamma_{a,2}} \\ \frac{\partial^2 P_{L,avg}}{\partial \Gamma_{a,2} \partial \Gamma_{a,1}} & \frac{\partial^2 P_{L,avg}}{\partial \Gamma_{a,2}^2} \end{bmatrix} \\ &= \begin{bmatrix} -2p_1 P_a & 0 \\ 0 & -2(1-p_1) P_a \end{bmatrix} \end{aligned}$$

We observed that the diagonal entries of $\mathbb{H}$ are ≤ 0, and the determinant of $\mathbb{H}$ being non-negative, $|\mathbb{H}| \geq 0$. Hence, we proved that the objective function of the problem $(P2)$ is a concave function. Besides, it is clearly noticed that constraints $C2$ and $C6$ are linear, which are also convex.

Next, we set $f_i \triangleq P_{L,min} - P_a \left(1 - \Gamma_{a,i}^2\right)$ corresponds to constraint $C7$. The second derivative of f_i with respect to $\Gamma_{a,i}$ is $\frac{\partial^2 f_i}{\partial \Gamma_{a,i}^2} = 2P_a \geq 0$, which implies constraint $C7$ is convex. Since the objective function is a concave function, and the constraints $C2$, $C6$ and $C7$ are all convex, problem $(P2)$ is a convex optimization problem. Hence, we proved Lemma 4.

REFERENCES

[1] H. Landaluce, L. Arjona, A. Perallos, F. Falcone, I. Angulo, and F. Muralter, "A review of IoT sensing applications and challenges using RFID and wireless sensor networks," *Sensors*, vol. 20, no. 9, p. 2495, apr 2020. [Online]. Available: DOI: 10.3390/s20092495

[2] A. C. Y. Goay, D. Mishra, Y. F. Shi, and A. Seneviratne, "Throughput and energy aware range maximization in cooperative backscatter communication systems," in *Proc. IEEE 95th Vehicular Technology Conference (VTC)*, 2022, pp. 1–4.

[3] M. Kaur, M. Sandhu, N. Mohan, and P. S. Sandhu, "RFID technology principles, advantages, limitations & its applications," *International Journal of Computer and Electrical Engineering*, pp. 151–157, 2011. [Online]. Available: DOI: 10.7763/ijcee.2011.v3.306

[4] R. Want, "An introduction to RFID technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25–33, 2006.

[5] C. Jing, Z. Luo, Y. Chen, and X. Xiong, "Blind anti-collision methods for RFID system: a comparative analysis," *Infocommunications Journal*, vol. 12, no. 3, pp. 8–16, 2020. [Online]. Available: DOI: 10.36244/icj.2020.3.2

[6] X. Lu, D. Niyato, H. Jiang, D. I. Kim, Y. Xiao, and Z. Han, "Ambient backscatter assisted wireless powered communications," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 170–177, apr 2018. [Online]. Available: DOI: 10.1109/mwc.2017.1600398

[7] G. D. Vita and G. Iannaccon, "Design criteria for the RF section of UHF and microwave passive RFID transponders," *IEEE Transactions on Microwave Theory and Techniques*, vol. 53, no. 9, pp. 2978–2990, sep 2005. [Online]. Available: DOI: 10.1109/tmtt.2005.854229

[8] P. Nikitin and K. Rao, "Performance limitations of passive UHF RFID systems," in *Proc. IEEE Antennas and Propagation Society International Symposium*. IEEE, 2006. [Online]. Available: DOI: 10.1109/aps.2006.1710704

[9] F. Muralter, H. Landaluce, R. Del-Rio-Ruiz, and A. Perallos, "Selecting impedance states in a passive computational RFID tag backscattering in PSK," *IEEE Microwave and Wireless Components Letters*, vol. 29, no. 10, pp. 680–682, oct 2019. [Online]. Available: DOI: 10.1109/lmwc.2019.2935303

[10] K. Rao, P. Nikitin, and S. Lam, "Impedance matching concepts in RFID transponder design," in *Proc. Fourth IEEE Workshop on Automatic Identification Advanced Technologies (AutoID'05)*. IEEE. [Online]. Available: DOI: 10.1109/autoid.2005.35

[11] A. Bletsas, A. G. Dimitriou, and J. N. Sahalos, "Improving backscatter radio tag efficiency," *IEEE Transactions on Microwave Theory and Techniques*, vol. 58, no. 6, pp. 1502–1509, jun 2010. [Online]. Available: DOI: 10.1109/tmtt.2010.2047916

[12] P. Nikitin, K. Rao, S. Lam, V. Pillai, R. Martinez, and H. Heinrich, "Power reflection coefficient analysis for complex impedances in RFID tag design," *IEEE Transactions on Microwave Theory and Techniques*, vol. 53, no. 9, pp. 2721–2725, sep 2005. [Online]. Available: DOI: 10.1109/tmtt.2005.854191

[13] P. Nikitin, K. Rao, and R. Martinez, "Differential RCS of RFID tag," *Electronics Letters*, vol. 43, no. 8, p. 431, 2007. [Online]. Available: DOI: 10.1049/el:20070253

[14] U. Karthaus and M. Fischer, "Fully integrated passive UHF RFID transponder IC with 16.7-μ minimum RF input power," *IEEE Journal of Solid-State Circuits*, vol. 38, no. 10, pp. 1602–1608, oct 2003. [Online]. Available: DOI: 10.1109/jssc.2003.817249

[15] D. Mishra and E. G. Larsson, "Optimal channel estimation for reciprocity-based backscattering with a full-duplex MIMO reader," *IEEE Transactions on Signal Processing*, vol. 67, no. 6, pp. 1662–1677, mar 2019. [Online]. Available: DOI: 10.1109/tsp.2019.2893859

[16] ——, "Multi-tag backscattering to MIMO reader: Channel estimation and throughput fairness," *IEEE Transactions on Wireless Communications*, vol. 18, no. 12, pp. 5584–5599, dec 2019. [Online]. Available: DOI: 10.1109/twc.2019.2937763

[17] ——, "Monostatic backscattering detection by multiantenna reader," in *Proc. 53rd Asilomar Conference on Signals, Systems, and Computers. IEEE*, nov 2019. [Online]. Available: DOI: 10.1109/ieeeconf44664.2019.9048853

[18] K. Finkenzeller, RFID Handbook. Wiley, jun 2010. [Online]. Available: DOI: 10.1002/9780470665121

[19] K. Kurokawa, "Power waves and the scattering matrix," *IEEE Transactions on Microwave Theory and Techniques*, vol. 13, no. 2, pp. 194–202, mar 1965. [Online]. Available: DOI: 10.1109/tmtt.1965.1125964

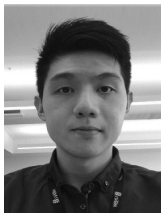
[20] A. C. Y. Goay, D. Mishra, and A. Seneviratne, "ASK modulator design for passive RFID tags in backscatter communication systems," in *Proc. IEEE 22nd Annual Wireless and Microwave Technology Conference (WAMICON)*. IEEE, apr 2022. [Online]. Available: DOI: 10.1109/wamicon53991.2022.9786078

[21] F. Fuschini, C. Piersanti, F. Paolazzi, and G. Falciasecca, "On the efficiency of load modulation in RFID systems operating in real environment," *IEEE Antennas and Wireless Propagation Letters*, vol. 7, pp. 243–246, 2008. [Online]. Available: DOI: 10.1109/lawp.2008.921354

[22] ——, "Analytical approach to the backscattering from UHF RFID transponder," IEEE Antennas and Wireless Propagation Letters, vol. 7, pp. 33–35, 2008. [Online]. Available: DOI: 10.1109/lawp.2007.914121

[23] P. Nikitin and K. Rao, "Theory and measurement of backscattering from RFID tags," *IEEE Antennas and Propagation Magazine*, vol. 48, no. 6, pp. 212–218, dec 2006. [Online]. Available: DOI: 10.1109/map.2006.323323

[24] D. Mishra and S. De, "Optimal power allocation and relay placement for wireless information and RF power transfer," in *Proc. IEEE International Conference on Communications (ICC)*. IEEE, may 2016. [Online]. Available: DOI: 10.1109/icc.2016.7511117



Amus Chee Yuen Goay (Student Member, IEEE) received the B.Eng.(Hons) degree in Mechanical Engineering from The University of New South Wales (UNSW), Australia, in 2021. Currently, he is pursuing a Ph.D. degree on the topic of Green Circuits Design for Enhancing RFID Networks Performance, in Electrical Engineering at UNSW since 2021. His current research interests include energy harvesting cooperative communication networks, backscatter tag design, backscatter communication and its application to RFID.

Deepak Mishra (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from Guru Gobind Singh Indraprastha University, New Delhi, India, in 2012, and the Ph.D. degree in electrical engineering from the Indian Institutes of Technology Delhi, New Delhi, in 2017. He has been a Senior Research Associate with the School of Electrical Engineering and Telecommunications, University of New South Wales Sydney, Australia, since August 2019. Before that, he was a Postdoctoral Researcher with the Department of Electrical Engineering (ISY), Linköping University, Linköping, Sweden, from August 2017 to July 2019. He has also been a Visiting Researcher with the Northeastern University, Boston, MA, USA, University of Rochester, Rochester, NY, USA, Huawei Technologies, Paris, France, and Southwest Jiaotong University, Chengdu, China.

His current research interests include energy harvesting cooperative communication networks, massive MIMO, backscattering, physical layer security, as well as signal processing and energy optimization schemes for the uninterrupted operation of wireless networks. He was a recipient of the IBM Ph.D. Fellowship Award in 2016, the Raman Charpak Fellowship Award in 2017, and the Endeavour Research Fellowship Award in 2018. He was selected as an Exemplary Reviewer of IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS in 2017 and 2018, IEEE WIRELESS COMMUNICATIONS LETTERS in 2019, and IEEE TRANSACTIONS ON COMMUNICATIONS in 2019 and 2020.

Aruna Seneviratne (Senior Member, IEEE) foundation Professor of Telecommunications at the University of New South Wales (Australia) where he holds the Mahanakorn Chair of Telecommunications. He has also worked at a number of other Universities in Australia, UK and France, and industrial organizations, including Muirhead, Standard Telecommunication Labs, Avaya Labs and Telecom Australia (Telstra). In addition, he has held visiting appointments at INIRA (France) and has been awarded a number of fellowships including one at the British Telecom and one at Telecom Australia Research Labs.

Aruna Seneviratne was the Director of the Australian Technology Park Laboratory of NICTA, Australia's Information and Communications Technology (ICT) Centre of Excellence. He is also the leader of the Networked System research activities within NICTA which focuses on the development of new technologies, such as methods of establishing trust, energy efficient content storage, search and distribution, that will facilitate the next generation of services in a digital economy. With the merger of NICTA with CSIRO and creation of the new CSIRO Business unit Data61, he became the Research Director for the Cyber Physical Systems Research Program.

His current research interest are in physical analytics: technologies that enable applications to interact intelligently and securely with their environment in real time. Most recently, his team has been working on using these technologies in behavioural bio-metrics, optimising the performance of wearables, and IoT system verification. He has published over 180 refereed technical papers, and book chapters. He has supervised 30 Ph.D. dissertations.

LoRa Positioning in Verification of Location Data's Credibility

Anna Strzoda, Rafał Marjasz, and Krzysztof Grochla

Abstract—**The LoRa is a novel radio communication technology providing low power and a high range of data transmission. The LoRa transmission may be used for a low-cost localization to estimate the network nodes' location. Some recent research showed that the location could be found with reasonable accuracy, with median error as low as tens of meters. Still, such results are achieved in a controlled environment with low interferences. We first evaluate the LoRa localization using an extensive data set of a telemetric network of a few thousand devices. We show that although the direct positioning based on trilateration provides limited accuracy, the measurement of LoRa transmission may be successfully used to evaluate the credibility of location information. The information about which gateways received the data and the RSSI measurements allow us to verify if the potential coordinates of a location are accurate. We propose a metric for location verification and estimate its credibility on a sample of measurements from the LoRa telemetry network.**

Index Terms—**LoRa, positioning, trilateration, multilateration**

I. INTRODUCTION

The Low Power Wide Area Networks (LP WAN) provide a high range of wireless communication, with distances up to a few tens of kilometres. Although the data rate is low, the device's low cost and energy utilization have allowed the LP WANs to attract many potential users. Few radio technologies are realizing the LP WAN concept, such as MIoTy, LoRa and Sigfox. Those technologies enable battery-powered devices to communicate over a long period using a single battery and have found multiple applications in telemetry, Smart City and remote control. The most commonly used LP WAN radio technology is LoRa. The LoRaWAN standard [1] defines the packet format and the message exchange sequence between end nodes and gateways. The LoRaWAN uses a star-of-stars topology, where multiple gateways receive messages transmitted by the end devices. The signal strength measurements received by the multiple gateways may be used to estimate the device location. The LP WANs are often used for use cases in which nodes are stationary (e.g. telemetry or lamp post control), so the measurements may be averaged over a long period to increase the accuracy. But the variability of a signal is significant due to the use of unlicensed spectrum and interferences of other transmissions using the same frequencies. Additionally, the multipath propagation and the signal deflection make the received signal level imprecise. It may change rapidly, e.g. the spatial location of objects between the node and the gateway. Some factors also influence the signal propagation over more extended periods, e.g. the presence of leaves on the trees.

Some recent research proved that LoRa and LoRaWAN communication may be used to estimate the transmitting devices' location. The true-range multilateration allows us to find the location of the signal source using the estimation of distances between the LoRa node and multiple gateways, being spatially-separated known locations. A few papers reported that the location could be found with good accuracy, with average error as low as tens of meters [2]–[4]. However, in many cases, it is evaluated in very optimistic transmission conditions, e.g. using line-of-sight communication and on a small data set. Very little research shows the accuracy of LoRa positioning in real life, with a large data set and placement of devices, including both indoor and outdoor nodes.

In many network deployments, a device's most probable location is known and denoted during the network deployment. In most telemetry networks, the technician denotes the coordinates at which the device is placed. In other use cases, such as e.g. smart metering, the nodes' location may is known from the address of the property in which the meter is installed. Such location information is, however, unreliable, as the technicians make errors when noting the location, devices are sometimes relocated, or the address may point to another owner's residence. Thus, the probable location information validation is also a valid problem and may be helpful for the network operator, e.g. to detect the errors within the location database or to detect whenever a device has been relocated. It has been referred to in the literature as a Location Verification System [5], [6], which verifies whether the location information provided by a device is credible or not.

This paper discusses whether the LoRa positioning accuracy allows us to pinpoint a device to specific coordinates directly or if it can be used to validate potential location data. We show an analysis of the true-range multilateration accuracy in realistic conditions when little is known about the radio link's attenuation and the node's placement. Based on a data set covering a city-wide telemetry network of more than 4 000 devices, we discuss the average error in distance and location estimation. Next, we propose a method for validation if a potential location is credible, and we evaluate this method using subsets of the above data.

The rest of the work is organized as follows: in the following section, we present a review of the LoRa position literature. The third section describes the dataset used. In the fourth section, we discuss the problem of verification of the potential location credibility and propose an algorithm. In the following

A. Strzoda, R. Marjasz and Krzysztof Grochla are with the Institute of Theoretical and Applied Informatics, Polish Academy of Sciences, Gliwice, Poland. (E-mails: astrzoda@iitis.pl, rmarjasz@iitis.pl, kgrochla@iitis.pl)

DOI: 10.36244/ICJ.2022.4.8

section, we evaluate the proposed algorithm using data from real transmission. We finish with conclusions in the sixth section.

II. LITERATURE REVIEW

The positioning in wireless networks is a widely researched topic. Although many of the wireless devices are equipped with a Global Positioning System (GPS) interface, the use of GPS increases the cost of device and uses additional energy. Therefore, the possibility of using low-power-wide-area signals for outdoor positioning is still needed, especially in low cost networks which do not require high accuracy or in indoor devices. The most commonly used positioning methods using LoRA signals are based on RSSI and path-loss-model, time of arrival (ToA), time difference of arrival (TDoA), and the fingerprint technique.

Semtech has implemented a proprietary geolocation functionality in LoRaWAN based on TDoA. The LoRa Alliance claims this solution achieves a positioning accuracy of 20 m to 200 m [7], depending on conditions. A positioning method based on TDoA is also used in [8] with a median location error below 500 m. The algorithm is evaluated on measurements collected during driving, cycling or walking in public with a mobile node. The same dataset has been used to evaluate the positioning proposals described in [9]. The authors compare the accuracy of TDoA-based and RSS-based (Received Signal Strength) localization in the LoRa network. A more pessimistic median error has been obtained for the RSS method - about 1 km, whereas, for TDoA, it is almost ten times smaller.

The combination of TDoA and AoA localisation in LoRaWAN is presented in [10] assuming LoS and NLoS scenarios. The most optimistic mean position error is around 160 m. In [11], the authors describe the LoRa localisation system using a multilateration algorithm based on TDoA. Experimental results give a positioning accuracy of around 0.1 km in a 6 km^2 urban area. But, the testbed is relatively poor and consists of one end node and four LoRa gateways. In [2], the authors propose algorithms to improve localization performance in noisy outdoor environments based on the path loss model and estimated RSSI error. Experimental results give an error from several to several dozen meters over the distance between devices of about 100 m. Similar results are obtained in [3]. The authors also present the RSSI-based localization techniques to reduce the effect of noise in LoRa networks for outdoor and indoor environments. The use of LoRa in outdoor and indoor positioning is also considered in [12]. The authors apply Wiener filters to reduce noise in RSSI measurements and use a trilateration algorithm. The most optimistic mean location error is less than 0.5 km in an urban area of 0.5 km^2, and 20-30 m for the indoor environment. The proposed method has been evaluated on the available dataset [13].

A LoRaWAN and Sigfox location datasets are presented in [14] as a material for evaluating fingerprint algorithms in large outdoor environments. Measurements were collected using mobile nodes (mounted on postal cars) moving around in the urban area of 50 km^2, which is a bit larger than in our dataset. The authors declare a mean location error of around 0.4 km achieved by the kNN-based fingerprint technique on the LoRaWAN dataset. Moreover, this collection has been also used to evaluate [4] or a fingerprinting and machine learning system-based architectures presented in [15], [16]. The most optimistic mean location error is below 200 m.

In [17], the authors propose the positioning system using the fingerprinting technique based on hi-res satellite images from the Deep Globe dataset [18]. In particular, the algorithm identifies the land-cover type using pixels classification and, depending on it, adjusts the path loss exponent to improve positioning. The median estimation error is below 50 m. Another locating proposal [19] is based on RSSI-interpolated fingerprint maps obtained from the propriety outdoor testbed deployed on an area several hundred times smaller than ours.

A few research papers have considered the problem of verifying location accuracy based on a wireless network signal. A. Tahbaz-Salehi and A. Jadbabaie in [20] present three distributed algorithms for coverage verification in sensor networks with no location information. Still, the paper only focuses on the localizing coverage holes problem and considers distributed sensor network topology. Some works use LoRa, e.g. [21], [22], which uses GPS to measure the location, not LoRa positioning. The paper [5] describes an information theory framework based on the threshold used in detecting a spoofed location.

Most of the mentioned papers include real deployment case studies. However, no works consider such a comprehensive, commercially used and real-life network topology as we do. Only one evaluation dataset includes a more significant number of LoRa gateways than ours. And a slightly greater testbed-deployment area. Nevertheless, the large-scale effect is achieved with vehicle-mounted mobile nodes rather than a regular network infrastructure.

III. DATASET

This section describes the comprehensive large-scale LoRa dataset considered in our research. We have used the data collection from our previous study [23]. The measurements are collected from the commercially-used network infrastructure deployed around 40 km^2 in one of the typical Polish cities. This network topology includes urban and suburban areas with different densities of node distribution in space. The network consists of over 6000 end devices and 16 LoRa gateways. The devices were transmitting two packets per day to LoRa gateways. The collection includes approximately 4 mln data points collected over seven months. The single data point provides information about RSSI and SNR measures, an id number of the LoRa gateway that received the radio packet and reception time.

The exploration of the dataset is twofold. First, estimate the RSSI-distance curve coefficients described in section IV-A and evaluate the localisation method. The measurements used for the positioning method evaluation are not included in the curve fitting process to provide valuable results. The evaluation process considers 400 end nodes with exact inevitable coordinates and at least 30 radio packages provided to each of at least three LoRa gateway.

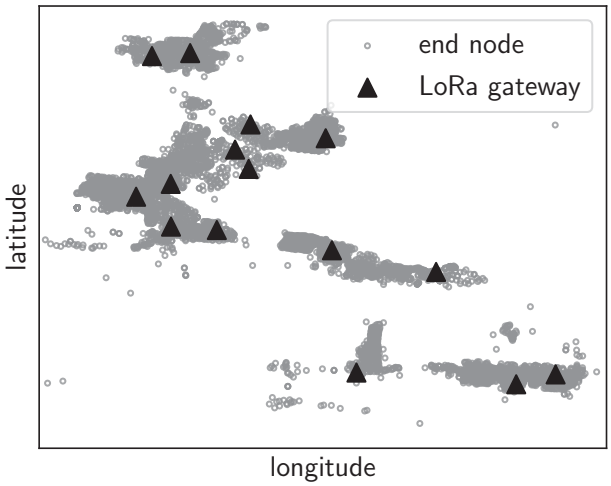


Fig. 1. The real-life LoRa network infrastructure deployed in a Polish city.

IV. Methodology

Techniques based on the signal level are commonly used for LoRa localization due to the availability of RSSI measurements in LoRa interfaces. The location is calculated using trilateration (true range lateration) which can be formulated as an optimization problem and solved by non-linear least-squares methods. An optimization method, e.g. Levenberg-Marquardt [24] may be used to find a location with the lowest square error. The trilateration algorithm requires at least three distance values between a search point (a point whose position is unknown) and nodes with known coordinates. However, this method assumes a strong correlation between the estimated distance and the actual distance in the field. Below we show the evaluation of how distance values are provided by a constructed function that maps RSSI values into the distance map to a distance measured on the ground.

A. Distance function

The estimated distance is expressed as an exponential function of the RSSI measure.

$$d(\overline{RSSI}_{ij}) = 10^{\frac{\overline{RSSI}_{ij}-a}{b}}, \qquad (1)$$

where $\overline{RSSI}_{ij}$ is a mean value calculated from all RSSI measurements obtained in the communication between i_{th} end node and j_{th} LoRa gateway. The parameters of the function: $a = -119.3$ and $b = -8.7$ are fitted curve coefficients fitted by the least-squares method. Figure 2 illustrates the logarithmic function that best fits a series of distance vs RSSI data points. Each point of the data series corresponds to an average RSSI value calculated from packets delivered from one end node to a given LoRa gateway. The parameters a and b determined in the fitted curve (fig. 2) were obtained for deployment with specific parameter values such as antenna gain or transmission power. In the case of applying this solution in different deployments, the path loss should be determined, considering the parameter values specific to given appliances, or a path loss estimation typical for a LoRa networks may be used, which has been estimated in a few research papers, e.g. in [23], [25]. These calculations should be considered to determine new parameters a and b, specific to the network implementation.

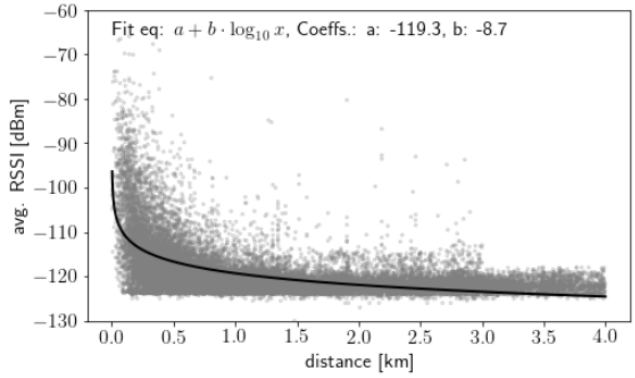


Fig. 2. The fitted logarithmic curve of the relationship between the distance and its average RSSI.

V. Comparison between estimated and real distance

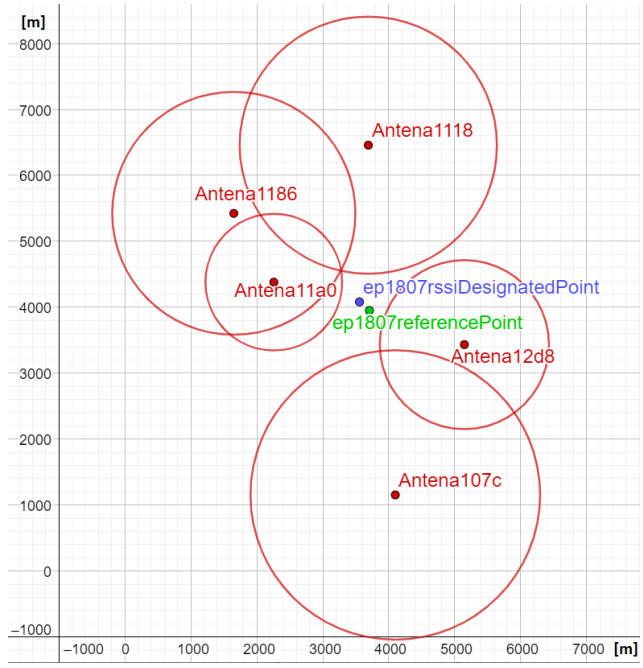


Fig. 3. Visualisation of selected single end node localisation using the proposed method. The blue point represents the localisation as an outcome of RSSI analyse based trilateration. The green point is the reference localisation taken from the GPS database. The red circles reflect the distances from the appropriate antennas resulting from the fitted RSSI vs distance curve. The error difference in distance between points equals 208.83 meters.

A particular case shown in 3 visualizes the outcome of the distance estimation for a sample end. The visible red circles represent the calculated distances from appropriate gateways receiving no less than the assumed number of packets. From these distances, the trilateration algorithm has calculated the

position marked with a blue point. The green point marks the reference location taken from a database, and the calculated error between both positions is 208.83 meters. We can see no single location where the circles showing the estimated distances meet, and the inaccuracy is significant due to the mismatching of the distances to different gateways.

The LoRa transmissions are characterized by high variability of received radio signal strength, which has been shown, e.g. [26] or in our previous work [23]. Additionally, according to [27], there are significant channel gain variations over different LoRa channels. Although the influence of this variability may be partially minimized using advanced filtering, it is unlikely that the distance estimation based on the signal level in LoRa is accurate, leading to even higher location accuracy errors.

A. Correlation between measured RSSI and the distance

Having a data set containing the actual positions of end nodes and data points with RSSI measure information received by the LoRa gateways, we attempted to verify each end node's actual position using the collected RSSI data. For each end node whose position needs to be verified, the population of RSSI measurements is considered in the communication between a given end node and each LoRa gateway. RSSI values recorded for received radio packets are calculated into distances according to the formula 1. We aim to provide a measure based on an obtained distribution of distances between the end node and the LoRa gateway.

The position verification process calculates the distance between a given end node and each LoRa gateway within range and determines the distance-based measures for included gateways. The accurate coordinates of the LoRa gateway are known. Then, the value of the cumulative distribution function at the obtained distance is determined for each LoRa gateway within range. Finally, the determined values per each gateway are used to derive measures from the formula 2.

In order to make distance comparisons, the following dependency measure was developed:

$$Rssi(d_i) = 1 - 2 \times |F(d_i) - 0.5|, \tag{2}$$

where

- d_i – is the distance in [km] between the real end node position and the i-th LoRa gateway position within the radio range of the end node,
- $F(d_i)$ – is the cumulative distribution value of the distance distribution determined from the RSSI data in the communication between the end node and the LoRa gateway.

The constructed measure rewards distances d_i having values equal to or close to the distance being the median of the distance distribution determined based on RSSI data. The values of the thus constructed measure belong to the interval $[0, 1]$. Depending on the number of LoRa gateways recording the radio signal from the end point, we get the vector $\overrightarrow{Rssi} = [Rssi(d_{i_1}), \cdots, Rssi(d_{i_n})]$ having from $n = 1$ to a maximum of $n = 16$ values calculated individually for each LoRa gateway within the radio range of the end point. For obtained vectors, we define a consistent measure $\overrightarrow{Rssi}_{(kp)}$ independent of their size, where (kp) is the k-th percentile of the vector $\overrightarrow{Rssi}$. The value represented by the hundredth percentile is the best result achieved by one of the LoRa gateways. Figure 4 presents the distribution of the value of the dependency measure $\overrightarrow{Rssi}_{(100)}$.

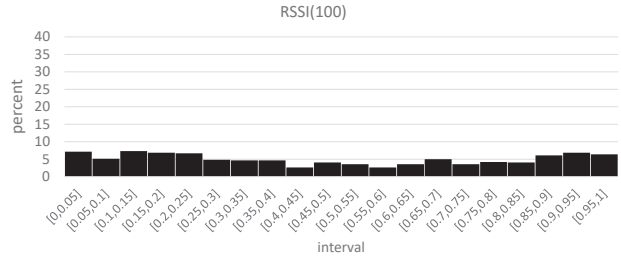


Fig. 4. The distribution of values achieved by $\overrightarrow{Rssi}_{(100)}$ measure.

The plot in fig. 4 shows the minimal dependency between the measured average RSSI and the distance. The distribution is almost uniform, and as a result, there is no clear correlation that can be derived, and the use of RSSI to validate if the distance between the node and the gateway is correct is not conclusive.

VI. PROPRIETARY METHOD OF LOCATION VERIFICATION

We developed a method for verifying the reliability of the end node location based on the proposed measure M_v that calculates one consistent numerical value characterizing the end node based on its set of features. Considerations for the measure were based on identifying irregular distances between LoRa gateways receiving the signal from the end nodes. If the end node location is accurate, then the end node signal should be received by access points in its immediate vicinity with the appropriate frequency (number of received packets). The following measure was developed based on the information about packet transmission in the LoRa network:

$$M_v = 1 - \sum_{i=1}^{N} f_{0-1}\left(\frac{diff_i}{Grdn}\right) \times \frac{Counts_i}{Soc}, \tag{3}$$

where

- $f_{0-1}(x) := \begin{cases} x, & \text{for } x \in [0, 1) \\ 1, & \text{for } x \geq 1 \end{cases}$
- $diff_i$ – denotes the difference in the positions of the array cells between the two ways of sorting the array:
  - in ascending order of the distance between the end node and the location of the i-th LoRa gateway;
  - in ascending order of the number of packets delivered to the i-th LoRa gateway.
- N – number of gateways
- $Grdn$ – (Gateways Receiving Data from Node) number of LoRa gateways recording packets received from the end node,
- $Counts_i$ – number of packets received by the i-th LoRa gateway,

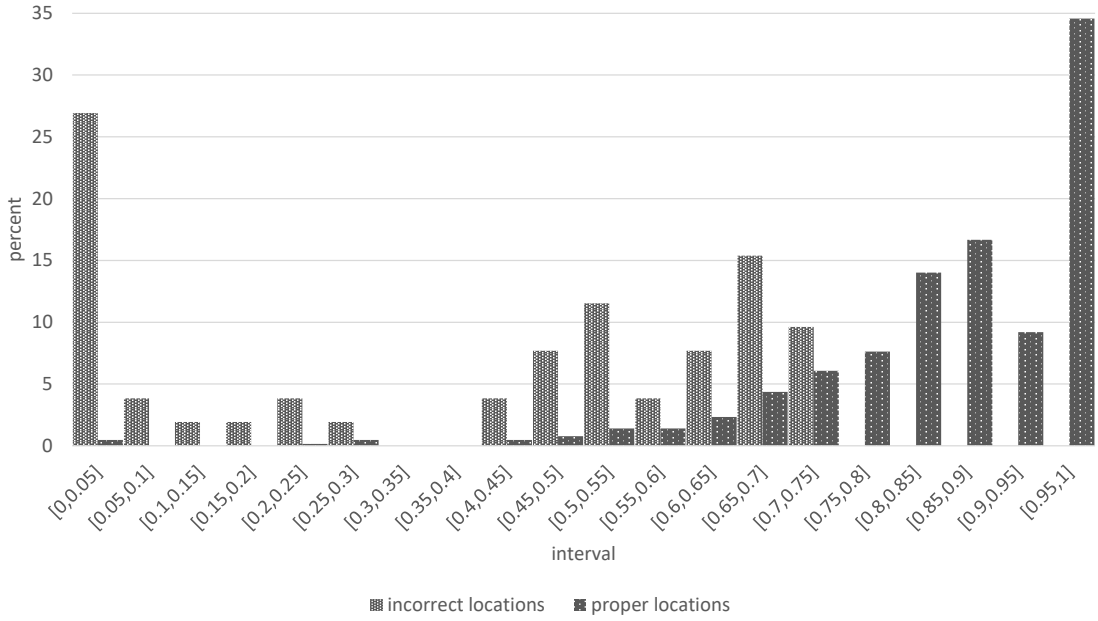


Fig. 5. The distribution of values achieved by M_v measure. The "proper locations" set stands for accurate and verified coordinates, while the "incorrect locations" set contains coordinates verified to be incorrect entries in the available LoRa dataset.

- Soc – (Sum Of Counts) the total number of packets received by the LoRa gateway.

The values of this measure belong to the interval $[0, 1]$. Figure 5 presents the measure distribution of values calculated for two sets of locations. The "proper locations" set contains end nodes with verified location coordinates. The "incorrect locations" set contains unique 52 end nodes coordinates verified as incorrect entries in the available LoRa dataset.

The proposed measure reaches high values for locations considered to be accurate. A M_v metric value higher than 0.8 indicates the correctness of the coordinates correlated with the measure. On the other side of the scale, we can observe that M_v values being close to zero indicates that it is almost certain that the node coordinates are not correct. The intermediate values within the interval $[0.2; 0.8]$ include cases for both sets of end node locations; thus, we cannot determine whether the coordinates are accurate or faulty.

The proposed metric is based on the correlation between the packet delivery to different gateways and the location. While it is highly unlikely that a distant location served by other gateways has a similar value of the proposed metrics, it may happen that some obstacles may increase the attenuation and slightly reorder the gateways. This leads to the metric values in the middle of the scale, showing some uncertainty. But the comparison between the plots shown in figures 6 and 4 shows that the proposed metric can be useful to indicate the location credibility.

VII. CONCLUSIONS

This paper discusses the applicability of LoRa positioning in a real-life, large-scale telemetry network. We first evaluate the LoRa localization using an extensive data set of a telemetric network of a few thousand devices. Our analysis shows little correlation between the distance from the gateway to the end node estimated using RSSI and the real distance measured in the field. We show that although the direct positioning based on trilateration provides limited accuracy, the measurement of LoRa transmission may be successfully used to evaluate the credibility of location information. The information about which gateways received the data and the RSSI measurements allow us to verify if potential coordinates of a location are accurate and create a LoRa location verification system.

ACKNOWLEDGMENTS

This research was funded by Polish National Center for Research and Development grant number POIR.04.01.04-00-1414/20.

REFERENCES

[1] N. Sornin, M. Luis, T. Eirich, T. Kramp, and O. Hersent, "LoRaWAN Specification v.1.1," LoRa Alliance, 2015 [Online; accessed 21-Nov-2022], https://lora-alliance.org/resourcehub/lorawan-specification-v1-1/

[2] K.-H. Lam, C.-C. Cheung, and W.-C. Lee, "New RSSI-based LoRa localization algorithms for very noisy outdoor environment," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 02, 2018, pp. 794–799, DOI: 10.1109/COMPSAC.2018.10340.

[3] ——, "RSSI-based lora localization systems for large-scale indoor and outdoor environments," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 12, pp. 11 778–11 791, 2019, DOI: 10.1109/TVT.2019.2940272.

[4] W. Ingabire, H. Larijani, R. M. Gibson, A.-U.-H. Qureshi et al., "Outdoor node localization using random neural networks for large-scale urban IoT LoRa networks," *Algorithms*, vol. 14, no. 11, p. 307, 2021, DOI: 10.3390/a14110307.

[5] S. Yan, R. Malaney, I. Nevat, and G. W. Peters, "An information theoretic location verification system for wireless networks," in *2012 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2012, pp. 5415– 5420, DOI: 10.1109/GLOCOM.2012.6503982.

[6] S. Yan, I. Nevat, G. W. Peters, and R. Malaney, "Location verification systems under spatially correlated shadowing," *IEEE Transactions on Wireless Communications*, vol. 15, no. 6, pp. 4132–4144, 2016, DOI: 10.1109/TWC.2016.2535303.

[7] L. A. S. Commitee, "LoRaWAN Geolocation Whitepaper", 2018, [Online; accessed 10-June-2022]. https://docs.wixstatic.com/ugd/eccc1a_d43b3b29dfff4ec2b00f349ced4225c4.pdf/

[8] N. Podevijn, D. Plets, J. Trogh, L. Martens, P. Suanet, K. Hendrikse, and W. Joseph, "TDoA-based outdoor positioning with tracking algorithm in a public LoRa network," *Wireless Communications and Mobile Computing*, vol. 2018, 2018, DOI: 10.1155/2018/1864209.

[9] D. Plets, N. Podevijn, J. Trogh, L. Martens, and W. Joseph, "Experimental performance evaluation of outdoor TDoA and rss positioning in a public LoRa network," in *2018 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. IEEE, 2018, pp. 1–8, DOI: 10.1109/IPIN.2018.8533761.

[10] M. Aernouts, N. BniLam, R. Berkvens, and M. Weyn, "TDAoA: A combination of TDoA and AoA localization with LoRaWAN," *Internet of Things*, vol. 11, p. 100236, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S254266052030069X

[11] B. C. Fargas and M. N. Petersen, "GPS-free geolocation using LoRa in low-power WANs," in *2017 Global Internet of Things Summit (GIoTS)*, 2017, pp. 1–6., DOI: 10.1109/GIOTS.2017.8016251.

[12] P. Savazzi, E. Goldoni, A. Vizziello, L. Favalli, and P. Gamba, "A wiener-based RSSI localization algorithm exploiting modulation diversity in LoRa networks," *IEEE Sensors Journal*, vol. 19, no. 24, pp. 12 381–12 388, 2019, DOI: 10.1109/JSEN.2019.2936764.

[13] E. Goldoni, L. Prando, A. Vizziello, P. Savazzi, and P. Gamba, "Experimental data set analysis of RSSI-based indoor and outdoor localization in LoRa networks," *Internet Technology Letters*, vol. 2, no. 1, p. e75, 2019, DOI: 10.1002/itl2.75.

[14] M. Aernouts, R. Berkvens, K. Van Vlaenderen, and M. Weyn, "Sigfox and LoRaWAN datasets for fingerprint localization in large urban and rural areas," *Data*, vol. 3, no. 2, p. 13, 2018, DOI: 10.3390/data3020013.

[15] J. Purohit, X. Wang, S. Mao, X. Sun, and C. Yang, "Fingerprinting-based indoor and outdoor localization with lora and deep learning," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 2020, pp. 1–6, DOI: 10.1109/GLOBECOM42002.2020.9322261.

[16] Z. A. Pandangan and M. C. R. Talampas, "Hybrid LoRaWAN localization using ensemble learning," in *2020 Global Internet of Things Summit (GIoTS)*, 2020, pp. 1–6, DOI: 10.1109/GIOTS49054.2020.9119520.

[17] Y. Lin, W. Dong, Y. Gao, and T. Gu, "Sateloc: A virtual fingerprinting approach to outdoor lora localization using satellite images," in *2020 19th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, 2020, pp. 13–24, DOI: 10.1145/3461012.

[18] I. Demir, K. Koperski, D. Lindenbaum, G. Pang, J. Huang, S. Basu, F. Hughes, D. Tuia, and R. Raskar, "Deepglobe 2018: A challenge to parse the earth through satellite images," *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 172–17 209, 2018.

[19] W. Choi, Y.-S. Chang, Y. Jung, and J. Song, "Low-power LoRa signal-based outdoor positioning using fingerprint algorithm," *ISPRS International Journal of Geo-Information*, vol. 7, no. 11, p. 440, 2018, DOI: 10.3390/ijgi7110440.

[20] A. Tahbaz-Salehi and A. Jadbabaie, "Distributed coverage verification in sensor networks without location information," *IEEE Transactions on Automatic Control*, vol. 55, no. 8, pp. 1837–1849, 2010, DOI: 10.1109/TAC.2010.2047541.

[21] K. Lappanitchayakul, "Anti-theft device for car: Alert system using radio wave," in *2019 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS)*. IEEE, 2019, pp. 351–355, DOI: 10.1109/ICIIBMS46890.2019.8991531.

[22] N. Ramli, M. Mun'im Zabidi, A. Ahmad, and I. A. Musliman, "An open source LoRa based vehicle tracking system," *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, vol. 7, no. 2, pp. 221–228, 2019, DOI: 10.52549/ijeei.v7i2.1174.

[23] A. Strzoda, K. Grochla, A. Frankiewicz, and Z. Laskarzewski, "Measurements and analysis of large scale lora network efficiency," in *2022 International Wireless Communications and Mobile Computing (IWCMC)*, 2022, pp. 818–823, DOI: 10.1109/IWCMC55113.2022.9824317.

[24] J. J. Moré, "The Levenberg-Marquardt algorithm: Implementation and theory," in *Numerical Analysis*, G. A. Watson, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1978, pp. 105–116, DOI: 10.1007/BFb0067700.

[25] K. Mikhaylov, M. Stusek, P. Masek, R. Fujdiak, R. Mozny, S. Andreev, and J. Hosek, "On the performance of multi-gateway LoRaWAN deployments: An experimental study," in *2020 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2020, pp. 1–6, DOI: 10.1109/WCNC45663.2020.9120655.

[26] J. Petäjäjärvi, K. Mikhaylov, M. Pettissalo, J. Janhunen, and J. Iinatti, "Performance of a low-power wide-area network based on LoRa technology: Doppler robustness, scalability, and coverage," *International Journal of Distributed Sensor Networks*, vol. 13, no. 3, p. 1550147717699412, 2017, DOI: 10.1177/1550147717699412.

[27] A. Abdelghany, B. Uguen, C. Moy, and D. Lemur, "On superior reliability of effective signal power versus RSSI in LoRaWAN," in *2021 28th International Conference on Telecommunications (ICT)*. IEEE, 2021, pp. 1–5, DOI: 10.1109/ICT52184.2021.9511510.

Anna Strzoda received the M.Sc. degree in mathematics from the Silesian University of Technology in Gliwice, Poland in 2019. She is PhD student at Institute of Theoretical and Applied Informatics Polish Academy of Sciences in Gliwice. Her research interests include optimization and data analysis.

Rafał Marjasz received the M.Sc. degree in mathematics from Silesian University of Technology in Gliwice, Poland, in 2010, and the B.E. degree in information science also from Silesian University of Technology in 2014, where he is currently pursuing the Ph.D. degree. He works as an assistant in Institute of Theoretical and Applied Informatics, Polish Academy of Sciences. His research interests include wireless communication, optimization, queuing theory and discrete event simulations.

Krzysztof Grochla received the M.S. degree in computer science from the Silesian University of Technology in 2001, the Ph.D. degree from the ITAI PAS in 2007 and habilation in 2020. From 2008 he has been with Proximetry, from 2010 serving as a head of the R&D department in an SME developing software for management of wireless networks. From 2018 he is leading the Internet of Things Group at ITAI PAS, working on IoT in Smart City applications. His research is oriented on performance evaluation of networking protocols and mechanisms for autoconfiguration and optimization of wireless networks.

Using Dynamic Programming to Optimize Cellular Networks Modeled as Graphical Games

Artur Popławski, and Szymon Szott

***Abstract*—Cellular networks are often modeled using game theory, with base stations as players contending for a shared resource (the radio channel). Alternatively, if base stations are considered as nodes joined by edges (which represent significant interference), we obtain a graph structure. A game represented in this way is called a graphical game. We explore this representation by decomposing the network graph through tree decomposition and apply dynamic programming to find the optimum welfare, i.e., a resource allocation strategy profile most effective from the point of view of the overall network performance. We verify our approach through simulations and discuss the possibility of implementing this solution in a distributed manner.**

***Index Terms*—cellular networks, game theory, graphical games, LTE, optimization, welfare, tree decomposition**

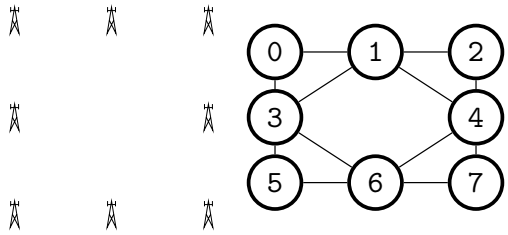


Fig. 1. An arrangement of wireless base stations (left) and their corresponding graph (right). The edges connect nodes corresponding to base stations whose distance from each other does not exceed, in this case, half of the length of the diagonal between the stations furthest apart from each other.

I. INTRODUCTION

OPTIMISING the performance of a single base station (BS) in a cellular network is a relatively well understood problem. In an OFDM-based cellular network, such as Long Term Evolution (LTE) or New Radio (NR), the core part of this optimization task is to find the allocation of time and frequency resources to optimally fulfill throughput demands considering current radio conditions, fairness between user equipment (UEs), etc. Optimising the global performance of a network is a completely different problem. A basic issue is that transmitters interact, i.e., a single BS receives both the signal dedicated to it and signals from other BSs. On a rudimentary level, the activity of these other transmitters adds to the noise in the channel formed between the transmitter and receiver and as such is destructive to the transmission. Advanced mechanisms such as coordinated multi-point (CoMP) [1] or distributed massive multiple-input and multiple-output (MIMO) [2] are designed to gain from these interactions. In this paper, however, we focus on network performance optimisation by minimising the negative effects of interference rather than gaining from them. We also work under the approximation that only the most interfering transmitters (typically the closest ones) are considered. Thus, the network is considered as a graph where nodes represent BSs and edges connect the most severely interfering ones (Fig. 1).

A situation where there is an internal conflict between agents engaged in a joint activity is naturally modeled using game theory [3], [4]. We consider a sequence of decisions made by a BS, which can be an evolved Node B (eNB) in the LTE case or a next generation Node B (gNB) in the NR case. Each decision is of the form "transmit" or "do not transmit" at a given moment. The "do not transmit" decision in this framework does not arise from the fact that there is no data to be sent. It is rather a kind of "sacrifice" made by the BS to reduce interference and increase the overall performance of the network. The strategy applied by the BS is a probability distribution over these two possible decisions. In other words, at any time the decision at the transmitter is made randomly with a certain probability and this probability is considered its strategy. Since decisions made by different transmitters are independent, this brings us into the realm of games in mixed strategies. Thus, the optimisation domain in our model is the set of possible assignments of mixed strategies to all BSs and the utility function of interest is the average throughput of the whole network.

To find the optimal network operating point, we propose an algorithm within the dynamic programming paradigm. Dynamic programming is now a commonly used tool in algorithm design, network science, control theory, and others [5]. The specific method presented here is an adaptation of an algorithm for computing a mixed strategy Nash equilibrium in a graphical game where the graph structure associated with the game is a tree [6]. We apply this algorithm to the problem of finding the optimal assignment of a transmission strategy for each BS. We relax the assumption of [6] about the graph structure, as we consider general graphs, not only trees. To consider general graphs, we turn our attention to the *tree decomposition of graphs*, which constructs trees that approximate arbitrary graphs. Another inspiration to use tree decomposition is the dynamic programming algorithms of [6], [7] and the methods described in [8].

A. Popławski is with Nokia Technology Center Krakow, Poland and AGH University of Science and Technology, Kraków, Poland (E-mail: artur.poplawski@nokia.com)

S. Szott is with AGH University of Science and Technology, Kraków, Poland (E-mail: szott@agh.edu.pl)

This work was partially supported by the Polish Ministry of Science and Higher Education with the subvention funds of the Faculty of Computer Science, Electronics, and Telecommunications of AGH University.

DOI: 10.36244/ICJ.2022.4.9

The tree decomposition, as well as the associated notion of *treewidth* (the minimum width of a tree decomposition, cf. Section II-D), has been studied extensively since its introduction [9]. We refer the reader to [10] for a graph-theoretic perspective on tree decomposition and treewidth. From an algorithmic perspective, having a precomputed tree decomposition of a graph where the treewidth of the decomposition is small, dynamic programming allows computing functions of a graph where the computation time depends on the size of the graph as a small-degree polynomial. This approach reduces the problem of efficiently calculating a function of the graph to finding a good tree decomposition of the graph. Obviously, not all graphs have a good decomposition and in general it is not easy to find such a decomposition even if they have one. However, algorithms have been proposed that allow us to find the decomposition quickly if the treewidth is small: [11]–[13].

Methods based on dynamic programming for good tree decomposition, in addition to having theoretical significance, have found their way to practical engineering and computing. An early review of applications, including those beyond theoretical interest, is given in [14]. In the area strictly related to telecommunications, it is worth mentioning [15] in which applications have been developed to the problem of routing in wireless sensor networks.

We provide a dynamic programming algorithm that finds the optimal assignment of strategies, from the point of view of global performance, given its tree decomposition. As an immediate application of the algorithm, motivating this study, we propose a mechanism of downlink transmission optimisation in an LTE or NR cellular network by changing the activity of BSs in time and reducing the negative impact of interference on network performance.

The remainder of the work is structured as follows. In Section II, we recall basic definitions related to combinatorics and game theory, including the notion of tree decomposition. Then, in Section III, the main algorithm is proposed for an abstract setting. Next, we describe the realization of the algorithm in a network of interactive devices considering distributed optimisation (Section IV). We also discuss the application of the method to solve the problem of channel allocation in cellular networks (Section V), which constitutes the main motivation for this work, and validate our approach with simulations (Section VI). Finally, Section VII summarises the results and gives insight into the perspective of further research and applications.

II. Formal Definitions and Notation

In this section, we present notational conventions used later in the text and basic definitions related to graphs, game theory, and tree decomposition, which are relevant to the modelling and analysis of cellular networks.

A. Conventions

If P is a set, then by $\{S_p\}_{p\in P}$ we understand the family of sets indexed by P. Having such a family, by $\prod_{p\in P} S_p$ we understand the Cartesian product indexed by P, i.e., $\prod_{p\in P} S_p = \{f : P \to \bigcup_{p\in P} S_p, \text{s.t. for each } p,\ f(p) \in S_p\}$.

Having $K \subset P$ and the family $\{S_p\}_{p\in P}$, by $\pi_K : \prod_{p\in P} S_p \to \prod_{k\in K} S_k$ we understand the projection operator, i.e., for $f \in \prod_{p\in P} S_p$ and $x \in K$, $\pi_K(f)(x) = f(x)$. When using the Cartesian product, we label factors of the product with an index taken from a set. The set-theoretic operation of disjoint sum on the indexing sets easily transfers to the product. Namely, if $K \cap L = \emptyset$, $(K \cup L) \subset P$, we have $\prod_{k\in K} S_k \times \prod_{l\in L} S_l = \prod_{k\in K\cup L} S_k$. We also disregard the order when referring to the elements of such a product, i.e., in our convention with the same assumptions about sets K and L as above we have: if $x \in \prod_{k\in K} S_k$, $y \in \prod_{l\in L} S_l$ then we denote $(x, y) = (y, x) = z \in \prod_{k\in K} S_k \times \prod_{l\in L} S_l = \prod_{l\in K\cup L} S_l$. To simplify exposition of the algorithm, we formally allow the Cartesian product to be taken over empty sets. By convention, a product over an empty set is the neutral element for the operation on Cartesian products: $\prod_{k\in K} S_k \times \prod_{l\in\emptyset} S_l = \prod_{k\in K} S_k$. With this convention, if formally $s' \in \prod_{l\in\emptyset} S_l$, we have $(s, s') = s$. For the $\arg\max$ operator we take the convention that for the function $f : \prod_{k\in K} S_k \to \mathbb{R}$, $s \in \prod_{k\in K} S_k$ we define $\arg\max_{s'\in\prod_{l\in\emptyset} S_l} f(s', s) = f(s)$. For function $f : X \to Y$, we refer to X also by $dom(f)$.

B. Graphs

Definition 1. *An* undirected graph *G is a pair $G = (V, E)$ where V is a finite set of vertices (representing BSs), E is the set of edges (representing interference), and $E \subset \{e \subset V : |e| = 2\}$.*

We consider only undirected graphs, which we later refer to simply as *graphs*.

Definition 2. *A* path *between elements $x, y \in V$ in graph (E, V) is a sequence $x = v_0, \ldots, v_{k-1} = y$, where for each $0 < i \leq j < k$ we have:*

1) *if $i \neq j$ then $v_i \neq v_j$,*
2) *$\{v_{i-1}, v_i\} \in E$.*

Having graph $G = (V, E)$ and vertex $v \in V$ we have a function $nb_G : 2^V \to 2^V$ defined as $nb_G(S) = \{w \in V : \exists v \in S, \{v, w\} \in E\}$. We call $nb_G(S)$ the *neighbourhood* of S in G. For the singleton $\{v\}$, we slightly abuse the notation and simply write $nb_G(v)$ instead of $nb_G(\{v\})$. For convenience, we define the *extended neighbourhood* of S in G by $xnb_G(S) = S \cup nb_G(S)$, preserving the same notation convention for singletons as in the case of the operator nb_G.

Definition 3. *An undirected graph is a tree when there is only one path between any pair of vertices. Let $G = (V, E)$ be a tree and consider any arbitrary vertex $t \in V$. Then, the pair (G, t) is called a* rooted tree *and t is called a* root.

For a rooted tree (G,t), we define a function

$$parent : V \setminus \{t\} \to V$$

such that $parent(x) = y$ iff there is a $x, y, \ldots, t$ path in G. We also define a function $children : V :\to 2^V$ such that

$$children(x) = \{y : parent(y) = x\}.$$

We refer to $v \in V$ such that $children(v) = \emptyset$ as *leaves*.

For convenience, we also define a function $offspring : V \to 2^V$ inductively (by induction starting from the leaves) as

$$offspring(x) = \emptyset,$$

where x is a leaf, and

$$offspring(x) = children(x) \cup \bigcup_{y \in children(x)} offspring(y).$$

C. Game Theory

Definition 4. *An $n-$player game Γ is a triple*

$$\Gamma = (P, \{S_p\}_{p\in P}, \{u_p\}_{p\in P}),$$

where P is the set of players ($|P| = n$), for each $p \in P$, S_p is the set of strategies available to the players, and $u_p : \prod_{p\in P} S_p \to \mathbb{R}$ is the payoff function.

For a finite set K, we define a simplex $\Delta_K = \{x \in \mathbb{R}^{|K|} : x \geq 0 \wedge \sum_{k\in K} x_k = 1\}$. Elements of the simplex represent possible probability distributions on the set K treated as a finite probability space.

Definition 5. *For game $\Gamma = (P, \{S_i\}_{i\in P}, \{u_i\}_{i\in P})$, where P and each S_p is finite, we call the game Γ in mixed strategies and denote by $M(\Gamma)$ the following game:*

$$M(\Gamma) = (P, \{\Delta_{S_i}\}_{i\in P}, \{u_{\Delta,i}\}_{i\in P}),$$

where

$$u_{\Delta,i} : \prod_{i\in P} \Delta_{S_i} :\to \mathbb{R}$$

is defined by

$$u_{\Delta,i}(x) = \sum_{s\in \prod_{j\in P} S_p} \left(\prod_{j\in P} x_j(s_j)\right) u_i(s).$$

To capture the quantitative *influence* of nodes in a game Γ, we define the function $Infl_\Gamma : P \times 2^P \to \mathbb{R}$ as

$$Infl_\Gamma(i, I) = \max_{s_{-I}\in S_{-I}} (\max_{s_I\in S_I} u_i(s_I, s_{-I}) - \min_{s_I\in S_I} u_i(s_I, s_{-I})).$$

We state that $i \in P$ is $\epsilon-$independent from $I \subset P$ if $Infl_\Gamma(i, I) \leq \epsilon$.

The intuitive meaning of this function is as follows: for a given game Γ, player i, and set of players I, it provides information about the maximal possible change of payoff of player i caused by the actions of players from I. If the value of $Infl_\Gamma(i, I)$ is small it means that in practice player i is not affected by other players in I. If the players are wireless BSs and their interaction is the radio interference, this function measures to what extent BSs from the set I interfere with the transmissions from BS i to UEs.

We assume a fixed ϵ and that for each p we have a (non-unique and possibly empty) set of non-influencing players $NI_p \subset P$ such that $p \notin NI_p$ and $Infl_\Gamma(p, NI(p)) \leq \epsilon$. This set contains those elements of P different than p itself, that collectively have little influence on the payoff p despite the action they take. Then, fixing the choice of NI_p for each p, we associate with Γ a graph $(P, E_{\Gamma,\epsilon})$ in the following manner:

$$\{v, w\} \in E_{\Gamma,\epsilon} \Leftrightarrow v \notin NI_w \vee w \notin NI_v.$$

The graph $(P, E_{\Gamma,\epsilon})$ under a suitable choice of NI is called the *ϵ graphical representation of* Γ. For $\epsilon = 0$ it is the *graphical representation of* Γ.

We emphasize once more that an ϵ graphical representation depends not only on the choice of ϵ but also on the choice of NI which is not canonical.

For a game with graphical representation $G = (P, E)$ and for player p, we formally consider u_p not as a function with the domain $\prod_{v\in P} S_v$ but as a function with the domain $\prod_{v\in xnb_G(p)} S_v$. We use the notation $dom_G(p)$ for set $xnb_G(p)$ omitting the subscript G when it is clear from the context. For the ϵ graphical representation G of Γ, there is a graphical game that approximates Γ.

The following theory gives the strongest results for games for which there exist sparse ϵ graphical representations of Γ for small ϵ. Games arising from the modeling of cellular networks where the interaction between the players representing BSs is caused by interference typically satisfy this condition. For any given BS there is a relatively small number (compared to the number of all BSs) of transmitters within the distance where interference influences signal reception.

D. Tree Decomposition

An example of how to apply dynamic programming methods in graphical games where the underlying graph is a tree is given in [6]. To apply algorithms suited to this regular structure in more general settings, we need to transform a general graph structure into a tree. A known technique of representing a general graph as a tree is tree decomposition.

Definition 6. *Let $G = (V, E)$, be a graph. The tree decomposition of G is a graph (X, F) such that:*

1) *(X, F) is a tree,*
2) *$x \subset V$ for each $x \in X$,*
3) *$\bigcup_{x\in X} x = V$,*
4) *for each $e \in E$ there is $x \in X$ such that $e \subset X$,*
5) *for each $v \in V$ if there are $x, y \in X$ such that $v \in x$ and $v \in y$, then for each z in the path from x to y in graph (X, F) we have $v \in z$.*

Having a tree decomposition $T = (X, F)$ we call $\max_{x\in X} |x| - 1$ the *treewidth* of T. The set of all tree decompositions of $G = (V, E)$ is denoted by $TD(G)$. We make the following observation:

Remark 1. *$TD(G) \neq \emptyset$ for any graph G.* □

This is the immediate consequence of the fact that the trivial graph $(\{V\}, \emptyset)$ is always a tree decomposition of $G = (V, E)$.

One can compare Fig. 2b depicting the graph with Fig. 2c depicting one of its tree decompositions to gain an intuitive understanding of the concept.

III. Welfare in Graphical Games

Using the provided definitions, we first provide a scheme for computing the welfare for a graphical game with tree decomposition and then proceed to analyze its performance. The scheme for calculating maximum welfare depends on:

- a graph $G = (P, E)$ describing the structure of the graphical game Γ,
- a particular representative $T \in TD(G)$, i.e., a tree decomposition of G.

Consider $(X, F) = T \in TD(G)$ and a distinguished element $t \in X$ as the root. We start with the following lemma:

Lemma 1. *For the tree $TD(G) \ni T = (X, F)$ rooted at $t \in X$, the following regularity condition is satisfied: for each $x \neq t$, if $v \in x \setminus parent(x)$ and $\{v, w\} \in E$ then*

$$w \in x \cup \bigcup_{z \in offspring(x)} z.$$

Proof. Assume, contrary to the thesis, that there is an $x \in X$ such that there is a $v \in (x \setminus parent(x))$ and $w \in V$ and such that $e = \{v, w\} \in E$ and $w \notin x \cup \bigcup_{z \in offspring(x)} z$. From Definition 6, we know there is a node $y \in X$ such that $e \subset y$. From the assumption we have $y \notin \{x\} \cup offspring(x)$. This means, again from Definition 6, that v belongs to every node of the tree T on the path from y to x, but such a path must contain $parent(x)$. This is a contradiction as we assumed that $v \in x \setminus parent(x)$. □

Consider the following scheme of computing welfare of Γ with operators dependent on the structure of T:

$$FD(x) = xnb_G(parent(x)) \cap \bigcup_{y \in \{x\} \cup offspring(x)} y$$

and

$$BD(x) = x \cup \bigcup_{y \in children(x)} FD(y).$$

Remark 2. *For root t, $FD(t) = \emptyset$.*

Remark 3. $BD(x) = x \cup (xnb_G(x) \cap \bigcup_{y \in offspring(x)} y)$.

Proof.

$$BD(x) = x \cup \bigcup_{y \in children(x)} FD(y) =$$
$$x \cup \bigcup_{y \in children(x)} (xnb_G(x) \cap \bigcup_{z \in \{y\} \cup offspring(y)} z) =$$
$$x \cup (xnb_G(x) \cap \bigcup_{y \in children(x)} \bigcup_{z \in \{y\} \cup offspring(y)} z) =$$
$$x \cup (xnb_G(x) \cap \bigcup_{y \in offspring(x)} y$$

The scheme works in two passes, each with two stages. In the first pass in stage one:

For $x \in X \setminus \{t\}$, let $y = parent(x)$ compute the function:

$$f_{x \to y} : \prod_{v \in FD(x)} S_v \to \mathbb{R}$$

as:

$$f_{x \to y}(s) = \max_{s' \in (\prod_{w \in BD(x) \setminus FD(x)} S_w)} \left(\sum_{v \in x \setminus y} u_v(\pi_{xnb_G(v)}(s', s)) + \sum_{z \in children(x)} f_{z \to x}(\pi_{FD(z)}(s', s)) \right)$$

and the (possibly empty) function

$$m_{x \to y} : \prod_{v \in FD(x)} S_v \to \prod_{w \in BD(x) \setminus FD(x)} S_w$$

as:

$$m_{x \to y}(s) = \arg\max_{s' \in \left(\prod_{w \in BD(x) \setminus FD(x)} S_w \right)} \left(\sum_{v \in x \setminus y} u_v(\pi_{xnb_G(v)}(s', s)) + \sum_{z \in children(x)} f_{z \to x}(\pi_{FD(z)}(s', s)) \right).$$

This ends stage one. At stage two, for root t we compute:

$$\max_{s' \in (\prod_{w \in BD(t)} S_w)} \left(\sum_{v \in x \setminus y} u_v(\pi_{xnb_G(v)}(s', s)) + \sum_{z \in children(x)} f_{z \to x}(\pi_{FD(z)}(s', s)) \right).$$

and

$$s_t = \arg\max_{s' \in (\prod_{w \in BD(t)} S_w)} \left(\sum_{v \in x \setminus y} u_v(\pi_{xnb_G(v)}(s', s)) + \sum_{z \in children(x)} f_{z \to x}(\pi_{FD(z)}(s', s)) \right).$$

Moving to the second pass, in the first stage, elements of $BD(t)$ are assigned strategies according to s_t. Then, in the second stage, assuming that for $x \in X$ the whole path from $parent(x)$ to t is processed, elements from $s' \in BD(x) \setminus FD(x)$ are assigned according to $m_{x \to parent(x)}(\pi_{BD(x) \setminus FD(x)}(s))$, where s are states already assigned.

We provide the following theorem that shows the correctness of this procedure, i.e., that all functions are well defined

and the procedure assigns strategies to all nodes in V. We show that the result of this assignment is indeed optimal in a separate theorem.

Theorem 1. *We have the following:*

1) *In the first stage of the first pass, if, for all $y \in children(x)$, functions $f_{y\to x}$ are known, then the computation of $f_{x\to parent(x)}$ is possible. For each $v \in x \setminus y$ we have $dom(u_v) \subset FD(x) \cup (BD(x) \setminus FD(x)) = BD(x) \cup FD(x)$ and for each $y \in children(x)$ we have $dom(f_{y\to x}) \subset BD(x) \cup FD(x)$.*
2) *Computation in the second stage of the second pass is possible, i.e., each $dom(u_v)$ is contained in nodes to which a strategy is already assigned or in nodes over which the max operator is calculated.*
3) *For each $y \in children(x)$, $dom(f_{y\to x})$ is contained in already set nodes and nodes over which the maximum is taken.*
4) *After the second pass all nodes have assigned strategies.*

Proof. First, we show that for $v \in x \setminus parent(x)$ we have $xnb_G(v) \subset BD(x) \cup FD(x)$. Consider $w \in xnb_G(v)$. If $w = v$ then obviously $w \in BD(x)$. If $w \in nb_G(v)$ then, by Lemma 1, $w \in x \cup \bigcup_{z\in offspring(x)} z$ and it obviously belongs to $xnb_G(x)$. Thus, by Remark 3, it also belongs to $BD(x)$. This gives us $w \in FD(x) \cup BD(x)$.

We also have, for all $z \in children(x)$, $FD(z) \subset BD(x)$. Thus, any element of the domain of $f_{z\to parent(z)} = f_{z\to x}$ is available when computing $f_{x\to y}$ according to the definition in the first pass of the algorithm. The same reasoning applies to $m_{x\to y}$ as this is just the selection of $\arg\max$ of $f_{x\to y}$.

Now, consider the second pass. The maxima can be calculated for the root, as according to the scheme functions and $f_{z\to t}$ for $z \in children(t)$ are known. Assume that assignments of the strategies are already done on the whole path from x to t. This means that it is a known argument for which the function $m_{z\to x}$ must be computed. The computation of this function extends the range over which the global solution is known. We must show that this extension is consistent among children of x. This is the case, however, where pieces of the solution computed for different children do not overlap. More formally, for $y_1, z_2 \in children(x)$ such that $z_1 \neq z_2$ we have $(BD(z_1) \setminus FD(z_1)) \cap (BD(z_2) \setminus FD(z_2)) = \emptyset$. Assume that this is not true, i.e., there exists $w \in (BD(z_1) \setminus FD(z_1)) \cap (BD(z_2) \setminus FD(z_2))$. We have an $w \in BD(z_1)$ that is either in z_1 or in one of its offspring. The same is true for z_2. From the definition of the tree, there is a path between any z_1 and any of its offspring to z_2 and any of its offspring leading through z_1, x, and z_2, as x is the common parent of z_1 and z_2. From the definition of tree decomposition we then must have $w \in z_1$, $w \in z_2$ and $w \in x$. This means that $w \in FD(z_1)$ and $w \in FD(z_2)$, which leads to a contradiction and concludes the proof. □

Now, we prove the correctness of the scheme in the case when domains S_v are finite.

Theorem 2. *For $(X, F) = T \in TD(G)$ and $t \in X$ being the root, and a set of functions $u_v : \prod_{xnb_G(v)} S_v \to \mathbb{R}$ where S_v is finite, the scheme finds a (global) maximum of the welfare function:*

$$wlf(x) = \sum_{v\in V} u_v(\pi_{xnb_G(v)}(x)).$$

Proof. Assume that $s \in \prod_{v\in V} S_v$ is the optimal assignment. In the second pass, the algorithm must consider it as part of the calculation of the operators max and $\arg\max$ in root assignment $\pi_{BD(t)}(s)$. □

IV. TOWARDS A DISTRIBUTED IMPLEMENTATION

We now outline an implementation of the algorithm presented in the previous section in a system where computations can be performed in a distributed manner. Assume that interacting nodes are organized in a way that reflects the structure of both graphs: the original interaction graph $G = (V, E)$ of the game and the chosen tree decomposition $(X, F) = T \in TD(G)$. Further, assume that each v is associated with a device. Devices can communicate with one another. Each device frequently decides about its action (strategy) from the set S_v and operates according to that choice. The result measured with numerical utility depends on the choice made by other devices associated with nodes in $nb_G(v)$. This utility function is denoted by u_v. Each device also knows the dependency of u_v from a combination of its own choice and the choices of other devices it depends on. This knowledge can be provided to the device or, in a more realistic scenario, it may come from empirical extrapolation of monitoring data. In the latter case, devices derive an empirical approximation of u_v from the observations of the actions of other devices, the knowledge of its own action, and the received utility[1]. Further, assume that for each $x \in X$ there is a distinguished device $v \in x$ which is further called the computation node and denoted by $cn(x)$. As the nodes in X (which are sets) are not disjoint, it is a valid situation where $cn(x) = cn(y)$ for $x \neq y$. The computation node is responsible for computing functions $f_{x\to parent(x)}$. Nodes for which u_v needs to be known directly by $cn(x)$, send to $cn(x)$ data which allows to compute u_v or its approximation, while the computation nodes $c(y)$ for $y \in children(x)$ send data that allows to compute the appropriate $f_{y\to x}$.

At some point (e.g., periodically) the following process occurs. Functions $f_{x\to parent(x)}$ and $m_{x\to parent(x)}$ are computed in the node $cn(x)$ for all x being leaves of T. Then, information sufficient to compute the function (or a sufficiently good approximation of the function) $f_{xparent(x)}$ and $m_{x\to parent(x)}$ is sent to $cn(parent(x))$. Each node not being the root, after receiving data from all its children, performs computation of $f_{x\to parent(x)}$ and $m_{x\to parent(x)}$ and sends information to computation node of the parent, etc. Finally, the computation node of the root t receives all information from computation nodes of its children and nodes it knows directly and itself performs computation corresponding to stage two of the first pass of the scheme. Next, the root sends information about m_t to all the nodes for which it determined an optimal strategy

[1]Such an empirical model easily captures the elements of randomness of the environment with statistical modeling.

and for all children sends $m_{x\to t}(m_t)$ to the computational node of child x. Then, for each x, the computational node that receives $m_{x\to parent(x)}(s)$ for an appropriate s sets the data in appropriate nodes and continues the process by sending appropriate data to its children. Upon receiving information about its assigned strategy, the node starts to apply it. After dissemination of the state across all nodes, the network should work in a new optimal regime.

V. INTERFERENCE GAME

We apply the proposed scheme to an interference game in a cellular network with downlink transmissions. To simplify the terminology, we identify BSs with a single cell. A set of these BSs is denoted by C. We assume that all stations use the same carrier and that downlink transmissions from BSs happen synchronously at discrete times. These assumptions are well justified for a large set of configurations of OFDM networks, e.g., for LTE TDD (Time Division Duplex) and NR networks.

For each discrete transmission opportunity, a BS decides if it transmits to at least one of the receivers assigned to it (UEs) or does not transmit at all. Again, to simplify we limit ourselves only to transmissions carrying user data, omitting in the model obligatory transmissions of reference and synchronisation signals, broadcast channels, etc. We also leave aside details of scheduling, i.e., to which of the devices the BS transmits.

In this setting, at each downlink transmission opportunity, the network is considered a game and each BS $c \in C$ is a player. With each player, we associate the strategy space $S_c = \{0, 1\}$, where 0 means that the BS is not transmitting and 1 means that it is transmitting. The payoff $u_c : \prod_{d\in C} S_d \to \mathbb{R}$ is defined as:

$$u_c(s) = \mathbb{E}[Tput_c(s)],$$

where $\mathbb{E}$ is the expected value and $Tput_c$ represents the downlink throughput and can be treated as a random variable depending on the selection of the receivers by the scheduling algorithm (so also based on the arriving data, what can be modeled as a stochastic process) and on activities of other BSs which are treated as interference. In general, the function of throughput may be complicated so, to pose the problem more concretely, we assume that if there is a transmission at all only one receiver is chosen for transmission at a given opportunity t and the function is of the form

$$Tput_c(s) = log_2\left(1 + \frac{Ps_c d(c, ue)^{-\theta}}{\sum\limits_{w\in C\setminus\{c\}} Ps_w d(w, ue)^{-\theta} + \nu}\right),$$

where the ue is a random position representing the receiver (UE) selected by c, $d(x, y)$ is the Euclidean distance between BS x and ue y , $\theta > 2$ is a propagation coefficient describing the attenuation of the signal with distance, ν is random noise and the expected value in u_c is taken over the distribution over the choice of ue.

We neglect the interference from far away stations, stations placed with an attenuating factor in between (e.g., walls), and stations that are close, but there are no receivers in the area where their interference is strong. The activity of these stations contributes to the interference term but this contribution is limited. This corresponds exactly to the elimination of the subset of players for which the influence function described in Section II-C is small. In this approximation, the sum in the denominator in the formula for u_c may be taken over the proper subset of $C \setminus \{c\}$. In other words, this leads to the assumption that the game has a graphical representation that is sparse.

We also assume that nodes exchange information about transmission allocation with their neighbours. That is, if a node strongly interferes with a given one, so that both are linked in the graph representing the game, it frequently sends information about its activity. This allows each node to estimate their u_c. Note that this information does not need to be exchanged in each cycle, which would be technically infeasible, but rather communicated in larger batches. To realize the scheme in a single cycle (i.e., when batches are sent and received, the amount node x must send and receive is $2 \times |nb_G(x)|$ messages. The length of the messages is proportional to the interval between subsequent exchanges counted in cycles as the information contains sequences of strategies used and payoffs received during the cycles.

Next, we move to the game in mixed strategies. In this case, the strategy space (we abuse notation and use the same letters for the new game) $S_c = [0, 1]$, and the choice of the strategy is a choice of the probability for transmission. Writing $u_{\Delta,c}$ explicitly leads us to the formula:

$$u_{\Delta,c}(x) = \sum_{s\in \prod\limits_{\{c\}\cup nb(c)} S_p} \left(\prod_{j\in\{c\}\cup nb(c)} x_j(s_j)\right) u_i(s).$$

Here we already incorporated into the formula the dependency of $u_{\Delta,c}$ only on its neighbours in the graphical representation. To restrict the domain of the utility functions to a finite set instead of the interval $[0, 1]$, for station c we restrict it to the subset $S_c = \{p_0, p_1\} \subset [0, 1]$. Finally, the game over which we optimize welfare is $(C, \{S_c\}_{c\in C}, \{u_c\}_{\Delta,c})$.

Assuming that the treewidth of the graphical representation is small and we can choose a proper tree decomposition T rooted in t, we apply the arrangement we prepared in the previous sections to calculate the maximum effectiveness of the game in terms of welfare. What needs to be calculated for node x is

$$f_{x\to parent(x)}(s) = \max_{s'\in BD(x)\setminus FD(x)} \left(\sum_{v\in x\setminus parent(x)} u_{\Delta,v}(\pi_v(s', s)) + \sum_{z\in children(x)} f_{z\to x}(\pi_{FD(z)}(s', s))\right).$$

As functions $f_{z\to x}$ are supposed to be known (and communicated to $cn(x)$, cf. Section IV), what remains to be computed is the maximum. The number of messages exchanged between $cn(x)$ in each step of the algorithm is proportional to $|nb_T(x)|$. The length of the message from $cn(x)$ to $cn(parent(x)$ in the

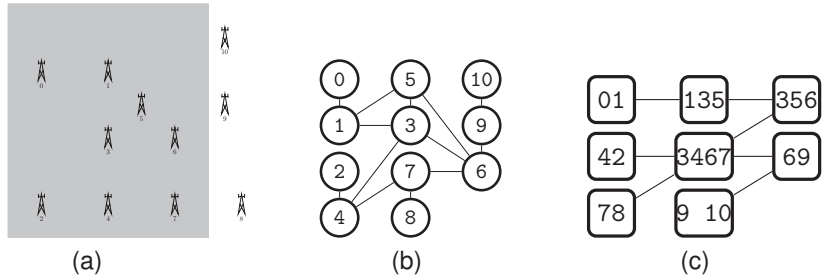


Fig. 2. Simulation topology: (a) BS arrangement, (b) corresponding graph, (c) corresponding tree. UEs are placed in the shaded area.

first stage of the algorithm is bounded by $|S|^{(|BD(x)\setminus FD(x)|}$, where $S = \max\_c \in C|S_c|$. This information, however, is passed between nodes once per single optimization run.

In this particular case, any computations of the maximum may be done by brute force. As a result, the network finds the best, from the global network's operation perspective, assignment of $\{p_c\}_{c\in C}$. Now, each node c in each moment independently performs a random decision if it should transmit (with probability p_c) or not (with probability $1 - p_c$). The whole process is repeated after a time reflecting the dynamic situation in the network.

The amount of brute force computation required depends on the treewidth, the structure of T . For networks with good structural properties , the computation may be feasible for even small computing units.

In the particular case discussed in this section, where we start from the interference game with two strategies for each player, then move to the mixed strategy game, and finally approximate the space of mixed strategies by discrete subsets, one can avoid brute force maximization over all possible combinations of strategies. The mixed strategy spaces, in this case, are one-dimensional and the payoff is monotonic with respect to each "mixed strategy variable" and allows maximization over each variable separately.

VI. SIMULATIONS

We evaluate the proposed algorithm by simulating the network topology of Fig. 2. We use a random and uniform distribution of 200 UEs within the grey-marked area. Each UE is assigned to the closest BS. BSs 7, 8 and 9, which are outside the grey rectangle, have all UEs assigned to them on the cell edge. For this arrangement, we measure the performance of the simulated network where BSs are busy 95% of the time. Then we run the same simulation, but with the optimisation algorithm enabled after 1000 steps. We restrict the choice of the BS time occupancy algorithm to two values: original 95% activity or decreased to 20%.

The results are presented in Fig. 3. The Y-axis is the average throughput over the whole history of the simulation, while the X-axis is the number of cycles since initializing the simulation. The average over history means that for cycle T we calculate $\frac{1}{T}\sum_{t=1}^{T} AvgTput(t)$, where $AvgTput(t)$ is the network throughput per UE in cycle t. The algorithm decides to decrease the activity of BSs 1, 3, 8, and 9 which results in an increase in overall network throughput compared to the situation when all BSs were busy. The increase is, however, in this setting relatively small (less than 5%). We conclude that the algorithm finds an optimal solution (subject to Theorem 2) under the proposed conditions.

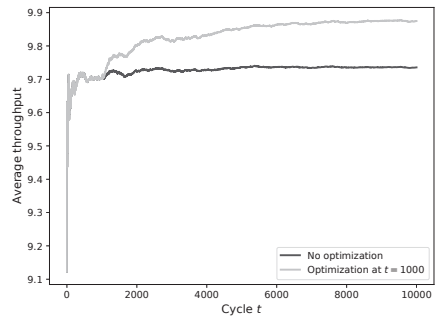


Fig. 3. Performance in the static scenario.

The previous example was static, i.e., the distribution of UE was constant and they were immobile. We obtain more interesting results for a changing environment. We add mobility to the initially randomly distributed UEs which are always assigned to the closest BS. Each UE moves on a piecewise linear trajectory with constant speed. We start from the random distribution in the same grey-marked area from Fig. 2a. Velocity changes only by changing direction which occurs when the device reaches a boundary of the rectangle, which is bigger than the initial area where we distributed UEs, and the change in direction follows a "billiard ball" rule.

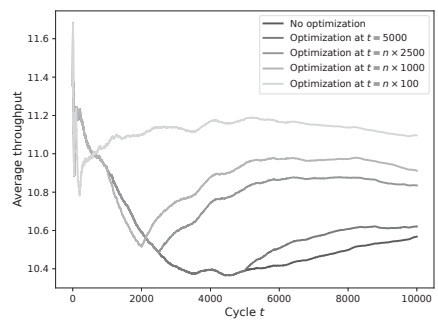


Fig. 4. Performance in the mobile scenario.

We check how the system performance changes when we apply the algorithm at various discrete moments: every 5000,

2500, 1000, and 100 cycles (Fig. 4). For "no optimization", the only change in the environment is due to UE mobility and we observe throughput to initially decrease and later increase. Meanwhile, for the optimisation cases, throughput immediately improves and, as expected, more frequent optimisation leads to better performance. An interesting phenomenon is, however, observed for the initial parts of the curves corresponding to 100 and 1000 where we see significant initial degradation. This effect seems to be contrary to the proven fact that the algorithm optimizes throughput. Two factors contribute to this behaviour. First, when the environment changes sufficiently fast, the optimisation performed at a given moment does not necessarily optimize the system for future cycles. The mobility model is such that the initial concentration of UE in the early stage of the simulation is replaced, due to the ergodicity of the movement, by uniform random distribution in the late phase. So, we expect that the fastest changing phase of the evolution of the environment is the initial one. Second, the BSs in this example learn about the dependency of the interference between them based on current activity. Therefore, initially, when the number of samples is small, the estimation of the influence of interference may be incorrect. As soon as the number of samples gives statistically sound estimations, the system starts to optimize the empirically determined function which correctly captures the influence of interference.

VII. Conclusions and Future Work

We have presented a dynamic programming method for the computation of the sum of the welfare in a graphical game assuming knowledge of the tree decomposition of the underlying graph. We also have shown how the method can optimize cellular networks modeled as graphical games where the arising conflict between players (base stations) comes from the interference between them. In the proposed algorithm, we have omitted the analysis of the influence of important parameters and factors on the quality of the solutions found by the methods. These parameters include the cut-off threshold for influence between the nodes leading to sparse graphical game representation and the size and structure of the space S_c that approximates the full space of mixed strategies $[0, 1]$ in Section V. Other important factors also not discussed here are changing demand for traffic from individual UEs, the impact of uncertainty about the utility function, and more sophisticated strategies for limiting transmission. A detailed analysis of these aspects is the subject of ongoing investigations.

We have also focused on the optimisation of a simple network operation mode, i.e., we attempt to optimize welfare over a subset of mixed strategies. More sophisticated schemes, where the non-trivial correlation between nodes is involved, can be also solved by this type of algorithm.

References

[1] M. S. Ali, E. Hossain, and D. I. Kim, "Coordinated multipoint transmission in downlink multi-cell noma systems: Models and spectral efficiency performance," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 24–31, 2018. DOI: 10.1109/MWC.2018.1700094

[2] U. Madhow, D. R. Brown, S. Dasgupta, and R. Mudumbai, "Distributed massive mimo: Algorithms, architectures and concept systems," in *2014 Information Theory and Applications Workshop (ITA)*, 2014. pp. 1–7. DOI: 10.1109/ITA.2014.6804225

[3] H. Garmani, D. Ait Omar, M. El Amrani, M. Baslam, and M. Jourhmane, "Joint beacon power and beacon rate control based on game theoretic approach in vehicular ad hoc networks," *Infocommunications Journal*, vol. 13, no. 1, pp. 58–67, 2021. DOI: 10.36244/ICJ.2021.1.7

[4] G. Hollósi, C. Lukovszki, M. Bancsics, and G. Magyar, "Traffic swarm behaviour: Machine learning and game theory in behaviour analysis," *Infocommunications Journal*, vol. 13, no. 4, pp. 19–27, 2021. DOI: 10.36244/ICJ.2021.4.3

[5] A. Lew and H. Mauch, Dynamic Programming: A Computational Tool (*Studies in Computational Intelligence*). Berlin, Heidelberg: Springer-Verlag, 2006. ISBN 3540370137

[6] M. J. Kearns, M. L. Littman, and S. P. Singh, "Graphical models for game theory," in *Proceedings of the 17th Conference in Uncertainty in Artificial Intelligence*, ser. UAI '01. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2001. ISBN 1558608001 pp. 253–260.

[7] H. L. Bodlaender, "Dynamic programming on graphs with bounded treewidth," in *Automata, Languages and Programming*, T. Lepistö and A. Salomaa, Eds. Springer, 1988. ISBN 978-3-540-39291-0 pp. 105–118.

[8] R. G. Downey and M. R. Fellows, *Fundamentals of Parameterized Complexity*, 1st ed. Springer Publishing Company, Incorporated, 2016. ISBN 1447171640

[9] N. Robertson and P. Seymour, "Graph minors. ii. algorithmic aspects of tree-width," *Journal of Algorithms*, vol. 7, no. 3, pp. 309–322, 1986. DOI: 10.1016/0196-6774(86)90023-4

[10] R. Diestel, *Graph Theory*, ser. Electronic library of mathematics. Springer, 2006. ISBN 9783540261834

[11] H. L. Bodlaender, "A linear time algorithm for finding tree-decompositions of small treewidth," in *ACM Symposium on Theory of Computing*, ser. STOC '93. New York, NY, USA: ACM, 1993. ISBN 0897915917 pp. 226–234. DOI: 10.1145/167088.167161.

[12] J. Matousek and R. Thomas, "Algorithms finding tree-decompositions of graphs," *J. Algorithms*, vol. 12, no. 1, pp. 1–22, 1991. DOI: 10.1016/0196-6774(91)90020-Y

[13] E. Amir, "Approximation algorithms for treewidth," *Algorithmica*, vol. 56, no. 4, pp. 448–479, 2010. DOI: 10.1007/s00453-008-9180-4

[14] H. L. Bodlaender, "Atourist guide through treewidth," *Acta Cybernetica*, vol. 11, pp. 1–23, 1993.

[15] B. Li, "Tree decompositions and routing problems. (décompositions arborescentes et problèmes de routage)," Ph.D. dissertation, University of Nice Sophia Antipolis, France, 2014.

Artur Popławski received his M.Sc. degree in mathematics from Jagiellonian University in 2000. He is currently working at Nokia Solutions and Networks as a specification engineer on 4G/5G radio resource management.

Szymon Szott received his Ph.D. degree in telecommunications from AGH University in 2011, where he works as an associate professor. His professional interests are related to wireless networks (channel access, QoS provisioning, security). He is the author of over 70 research papers.

Review of Some Recent European Cybersecurity Research and Innovation Projects

Mehmet Ufuk Çağlayan

Abstract—**This paper reviews research from several EU Projects that have addressed cybersecurity using techniques based on Machine Learning, including the security of Mobile Networks and the Internet of Things (IoT). These research projects have considered IoT Gateways and their design, security and performance, the security of digital health systems that are interconnected across Europe to provide health services to pople who travel through the EU, and related issues of the energy consumption and sustainability in Information and Communication Technologies (ICT) and their cybersecurity. The methods used in much of these research projects are based on Machine Learning both for attack detection and dynamic attack mitigation, as well as performance analysis and measurement techniques based on applied probability models.**

Index Terms—**Cybersecurity, Secure Mobile Networks, Machine Learning, IoT Gateways, Secure Health Informatics, Attack Detection, Cyber-Attack Mitigation, IoT Massive Access Problem, Adaptive Network Routing, ICT Sustainability.**

I. INTRODUCTION

Cybersecurity has substantially grown as a research area due to the massive growth of cyberattacks, the increasing interest in the IoT and cyber-physical systems [13], [14], and the European Union's recommendations with regard to security and privacy [15], which is our main area of research interest [10]–[12]. Even when they are unsuccessful, cyberattacks and the additional software needed to offer better security, create additional costs including increased energy consumption in computer systems and network and the resulting greenhouse gases (GHG) [16]–[19]. Hence energy consumption in mobile networks in the presence of attacks has also received attention [20], [21].

Thus several of the International Symposia on Computer and Information Sciences (ISCIS), that were held in Turkey, France, the USA, the UK, and Poland [1]–[8] have covered this important area over more than a decade. Most recently, the ISCIS CyberSecurity 2021 Symposium presented a summary of the work in several projects funded by the European Commision, just as the previous event [9],

The European Commission has funded an increasing number of research and innovation projects on cybersecurity that we will summarize in this paper, namely:

- NEMESYS on the cybersecurity of mobile telephone system [22]–[26],
- The project SDK4ED that mainly focused on energy savings [27], [28] but also considered issues of Cybersecurity and Reliability [29].
- KONFIDO [30]–[33] on the security of communications and data transfers for interconnected European national or regional health services,
- GHOST [34], [35] regarding the security of IoT systems for the home, and the design of secure IoT home gateways,
- SerIoT on the Cybersecurity of IoT systems [36], [37] with a range of applications in supply chains, smart cities, smart manufacturing, and other areas.
- IoTAC, which secures IoT networks by strengthening the protection of gateways and developing techniques such as Botnet detection, system wide vulnerability assessement [38], [39], and the optimization of the massive access to IoT gateways [40], [41].

Much of this research uses principles of probabilistic computing [42]–[46] due to the probabilistic and random nature of attacks themselves. Indeed cyberattacks occur at unpredictable instants, and themselves attempt to hide their own intentions by using random behaviours. It also discusses some results from the SDK4ED project concerning the energy efficient handling of system reliability issues through checkpointing [47], [48].

II. IMPROVING THE SECURITY OF MOBILE TELEPHONY

Cybersecurity of mobile telephony is a fundamental societal issue. The related problems are axacerbated by the fact that most mobile phones offer opportunistic connections [49], [50] to WIFI and other wireless networks which are not part of the mobile operators' core infrastructure. This creates vulnerabilities that need to be monitored on the mobile device itself, which is the motivation for the work in [51], [52].

On the other hand, the work described in [53], [54], concerns a form of Distributed Denial of Sevrice (DDoS) attacks on the signalling plane of the core mobile network which are caused by malicious software which is deposited in the mobile devices. Related work conducted witin the EU NEMESYS project [55]–[57] using queueing theoretic methods [58], [59].

Early work on DDoS Attacks [60] had proposed self-aware networks and the Cognitive Packet Network (CPN) [61]–[64] to detect and couter-attack against DDoS, by identifying sources of attacks by following upstream the attacking traffic, using CPN's ACK packets to "drop" attacking traffic at upstream routers [60], [65]. It was also applied to mitigate worm attacks and to deviate user traffic so as to avoid insecure nodes [66]–[68]. Related issues include the management of keys [69], [70], and the study and mitigation of signalling storms in mobile telephony [52], [53].

The author is with the Department of Computer Engineering, Yaşar University, Bornova, Izmir, Turkey. (E-mail: ufuk.caglayan@yasar.edu.tr) ORCID: 0000-0001-9688-2201

DOI: 10.36244/ICJ.2022.4.10

III. SECURITY OF THE TRANS-EUROPEAN HEALTH INFORMATICS NETWORK

Large numbers of travellers from one European country to another sometimes need to access health services in the country they are visiting. These health services are typically based on a national model, or a regional model inside a given country such as Italy. Thus the KONFIDO project addressed the important issue of providing a secure support to European health systems.

The corresponding informatics systems, with their patient data bases are also nationally or regionally based, so that when the medical practitioner in one country or region is required to diagnose and treat a visitor from some other region or country, she/he will will need to access the patient's data remotely. KONFIDO's aim is to improve the cybersecurity of such systems, while improving also their inter-operability across countries and regions in Europe.

Thus the work in [71] presents an overall view and challenges of the project, while in [72] the authors present an analysis of the corresponding user requirements. Such systems have obvious performance optimization issues which are discussed in [73]. Keeping track of the transactions in such a system through blockchains is suggested in [74].

IV. CONTRIBUTIONS TO THE SECURITY OF THE IOT

To exploit the value that the IoT generated provides requires the protection of privacy and in many cases data will have to be rendered strongly anonymous. It will also require specific security not just for the IoT devices and networks, but also for the IoT data repositories in the Cloud and their access networks. These aspects are complicated by the simplicity of many IoT devices which cannot be integrated in complex distributed communication infrastructures that would require communications to be synchronized or schedules [75], [76].

The Internet of Things (IoT) and its related software systems [77] are rapidly proliferating as their applications expand, with reports [78] indicating that 52% of IoT devices will be low-cost low-maintenance devices that can only perform one task at a time, and unable to handle the types of complex real-time algorithms that are neeed to detect, block and mitigate cyberattacks. Improving the security of cyberphysical systems via systematic approaches have been suggested [79], [80], but industry confirms that it is difficult to load simple IoT devices with foolproof security capabilities [81]. Thus such devices and their wired and wireless interconnections are vulnerable to attacks [82]–[84] such as Denial of Service (DoS) which represent some 20% of IoT attacks [85], where malicious devices generate usless requests that impede normal operation and saturate limited resources, and may also add malware [86], [87].

A single Distributed DoS (DDoS) attack can compromise thousands of devices [88] through Botnets where victims themselves join the attack by being turned into "bots" [89]. An example is the 2016 massive "Mirai" attack that brought down the Domain Name System (DNS) Dyn [90], and blocked access to Netflix, Reddit, Spotify, and Twitter [91], [92] , accessing the equipment of major cybersecurity providers [93], and also congesting IoT and IP networks [94]. Thus as soon as a Botnet attempts an attack, it is crucial to detect it, if possible block it, and especially avoid its propagation and proliferation.

Thus much work has been devoted to what we may call "the first stage" which is essentially comprised of attack detection. The characteristics of Botnet attacks have been analyzed [95], and in [90] capabilities of Mirai has been examined, while in [96] its source code has also been studied, others have suggested that blockchains can be used to protect [97] and much work has involved machine learning models to detect attacks such as KNN, Support Vector Machines (SVM), Decision Trees (DT) and MLP [98], Classification and Regression Trees (CART) [99]; DT, Gradient Boosting and Random Forests [100], Logistic Regression [101] and their comparative performance Tuan et al. [102] . Botnet attack detection via neural networks was also considered [103], [104] including with the and Naive Bayesian Models [105], the LSTM [106], and Convolutional Networks (CNN) [107], also combined with LSTM [108]. In [109] Botnet attacks were detected via a sparse representation framework with a large number of inputs using only normal non-attack traffic as in [110] that uses auto-associative learning with a variant of the Random Neural Network [111] adapted for deep learning [112] that was initially designed for image recognition [113]. The RNN was already used successfully to detect SYN attacks [35] and extended to a wide variety of attacks in [114], based on the function approximation capabilities of the RNN [115].

Thus in [34] an overview of the principles and achievements of the GHOST project are presented, which started in May of 2017 and which ran for three years. The project addressed safe-guarding home IoT environments through appropriate software that can be installed on home IoT gateways, and it also creates a prototype and test-bed using specific equipment from the TELEVES company.

Related to this project, machine learning methods were developed for the detection of network attacks on IoT gateways [116] based on Deep Learning [117]–[119] with the Random Neural Network [120]–[123] and its extensions [124].

A. Attacks on Battery Power

Related to the GHOST project, other recent work discusses the effect and mitigation of attacks on the batteries which supply the power of many light-weight IoT network nodes [125], [126].

To this effect much research has been devoted to creating viable mathematical models of sensors that incorporate both the data collection, processing and transmission role of sensors, and their consumption of energy from batteries [127]. Computational techniques for large scale system analysis, including both communication or computational steps and energy consumption have also been developed [128].

Important results have been obtained in this respect in our ability to analyze and predict the life-time of sensors with rgard to their available battery power under different assumptions regarding renewable bu unpredictable random source of energy such as photovoltaic, the normal energy consumption of the device, and the impact of attacks that tend

to deplete energy through spurious and undesired processing and transmission on the part of the sensor [129]–[134].

V. THE SERIOT PROJECT

The SerIoT project was started in 2018 [135] and produced important results [136]–[138], [138]–[140]. These have been summarized in a brief article recently published by the EU CORDIS web site [141] under the title "Getting more *intelligent* about Internet security," which we reproduce below.

"Cognitive packets of internet information could revolutionise cybersecurity. Rerouting themselves dynamically and with great agility, they can avoid security threats or breaches in the network.

Most of us are highly aware of the need to protect our personal data on the internet ? our email accounts, bank accounts, health information and so much more. As we rapidly move to the Internet of things (IoT), the "things" requiring protection range from home ovens to sophisticated industrial tools, self-driving cars and remotely operated surgical equipment. Underlying these and more, including military communications and defence, is the electric power grid. Current internet protection is primarily static, detecting and blocking portions of an IoT system under attack but not rerouting information intelligently and avoiding glitches or worse. The EU-funded SerIoT project has delivered an unprecedented adaptive and intelligent solution by the same name. It will ensure IoT networks safely continue business as usual regardless of network conditions.

IoT networks connect sensors and actuators related to a physical system like a factory, vehicle or smart grid with software systems that control the system?s functions. Conventional networks use hardware like routers and switches to direct network traffic. SerIoT relies on cognitive intelligent control based on random neural networks and implements the controls through software-defined networking (SDN). SDN uses software-based technologies to control routers and direct network traffic in the form of internet packets, or blocks of information. This also enables flexible and dynamic configuration of "virtual networks" from physical ones depending on needs at the time. SerIoT added to this flexibility by integrating AI into the packets themselves, creating a patented cognitive packet network (CPN) ... SerIoT introduced self-awareness into SDN through a CPN in which the packets route themselves adaptively via SDN controllers with integrated AI. Attack and security detectors support rerouting of traffic to avoid items or areas that may be insecure due to threats or attacks. Each cognitive packet is thus self-aware, adaptive and intelligent, reacting not only to security issues but also network congestion or changes in energy consumption to improve the IoT system's or network's performance. The background and description of the practical working system have been published."

Wesummarize that SerIoT not only allows the IoT system to operate normally while under attack, but even at such times it saves energy and optimises performance. It can be installed in existing SDN technology, allowing the approach to be ported to many unforeseen applications. SerIoT moves the field of cybersecurity from the static mentality to an active, highly mobile, agile and adaptive system that not only defends against cyberattacks but moves critical traffic away from attack paths ... The (project's) large-scale pilots, including with project partner Deutsche Telecom, targeted the smart grid, which uses the IoT extensively, exploiting smart meters to optimise electricity production and distribution. Smart vehicles and Industry 4.0 robots were also tested. SerIoT is available for demonstration and beta testing by commercial partners and is being exploited in the ongoing Horizon 2020 IOTAC project. SerIoT will ensure that global IoT traffic agilely detours around malicious and natural obstacles large and small, for business as usual."

A. SerIoT Technical Scope

Its technical scope included SerCPN [137], [142], a specific secure network [143] for managing geographically distributed IoT devices and services using the principles of the Cognitive Packet Network (CPN) tested in several experiments [144]–[148]. CPN uses "Smart" Packets (SPs) to search for paths and measure QoS while the network is in operation, via Reinforcement Learning using a Random Neural Network, and based on the QoS Goal pursued by the end user. When an SP reaches its destination, its measurements are returned by an ACK packet to the intermediate nodes of the path that was identified by the SP, and to the end user, providing the QoS offered by the path that the SP travelled. Source nodes receive ACKs and take the decision to switch to the path that offers the best security or quality of service [149]–[152].

Extensions with a genetic algorithm [153] was also also tested [154]. An interesting development in SerIoT combines energy aware routing [155], [156] and security, and admission control [157].

Adaptive techniques for wireless IoT traffic to achieve better QoS are also found in [158]–[161] and summarized in [162]–[164], [164]–[168], while the RNN with adaptive approaches was shown to offer opportunities for massive video compression [169], [170], as well as for managing Cloud servers [171]. Such adaptive techniques that support the interaction between security metrics, performance and energy consumption were also discussed in a recent paper [172].

B. Energy Aspects

The energy aspects of system performance are also of great interests, and go beyond the questions regarding the energy supplied by batteries. Software systems themselves have to be designed with energy optimization being kept in mind [173].

Similarly it is important to be able to share energy flows between subsystems so that their workload is provisioned in a manner that matches the load on each subsystem [174], [175].

C. System Dynamics

Whenever adaptive techniques are used, the system under consideration is likely to change state in order to reach a better level of system operation. For instance, paths in the system can be changed in response to cyberattacks [176] with impact on security, Quality of Service a well as dependability.

When this occurs the transient behaviour of the system must be considered, which was addressed in several recent papers [177]–[180].

VI. THE IOTAC PROJECT

The subsequent IoTAC project has lead to novel techniques for learning from user traffic and then testing for an attack as described in [181]. In IoTAC, there is also substantial work on dealing with severe performance issues due to the large flows of IoT packets towards gateways from thousands of IoT devices, so that the resulting Massive Access Problem (MAP) has to be mitigated with novel traffic shaping techniques [40], [41], [182], [183].

This project has created several novel attack detection techniques for attack detection of Botnets [184], [185]. The most original contribution in this respect has been to show that a large class of stochastic networks, of which the Random Neural Network is an instance, can in fact be used to detect cyberattacks [186].

Due to the role of transients due to the manner in which SDN routers operate, the SerIoT project also examined novel techniques to predict the time it takes to effect significant state changes such as re-routing of traffic in the network, using novel diffusion based techniques

VII. CONCLUSIONS

Frequent and effective cyberattacks on private and public networks, and on information technology infrustructures constantly motivates research on Cybersecurity. Starting with the encryption of massages and data, it has evolved to develop more secure systems through passwords, authentication schemes, firewalls and cryptographic keys. But it has now substantially been revolutionized as a means to detect and mitigate cyberattacks. Software's own specific vulnerabilities [187] have also become critical [176], [188]–[192]. Indeed, static means of Cybersecurity assurance are largely ineffective unless they incorportd real-time methods that can detect and rapidly react to attacks and malicious actions against a system.

Cybersecurity research is now encompassing a far broader approach, and the support of substantial European Union research programs has allowed the field to attain a higher level of maturity that includes performance, energy consumption and higher security levels through self-adaptation and system reconfiguration as demonstrated in the research projects that we have surveyed in this paper.

REFERENCES

[1] E. Gelenbe, *24th International Symposium on Computer and Information Sciences, ISCIS 2009*, 14-16 September 2009, North Cyprus. IEEE, 2009.

[2] E. Gelenbe, R. Lent, G. Sakellari, A. Sacan, I. H. Toroslu, and A. Yazici, *Computer and Information Sciences - Proceedings of the 25th International Symposium on Computer and Information Sciences,* London, UK, September 22-24, 2010, ser. Lecture Notes in Electrical Engineering. Springer, 2010, vol. 62. [Online]. Available: DOI: 10.1007/978-90-481-9794-1

[3] E. Gelenbe and R. Lent, *Eds., Computer and Information Sciences III - 27th International Symposium on Computer and Information Sciences*, Paris, France, October 3-4, 2012. Springer, 2013.

[4] ——, *Information Sciences and Systems 2013 - Proceedings of the 28th International Symposium on Computer and Information Sciences, ISCIS* 2013, Paris, France, October 28-29, 2013, ser. Lecture Notes in Electrical Engineering, vol. 264. Springer, 2013.

[5] O. H. Abdelrahman, E. Gelenbe, G. Görbil, and R. Lent, Eds., *Information Sciences and Systems 2015 - 30th International Symposium on Computer and Information Sciences, ISCIS* 2015, London, UK, 21- 24 September 2015, ser. Lecture Notes in Electrical Engineering, vol. 363. Springer, 2016.

[6] T. Czachórski, E. Gelenbe, and R. Lent, Eds., *Information Sciences and Systems 2014 - Proceedings of the 29th International Symposium on Computer and Information Sciences, ISCIS* 2014, Krakow, Poland, October 27-28, 2014. Springer, 2014.

[7] T. Czachórski, E. Gelenbe, K. Grochla, and R. Lent, Eds., *Computer and Information Sciences - 31st International Symposium, ISCIS* 2016, Kraków, Poland, October 27-28, 2016, *Proceedings*, ser. Communications in Computer and Information Science, vol. 659, 2016.

[8] T. Czachórski, E. Gelenbe, K. Grochla, and R. Lent, "*Computer and Information Sciences: 32nd International Symposium, ISCIS* 2018, Held at the *24th IFIP World Computer Congress, WCC* 2018, Poznan, Poland, September 20-21, 2018, Proceedings," 2018.

[9] E. Gelenbe, P. Campegiani, T. Czachórski, S. K. Katsikas, I. Komnios, L. Romano, and D. Tzovaras, "*Security in computer and information sciences: First International ISCIS Security Workshop* 2018, EURO-CYBERSEC 2018, London, UK, February 26-27, 2018, revised selected papers," 2018.

[10] A. Levi, M. U. Çaglayan, and Ç. K. Koç, "Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure," *ACM Trans. Inf. Syst. Secur.*, vol. 7, no. 1, pp. 21–59, 2004. [Online]. Available: http://doi.acm.org/10.1145/984334.984336

[11] M. Akgün and M. U. Çaglayan, "Towards scalable identification in RFID systems," *Wireless Personal Communications*, vol. 86, no. 2, pp. 403–421, 2016. [Online]. Available: DOI: 10.1007/s11277-015-2936-7

[12] O. Ermis, S. Bahtiyar, E. Anarim, and M. U. Çaglayan, "A key agreement protocol with partial backward confidentiality," *Computer Networks*, vol. 129, pp. 159–177, 2017. [Online]. Available: DOI: 10.1016/j.comnet.2017.09.008

[13] E. Gelenbe and F.-J. Wu, "Large scale simulation for human evacuation and rescue," *Computers & Mathematics with Applications*, vol. 64, no. 12, pp. 3869–3880, 2012.

[14] ——, "Future research on cyber-physical emergency management systems," *Future Internet*, vol. 5, no. 3, pp. 336–354, 2013.

[15] European Commission, "Cybersecurity Policies." [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

[16] H. Jiang, F. Liu, R. K. Thulasiram, and E. Gelenbe, "Guest editorial: Special issue on green pervasive and ubiquitous systems," *IEEE Systems Journal*, vol. 11, no. 2, pp. 806–812, 2017. [Online]. Available: DOI: 10.1109/JSYST.2017.2673218

[17] E. Gelenbe, "Search in unknown random environments," *Physical Review E*, vol. 82, p. 061112, 2010.

[18] O. H. Abdelrahman and E. Gelenbe, "Time and energy in team-based search," *Physical Review E*, vol. 87, no. 3, p. 032125, March 2013.

[19] F. Francois, O. H. Abdelrahman, and E. Gelenbe, "Towards assessment of energy consumption and latency of lte ues during signaling storms," in *Information Sciences and Systems* 2015. Springer, Cham, 2016, pp. 45–55.

[20] O. H. Abdelrahman and E. Gelenbe, "A diffusion model for energy harvesting sensor nodes," in *2016 IEEE 24th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS)*. IEEE, 2016, pp. 154–158.

[21] E. Gelenbe and O. H. Abdelrahman, "An energy packet network model for mobile networks with energy harvesting," *Nonlinear Theory and Its Applications, IEICE*, 2018, vol. 9, no. 3, pp. 1–15, 2018. DOI: 10.1587/nolta.9.1

[22] O. H. Abdelrahman, E. Gelenbe, G. Görbil, and B. Oklander, "Mobile network anomaly detection and mitigation: The nemesys approach," in *Information Sciences and Systems 2013*. Springer International Publishing, 2013, pp. 429–438.

[23] E. Gelenbe, G. Görbil, D. Tzovaras, S. Liebergeld, D. Garcia, M. Baltatu, and G. Lyberopoulos, "Nemesys: Enhanced network security for seamless service provisioning in the smart mobile ecosystem," in *Information Sciences and Systems 2013*. Springer International Publishing, 2013, pp. 369–378.

[24] E. Gelenbe, G. Gorbil, D. Tzovaras, S. Liebergeld, D. Garcia, M. Baltatu, and G. Lyberopoulos, "Security for smart mobile networks: The nemesys approach," in *Privacy and Security in Mobile Systems (PRISMS), 2013 International Conference on*. IEEE, 2013, pp. 1–8.

[25] G. Gorbil, O. H. Abdelrahman, M. Pavloski, and E. Gelenbe, "Storms in mobile networks," arXiv preprint arXiv:1411.1280, 2014.

[26] M. Pavloski and E. Gelenbe, "Mitigating for signalling attacks in umts networks," in *Information Sciences and Systems 2014*. Springer International Publishing, 2014, pp. 159–165.

[27] B. Pernici, M. Aiello, J. Vom Brocke, B. Donnellan, E. Gelenbe, and M. Kretsis, "What is can do for environmental sustainability: a report from caise?11 panel on green and sustainable is," *Communications of the Association for Information Systems*, vol. 30, no. 1, p. 18, 2012.

[28] E. Gelenbe and Y. Caseau, "The impact of information technology on energy consumption and carbon emissions," *ubiquity*, vol. 2015, no. June, pp. 1–15, 2015.

[29] M. G. Siavvas and E. Gelenbe, "Optimum interval for application-level checkpoints," in *CSCloud/EdgeCom*. IEEE, 2019, pp. 145–150.

[30] S. Diamantopoulos, D. Karamitros, L. Romano, L. Coppolino, V. Koutkias, K. Votis, O. Stan, P. Campegiani, D. M. Martinez, M. Nalin et al., "Secure cross-border exchange of health related data: The konfido approach," in *International Conference on Internet and Distributed Computing Systems*. Springer, Cham, 2019, pp. 318–327.

[31] S. Diamantopoulos, M. Nalin, I. Baroni, F. Clemente, G. Faiella, C. Mesaritakis, E. Grivas, J. Rasmussen, J. Petersen, I. Cano, E. Puig- domènech, D. Karamitros, E. Gelenbe, J. Dumortier, M. V. Voronkov, L. Romano, L. Coppolino, V. Koutkias, K. Votis, O. Stan, P. Campegiani, and D. M. Martinez, "Secure cross-border exchange of health related data: The KONFIDO approach," in *EDCC*. IEEE, 2019, pp. 73–74.

[32] M. Nalin, I. Baroni, G. Faiella, M. Romano, F. Matrisciano, E. Gelenbe, D. M. Martinez, J. Dumortier, P. Natsiavas, K. Votis et al., "The european cross-border health data exchange roadmap: Case study in the italian setting," *Journal of biomedical informatics*, vol. 94, p. 103183, 2019.

[33] P. Natsiavas, G. Mazzeo, G. Faiella, P. Campegiani, J. Dumortier, O. Stan, M. Nalin, D. Mari Martinez, A. Theodouli, K. Moschou et al., "Developing an infrastructure for secure patient summary exchange in the eu context: Lessons learned from the konfido project," *Health Informatics Journal*, vol. 27, no. 2, p. 14604582211021459, 2021.

[34] A. Collen, N. A. Nijdam, J. Augusto-Gonzalez, S. K. Katsikas, K. M. Giannoutakis, G. Spathoulas, E. Gelenbe, K. Votis, D. Tzovaras, N. Ghavami, M. Volkamer, P. Haller, A. Sánchez, and M. Dimas, "Ghost - safe-guarding home iot environments with personalised real-time risk control," in *Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London*, E. Gelenbe, P. Campegiani, T. Czachorski, S. Katsikas, I. Komnios, L. Romano, and D. Tzovaras, Eds. Lecture Notes CCIS No. 821, Springer Verlag, 2018.

[35] O. Brun, Y. Yin, and E. Gelenbe, "Deep learning with dense random neural network for detecting attacks against iot-connected home environments," *Procedia Computer Science*, vol. 134, pp. 458–463, 2018.

[36] A. Frötscher, B. Monschiebl, A. Drosou, E. Gelenbe, M. J. Reed, and M. Al-Naday, "Improve cybersecurity of c-its road side infrastructure installations: the seriot-secure and safe iot approach," in *2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE)*. IEEE, 2019, pp. 1–5.

[37] G. Baldini, P. Fröhlich, E. Gelenbe, Hernandez-Ramos, J. Luis, M. Nowak, S. Nowak, S. Papadopoulos, A. Drosou, and D. Tzovaras, "*Iot network risk assessment and mitigation: The seriot approach*," 2020.

[38] M. Nakip and E. Gelenbe, "Randomization of data generation times improves performance of predictive iot networks," in *IEEE World Forum on Internet of Things (WF IoT)*, July 14-21, 2021, p. 5161. https://wfiot2021.iot.ieee.org, 2021

[39] ——, "Mirai botnet attack detection with auto-associative dense ran- dom neural networks," in *2021 IEEE Global Communications Conference*, vol. 2021. IEEE Communications Society, 2021, pp. 1–6.

[40] E. Gelenbe, M. Nakip, D. Marek, and T. Czachorski, "Diffusion analysis improves scalability of iot networks to mitigate the massive access problem," in *IEEE MASCOTS 2021: 29th International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems*., 2021, pp. 1–6. https://zenodo.org/record/5501822#.YT3bri8itmA

[41] E. Gelenbe and K. Sigman, "Iot traffic shaping and the mas- sive access problem," in *ICC 2022, IEEE International Conference on Communications*, 16–20 May 2022, Seoul, South Korea, no., 2022, pp. 1–6., https://zenodo.org/record/5918301#.YgaCP

[42] E. Gelenbe, "On languages defined by linear probabilistic automata," *Information and Control*, vol. 16, no. 5, pp. 487–501, 1970.

[43] ——, "On the loop-free decomposition of stochastic finite-state systems," *Information and Control*, vol. 17, no. 5, pp. 474–484, 1970.

[44] S. E. Gelenbe, "A realizable model for stochastic sequential machines," *IEEE Trans. Computers*, vol. 20, no. 2, pp. 199–204, 1971.

[45] S. E. Gelenbe and N. Rossi, "Uniform modular realizations and linear machines," *IEEE Trans. Computers*, vol. 20, no. 12, pp. 1616–1617, 1971.

[46] E. Gelenbe, "A unified approach to the evaluation of a class of replacement algorithms," *IEEE Trans. Computers*, vol. 22, no. 6, pp. 611–618, 1973.

[47] M. Siavvas and E. Gelenbe, "Optimum checkpoints for programs with loops," *Simulation Modelling Practice and Theory*, vol. 97, p. 101951, 2019.

[48] M. Siavvas, D. Tsoukalas, M. Jankovic D. Kehagias, A. Chatzigeorgiou, D. Tzovaras, N. Aničic, and E. Gelenbe, "An empirical evaluation of the relationship between technical debt and software security," in *ICIST 2019 Proceedings*, vol. 1, 2019, pp. 199–203.

[49] G. Gorbil and E. Gelenbe, "Opportunistic communications for emergency support systems," *Procedia Computer Science*, vol. 5, pp. 39–47, 2011.

[50] ——, "Resilience and security of opportunistic communications for emergency evacuation," in *Proceedings of the 7th ACM workshop on Performance monitoring and measurement of heterogeneous wireless and wired networks*, 2012, pp. 115–124.

[51] G. Gorbil, O. H. Abdelrahman, and E. Gelenbe, "Modeling and analysis of rrc-based signaling storms in 3g networks," *IEEE Transactions on Emerging Topics in Computing, Special Issue on Emerging Topics in Cyber Security*, p. 1-14, January 2015.

[52] F. Francois, O. H. Abdelrahman, and E. Gelenbe, "Feasibility of signaling storms in 3g/umts operational networks," in *International Internet of Things Summit*. Springer, Cham, 2015, pp. 187–198.

[53] M. Pavloski, G. Görbil, and E. Gelenbe, "Bandwidth usage?based detection of signaling attacks," in *Information Sciences and Systems 2015*. Springer, Cham, 2016, pp. 105–114.

[54] O. H. Abdelrahman and E. Gelenbe, "A data plane approach for detecting control plane anomalies in mobile networks," in *International Internet of Things Summit*. Springer, Cham, 2015, pp. 210–221.

[55] E. Gelenbe, O. H. Abdelrahman, and G. Gorbil, "Detection and mitigation of signaling storms in mobile networks," in *2016 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2016, pp. 1–5.

[56] E. Gelenbe and O. H. Abdelrahman, "Countering mobile signaling storms with counters," in *International Internet of Things Summit. Springer, Cham*, 2015, pp. 199–209.

[57] G. Gorbil, O. H. Abdelrahman, M. Pavloski, and E. Gelenbe, "Modeling and analysis of rrc-based signalling storms in 3g networks," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 1, pp. 113– 127, 2016.

[58] E. Gelenbe, "G-networks with instantaneous customer movement," *Journal of Applied Probability*, vol. 30, no. 3, pp. 742–748, 1993.

[59] J.-M. Fourneau, E. Gelenbe, and R. Suros, "G-networks with multiple classes of negative and positive customers," *Theoretical computer science*, vol. 155, no. 1, pp. 141–156, 1996.

[60] E. Gelenbe and G. Loukas, "A self-aware approach to denial of service defence," *Computer Networks*, vol. 51, no. 5, pp. 1299–1314, 2007.

[61] E. Gelenbe, Z. Xu, and E. Seref, "Cognitive packet networks," in *Conference Tools with Artificial Intelligence, 1999. Proceedings. 11th IEEE International Conference on, Publisher IEEE*, 1999, pp. 47–54.

[62] S. E. Gelenbe, "Cognitive packet network," Oct. 12 2004, uS Patent 6,804,201.

[63] E. Gelenbe, "Steps toward self-aware networks," *Communications of the ACM*, vol. 52, no. 7, pp. 66–75, 2009.

[64] E. Gelenbe and Y. Cao, "Autonomous search for mines," *European Journal of Operational Research*, vol. 108, no. 2, pp. 319–333, 1998.

[65] G. Oke, G. Loukas, and E. Gelenbe, "Detecting denial of service attacks with bayesian classifiers and the random neural network," in *Fuzzy Systems Conference*, 2007. FUZZ-IEEE 2007. IEEE International. IEEE, 2007, pp. 1–6.

[66] E. Gelenbe, "Dealing with software viruses: a biological paradigm," *Information security technical report*, vol. 12, no. 4, pp. 242–250, 2007.

[67] G. Sakellari, L. Hey, and E. Gelenbe, "Adaptability and failure resilience of the cognitive packet network," *DemoSession of the 27th IEEE Conference on Computer Communications (INFOCOM2008)*, Phoenix, Arizona, USA, 2008.

[68] G. Sakellari and E. Gelenbe, "Adaptive resilience of the cognitive packet network in the presence of network worms," *Proceedings of the NATO Symposium on C3I for Crisis, Emergency and Consequence Management*, pp. 11–12, 2009.

[69] C.-M. Yu, G.-K. Ni, Y. Chen, E. Gelenbe, and S.-Y. Kuo, "Top-k query result completeness verification in sensor networks," in *Communications Workshops (ICC)*, 2013 IEEE International Conference on. IEEE, 2013, pp. 1026–1030.

[70] C. Yu, G. Ni, I. Chen, E. Gelenbe, and S. Kuo, "Top- k query result completeness verification in tiered sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 1, pp. 109–124, 2014. [Online]. Available: http://dx.doi.org/10.1109/TIFS.2013.2291326

[71] M. Staffa, L. Sgaglione, G. Mazzeo, L. Coppolino, S. D'Antonio, L. Romano, E. Gelenbe, O. Stan, S. Carpov, E. Grivas et al., "An openncp-based solution for secure ehealth data exchange," *Journal of Network and Computer Applications*, vol. 116, pp. 65–85, 2018.

[72] P. Natsiavas, J. Rasmussen, M. Voss-Knude, K. Votis, L. Coppolino, P. Campegiani, I. Cano, D. Marí, G. Faiella, F. Clemente et al., "Comprehensive user requirements engineering methodology for secure and interoperable health data exchange," *BMC medical informatics and decision making*, vol. 18, no. 1, pp. 1–16, 2018.

[73] E. Gelenbe and M. Pavloski, "Performance of a security control scheme for a health data exchange system," in *IEEE International Black Sea Conference on Communications and Networking* 26-29 May 2020 // Virtual Conference, 2020.

[74] L. Castaldo and V. Cinque, "Blockchain-based logging for the cross-border exchange of ehealth data in europe," in Euro-CYBERSEC, ser. *Communications in Computer and Information Science*, vol. 821. Springer, 2018, pp. 46–56.

[75] E. Gelenbe and K. Sevcik, "Analysis of update synchronization for multiple copy data bases," *IEEE Transactions on Computers*, no. 10, pp. 737–747, 1979.

[76] A. Chesnais, E. Gelenbe, and I. Mitrani, "On the modeling of parallel access to shared data," *Communications of the ACM*, vol. 26, no. 3, pp. 196–202, 1983.

[77] R. Buyya, S. N. Srirama, G. Casale, R. Calheiros, Y. Simmhan, B. Varghese, E. Gelenbe, B. Javadi, L. M. Vaquero, M. A. Netto et al., "A manifesto for future generation cloud computing: Research directions for the next decade," *ACM Computing Surveys (CSUR)*, vol. 51, no. 5, pp. 1–38, 2019.

[78] Cisco, "Cisco annual internet report (2018–2023)." [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[79] G. Matta, S. Chlup, A. M. Shaaban, C. Schmittner, A. Pinzenöhler, E. Szalai, and M. Tauber, "Risk management and standard compliance for cyber-physical systems of systems," *Infocommunications Journal*, vol. 13, no. 2, pp. 32–39, June 2021. [Online]. Available: DOI: 10.36244/ICJ.2021.2.5

[80] S. Maksuti, M. Zsilak, M. Tauber, and J. Delsing, "Security and autonomic management in system of systems," *Infocommunications Journal*, vol. 13, no. 3, pp. 66–75, September 2021. [Online]. Available: DOI: 10.36244/ICJ.2021.3.7

[81] "Hp study reveals 70 percent of Internet of Things devices vulnerable to attack," Accessed on 25.01.2022. [Online]. Available: https://www.securityweek.com/70-iot-devices-vulnerable-cyberattacks-hp

[82] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483–2495, 2018.

[83] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, 2017.

[84] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, 2017.

[85] S. Benzarti, B. Triki, and O. Korbaa, "A survey on attacks in Internet of Things based networks," in *2017 International conference on engineering & MIS (ICEMIS)*. IEEE, 2017, pp. 1–7.

[86] CISA, "Understanding Denial-of-Service attacks." [Online]. Available: https://us-cert.cisa.gov/ncas/tips/ST04-015

[87] G. Carl, G. Kesidis, R. Brooks, and S. Rai, "Denial-of-Service attack-detection techniques," *IEEE Internet Computing*, vol. 10, no. 1, pp. 82–89, 2006.

[88] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer networks*, vol. 44, no. 5, pp. 643–666, 2004.

[89] D. Goodin, "100,000-strong Botnet built on router 0-day could strike at any time," *Ars Technica*, December 2017. [Online]. Available: https://arstechnica.com/information-technology/2017/12/100000-strong-botnet-built-on-router-0-day-could-strike-at-any-time/

[90] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim, and J. N. Kim, "An in-depth analysis of the mirai botnet," in *2017 International Conference on Software Security and Assurance (ICSSA)*. IEEE, 2017, pp. 6–12.

[91] J. Biggs, "Hackers release source code for a powerful DDoS app called Mirai," *TechCrunch*, October 2018. [Online]. Available: https://techcrunch.com/2016/10/10/hackers-release-source-code-for-a-powerful-ddos-app-called-mirai/

[92] R. Hackett, "Why a hacker dumped code behind colossal website-trampling botnet," *Fortune*, October 2016. [Online]. Available: https://finance.yahoo.com/news/why-hacker-dumped-code-behind-145847907.html

[93] N. Statt, "How an army of vulnerable gadgets took down the web today," *The Verge*, October 2016. [Online]. Available: https://www.theverge.com/2016/10/21/13362354/dyn-dns-ddos-attack-cause-outage-status-explained

[94] B. Tushir, H. Sehgal, R. Nair, B. Dezfouli, and Y. Liu, "The impact of dos attacks onresource-constrained iot devices: A study on the mirai attack," arXiv preprint *arXiv:2104.09041*, 2021.

[95] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the Mirai Botnet," in *Proceedings of the 26th USENIX Security Symposium*, 2017. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

[96] H. Sinanović and S. Mrdovic, "Analysis of mirai malicious software," in *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE, 2017, pp. 1–5.

[97] Z. Ahmed, S. M. Danish, H. K. Qureshi, and M. Lestas, "Protecting IoTs from Mirai Botnet attacks using blockchains," in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1–6.

[98] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," in *2018 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2018, pp. 29–35.

[99] C. S. Htwe, Y. M. Thant, and M. M. S. Thwin, "Botnets attack detection using machine learning approach for iot environment," in *Journal of Physics: Conference Series*, vol. 1646, no. 1. IOP Publishing, 2020, p. 012101.

[100] M. Banerjee and S. Samantaray, "Network traffic analysis basediot botnet detection using honeynet data applying classification techniques," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 17, no. 8, 2019.

[101] A. O. Prokofiev, Y. S. Smirnova, and V. A. Surov, "A method to detect internet of things botnets," in *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE, 2018, pp. 105–108.

[102] T. A. Tuan, H. V. Long, R. Kumar, I. Priyadarshini, N. T .K. Sonetal., "Performance evaluation of botnet ddos attack detection using machine learning," *Evolutionary Intelligence*, pp. 1–12, 2019.

[103] I. Letteri, M. Del Rosso, P. Caianiello, and D. Cassioli, "Performance of botnet detection by neural networks in software-defined networks." in *ITASEC: Proceedings of the Second Italian Conference on Cyber Security*, Milan, Italy, 6-9 February, 2018.

[104] S. Sriram, R. Vinayakumar, M. Alazab, and K. Soman, "Network flow based iot botnet attack detection using deep learning," in *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. IEEE, 2020, pp. 189–194.

[105] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based iot-botnet attack detection with sequential architecture," *Sensors*, vol. 20, no. 16, p. 4372, 2020.

[106] C. D. McDermott, F. Majdani, and A. V. Petrovski, "Botnet detection in the Internet of Things using deep learning approaches," in *2018 international joint conference on neural networks (IJCNN)*. IEEE, 2018, pp. 1–8.

[107] J. Liu, S. Liu, and S. Zhang, "Detection of iot botnet based on deep learning," in *2019 Chinese Control Conference (CCC)*. IEEE, 2019, pp. 8381–8385.

[108] G. D. L. T. Parra, P. Rad, K.-K. R. Choo, and N. Beebe, "Detecting Internet of Things attacks using distributed deep learning," *Journal of Network and Computer Applications*, vol. 163, p. 102662, 2020.

[109] C. Tzagkarakis, N. Petroulakis, and S. Ioannidis, "Botnet attack detection at the iot edge based on sparse representation," in *2019 Global IoT Summit (GIoTS)*. IEEE, 2019, pp. 1–6.

[110] M. Nakip and E. Gelenbe, "MIRAI botnet attack detection with auto-associative dense random neural network," in *IEEE Global Communications Conference (Globecom)*, 2021, pp. 1–6.

[111] E. Gelenbe, "Random neural networks with negative and positive signals and product form solution," *Neural Computation*, vol. 1, no. 4, pp. 502–510, 1989.

[112] E. Gelenbe and Y. Yin, "Deep learning with random neural networks," in *2016 International Joint Conference on Neural Networks (IJCNN)*, 2016, pp. 1633–1638.

[113] E. Gelenbe and Y. Yin, "Deep learning with dense random neural networks," in *International Conference on Man–Machine Interactions*. Springer, 2017, pp. 3–18.

[114] E. Gelenbe and M. Nakıp, "G-networks can detect different types of cyberattacks," in *MASCOTS'22: 30th International Symposium on the Modeling, Analysis, and Simulation of Computer and Telecommunication Systems, IEEE Computer Society*. IEEEXplore, pp. 1–6.

[115] E. Gelenbe, Z.-H. Mao, and Y.-D. Li, "Function approximation with spiked random networks," *IEEE Trans. Neural Networks*, vol. 10, no. 1, pp. 3–9, 1999.

[116] O. Brun, Y. Yin, and E. Gelenbe, "Deep learning with dense random neural network for detecting attacks against iot-connected home environments," *Procedia Computer Science*, vol. 134, pp. 458–463, 2018.

[117] E. Gelenbe and Y. Yin, "Deep learning with random neural networks," in *2016 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 2016, pp. 1633–1638.

[118] ——, "Deep learning with dense random neural networks," in *International Conference on Man–Machine Interactions*. Springer, Cham, 2017, pp. 3–18.

[119] W. Serrano, E. Gelenbe, and Y. Yin, "The random neural network with deep learning clusters in smart search," *Neurocomputing*, vol. 396, pp. 394–405, 2020.

[120] E. Gelenbe, "Random neural networks with negative and positive signals and product form solution," *Neural computation*, vol. 1, no. 4, pp. 502–510, 1989.

[121] ——, "Stability of the random neural network model," *Neural computation*, vol. 2, no. 2, pp. 239–247, 1990.

[122] ——, "Learning in the recurrent random neural network," *Neural Computation*, vol. 5, no. 1, pp. 154–164, 1993.

[123] E. Gelenbe and K. F. Hussain, "Learning in the multiple class random neural network," *IEEE Transactions on Neural Networks*, vol. 13, no. 6, pp. 1257–1267, 2002.

[124] D. Konar, E. Gelenbe, S. Bhandary, A. D. Sarma, and A. Cangi, "Random quantum neural networks (RQNN) for noisy image recognition," CoRR, vol. abs/2203.01764, 2022.

[125] E. Gelenbe, "Energy packet networks: adaptive energy management for the cloud," in *CloudCP'12: Proceedings of the 2nd International Workshop on Cloud Computing Platforms. ACM*, 2012, pp. 1–5. **DOI**: 10.1145/2168697.2168698

[126] E. Gelenbe and Y. M. Kadioglu, "Energy life-time of wireless nodes with network attacks and mitigation," in *Proceedings of ICC 2018, 20-24 May 2018, W04: IEEE Workshop on Energy Harvesting Wireless Communications*. IEEE.

[127] E. Gelenbe and E. T. Ceran, "Energy packet networks with energy harvesting," *IEEE Access*, vol. 4, pp. 1321–1331, 2016.

[128] Y. M. Kadioglu and E. Gelenbe, "Product-form solution for cascade networks with intermittent energy," *IEEE Systems Journal*, vol. 13, no. 1, pp. 918–927, 2018.

[129] E. Gelenbe and Y. M. Kadioglu, "Energy loss through standby and leakage in energy harvesting wireless sensors," in *2015 IEEE 20th International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD)*. IEEE, 2015, pp. 231– 236.

[130] Y. M. Kadioglu and E. Gelenbe, "Packet transmission with k energy packets in an energy harvesting sensor," in *Proceedings of the 2nd International Workshop on Energy-Aware Simulation*, 2016, pp. 1–6.

[131] E. Gelenbe and Y. M. Kadioglu, "Performance of an autonomous energy harvesting wireless sensor," in *Information sciences and systems 2015. Springer, Cham*, 2016, pp. 35–43.

[132] Y. M. Kadioglu and E. Gelenbe, "Wireless sensor with data and energy packets," in *2017 IEEE international conference on communications workshops (ICC Workshops)*. IEEE, 2017, pp. 564–569.

[133] E. Gelenbe and Y. M. Kadioglu, "Energy life-time of wireless nodes with network attacks and mitigation," in *2018 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE, 2018, pp. 1–6.

[134] ——, "Battery attacks on sensors," in *EuroCybersec 2018: International symposium on computer and information sciences, Security Workshop*. Springer, 2018.

[135] J. Domanska, E. Gelenbe, T. Czachorski, A. Drosou, and D. Tzovaras, "Research and innovation action for the security of the internet of things: The seriot project," in *Recent Cybersecurity Research in Europe: Proceedings of the 2018 ISCIS Security Workshop, Imperial College London*, E. Gelenbe, P. Campegiani, T. Czachorski, S. Katsikas, I. Komnios, L. Romano, and D. Tzovaras, Eds. Lecture Notes CCIS No. 821, Springer Verlag, 2018.

[136] E. Gelenbe, J. Domanska, T. Czachorski, A. Drosou, and D. Tzovaras, "Security for internet of things: The seriot project," in *International Symposium on Networks, Computers and Communications, Proceedings of the. IEEE*, June 2018.

[137] P. Fröhlich, E. Gelenbe, J. Fiołka, J. Checinski, M. Nowak, and Z. Filus, "Smart sdn management of fog services to optimize qos and energy," *Sensors*, vol. 21, no. p. 3105, 2021. **DOI**: 10.3390/s21093105

[138] P. Frohlich, E. Gelenbe, and M. P. Nowak, "Smart sdn management of fog services," in *GIOTS 2020: Global IoT Summit 2020, IEEE Communications Society*, 1-5 June 2020, Dubin, Ireland. TechRxiv, 2020.

[139] E. Gelenbe, P. Frohlich, Nowak, Mateusz, S. Papadopoulos, Protogerou, Aikaterini, A. Drosou, and D. Tsovaras, "Iot network attack detection and mitigation," in T*he 9th Mediterranean Conference on Embedded Computing (MECO'2020)*, June 8-11, 2020, Budva, Montenegro, 2020, pp. 1–6.

[140] P. Fröhlich, E. Gelenbe, and M. Nowak, "Reinforcement learning and energy-aware routing," in *Proceedings ACM SIGCOMM 4th FlexNets Workshop on Flexible Networks: Artificial Intelligence Supported Network Flexibility and Agility*, 2021, pp. 26–31.

[141] E. C. H2020, "Getting more "intelligent"about internet security." [Online]. Available: https://cordis.europa.eu/article/id/436278-getting-more-intelligent-about-internet-security

[142] P. Frohlich and E. Gelenbe, "Optimal fog services placement in sdn iot network using random neural networks and cognitive network map," in *The 19th International Conference on Artificial Intelligence and Soft Computing*, Zakopane, PL, Springer LNAI, vol. 12415., 2020, pp. 78–89. **DOI**: 10.1007/978-3-030-61401-0

[143] E. Gelenbe, J. Domanska, P. Frohlich, M. Nowak, and S. Nowak, "Self-aware networks that optimize security, qos and energy," *Proceedings of the IEEE*, vol. 108, no. 7, pp. 1150–1167, 2020.

[144] E. Gelenbe, R. Lent, and Z. Xu, "Measurement and performance of a cognitive packet network," *Computer Networks*, vol. 37, no. 6, pp. 691–701, 2001.

[145] ——, "Design and performance of cognitive packet networks," *Performance Evaluation*, vol. 46, no. 2, pp. 155–176, 2001.

[146] E. Gelenbe, R. Lent, A. Montuori, and Z. Xu, "Cognitive packet networks: Qos and performance," in *Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 2002. MASCOTS 2002. Proceedings. 10th IEEE International Symposium on. IEEE*, 2002, pp. 3–9.

[147] E. Gelenbe and P. Liu, "Qos and routing in the cognitive packet network," in *World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a. IEEE*, 2005, pp. 517–521.

[148] F. Francois and E. Gelenbe, "Optimizing secure sdn-enabled inter-data centre overlay networks through cognitive routing," in *2016 IEEE 24th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS)*. IEEE, 2016, pp. 283–288.

[149] E. Gelenbe, R. Lent, and Z. Xu, "Towards networks with cognitive packets," in *Performance and QoS of next generation networking*. Springer, 2001, pp. 3–17.

[150] E. Gelenbe and R. Lent, "Power-aware ad hoc cognitive packet networks," *Ad Hoc Networks*, vol. 2, no. 3, pp. 205–216, 2004.

[151] E. Gelenbe and M. Gellman, "Oscillations in a bio-inspired routing algorithm," in *2007 IEEE International Conference on Mobile Adhoc and Sensor Systems*. IEEE, 2007, pp. 1–7.

[152] ——, "Can routing oscillations be good? the benefits of route-switching in self-aware networks," in *2007 15th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems*. IEEE, 2007, pp. 343–352.

[153] E. Gelenbe, "Genetic algorithms with analytical solution," in *Proceed- ings of the 1st annual conference on genetic programming*. MIT Press, 1996, pp. 437–443.

[154] P. Liu and E. Gelenbe, "Recursive routing in the cognitive packet network," in *Testbeds and Research Infrastructure for the Development of Networks and Communities*, 2007. TridentCom 2007. 3rd International Conference on. IEEE, 2007, pp. 1–6.

[155] E. Gelenbe and T. Mahmoodi, "Energy-aware routing in the cognitive packet network," *Energy*, pp. 7–12, 2011.

[156] ——, "Distributed energy-aware routing protocol," in Computer and Information Sciences II. Springer London, 2012, pp. 149–154.

[157] E. Gelenbe, G. Sakellari, and M. D'arienzo, "Admission of qos aware users in a smart network," *ACM Transactions on Autonomous and Adaptive Systems (TAAS)*, vol. 3, no. 1, pp. 1–28, 2008.

[158] E. Gelenbe and E. C.-H. Ngai, "Adaptive qos routing for significant events in wireless sensor networks," in *2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*. IEEE, 2008, pp. 410–415.

[159] E. Gelenbe and E. C. Ngai, "Adaptive random re-routing in sensor networks," *Proceedings of the Annual Conference of ITA (ACITA'08)* September 16, vol. 18, pp. 348–349, 2008.

[160] E. C. Ngai, E. Gelenbe, and G. Humber, "Information-aware traffic reduction for wireless sensor networks," in *Local Computer Networks*, 2009. LCN 2009. IEEE 34th Conference on. IEEE, 2009, pp. 451–458.

[161] E. Gelenbe, E. C. Ngai, and P. Yadav, "Routing of high-priority packets in wireless sensor networks," *IEEE Second International Conference on Computer and Network Technology*, IEEE, 2010.

[162] N. Li, X. Hu, E. Ngai, and E. Gelenbe, "Cooperative wire-less edges with composite resource allocation in hierarchical networks," in *2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM)*, 2021, pp. 1–6.
DOI: 10.1109/HEALTHCOM49281.2021.9398997

[163] J. Du, C. Jiang, E. Gelenbe, H. Zhang, and Y. Ren, "Traffic offloading in software defined ultra-dense networks," *Ultra-Dense Networks: Principles and Applications*, p. 164, 2020.

[164] J. Du, E. Gelenbe, C. Jiang, H. Zhang, and Y. Ren, "Contract design for traffic offloading and resource allocation in heterogeneous ultra-dense networks," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2457–2467, 2017.

[165] J. Du, E. Gelenbe, C. Jiang, H. Zhang, Y. Ren, and H. V. Poor, "Peer prediction-based trustworthiness evaluation and trustworthy service rating in social networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6, pp. 1582–1594, 2018.

[166] J. Du, C. Jiang, E. Gelenbe, L. Xu, J. Li, and Y. Ren, "Distributed data privacy preservation in iot applications," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 68–76, 2018.

[167] J. Du, C. Jiang, E. Gelenbe, H. Zhang, Y. Ren, and T. Q. Quek, "Double auction mechanism design for video caching in heterogeneous ultra-dense networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 3, pp. 1669–1683, 2019.

[168] J. Du, E. Gelenbe, C. Jiang, Z. Han, and Y. Ren, "Auction-based data transaction in mobile networks: Data allocation design and performance analysis," *IEEE Transactions on Mobile Computing*, vol. 19, no. 5, pp. 1040–1055, 2019.

[169] C. Cramer, E. Gelenbe, and H. Bakircloglu, "Low bit-rate video compression with neural networks and temporal subsampling," *Proceedings of the IEEE*, vol. 84, no. 10, pp. 1529–1543, 1996.

[170] C. E. Cramer and E. Gelenbe, "Video quality and traffic qos in learning-based subsampled and receiver-interpolated video sequences," *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 2, pp. 150– 167, 2000.

[171] L. Wang and E. Gelenbe, "Adaptive dispatching of tasks in the cloud," *IEEE Transactions on Cloud Computing*, vol. 6, no. 1, pp. 33–45, 2018.

[172] E. Gelenbe, M. P. Nowak, P. Frohlich, J. Fiolka, and J. Checinski, "Energy, qos and security aware services at the edge," in *EuroCyber-Sec2021*. Springer, Cham, 2022.

[173] E. Gelenbe and M. Siavvas, "Minimizing energy and computation in long-running software," *Applied Sciences*, vol. 11, no. 3, p. 1169, 2021.

[174] E. Gelenbe and Y. Zhang, "Performance optimization with energy packets," *IEEE Systems Journal*, vol. 13, no. 4, pp. 3770–3780, 2019.

[175] ——, "Sharing energy for optimal edge performance," in *International Conference on Current Trends in Theory and Practice of Informatics*. Springer, Cham, 2020, pp. 24–36.

[176] D. Kehagias, M. Jankovic, M. Siavvas, and E. Gelenbe, "Investigating the interaction between energy consumption, quality of service, reliability, security, and maintainability of computer systems and networks," *SN Computer Science*, vol. 2, no. 1, pp. 1–6, 2021.

[177] T. Czachorski, E. Gelenbe, G. S. Kuaban, and D. Marek, "A time-dependent routing model of software defined networks," in *The Second International Workshop on Stochastic Modeling and Applied Research of Technology: SMARTY* 2020, August 16-20, 2020, Karelian Research Center, Russian Academy of Sciences, Petrozavodsk, CEUR Workshop Proceedings, vol. 2792. ISSN: 1613-0073, 2020, pp. 38–56.

[178] T. Czachórski, E. Gelenbe, G. S. Kuaban, and D. Marek, "Time-dependent performance of a multi-hop software defined network," *Applied Sciences*, vol. 11, no. 6, p. 2469, 2021.

[179] T. Czachórski, E. Gelenbe, and D. Marek, "Software defined network dynamics via diffusions," in *Symposium on Modelling, Analysis, and Simulation of Computer and Telecommunication Systems*. Springer, Cham, 2021, pp. 29–47.

[180] T. Czachórski, E. Gelenbe, G. S. Kuaban, and D. Marek, "Optimizing energy usage for an electric drone," in *International ISCIS Security Workshop*. Springer, Cham, 2022, pp. 61–75.

[181] M. Nakip and E. Gelenbe, "Botnet attack detection with incremental online learning," in *EuroCyberSec2021*. Springer, Cham, 2022.

[182] E. Gelenbe, T. Czachorski, D. Marek, and M. Nakıp, "Mitigating the massive access problem in the internet of things," in *EuroCyber-Sec2021*. Springer, Cham, 2022.

[183] E. Gelenbe, M. Nakip, and T. Czachorski, "Improving massive access to iot gateways," *Performance Evaluation*, p. 102308, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0166531622000219

[184] M. Nakip and E. Gelenbe, "Mirai botnet attack detection with auto-associative dense random neural networks," in *2021 IEEE Global Communications Conference*, vol. 2021. IEEE Communications Society, 2021, pp. 1–6.

[185] ——, "Botnet attack detection with incremental online learning," in *International ISCIS Security Workshop*. Springer, Cham, 2022, pp. 51–60.

[186] E. Gelenbe and M. Nakip, "G-networks can detect different types of cyberattacks," in *MASCOTS 2022: IEEE 30th International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems*, no., 2022, pp. 1–6.
https://zenodo.org/record/6969827#.Yu6fc

[187] K. Filus, P. Boryszko, J. Domanska, M. G. Siavvas, and E. Gelenbe, "Efficient feature selection for static analysis vulnerability prediction," *Sensors*, vol. 21, no. 4, p. 1133, 2021.

[188] M. Siavvas and E. Gelenbe, "Optimum interval for application-level checkpoints," in *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. IEEE, 2019, pp. 145–150.

[189] E. Gelenbe, P. Boryszko, M. Siavvas, and J. Domanska, "Optimum checkpoints for time and energy," in *2020 28th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*. IEEE, 2020, pp. 1–8.

[190] K. Filus, M. Siavvas, J. Domańska, and E. Gelenbe, "The random neural network as a bonding model for software vulnerability prediction," in *Symposium on Modelling, Analysis, and Simulation of Computer and Telecommunication Systems, Workshop*. Springer, Cham, 2021, pp. 102–116.

[191] K. Filus, P. Boryszko, J. Domańska, M. Siavvas, and E. Gelenbe, "Efficient feature selection for static analysis vulnerability prediction," *Sensors*, vol. 21, no. p. 1133, 2021. **DOI**: 10.3390/s21041133

[192] M. Siavvas, D. Kehagias, D. Tzovaras, and E. Gelenbe, "A hierarchical model for quantifying software security based on static analysis alerts and software metrics," *Software Quality Journal*, vol. 29, no. 2, pp. 431–507, 2021.

Mehmet Ufuk Çağlayan holds a BS and MS in CS from METU (Ankara), and the PhD from Northwestern University, USA. He is Professor and Head of the Department of Computer Engineerng at Yaşar University in Izmir, Turkey. Previously Professor of Computer Engineering at Boğaziçi University, Turkey's most selective university. His research includes Computer and Network Security, Computer Communications, Computer Networks and Internet, Wireless and Mobile Networks, Distributed Systems, Operating Systems, Software Engineering, Software Design and Software Project Management. In 1979-81 he served as Instructor in the Department of Electrical Engineering and Computer Science, North-western University and in 1978-79 he was Instructor in Mathematics at DePaul University in Chicago. In 1981-87 he was an Assistant Professor of Computer Science and Engineering at King Fahd University of Petroleum and Minerals, in Dhahran, Saudi Arabia. He joined Boğaziçi University in 1987 as an Assistant Professor, and on leave of absence in 1989-91 was a Computer Scientist at BASF AG, Ludwigshafen, Germany. Author of some two-hundred publications, full Professor since 1999, he Coordinated the nationally funded TAM Project, aiming to increase the PhD graduates in Computer Engineering at his university and in Turkey. In 2000-04 he served as Chair of the Department of Computer Engineering of Boğaziçi University. He graduated several PhDs who are faculty in Turkey's leading universities and many Master's students.

A Fine-grained Dynamic Access Control Method for Power IoT Based on Kformer

Rixuan Qiu, Xue Xue, Mingliang Chen, Jinkun Zheng, Sitong Jing, and Yuancheng Li

Abstract—**The existing static ABAC(Attribute-Based Access Control) model cannot fully meet the increasingly complex, dynamic and scalable demands of the power grid. At the same time, its versatility and flexibility bring high costs. Additionally, the increasing complexity of organizational systems and the need for federated access to their resources make implementing and managing access control more challenging. This paper proposes a fine-grained dynamic access control method based on Kformer to automate authorization management tasks. We use Kformer, which filters and integrates external knowledge through feed-forward layers in Transformer. Then, we use BERT(Bidirectional Encoder Representations from Transformer) to perform feature extraction on the input fused text, extract the implied attribute-authority relationship from the log records and external documents, and finally, perform sequence modeling on the extracted attribute features and input the obtained results. The final authorization result is obtained by classification through the softmax function in the final fully connected layer. The authorization management of the user's request to the object is dynamically completed. Finally, using the access data of the grid information system to evaluate the method proposed by us, the experimental results show that the model can continuously monitor the access behavior of users inside the grid information system, change the access rights of entities and adjust the policy in real-time, and carry out dynamic access authorization. At the same time, the accuracy of the generated access control policy can reach 87.73%.**

Index Terms—**ABAC, Dynamic Authorization, Kformer, Knowledge Injection, Access Control Policy**

I. INTRODUCTION

Access control is one of the essential services responsible for protecting the underlying data of the information system from attack. With the rapid development of computing and information technology, the traditional access control model can no longer meet emerging applications' fine-grained capture and expression security requirements. To improve the power grid informatization and business service capability, the introduced emerging technologies expose some key data of the power grid in the application process, bringing new challenges to the power grid information security [1]. The devices are interconnected and connected to the Internet to realize the effective management of the enterprise. However, there are many security vulnerabilities and threats in data management. The uncertainty may come from internal factors like system failure or external ones like malicious attacks [2]. The Internet of things is dynamic, and there is no clearly defined network boundary. How to solve the access control problem in the Internet of things environment is an important and challenging problem. On the one hand, the security of such protective measures is seriously insufficient, and there is a risk of being broken through. On the other hand, the existing static access control methods and defense strategies are static, solidified, strict, and extensive authority control.

To further standardize the network security system, the International Organization for Standardization (ISO) defines five security services in the network security system standard (ISO7498-2): identity authentication services, access control services, data confidentiality services, data integrity services, and anti-repudiation services. As one of the important components of access control, it was formally proposed in the 1960s and 1970s. In the following decades, many relatively complete and mature access control models appeared successively, among which the widely used models mainly include: Discretional Access Control (DAC) model [3], Mandatory Access Control (MAC) model [4], Role-based access control model (RBAC) [5]. The main problem with these access policies is that they often assign more access rights than the requesting entity needs, exposing system resources to insider attacks [6]. Furthermore, these access policies are manually specified and maintained, assuming the operation is in a closed environment and interaction conditions rarely change. The highly dynamic nature of the IoT environment results in predefined access control policies in the access context that cannot meet policy administrators' security and privacy goals. In an IoT environment, access control policies quickly become outdated due to frequent changes in security and privacy requirements, increasing the risk of insider attacks and making policy management and maintenance tedious and error-prone.

Access control technology will develop in a new direction of fine-grained, flexible, and dynamic. Therefore, an adaptive access control mechanism is needed to respond immediately to changes in the Internet of things environment and refine the access control strategy with minimal or no human intervention at runtime.

The structure of this paper is as follows. Section 2 reviews the existing work on access control policy extraction and application of machine learning. Section 3 designs and implements the main framework of Kformer and describes its use in dynamic access control policy learning. The application and steps of the fourth part introduce the settings and experimental results of the experiment. Section V provides an overview of the results and future work.

Rixuan Qiu, Xue Xue and Yuancheng Li are with School of Control and Computer Engineering, North China Electric Power University (Corresponding author e-mail: ncepua@163.com).

Rixuan Qiu and Jinkun Zheng are with Information & Telecommunication Branch of State Grid Jiangxi Electric Power Supply Co., Ltd.

Mingliang Chen are with State Grid Jiangxi Electric Power Co., Ltd.

Sitong Jing are with PowerChina Jiangxi Electric Power Engineering Co., Ltd.

DOI: 10.36244/ICJ.2022.4.11

II. RELATED WORK

Strategy mining technology has been proposed in the literature to meet these challenges to help organizations reduce the cost, time, and errors of strategy formulation and management. The policy mining algorithm simplifies the migration to the updated or appropriate authorization model by fully (or partially) automating the process of constructing access control policies. Policy mining technology is first introduced into the development of the RBAC strategy. [7] proposed the term "role mining" to refer to a data mining method that constructs roles from a given permission assignment dataset. This work is followed by various role mining technologies, such as [8], [9], [10]. Although the proposed methods help develop the best character set, they are unsuitable for extracting ABAC strategies. [11] first studied the problem of mining ABAC policies from a given access control matrix or log. Subsequently, [12] proposed a new method for mining ABAC policies, including positive and negative authorization rules, by generating authorization logs as the input of the mining algorithm. In contrast, [13] proposed a rule mining algorithm for creating ABAC policies with rules and a scoring algorithm for evaluating policies from a least-privilege perspective, generating fewer over- and under-privileged than RBAC methods.

However, the current solution assumes that the rules are mined from a static dataset of access rights, and this process only needs to be performed once. Whereas in real life, access policies are dynamic and may change depending on the situation. Using the current method, it is necessary to re-execute the mining algorithm for each update in the permissions or user and object attributes, which will greatly reduce the efficiency. At the same time, the above strategy mining method is difficult to find the error of the original authority distribution relationship, and it is difficult to optimize the strategy.

The state of existing devices changes dynamically, for example, sleep and wake, connect or disconnect, and the context of the device, including location and speed. The above will result in unsuitable policies for the current environment, i.e., low-quality rules. If there are a lot of bad rules in the system, it can lead to delayed access and wrong authorization. In the traditional ABAC access control model, the rules will not change during system operation once the rules are specified. Therefore, these static rules are inefficient and fail to comply with the IoT environment.

Machine learning and deep learning methods are gradually applied to the ABAC policy learning problem and significantly improve traditional policy mining methods. [14] proposed Polisma, which combines data mining, statistics, and machine learning techniques. Polisma learns from logs of historical access requests and their corresponding decisions, leveraging latent contextual information obtained from external sources such as LDAP directories to enhance the learning process. [15] proposed a method to automatically learn ABAC policy rules from system access logs to simplify the policy development process. The method employs an unsupervised learning-based algorithm to detect patterns in access logs and extracts ABAC authorization rules from these patterns. Two policy improvement algorithms are proposed to generate higher-quality mining policies, including rule pruning and policy refinement algorithms. However, this unsupervised clustering algorithm is difficult to find a suitable number of clusters, and it is easy to fall into the minimum optimum.

Subject-object dynamic access control determines the legitimacy of the subject's identity according to a predetermined policy and dynamically authorizes resource access requests from trusted subjects. The network security architecture based on zero trust emphasizes the requirements of dynamic authorization and requires evaluation and authentication for all resource access behaviors of each business. We will study a fine-grained dynamic access control method based on Kformer. Our goal is to dynamically calculate and determine according to the subject attribute, object attribute, and environment attribute to prevent the Internet of things device users from abusing their access privileges or using outdated access control policies to obtain unauthorized access, simplify the management of access control policies and realize the real-time evaluation of the service access behavior of distribution Internet of things terminals Real-time authorization and disposal.

III. A FINE-GRAINED DYNAMIC ACCESS CONTROL METHOD BASED ON KFORMER

This section will provide an overview of Attribute-Based Access Control (ABAC), Kformer Network Design, Power IoT, and its authorization framework.

A. ABAC

In 2013, NIST published the Guidelines for ABAC Definitions and Considerations [16], according to which "ABAC engines can be based on specified attributes of requestors, specified attributes of objects, environmental conditions, and a set of policies specified following these attributes and conditions. Make access control decisions." This paper uses subject attributes, object attributes, and ambient attributes to denote requester attributes, and ambient attributes, respectively. A property is any property of a subject, object, and environment, encoded as name: value pairs. Subjects can be personal or impersonal entities. Objects are system resources, operations are functions performed on objects at the subject's request, and environmental conditions are characteristics of the context in which the access request occurs, independent of subjects and objects.

Therefore, it is defined that U,O,E,OP is the set of subjects, objects, environments, and operations in the system, and user attributes (A_U), object attributes (A_O) and session attributes (A_E) are the subject attributes, objects defined in the NIST guidelines, And mapping of properties and environment properties.

User (U): represents a collection of users. The visitor's attributes, such as age, gender, department, role, etc. the user is the service requester interacting with the computing system, and the access request of the computing system is controlled.

Object (O): represents a collection of objects. The attributes of the accessed object, such as the modification time of a record, the creator, the security level, etc.

Environment (E): represents a collection of environmental information, such as time information, geographic location information, access platform information, etc.

Operation (OP): represents a set of operations on a resource. Actions are operations that can be performed on resources, such as CRUD.

The decision D of the authorization tuple can be either allowed or denied. A tuple with permission decisions means that user U canoperaten OP on object O under context attribute E. An authorization tuple with denying means that the user cannot gain such access

ABAC rules (γ): ABAC rules are a tuple

$$\gamma = \{U, O, E, OP, D\} \tag{1}$$

D represents the decision of the ABAC rule for this combination of attributes and the requested action.

B. Kformer network design

This paper decomposes the problem of access control policy generation into two key tasks: external knowledge injection and statement recognition of access control policy. The statement recognition task of the access control policy is to extract access control-related statements from project-related documents (such as user manuals, requirements analysis documents, instructions for use, etc.). Extractive, the attribute feature of Access control policy, extracts the information of subject attribute, action attribute, object attribute, environment attribute, and the relationship between attributes from the policy statements in natural language. We can directly obtain readable and executable access control policies according to these attribute information.

We use a new model Kformer [17], to inject external knowledge. Kformer consists of three main parts: First, the top N pieces of latent knowledge are retrieved from the knowledge base for each question. Then, knowledge representation is obtained through knowledge embedding. Finally, the retrieved N pieces of knowledge are fused into the pre-trained model through the feed-forward layer in the Transformer.

L layers usually stack transformer encoders. Each layer contains a multi-head self-attention and a feed-forward network (FFN). FFN consists of two linear networks. Assuming that the final attention output of the Transformer layer is $x \in \mathbb{R}^d$. The computation of the feed-forward network can be expressed as (omitting the bias term):

$$FFN = f(x \cdot K^T) \cdot V \tag{2}$$

Among them, K,$V \in \mathbb{R}^{d_m \times d}$, Where K,V is the paaremeter matrices of the two linear networks. The input x is first multiplied by K to generate coefficients, which are activated by f and used to compute the weighted sum of V as the output of the feed-forward layer.

The Apache Lucence-based sparse searcher Elasticsearch is used here, using an inverted index lookup. The attribute description and authorization decision are combined as a query sent to the search engine for each policy. The sentences with the highest scores are then selected as candidate knowledge from the results returned by the search engine. Then a dense representation of each knowledge k is obtained through knowledge embedding, and the input sentence x is calculated through the average embedding of each word. Then, use the question embedding and the knowledge embedding to do the inner product to calculate the score of each candidate's knowledge [18]. Finally, we select the top N candidate knowledge scores as external knowledge dependencies and incorporate them into the model in the knowledge injection part.

Each candidate's knowledge is treated as a sentence, and an embedding layer is used for knowledge representation. Initialize the knowledge embedding matrix to be the same as the embedding matrix in Transformer and update the knowledge embedding layer simultaneously during training. For each knowledge $\mathbf{k}$, the tokens are embedded as $k_1, k_2, \ldots, k_l$ via knowledge embedding. k is expressed as the mean of these token embeddings:

$$Embed(\mathbf{k}) = Aug(k_1, k_2, \ldots, k_l) \tag{3}$$

Here, the candidate knowledge is denoted as $k_1, k_2, \ldots, k_M$, Where M is the number of candidate knowledge.

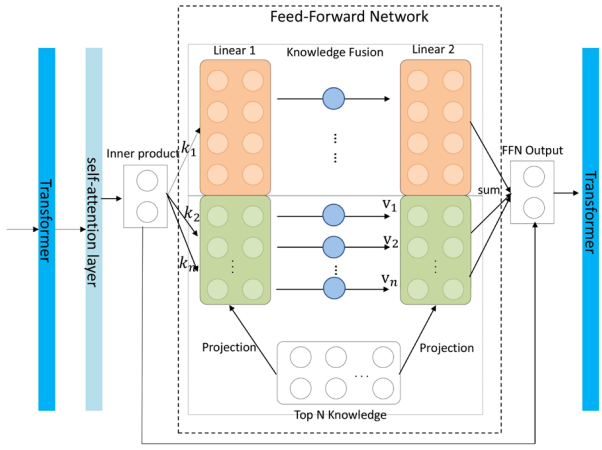


Fig. 1. Knowledge injection process in Kformer.Input vectors are multiplied by each knowledge vector. The final output of the feed-forward network is the sum of the original linear layers' output and the knowledge fusion's output.

The Transformer layer is shown in Figure1, where knowledge fusion is performed. The feed-forward network in each Transformer layer consists of two linear transforms with a GeLU activation in the middle. Assuming that the final attention output of layer l is H^l, the outputs of the two linear layers are:

$$FFN(H^l) = f(H^l \cdot K^l) \cdot V^l \tag{4}$$

where K,$V \in \mathbb{R}^{d_m \times d}$ is the parameter matrix of the first and second linear layers, and f represents the non-linear function. d_m is the intermediate layer size of the Transformer, and d is the hidden layer size. After retrieval, Suppose we get the top N knowledge documents $\mathbf{k} \in \mathbb{R}^{\mathbf{d_n} \times \mathbf{d}}$. Through Knowledge Embedding, we get each knowledge as $k_1, k_2, \ldots, k_N \in \mathbb{R}^{d_n}$. To inject knowledge into a specific layer l, we need to map the knowledge to the corresponding vector space. Here, for each layer l, we use two different linear layers for knowledge

mapping. W^K and W^V represent the weights of the two linear layers ($W^K, W^V \in \mathbb{R}^{d\times d}$). The two matrices W^K and W^V are randomly initialized and will be updated during fine-tuning.

$$\phi_k^l = Pr_k\mathbf{k} = W_k^l \cdot \mathbf{k} \tag{5}$$

$$\phi_v^l = Pr_v\mathbf{k} = W_v^l \cdot \mathbf{k} \tag{6}$$

After projection, ϕ_k^l and ϕ_v^l are injected into the corresponding$\mathbf{K}^l$ and $\mathbf{V}^l$, We extend the FFN by concatenating the projection knowledge to the end of the linear layer and obtain the extended $\mathbf{K}_E^l, \mathbf{V}_E^l \in \mathbb{R}^{(d_m+d_n)\times d}$. Therefore, after injection, the calculation of FFN can be described as:

$$FFN(H^l) = f(H^l \cdot \mathbf{K}_E^l) \cdot V^l = f(H^l \cdot [\phi_k^l : \mathbf{K}^l]) \cdot [\phi_v^l : \mathbf{V}^l] \tag{7}$$

The model activates knowledge relevant to the access control policy and injects it through the knowledge fusion part. Next, the collected information will be processed and aggregated by the following Transformer layers.

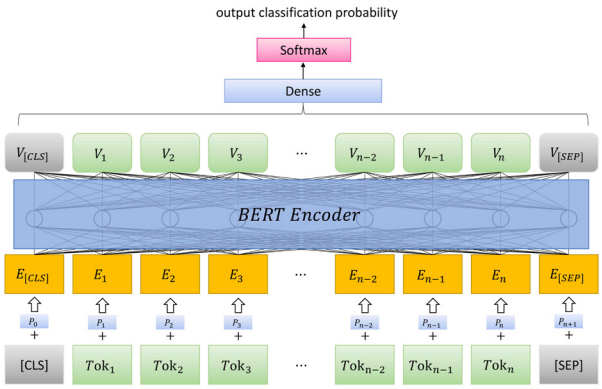


Fig. 2. Bert model architecture diagram. The input embeddings are the sum of the token embeddings, the segmentation embeddings and the position embeddings.

We use Bert [19] for subsequent processing. The model architecture is shown in Figure2. A Bert model is used at the word level, and the word flattening tokens in the sentence are fed into the model. Words are [CLS] preprocessed by the preprocessing module, and the same token vocabulary is used in Bert to obtain word-patched tokens. We keep two special tokens [CLS] and [SEP] at the beginning and end of sentences, respectively, like the Bert word-level module. The first token of each sentence is [CLS], and its corresponding hidden state is considered to represent the aggregate of the entire sentence. [SEP] is at the end of a sentence and is important to distinguish sentences. We omit segment embeddings and keep positional encodings. Therefore, for a given token i, the input embedding E_i is constructed by concatenating the token embedding Tok_i and the position encoding vector P_i. We simply apply a dense layer with a $softmax$ function to output the classification probabilities for the final labels.

C. A Fine-grained dynamic access control method based on Kformer

The terminal is the subject of the permission request, the accessed network resource is the object, and the owner of the resource is the user. Access rules can be set to restrict the user's access to the resource. The terminal makes a resource access request, and the system judges whether to grant the current user access rights according to the access control rules. When the terminal environment changes, it is necessary to evaluate it to give the corresponding permissions dynamically.

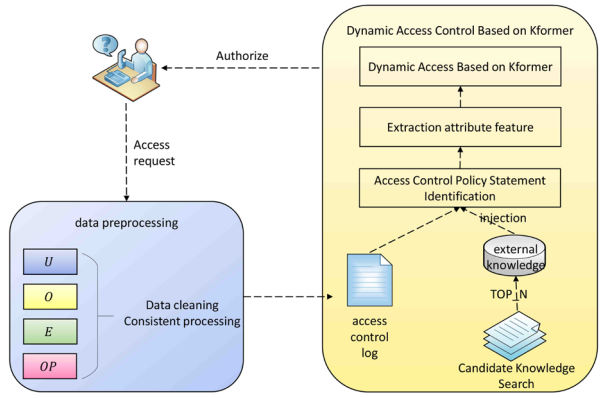


Fig. 3. Kformer-based fine-grained dynamic access control.

After the Kformer network structure is trained according to the above description, it can be used for dynamic and fine-grained access control authorization.As shown in Figure3 The main steps of the fine-grained dynamic access control authorization method based on Kformer are as follows:

Step 1: Data preprocessing: Each access control log record contains information such as the subject user, object resource, action, and operation execution result corresponding to the record. First, perform consistent processing on duplicate and conflicting log data in the log. Remove redundant duplicate log records that exist in the log. Consistently process log records with inconsistent operations according to the time dimension, delete other conflicting log records, and build a globally consistent set of log records.

Step 2: Using the sparse searcher Elasticsearch, we combine attributes and authorization decisions as a query sent to the search engine for each policy. We select the sentence with the highest score as candidate knowledge from the results returned by the search engine.

Step 3: Each Transformer block contains two important modules: multi-head self-attention and feed-forward layers. Multi-head self-attention is an important part that plays the role of message passing between tokens [18]. In the self-attention module, input tags interact and determine what they should pay more attention to. In this part, we inject knowledge into the self-attention module, and the fusion calculation is as follows:

$$Attention^l = softmax(\frac{Q^l[\phi_k^l : \mathbf{K}^l]^T}{\sqrt{d}})[\phi_v^l : \mathbf{V}^l] \tag{8}$$

Knowledge is connected in the K and V parts of self-attention.

Step 4: BERT uses Transformers as the feature extractor, mainly focusing on the part of the Encoder. First, the irregular text is transformed to improve the performance and robustness of the model. The feature extraction is performed on the input fused text, and finally, the extracted text is extracted. The obtained attribute features are sequenced, and the features extracted in the previous step can be reshaped into sequences (Batch size, Seq length, Embedding size).

Step 5: Input the obtained result into the final fully connected layer, and classify it through the $softmax$ function to obtain the final authorization result.

IV. EXPERIMENTS

We have implemented a prototype of the method proposed in Section 3. In this section, we present our experimental evaluation.

A. Experimental Setting

To verify the effectiveness of this method, simulation experiments are performed based on derived from the information system of a provincial power grid company of State Grid Co., Ltd.. The experimental environment is as follows: the operating system is Win10 64 bit, the CPU is Intel(R) Core(TM) i5-6300HQ@ 2.5 GHz, and the GPU is GeForce GTX 850 M, the memory size is 16 GB, and the Python version is 3.6. The metrics used to address our research question are then given, first defining the following variables:

1) True class TP (True Positive) indicates that the policy that allows authorization is identified as the number of policies allowed.

2) The false-positive class FP (False Positive) indicates that the policy that refuses authorization is identified as the number of allowed policies.

3) The False Negative class FN (False Negative) indicates the number of policies that allow authorities to be identified as the number of denied policies.

4) The true negative class TN (true Negative) indicates the number of policies that recognize the policies that refuse authorization as rejected.

We use accuracy to measure the performance of the Kformer model. In addition to $Accuracy$, it also includes $Precision$, $Recall$ and $F1$. Therefore, the definitions of the three indicators are described as follows.

1) The calculation expression of the accuracy rate is:

$$Accuracy = \frac{TP + TN}{TP + FP + TN + FN} \tag{9}$$

It represents the ratio of all correctly judged samples to the entirety. The higher the accuracy, the better the algorithm effect.

2) The recall calculation expression is:

$$Recall = \frac{TP}{TP + FN} \tag{10}$$

It indicates how many positive examples in the original sample are correctly predicted. The higher the recall rate, the better the algorithm effect.

3) The F1 calculation expression is:

$$F1 = \frac{2Precision \times Recall}{Precision + Recall} \tag{11}$$

F1 is an indicator used in statistics to measure the accuracy of a binary classification model. It takes into account the accuracy and recall of the classification model simultaneously. It is a weighted average of the accuracy and recall of the model. The maximum value is 1, and the minimum value is 0. The larger the value, the better the model.

B. Dataset

The data of this experiment are mainly derived from the information system of a provincial power grid company of State Grid Co., Ltd. First of all, the current assets of the power grid are analyzed, and there are currently 30 kinds of Internet of Things business systems and 131 kinds of equipment terminals in the company's management information region, totaling 6.6983 million units. The company/service is mainly the traditional information service of the State Grid Co., Ltd., mainly involving vehicle management, infrastructure projects, storage materials, electric vehicles, power payment, online monitoring of transmission and distribution and transformation lines, online monitoring of power quality, electricity information collection, power supply voltage collection, power inspection/emergency repair, distribution automation, etc. The data source used in the experiment is the network traffic data collected by the information system from 2019.03 to 2019.05, with about 97,000 messages, which mainly come from two ports, one is the upstream message of business requests sent by the terminal to the master station (port 5200). The other type is the downstream message of business requests sent by the master to the terminal (port 5100). The corresponding business types of data messages include power information collection, remote intelligent payment, remote fee control power outage, and power load control.

C. Experimental results

Each access control log record contains information such as the subject user, object resource, action, and operation execution result corresponding to the record. First, we cleaned and consistently processed the duplicate and conflicting log data in the log and then used the sparse searcher Elasticsearch to select the sentence with the highest score from the results returned by the search engine as candidate knowledge and performed it in the feed-forward layer of the Transformer. Knowledge fusion injects knowledge into the self-attention module; uses BERT as a feature extractor, converts the irregular text, performs feature extraction on the input fused text, and performs feature extraction on the extracted attributes. Sequence modeling, input the obtained results into the final fully connected layer and classify through the softmax function to obtain the final authorization result.

We adjusted the number of candidates' knowledge and listed the results in Figure4. The extracted information has both positive and negative effects on the model. If we retrieve less information, the model will not be able to solve the problem

TABLE I
MODEL COMPARISON EXPERIMENTAL RESULTS

Metrics	Transformer	BERT	RoBERTa	Kformer
Accuracy	79.22%	82.23%	84.65%	87.73%
Recall	90.73%	91.35%	93.13%	92.27%
F1-score	0.846	0.866	0.887	0.899
Running Time (s)	90.3	88.58	80.6	86.4

due to a lack of sufficient evidence. However, if we retrieve too much information, the model will suffer from knowledge noise and make wrong predictions. In the figure, when the retrieval information exceeds the first 10 sentences, the performance on our datesets drops. Figure4 shows the impact of different TOP_Ns on model accuracy in the knowledge fusion stage on our datasets.

Fig. 4. Influence of different TOP_N on model accuracy.

We also conducted comparative experiments with the other three models to evaluate the model's performance. The models are as follows:

Transformer [20]: mainly divided into Encoder and decoder. The basic principle is to input a sequence, process it through the Encoder, consider the correlation of the information before and after the whole sequence with the self-attention mechanism, and then input it into the decoder. The decoder will process the input, then classify it through a softmax, and output the final result.

Bert [19]: it is an algorithm proposed by some researchers of Google. Pre-training is carried out in a large-scale corpus, and then fine-tuning is carried out in downstream tasks. The basic model of pre-training is still the transformer model. Bert uses three ways of embedding accumulation in the embedding layer and proposes a two-way language model.

Roberta [21]: it is a method jointly proposed by Facebook and the University of Washington. By adjusting some parameters and step length of Bert, the SOTA effect is achieved in multiple tasks. Roberta's main experimental tuning aspects are as follows: Increase the training data set, batch and epoch. Replace static masked LM with dynamic masked LM. Remove the NSP. Replace characters with bytes.

We compared the four dimensions of Accuracy, Recall, F1-score, and running time, respectively. The experimental results are shown in Table I. The variance of these means is between 0.001 and 0.1.

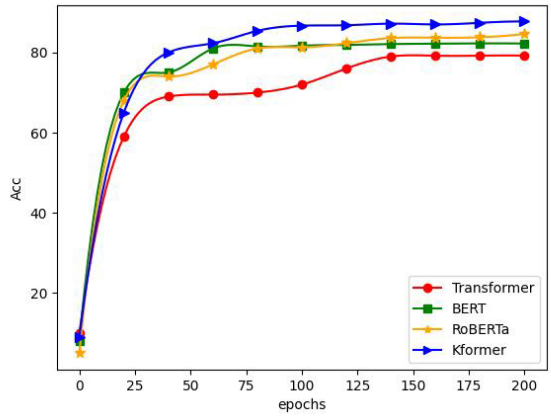


Fig. 5. Accuracy of different models.

As can be seen from TableI, Kformer has the highest accuracy of the two data sets, and the average accuracy in large real data sets can reach 87.73%. Considering the knowledge fusion in Transformer feed-forward layer, Kformer runs slowly. As can be seen from Figure5, these four models all perform well on this dataset. However, due to the injection of external knowledge, KFomer's performance is more stable than other models and has higher accuracy.

V. CONCLUSION

This paper proposes a Kformer-based fine-grained dynamic access control method to automate authorization management tasks. We use Kformer to filter and integrate external knowledge through the feed-forward layer in Transformer. Then, we use BERT to perform feature extraction on the input fused text and extract the implied attribute-authority relationship from log records and external documents. Finally, we perform sequence modeling on the extracted attribute features and input the obtained results. The final authorization result is obtained by classification through the softmax function in the final fully connected layer. The authorization management of the subject's access to the object is dynamically completed. Finally, we conducted experiments on the power information system. The experimental results show that KFormer is stable and has high accuracy. At the same time, the model can continuously monitor the user's access behavior and change it in real-time—entity access rights, real-time policy adjustment, and dynamic access authorization. For future work, We plan to extend our framework with an anomaly detection component to detect changes in normal access behaviors (i.e.,unseen behaviors) to maintain accurate and up-to-date access control policies.

ACKNOWLEDGMENT

This work was supported in part by the State Grid Jiangxi Information & Telecommunication Company Project "Research on de boundary security protection technology based on zero trust framework" under Grant 52183520007V.

REFERENCES

[1] C. Wang, J. Chen, Y. Yang, X. Ma, and J. Liu, "Poisoning attacks and countermeasures in intelligent networks: Status quo and prospects," *Digital Communications and Networks*, vol. 8, no. 2, pp. 225–234, 2022, DOI: 10.1016/j.dcan.2021.07.009.

[2] S. Maksuti, M. Zsilak, M. Tauber, and J. Delsing, "Security and autonomic management in system of systems," *Infocommunications Journal: A Publication Of The Scientific Association For Infocommunications (HTE)*, vol. 13, no. 3, pp. 66–75, 2021, DOI: 10.36244/ICJ.2021.3.7.

[3] M. A. Harrison, W. L. Ruzzo, and J. D. Ullman, "Protection in operating systems," *Communications of the ACM*, vol. 19, no. 8, pp. 461–471, 1976, DOI: 10.1145/360303.360333.

[4] R. S. Sandhu, "Lattice-based access control models,"*Computer*, vol. 26, no. 11, pp. 9–19, 1993, https://doi.org/10.1109/2.241422.

[5] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Role-based access control models," *Computer*, vol. 29, no. 2, pp. 38–47, 1996, DOI: 10.1109/2.485845.

[6] J. K. Lee, J. Park, S. Gregor, and V. Yoon, "Axiomatic theories and improving the relevance of information systems research," *Information Systems Research*, vol. 32, no. 1, pp. 147–171, 2021, DOI: 10.1287/isre.2020.0958.

[7] M. Kuhlmann, D. Shohat, and G. Schimpf, "Role mining-revealing business roles for security administration using data mining technology," in *Proceedings of the eighth ACM symposium on Access control models and technologies*, 2003, pp. 179–186, DOI: 10.1145/775412.775435.

[8] Q. Guo and M. Tripunitara, "The secrecy resilience of access control policies and its application to role mining," in *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies,* 2022, pp. 115–126, DOI: 10.1145/3532105.3535030.

[9] C. Blundo, S. Cimato, and L. Siniscalchi, "Role mining heuristics for permission-role-usage cardinality constraints," *The Computer Journal*, vol. 65, no. 6, pp. 1386–1411, 2022, DOI: 10.1093/comjnl/bxaa186.

[10] M. Abolfathi, Z. Raghebi, H. Jafarian, and F. Banaei-Kashani, "A scalable role mining approach for large organizations," in *Proceedings of the 2021 ACM Workshop on Security and Privacy Analytics*, 2021, pp. 45–54, DOI: 10.1145/3445970.3451154.

[11] Z. Xuand S. D. Stoller, "Mining attribute-based access control policies," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 5, pp. 533–545, 2014, DOI: 10.1109/TDSC.2014.2369048.

[12] P. Iyer and A. Masoumzadeh, "Mining positive and negative attribute-based access control policy rules," in *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*, 2018, pp. 161–172, DOI: 10.1145/3205977.3205988.

[13] M. W. Sanders and C. Yue, "Mining least privilege attribute based access control policies," in *Proceedings of the 35th Annual Computer Security Applications Conference*, 2019, pp. 404–416, DOI: 10.1145/3359789.3359805.

[14] A. Abu Jabal, E. Bertino, J. Lobo, M. Law, A. Russo, S. Calo, and D. Verma, "Polisma-a framework for learning attribute-based access control policies," in *European Symposium on Research in Computer Security*. Springer, 2020, pp. 523–544, DOI: 10.1007/978-3-030-58951-6_26.

[15] L. Karimi, M. Aldairi, J. Joshi, and M. Abdelhakim, "An automatic attribute based access control policy extraction from access logs," *IEEE Transactions on Dependable and Secure Computing*, 2021, DOI: 10.1109/TDSC.2021.3054331.

[16] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone et al., "Guide to attribute based access control (abac) definition and considerations (draft)," *NIST special publication*, vol. 800, no. 162, pp. 1–54, 2013.

[17] Y. Yao, S. Huang, N. Zhang, L. Dong, F. Wei, and H. Chen, "Kformer: Knowledge injection in transformer feed-forward layers," arXiv preprint *arXiv:2201.05742*, 2022.

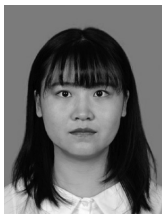
[18] Y. Hao, L. Dong, F. Wei, and K. Xu, "Self-attention attribution: Interpreting information interactions inside transformer," in *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 35, no. 14, 2021, pp. 12 963–12 971, DOI: 10.1609/aaai.v35i14.17533.

[19] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding." Minneapolis, Minnesota: Association for Computational Linguistics, jun 2019, pp. 4171–4186, DOI: 10.18653/v1/N19-1423. [Online]. Available: https://aclanthology.org/N19-1423

[20] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," *Advances in neural information processing systems*, vol. 30, 2017.

[21] Y. Liu, M. Ott, N. Goyal, J. Du, M. Joshi, D. Chen, O. Levy, M. Lewis, L. Zettlemoyer, and V. Stoyanov, "Roberta: A robustly optimized bert pretraining approach," arXiv preprint *arXiv:1907.11692*, 2019.

Rixuan Qiu was born in 1994, graduated from North China Electric Power University majoring in computer application technology, his research direction is new power system network and information security.



Xue Xue was born in Langfang, Hebei Province, China, in 1997. She received the B.S. degree in software engineering from Shijiangzhuang University, in 2019. She is currently pursuing the M.S. degree with North China Electric Power University. She has published one articles in Chinese Core Journals. Her research interests include zero trust networks and access control.

Mingliang Chen was born in Ganzhou, Jiangxi Province, China, in 1989. He received the B.Eng. degree and the M.Eng. degree from Nanchang University, Nanchang, China, in 2011 and 2017. He is currently working towards the Ph.D. degree at Xi'an Jiaotong University, Xi'an, China, and a deputy director of Power Dispatch Control Center of State Grid Jiangxi Electric Power Co., Ltd, Nanchang, China. His research interests include power system network security.

Jinkun Zheng was born in Nanchang, Jiangxi Province, China, in 1992. He received the master's degree in engineering from Harbin Institute of Technology in 2016, and has been engaged in digital development and implementation in State Grid Jiangxi Electric Power Co., Ltd. since 2016, his research areas are mainly data mining and analysis in the energy industry.

Sitong Jing is Female, Engineer. She received the master's degree from North China Electric Power University. Research Direction relay protection and scheduling automation of power systems.

Yuancheng Li received the Ph.D. degree from University of Science and Technology of China, Hefei, China, in 2003. From 2004 to 2005, he was a postdoctoral research fellow in the Digital Media Lab, Beihang University, Beijing, China. Since 2005, he has been with the North China Electric Power University, where he is a professor and the Dean of the Institute of Smart Grid and Information Security. From 2009 to 2010, he was a postdoctoral research fellow in the Cyber Security Lab, college of information science and technology of Pennsylvania State University, Pennsylvania, USA.

WS-04: 2ND WORKSHOP ON INDUSTRIAL PRIVATE 5G-AND-BEYOND WIRELESS NETWORKS

SCOPE

The fifth generation (5G)-and-beyond of radio technology delivers multi-Gbps peak data rates, ultra-reliable low latency, and massive connectivity. Thus, it provides a large number of new applications and opens a wide variety of business opportunities. 5G-and-beyond has the potential to shape the industrial world through the automation of everything. However, public 5G networks, which are owned and operated by mobile network operators, have drawbacks. On their pursuit of revenue, mobile network operators may deploy networks only in densely populated areas with a vast number of subscribers. This may result in limited public network coverage, particularly in some enterprise and remote areas, far away from business hubs. Public network coverage may also often be insufficient within some industrial buildings and factories, with harsh radio frequency operating conditions. Industrial private networks have emerged and are attracting a significant interest to address the above-mentioned challenges. This workshop aims to bring researchers together for technical discussion on fundamental and practically relevant questions to many emerging challenges in industrial private wireless networks.

TOPICS OF INTEREST

This workshop seeks original completed and unpublished work, not currently under review by any other journal/magazine/conference. Topics of interest include, but are not limited to:

- New private networking architectures, including OpenRAN
- Integration of wireless systems into currently deployed industrial networks
- Intelligent network orchestration and radio resource management (including cooperative edge computing, reinforcement learning, spectrum allocation, and spectrum management)
- Wireless data traffic characterization and forecasting
- Further enhanced URLLC for industrial private networks
- Intelligent signal processing for reduced interference
- Spectrum agile and robust hardware
- Integration of time sensitive networking in industrial wireless networks
- Private network planning, optimization, and energy efficiency
- Distributed privacy-preserving learning across multiple private networks
- RF-controlled intelligent reflecting surface for industrial private networks
- Use of unmanned vehicles, e.g., UAVs, in industrial networks
- Accurate localization and tracking and its integration with integrated sensing and communications
- Efficient multi-band aggregation, multi-node cooperation, and distributed MIMO

PAPER SUBMISSIONS

All papers for Workshops should be submitted via EDAS.

Full instructions on how to submit papers are provided on the IEEE ICC 2023 website:

icc2023.ieee-icc.org

WORKSHOP CO-CHAIRS

Kyeong Jin Kim, Mitsubishi Electric Research Lab., USA (kkim@merl.com)
David López-Pérez, Huawei Technologies, France (dr.david.lopez@ieee.org)
Kwang-Cheng Chen, University of South Florida, USA (kwangcheng@usf.edu)
Miaowen Wen, South China University of Tech, China (eemwwen@scut.edu.cn)
Petar Popovski, Aalborg University, Denmark (petarp@es.aau.dk)
Theodoros A. Tsiftsis, Jinan University, China (theo_tsiftsis@jnu.edu.cn)

WORKSHOP TPC MEMBERS

David López-Pérez, Huawei Technologies, France
Giovanni Geraci, UPF, Spain
Hongwu Liu, Shandong Jiaotong University, China
Jianlin Guo, MERL, USA
Lingjia Liu, Virginia Tech, USA
Miaowen Wen, South China University of Tech., China
Namyoon Lee, Postech, Korea
Shao-Yu Lien, National Chung-Cheng Univ., Taiwan
Phee Lep Yeoh, University of Sydney, Australia
Sunwoo Kim, Hanyang University, Korea
Hui-Ming Wang, Xi'an Jiaotong University, China
Yansha Ding, King's College London, UK
Zhiguo Ding, The University of Manchester, UK

IMPORTANT DATES

Paper Submission Deadline: 20 January 2023
Paper Acceptance Notification: 6 March 2023
Camera Ready and Registration for accepted papers: 15 March 2023

IEEE HPSR™

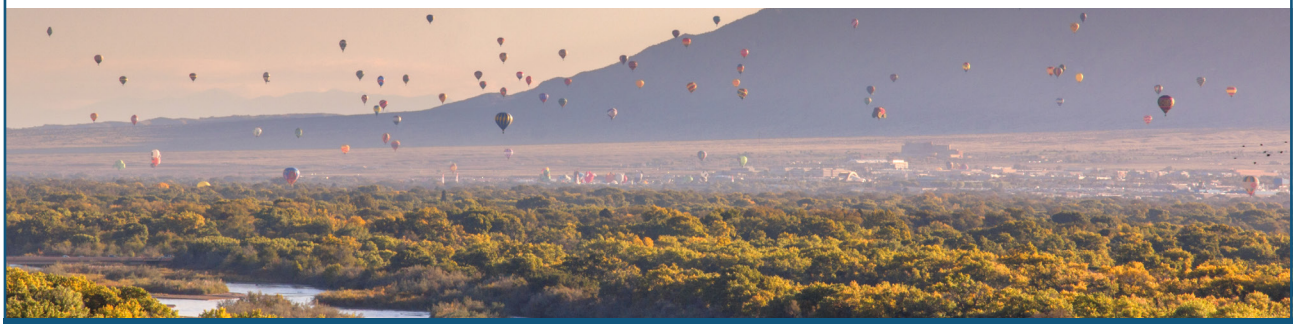
IEEE International Conference on High Performance Switching and Routing

Artificial Intelligent Next Generation (NextG) Integrated Communications and Computing Systems

5–7 June 2023 // Albuquerque, NM, USA

IEEE Advancing Technology for Humanity

IEEE ComSoc IEEE Communications Society



CALL FOR PAPERS

Next Generation (NextG) Integrated Communications and Computing Systems are envisioned to be characterized by resiliency, security, robustness, adaptability, and autonomy, while being supported by modern communication devices, computing solutions, networks, and systems. New networking technologies and intelligent techniques are needed to efficiently and effectively cope with the intricacy in traffic demands, as well as the heterogeneity of the services and applications requested by the end-users. In parallel, the advent of the Digital Continuum, i.e., device-to-edge-to-fog-to-Cloud continuum, promises to offer low-latency and ubiquitous computation to heterogeneous mobile and Internet of Things devices. A rich array of network services is expected to emerge seeking to realize greater synergy across the various component subsystems of the NextG Integrated Communications and Computing Systems.

The main focus of the HPSR 2023 – the 24th edition of HPSR conference – will be to assess how breakthrough changes occurring to NextG Integrated Communications and Computing Systems are affecting areas related to switching and routing, and NextG networks and systems in general. We are soliciting original and thought-provoking works on big data, data analytics, cloud and edge services, and artificial intelligent techniques applied to networking and switching and routing. Works on autonomous networks, 5G/6G, Industry 4.0, social networks, network, cybersecurity, virtualization, and other advanced topics are also welcome. Papers describing original, previously unpublished research, experimental efforts, practical experiences, as well as visionary roadmaps, in all aspects of switching and routing, and NextG networks and systems are solicited. Research works on the following topics, but not limited to, are welcome for submission through the following symposia:

Track A: NextG Integrated Communications and Computing Systems Symposium

- Application of data analytics to switching and routing
- Artificial intelligent routing and resource-allocation algorithms
- Behavior-aware human-centric NextG networks and systems
- Deep-learning technologies for NextG networks
- Digital Continuum — device-to-edge-to-fog-to-Cloud continuum
- Dynamic bandwidth access and management for smart-factory/Industry 4.0 applications
- Experimental measurements and testbed implementations
- Game theory enabling resource allocation and routing
- High performance, programmable networks for the Internet of Things
- Integrated access and backhaul technologies
- Integrated caching, computation, and communications
- Positioning, Navigation, and Timing techniques
- Quality of Experience resulting from intelligent routing
- Quality of Service Optimization and resource allocation
- Reconfigurable Intelligent Surfaces-enabled switching and routing
- Switching architectures for NextG applications
- Traffic monitoring and modeling applied to switching and routing
- Traffic predictions in routing and resource assignment

Track B: High-Performance High Functionality Architectures Symposium

- Address lookup algorithms, packet classification, scheduling, and dropping
- Applications of data science and analysis on high-performance networks
- Applications of GPU on network functions
- Efficient data structures for networking applications
- Future technologies for IoT
- High-speed packet processors
- ICT enabling technologies for e-health systems
- Multiprocessor networks
- Nano-communication networks
- Network management
- Network traffic characterization and measurements
- Optical switching and routing
- Power-aware switching, bridging, and routing protocols
- Routing and resource allocation for Tactile Internet
- Switching, bridging, and routing protocols whether wide-area or data centers
- Switching support to Extended reality (including virtual, augmented, and mixed reality)
- Traffic characterization and engineering
- Standardization activities of emerging high performance switching and routing

Track C: Autonomous Networks Symposium

- Architectures of high-performance switches and routers, with a focus towards reconfigurable pipelines (P4, OpenFlow, etc.)
- Blockchain technologies
- Computation offloading
- Decentralized applications (DApps)
- Decentralized autonomous organizations (DAOs)
- Economics and pricing
- Energy harvesting, storage, recycling, wireless power transfer
- Green network monitoring and routing
- Intelligent and connected vehicular networks
- Medium access control, routing, and path selection
- Middleware services for wireless, mobile and multimedia networks
- Mobile social networks and routing
- Multi-access edge computing (MEC)
- Network and switch slicing
- Network performance for Human-Agent-Robot Teamwork (HART)
- Physical-layer aspects of switching and routing
- Software-defined networking
- Space-air-ground integrated networks (wwSAGIN)

Track D: Network Security Symposium

- Adversarial machine learning
- Applied cryptography for cyber, information, and network security
- Attack prediction, detection, response, and prevention
- Authentication protocols and key management
- Blockchain security
- Cloud, data center, and distributed systems security
- Future Internet Architecture (FIA) security and privacy
- Intrusion detection with artificial intelligent techniques
- Malware detection and damage recovery
- Network security and privacy protection
- NextG networks and Internet security
- Security in SDN and networking slicing
- Security aspects of social networks
- Security in smart grid communications
- Security in virtualized network functions built or managed using software-defined networks
- Security and privacy in the Age of Information
- Trust management in networks through emerging technologies
- Virtual Private WANs
- Zero Trust Architecture

IMPORTANT DATES

Paper Submission Due: **January 23, 2023**
Acceptance Notifications: **April 3, 2023**
Author Registration Deadline: **April 24, 2023**
Final Version Submission Due: **May 1, 2023**

For more information about this conference, please visit
https://hpsr2023.ieee-hpsr.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

IECON 2023

49th Annual Conference of the IEEE Industrial Electronics Society

Marina Bay Sands Expo and Convention Centre, Singapore

IEEE

Industrial Electronics Chapter
IEEE Singapore Section

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

IECON 2023 is the 49th Annual Conference of the IEEE Industrial Electronics Society (IES), focusing on contemporary industry topics ranging from electronics, controls, manufacturing, to communications and computational intelligence.

IECON is the flagship annual conference of IES and returns to Singapore for the first time after 1988. It aims to create a forum for scientists and practising engineers throughout the world to present the latest research findings and ideas in the areas of Industrial Electronics, and possible contributions toward sustainable development and environment preservation.

Regular sessions within the scope of the following topics, but not limited to:

I. ENERGY

Power Systems and Smart Grids; Electrical Machines and Industrial Drives; Power Electronic Converters; Smart Building Technologies; Renewable Energy and Energy Storage Systems; Transportation Electrification and Automotive Technologies

II. CONTROL, INTELLIGENT SYSTEMS, AND ROBOTICS

Control Systems and Applications; Machine Learning & Signal and Image Processing; Mechatronics and Robotics; Sensors, Actuators and Micro-Nanotechnology; Resilience and Security for Industrial Applications; Smart Manufacturing Technologies; Unmanned Systems.

III.INFORMATION AND COMMUNICATION TECHNOLOGIES

Electronic Systems on Chip and Embedded Systems; Cyber Physical Systems and Internet of Things in Industry; Communications for Industrial and Factory Automation; Industrial Electronics and Education; Cloud Computing, Big Data, Industrial Informatics

Special sessions: Special sessions covers subjects or cross-subjects belonging to the topics of interest, or novel topics related with the ones identified within the topics of interest.

Submission of Papers

The working language of the conference is English. Prospective participants are requested to electronically submit full papers of their work to https://confcomm.ieee-ies.org/ Accepted, registered, and presented papers will be IEEE copyrighted and published in the conference proceedings. The proceedings is planned to be submitted for inclusion in IEEE Xplore® Digital Library and therefore indexed by EI Compendex. In order for the accepted paper to be submitted for inclusion into the IEEE Xplore® Digital Library, all of the following requirements must be satisfied: 1. Appropriate publication materials: final paper and transfer of copyright to IEEE must be submitted. 2. At least one full registration has to be paid. 3. The paper must be presented at the conference.

Important Dates:

Deadline for submission of regular papers	**April 30, 2023**
Deadline for submission of special session papers	**May 31, 2023**
Notification of acceptance	**July 01, 2023**
Deadline for submission of camera-ready manuscripts	**July 31, 2023**
Deadline for author registration	**July 31, 2023**

Supported by

SINGAPORE EXHIBITION & CONVENTION BUREAU

Held in

SINGAPORE
Passion Made Possible

SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS

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: Híradástechnikai 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*