Cyber-Twin: Digital Twin-boosted Autonomous Attack Detection for Vehicular Ad-Hoc Networks

Yagmur Yigit*, Ioannis Panitsas†, Leandros Maglaras*, Leandros Tassiulas†, and Berk Canberk*
* School of Computing, Engineering and The Build Environment, Edinburgh Napier University, United Kingdom
† Department of Electrical Engineering, Yale University, New Haven, CT, USA
Email: {yagmur.yigit, L.Maglaras, B.Canberk}@napier.ac.uk, {ioannis.panitsas, leandros.tassiulas}@yale.edu

ICC 2024 - IEEE International Conference on Communications | 978-1-7281-9054-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICC51166.2024.10622784

***Abstract*—The rapid evolution of Vehicular Ad-hoc NETworks (VANETs) has ushered in a transformative era for intelligent transportation systems (ITS), significantly enhancing road safety and vehicular communication. However, the intricate and dynamic nature of VANETs presents formidable challenges, particularly in vehicle-to-infrastructure (V2I) communications. Roadside Units (RSUs), integral components of VANETs, are increasingly susceptible to cyberattacks, such as jamming and distributed denial of service (DDoS) attacks. These vulnerabilities pose grave risks to road safety, potentially leading to traffic congestion and vehicle malfunctions. Existing methods face difficulties in detecting dynamic attacks and integrating digital twin technology and artificial intelligence (AI) models to enhance VANET cybersecurity. Our study proposes a novel framework that combines digital twin technology with AI to enhance the security of RSUs in VANETs and address this gap. This framework enables real-time monitoring and efficient threat detection while also improving computational efficiency and reducing data transmission delay for increased energy efficiency and hardware durability. Our framework outperforms existing solutions in resource management and attack detection. It reduces RSU load and data transmission delay while achieving an optimal balance between resource consumption and high attack detection effectiveness. This highlights our commitment to secure and sustainable vehicular communication systems for smart cities.**

***Index Terms*—VANETs, ITS, Digital Twin, Cybersecurity in Transportation, Green Communication.**

I. Introduction

In recent years, the advent of Vehicular Ad-hoc NETworks (VANETs) has marked a significant milestone in the evolution of intelligent transportation systems (ITS). These networks, which seamlessly integrate mobile ad hoc networks (MANET), Internet of Things (IoT), and ITS, are at the forefront of revolutionizing road safety and vehicular communication. The critical role of VANETs in reducing traffic accidents and enhancing road safety cannot be overstated, given the alarming statistics from the World Health Organization highlighting the high incidence of road traffic deaths globally [1].

However, the dynamic and complex nature of VANETs introduces significant challenges, particularly in vehicle-to-infrastructure communications [2]. Road Side Units (RSUs), as critical components of VANETs, are often the targets of cyberattacks, including but not limited to jamming and distributed denial of service (DDoS) attacks, which can severely disrupt vehicular communication and pose significant risks to road safety, leading to potential traffic congestion, vehicle malfunctions, and even accidents [3]. This vulnerability underscores the urgency for innovative solutions to safeguard these systems against such threats. The prevalence of connected and autonomous vehicles in modern urban environments underscores the urgent need to address these vulnerabilities due to the rapid evolution of vehicular technology.

In addressing these challenges, our work focuses primarily on vehicle-to-infrastructure communication, explicitly targeting the security of RSUs. We introduce a novel framework that employs digital twin technology and an advanced artificial intelligence (AI) model. The digital twin concept, a digital replica of a physical asset or system, is central to our approach [4]. By creating a digital twin of RSUs, we achieve a real-time, dynamic representation of the physical units, which allows for the meticulous monitoring and analysis of network interactions. This capability is crucial in detecting and mitigating the aforementioned cyber threats, ensuring the integrity and reliability of vehicle-to-infrastructure communications [5]. We referred to digital twins as 'cyber-twins' since we utilized them in the field of cybersecurity. Reducing computational demands and minimizing the average data transmission delay are some of the key areas of research in green VANET technology [6]. Our solution secures communication and contributes to green communications. Our framework focuses on optimizing RSUs' efficiency by reducing their computational demands and minimizing the average data transmission delay. This aligns with the growing emphasis on sustainable and eco-friendly technologies in smart cities. This focus on both security and sustainability places us at the forefront of ITS advancement. Furthermore, our dedication to creating environmentally friendly technologies for smart cities is highlighted by our efforts to reduce energy consumption and extend the lifespan of hardware. The key contributions of this paper include:

- We propose a novel framework tailored explicitly for securing vehicle-to-infrastructure communication in VANETs, utilizing cyber twins and an AI model for efficient threat detection.
- Our approach integrates cyber twins for real-time monitoring, management of vehicular networks, and analysis of RSU performance and security.
- Proposed framework reduces RSUs' computational load, improving hardware longevity and energy efficiency.
- Our solution significantly advances green communica-

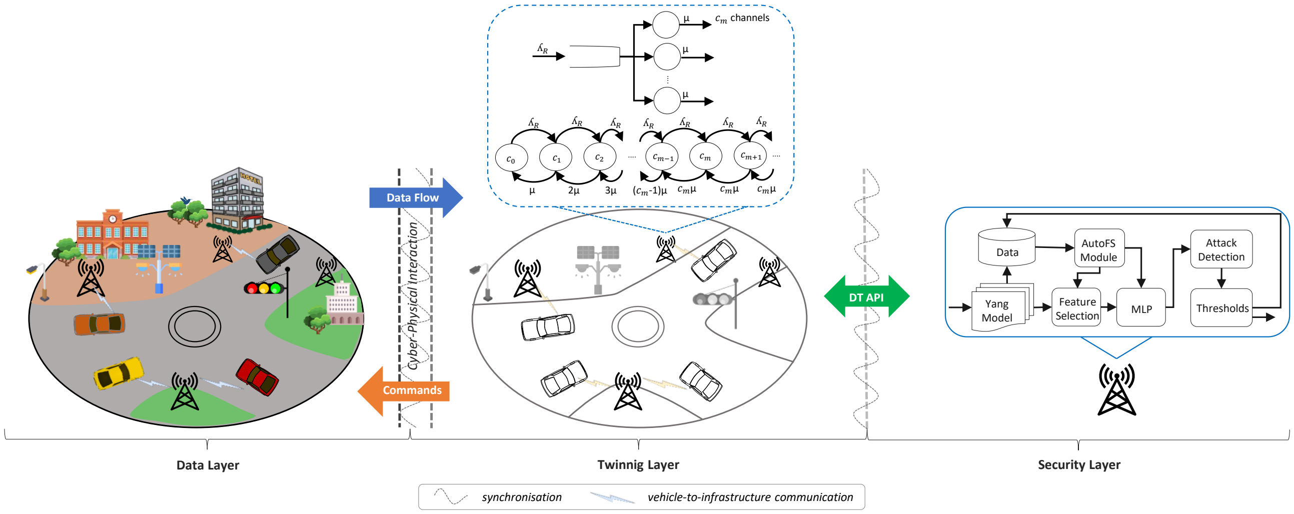

Fig. 1. The proposed architecture.

tions in VANETs by reducing computational demands, minimizing data transmission delays, and contributing to the sustainability of ITS.

Our paper proposes a new approach to enhance vehicle-to-infrastructure communication in VANETs while addressing road safety, sustainability, and security concerns. We use cyber twins and AI models to set a new standard for developing intelligent and secure transportation systems. Our work paves the way for safer and greener smart cities. This work proceeds with an overview of relevant literature in Section II, then delves into the proposed solution in Section III, and evaluates its performance in Section IV. The paper is concluded in Section V.

II. Related Work

This section highlights recent advancements in improving road safety and efficiency in VANETs and their integration into ITS, setting the stage for our novel framework.

Alhaidari *et al.* introduced a simulation method to create the VANET DDoS dataset, encompassing critical VANET features like traffic density and node mobility. However, it remains inaccessible to the public [7]. Bangui *et al.* tackled VANETs' vulnerability to malicious jamming, proposing a data prioritization model enhancing Big Data Analytics' efficiency in jamming detection, a leap forward in real-time anti-jamming applications [8]. Mokhtar *et al.* surveyed VANETs' security, highlighting the challenges due to their mobile, infrastructure-less nature [2]. They emphasized the network's inherent security vulnerabilities, paving the way for innovative solutions. Another notable study introduced a machine learning-based system for real-time identification of malicious nodes in VANETs, achieving high accuracy with random forest and gradient-boosted trees models [9].

Haydari *et al.* developed advanced machine learning methods for intrusion detection in VANETs, targeting sophisticated attacks like DDoS [10]. Their RSU-based non-parametric detection system has the potential for improvement against sporadic attacks. Zhou *et al.* concentrated on enhancing VANET security within ITS for 6G systems, introducing a framework combining identity-based encryption and deep learning, primarily addressing DDoS attack scenarios [11]. Alrehan *et al.* reviewed VANET architectures, advocating for security solutions uniquely tailored to VANET characteristics, diverging from conventional methods [12]. Anyanwu *et al.* focused on a software-defined network integrated VANETs' vulnerability to identify DDoS attacks utilizing a support vector machine (SVM) classifier, a significant step in vehicle security [13]. A novel self-powered, fog-based VANET infrastructure was also proposed, focusing on sustainable and secure communication, including innovative power management and fog clustering strategies for enhanced network resilience [14].

In VANET research, the utilization of digital twin technology has not yet been widely explored. Among the few, Arya *et al.* utilized it for identifying malicious nodes, employing machine learning for practical traffic analysis [15]. Ak *et al.* developed T6CONF, a new framework that enhances IoT communication in smart cities, thereby improving waste management predictions and achieving net-zero waste objectives [16]. Additionally, Hu *et al.* explored the internet of vehicles, forming a digital twin connection between physical and virtual vehicles for real-time traffic prediction, highlighting the potential and challenges in handling extensive, sparse data sets [17].

The studies have highlighted VANETs' immense potential for improving road safety and network security. However, there is a noticeable gap in effectively combining digital twins with AI models to enhance security and environmental sustainability in VANETs. We propose a new framework to secure vehicle-to-infrastructure communication and advance green communication in smart city infrastructures to address this gap.

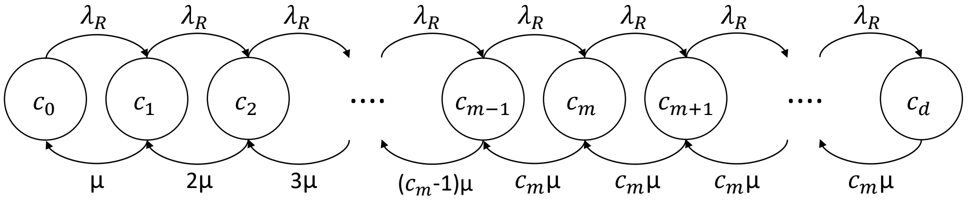

Fig. 2. The state diagram.

III. Proposed System Model for Vehicle-to-Infrastructure Security

Our proposed system is designed to foster a resilient and robust communication framework for vehicles in 6G smart cities, leveraging cyber twins to optimize the computational efficiency of RSUs. This enhances the reliability and stability of the RSUs. Some potential benefits of our system can be:

- Enhanced energy efficiency in RSUs, achieved through reduced computational demands and minimizing the average data transmission delay.
- Extension of hardware lifespan, resulting in economic benefits due to decreased replacement and maintenance needs.
- Greater adaptability of RSUs to emerging technologies, eliminating the need for comprehensive hardware overhauls.

Our system adopts a holistic approach with a three-tiered structure comprising physical-to-virtual and virtual-to-virtual communications between layers. This structure forms a comprehensive cyber-twin framework within VANET. Our system is segmented into three layers: data, twinning, and security, each crucial in ensuring the network's functionality and resilience, as seen in Fig. 1.

A. Data Layer

The Data Layer is the foundational segment of our cyber-twin architecture, primarily focusing on data acquisition and transmission. It integrates vehicles and RSUs, collecting critical data for higher-level simulation and security analysis. Its precision in real-time data representation and communication is crucial for maintaining the integrity and effectiveness of the digital twin simulations.

B. Twinning Layer

This layer is pivotal in creating digital replicas of VANET's physical components. We used queuing theory to model the VANET environment. We have implemented the M/M/m queuing model with a first-in-first-out strategy for efficient data network simulation. The model evaluates the system's state by analyzing communication requests against channel availability, providing insights into average waiting times and queue lengths [18].

In this model, channels are linked to servers, and the system's state is evaluated by comparing the total communication requests against available channels. For the M/M/m queuing model, our key assumptions and parameters are as follows:

- Vehicles share channels equally within a transmission area.
- λ_R denotes the arrival rate of communication requests.
- μ expresses the channel's service rate per request, which is time-dependent.
- c represents the channel states.
- m defines the total number of channels.
- d denotes the total number of vehicles with communication requests.

These parameters feed into the M/M/m model to determine average wait time and queue length metrics. These parameters are crucial in the M/M/m model for assessing the system's efficiency and managing channel requests.

We formulate basic equations using a state diagram in Fig. 2. When the number of vehicle requests c_{di} is less than or equal to the number of available channels c_m (i.e., $c_{di} \leq c_m$), all requests are accommodated immediately. However, if the requests exceed the available channels (i.e., $c_d > c_m$), the system processes requests up to the limit of c_m, and the remaining requests are queued for subsequent processing. There are c_m channels so the probability is increasing $(\mu, 2\mu, 3\mu \ldots c_m\mu)$ until reaching c_mth channel. After the c_mth channel, the leaving of the one request stays the same with probability c_mth.

The utilization factor for this model can be calculated as follows:

$$\rho = 1 - \frac{\lambda_R}{c_m \mu} \tag{1}$$

For zero request state:

$$P_0 = \left[\sum_{c_d=0}^{c_m-1} \frac{(c_m\rho)^{c_d}}{c_d\ !} + \frac{(c_m\rho)^{c_m}}{c_m\ !(1-\rho)} \right] \tag{2}$$

P_{c_d} is the probability of all channels busy in the system:

$$P_{c_d} = \begin{cases} P_0 \dfrac{(c_m\rho)^{c_d}}{c_d\ !}, & c_d \leq c_m \\ P_0 \dfrac{(c_m)^{c_m}(\rho)^{c_d}}{c_m\ !}, & c_d > c_m \end{cases} \tag{3}$$

The probability of arriving request has to wait in the queue (c_m request or more in the system):

$$P_{Q_R} = \sum_{c_d=c_m}^{\infty} P_{c_d} = P_0 \frac{(c_m\rho)^{c_m}}{c_m\ !(1-\rho)} \tag{4}$$

When the channel is the full state, the average number of requests in the queue:

$$N_{Q_R} = \frac{P_{Q_R}\rho}{(1-\rho)} \tag{5}$$

The amount of time spent in the queue, which is the average waiting time in the queue:

$$T_{Q_R} = \frac{P_{Q_R}\rho}{\lambda_R(1-\rho)} \tag{6}$$

The total time in the system, which is the sum of queue time and the service time:

$$T = T_{Q_R} + \frac{1}{\mu} \tag{7}$$

Lastly, we calculated the average number of channel requests in the system as follows:

$$N_R = c_m\rho + \frac{P_{Q_R}\rho}{1-\rho} \tag{8}$$

Data from the twinning layer is transferred to the security layer via a YANG model for robust data transfer. We used the YANG model from previous work [19] and adapted it to VANET.

C. Security Layer

The system's security mechanism is based on our previous research [20]. It includes an AutoFS Module and a Multilayer Perceptron, both essential for effective attack detection.

1) AutoFS Module: This module dynamically selects the most effective Feature Selection (FS) methods under varying network conditions. The system incorporates various techniques such as Recursive Feature Elimination, Backward Feature Elimination, Chi-square, Fisher Score, and ANOVA F-value Selection, adapting to the dynamic nature of network data. Each FS method has a unique approach to feature selection, influencing DDoS detection efficiency. The module identifies the optimal MLP model and FS method based on system performance metrics.

2) Labelling Algorithm: Our labelling method efficiently categorizes data using the expectation-maximization and K-means algorithms, improving precision. The method clusters and labels data to accurately predict attacks, considering their infrequency.

3) Multilayer Perceptron: Our MLP network adapts to continuously changing network data through online learning. It uses a five-layer architecture with relu and softmax activation functions for effective data classification. It constantly updates model weights, ensuring stable performance in a dynamic network environment.

The proposed system model is an adaptive approach to vehicular communication that bolsters security and optimizes performance for smart city infrastructure. It is a pioneering approach to green and secure 6G smart cities.

IV. Performance Evaluation

To test the performance of our proposed system, we used OMNeT++ version 5.1, INET version 3.6, Veins version 4.7, and SUMO version 0.30.0 as the previous work [7]. We utilized Eclipse Ditto, which is a scalable and flexible open-source framework, to create cyber twins of physical entities [21]. Our evaluation focused on two main aspects: the efficiency of cyber twins in RSU resource utilization and the effectiveness of our framework in attack detection.

Firstly, we tested the performance of cyber twins in RSU. Therefore, we check the average resource usage of the system with and without the cyber twin. As seen in Fig. 3, when we employed the cyber-twin in the system, the system utilised the resource more efficiently since we reduced the load of the roadside unit. Integrating the cyber-twin system model resulted in more efficient resource utilization, thereby lightening the RSU's load.

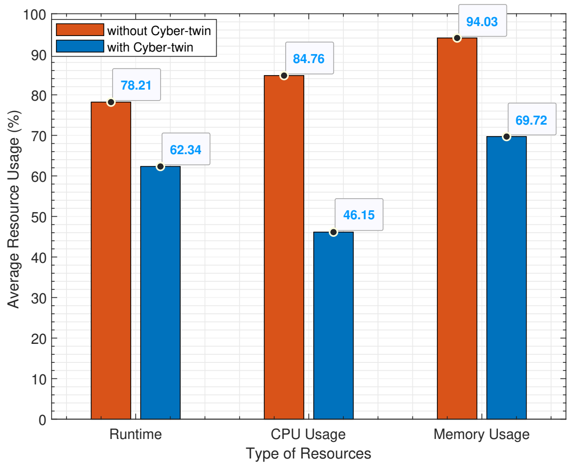

Fig. 3. The average resource usage comparison.

After testing the cyber twin effect of the roadside unit resource performance, we experiment with the attack detection performance of the cyber-twin framework. To this end, we used two datasets. The first dataset is the RF Jamming Dataset [22], which comprises diverse scenarios of RF jamming attacks and interference in VANET. This dataset includes two datasets for two maximum estimated relative speed types. We combined them, adding a new column with the maximum estimated relative speed. The ToN-IoT dataset [23], specifically designed for assessing the reliability and performance of various AI-driven cybersecurity applications, is utilized in our study since Gad *et al.* used this dataset for attack detection in VANET [24]. This dataset is particularly tailored for next-generation IoT and industrial IoT scenarios. However, the current version of the ToN-IoT dataset is not VANET-oriented; therefore, we combine the first dataset's no-attack samples and the ToN-IoT dataset's attack samples. We selectively used a specified number of samples from these datasets to construct Dataset 2. The details of this selection, including the number of samples from each dataset, are meticulously outlined in Table I.

TABLE I
THE SAMPLE DISTRIBUTION IN DATASET 2

Dataset Name (Feature)	Number of Samples
RF Jamming Dataset-1 (No Attack Samples)	1000
RF Jamming Dataset-2 (No Attack Samples)	1000
ToN-IoT Network Dataset (Attack Samples)	400

We compare our solution (PS) with KNN and SVM algorithms since they gave the best result in the following works: [25] and [26], respectively. Table II compares the performance of different methods on the datasets. Our solution outperforms the others.

TABLE II
THE PERFORMANCE COMPARISON OF METHODS

		Precision (%)	F-Measure (%)	Sensitivity (%)
Dataset-1	KNN	95.72	96.28	96.85
	SVM	89.27	91.84	94.58
	PS	98.96	98.99	99.03
Dataset-2	KNN	88.67	88.90	89.14
	SVM	84.67	85.91	87.19
	PS	97.53	98.08	98.64

After that, we examined the performance of our solution in terms of average delay and delivery rate under various data message times.

Fig. 4 indicates that PS is performing significantly better in reducing delay than KNN, approximately 1.41 times, and approximately 1.61 times faster than SVM. In terms of average delivery rate, our solution delivers a stable performance. It is approximately 1.11 times more effective than KNN and about 1.21 times more effective than SVM. As can be seen in Fig. 4, PS has significantly lower delays and higher delivery rates compared to the other two methods.

We also investigate the twinning rate performance according to the system's detection rate and total RAM usage. To this end, we used the dataset 2. We define the twinning rate as follows:

$$\gamma = \frac{\tau}{\sigma} * 100 \tag{9}$$

where γ is the twining rate, σ is the total number of packages in the roadside units in the data layer, and τ is the total number of packages taken to the twinning layer from the data layer.

We explored the relationship between the twinning rate, detection rate, and total RAM usage. Fig. 5 depicts the detection rate and total RAM usage comparison according to the twinning rate. According to the results, we defined the optimum twinning rate range between seventy-six and ninety per cent to minimize the total RAM usage while protecting a high attack detection rate. Thus, we established an optimal range that balances resource consumption with high attack detection efficiency by fine-tuning the twinning rate.

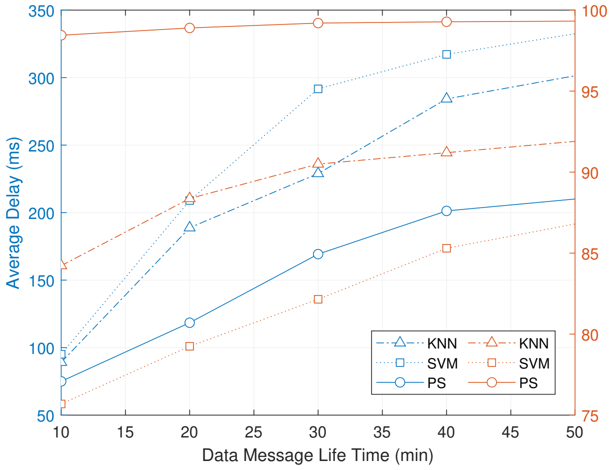

Fig. 4. The comparison of methods regarding the average delay and delivery rate under different data message lifetime.

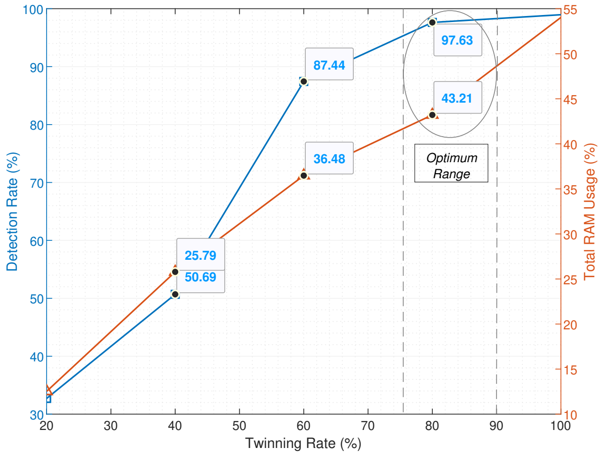

Fig. 5. The detection rate and total RAM usage comparison according to the twinning rate.

In addition to its robust security and efficiency features, our proposed system significantly contributes to green communication practices in 6G smart city infrastructures. The system's advanced cyber twins optimise RSU performance and reduce energy consumption. Moreover, it contributes to green communications by reducing their computational demands and minimizing the average data transmission delay. By efficiently managing data traffic and processing demands, the system minimizes the environmental impact of urban communication networks. This reduction in energy requirements aligns with eco-friendly objectives and diminishes operational costs, making it a sustainable solution for future smart cities. Furthermore, the extended lifespan of hardware components due to reduced strain translates into fewer replacements and maintenance needs, further reinforcing the system's environmentally conscious design. The cumulative effect of these factors underscores our system's role in advancing green communication technology, a critical consideration in the development of sustainable urban environments.

V. Conclusion

Our research has successfully introduced a novel framework that significantly enhances the security of RSUs in VANETs. We have developed a robust real-time vehicular network framework that integrates cyber twins with advanced AI models. The framework adeptly addresses the complexities of VANETs, particularly in vehicle-to-infrastructure communications. Our research findings demonstrate substantial resource utilization and attack detection improvements, which outperform existing solutions. The framework's cyber twins of RSUs help detect and mitigate cyber threats, ensuring communication integrity and reliability. Our framework also contributes to green communications by improving the computational efficiency of RSUs, reducing the average delay of data transmission, and leading to increased energy efficiency and extended hardware durability. It has also achieved an optimal balance between resource consumption and high attack detection effectiveness, with a defined twinning rate range of seventy-six to ninety per cent. These advancements underscore our commitment to developing sustainable, secure, and resilient vehicular communication systems for the future of smart cities. Overall, our framework sets a new benchmark in developing secure and green ITS, addressing security challenges while paving the way for a future of safer and greener smart cities.

Acknowledgment

This work is supported by The Scientific and Technological Research Council of Turkey (TUBITAK) 1515 Frontier R&D Laboratories Support Program for BTS Advanced AI Hub: BTS Autonomous Networks and Data Innovation Lab Project 5239903.

References

[1] W. H. Organization. Global Status Report on Road Safety 2018. [Online]. Available: https://www.who.int/publications/i/item/9789241565684, Accessed Sept. 25, 2023.

[2] B. Mokhtar and M. Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks," *Alexandria Engineering Journal*, vol. 54, no. 4, pp. 1115–1126, 2015.

[3] I. Almomani, M. Ahmed, D. Kosmanos, A. Alkhayer, and L. Maglaras, "An Efficient Localization and Avoidance Method of Jammers in Vehicular Ad Hoc Networks," *IEEE Access*, vol. 10, pp. 131 640–131 655, 2022.

[4] Y. Yigit, L. D. Nguyen, M. Ozdem, O. K. Kinaci, T. Hoang, B. Canberk, and T. Q. Duong, "TwinPort: 5G Drone-assisted Data Collection with Digital Twin for Smart Seaports," *Scientific Reports*, vol. 13, p. 12310, 2023.

[5] Y. Yigit, O. K. Kinaci, T. Q. Duong, and B. Canberk, "TwinPot: Digital Twin-assisted Honeypot for Cyber-Secure Smart Seaports," in *2023 IEEE International Conference on Communications Workshops (ICC Workshops)*, 2023, pp. 740–745.

[6] A. Borah and A. Paranjothi, "Research Issues in False Information Broadcasting Rogue Node Detection for Green VANETs," in *2023 26th International Symposium on Wireless Personal Multimedia Communications (WPMC)*, 2023, pp. 1–6.

[7] F. A. Alhaidari and A. M. Alrehan, "A Simulation Work for Generating a Novel Dataset to Detect Distributed Denial of Service Attacks on Vehicular Ad hoc NETwork systems," *International Journal of Distributed Sensor Networks*, vol. 17, no. 3, p. 15501477211000287, 2021.

[8] H. Bangui, M. Ge, B. Buhnova, and L. H. Trang, "Towards Faster Big Data Analytics for Anti-jamming Applications in Vehicular Ad-hoc Network," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 10, 2021.

[9] K. Rashid, Y. Saeed, A. Ali, F. Jamil, R. Alkanhel, and A. Muthanna, "An Adaptive Real-Time Malicious Node Detection Framework Using Machine Learning in Vehicular Ad-Hoc Networks (VANETs)," *Sensors*, vol. 23, no. 5, p. 2594, Feb 2023. [Online]. Available: http://dx.doi.org/10.3390/s23052594

[10] A. Haydari and Y. Yilmaz, "RSU-Based Online Intrusion Detection and Mitigation for VANET," *Sensors*, vol. 22, no. 19, p. 7612, Oct 2022. [Online]. Available: http://dx.doi.org/10.3390/s22197612

[11] Z. Zhou, A. Gaurav, B. B. Gupta, M. D. Lytras, and I. Razzak, "A Fine-Grained Access Control and Security Approach for Intelligent Vehicular Transport in 6G Communication System," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 9726–9735, 2022.

[12] A. M. Alrehan and F. A. Alhaidari, "Machine Learning Techniques to Detect DDoS Attacks on VANET System: A Survey," in *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, 2019, pp. 1–6.

[13] G. Oluchi Anyanwu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Optimization of RBF-SVM Kernel Using Grid Search Algorithm for DDoS Attack Detection in SDN-Based VANET," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8477–8490, 2023.

[14] Q. I. Ali, "Realization of a Robust Fog-Based Green VANET Infrastructure," *IEEE Systems Journal*, vol. 17, no. 2, pp. 2465–2476, 2023.

[15] V. Arya, A. Gaurav, B. B. Gupta, C.-H. Hsu, and H. Baghban, "Detection of Malicious Node in VANETs Using Digital Twin," in *Big Data Intelligence and Computing*, C.-H. Hsu, M. Xu, H. Cao, H. Baghban, and A. B. M. Shawkat Ali, Eds. Singapore: Springer Nature Singapore, 2023, pp. 204–212.

[16] E. Ak, K. Duran, O. A. Dobre, T. Q. Duong, and B. Canberk, "T6CONF: Digital Twin Networking Framework for IPv6-Enabled Net-Zero Smart Cities," *IEEE Communications Magazine*, vol. 61, no. 3, pp. 36–42, 2023.

[17] C. Hu, W. Fan, E. Zeng, Z. Hang, F. Wang, L. Qi, and M. Z. A. Bhuiyan, "Digital Twin-Assisted Real-Time Traffic Data Prediction Method for 5G-Enabled Internet of Vehicles," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 4, pp. 2811–2819, 2022.

[18] E. Bozkaya and B. Canberk, "Robust and Continuous Connectivity Maintenance for Vehicular Dynamic Spectrum Access Networks," *Ad Hoc Networks*, vol. 25, pp. 72–83, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870514002042

[19] Y. Yigit, K. Huseynov, H. Ahmadi, and B. Canberk, "YA-DA: YAng-Based DAta Model for Fine-Grained IIoT Air Quality Monitoring," in *2022 IEEE Globecom Workshops (GC Wkshps)*, 2022, pp. 438–443.

[20] Y. Yigit, B. Bal, A. Karameseoglu, T. Q. Duong, and B. Canberk, "Digital Twin-Enabled Intelligent DDoS Detection Mechanism for Autonomous Core Networks," *IEEE Communications Standards Magazine*, vol. 6, no. 3, pp. 38–44, 2022.

[21] Eclipse, "Eclipse Ditto Documentation," [Online]. Available: https://www.eclipse.org/hono/docs/, Accessed June. 18, 2023.

[22] D. Kosmanos, D. Karagiannis, A. Argyriou, S. Lalis, Y. Yigit, and L. Maglaras. (2023) RF Jamming Dataset for Vehicular Wireless Networks. [Online]. Available: https://dx.doi.org/10.21227/4zwk-yw78

[23] N. Moustafa. ToN IoT datasets. [Online]. Available: https://ieee-dataport.org/documents/toniot-datasets, Accessed June 21, 2021.

[24] A. R. Gad, A. A. Nashat, and T. M. Barkat, "Intrusion Detection System Using Machine Learning for Vehicular Ad Hoc Networks Based on ToN-IoT Dataset," *IEEE Access*, vol. 9, pp. 142 206–142 217, 2021.

[25] D. Kosmanos, D. Karagiannis, A. Argyriou, S. Lalis, and L. Maglaras, "RF Jamming Classification Using Relative Speed Estimation in Vehicular Wireless Networks," *Security and Communication Networks, Hindawi*, pp. 142 206–142 217, 2021.

[26] G. Oluchi Anyanwu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Optimization of RBF-SVM Kernel Using Grid Search Algorithm for DDoS Attack Detection in SDN-Based VANET," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8477–8490, 2023.