Toward Enhancing Security in Intelligent Transportation: A Simulation-Based Approach

Article *in* IFAC-PapersOnLine · January 2024

DOI: 10.1016/j.ifacol.2024.07.210

5 authors, including:

Wasim A. Ali
Polytechnic University of Bari
14 PUBLICATIONS **117** CITATIONS

SEE PROFILE

Agostino Marcello Mangini
Polytechnic University of Bari
154 PUBLICATIONS **2,209** CITATIONS

SEE PROFILE

Jorge Júlvez
University of Zaragoza
96 PUBLICATIONS **941** CITATIONS

SEE PROFILE

Cristian Mahulea
University of Zaragoza
141 PUBLICATIONS **1,641** CITATIONS

SEE PROFILE

Available online at www.sciencedirect.com

ScienceDirect

IFAC PapersOnLine 58-4 (2024) 156–161

Toward Enhancing Security in Intelligent Transportation: A Simulation-Based Approach ⋆

Wasim A. Ali * **Agostino M. Mangini** * **Jorge Júlvez** **
Cristian Mahulea ** **Maria Pia Fanti** *
* *Polytechnic University of Bari, Via Edoardo Orabona,4, Bari, 70126, Italy (e-mail: wasim.ali,agostinomarcello.mangini,mariapia.fanti@poliba.it).*
** *Aragón Institute for Engineering Research, University of Zaragoza, Zaragoza 50018, Spain(e-mail: julvez,cmahulea@unizar.es)*

Abstract: This study undertakes a comprehensive examination within the dynamic framework of an urban setting, employing the SUMO simulation testbed for the city of Bologna, Italy, as a realistic traffic simulation model. This study uses a hybrid methodology that integrates the SUMO, OMNeT++, and VEINS framework to simulate communication within vehicle networks. The main emphasis is examining the different types of attacks that could happen on VANET network through various messages facilitated by the IEEE 802.11p protocol / WAVE (Wireless Access in vehicular Environments) standard. The primary objective of this simulation-based study is to improve vehicular network security by leveraging the inherent benefits of using WAVE standard messages, applying and analyzing techniques to detect intrusions in the network. We tested our simulation performance by applying a statistical threshold model for anomaly detection on the data generated from the simulation. Although the data was not enough for training, our goal was to test the possibility of simulating various types of attacks to generate big data that machine learning models can train in the future. This study highlights the importance of practical and realistic simulations, highlighting the importance of the IEEE 802.11p protocol and the WAVE standard in vehicular communication.

Keywords: ITS Security, Connected Vehicles, Network simulation, SUMO, VANET.

1. INTRODUCTION

The development of Intelligent Transportation Systems (ITS) and the broader concept of Smart Cities have catalyzed significant advances in urban mobility, introducing disruptive changes. Central to this evolution are Vehicular Ad Hoc Networks (VANETs), which have become a pivotal element in facilitating Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. These networks are instrumental in the design of intelligent and adaptable transportation systems (Mchergui et al., 2022). As a specialized subset of mobile ad hoc networks, VANETs focus on improving inter-vehicle communication, optimizing routing protocols, and fostering a dynamic networking infrastructure (Damaj et al., 2021).

VANETs have attracted considerable interest due to their potential to enhance road safety and traffic efficiency. Research in this domain spans various areas, including broadcasting, Quality of Service (QoS), routing, and security. The integration of network communication in Electric Vehicles (EV) and Autonomous Vehicles (AV) significantly enhances their situational awareness and decision-making capabilities (Marroquin et al., 2019). In VANETs, each vehicle acts as both a wireless receiver and transmitter, relaying data to nearby vehicles or infrastructure. Standard protocols like IEEE 802.11p and IEEE 1609.4 are employed for inter-vehicle communication (IVC), with IEEE 802.11p being an adaptation of IEEE 802.11, tailored for the dynamic and complex environments of VANETs. This protocol is also known as Wireless Access in Vehicular Environment (WAVE).

Dedicated Short-Range Communications (DSRC) is a technology designed for short-range wireless communication, operating within the 5.9 GHz ITS band (5.85–5.925 GHz). It plays a crucial role in improving public and private safety by enabling effective V2I and V2V communications (Kenney, 2011). WAVE, which operates under the IEEE 802.11 standard, utilizes the DSRC band and is based on the IEEE P1609 family of standards. This framework defines the structure, communication model, management, and security aspects of vehicular communications, with key components including Roadside Units (RSUs), Onboard Units (OBUs), and the WAVE interface. The significance of three message types in the context of the IEEE 802.11p protocol in VANETs will be elaborated in Section 3.2.

In VANETs, continuous exchange of messages is vital to sharing crucial information. However, unauthorized access to these data introduces security risks and potential net-

⋆ This work was partially supported by CICYT-FEDER project number PID2021-125514NB-I00 in Spain.

10.1016/j.ifacol.2024.07.210

work vulnerabilities. Current research is focused on improving security through AI-driven anomaly and intrusion detection systems. These systems, deployed in vehicles and roadside units, scrutinize network behavior to identify patterns indicative of security threats, ensuring real-time monitoring and a robust network security strategy.

This research aims to simulate VANET communication protocols, studying WAVE standards, and analyzing message exchanges to bolster vehicle security and detect attacks using AI and Machine Learning (ML) tools. The approach involves integrating network and traffic simulations into a unified framework, enabling the simulation of real networks, vehicle communications, WAVE message analysis, and the development of security solutions based on simulation data. Additionally, it is important to note that this study is a stepping stone toward a more comprehensive investigation in our future work. Subsequent extensions of this work will delve into further details regarding the methodology and results, providing a more thorough understanding of VANET security and communication protocols.

A case study was conducted using the Simulator of Urban MObility (SUMO) to model vehicle traffic, specifically focusing on the real traffic dynamics of the Pasubio region of Bologna in Italy, as per a previous study by Bieker et al. (2015). Additionally, the OMNeT++ software was used to simulate communication and network protocols (Varga and Hornig, 2010), with the VEINS framework integrated into OMNeT++ to simulate the vehicular environment, linking traffic and network simulations into a cohesive model that accurately represents VANETs.

The sections of the paper are organized as follows. Section 2 provides a general description of VANET security. Section 3 presents the IEEE 802.11p (WAVE) protocol. Section 4 describes simulation tools. Section 5 proposes a case study and discusses the study results, and Section 6 draws conclusions and considers future work.

2. VANET SECURITY

VANETs enable vehicles to communicate wirelessly, improving road safety and traffic efficiency. Enabled by technologies like IEEE 802.11p, VANETs facilitate real-time data exchange among vehicles, enabling collision warnings and traffic management features. Although these networks facilitate communication and data exchange between vehicles and network components, there are significant challenges in maintaining the integrity and security of the data (see Fig. 1 as an example of VANETs application).

Securing VANETs is imperative to prevent potential threats and ensure the trustworthiness of vehicular communication. Encryption techniques protect the integrity and confidentiality of the data, while authentication mechanisms validate the identities of participating entities. Anomaly detection systems improve security by identifying unusual patterns of behavior. Numerous studies explore VANET security challenges and solutions. In particular, a survey on AI techniques for VANET security has been presented in (Mchergui et al., 2022). The work (Eze et al., 2016) discusses advances and challenges in VANETs, including security aspects. Raja et al. (2020) proposed

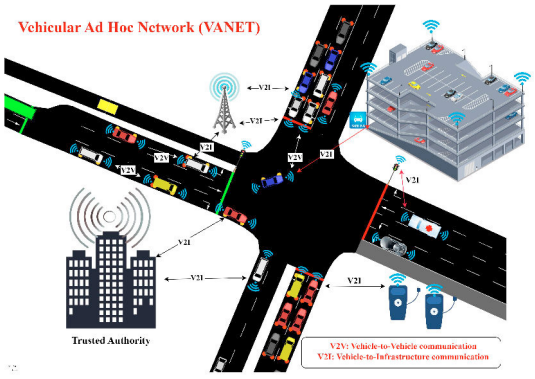


Fig. 1. Vehicular Ad Hoc Networks (VANETs)

a Secure and Private-Collaborative Intrusion Detection System (SP-CIDS) to detect network attacks and mitigate security concerns. (Ali et al., 2024) developed a multi-level Intrusion Detection System based on ML algorithms to detect multiple types of attacks on VANET. Moreover, Liang et al. (2019) introduced a novel IDS that can mitigate message congestion and accurately detect attacks using VANET. In previous studies, VANET was used as a dynamic wireless network to establish vehicle communication, and the system was built to detect intrusions and anomalies. ML and AI techniques were used in these models based on ready-made data from previous studies or government data that were requested and extracted. The lack of integrated simulation models for traffic and networking motivated us to conduct this study to obtain realistic data on which the researcher can rely instead of considering data from other studies. We succeeded in building the simulation model with SUMO and Omnit++, using the WAVE protocol in the model, and analyzing the different messages that are exchanged between vehicles in order to find anomalies.

3. THE IEEE 802.11P (WAVE) PROTOCOL

3.1 Dedicated Short-Range Communications (DSRC)

DSRC is a communication service that operates in the 5.9 GHz frequency band. It is designed for specific wireless communication technology for short-range communication between devices. This facilitates direct short-to-medium-range communication between vehicles within approximately 300 meters (Kenney, 2011). Essentially, an extension of Wi-Fi, DSRC serves as a breakthrough, enabling direct device-to-device data transmission without intermediaries, which is particularly beneficial in areas lacking telecommunication infrastructure. DSRC technology is often used in vehicular networks for V2V and V2I communication.

3.2 Wireless Access in Vehicular Environments (WAVE)

The IEEE 802.11p protocol, also called the Wireless Access in Vehicular Environments (WAVE) protocol, is an essential standard in vehicular communication (Arena et al., 2020) that operates in the 5.9 GHz frequency band. It was developed by the Institute of Electrical and Electronics Engineers (IEEE) to meet the distinct requirements of

VANETs. The WAVE system offers a complete framework for enabling DSRC among vehicles, thus facilitating direct and reliable information exchange at distances ranging from short to medium. Its adoption signifies a fundamental step in improving road safety, traffic efficiency, and intelligent transportation systems.

In the context of the IEEE 802.11p protocol used in VANETs, three main types of messages play crucial roles. The first message is the Basic Safety Message (BSM), the second is the WAVE Short Message (WSM), and the last is the WAVE Service Advertisement (WSA). BSM messages, alternatively referred to as "Beacon messages", are generally sent frequently with basic information about vehicles, such as identification, route, location, etc. In contrast, WSM messages include BSMs and send road conditions and requests such as route requests (RRQ), authentication certificates, and network verification. The WSM format is developed to enhance the efficacy of WAVE Short Message Protocols (WSMP). WSM communications are transmitted only when necessary and not periodically (Vertal et al., 2022). The third type of WSA message, introduced by Vendor Specific Action (VSA), is used among the organization network to send service advertisements. WSA frame can announce the availability of some services, alerting in some cases, parking, commercial purposes, etc. BSM, WSM, and WSA are transmitted to all communication channels or can be transmitted to a specific service channel.

4. SIMULATION TOOLS FOR VANET

Simulation tools play an important role in understanding and optimizing network dynamics. VANETs operate in diverse real-world environments. The simulation replicates these environments, incorporating road structures, traffic patterns, and urban layouts. This ensures a realistic representation to evaluate the network performance. Simulation tools facilitate scalability by comprising many vehicles and infrastructure elements in VANET. Communication protocols such as IEEE 802.11p can be enabled and evaluated in such simulation environments. Finally, security analysis is a critical issue for VANET. Before implementing security measures in the real world, researchers can evaluate vulnerabilities, test countermeasures, and model and analyze security systems using simulation tools. Researchers use different tools for research purposes to evaluate vehicular networks, including SUMO, UNITY, OMESON, NS3, NS2, OMNeT++, OPNET, VISSM, and VISUM. In this study, we use the software and tools described in the following subsections. Many reasons drive the choice to use SUMO with OMNeT++ in this study. SUMO is designed to simulate complex traffic scenarios, crucial for studying realistic traffic. Moreover, OMNeT++ is widely used for network simulations and allows researchers to model traffic and network communication in a unified simulation environment. The presence of a VEINS framework within OMNeT++ is the key factor to this integration. It also provides the ability to simulate VANET protocols, which may not be available in other simulation tools. Finally, all these tools are open-source tools where we can modify and extend them based on our specific simulation requirements.

4.1 SUMO, OMNeT++ and VEINS

SUMO is a powerful microscopic traffic simulator that simulates realistic automotive dynamics in urban environments. Due to its microscopic methodology, the system constructs individual models for each vehicle, capturing small and complex details of their movements. Integration of the software with other simulators, such as OMNeT++, provides researchers with a comprehensive platform for VANET simulations. Researchers frequently leverage SUMO's capabilities to analyze and optimize VANET behavior in urban scenarios, making it an important software in vehicular network research.

OMNeT++, a discrete-event simulation toolkit, is essential for network simulations. It is easier to model complex VANET communication protocols and behaviours with OMNeT++ due to its adaptability and ability to simulate different scenarios. Oment++ has provided several frameworks that can be integrated into the software so that the researcher can simulate all types of networks, including LTE and 5G, and VEINS framework dedicated to the vehicular environment. The research community prefers it because of its robust and extendable C++ architecture, which helps them investigate communication dynamics in complicated networks such as VANET.

VEINS is an open source framework built to simulate vehicular networks in OMNeT++. It integrates seamlessly with SUMO through the Traffic Control Interface (TraCi) (Wegener et al., 2008) to realistically represent urban and suburban mobility. VEINS supports multiple VANET communication protocols such as IEEE 802.11p, AODV, UDP, TCP, etc. Its accessibility helps researchers study vehicle communication, and the integration between VEINS and SUMO makes VANET simulations more realistic and accurate.

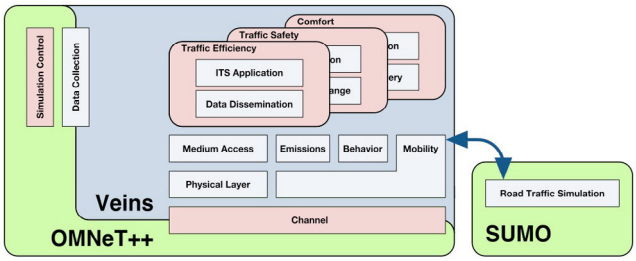


Fig. 2. VEINS Architecture with SUMO and OMNeT++

We use those simulators and tools because we believe that they can provide realistic emulation and let us focus on the study objectives at hand rather than side concerns such as networks, signals, and traffic. Fig. 2 shows the integration between the tools and how VEINS can be connected to SUMO and OMNeT++. SUMO generally provides authentic mobility patterns and integrates real-world road networks and traffic conditions into our simulations. On the other hand, OMNeT++ facilitates the modeling of communication protocols, adding an additional layer of realism to the exchange of messages in V2V and V2I communications. The integration process encounters challenges arising from the distinct paradigms employed by SUMO and OMNeT++. Real-time communication between these tools is enabled through the TraCI interface, which is

embedded in the VEINS framework and represented in the TraCiDemo11p.cc and TraCiDemo11p.h files. We built our integration script and scenario functions within C++-based TraCiDemo11p files to execute code seamlessly in OMNet++ as shown in Fig. 3. Furthermore, making these different simulations work together requires adjusting the parameters, data formats, nodes, RSUs, and communication setup, and all these parameters are adjusted in the omnet.ini file as shown in Fig. 4. Despite integration challenges, our simulation successfully handled these intricacies, proving its strength in accurately representing different attack scenarios.

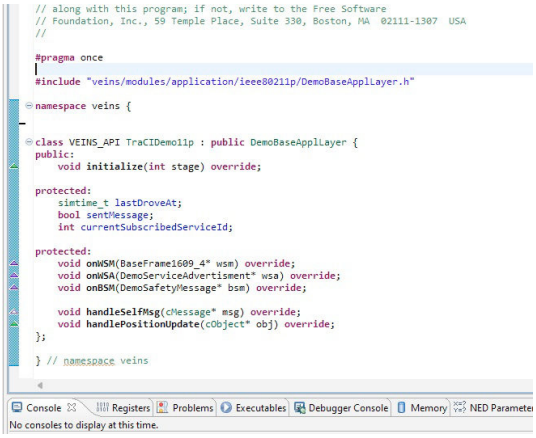


Fig. 3. TraCiDemo11p.h implementation in OMNeT++

Fig. 4. Sample of parameters setup in omnet.ini file

Implementing the IEEE 802.11p protocol and the WAVE standard enables modeling specific attack scenarios, such as evading vehicles from charging stations and DDOS attacks. The flexibility of these tools has been demonstrated in the ability to simulate different types of attacks and analyze the messages exchanged between vehicles through the WAVE protocol to identify malicious traffic. The amalgamation of SUMO, OMNeT++, and VEINS provides a robust platform that harmoniously blends scalability and realism to help implement security solutions for vehicular networks.

5. CASE STUDY

5.1 Simulation Description

In the proposed study, we used a realistic traffic simulation scenario from Bologna, specifically focusing on the Pasubio area, during the city's peak traffic hour (8:00 - 9:00 a.m.) as shown in Fig. 5. The simulation incorporates additional datasets provided by the municipality of Bologna, including the positions and plans of the traffic lights, the positions of the inductive loops and measurements, among others. Initially, the scenario featured 3700 conventional vehicles. However, to align with our objective of simulating the behavior of electric vehicles (EV) in the network, we adapted the vehicle specifications in SUMO to represent electric vehicles and scaled the number down to 500. This adjustment aims to create a more realistic representation of EV communication within the network. The authenticity of our simulated traffic scenario is further enhanced by integrating real traffic data from Bologna into the OMNeT++ model.

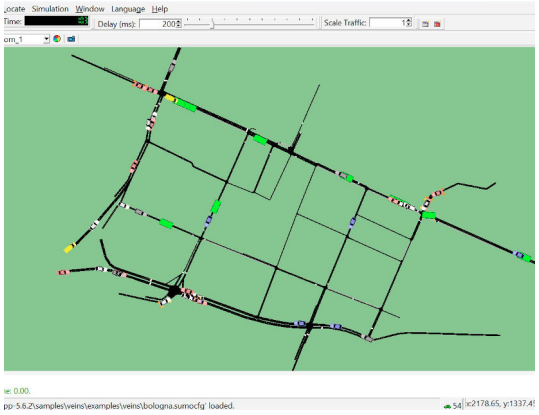


Fig. 5. Realistic traffic environment in Bologna city.

For the network model in OMNeT++, we based our design on the SUMO simulation and meticulously defined the network components. As depicted in Fig. 6, two Road Side Units (RSUs) were strategically positioned to cover a large area of the map. Additionally, we incorporated three charging stations on the map. These stations are capable of sending and receiving beacons from RSUs, EVs, and other objects within the network's range, thereby enhancing the simulation's realism and applicability.

5.2 Attacks Simulation

In our simulation, as illustrated in Fig. 6, we introduced two vehicles designated as attackers. These attackers, who have gained unauthorized access to the network through fake identities or other hacking methods, are positioned at fixed locations to initiate their attacks at varying intensities.

The first attacker, represented in red, has a relatively mild impact on the network. Their strategy involves exploiting the WAVE protocol's WSA messages, which are

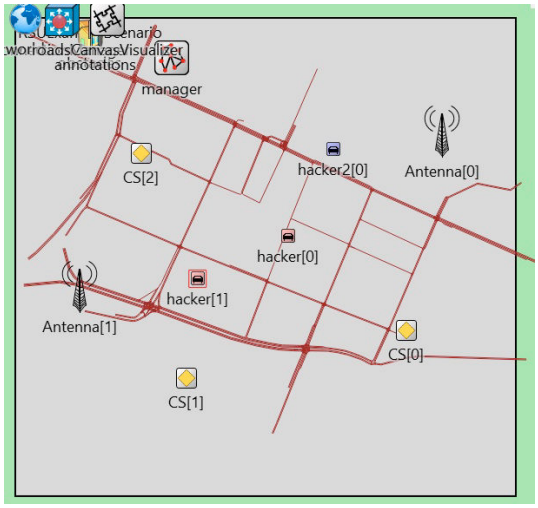
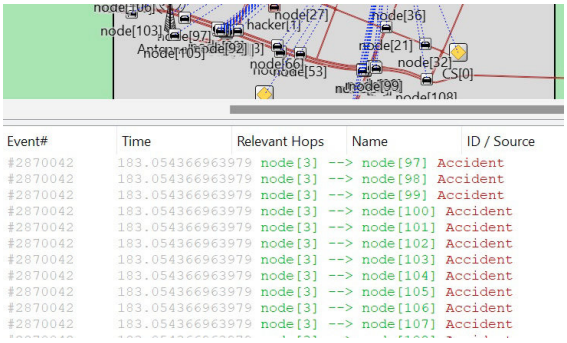


Fig. 6. RSU and attackers position in OMNeT++

typically used for network advertisements. The attacker sends false alerts about an accident in a specific location to neighboring vehicles every 60 seconds, as shown in Fig. 7. This deliberate dissemination of misleading information deceives nearby vehicles, forcing them to alter their routes outside designated charging stations. Consequently, this orchestrated misinformation campaign disrupts the normal flow of traffic and compromises the efficiency of vehicular navigation systems, potentially leading to congestion and delays in reaching intended destinations.



Event#	Time	Relevant Hops	Name	ID / Source
#2870042	183.054366963979	node[3] --> node[97]	Accident	
#2870042	183.054366963979	node[3] --> node[98]	Accident	
#2870042	183.054366963979	node[3] --> node[99]	Accident	
#2870042	183.054366963979	node[3] --> node[100]	Accident	
#2870042	183.054366963979	node[3] --> node[101]	Accident	
#2870042	183.054366963979	node[3] --> node[102]	Accident	
#2870042	183.054366963979	node[3] --> node[103]	Accident	
#2870042	183.054366963979	node[3] --> node[104]	Accident	
#2870042	183.054366963979	node[3] --> node[105]	Accident	
#2870042	183.054366963979	node[3] --> node[106]	Accident	
#2870042	183.054366963979	node[3] --> node[107]	Accident	

Fig. 7. First attack: broadcast fake accident advertisement

Although this attack does not completely incapacitate the network, it disrupts the charging reservation system and the coordination between vehicles and charging stations. Consequently, many vehicles miss out on their opportunity to secure a charging slot at the desired time, potentially allowing the attacker to monopolize charging availability. Furthermore, such attacks can undermine the credibility of service providers and the reliability of their services, leading to significant losses due to the compromised reservation system.

The second attacker, shown in blue in Fig. 8, poses a more serious threat to the network. Their objective is to execute a Denial of Service (DoS) attack, aiming to disrupt the network and deny service to all antennas and vehicles. DoS attacks in VANETs constitute malicious attempts to overwhelm communication channels, resulting in unavailability or degradation of services. These attacks mainly focus on the communication infrastructure, exploiting vulnerabilities to hinder the exchange of crucial traffic and safety information. Such disruptions undermine the reliability of communication among vehicles and infrastructure, potentially leading to hazardous road conditions and traffic congestion. In our case study, the attacker floods the RSUs with 1000 WSM messages per second, far exceeding the network capacity of 300 messages per second. This deluge of messages overloads the communication channel, leading to the shutdown of the RSUs and rendering the entire network inoperable.

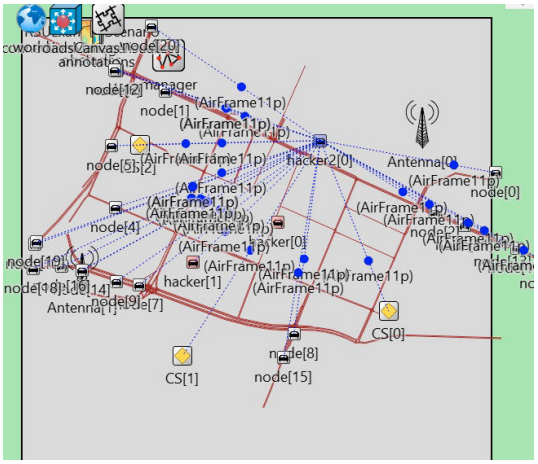


Fig. 8. Second attack: DDoS attacks on the entire network

5.3 Discussion

In our study, we observed that hackers, having gained legitimate access to the network, could exploit WAVE message broadcasting. They misused this access by flooding the WSM with numerous requests, such as RRQ, verification certificates, and permissions, or by using WSA to disseminate false advertisements. This form of broadcasting, being a standard mode of communication within the VANET network, poses a challenge in distinguishing legitimate operations from malicious activities.

Due to the limited duration of our simulation and the number of vehicles involved, the simulation yielded a relatively small unlabeled dataset. Consequently, traditional machine learning techniques were not feasible to evaluate our simulation. Instead, we develop a simple Python script based on threshold analysis to identify anomalies in the dataset.

The results of our simulations, as shown in Table 1, are credible and applicable, making a significant contribution to the field of VANET simulation, particularly in the realm of network security. After running the simulation for 3600 seconds, we were able to capture critical data, including the number of generated WSMs and WSAs, as well as packets sent by the injected attackers. The data highlight the extensive number of DoS attacks initiated by Hacker Type2 and the volume of misleading messages propagated by Hacker Type1. Additional metrics such as TimesIntoBackoff, Channel Busy, and TotalBusyTime were also recorded, providing information on network behavior under attack conditions.

In the future, we will extend the duration of our experiments and work with larger datasets and intend to

Table 1. Simulation Results

	Hacker Type1	Hacker Type2	Antena
generatedWSMs	0	3599900	0
generatedWSAs	2000	0	0
SendPackets	840	359985	3600
SlotsBackoff	1207	5400510	5312
Channel Busy	1.1433333E-5	0.01049956	1.05E-4
totalBusyTime	0.04116	37.798	0.378
totalTime	3600s	3600s	3598s

use ML techniques to detect potential malicious attacks and anomalies across a broader spectrum. This extension will enhance our approach's scalability and strengthen our findings' reliability. We also plan to evolve this model to more closely mirror real-world conditions. This will involve incorporating a mixture of regular and electric vehicles, extending the duration of the simulation, and introducing a wider range of attack types. Our focus will be replicating real-life events and potential faults within the simulation environment. This approach is expected to generate a larger dataset, suitable for applying machine learning algorithms to detect and analyze network intrusions and attacks more effectively.

6. CONCLUSION

In this study, we have successfully developed and implemented a comprehensive simulation framework that integrates the realistic traffic scenarios of SUMO (specifically, the Bologna model) with the advanced network simulation capabilities of OMNeT++ and VEINS. This integration has been instrumental in evaluating the impact of various cyber attacks on Vehicular Ad Hoc Networks (VANETs). Our work significantly enhances the understanding of the WAVE protocol's mechanisms, highlighting the critical need for robust and resilient security systems within VANETs.

The central element of our study was the exploration of vulnerabilities in the IEEE 802.11p and WAVE standards. We demonstrate this through the simulation of two different types of network attackers. The first type of attacker exploited the features of the WAVE message to disrupt the charging reservation system, sending misleading WSA messages that adversely affected vehicle routing and compromised the reliability of the service provider. The second type of attacker launched a Denial of Service (DoS) attack, flooding Road Side Units (RSUs) with an overwhelming number of WSM messages, ultimately leading to complete network breakdown. The high degree of realism in our traffic simulation, mirroring the intricate traffic patterns of Bologna, lends substantial credibility to our experimental findings. It underscores the urgency of analyzing WAVE protocol messages to develop more sophisticated and impenetrable security mechanisms in VANETs.

Looking ahead, our research will pivot towards further enhancing the realism and complexity of our simulation scenarios. We plan to extend the duration of our simulations and introduce a broader spectrum of attack scenarios. This expansion is not just a step towards creating a more comprehensive simulation environment; it is a strategic move designed to produce a rich dataset. This dataset will be critical for the application of advanced machine learning techniques, which we anticipate will significantly contribute to ongoing efforts to improve VANET security. Through this future work, our aim is to bridge the gap between theoretical research and practical, real-world applications, ultimately leading to safer and more secure vehicular networks.

REFERENCES

Ali, W.A., Roccotelli, M., Boggia, G., and Fanti, M.P. (2024). Intrusion detection system for vehicular ad hoc network attacks based on machine learning techniques. *Information Security Journal: A Global Perspective*, 1–19.

Arena, F., Pau, G., and Severino, A. (2020). A review on ieee 802.11 p for intelligent transportation systems. *Journal of Sensor and Actuator Networks*, 9(2), 22.

Bieker, L., Krajzewicz, D., Morra, A., Michelacci, C., and Cartolano, F. (2015). Traffic simulation for all: a real world traffic scenario from the city of bologna. In *Modeling Mobility with Open Data: 2nd SUMO Conference 2014 Berlin, Germany, May 15-16, 2014*, 47–60. Springer.

Damaj, I.W., Serhal, D.K., Hamandi, L.A., Zantout, R.N., and Mouftah, H.T. (2021). Connected and autonomous electric vehicles: Quality of experience survey and taxonomy. *Vehicular Communications*, 28, 100312.

Eze, E.C., Zhang, S.J., Liu, E.J., and Eze, J.C. (2016). Advances in vehicular ad-hoc networks (vanets): Challenges and road-map for future development. *International Journal of Automation and Computing*, 13, 1–18.

Kenney, J.B. (2011). Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7), 1162–1182.

Liang, J., Chen, J., Zhu, Y., and Yu, R. (2019). A novel intrusion detection system for vehicular ad hoc networks (vanets) based on differences of traffic flow and position. *Applied Soft Computing*, 75, 712–727.

Marroquin, A., To, M.A., Azurdia-Meza, C.A., and Bolufé, S. (2019). A general overview of vehicle-to-x (v2x) beacon-based cooperative vehicular networks. In *2019 IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX)*, 1–6. IEEE.

Mchergui, A., Moulahi, T., and Zeadally, S. (2022). Survey on artificial intelligence (ai) techniques for vehicular ad-hoc networks (vanets). *Vehicular Communications*, 34, 100403.

Raja, G., Anbalagan, S., Vijayaraghavan, G., Theerthagiri, S., Suryanarayan, S.V., and Wu, X.W. (2020). Spcids: Secure and private collaborative ids for vanets. *IEEE Transactions on Intelligent Transportation Systems*, 22(7), 4385–4393.

Varga, A. and Hornig, R. (2010). An overview of the omnet++ simulation environment. In *1st International ICST Conference on Simulation Tools and Techniques for Communications, Networks and Systems*.

Vertal, D., Baronak, I., and Hosek, J. (2022). Options to broadcast information in vanet. *Advances in Electrical and Electronic Engineering*, 20(2), 185–192.

Wegener, A., Piórkowski, M., Raya, M., Hellbrück, H., Fischer, S., and Hubaux, J.P. (2008). TraCI: an interface for coupling road traffic and network simulators. In *11th communications and networking simulation symposium*, 155–163.