Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Smart detection of denial of service (DoS) attacks in internet of vehicles (IoV) networks

Maha Helal [1, *], Mohammed Bakhamis [1], Mousa Al-Akhras [2], Samer Atawneh [1], Ibrahim Al-Oqily [3], Tariq Kashmeery [4]

[1]*College of Computing and Informatics, Saudi Electronic University, Riyadh, Saudi Arabia*
[2]*King Abdullah II School of Information Technology, The University of Jordan, Amman 11942, Jordan*
[3]*Prince Al-Hussein Bin Abdallah II for Information Technology, The Hashemite University, Zarqa 131333, Jordan*
[4]*College of Computing, Umm Al-Qura University, Makkah, Saudi Arabia*

ARTICLE INFO

Article history:
Received 29 May 2024
Received in revised form
28 September 2024
Accepted 19 October 2024

Keywords:
Smart cities
Internet of things
Internet of vehicles
Denial of service
Honeypot strategy

ABSTRACT

Smart cities are receiving increasing attention because of their potential to improve quality of life. Roads and transportation systems have seen significant improvements, particularly in terms of safety. Technologies like the internet of things (IoT) have introduced new features and services for both drivers and governments to reduce road risks and manage transportation more efficiently. Vehicles can now connect to either self-organized or public networks to share information about incidents and road conditions. Access to the Internet and cloud services further enhances these systems by enabling real-time interactions with data collected from various sources, such as other vehicles and road signs. This has led to the development of a new concept called the internet of vehicles (IoV), where vehicles and road objects communicate with each other, and connect to the Internet and services like cloud or fog computing to process large amounts of data. However, implementing IoV comes with challenges, particularly related to security and privacy, which could put road users at risk. One major threat is a denial of service (DoS) attack, which can disrupt these networks. This paper presents a smart detection system that ensures secure communication between nodes, such as vehicles and road objects. To counter DoS attacks, the system also introduces a "honeypot" strategy, which can be used by government vehicles or road objects. The results show that the proposed solution is practical and can be applied in real-world scenarios.

1. Introduction

Today, the concept of the smart city is widely implemented in modern countries, aiming at improving people's lives and ensuring a high level of safety (Gracias et al., 2023). One of the important aspects of smart cities is the introduction of technology to improve transportation and road safety. This effort has resulted in the creation of new technological systems known as intelligent transportation systems (ITS). These systems are used to ensure the efficient monitoring and control of transportation networks. An ITS is intended to make use of the following components of a network: (1) a Vehicle Subsystem, such as the Global Positioning System (GPS), radio frequency identification (RFID) reader, on-board unit (OBU), communication unit, and ITS monitoring unit; (2) Station Subsystems, such as roadside equipment; and (3) Security Subsystems to ensure the reliability, availability, efficiency and security of the transport system (Panigrahy and Emany, 2023).

Similarly, the internet of things (IoT) is a growing technology platform that is widely dispersed through an interconnected network of smart and autonomous devices aimed at increasing productivity, performance, and profitability using predictive analytics and big data technologies (Rose et al., 2015). The physical business environment has been digitized by IoT into an advanced and smart form of organization. Conceptually, IoT aims to link every item independent of its location, time, and motion across error-free networks, resulting in more agile manufacturing operations and successful stakeholder collaboration (Baldini et al., 2018).

* Corresponding Author.
Email Address: mhelal@seu.edu.sa (M. Helal)
https://doi.org/10.21833/ijaas.2024.11.004
Corresponding author's ORCID profile:
https://orcid.org/0000-0002-3834-4410

Industrial businesses are gaining traction via a broad spectrum of strategic gains across multiple technologies, such as robotics, autonomous vehicles, mobile devices, and IoT platforms (Kamble et al., 2019).

Like the concept of IoT, the Internet of Vehicles (IoV) is a network to improve road safety and driving conditions, whereby vehicles, road signs, and other objects can connect with each other to handle road hazards (Priyan and Devi, 2019). In addition, IoV networks reinforce ITS. The architecture of IoV networks is divided into four layers: an environment-sensing and control layer, an application layer, a network access and transport layer, and a coordinative computing control layer (Sharma and Kaushik, 2019). Fig. 1 presents the structure and layers of IoV networks and Vehicular Ad Hoc Networks (VANETs) graphically, where different types of vehicle networks are shown, such as vehicle-to-vehicle (V2V), vehicle-to-roadside units (V2R), vehicle-to-infrastructure (V2I), vehicle-to-sensors (V2S), and vehicle-to-personal devices (V2P). Fig. 1 also presents the concept of introducing cloud computing.

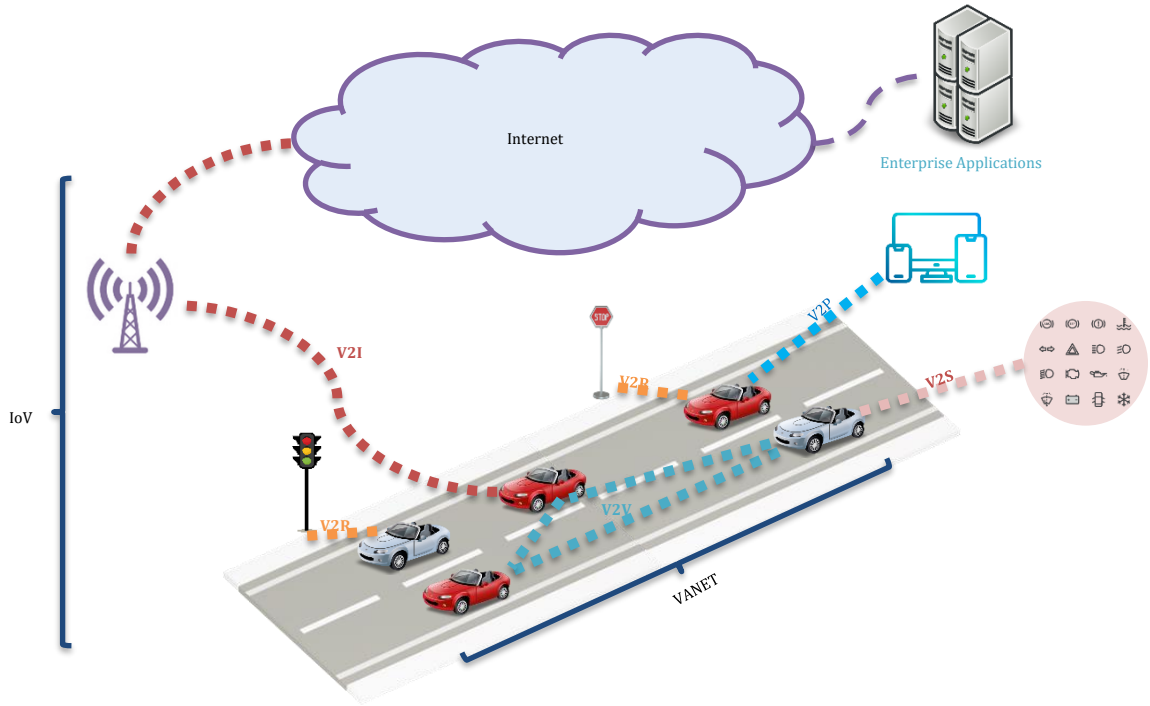


Fig. 1: IoV and VANET structure and layers

As a part of vehicle networks (or IoV), vehicles can form a network that allows moving vehicles to connect with each other. In these networks, with a short transmission range of 100–300 meters, communication is carried out between vehicles and roadside units (RSUs) or vehicle-to-vehicle. Such a network does not have a fixed infrastructure and can be viewed as a special form of mobile ad hoc network (MANET). It is known as a VANET and allows vehicles to send and receive messages from each other as well as from RSUs for the purpose of being aware of their surroundings (Surutkar and Jadhav, 2024). Regardless of its security and privacy limitations, VANETs are intended to enhance road safety and the driving experience (AlMarshoud et al., 2024). VANETs may, for example, provide certain safety-related services, such as reporting hazardous road conditions, providing information on road conditions, and offering car accident alerts and cooperative driving provisions. VANETs are self-organizing networks that enforce network functionality. Vehicles exchange messages with each other, which include information about road traffic and weather conditions, as well as accident- or incident-related location-based information about routes that may be blocked. Furthermore, VENETs could enable vehicles to link to networks, infrastructure, people, and the Internet, leading to the advancement of a universal IoV paradigm (Quyoom et al., 2015).

IoV and VANET technologies seem close to each other due to their shared goal of improving the overall roadside driving experience and reducing road injuries, but, at the same time, there are different criteria that can distinguish the two networks. Contreras-Castillo et al. (2017) and Sharma and Kaushik (2019) discussed the main differences between these networks. Their findings are summarized in Table 1.

New security challenges arise with any new technological application, especially computer and network applications. In modern times, any network is susceptible to security attacks, and IoV is no exception. In addition to the benefits of implementing IoV, several challenges arise, particularly in routing messages between objects (Obaidat et al., 2020). To provide a secure connection, network availability must always be achieved since the availability of the network is essential when a node sends any life-critical

information to other nodes. In this respect, network availability is exposed to many types of attacks. Denial of Service (DoS) is the most notorious of such attacks and is inevitable since the data packets used in it are legitimate packets, unlike other security attacks.

Table 1: Summary of the differences between IoV and VANETs

Parameter	VANET	IoV
Goal	Improve traffic safety to avoid casualties and enhance traffic effectiveness	Enhance traffic safety, effectiveness and commercial infotainment for passengers to improve the driving experience
Communication types	V2V and V2I	V2V, V2R, V2I, V2S, and V2P
Network connectivity	Composed of singleton network architecture that restricts their use	Uses radio, Wi-Fi, 4G/LTE and satellite networks
Decision making	Intelligent decisions are not possible	Intelligent decisions are possible based on AI, big data, and data mining computations
Cloud computing	Not supported due to unreliable Internet connectivity and limited data size	Supported due to the presence of vast real-time traffic information
Data size	Limited data due to local information and non-collaboration	No limitation as a vast amount of data can be generated in real time

IoV has improved transportation systems by enhancing road safety and traffic efficiency. However, various challenges still exist that are not desirable in modern transportation systems (Alalwany and Mahgoub, 2024). It is, therefore, crucial to ascertain the status of the existing security solutions and the problems they pose.

1.1. Main contribution of the research

This research proposes a smart security solution for IoV networks to detect DoS attacks and malicious messages that might be propagating through the IoV network. As part of the contribution, the proposed solution has been simulated to ensure the validity and suitability of its application in real-world scenarios.

The remainder of the paper is organized as follows: Section 2 investigates the literature and similar work, while Section 3 outlines the materials and methods used. Section 4 presents the experimental results and related discussion. Section 5 concludes the paper and highlights future research directions.

2. Literature survey

This section reviews previous research conducted in the field of IoV, explaining the difference between IoV and VANETs. It also distinguishes between different types of attacks and existing solutions in IoV networks.

There are many different technologies, facilities, and standards that need to be incorporated into IoV. The need for data protection would, however, seem to be one of the most crucial aspects that need to be addressed, especially as the number of vehicles on the roads is increasing. As reported by many researchers, IoV has several security and privacy vulnerabilities which compromise its reliability, efficiency, and overall use (Contreras-Castillo et al., 2017; Bagga et al., 2020; Ali et al., 2021; Kumar et al., 2024). As a result, IoV networks are extremely susceptible to many types of cyberattacks (Gupta et al., 2020).

For example, malicious individuals can exploit weak link points and manipulate vehicular data streams, which can lead to devastating consequences. Once the data system of a vehicle has been exploited, access to various vehicle components will be under the control of these malicious attackers. The level of danger depends on the type of attack. Disrupting the communication of a vehicle or sensors would involve a more complicated and sophisticated attack than one designed simply to collect information (Contreras-Castillo et al., 2017). In all cases, the danger posed is significant, and a security breach may have serious repercussions for drivers, passengers, other vehicles, and the overall infrastructure. Hence, it is crucial to make data protection a high priority in IoV networks.

According to many researchers, the key requirement of IoV types of networks is the protection of the data and communication networks used (Contreras-Castillo et al., 2017; Sharma and Kaushik, 2019; Kumar et al., 2021; Wang et al., 2021). Therefore, it is important to ensure a stable system. The messages that are communicated can either save lives or cause casualties, such as in the case of a malicious node inserting false data. Security considerations must be considered before the implementation of any system. These considerations are derived from basic security objectives, such as authentication, confidentiality, integrity of data, authenticity, non-repudiation, availability, and access control. In addition, different vehicular contact problems must be considered in the adoption of IoV. For instance, mobility, low error tolerance, key management, cloud stability and security, and privacy.

In the comparison of IoV and VANETs, it has been found that IoV is more vulnerable as it is connected to the Internet and the cloud, which increases the number of threats as well as the probability and severity of an attack launched against it. The literature discusses many different possible threats and attacks, such as Sybil, DoS, distributed denial of service (DDoS), black hole, grey hole, and man-in-the-middle (MITM) attacks (Sharma and Kaushik, 2019; Bagga et al., 2020; Yu et al., 2020). These attacks can be classified into attacks on the fundamental requirements presented earlier, such as authenticity, availability, integrity and data trust, confidentiality, and non-repudiation.

Hasbullah et al. (2010) proposed a model to handle the security risk of DoS attacks with the use

of an OBU that is fitted on each vehicle. Their model relies on using this OBU, which resides on every vehicle node, to prevent DoS attacks. The system's processing unit transfers the collected information to the OBU, which chooses from four options to decide based on the type of malicious message received. After executing the necessary processing and assessment, the OBU sends the information to the OBU in the other vehicle in the network. In the researchers' model, the OBUs can use the switching options available, such as channel switching, switching technology, frequency-hopping spread spectrum, and multiple radio transceivers.

Sinha and Mishra (2014) introduced a Queue Limiting Algorithm (QLA) designed to limit the number of safety messages each vehicle in the network can receive, thereby defending against DoS attacks without compromising security. The algorithm categorizes incoming messages into four groups, assigning different priorities to each group for accessing dedicated short-range communication channels. Each vehicle's OBU has a scheduler that controls message transmission to avoid internal collisions, ensuring that high-priority messages are sent before lower-priority ones. The QLA sets the maximum capacity for message handling.

In summary, IoV networks gain advantages from connecting to the Internet, while VANETs function as a component within IoV networks. Among various attacks targeting IoV, DoS attacks pose significant threats. Therefore, innovative solutions are essential to mitigate their impact.

3. Materials and methods

It is possible to identify defense mechanisms against DoS attacks through different techniques, such as prevention, identification, mitigation, and response. As mentioned earlier, researchers have managed to apply switching techniques, such as switching channels and technologies, to detect and mitigate DoS attacks. This is considered a passive method of dealing with such an attack. However, the solution proposed in this paper implements a smart solution of using SYN TCP, as shown in the following scenarios:

- Many SYN packets (mainly more than 15) with the same IP or MAC address are received in a short period of time.
- A large volume of traffic within a short period of time simulates the possibility of spoofing the IP or MAC address.

3.1. Honeypot deployment

The proposed solution deploys a honeypot node with the same computing resources as a typical network node to act as a victim or potential target. The honeypot node is a machine resource that will be examined, attacked, or even compromised. It could be a physical node, which can be situated on a real vehicle, or a virtual node, in which another vehicle node runs in parallel (preferably a government vehicle, such as a police car). The honeypot's output value is zero, and it is considered suspicious if an attempt at communication occurs. Once a honeypot is deployed, identification and prevention take place.

3.2. Detection algorithm overview

The proposed detection solution utilizes the code available at GitHub†, which was built on Python and can run on any operating system (OS). Once a DoS attack is detected, the honeypot node records the details of the attacker, such as the IP or MAC address. The honeypot will then update its database and share the details with other legitimate nodes to update their databases and discard any messages from the detected attacker. The framework of the proposed detection algorithm is shown in Figs. 2a and 2b.

As previously mentioned, honeypots can be virtual or physical. A physical computer node could pose as a honeypot on computer networks, or it can run an Internet-connected virtual OS that will ultimately serve as a honeypot. A police car, or any other government vehicle, can be a physical node in the IoV network. In virtual terms, a node can be generated in simulation software to simulate the behavior of a virtual node in the simulation environment. Fig. 3 presents the honeypot scenario of the proposed solution, whereby the attacker generates a DoS attack by sending SYN and flooding all surrounding nodes. Once the DoS attack is detected, the attacker's details will be added to the database. The honeypot will also share the information collected with all legitimate nodes around it. As a result, when the attacker tries to carry out another DoS attack, all nodes will discard the messages received.

3.3. Simulation details

The vehicles in network simulation (Veins) framework were used to implement the proposed smart detection solution. Veins is an open-source platform used to run vehicular network simulations (Sommer et al., 2010). It is based on two well-established simulators:

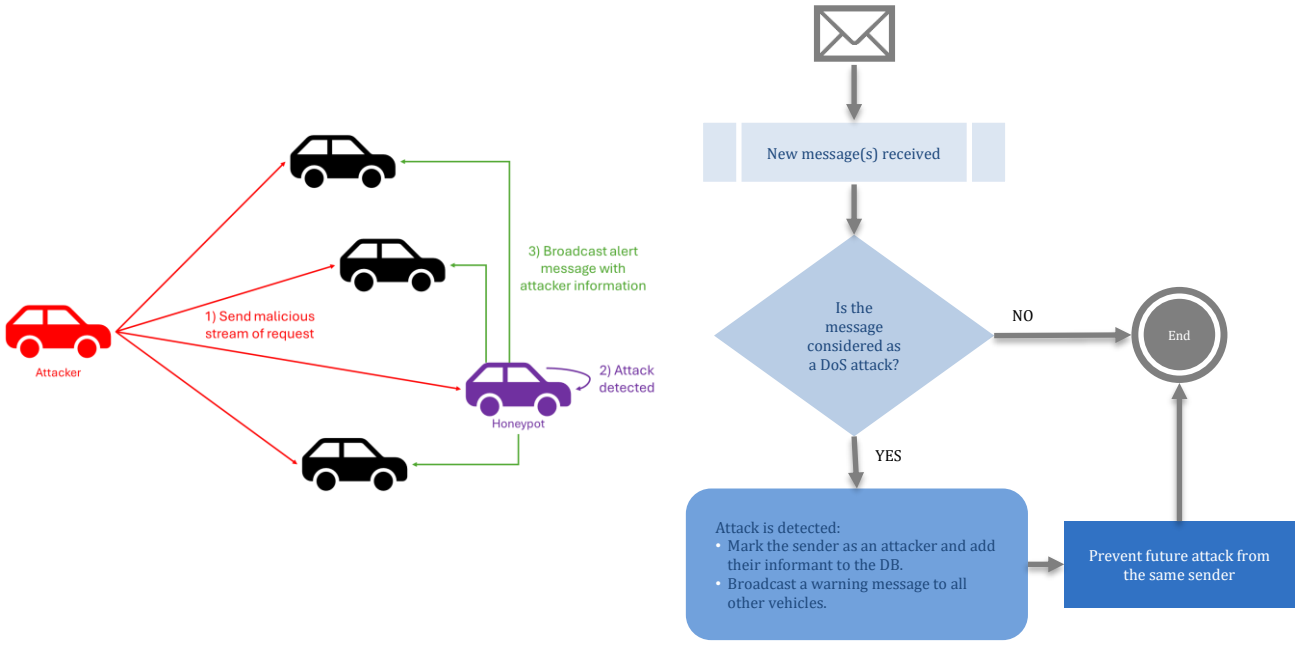
- OMNeT++: an event-based network simulator used to move the nodes in a network.
- SUMO: a road traffic simulator that offers a comprehensive suite of models for inter-vehicular communication simulation (Alvarez Lopez et al., 2018).

4. Results and discussion

This section presents the experimental results and discusses the proposed smart detection solution and its scenarios. These scenarios have been

† https://github.com/justinelhalabi/DosAttack_DosDetection

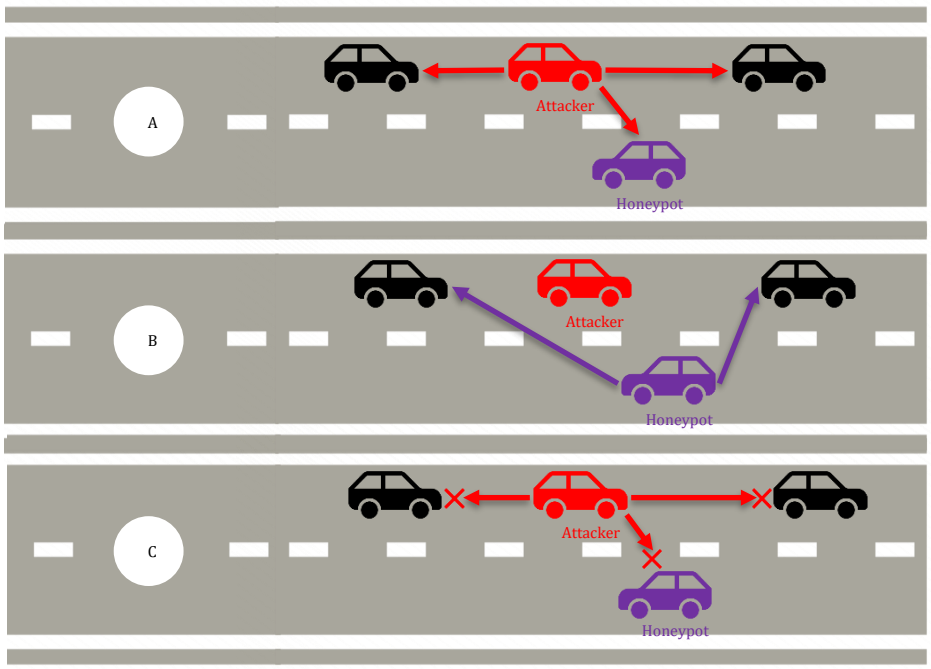
validated using the Veins simulation framework to build communication between the different vehicles and apply the honeypot technique. The implementation prerequisites are presented first, followed by an explanation of the implementation process.



a: Explaining the deployment of honeypots where the attack is detected, and other vehicles are notified to avoid future attacks

b: Illustrating the proposed detection algorithm framework and its behavior once a new message is received

Fig. 2: The framework of the proposed detection algorithm



(A) a DoS attack due to the network overloading in V2V; (B) the honeypot shares the attacker's details with the surrounding legitimate nodes; (C) a DoS attack due to a packet drop V2V

Fig. 3: Honeypot scenario of the proposal solution

The Veins framework requires several prerequisites to be installed before it can be ready for use. The recommended OS for this framework is any Linux distribution, such as Debian or Ubuntu. Any OS can be built over virtual machine (VM) software, such as VirtualBox, which is open source and offered by Oracle. In this research, Instant Veins was installed, which is a VM that can run Veins. It is distributed as a single-file virtual appliance, ready for one-click import into software such as Oracle VM VirtualBox and VMware Workstation. Instant Veins uses Debian OS version 10 and some prerequisite packages and software, as shown in Table 2.

The Veins framework is accessible using the OMNeT++ Integrated Development Environment (IDE), where the project can be created and then the framework can be used to build the required logic and scenarios. Although there are various types of nodes that can be used, including obstacles, pedestrians, vehicles, and traffic lights, the proposed

solution focuses on vehicles and traffic light nodes to test the above-mentioned scenarios. Each node has a simulated computer that facilitates the interaction with other nodes in addition to other components, such as messages and network description files. The nodes can have distinct graphical and code representations.

Table 2: Prerequisite packages and software in the Veins framework

Component	Description
Simulation modules	
Veins 5.0	Framework for vehicular network simulations
INET Framework 4.1.1	Network communication module
SimuLTE (selected versions)	Simulation tool for LTE communication
Veins_INET included with Veins 5.0	Integration of Veins with INET
Software	
OMNeT++ 5.5.1	Event-based network simulator
SUMO 1.4.0	Road traffic simulation
Cookiecutter 1.6.0	Project template generator for Veins projects
Operating system	
Debian 10, Linux 4, GNOME 3	Recommended OS for simulations

There are two main nodes in the implementation: the vehicles and the traffic light. The former can communicate with the RSU and other vehicles. It is considered a compound module, as shown in Fig. 4. The second node is the traffic light and is considered a compound module as it has various submodules inside it, as shown in Fig. 5.

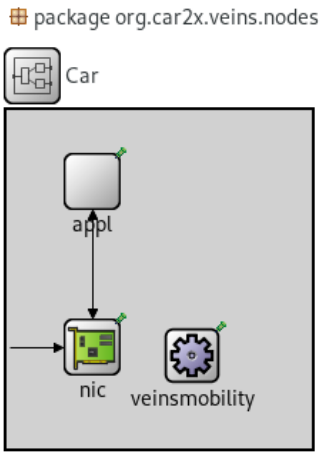


Fig. 4: Simulation graphical network description file for the vehicle

SUMO allows the modeling of intermodal traffic systems, including roads, public transportation, and pedestrians. It also includes route finding, visualization, and network import and emission calculation. SUMO can be enhanced with custom models and provides various APIs to control the simulation remotely (Alvarez Lopez et al., 2018). To implement the proposed solution, a road with two path lines was created with several vehicles, as shown in Fig. 6. Another model was created, which has four roads, in addition to traffic lights and vehicles, as shown in Fig. 7. The simulation parameters for both scenarios are presented in Table 3. To simulate DoS attack detection, the Python library mentioned earlier was used with a set of prerequisite software, as shown in Table 4.

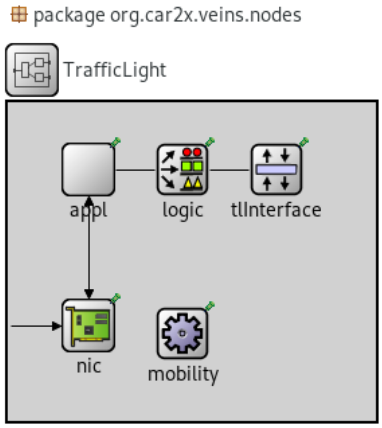


Fig. 5: Simulation graphical network description file for the traffic light

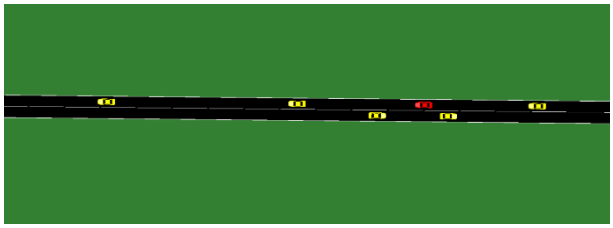


Fig. 6: SUMO simulation of a two-way scenario

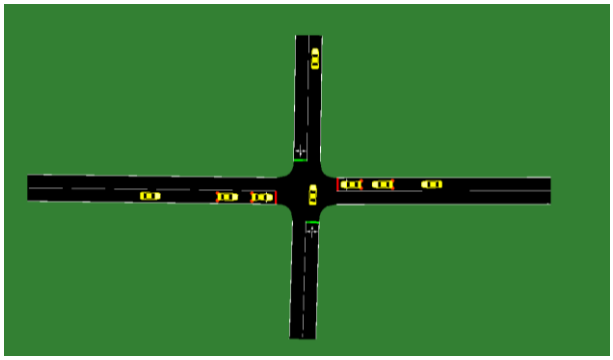


Fig. 7: SUMO simulation of a crossroads and traffic lights scenario

Table 3: The used parameters in the simulation

Parameter	Description
Number of nodes (vehicles)	6
Simulation road length	224.43 m
Road speed	13.89 m/s
Simulation time	60 s
SUMO configuration	Two-way scenario

Table 4: DoS attack detection software prerequisites

Parameter	Description
Python 2.7.18	Programming language
Scapy 2.4.4	Packet manipulation tool for computer networks
Windows 10	Operating system to run all components
Nmap	Network scanner

The first scenario simulation process starts by launching a DoS attack from one of the nodes by sending one packet every 0.1 s. Once the attack is detected, an alert is sent to all nodes in the network with the details of the attacker (MAC address 00:0c:29:93:d1:e0 in this case). Fig. 8 presents the network utilization when the attack is detected.

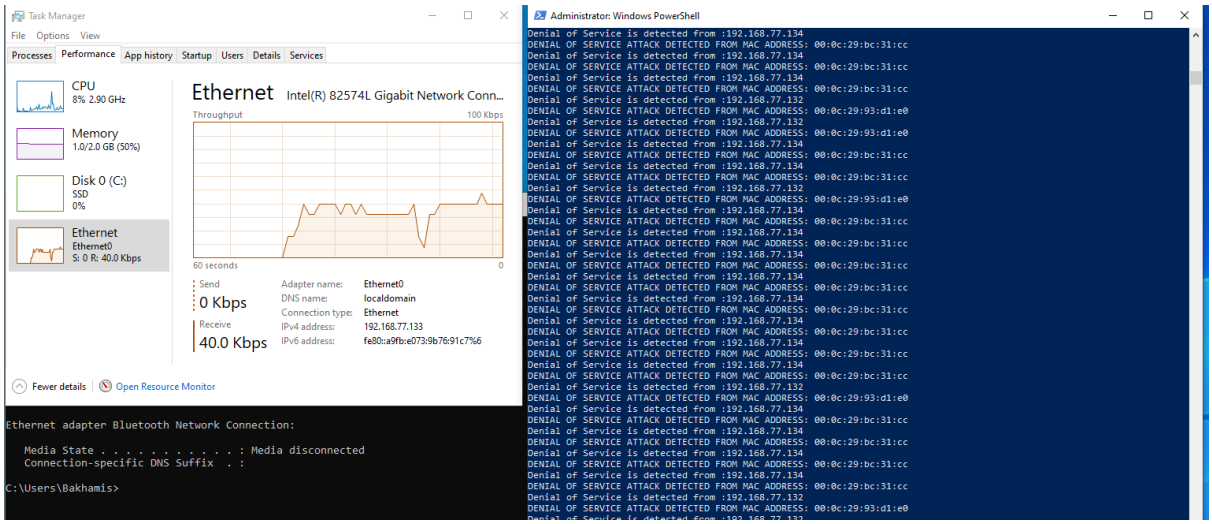


Fig. 8: Simulation screenshot showing the detection of a DoS attack from one attacker

The second scenario simulation is implemented when a DoS attack is carried out from two nodes. In this case, the network utilization, as in Fig. 9, shows double the consumption cost compared to the previous scenario, in which there was only one node carrying a DoS attack. Once again, the attackers' information is distributed to all surrounding nodes to identify them as attackers (MAC addresses 00:0c:29:bc:31:cc and 00:0c:29:93:d1:e0 in this case). However, the experiment reveals that the detection solution is light and can be run virtually on any OS on the vehicle OBU (parallel to the main system) or as a standalone, as in the case of a honeypot vehicle.

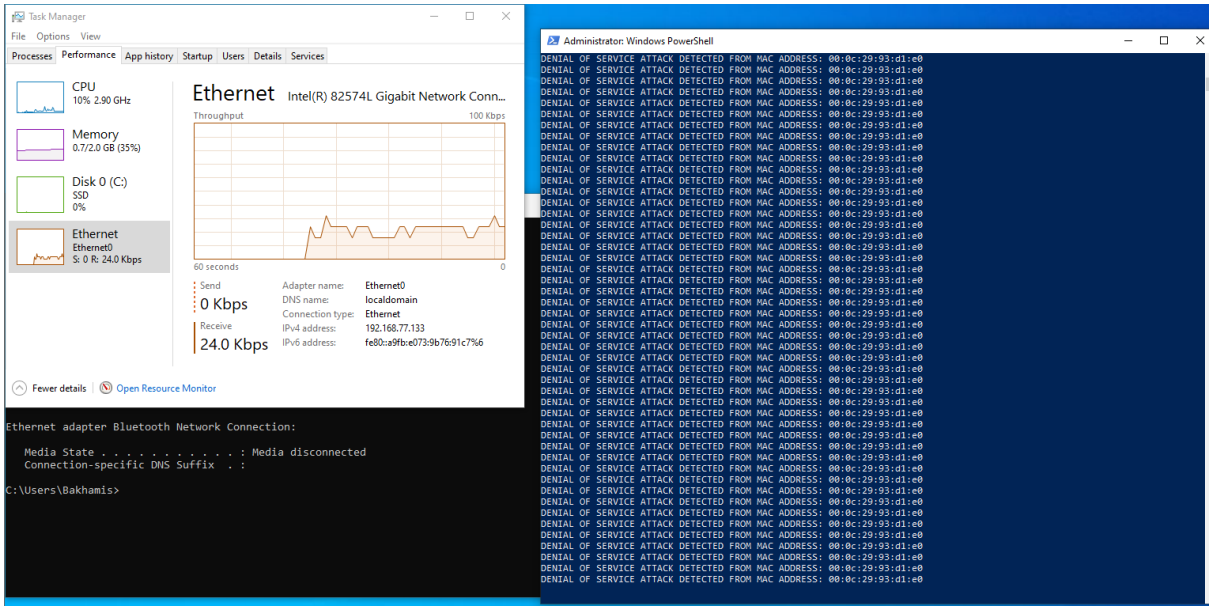


Fig. 9: Simulation screenshot showing the detection of a DDoS attack from two attackers

5. Conclusion and future work

The primary concern for many road users is safety. Several safety solutions and applications have been applied as part of ITS efforts, such as reporting traffic and accident warnings aiming at supporting the safety criteria. Introducing the concept of IoT and creating VANETs has led to the formation of what is now known as IoV networks, which present the opportunity to include certain specifications for safety. In addition to the many benefits of applying such IoV technologies, some challenges have been observed that require security mechanisms to eliminate negative impacts. For instance, secure and timely life-critical messaging might be exchanged between nodes/vehicles within an IoV network. To accomplish such a goal, a strong and reliable security mechanism needs to be in place to provide safe communication and ensure network availability.

One possible attack on IoV networks is to carry out a DoS type of attack aimed at flooding the network with messages to disturb the communication between nodes, such as vehicles and road signs. As stated earlier, several solutions have been proposed for implementation using vehicle resources, which has led to the unfavourable consumption of these resources, especially because they are already limited. Hence, this research proposes a smart detection solution to be configured as a separate node (a honeypot) that helps detect

DoS types of attacks. Furthermore, the honeypot prevents future attacks from the same source by alerting all the surrounding nodes in the same IoV network.

The proposed solution has been tested using a well-known simulation framework to ensure its validity in detecting DoS attacks in two main scenarios: firstly, when many messages are received from a single source, and secondly, when many messages are received from two different nodes. It was found that the proposed solution is light and can either be implemented as a standalone, as in the case of the honeypot, or implemented in parallel and virtually on one of the node's resources.

In future work, the proposed solution can be enhanced in many directions. First, the proposed solution can be extended and enhanced to detect complex DoS attacks, such as sending packets in different sequences of time from the same node (or different nodes). Second, the proposed solution can also be extended to include the detection of other types of attacks, such as black hole MITM attacks. Another direction of this research is implementing the proposed solution in real-world scenarios to examine its validity and impact.

Compliance with ethical standards

Conflict of interest

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Alalwany E and Mahgoub I (2024). Security and trust management in the internet of vehicles (IoV): Challenges and machine learning solutions. Sensors, 24(2): 368. https://doi.org/10.3390/s24020368 **PMid:38257461 PMCid:PMC10819911**

Ali ES, Hasan MK, Hassan R, Saeed RA, Hassan MB, Islam S, Nafi NS, and Bevinakoppa S (2021). Machine learning technologies for secure vehicular communication in internet of vehicles: Recent advances and applications. Security and Communication Networks, 2021: 8868355. https://doi.org/10.1155/2021/8868355

AlMarshoud M, Sabir Kiraz M, and H Al-Bayatti A (2024). Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions. ACM Computing Surveys, 56(10): 1-39. https://doi.org/10.1145/3656166

Alvarez Lopez M, Behrisch M, Bieker-Walz L, Erdmann J, Flötteröd YP, Hilbrich R, Lücken L, Rummel J, Wagner P, and Wießner E (2018). Microscopic traffic simulation using SUMO. In the IEEE Intelligent Transportation Systems Conference (ITSC), IEEE, Auckland, New Zealand: 2575-2582. https://doi.org/10.1109/ITSC.2018.8569938

Bagga P, Das AK, Wazid M, Rodrigues JJ, and Park Y (2020). Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. IEEE Access, 8: 54314-54344. https://doi.org/10.1109/ACCESS.2020.2981397

Baldini G, Botterman M, Neisse R, and Tallacchini M (2018). Ethical design in the internet of things. Science and Engineering Ethics, 24: 905-925. https://doi.org/10.1007/s11948-016-9754-5 **PMid:26797878 PMCid:PMC5972157**

Contreras-Castillo J, Zeadally S, and Guerrero-Ibañez JA (2017). Internet of vehicles: architecture, protocols, and security. IEEE Internet of Things Journal, 5(5): 3701-3709. https://doi.org/10.1109/JIOT.2017.2690902

Gracias JS, Parnell GS, Specking E, Pohl EA, and Buchanan R (2023). Smart cities—A structured literature review. Smart Cities, 6(4): 1719-1743. https://doi.org/10.3390/smartcities6040080

Gupta N, Manaswini R, Saikrishna B, Silva F, and Teles A (2020). Authentication-based secure data dissemination protocol and framework for 5G-enabled VANET. Future Internet, 12(4): 63. https://doi.org/10.3390/fi12040063

Hasbullah H, Soomro IA, and Ab Manan JL (2010). Denial of service (DOS) attack and its possible solutions in VANET. International Journal of Electronics and Communication Engineering, 4(5): 813-817. https://doi.org/10.5281/zenodo.1085740

Kamble SS, Gunasekaran A, Parekh H, and Joshi S (2019). Modeling the internet of things adoption barriers in food retail supply chains. Journal of Retailing and Consumer Services, 48: 154-168. https://doi.org/10.1016/j.jretconser.2019.02.020

Kumar R, Kumar P, Tripathi R, Gupta GP, and Kumar N (2021). P2SF-IoV: A privacy-preservation-based secured framework for internet of vehicles. IEEE Transactions on Intelligent Transportation Systems, 23(11): 22571-22582. https://doi.org/10.1109/TITS.2021.3102581

Kumar S, Velliangiri S, Karthikeyan P, Kumari S, Kumar S, and Khan MK (2024). A survey on the blockchain techniques for the internet of vehicles security. Transactions on Emerging Telecommunications Technologies, 35(4): e4317. https://doi.org/10.1002/ett.4317

Obaidat M, Khodjaeva M, Holst J, and Ben Zid M (2020). Security and privacy challenges in vehicular ad hoc networks. In: Mahmood Z (Ed.), Connected vehicles in the internet of things: Concepts, technologies and frameworks for the IoV: 223-251. Springer International Publishing, Cham, Switzerland. https://doi.org/10.1007/978-3-030-36167-9_9

Panigrahy SK and Emany H (2023). A survey and tutorial on network optimization for intelligent transport system using the internet of vehicles. Sensors, 23(1): 555. https://doi.org/10.3390/s23010555 **PMid:36617152 PMCid:PMC9824436**

Priyan MK and Devi GU (2019). A survey on internet of vehicles: Applications, technologies, challenges and opportunities. International Journal of Advanced Intelligence Paradigms, 12(1-2): 98-119. https://doi.org/10.1504/IJAIP.2019.096957

Quyoom A, Ali R, Gouttam DN, and Sharma H (2015). A novel mechanism of detection of denial of service attack (DoS) in VANET using malicious and irrelevant packet detection algorithm (MIPDA). In the International Conference on Computing, Communication and Automation, IEEE, Greater Noida, India: 414-419. https://doi.org/10.1109/CCAA.2015.7148411

Rose K, Eldridge S, and Chapin L (2015). The internet of things: An overview. Technical Report, The Internet Society (ISOC), Geneva, Switzerland.

Sharma S and Kaushik B (2019). A survey on internet of vehicles: Applications, security issues and solutions. Vehicular Communications, 20: 100182. https://doi.org/10.1016/j.vehcom.2019.100182

Sinha A and Mishra SK (2014). Queue limiting algorithm (QLA) for protecting VANET from denial of service (DoS) attack. International Journal of Computer Applications, 86(8): 14-17. https://doi.org/10.5120/15004-3153

Sommer C, German R, and Dressler F (2010). Bidirectionally coupled network and road traffic simulation for improved IVC

analysis. IEEE Transactions on Mobile Computing, 10(1): 3-15. https://doi.org/10.1109/TMC.2010.133

Surutkar R and Jadhav C (2024). VANET for autonomous vehicles. In the IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), IEEE, Bhopal, India: 1-7. https://doi.org/10.1109/SCEECS61402.2024.10482135

Wang C, Cheng X, Li J, He Y, and Xiao K (2021). A survey: Applications of blockchain in the internet of vehicles. EURASIP Journal on Wireless Communications and Networking, 2021: 1-16. https://doi.org/10.1186/s13638-021-01958-8

Yu S, Lee J, Park K, Das AK, and Park Y (2020). IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment. IEEE Access, 8: 167875-167886. https://doi.org/10.1109/ACCESS.2020.3022778