Available online at www.ijournalse.org

Emerging Science Journal

(ISSN: 2610-9182)

Vol. 10, No. 1, February, 2026

Assessing the Impact of Ghost Car Attacks on Traffic Flow in Vehicular Ad Hoc Networks

Isyraf Nazmi Drahman [1], Sumendra Yogarayan [1*], Siti Fatimah Abdul Razak [1], Md. Shohel Sayeed [1], Mohd. Fikri Azli Abdullah [1], Subarmaniam Kannan [1], Afizan Azman [2]

[1] *Faculty of Information Science and Technology, Multimedia University, Melaka 75450, Malaysia.*

[2] *School of Computing, Faculty of Information and Technology, Taylors University, Subang Jaya, Selangor, Malaysia.*

Abstract

Vehicular Ad Hoc Networks (VANETs) play a crucial role in enhancing road safety, traffic management, and driving efficiency through real-time communication between vehicles and infrastructure. However, VANETs are vulnerable to various security threats, one of which is the "ghost car" attack. In this attack, a malicious entity injects false information into the network, simulating the presence of a non-existent or "ghost" vehicle. This can lead to severe consequences such as traffic disruptions, accidents, and a compromised trust in the system's reliability. This study aims to simulate and analyze the impacts of ghost car attacks on Vehicular Ad Hoc Networks (VANETs), focusing specifically on intersection waiting times and overall traffic flow. We used Simulation of Urban Mobility (SUMO) integrated with ns-3 for realistic VANET simulations, introducing varying numbers of ghost vehicles. Results indicate significant increases in waiting times and vehicle counts at intersections due to ghost cars, leading to traffic disruptions. This study evaluates ghost car attacks within realistic urban scenarios and proposes targeted detection and mitigation strategies, leveraging authentication, machine learning, and blockchain technologies.

Keywords:

VANET; Security Attacks;

Ghost Car;

Traffic Flow;

Vehicle Coordination.

Article History:

Received:	27	February	2025
Revised:	13	December	2025
Accepted:	25	December	2025
Published:	01	February	2026

1- Introduction

Vehicular Ad Hoc Networks (VANETs) are an integral part of modern Intelligent Transportation Systems (ITS), enabling vehicles to communicate with each other (Vehicle-to-Vehicle or V2V) and with infrastructure (Vehicle-to-Infrastructure or V2I) [1]. By allowing vehicles to share real-time information such as traffic conditions, accident alerts, and navigation data, VANETs promise to revolutionize road safety, traffic efficiency, and overall driving experience [2]. According to recent studies, the global market for connected cars is expected to reach $225.16 billion by 2027, driven largely by advances in VANET technology [3, 4]. These networks reduce traffic congestion, improve emergency response times, and enhance fuel efficiency by coordinating the movement of vehicles on roadways [5]. However, the connectivity that makes VANETs advantageous also exposes them to a range of security threats, which could compromise both vehicle safety and traffic management systems.

One of the primary security challenges in VANETs is their open and decentralized nature [6]. Since vehicles frequently join and leave the network while on the move, maintaining trust and secure communication between them is inherently difficult [7]. This creates opportunities for various attacks, including sybil attacks, replay attacks, man-in-the-middle attacks, and the increasingly prominent "ghost car" attack [8, 9]. In sybil attacks, for instance, an attacker

[*] **CONTACT**: sumendra@mmu.edu.my

DOI: http://dx.doi.org/10.28991/ESJ-2026-010-01-024

© 2026 by the authors. Licensee ESJ, Italy. This is an open access article under the terms and conditions of the Creative Commons Attribution (CC-BY) license (https://creativecommons.org/licenses/by/4.0/).

generates multiple fake identities to overwhelm the network, while in replay attacks, valid data is captured and resent later to confuse vehicles [10]. The ghost car attack is particularly concerning because it involves injecting false information into the network to simulate the presence of a non-existent vehicle, which can lead to significant disruptions in traffic flow.

The ghost car attack works by fabricating a vehicle that does not physically exist but appears to be present within the network [11]. This deceptive information can be used to manipulate traffic conditions in several ways, such as forcing vehicles to slow down, reroute unnecessarily, or make abrupt stops to avoid collisions with the fake vehicle. In urban environments, where traffic density is high and intersections are frequent, the presence of a ghost car can lead to substantial delays [12]. Waiting times at intersections may increase as real vehicles respond to the false signals generated by the ghost car, causing cascading effects on overall traffic efficiency. In addition, the risk of accidents and road congestion grows as legitimate vehicles react to non-existent obstacles, eroding the trust that VANETs rely on to function optimally.

Research into VANET security attacks has highlighted the need for robust detection and mitigation techniques to counter such threats. Studies have shown that security breaches in VANETs can lead to economic losses, traffic inefficiencies, and even life-threatening accidents [13]. For example, according to a report by the National Highway Traffic Safety Administration (NHTSA), traffic-related fatalities could increase by 10-20% if VANET systems are compromised [14-16]. The need to address these vulnerabilities is especially critical given the anticipated expansion of autonomous vehicles, which will rely heavily on secure VANET communications.

Despite the recognized risks, there is a gap in the literature concerning the specific impact of ghost car attacks on traffic dynamics, particularly regarding the effect on waiting times and traffic flow at intersections. Understanding these effects is essential for developing robust countermeasures. This study aims to fill that gap by simulating a ghost car attack in a VANET environment, with a focus on evaluating the delays and traffic disruptions it causes. By analyzing waiting times at key points in traffic, such as intersections, and measuring the overall impact on traffic flow, the research will provide insights into how disruptive a ghost car can be and offer potential strategies for mitigating the attack. The findings of this study will contribute to the development of secure VANET architecture, helping to protect the future of intelligent transportation systems.

2- Simulation Approach

The simulation of the ghost car attack and its effects on traffic flow was conducted using two primary tools: Simulation of Urban Mobility (SUMO) for traffic simulation and ns-3 for network simulation. These tools were chosen to replicate a realistic vehicular ad hoc network (VANET) environment, where the impact of a ghost car attack on traffic dynamics, particularly waiting times at intersections and overall traffic flow, could be assessed. We simulated a typical urban T-junction with moderate to high traffic density to reflect real-world congestion scenarios. The road network was extracted from OpenStreetMap (Ayer Keroh, Melaka, Malaysia) to ensure a realistic layout with traffic lights and multiple lanes as shown in Figure 1. While the study focused on a single type of intersection, the setup allowed for dynamic variations in vehicle counts, enabling the assessment of how ghost cars disrupt traffic under increasing load. Table 1 presents the detailed simulation parameters used in the study.

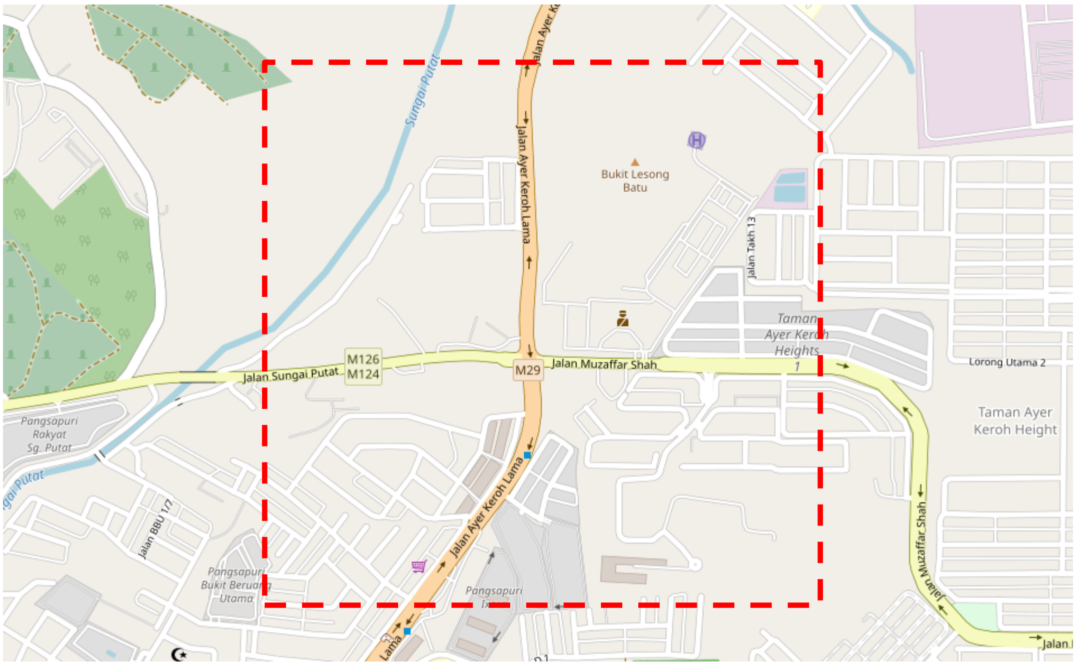


Figure 1. T-Junction of Ayer Keroh, Melaka, Malaysia on OSMWebWizard

Table 1. Simulation parameter

Parameter	Settings
Network simulator	ns-3.39 and SUMO
Wireless communication	WAVE/IEEE 802.11p
Selected network traffic area	T-junction near Ayer Keroh, Melaka
Maximum simulation time	200 seconds
Number of legitimate vehicle nodes	50-100
Number of ghost car nodes	1-10
Delay in point-to-point channel	2ms

To simulate the ghost car attack, a non-existent vehicle was introduced into the VANET system. This ghost car injected false information into the network, creating a virtual presence that disrupted normal traffic operations. The ghost car was designed to cause delays at intersections by generating false occupancy data that forced real vehicles to alter their behaviour, such as slowing down, rerouting, or stopping to avoid a collision with the non-existent vehicle. Two variations of the ghost car were implemented: one where the ghost car was visible within the simulation, and another where it operated invisibly, affecting traffic without being observed by the vehicles or infrastructure.

The network simulation was performed in ns-3, utilizing the WAVE/802.11p protocol to enable real-time communication between vehicles (V2V) and between vehicles and infrastructure (V2I). This communication was essential for simulating the behaviour of the vehicular network during the ghost car attack. To ensure synchronized operation between SUMO and ns-3, the Traffic Control Interface (TraCI) was used, allowing for real-time traffic movement and network interactions. The integration between SUMO and ns-3 provided a comprehensive view of how the ghost car affected both the traffic flow and the communication network. Traffic data, such as waiting times at intersections and the number of vehicles affected by the ghost car, were collected and analysed. Visualization of the traffic patterns and congestion levels was achieved using Matplotlib. Comparisons were drawn between the normal traffic scenario and the scenario affected by the ghost car attack, with a focus on waiting times at intersections and the overall impact on traffic flow. Figure 2 illustrates the simulation methodology includes defining the simulation area, configuring traffic scenarios, integrating SUMO and ns-3 simulations, ghost cars in phased intervals, recording waiting times, analyzing data, and comparing with normal traffic flow.

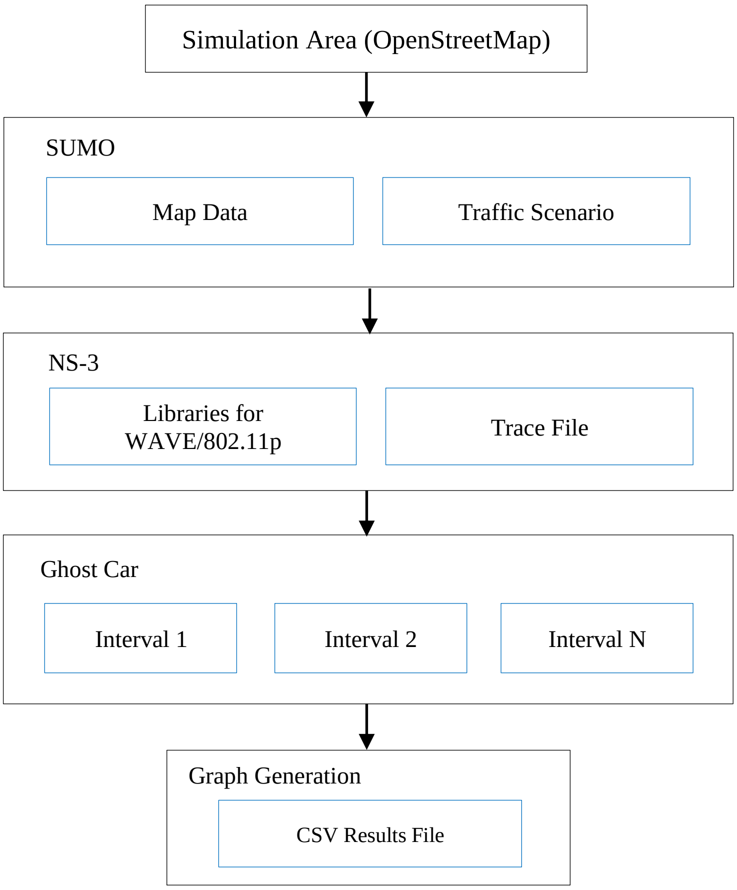


Figure 2. Simulation Block Diagram

2-1- Ghost Car Setup

The primary objective of the ghost car simulation was to evaluate the disruptive impact of non-existent, or "ghost," vehicles on real-world traffic flow and waiting times, particularly at a critical intersection near Multimedia University (MMU), Melaka. Ghost cars, in this context, represent vehicles that do not physically exist but are falsely introduced into a traffic system, misleading the traffic management systems and other vehicles into treating them as real. By simulating these phantom vehicles, the study sought to explore how they could influence congestion, delay legitimate traffic, and cause inefficiencies in urban mobility.

The simulation was conducted using two platforms: SUMO (Simulation of Urban Mobility) for generating realistic traffic flows and modelling vehicle behaviour, and ns-3 for handling network communications between the vehicles. Together, these platforms allowed for a detailed examination of both traffic and communication aspects. The simulation was centered on a T-junction, a commonly congested intersection type in urban traffic systems, providing a representative and relevant testbed for understanding how ghost cars might affect typical traffic flow.

In configuring the ghost vehicles for the simulation, a maximum limit of 10 ghost cars was set. This decision allowed the simulation to maintain balance and avoid overwhelming the system, thus ensuring that the results reflected a realistic traffic scenario. The ghost cars were not introduced all at once; rather, they were added in phases, with one vehicle being introduced every 20 simulation steps following an initial 10-second delay. This gradual influx of ghost vehicles was intended to mimic the real-world scenario of vehicles steadily approaching an intersection, while also providing insight into how the timing of such ghost vehicle attacks affects traffic flow. Ghost cars were differentiated from real vehicles through parameters including lack of physical presence (no collision detection), consistent introduction intervals (every 20 simulation steps), and artificially induced waiting delays (an additional 5 seconds per ghost vehicle introduced).

Once introduced, each ghost vehicle contributed an additional 5 seconds to the waiting time of legitimate, real vehicles at the T-junction. This configuration simulated the congestion that ghost vehicles would create by falsely occupying space in the traffic system. Throughout the simulation, detailed data on vehicle counts and waiting times were recorded at every step, allowing for a comprehensive analysis of how ghost vehicles alter the dynamics of traffic.

Throughout the simulation, detailed data was collected at every simulation step, capturing the number of real and ghost vehicles present, as well as the respective waiting times for each. This allowed for an in-depth analysis of how ghost vehicles disrupted the flow of legitimate traffic. The data was then visualized through graphs showing the variations in traffic conditions before and after the ghost cars were introduced. These visualizations were critical in illustrating the stark contrast between normal traffic flow and the congested conditions caused by the introduction of ghost vehicles.

The gradual increase in ghost vehicle presence demonstrated how even a small number of such vehicles could significantly disrupt traffic operations. The data clearly indicated that as the number of ghost cars grew, traffic delays worsened, creating an increasingly chaotic traffic environment. The insights gleaned from this simulation provided a better understanding of how ghost car attacks could exploit vulnerabilities in traffic management systems, causing cascading delays that, over time, could lead to gridlock or severe congestion, especially in densely populated urban area

2-2- Performance Metrics

In evaluating the impact of ghost car attacks on Vehicular Ad Hoc Networks (VANETs), several performance metrics were considered. One key metric is the vehicle count at the intersection, which tracks the number of vehicles present during the simulation. In the ghost car scenario, vehicle counts were artificially inflated, causing congestion and leading to inefficient traffic management as the system responded to non-existent vehicles.

Another important metric is waiting time, which measures how long vehicles remain idle at the intersection. The introduction of ghost cars led to significantly longer waiting times, as real vehicles were delayed by the fabricated presence of ghost vehicles, highlighting the disruptive nature of the attack on traffic flow. Traffic throughput, or the number of vehicles successfully passing through the intersection, was also measured. Throughput decreased during the ghost car scenario due to these delays, demonstrating the negative impact of ghost cars on overall traffic efficiency.

Additionally, the congestion level at the intersection was examined by analysing vehicle density and waiting times. The presence of ghost cars led to higher congestion levels, creating artificial traffic jams that severely affected the normal flow of vehicles. Lastly, the response time to ghost car presence was assessed by observing how quickly real vehicles adjusted to the appearance of ghost cars. The longer response times further illustrated the impact of the attack, as vehicles had to react to fabricated obstacles that disrupted normal traffic coordination

3- Results

In the normal traffic flow, vehicles move through the intersection based on typical traffic conditions without external interference. Vehicle counts and waiting times fluctuate naturally but remain within expected ranges. In contrast, when a ghost car is introduced, it disrupts this flow by creating false congestion. This leads to longer waiting times, more erratic vehicle counts, and overall inefficiencies, as real vehicles are forced to react to non-existent threats, significantly impacting traffic coordination and causing unnecessary delays.

3-1- Normal Traffic Flow

Figure 3 shows the normal traffic scenario; vehicles are behaving as expected in response to the intersection's traffic signals and lane assignments. There appear to be moderate numbers of vehicles, and traffic flow seems manageable, with no significant buildup or abnormal congestion. This reflects typical intersection behavior without external interference, such as ghost cars, allowing the traffic system to function efficiently based on real conditions.

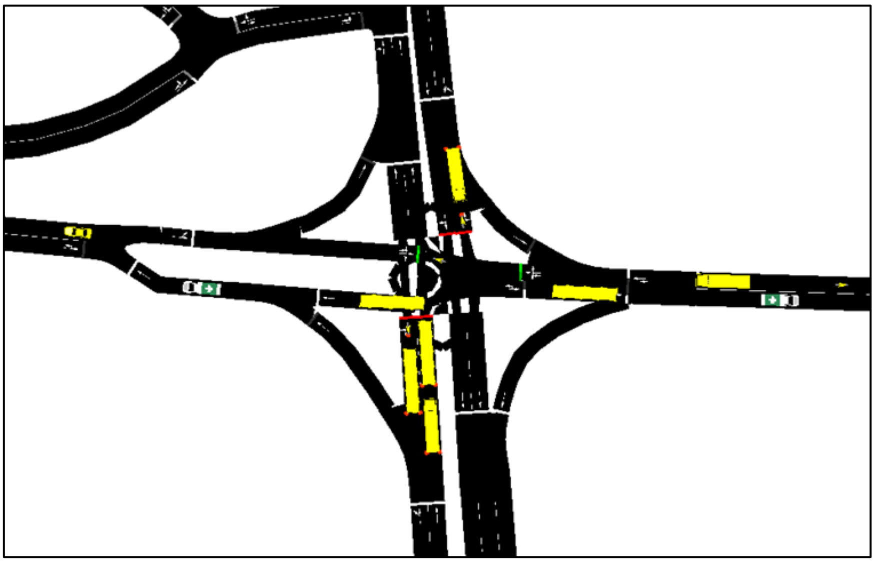
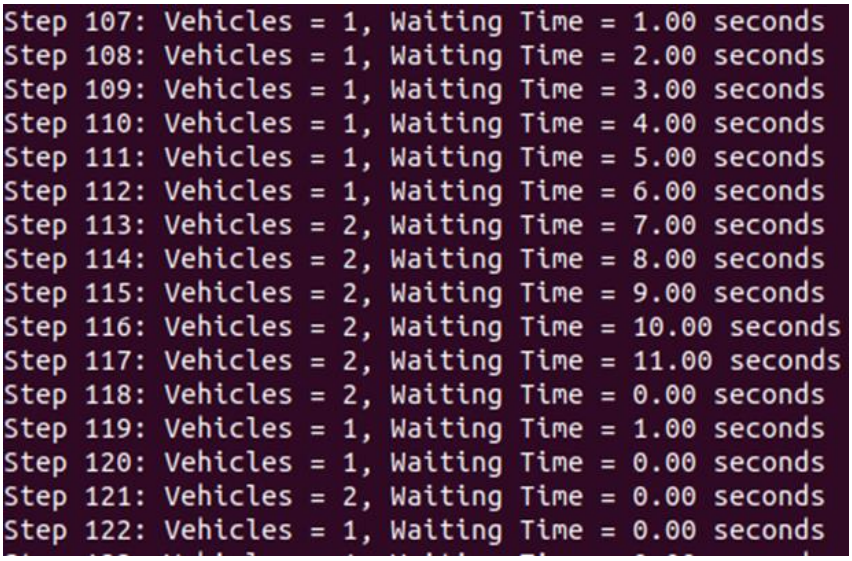


Figure 3. Simulation of normal traffic flow

Figure 4 shows vehicle activity at an intersection during a traffic simulation. It records the number of vehicles present and the waiting time at each step. The simulation tracks how long vehicles are delayed at the intersection, with waiting times increasing as more vehicles approach and decreasing as vehicles move through. This log offers insight into the flow of traffic, showing how congestion builds up and clears over time. It helps analyze traffic patterns and identify periods of delay and smooth flow in real-time scenarios.



```
Step 107: Vehicles = 1, Waiting Time = 1.00 seconds
Step 108: Vehicles = 1, Waiting Time = 2.00 seconds
Step 109: Vehicles = 1, Waiting Time = 3.00 seconds
Step 110: Vehicles = 1, Waiting Time = 4.00 seconds
Step 111: Vehicles = 1, Waiting Time = 5.00 seconds
Step 112: Vehicles = 1, Waiting Time = 6.00 seconds
Step 113: Vehicles = 2, Waiting Time = 7.00 seconds
Step 114: Vehicles = 2, Waiting Time = 8.00 seconds
Step 115: Vehicles = 2, Waiting Time = 9.00 seconds
Step 116: Vehicles = 2, Waiting Time = 10.00 seconds
Step 117: Vehicles = 2, Waiting Time = 11.00 seconds
Step 118: Vehicles = 2, Waiting Time = 0.00 seconds
Step 119: Vehicles = 1, Waiting Time = 1.00 seconds
Step 120: Vehicles = 1, Waiting Time = 0.00 seconds
Step 121: Vehicles = 2, Waiting Time = 0.00 seconds
Step 122: Vehicles = 1, Waiting Time = 0.00 seconds
```

Figure 4. Simulation log for normal traffic flow

Figure 5 tracks the real vehicles detected at the intersection over time. In the first part of the simulation, no vehicles are present until around the 40-second mark, when a few vehicles begin arriving at the intersection. The vehicle count then fluctuates as more vehicles enter and leave the intersection. The highest number of vehicles detected at the intersection is around four, occurring around the 75-second mark. After that peak, the number of vehicles gradually decreases, with a few intermittent arrivals and departures before the traffic flow returns to zero around the 170-second mark. This indicates a typical pattern of traffic flow where vehicles occasionally queue and disperse as they pass through the intersection

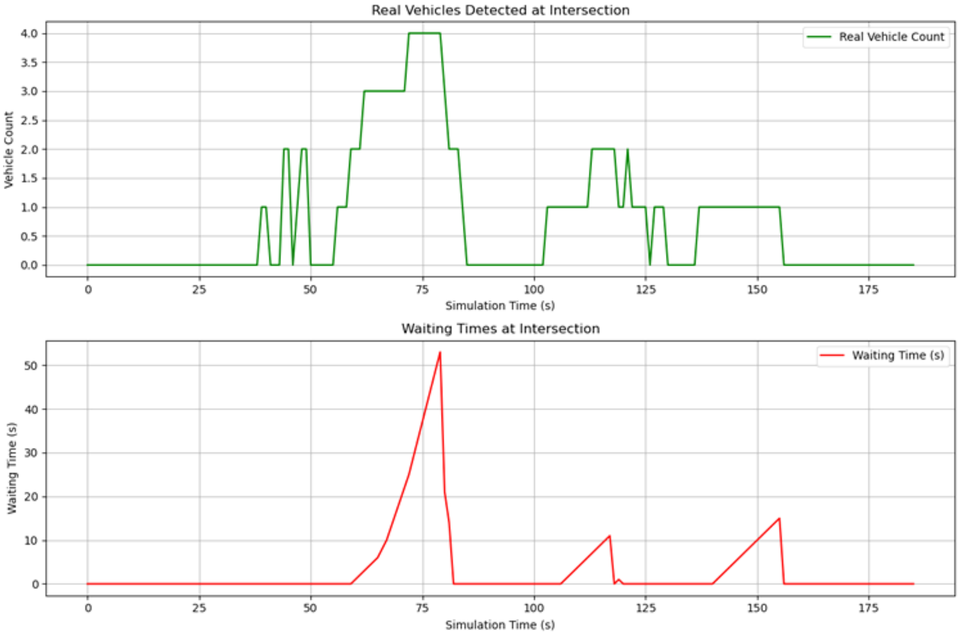


Figure 5. **Normal traffic flow**

In the bottom graph, the waiting times at the intersection appeared over the same period. Initially, there is no waiting time since no vehicles are present. However, as the vehicle count increases (as seen in the upper graph), the waiting time also rises, peaking sharply at around 50 seconds. This peak is significant, showing a maximum waiting time of approximately 50 seconds, which aligns with the high traffic volume indicated in the upper graph. After this peak, the waiting time rapidly decreases, reflecting the clearance of vehicles from the intersection. There are a few smaller spikes in waiting time later in the simulation, correlating with the brief arrival of vehicles after the 100-second mark. However, these spikes are much lower compared to the main peak.

3-2- Ghost Cars Traffic Flow

In comparison to normal traffic flow, the introduction of ghost cars significantly disrupts the system. In the ghost car scenario, vehicle counts increase steadily due to the non-existent ghost cars, leading to much longer waiting times at intersections. While normal traffic flow sees fluctuations and eventual reductions in waiting times as vehicles clear the intersection, the ghost car scenario causes prolonged delays, as real vehicles are forced to respond to the fake congestion created by the ghost cars. This results in a chaotic and inefficient traffic flow compared to the smoother, more predictable patterns of normal traffic.

Figure 6 shows the intersection with the introduction of a ghost car, represented by the blue vehicle. The ghost car does not physically exist but appears within the system, causing real vehicles to adjust their behavior. Real vehicles, represented by yellow cars, are seen waiting at various points in the intersection. The presence of the ghost car can lead to unnecessary stops or slowdowns, as the system treats the ghost car as a real vehicle, potentially increasing congestion and disrupting the normal flow of traffic. This highlights how the ghost car attack creates artificial congestion in the network.

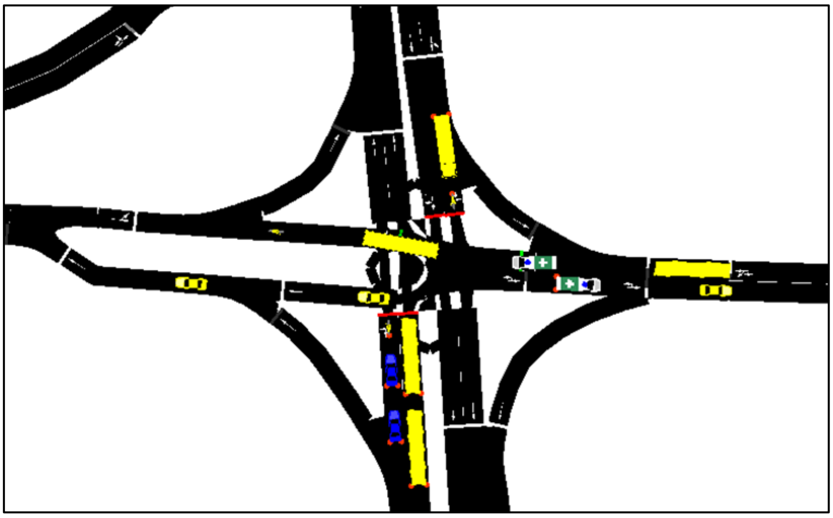
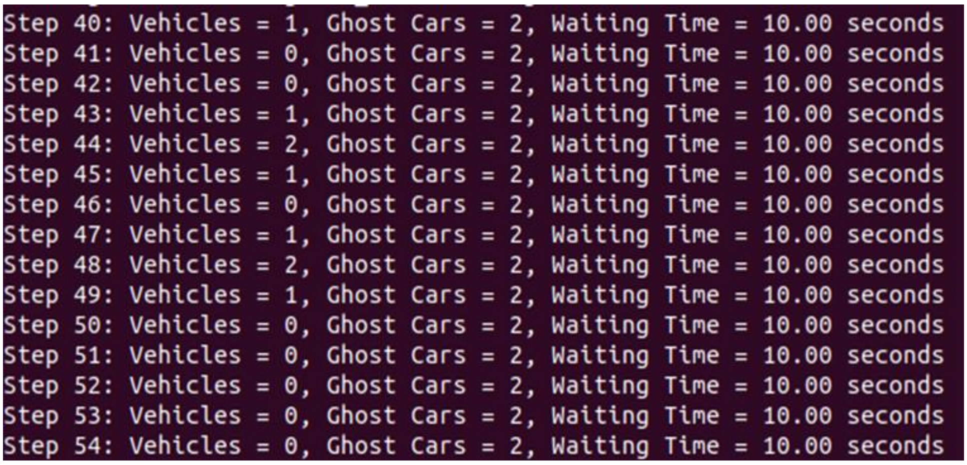


Figure 6. **Simulation of traffic with ghost cars appeared**

Figure 7 shows the detail of how the presence of both real vehicles and ghost cars affects waiting times at an intersection. Each step records the number of real vehicles, ghost cars, and the waiting time for vehicles. As the simulation progresses, the waiting time increases significantly due to the presence of ghost cars. This log illustrates the impact of ghost cars on traffic flow, highlighting how they cause delays by making real vehicles wait longer than they would in a normal traffic scenario.



```
Step 40: Vehicles = 1, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 41: Vehicles = 0, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 42: Vehicles = 0, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 43: Vehicles = 1, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 44: Vehicles = 2, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 45: Vehicles = 1, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 46: Vehicles = 0, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 47: Vehicles = 1, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 48: Vehicles = 2, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 49: Vehicles = 1, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 50: Vehicles = 0, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 51: Vehicles = 0, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 52: Vehicles = 0, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 53: Vehicles = 0, Ghost Cars = 2, Waiting Time = 10.00 seconds
Step 54: Vehicles = 0, Ghost Cars = 2, Waiting Time = 10.00 seconds
```

Figure 7. Simulation Log for ghost car flow

Figure 8 demonstrates the real and ghost vehicles detected at the intersection over time. Initially, only real vehicles are present, but as the simulation progresses, ghost vehicles (represented by the blue line) start to appear. Unlike the real vehicles, which fluctuate in number, the ghost vehicles steadily increase, eventually reaching a count of eight by the end of the simulation. This steady growth in ghost vehicles highlights the disruptive nature of the attack, as the non-existent vehicles persistently occupy virtual space in the network, forcing real vehicles to alter their behavior unnecessarily.

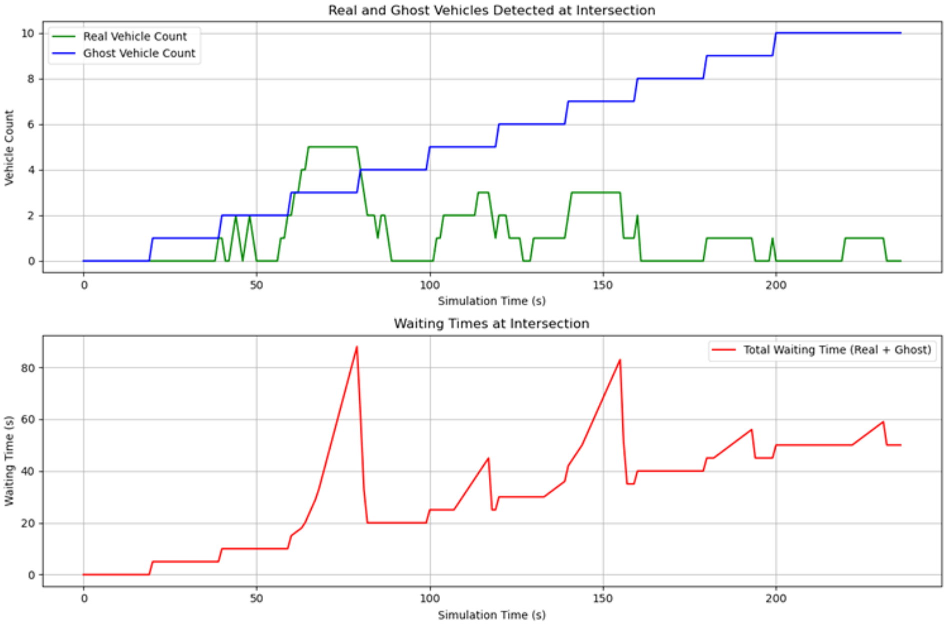


Figure 8. Ghost car flow

The bottom graph shows the waiting times at the intersection. Like the normal flow, waiting times begin to increase as real vehicles accumulate. However, once ghost cars are introduced, the waiting times grow significantly higher and more erratic. At around the 75-second mark, the waiting time reaches a peak of nearly 70 seconds, far exceeding the peak seen in the normal traffic scenario. Even after this peak, the waiting times continue to fluctuate, reflecting the ongoing impact of ghost vehicles as they continue to disrupt traffic coordination. The total waiting time remains high throughout the simulation, contrasting sharply with the normal scenario, where waiting times decreased after vehicles cleared the intersection.

The introduction of ghost cars clearly increases both the vehicle count and waiting times at the intersection. Ghost vehicles create persistent congestion that forces real vehicles to experience delays far beyond what would occur under normal conditions. This demonstrates how a ghost car attack can severely disrupt traffic efficiency, causing significant delays and inefficiencies in vehicular coordination. In our simulation, the average waiting time at the intersection increased from approximately 18.4 seconds under normal traffic conditions to over 47.2 seconds during the peak of the ghost car scenario, representing a nearly 2.5 times increase in waiting time. Vehicle counts at the intersection peaked at nearly double the normal values due to the presence of ghost cars. Compared to other known VANET attacks such as Sybil attacks (which in past studies led 90 to 100% increase in delays), the ghost car scenario exhibited a more persistent disruption due to its illusion of continuous physical presence. This persistence caused ongoing false congestion, which is less transient than other attacks relying on identity duplication or message delays.

4- Discussion

To effectively mitigate the ghost car attack in VANETs, a combination of security measures, detection algorithms, and network protocols can be employed. Authentication is a fundamental strategy to ensure that only legitimate vehicles can participate in a VANET. By implementing digital signatures and certificates, vehicles are assigned unique identities issued by a trusted authority. This ensures that all messages exchanged within the network are signed and verified before being accepted. For example, a vehicle can sign its data with its private key, and other vehicles can verify it using the sender's public key. This prevents malicious nodes from introducing fabricated vehicles like ghost cars.

Reputation-based systems help in distinguishing between trustworthy and potentially malicious vehicles. Every vehicle is assigned a reputation score based on its behavior and the accuracy of its transmitted information. Vehicles that consistently send valid and reliable data gain a higher reputation score, while those that transmit suspicious data lose reputation. This system helps mitigate ghost car attacks by making it difficult for attackers to build a trusted presence in the network. If a vehicle is flagged due to suspicious behavior, its messages will be disregarded by other vehicles.

Position verification mechanisms involve cross-checking the physical location of a vehicle using multiple sources. Vehicles can utilize data from onboard sensors or communicate with nearby nodes to validate the claimed position of other vehicles. If discrepancies are detected, such as a vehicle claiming to be in a location that contradicts sensor data or network inputs, it is flagged as a potential ghost car. Time-stamping each message ensures that outdated or replayed messages cannot be used to manipulate the network. Every message transmitted includes a timestamp, and receiving vehicles check if the message is recent enough. If a ghost car tries to introduce old or delayed messages, they will be flagged as invalid due to incorrect timestamps. This prevents attackers from using replay attacks to create ghost cars.

Machine learning and anomaly detection techniques can be used to analyze vehicle behaviors and detect unusual patterns indicative of a ghost car attack. For instance, a ghost car might exhibit erratic movements, such as unrealistic speeds or sudden position changes, which can be detected through anomaly detection algorithms. Vehicles with abnormal behaviors are flagged and isolated from the network. Crowdsourced verification relies on the collective input from multiple vehicles to confirm the presence of other vehicles. When a suspicious vehicle is detected, nearby vehicles are asked to verify its existence through their own sensors or observations. If most vehicles report that the suspected vehicle is not present, it is flagged as a ghost car. Recommended machine learning algorithms include Random Forest and Deep Neural Networks due to their effectiveness in pattern recognition of anomalous vehicular behavior. Training these algorithms requires realistic traffic data, both normal and under attack conditions.

Secure neighbor discovery protocols ensure that vehicles can only communicate with legitimate and physically proximate nodes. This is done by verifying that vehicles are within a valid communication range before establishing a connection. If a vehicle claiming to be a neighbor is not detected within a reasonable distance using onboard sensors, it is flagged as suspicious. This strategy helps in detecting ghost cars by limiting communication to physically present vehicles, preventing attackers from injecting ghost vehicles from a distance.

Blockchain technology can be applied to VANETs to create an immutable and decentralized ledger of all vehicle communication. Each message exchanged between vehicles is recorded on the blockchain, ensuring that the data is secure, verifiable, and tamper-proof. In this scenario, ghost car data cannot be easily introduced into the network because every vehicle must be verified through the blockchain before its data is accepted. This decentralized security method significantly enhances the trustworthiness of VANET communications. However, implementation challenges include computational overhead, latency concerns, and the complexity of integrating with existing VANET infrastructures.

An Intrusion Detection System (IDS) for VANETs continuously monitors network traffic and detects abnormal patterns that could indicate security breaches, such as ghost car attacks. The IDS uses predefined rules or machine learning algorithms to identify deviations in vehicle behavior, such as unrealistic positions, speeds, or message contents. When suspicious behavior is detected, the system raises an alert, and further actions, such as isolating the suspicious vehicle, are taken to prevent network disruptions.

5- Conclusion

The findings from this study highlight the impacts of ghost car attacks on VANETs, particularly emphasizing disruptions to traffic efficiency and safety. The simulation results show clearly increased waiting times at intersections and inflated vehicle counts due to the artificial congestion generated by ghost vehicles. These disruptions reveal vulnerabilities in current VANET architectures, as ghost cars can persistently occupy virtual space, misleading legitimate traffic systems and causing delays. This research demonstrates that ghost car attacks have the potential to significantly degrade the operational reliability of intelligent transportation systems (ITS), compromising their primary functions of improving road safety, traffic efficiency, and overall driving experience. The practical implications are critical, as any degradation in VANET reliability directly impacts public safety, infrastructure efficiency, and user trust in vehicular technologies. Therefore, robust detection and mitigation strategies, such as leveraging machine learning, blockchain, and enhanced authentication methods, are essential to secure VANETs against ghost car threats effectively.

To ensure broader applicability of these findings, future research should address the generalizability of the proposed detection and mitigation strategies across different environments. Specifically, subsequent studies should simulate ghost car attacks in varied geographic settings, including both urban and rural areas with different infrastructure complexities. Testing these scenarios would reveal how diverse road types and adapting traffic densities influence the impact of ghost cars, providing insights for more universal mitigation strategies. Additionally, future studies should explore the effectiveness of the proposed detection mechanisms with different types of vehicles, including autonomous vehicles and traditional human-driven vehicles, to evaluate potential differences in susceptibility and response. Real-world testing or advanced simulations incorporating heterogeneous vehicle networks could further validate the practicality of proposed solutions. Exploring combined cyber threats, such as simultaneous ghost car and Sybil or replay attacks, could present deeper insights into the resilience of VANETs under compound threat scenarios. By thoroughly addressing these considerations, future research can substantially enhance the reliability and security of VANET-based transportation systems, contributing to safer and efficient traffic management worldwide.

6- Declarations

6-1- Author Contributions

Conceptualization, S.Y., S.F.A.R., and A.A.; methodology, I.N.D., M.S.S., and S.K.; software, I.N.D. and M.F.A.A.; writing—original draft preparation, I.N.D., S.F.A.R., M.F.A.A., and A.A.; writing—review and editing, S.Y., M.S.S., and S.K.; visualization, I.N.D. and S.Y.; funding acquisition, S.Y.; supervision, S.Y. All authors have read and agreed to the published version of the manuscript.

6-2- Data Availability Statement

The data presented in this study are available on request from the corresponding author.

6-3- Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

6-4- Institutional Review Board Statement

Not applicable.

6-5- Informed Consent Statement

Not applicable.

6-6- Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

7- References

[1] Bintoro, K. B. Y. (2024). Vehicular Ad-Hoc Networks for Intelligent Transportation System: A Brief Review of Protocols, Challenges, and Future Research. Jurnal Informatika Dan Sains: JISA, 7(2), 206–216. doi:10.31326/jisa.v7i2.2125.

[2] Abdelkader, G., Elgazzar, K., & Khamis, A. (2021). Connected vehicles: Technology review, state of the art, challenges and opportunities. Sensors, 21(22), 7712. doi:10.3390/s21227712.

[3] Topman, N., & Adnane, A. (2022). Mobile applications for connected cars: Security analysis and risk assessment. Proceedings of the IEEE/IFIP Network Operations and Management Symposium 2022: Network and Service Management in the Era of Cloudification, Softwarization and Artificial Intelligence, NOMS 2022, 1–6. doi:10.1109/NOMS54207.2022.9789873.

[4] Damaj, I. W., Yousafzai, J. K., & Mouftah, H. T. (2022). Future Trends in Connected and Autonomous Vehicles: Enabling Communications and Processing Technologies. IEEE Access, 10, 42334–42345. doi:10.1109/ACCESS.2022.3168320.

[5] Yu, W., Bai, W., Luan, W., & Qi, L. (2022). State-of-the-Art Review on Traffic Control Strategies for Emergency Vehicles. IEEE Access, 10, 109729–109742. doi:10.1109/ACCESS.2022.3213798.

[6] Almarshoud, M., Sabir Kiraz, M., & Al-Bayatti, A. H. (2024). Security, Privacy, and Decentralized Trust Management in VANETs: A Review of Current Research and Future Directions. ACM Computing Surveys, 56(10), 1–39. doi:10.1145/3656166.

[7] Lone, F., Verma, H. K., & Sharma, K. P. (2024). A systematic study on the challenges, characteristics and security issues in vehicular networks. International Journal of Pervasive Computing and Communications, 20(1), 56–98. doi:10.1108/IJPCC-04-2022-0164.

[8] Vamshi Krishna, K., & Ganesh Reddy, K. (2023). Classification of Distributed Denial of Service Attacks in VANET: A Survey. Wireless Personal Communications, 132(2), 933–964. doi:10.1007/s11277-023-10643-6.

[9] Chen, Y., Lai, Y., Zhang, Z., Li, H., & Wang, Y. (2022). Malicious attack detection based on traffic-flow information fusion. 2022 IFIP Networking Conference, IFIP Networking 2022, 1–9. doi:10.23919/IFIPNetworking55013.2022.9829793.

[10] Syla, V., Lala, A., & Biberaj, A. (2024). VANET security and privacy–an overview. EIRP Proceedings, 19(1), 414-423.

[11] Liu, X., Yang, L., Alvarez, I., Sivanesan, K., Merwaday, A., Oboril, F., Buerkle, C., Sastry, M., & Baltar, L. G. (2021). MISO-V: Misbehavior detection for collective perception services in vehicular communications. IEEE Intelligent Vehicles Symposium, Proceedings, 2021-July, 369–376. doi:10.1109/IV48863.2021.9575970.

[12] Chen, Y., Lai, Y., Zhang, Z., Li, H., & Wang, Y. (2023). MDFD: A multi-source data fusion detection framework for Sybil attack detection in VANETs. Computer Networks, 224, 109608. doi:10.1016/j.comnet.2023.109608.

[13] Farsimadan, E., Moradi, L., & Palmieri, F. (2025). A review on security challenges in V2X communications technology for VANETs. IEEE Access, 13, 31069 – 31094. doi:10.1109/ACCESS.2025.3541035.

[14] Elassy, M., Al-Hattab, M., Takruri, M., & Badawi, S. (2024). Intelligent transportation systems for sustainable smart cities. Transportation Engineering, 16. doi:10.1016/j.treng.2024.100252.

[15] Ullah, N., Khan, S. U., Niazi, M., Esposito, M., Khan, A. A., & Nasir, J. A. (2025). Solutions toCybersecurity Challenges in Secure Vehicle-to-Vehicle Communications: A Multivocal Literature Review. Information and Software Technology, 179, 107639. doi:10.1016/j.infsof.2024.107639.

[16] Zeadally, S., Guerrero, J., & Contreras, J. (2020). A tutorial survey on vehicle-to-vehicle communications. Telecommunication systems, 73(3), 469-489. doi:10.1007/s11235-019-00639-8.