Sybil Attack Prevention and Detection Mechanism in VANET Based on Multi-Factor Authentication

Ermias Melku Tadesse * , Abubeker Girma , Abebaw Mebrate

Posted Date: 18 November 2025

doi: 10.20944/preprints202511.1163.v1

Keywords: sybil attack; multi-factor authentication; detection rate; false positive rate and false negative rate

 doi:10.20944/preprints202511.1163.v1

Article

Sybil Attack Prevention and Detection Mechanism in VANET based on Multi-Factor Authentication

Ermias Melku Tadesse [1,*], Abubeker Girma [2] and Abebaw Mebrte [2]

[1] Department of Information Technology, Wollo University, Kombolcha Institute of Technology, Kombolcha, Ethiopia

[2] Department of Software Engineering, Wollo University, Kombolcha Institute of Technology, Kombolcha, Ethiopia

* Correspondence: ermiasmelku3400@gmail.com

Abstract

In recent years, there has been fast development within the area of vehicular ad hoc networks (VANET). In the future, VANET communication will play a first-rate position in improving the protection and performance of the transportation system. If security isn't always furnished in VANET, then it may result in apparent misapplication. One of the dangerous or risky attacks in VANETs is the Sybil, which forges fake identities inside the network to disrupt or compromise the communication among the network nodes. Sybil attacks have an effect on the carrier transport associated with road safety, traffic congestion, multimedia entertainment and others. Thus, VANETs claim for a security mechanism to prevent Sybil attacks. Within this context, this paper proposes a mechanism, known as Sybil Attack Prevention and Detection Mechanism in VANET based on Multi-Factor Authentication (SAPDMV), to detect Sybil attacks in VANETs based on Multi-Factor Authentication. The proposed system works based on the principle of registration, and use identification number, status, Maximum and minimal threshold value and security key for the verification. The paper proposes a Sybil Attack Prevention and Detection Mechanism in VANET (SAPDMV) based on multifactor authentication. The mechanism uses vehicle identification, status, security key, and both minimum and maximum speed thresholds to authenticate nodes and detect Sybil attacks. Implemented and tested using Network Simulator-2.35, the system demonstrates an improved detection rate, reduced false positive and false negative rates, and enhanced network performance metrics such as end-to-end delay, throughput, and packet delivery ratio. The simulation result shows our proposed algorithm enhances detection rate, false positive rate, and false negative rate. The proposed solution is improved to 96%, 5%, and 4%, respectively, compared with the Sybil attack-AODV and existing/old work. The approach is scalable and effective in real-world VANET environments, making it a promising framework for future intelligent transportation systems.

Keywords: sybil attack; multi-factor authentication; detection rate; false positive rate and false negative rate

1. Introduction

In the last few years, Vehicular Ad Hoc Networks (VANETs) became popular and attractive for services delivery to end users, such as traffic security, mobility efficiency, infotainment, safety navigation, etc.[1]. This fact promoted VANET deployment investments by several vehicles manufacturers and public transport authorities. The communication between vehicles in VANETs is based on short-range communications without the need of an infrastructure on the roads (RSUs). VANETs are composed by fast mobile self-organized nodes, resulting in a high mobility distributed nodes and frequently changing topology environment[2].

A VANET is a system that does not depend on any central system for giving communication among the claimed-On Board Units (OBUs) in adjacent vehicles, and among OBUs and nearby fixed

 doi:10.20944/preprints202511.1163.v1

framework RSU utilizing a method called, Dedicated Short Range Communication (DSRC)[3]. VANET have lack of central management and highly dynamically change of topology. Due to this nature the network, VANETs are prone to different challenges such as network management, congestion and collision control, environmental impact, social and economic challenges and security in VANET[4]. Securely communicate over the VANETs are key idea which attract an attention of many researchers now a day.

Vehicular Ad-hoc Networks (VANETs) are a subset of Mobile Ad-hoc Networks (MANETs). They are deployed to introduce the ability of inter-communication amongst vehicles if you want to assure safety and offer offerings for humans while driving[5]. Vehicular Ad Hoc Networks (VANETs) have a way attaining software potentials with inside the Intelligent Transportation System (ITS) consisting of traffic management, coincidence avoidance and in-vehicle infotainment. However, security has continually been a project to VANETs, which might also additionally purpose extreme damage to the ITS[5]. Despite the current evolution of VANETs, security, data integrity and customers privateness facts are primary concerns, on account that attacks prevention continues to be open issue. One of the maximum risky attacks in VANETs is the Sybil, which forges fake identities with inside the community to disrupt compromise the conversation among the community nodes. Sybil attacks have an effect on the service delivery related to road safety, traffic congestion, multimedia amusement and others [6]. Sybil attack is taken into consideration as a serious security threat to VANETs because the adversary can disseminate fake messages with a couple of forged identities to attack numerous programs with inside the ITS[5].

So, it is necessary to have some preventive mechanism against these attacks. In [6] author has been proposed a technique to detect and isolate Sybil attack in VANET by using neighboring information. But this research work has some limitation (1) after verified identification number does not check the status of vehicles. (2) If the internal node becomes a malicious node this algorithm will not detect and isolate the Sybil attack.

Contributions

- Proposed a Sybil Attack Prevention and Detection Mechanism in VANET (SAPDMV) based on multi-factor authentication, integrating identification number, status, security key, and both minimum and maximum speed thresholds for node verification.
- Enhanced detection accuracy by using precise threshold values, resulting in a high detection rate and reduced false positive and false negative rates compared to existing schemes.
- Implemented and tested the mechanism using Network Simulator-2.35, demonstrating superior performance in key network metrics such as end-to-end delay, throughput, and packet delivery ratio.
- Addressed limitations of previous approaches by allowing nodes without identification numbers to reattempt registration and by verifying both minimum and maximum speed thresholds to prevent misclassification of legitimate and malicious nodes.
- Provided a robust and scalable solution for securing vehicular networks against Sybil attacks, making it suitable for real-world intelligent transportation systems.

2. Related Work

As one way of data collection tool, the researcher tried to review the papers with related works on Sybil attack detection.

Table 1. Related Work.

Author/Reference	Simulation	Method	Strength	Weakness
Soyoung Park[7]	NS2/Custom	Time Stamp Series	Detects Sybil nodes using time stamp similarity	Detection slow if RSUs are far apart; ineffective if

 doi:10.20944/preprints202511.1163.v1

				attacker stays under one RSU
Pareek et al.[8]	NS2/Custom	MAC Address Check	Prevents duplicate MAC addresses	MAC addresses can be spoofed by attackers
P. Gu et al. [9]	NS2/Custom	Machine Learning (KNN, SVM)	High accuracy in classification	High runtime complexity; limited to light traffic and rational model attacks
Hamed et al.[10]	NS2/Custom	Infrastructure Observation	Observes moving dynamics for detection	Requires RSU synchronization; soft identification reduces efficiency
Reddy et al.[11]	NS2/Custom	Digital Signatures	Uses encrypted signatures for identity verification	Does not consider vehicle mobility; limited in high mobility/density
Sharma et al.[12]	NS2/Custom	Short-lived Pseudo Certificates	Provides privacy and anonymity	Depends on vehicle feedback; does not consider vehicle behavior
Eziama et al.[13]	NS2/Custom	Bayesian Neural Network	Probabilistic modeling for node identification	Does not consider mobility patterns; lacks adaptability
Saggi & Kaur[6]	NS2/Custom	Neighboring Information	Uses identification and speed threshold	Does not check vehicle status; cannot detect internal malicious nodes

To address these limitations, we propose a Sybil Attack Prevention and Detection Mechanism in VANET based on Multi-Factor Authentication (SAPDMV), which enhances Sybil attack detection. Our approach integrates both minimum and maximum threshold values along with identification number, status, and security key verification. The proposed algorithm investigates VANET security by validating vehicles' identity and behavior through multi-factor authentication, leveraging the AODV routing protocol for reliable and secure communication.

3. Methodology

3.1. Design and Development of the Proposed Algorithm

The methodology of the paper proposes a Sybil Attack Prevention and Detection Mechanism in VANET (SAPDMV) based on multi-factor authentication. The approach involves the following steps:

- Each vehicle and Roadside Unit (RSU) is registered by a trusted authority, ensuring only registered vehicles are considered legitimate.
- During registration, the RSU assigns each vehicle an identification number, status, security key, and both minimum and maximum speed threshold values.
- Vehicles must register with the RSU before joining the network, and their legitimacy is verified based on these multi-factor criteria.
- When a vehicle requests to join the network, the RSU checks its identification number, status, security key, and speed against stored values.

 doi:10.20944/preprints202511.1163.v1

- If all criteria are met, the vehicle is permitted to communicate; otherwise, it is rejected as a potential Sybil node.
- The mechanism is implemented and tested using Network Simulator-2.35, with simulation parameters including varying numbers of nodes, malicious nodes, and vehicle speeds.
- The performance of the proposed system is compared with existing schemes and AODV with Sybil attack, focusing on detection rate, false positive rate, false negative rate, end-to-end delay, throughput, and packet delivery ratio.

Figure 1 illustrates the proposed VANET architecture, which consists of vehicles equipped with On-Board Units (OBUs) and Roadside Units (RSUs) deployed along the roadside. The OBUs enable communication between vehicles (V2V) and between vehicles and RSUs (V2I). The RSUs are static and interconnected, extending the communication range and providing services such as traffic updates, safety alerts, and internet access. Vehicles register with a trusted authority through the RSU, which assigns identification numbers, security keys, and speed thresholds. The architecture ensures that only registered and authenticated vehicles can join the network, enhancing security and reliability. The dynamic nature of VANET allows vehicles to form ad-hoc networks, with the RSUs supporting data forwarding and network management. This setup facilitates efficient and secure communication in vehicular environments, supporting applications like traffic management, safety, and infotainment.

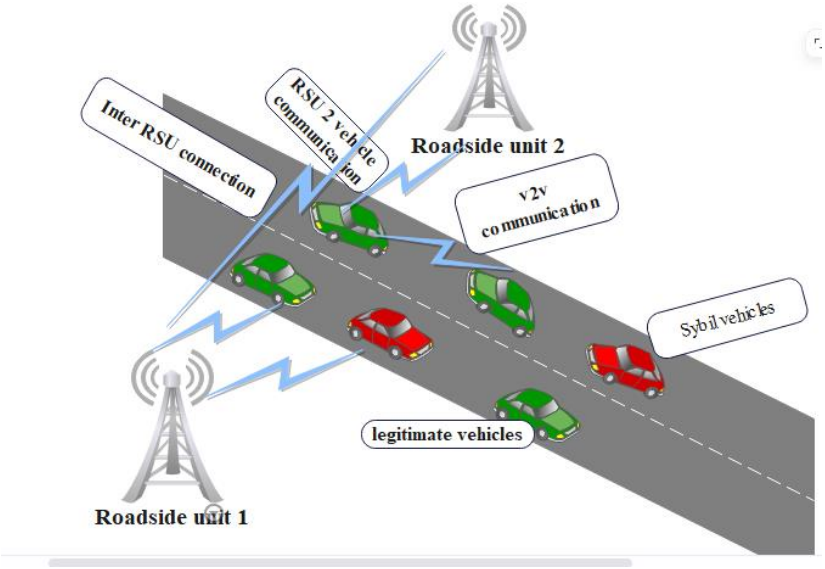

Figure 1. VANET proposed architecture.

Figure 2, the flowchart for the proposed methodology, outlines the step-by-step process for detecting and rejecting Sybil attacks in VANET using the SAPDMV mechanism. The flowchart begins with a vehicle sending a Hello message to the Roadside Unit (RSU) to request network access. The RSU then sets the maximum and minimum speed threshold values and compares the vehicle's speed with these thresholds. If the speed is within the allowed range, the RSU requests the vehicle's identification number and checks it against the stored registered vehicle IDs. Next, the RSU asks for the vehicle's security key and verifies it. The RSU also checks the vehicle's status; if the status is offline (0), the vehicle is considered legitimate and allowed to communicate. If any of these checks fail such as incorrect identification, security key, or status, or if the speed is outside the threshold the vehicle is detected as a Sybil node and rejected from the network. The flowchart visually represents these sequential verification steps, ensuring only legitimate vehicles are permitted to join the network while effectively isolating potential Sybil attackers.

 doi:10.20944/preprints202511.1163.v1

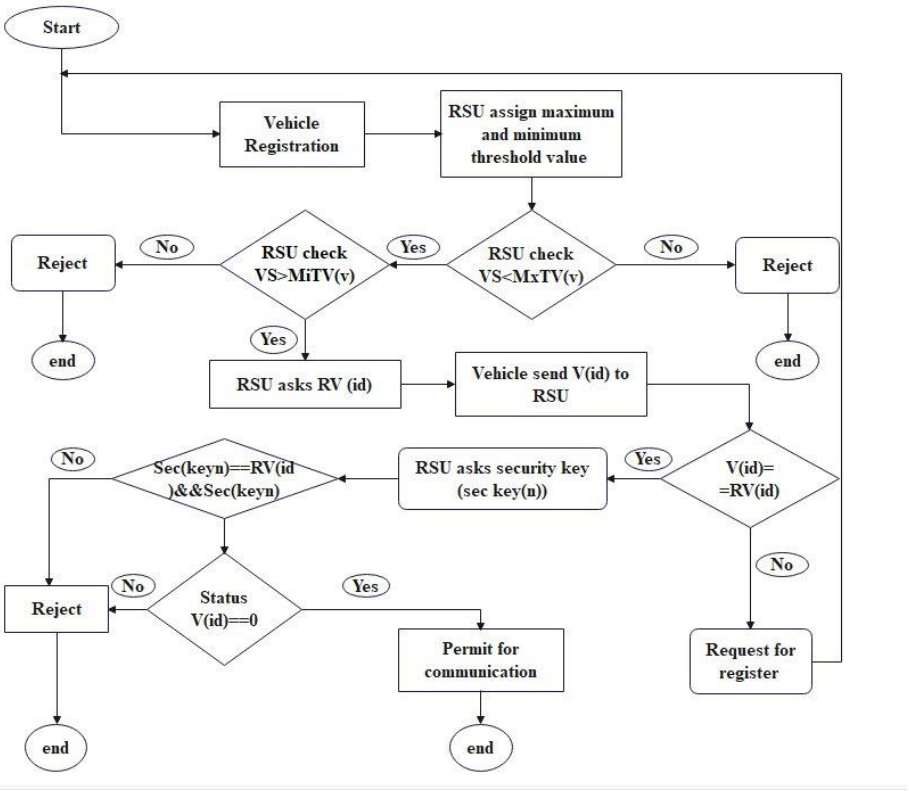

Figure 2. Flowchart for proposed Methodology.

The description of abbreviation words on flowchart is:
V (id): vehicle id which send a request.
Sec key (id): security key of RV (id).
STV: status of vehicle (either 0 or 1).
RV (id): registered vehicle id.
VS: vehicle speed V (id).
TV: threshold value
MxTV: maximum threshold value
MiTV: minimum threshold value and
R: an RSU.

The general steps of the input are:

1. Vehicle sends a Hello message to the RSU to request network access.
2. RSU sets maximum and minimum speed threshold values for the vehicle.
3. RSU compares the vehicle's speed with the stored threshold values.
4. RSU requests the vehicle's identification number and checks it against registered IDs.
5. RSU asks for the vehicle's security key and verifies it.
6. RSU checks the vehicle's status to determine if it is offline (legitimate) or online (duplicate).
7. If all checks pass, the vehicle is permitted to communicate; otherwise, it is rejected as a Sybil node.

3.2. Legitimate and Sybil Vehicle Detection

Legitimate and Sybil vehicle detection is described through two main scenarios:

Scenario One (**legitimate vehicle**)

A legitimate vehicle sends a Hello message to the RSU. The RSU verifies its identification number, status, security key, and speed. If all checks pass identification matches, status is offline,

 doi:10.20944/preprints202511.1163.v1

security key is correct, and speed is within the threshold the vehicle is permitted to communicate as a legitimate node.

Figure 3 illustrates the legitimate vehicle detection process in the proposed VANET architecture. The diagram shows a legitimate vehicle sending a Hello message to the Roadside Unit (RSU) to request network access. The RSU then verifies the vehicle's identification number, status, security key, and speed against stored values. If the identification matches, the status is offline, the security key is correct, and the speed is within the allowed threshold, the vehicle is recognized as legitimate and permitted to communicate within the network. The figure visually represents these verification steps, emphasizing that only vehicles meeting all authentication criteria are allowed to join, ensuring secure and reliable communication in the VANET environment.

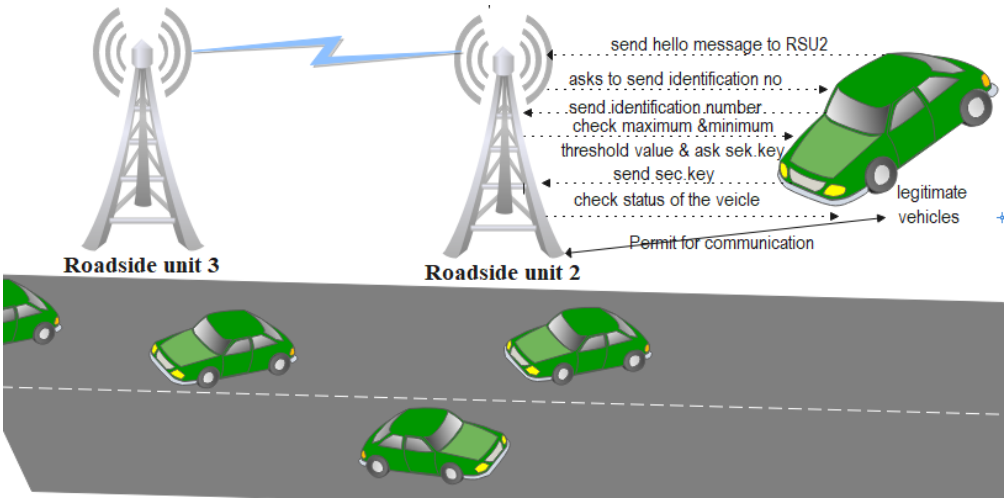

Figure 3. Legitimate vehicle detection.

The step-by-step detection process in Figure 3 for legitimate vehicle detection is as follows:

1. A vehicle sends a Hello message to the Roadside Unit (RSU) to request network access.
2. The RSU sets the maximum and minimum speed threshold values for the vehicle.
3. The RSU compares the vehicle's speed with the stored threshold values.
4. If the speed is within the allowed range, the RSU requests the vehicle's identification number and checks it against the registered vehicle IDs.
5. The RSU asks for the vehicle's security key and verifies it.
6. The RSU checks the vehicle's status to determine if it is offline (legitimate) or online (duplicate).
7. If all checks pass identification matches, status is offline, security key is correct, and speed is within the threshold the vehicle is recognized as legitimate and permitted to communicate within the network.

This process ensures that only vehicles meeting all authentication criteria are allowed to join, maintaining secure and reliable communication in the VANET environment.

Scenario Two (Sybil Vehicle):

Case 1: The vehicle sends a fake identification number; the RSU rejects it immediately.

Case 2: The vehicle sends a stolen identification number, but its speed is outside the threshold (e.g., too slow); the RSU rejects it.

Case 3: The vehicle sends a stolen identification number, but its status is online (indicating duplication); the RSU rejects it.

Case 4: The vehicle sends a stolen identification number, but cannot provide the correct security key; the RSU rejects it as a Sybil node.

These scenarios ensure that only vehicles meeting all authentication criteria are allowed to join the network, while Sybil attackers are detected and rejected at various stages of the verification process

 doi:10.20944/preprints202511.1163.v1

Figure 4 illustrates the Sybil vehicle detection process in the proposed VANET architecture. The diagram shows how a malicious (Sybil) vehicle attempts to join the network by sending a Hello message to the Roadside Unit (RSU). The RSU then checks the vehicle's identification number, speed, status, and security key. If the vehicle provides a fake or stolen identification number, its speed is outside the allowed threshold, its status is already online (indicating duplication), or it cannot provide the correct security key, the RSU rejects the vehicle as a Sybil node. The figure visually represents these rejection cases, highlighting the multi-factor authentication steps that ensure only legitimate vehicles are allowed to communicate, while Sybil attackers are detected and isolated at various stages of the verification process.

The detection algorithm steps represented in Figure 4 are as follows:

1. A vehicle sends a Hello message to the Roadside Unit (RSU) to request network access.
2. The RSU sets the maximum and minimum speed threshold values for the vehicle.
3. The RSU compares the vehicle's speed with the stored threshold values.
4. If the speed is within the allowed range, the RSU requests the vehicle's identification number and checks it against the registered vehicle IDs.
5. The RSU asks for the vehicle's security key and verifies it.
6. The RSU checks the vehicle's status to determine if it is offline (legitimate) or online (duplicate).
7. If all checks pass identification matches, status is offline, security key is correct, and speed is within the threshold the vehicle is permitted to communicate.
8. If any check fails (e.g., fake or stolen identification, speed outside threshold, status online, or incorrect security key), the vehicle is detected as a Sybil node and rejected from the network.

These steps ensure that only legitimate vehicles are allowed to join the network, while Sybil attackers are detected and isolated at various stages of the verification process.

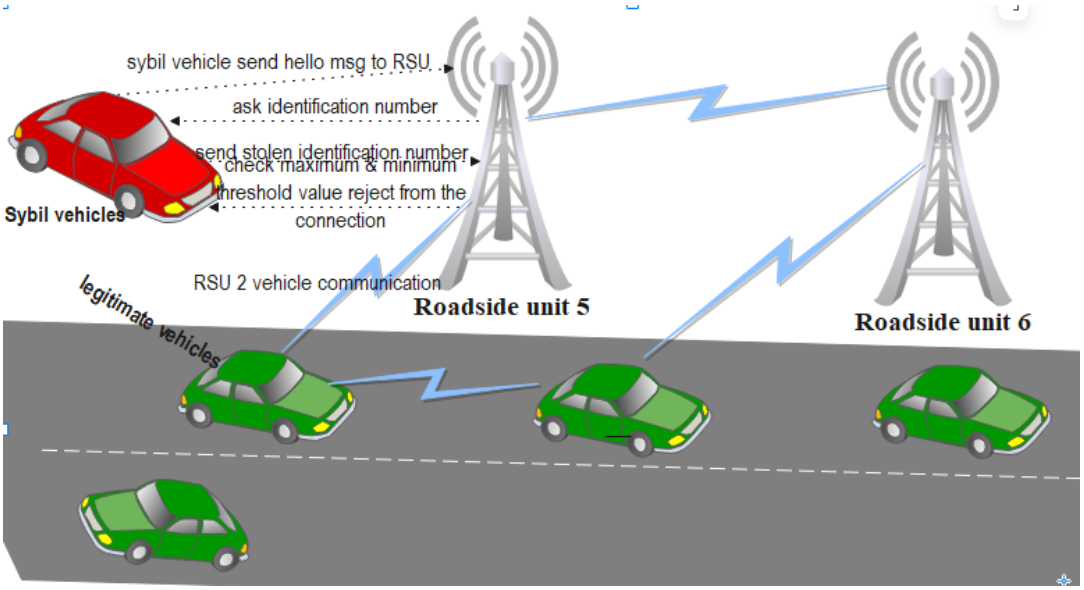

Figure 4. Sybil vehicle detection.

Algorithm 1: Detection and Rejection Algorithm
Step1: Registration Process Start on R
Step 2: V[id] communication with "Hello message" with R
R set threshold value
if (SV (V [id]) < MxTV) && (SV(v[id])> MiTV) &&
Step3: R check V[id] = = RV [id] &&
R ask to send RV [id] security key
V[id] send Sec key[id] to R
if (Sackey[id] = = RV [id]) && Sec key[id] &&

 doi:10.20944/preprints202511.1163.v1

(STV [id] = = 0) then
Vehicle is detected as legitimate vehicle& communication being between vehicle
else
Vehicle is detected as Sybil vehicle
end if
else
vehicle is detected as Sybil vehicle
end if
else
vehicle is detected as Sybil vehicle
end if
Step4: if new vehicle detected as legitimate node, then
R stores STV [id] = 1 to R
end if
Step5: if V[id] = = detected as Sybil vehicle then
isolate Sybil vehicle with its ID
end if
Step6: if V[id] is not registered V[id]! = RV [id] then V[id] should have been first request for register registration
end if
else
vehicle is detected as Sybil vehicle
end if

3.3. Experimental Setup

Simulation

Network Simulator-2.34 (NS2) and a 3 m to 3000 m simulation area are used to run the simulation[14]. The suggested protocol was put into practice using the simulation parameters given in Table 2, and its effectiveness was compared with the performance of existing routing methods.

Table 2. Simulation parameters.

Parameters	Value
Simulator NS2	Version Ns-allinone-2.35
Simulation Area (Grid Size)	3m x 3000m
Total number of nodes	50
Number Simulated node	10,15,20,25,30,35,40,45,50
Number of malicious nodes	36,38,40,49
Number of static nodes	21,22,24,27,28,29,30,33
Maximum Vehicle speed	50m/s
Minimum vehicle speed	20m/s
Routing protocol	AODV
Packet size	512kb
Packet type	TCP
Node Communication range	3000m

 doi:10.20944/preprints202511.1163.v1

Simulation Time	150sec
Antenna model	Omnidirectional Antenna

4. Result and Discussions

The results and discussion section evaluates the performance of the proposed Sybil Attack Prevention and Detection Mechanism in VANET (SAPDMV) using simulation and comparative analysis. The simulation was conducted using Network Simulator-2.35, with various scenarios involving different numbers of nodes and malicious vehicles. The proposed mechanism was compared with existing schemes and AODV with Sybil attack, focusing on key metrics such as detection rate, false positive rate, false negative rate, end-to-end delay, throughput, and packet delivery ratio.

4.1. Analyzing Trace Files

To analyzing the trace files, we have used NS2 version 2.35 simulation tool. We have analyzed the security detection algorithm and performance of the network related to speed and number of legitimate and malicious vehicles in the network with respect to the existing algorithms. Also, we have analyzed the simulation result using 10, 15, 20, 25, 30, 35, 40, 45 and 50 nodes, and 20, 25, 30, 35, 40, 45, 50, 55 and 60 speed of vehicles in m/s. Analysis of proposed algorithm security and network performance are done with respect to existing work based on simulation results.

4.2. Performance Metrics

The performance metrics used in the paper evaluate the effectiveness of the proposed Sybil Attack Prevention and Detection Mechanism in VANET (SAPDMV). These metrics include:

- Detection Rate: The proportion of Sybil attacks correctly identified by the system.
- False Positive Rate: The ratio of legitimate vehicles incorrectly flagged as Sybil nodes.
- False Negative Rate: The ratio of Sybil vehicles that are not detected by the system.
- End-to-End Delay: The time taken for a packet to travel from source to destination, indicating network responsiveness.
- Throughput: The amount of data successfully transmitted per unit time, reflecting network efficiency.
- Packet Delivery Ratio (PDR): The percentage of packets successfully delivered to their destination, measuring reliability.
- Computation Time: The time required for authentication and verification processes, affecting real-time performance.

These metrics collectively assess the security, reliability, and efficiency of the proposed mechanism, ensuring robust protection against Sybil attacks while maintaining high network performance.

4.2.1. Malicious Node Detection Rate (DR)

In our simulation result, Figure 5 in the document illustrates the detection rate comparison under Sybil attack for the proposed Sybil Attack Prevention and Detection Mechanism in VANET based on Multi-Factor Authentication (SAPDMV) against existing algorithms and AODV with Sybil attack. The detection rate (DR) measures the accuracy of the algorithm in identifying malicious nodes from normal nodes. According to the text, the proposed algorithm achieves a detection rate of 100% when there are up to 15 malicious nodes, but the rate declines as the number of malicious nodes increases beyond that threshold. The average detection rate for the proposed algorithm is 96%, which is higher than the existing algorithms and AODV with Sybil attack. This improvement is attributed to the use of more precise threshold values in the proposed system, making it more effective at detecting Sybil attacks compared to the baseline schemes.

 doi:10.20944/preprints202511.1163.v1

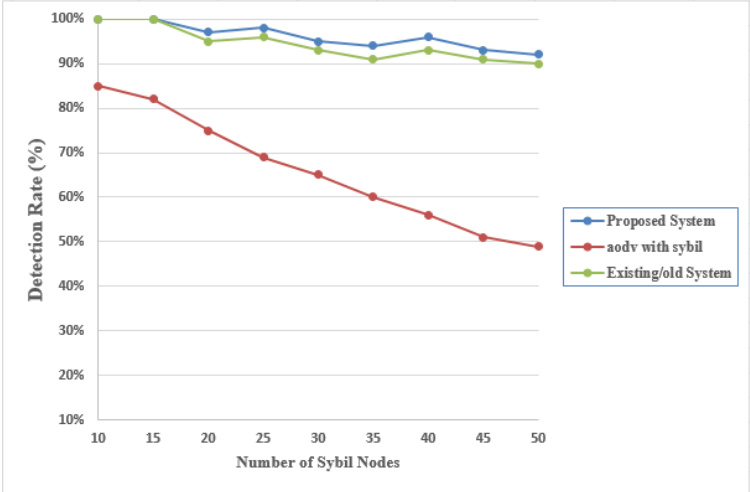

Figure 5. Detection Rate comparison under Sybil attack.

4.2.2. False Negative Rate (FNR)

In our simulation result, Figure 6 illustrates the False Negative Ratio (FNR) under Sybil attack for the proposed Sybil Attack Prevention and Detection Mechanism in VANET based on Multi-Factor Authentication (SAPDMV), compared to existing algorithms and AODV with Sybil attack. The False Negative Ratio measures the proportion of legitimate vehicles that are incorrectly identified as malicious nodes. According to the document, the average FNR for the proposed algorithm is 4%, which is significantly lower than the existing schemes. The FNR remains at zero for up to 20 Sybil attack nodes, but increases slightly as the number of malicious nodes grows beyond that threshold. The proposed algorithm demonstrates a minimal false negative rate, indicating its effectiveness in correctly identifying legitimate vehicles and reducing misclassification compared to baseline approaches.

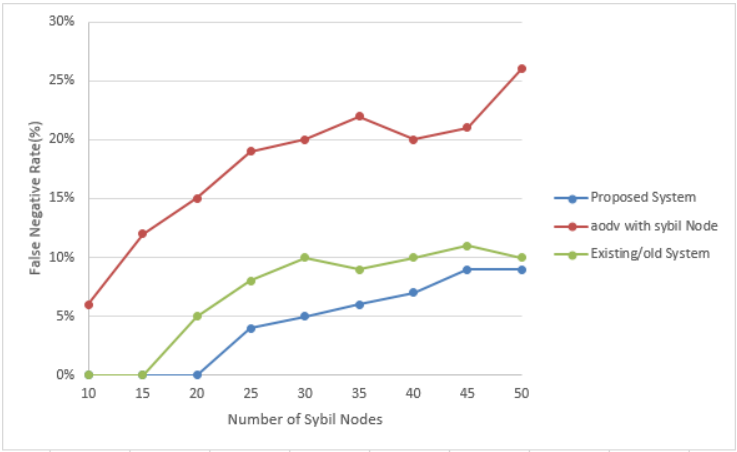

Figure 6. False Negative Ratio under Sybil attack.

4.2.3. False Positive Rate (FPR)

In our simulation result, Figure 7 presents the False Positive Ratio (FPR) under Sybil attack for the proposed Sybil Attack Prevention and Detection Mechanism in VANET based on Multi-Factor Authentication (SAPDMV), compared to existing algorithms and AODV with Sybil attack. The False Positive Ratio measures the proportion of malicious nodes that are incorrectly identified as legitimate nodes. According to the document, the average FPR for the proposed algorithm is 5%. The figure shows that as the number of Sybil nodes increases, there is only a very small increase in the FPR,

 doi:10.20944/preprints202511.1163.v1

indicating that the proposed algorithm maintains a low false positive rate even with a higher number of malicious nodes. This demonstrates the algorithm's effectiveness in minimizing misclassification of malicious nodes as legitimate, outperforming the baseline schemes in terms of accuracy and reliability

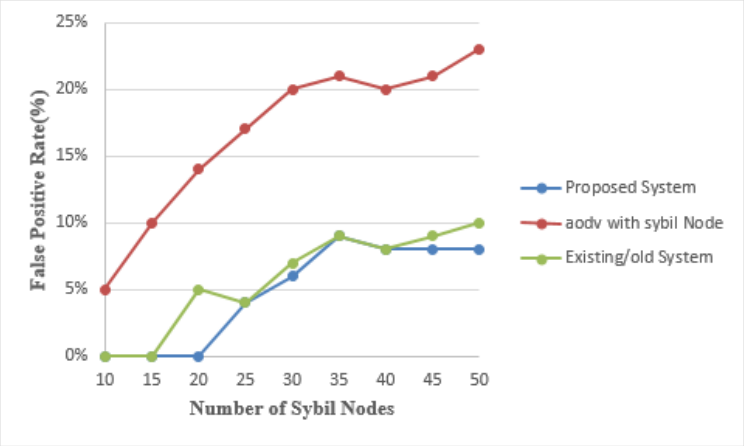

Figure 7. False Positive Ratio under Sybil attack.

4.2.4. End-to-End Delay (E2E):

In our simulation result, Figure 8 illustrates the end-to-end (E2E) delay with respect to the number of vehicles in the network for the proposed Sybil Attack Prevention and Detection Mechanism in VANET based on Multi-Factor Authentication (SAPDMV), compared to AODV with Sybil attack and existing benchmark systems. The end-to-end delay is defined as the average time taken by data packets to travel from the sender to the receiver, including all possible delays such as buffering, queuing, and retransmission. According to the document, the proposed algorithm demonstrates a significantly lower communication delay compared to both AODV with Sybil attack and the existing benchmark systems across different numbers of vehicles. This indicates that the proposed mechanism is more efficient in minimizing delays, thereby improving the overall network performance and reliability in VANET environments.

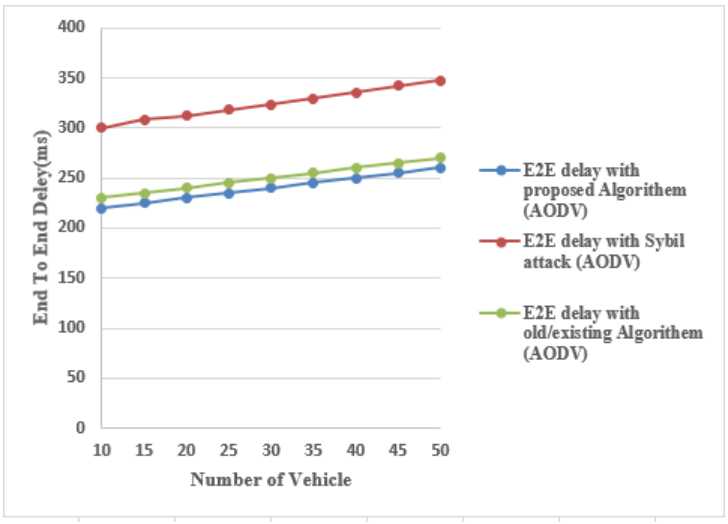

Figure 8. E2E delay respect to No of vehicles.

4.2.5. Throughput

In our simulation result, Figure 9 illustrates the throughput with respect to the number of vehicles in the network for the proposed Sybil Attack Prevention and Detection Mechanism in

 doi:10.20944/preprints202511.1163.v1

VANET based on Multi-Factor Authentication (SAPDMV), compared to AODV with Sybil attack and existing benchmark algorithms. Throughput measures the actual amount of data successfully transmitted across the network per unit time. According to the document, the throughput of the proposed algorithm is considerably higher than both AODV with Sybil attack and the existing benchmark algorithms. As the number of vehicle nodes increases, the throughput of all systems tends to decline, but the proposed system maintains a higher throughput even with increased node density. This demonstrates the robustness and efficiency of the proposed mechanism in handling data transmission under varying network loads, making it more suitable for real-world VANET applications.

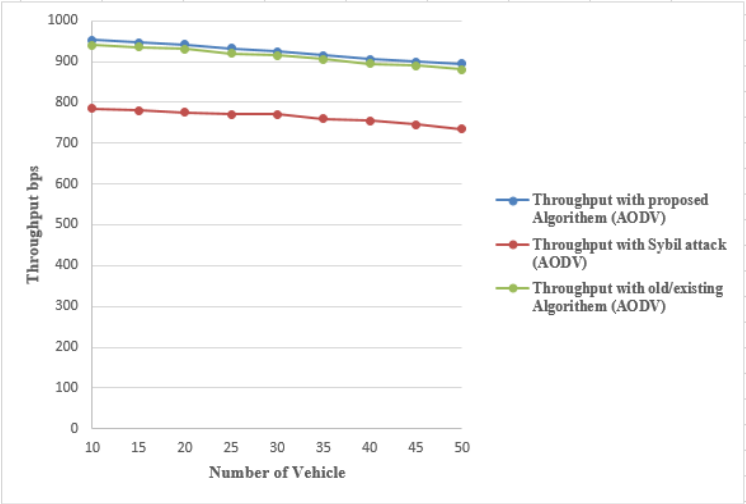

Figure 9. Throughput respect to No of vehicles.

4.2.6. Packet Deliver Ratio (PDR)

In our simulation result, Figure 10 illustrates the Packet Delivery Ratio (PDR) with respect to the number of vehicles in the network for the proposed Sybil Attack Prevention and Detection Mechanism in VANET based on Multi-Factor Authentication (SAPDMV), compared to AODV and existing benchmark algorithms. The PDR measures the percentage of packets successfully received by the destination vehicles out of the total packets sent by the source vehicles. According to the document, the PDR of the proposed algorithm is higher than both AODV and existing benchmark systems, especially when the vehicle density is low. As the number of vehicles increases, the PDR tends to decrease due to the impact of Sybil attacks and network congestion, but the proposed system maintains a better delivery ratio than the baseline schemes. This demonstrates the effectiveness of the proposed mechanism in ensuring reliable packet delivery even under challenging network conditions.

 doi:10.20944/preprints202511.1163.v1

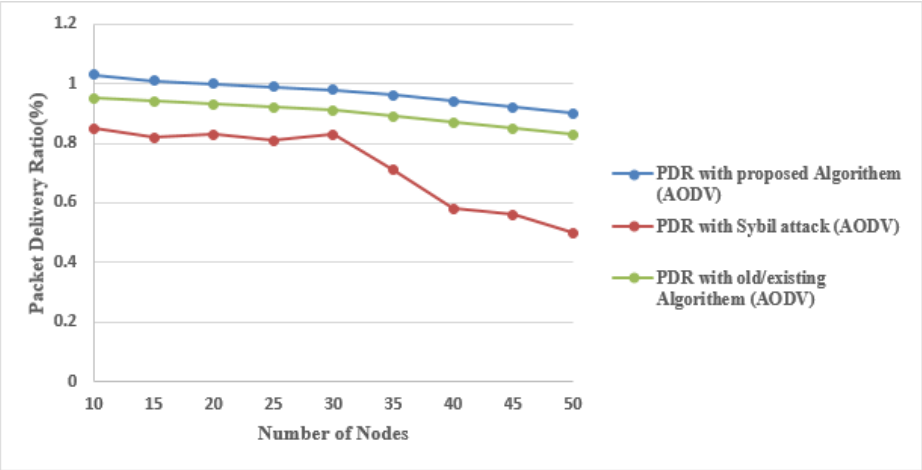

Figure 10. PDR respect to No of vehicles.

5. Conclusions

The paper concludes that the proposed Sybil Attack Prevention and Detection Mechanism in VANET (SAPDMV), based on multi-factor authentication, significantly enhances the security and reliability of vehicular networks. Through extensive simulation, the system demonstrated superior performance in detecting malicious nodes, minimizing false positives and negatives, and maintaining high packet delivery ratios, throughput, and low end-to-end delays. The multi-factor approach—including vehicle identification, status, security keys, and speed thresholds—proved effective in accurately identifying legitimate vehicles and extricating Sybil attackers, even under high node density and mobility conditions. The results affirmed that SAPDMV is a robust and scalable solution capable of mitigating Sybil threats in real-world VANET scenarios. Ultimately, this mechanism offers a promising framework for future vehicular network security, fostering safer and more efficient intelligent transportation systems. The paper emphasizes the importance of continuous refinement and real-world testing to further adapt the approach to evolving attack vectors, ensuring resilient vehicular communication infrastructure.

The paper recommends the adoption of the proposed Sybil Attack Prevention and Detection Mechanism in VANET (SAPDMV) for securing vehicular networks. The mechanism, based on multi-factor authentication, demonstrates high detection accuracy, low false positive and false negative rates, and improved network performance metrics. It is suggested that future research should focus on enhancing the scalability of the system for larger networks and integrating adaptive learning techniques to counter evolving attack strategies. Additionally, the paper recommends further exploration of real-time deployment and field testing to validate the mechanism's effectiveness in diverse traffic conditions and urban environments.

References

1. K. Tanuja, "A Survey on VANET Technologies," vol. 121, no. 18, pp. 1–9, 2015.
2. P. Gu, R. Khatoun, Y. Begriche, A. Serhrouchni, and T. Paristech, "Vehicle Driving Pattern Based Sybil Attack Detection," pp. 1282–1288, 2016, doi: 10.1109/HPCC-SmartCity-DSS.2016.216.
3. S. A. Syed, "Merged technique to prevent SYBIL Attacks in VANETs," *2019 Int. Conf. Comput. Inf. Sci.*, pp. 1–6, 2019.
4. I. Transportation, S. Committee, I. Vehicular, and T. Society, IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture IEEE Vehicular Technology Society. 2013.
5. M. Khalil and M. A. Azer, "Scheme in Vehicular Ad-Hoc Networks," pp. 184–186, 2018.
6. M. K. Saggi, "Isolation of Sybil Attack in VANET using Neighboring Information," pp. 46–51, 2015.
7. J. Grover, "A Sybil Attack Detection Approach using Neighboring Vehicles in VANET," pp. 151–158, 2011.

 doi:10.20944/preprints202511.1163.v1

8. A. Pareek, "Detection and Prevention of Sybil Attack in MANET using MAC Address," vol. 122, no. 21, pp. 20–23, 2015.
9. P. Gu, R. Khatoun, Y. Begriche, A. Serhrouchni, and T. Paristech, "k-Nearest Neighbours Classification Based Sybil Attack Detection in Vehicular Networks".
10. H. Hamed, "Sybil Attack Detection in Urban VANETs Based on RSU Support," *Electr. Eng. (ICEE), Iran. Conf.*, pp. 602–606, 2018, doi: 10.1109/ICEE.2018.8472629.
11. D. S. Reddy and V. Bapuji, "Sybil Attack Detection Technique Using Session Key Certificate in Vehicular Ad Hoc Networks," pp. 2–6.
12. A. K. Sharma, "Sybil Attack Prevention and Detection in Vehicular Ad hoc Network," pp. 594–599, 2016.
13. E. Eziama, K. Tepe, A. Balador, K. S. Nwizege, and L. M. S. Jaimes, "Malicious Node Detection in Vehicular Ad-Hoc Network Using Machine Learning and Deep Learning," *2018 IEEE Globecom Work. (GC Wkshps)*, pp. 1–6, 2018.
14. S. Agrawal and R. Lingawar, "Application of Ns2 To Overcome Computer Networks Attacks," *World Res. J. Comput. Archit.*, vol. 1, no. 1, pp. 6–10, 2012.