International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Identity Spoofing Sybil Attack Protective Measures using Physical & Logical Address Mapping for the VANET (ISPLM)

[1]Ms. Shubhra Mukherjee Mathur, [2]Dr. Prof. Ravindra Gupta

Submitted: 11/01/2024 **Revised**: 17/02/2024 **Accepted**: 25/02/2024

Abstract: Vehicular Ad Hoc Networks (VANETs) is a kind of ad hoc network that enables communication among vehicle to vehicle (V2V) and between vehicles and roadside infrastructure (V2I). VANETs are a sub class of mobile ad hoc network (MANET) and have unique characteristics and challenges due to the dynamic nature of vehicular environment. The main challenges such as topology unsustainable and security, due to movement of vehicle is dynamic which directly or indirectly monitored or guided by road side units (RSUs) somehow resolve the problem of topology. Other side vehicular ad hoc network is unsecure due to various attack spread into network such are traffic jamming, denial of service, routing misbehavior, identity spoofing etc. In the previous research, the a few of security issues are resolve through the hardware or software based approach, out of above insecurity identity spoofing is one of the major challenging attack because its generate false identity to capture the data packet as a legitimate user. In this article resolve the issue of identity spoofing attack using physical & logical address mapping (ISPLM), the identity spoofing is a kind of sybil attack where vehicle capture the identity of other vehicle and represent as a genuine receiver in the network. Sybil attacks are two types which are same time multiple identities and different time generates multiple identities to gain the network data and spread insecurity in VANET. The proposed ISPLM security technique is inbuilt in the RSU's which keep records of every vehicle related to logical into physical address mapping and if they found multiple logical address mapped with one physical address than detected identity treated as attacker vehicle and block from the communication. The overall security system produce secure communication which finally compare with existing AODV-WA and AODV-Sybil and get analysis in terms of throughput, packet delivery ratio, routing overhead, true false positive ratio and infection percentage.

Keywords: *VANET, Sybil, Routing, Security, AODV.*

1. Introduction

Vehicular Ad Hoc Networks, also known as VANETs, have become an essential component of intelligent transportation systems as a result of the significant improvements that have been made in wireless communication technology for vehicles. In order to improve road safety, traffic efficiency, and the overall driving experience, these networks make it possible for cars to interact with one another as well as with the infrastructure that is located along the roadside. On the other hand, due to the fact that VANETs are open and dynamic, they are vulnerable to a wide range of security concerns, such as identity spoofing and Sybil attacks.

A Sybil attack in Vehicular Ad Hoc Networks (VANETs) refers to a security threat where a malicious entity creates multiple fake identities, known as Sybil nodes, to compromise the integrity and functionality of the network. This type of attack is particularly concerning in VANETs, where vehicles communicate with each other and with roadside infrastructure to improve road safety, traffic efficiency, and overall transportation systems.

[1]Department of Computer Science and Engineering, Sarvepalli Radakrishnan University ,Bhopal MIT-Art, Design and Technology University,Pune
mukherjeeshubhra@gmail.com
[2]Department of Computer Engineering Sarvepalli Radakrishnan University ,Bhopal
ravindra_p84@rediffmail.com

Identity Spoofing occurs when malicious entities impersonate legitimate vehicles, leading to unauthorized access and potential disruption of communication. Sybil attacks involve the creation of multiple fake identities by a single malicious node, leading to a compromised network. These attacks can severely impact the reliability and security of VANETs, posing threats to safety-critical applications.

To mitigate the risks associated with Identity Spoofing and Sybil attacks, the Identity Spoofing Sybil Attack Protective Measures using Physical & Logical Address Mapping (ISPLM) approach is proposed. This comprehensive approach combines both physical and logical address mapping techniques to strengthen the security of VANETs.

The ISPLM strategy intends to provide a strong and resilient defense against Identity Spoofing and Sybil attacks by combining Physical and Logical Address Mapping inside the VANET architecture, thereby supporting the secure and efficient functioning of intelligent transportation systems.

The article consist of VII section, in section I describe the introduction about VANET security and sybil attack, section II elaborate about related work of sybil attack detection and prevention, section III describe about proposed ISPLM security technique, in section IV discuss

the proposed ISPLM algorithm, section V describe the simulation parameters, section in the section VI describe the simulation result and in section VII describe about conclusion and future approach on VANET.

2. Related Work

In this section describe about various existing system of attack detection and security system for increasing the reliability and efficient data transmission under vehicular ad hoc network, here those work are briefly elaborated to secure VANET.

Bo Yu, *et al.* [1] has been analyzing the sybil attack behavior using statistical analysis, they undertake many attempts to investigate the possibility of identifying Sybil attack by analyzing signal strength distribution. First, they suggest a collaborative technique for validating the placement of putative Sybil nodes. They deploy a Random Sample Consensus (RANSAC)-based approach to strengthen this cooperative strategy against outlier data generated by Sybil nodes. However, numerous inherent shortcomings of this cooperative strategy motivate us to investigate alternative ways. They devise a statistical approach and a system for determining the origin of a vehicle. The system is known as the Presence Evidence System (PES).

Muhammad Iqbal Younis, *et al.* [2] has been evaluating the detection of sybil attack in VANET. This study first defined the characteristics of the approach utilized in each of the three main categories into which the research on Sybil attacks fell. In order to find and prevent Sybil attack, researchers shed light on the pros and cons of each method. The characteristics of the Sybil attack make the resource testing technique insufficient for securing the vehicle ad-hoc network. It is important to keep in mind that there shouldn't be any additional overheads only for detecting Sybil attacks in VANETs while deciding on the optimal method for doing so. In the said cases, the localization method is suitable for both the verification goals and the position detection.

Based on the type of certificate, the Park, S., *et al.* [3] presented two different methods in their research. They hope that by implementing their plans, the computational certificate management costs and system architectural requirements will be cut in half. They are also working on making their schemes compatible with early-stage VANET deployments. Their plan relies on RSUs and certificate authorities (CAs). The release of public key certificates for RSUs is the responsibility of the RSU.

Salam Hamdan, *et al.* [4] has been detect the sybil attack, in this study proposes a hybrid approach that combines fingerprint and P2DAP (privacy-preserving detection of pseudonym abuses) techniques. Using the ns2 simulator, the hybrid detection system is put into action. Following is the operation of the suggested algorithm. As the number of cars rises, P2DAP outperforms the footprint algorithm. Conversely, when vehicle speeds increase, the footprint algorithm performs better. Security measures, such as encryption and authentication, as well as the vehicle's trajectory, are crucial to the hybrid algorithm.

Pattanayak, Binod, *et al.* [5] has been dealing with sybil attack, they allow vehicles to communicate with one another, Vehicular Ad hoc Networks (VANETs) have the potential to reduce the number of accidents and deaths that occur on their roads. Additionally, VANETs allow traffic controllers to monitor and regulate cars for reckless driving and rapid assistance. Regardless, Design, Routing, Communication, and Security are challenges that these systems encounter. A number of security threats have rendered these systems useless due to the widespread use of remote vehicles for communication. When a malicious vehicle or RSU can take on new personalities, it can unleash a cascade of devastating effects on such systems. on this study, they applied several approaches, such as RTM techniques, PVM, and PKC, to identify Sybil attacks on VANET.

Seyed Salar Sefati, Sara Ghiasi Tabrizi [6] was proposed signal strength index bases sybil attack detection, the detection of attacks on these networks could have a significant impact on VANETs' effectiveness. Preventing road casualties and maintaining traffic control require the timely discovery of assaults. Neighbouring nodes do the first identification. Nodes check their unique identifiers (IDs) against each other's messages whenever they get messages from nearby nodes. When two or more nodes transmit identical messages, the nodes in the immediate vicinity will share some of the data with the RSU. When RSU has reservations about an ID, it creates a table with factors like throughput, packet loss, and latency. All fitness functions added together must equal one. Nodes will keep operating even if the fitness function of these parameters exceeds the specified limit.

Carlos H. O. O. Quevedo, *et al.* [7] was proposed an approach to identify Sybil attacks on VANETs is proposed in this research; it is referred to as SyDVELM. Its foundation is the Extreme Learning Machine method, which improves the reliability, effectiveness, and precision of services pertaining to transportation security, traffic jams, and multimedia entertainment, among other areas. Nodes in metropolitan areas can have their movement patterns detected using the proposed SyDVELM method.

Sofia Azam, *et al.* [8] The researchers offered numerous detection algorithms for distinct types of network threats. However, VANET is still vulnerable to a variety of assaults, most notably the Sybil attack. Sybil Attack is one of the most difficult VANETs attacks, in which fake identities are created in the network to disrupt communication between

network nodes. This attack has a significant impact on transportation safety and may cause traffic congestion. To identify the Sybil attack in the network, a unique collaborative architecture based on majority voting is presented in this respect. Individual classifiers such as K-Nearest Neighbour, Nave Bayes, Decision Tree, SVM, and Logistic Regression are assembled in parallel using the framework. When compared to earlier research that employed a single classifier for attack detection, the suggested ensemble technique seeks to have a more trustworthy prediction.

The privacy-preserving detection of Sybil attacks in vehicular ad hoc networks (P2DAP) was proposed by Zhou. T *et. al.* [9] P2DAP assigns unique identities to the same vehicle based on their hash values. One Sybil node, RSU, got an event from two identities sharing the same hash value. The technique was ineffective for the high-density vehicle network because the nodes were communicating too much. In [10], Reddy proposes an alternative approach that makes use of encrypted digital signals. The basis of this approach is the use of digital signatures as a hash function to establish a level of confidence across cars. The identification process is hindered in situations when there is a lot of movement since this technique doesn't take the nodes' mobility behaviour into consideration. Using Mahalanobis Distance, the Sybil node is detected in [11] by measuring the similarity between the driving patterns of automobiles. Using K-NN algorithms to classify the nodes and differentiate Sybil nodes from other nodes, a mechanism is devised later that year to identify Sybil assaults [12].

Helmi. Z, *et al.* discovered a way to use deep learning to identify Sybil attacks [13]. This study isolated patterns of Sybil attacks in a single VANET region by integrating relevant data. With the use of three layers of protection, the research was able to achieve a prediction accuracy of 94%. On the VeReMi dataset, ML classifiers—specifically, AdaBoost, Decision tree, and XG Boost—trained with Eigen values were used for behavioral-based classification [14]. For the classifier to work better, a plausibility factor was included. When it comes to calculating Eigen values, nevertheless, this work falls short. Multiple classification techniques, including SVM, logistic regression, and Random Forest, are used to identify Sybil attacks in [15]. Preparing the simulated VANET data for machine learning algorithms involves employing SMOTE to ensure data balance. There are fewer vehicles in this trial compared to the others, but the accuracy performance is still impressive. The Sybil attack on VANET may be detected using an intrusion detection system (IDS) based on deep learning and CMEHA-DNN-CMEHA-DNN, as suggested in reference [16]. The outcomes were superior than all other procedures that were previously used.

Nirbhay Kumar Chaubey & Dhananjay Yadav [17] He presented a novel method in this research for detecting Sybil attacks that does not involve certifications of vehicles or constant monitoring of those vehicles. Additionally, vehicles are not obligated to provide their location or identity, so protecting their privacy. In the event of a harm, their simulation results reveal that the packet delivery ratio (PDR) drops for the same quantity of vehicles. As a result of increased packet loss caused by nonexistent vehicles, the PDR drops since no one false ID can receive the confirmation message simultaneously. Furthermore, their method entails executing the attack detection algorithm just when necessary, i.e., when traffic exceeds the assigned threshold. However, their previous work necessitates the method they developed to store and retrieve vehicle data (such as id, location, and neighbour information) in a continual fashion, keeping the network always active with computation.

G. Soni, *at. el.* [18] offers a unique secure IPS method that can identify and stop malevolent (blackhole) and wormhole vehicles from communicating further over the network by using a novel PSO. The proposed RSU-based IPS in this article has successfully stopped the attacker's harmful activities in addition to generating a warning. By implementing IPS protection in RSUs, the primary benefit is the ability to simply share particular information about identified attackers with all RSUs, allowing for future alerts regarding network-wide harmful behaviors. Finally, the purpose of transmitting this data is to prevent dangerous vehicles from passing through. It is possible to identify intruder infections and reduce the loss of valuable traffic packets with the proposed IPS protection with PSO.

G. Soni & K. Chandravanshi [19] Presented a new approach to routing 6G-VANET data that protects it against harmful black hole assaults in VANET. When leading vehicles provide traffic status packets to subsequent vehicles, black hole vehicles ignore all of the crucial information in those packets. Node packet dropouts can be detected and prevented by a security system. Here they compare the current SAODV security system's performance to that of the advanced PPDM. The PPDM protects the VANET and increases performance after prohibiting rogue cars from functioning in the network. We evaluate a proposed PPDM scheme's efficiency in comparison to the current SAODV. When compared to SAODV, PPDM improves performance and decreases data dropping.

G. Soni, *et al.* [20] Develop a new technique for improving bandwidth utilization for VANET on 6G networks: the TCCQ technique. When it comes to traffic status packet flooding, the TCCQ approach has you covered. It works by looking at the number of nearby cars and 6G data rate, which helps with quickly transmitting information about sustained new vehicles. This means that the transmission of the car's traffic status is limited to the vehicle that follows

it. When one vehicle loses track of its state, the one immediately following it gains that information. There will be less unnecessary traffic overhead and less chance of network congestion using this method.

3. Proposed Research

The Vehicular Ad-Hoc Network is a subset of MANET that facilitates two-way communication between moving vehicles (V2V communication) and fixed infrastructure (V2I communication). When it comes to Intelligent Transportation Systems (ITS), VANETs play an essential role in enhancing road safety, streamlining traffic, and offering a few other services. The vehicular communication is uses dynamic topology which lead to arises security issue because vehicles in the network independently move and able to transmit data from anywhere any time bases. The measure insecurity by unauthorized access such attack is called sybil attack. A Sybil attack involves a single adversary controlling multiple nodes on a network to manipulate or control the network's behavior. The attacker creates a large number of pseudonymous identities to gain a disproportionately large influence. In this proposal use the concept of physical and logical address mapping technique to detect the sybil attacker node in vehicular communication. Sybil attacker has two types, same time more than two or more identity other is different time different identity.

A. Same time multiple Identity

At the same time, the attacker uses the same physical address and maps it to several logical addresses of the receiving node. When multiple source vehicles want to communicate with their respective receivers using their logical addresses and an attacker is present in between the routes, the attacker does not forward the route packet to the intended receiver but instead captures the routing packet and sends acknowledgment to the respective source vehicles. The attacker node uses the same physical address and is mapped with different logical addresses of actual receivers at the same time, acting as the actual receiver for all source cars and capturing data packets sent by source vehicles. This type of Sybil attacker is a simple approach for detecting malicious vehicles.

B. Different Time different Identity

The Sybil attacker is also another nature, which takes the logical identities of receiver nodes at different times and maps them with the same physical address. Due to no changes in physical address, it produces different logical addresses for different receiver nodes at different times. The attacker node takes on the role of the receiving node in order to grab control of the data packets that the source vehicle is transmitting. This kind of attack detection is more critical as compared to the same-time multiple-identity Sybil attacker.

In this proposed approach, Sybil attack detection and protection using physical to logical address mapping is a lightweight security system. Vehicular networks form with the help of roadside units (RSU's), which are responsible for monitoring, assisting, and controlling the vehicles in the network. Those RSU's further take on the responsibility of securing the network.

To provide security, RSU's watch the activity of every vehicle during route discovery time, and if they find any vehicle in the network that uses the same physical address and is mapped with multiple logical addresses at the same time, it is treated as an attacker node. Another way to detect the Sybil attack is to map one physical address to one logical address at any instance of time, but after the route establishment process, the node blocks or captures the data packets, which means nodes are attacker vehicles. In the proposed security system Sybil attack detection and prevention in a distributed manner, it means more than one RSU's collaborative way to take decisions about attacker vehicles. After the Sybil attack node detection is the second step to prevent future attacks using the node blocking method. If a vehicle identifies as an attacker, all the RSU's make the decision for the attacker node to block the vehicle from communication and spread the blocking message into the network, so no one can communicate with the attacker node and secure the complete network.

4. Proposed ISPLM Algorithm

Vehicular network are more vulnerable due to the dynamic motion and topology of vehicles. Every vehicle in the network is controlled by a roadside unit that is capable of monitoring, controlling, and giving security instructions to the vehicles. In this section, we describe the formal structure of a security system. The algorithm is subdivided into three sections: input, output, and procedure. In the input section, explain the input variables for algorithm execution, which help configure the vehicles. The output section describes all the relative output variables that were extracted after the algorithm was completely executed. The procedure section describes how the algorithm control structure is executed and how to use the input variable to deploy the ISPLM security system. Their complete structure is described in the below section.

Algorithm: Identity Spoofing Protective Measures using Physical & Logical Address Mapping

Input: V_m: Vehicle in the network

S_v: Source vehicle $\in V_m$

R_v: receiver vehicle $\in I_m$

N_v: vehicle in route $\in I_m$

R_{prt}: routing protocol AODV

Sec_t: security technique ISPLM

a_{ttk}: sybil attacker

l_{addr}: logical address

p_{addr}: physical address

RSU: road side unit

D_{type}: data type tcp/udp

Ψ: Network communication range 550^2m

Output: Throughput, NRL, PDR, true false positive ratio, packet capture identification.

Procedure:

Deploy V_m & RSU_i and form VANET

S_v initiate $R_{prt}(S_v(l_{addr}), R_v(l_{addr}), R_{prt})$

While visited!= V_m || $N_v(l_{addr})$!= $R_v(l_{addr})$

If N_v in Ψ & $N_v(l_{addr})$!= $R_v(l_{addr})$ **then**

N_v← store temp(N_v)

N_v forward R_{prt} to next N_{v+1}

Else if N_v in Ψ & $N_v(l_{addr})$ == $R_v(l_{addr})$ **then**

RSU_i node active & use Sec_t

If $N_v(p_{addr})$ = 1 & $N_v(l_{addr})$ > 1 **then**

N_v ← as a_{ttk}

RSU_i block N_v

RSU_i broadcast blocking message ∀V_m

V_m stop communication with N_v

Else if $N_v(p_{addr})$ = 1 & $N_v(l_{addr})$ == 1 **then**

R_v ← N_v

R_v found & create routing table($S_v(l_{addr})$, $N_v(l_{addr})$)

R_v send acknowledgment to S_v

Call $D_{packet}(S_v , R_v, D_{type})$

End if

V_m^{++}

End while

Else

R_v not found || node out of range

End if

$D_{packet}(S_v , R_v, D_{type})$

While existing Route active

RSU_i execute Sec_t

S_v start sending data to R_v

If $N_v(p_{addr})$ = 1 & $N_v(l_{addr})$ > 1 **then**

N_v capture D_{packet}

RSU_i monitor N_v for analyzing behaviour

RSU_i block N_v

RSU_i broadcast blocking message ∀V_m

V_m stop communication with N_v

Else

S_v continue sending data to R_v

R_v send acknowledgment to S_v

End if

5. Simulation Environment

In this section describe about simulation parameters which used for vehicular network configuration, these parameter are simulation area, number of vehicles, routing protocol, attack type, security technique etc. This parameter helps to design the vehicular ad hoc network structure under network simulator -2.

Table 1: Simulation Parameter for Deployment of MANET

Parameters	**Configuration Value**
Simulation Tool	NS-2.31
Simulation Area	1800m*1800m
Routing Protocol	AODV
Network Type	VANET
Attack Type	Sybil
Security Technique	ISPLM
Number of Vehicles	50
Number of RSU	9
Physical Medium	Wireless
MAC Layer	802.11
Antenna Model	Omni Antenna
Traffic Type	CBR, FTP
Propagation radio model	Two ray ground
Packet Size	512 Byte
Simulation Time (Sec)	300 Sec

6. Simulation Result

A. Result Analysis

Compare the simulation results of attack, AODV-WA, AODV Sybil, and ISPLM in this section. When compared to the previous approach to VANET, the new security scheme produces better outcomes.

B. Network Animation Scenario

The number of vehicles on the road is always increasing, and proper vehicle management is only feasible by controlling traffic on the road and being vigilant to the activities of malevolent vehicles in the network. In the road map scenario, vehicles are constantly moving on roadways at varying speeds. There are many terminals here, and many vehicles change directions from the terminal in the network. Here, preventer vehicles provide network protection against Sybil attackers.

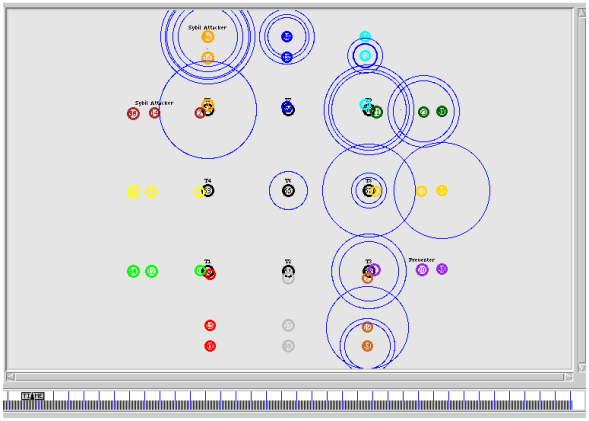

Fig 1: Network Visualization

C. Throughput Performance Analysis

The quantity of packets or bits received at the destination is measured by throughput performance of a network. The throughput performance is measured in presence of AODV-WA, AODV Sybil and proposed ISPLM in VANET. The proposed ISPLM detection and prevention strategy performs better in the presence of an attacker in network. The throughput is essentially minimal in the presence of an attacker, but in the case of the suggested ISPLM scheme, the throughput performance is maximal, providing higher routing performance in a dynamic network.

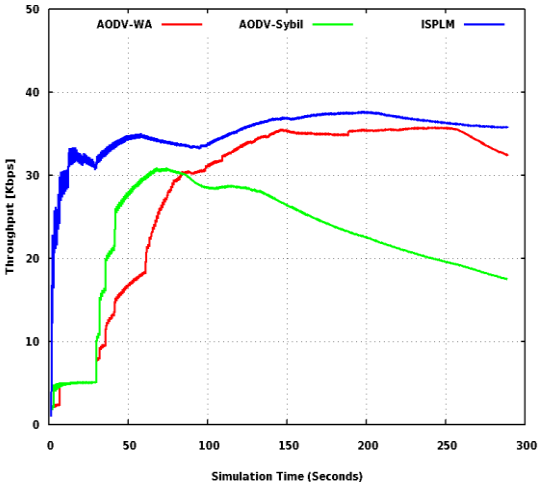

Fig 2: Throughput Performance Analysis

D. Overhead Analysis

The sender is flooding the network with packets in order to find the destination. Every node in the network forwards routing packets until the destination is not located. In this graph, measure the routing overhead in terms of normal time, attacker, and security scheme, but in the absence of an attacker overhead is maximum and the overhead of proposed ISLM is less. If the sender searches for the actual receiver while any nearby Sybil attacker is present, that certainly gives the misidentification number of the receiver and routes reply message sent to the sender by the receiver. In such an instance, the true sender is unable to search any of the route and all data packets are dropped by the attacker. The routing of packets is high in both the standard and proposed security schemes, while data receiving is likewise high with minimal overhead.

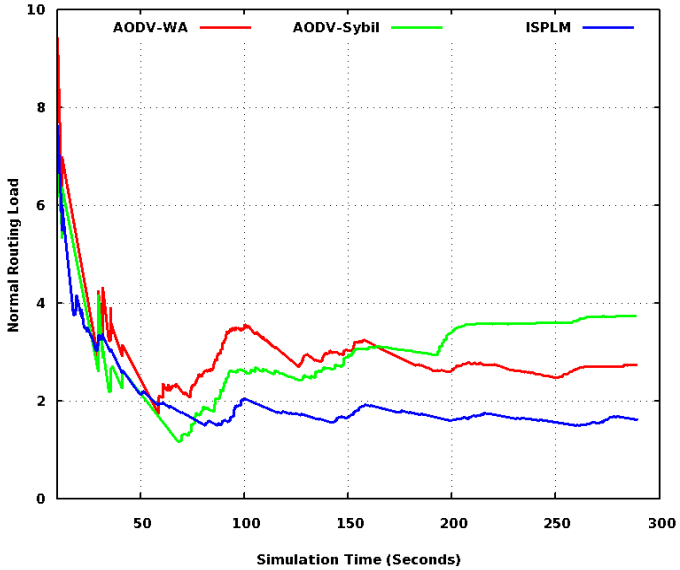

Fig 3: Overhead Analysis

E. Packets Receiving Percentage Analysis

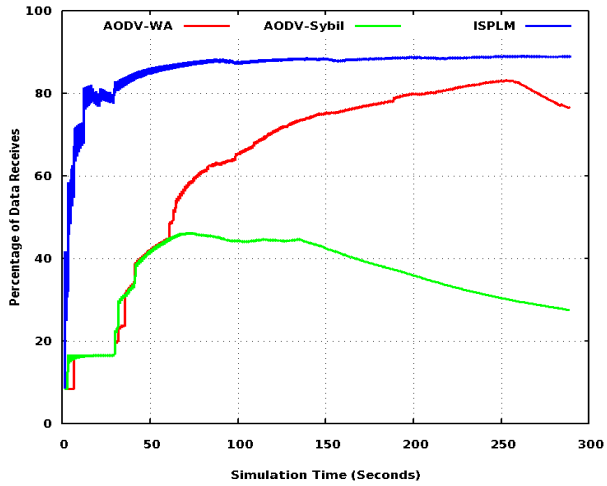

Fig 4: Percentage of Data Receiving

The packet percentage indicates how well data is received in comparison to how well it is sent in the network. Data loss in the network limits packet receipt, and, as a result, PDR performance suffers. In this graph, the PDR performance of normal AODV-WA routing, the presence of Sybil attackers, and the presence of the proposed ISPLM security scheme are all examined, with the overall result favoring the proposed security strategy in VANET against Sybil attacks. In this graph, PDR performance is approximately 90% in the presence of normal and prevention, but only 27% in the presence of Sybil attacker.

F. False and True Positive Analysis

In VANET, attacker detection is achievable by detecting false detection ratios and true detection ratios. In true detection analysis, the presence of an attacker in the network is negligible or non-existent, indicating that the network is performing well, and the drop percentage is likewise low. In this graph, attacker is positively detected, and the true positive ratio is greater than 99%, indicating the attacker's existence in the network. False detection indicates that the network performance is the same as regular network behaviour. It means that a higher percentage ratio for false detection is always desirable. It recognizes Sybil identities in the network.

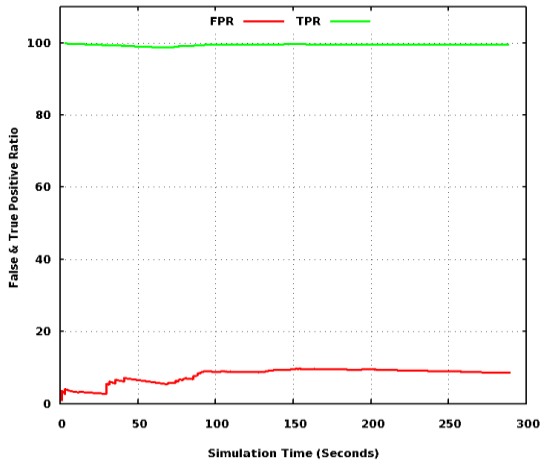

Fig 5: True & False Positive Analysis

G. Sybil Infection Analysis

In this graph, two modules with various Sybil identities represent the Sybil attacker. The infection percentage ratio is used to calculate the percentage decline in the presence of an attacker in a network. The drop percentage of the Sybil scenario is at least 40%, up to a simulation time of 300 seconds; however, after implementing the security scheme, the infection count in the network is nearly nil. The proposed ISPLM security method improves network performance by preventing malicious attack activity.

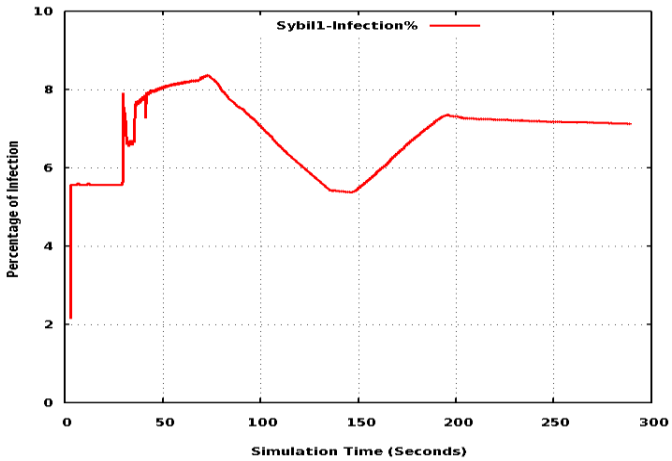

Fig 6: Sybil Attacker Infection Analysis

H. Packet Capture Analysis

Sybil attack detection is a challenging task due to the change in the internal routing architecture under route packets; other parts remain the same. In this article, we use the concept of physical-to-logical address mapping, which monitors every node by the RSU and detects the attack behaviors of the network. The figure shows that attacker vehicles capture the data from the network. In the simulation, we take fifty vehicular nodes out of which two (14 & 52) are detected as Sybil attacker nodes, that capture the packets of twelve receiver nodes, which further blocks communication and secure data transmission. In the figure, the total number of packets captured during the Sybil attack is nearly 1000.

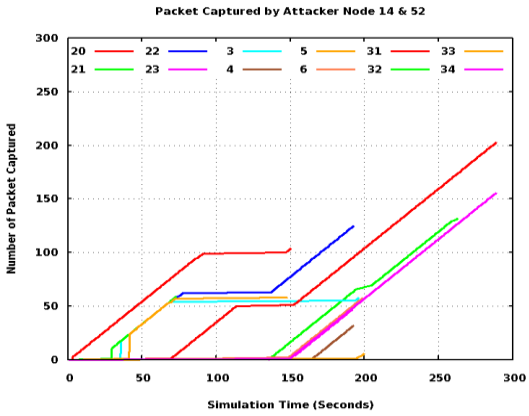

Fig 7: Analysis of Packet Capture by Attacker node

I. Overall Performance Analysis

Overall network performance refers to how well a network performs in AODV-WA, in presence of Sybil attacker and ISPLM. Table 2 clearly shows that the proposed security ISPLM technique gives better outcomes after blocking the attacker node in the network. In this case, PDR, packet loss, and other metrics provide better network outcomes.

Table 2: Network Overall Analysis

Parameters	AODV-WA	AODV-Sybil	ISPLM
Packet Sends	3852	3852	3852
Packet Receives	2944	1059	3431
Packet Drop	908	2793	421
NRL	2.73	3.73	1.63
PDR	76.43	27.49	89.07

7. Conclusion and Future Work

The implementation of protective measures against identity spoofing and Sybil attacks in Vehicular Ad Hoc Networks (VANETs) is crucial for ensuring the integrity and security of communication among vehicles. The combination of physical and logical address mapping represents a comprehensive approach to mitigate these threats. In this article, we propose an ISPLM detection and security system inbuilt into the RSU's that is capable of detecting and protecting from Sybil attacks. The system monitors and controls all vehicles that are in the radio range of roadside units (RSU's); it traces incoming and outgoing packets into every vehicle and identifies the activity of vehicles; it gets vehicle maps from one physical address to multiple logical addresses, blocks them, and protects the network system from attack. The article shows the comparative outcomes between AODV-WA, AODV-Sybil, and proposed ISPLM routing in terms of throughput, percentage of data received, normal routing load, true and false positive ratio, and percentage of infection. The results conclude that the ISPLM system provides secure communication and provides better results in terms of throughput, percentage of data received, and accurate detection of infection. In the future, we will try to adopt the ISPLM proposed system in different network environments, such as the number of vehicles, their speed variation, and the number of RSU, which will further assure the feasibility of the proposed system.

Reference

[1] Bo Yu, Cheng-Zhong Xu, Bin Xiao "Detecting Sybil attacks in VANETs", Elsevier Inc, J. Parallel Distrib. Comput. 73 (2013) 746–756.

[2] Muhammad Iqbal Younis, Rana M. Amir Latif, Izharul Haq, NZ Jhanjhi, Abdul Karim, "An Evaluation of Sybil Attack's Detection Approaches in Vehicular Ad-Hoc Networks (VANETs)", International Journal of Intelligent Systems and Applications in Engineering IJISAE, 2022, 10(2s), 124–133

[3] Park, S., et al., Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support. Security and Communication Networks, 2013. 6(4): p. 523- 538.

[4] Salam Hamdan, Amjad Hudaib, Arafat Awajan [4] Detecting Sybil attacks in vehicular ad hoc networks", Networking and Internet Architecture, arXiv:1905.03507, Year-2019.

[5] Pattanayak, Binod & Pattnaik, Omkar & Pani, Sasmita. (2021). Dealing with Sybil Attack in VANET. 10.1007/978-981-15-5971-6_51, In book: Intelligent and Cloud Computing (pp.471-480).

[6] Sefati, Seyed Salar & Ghiasi, Sara, "Detecting Sybil Attack in Vehicular Ad-hoc Networks (Vanets) by Using Fitness Function, Signal Strength Index and Throughput". Wireless Personal Communications. 123. 10.1007/s11277-021-09261-x, Year-2022.

[7] Quevedo, Carlos H. O. O. et al. "An Intelligent Mechanism for Sybil Attacks Detection in VANETs." ICC 2020 - 2020 IEEE International Conference on Communications (ICC) (2020): 1-6.

[8] Azam, S.; Bibi, M.; Riaz, R.; Rizvi, S.S.; Kwon, S.J. Collaborative Learning Based Sybil Attack Detection in Vehicular AD-HOC Networks (VANETS). Sensors 2022, 22, 6934. https://doi.org/10.3390/s22186934

[9] Zhou, T.; Choudhury, R.R.; Ning, P.; Chakrabarty, K. P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks. IEEE J. Sel. Areas Commun. 2011, 29, 582–594.

[10] Reddy, D.S.; Bapuji, V.; Govardhan, A.; Sarma, S.S.V.N. Sybil attack detection technique using session key certificate in vehicular ad hoc networks. In Proceedings of the 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), Chennai, India, 16–18 February 2017; pp. 1–5.

[11] Gu, P.; Khatoun, R.; Begriche, Y.; Serhrouchni, A. Support Vector Machine (SVM) Based Sybil Attack Detection in Vehicular Networks. In Proceedings of the 2017 IEEE Wireless Communications and Networking Conference (WCNC), San Francisco, CA, USA, 19–22 March 2017; pp. 1–6.

[12] Gu, P.; Khatoun, R.; Begriche, Y.; Serhrouchni, A. k-Nearest Neighbours classification based Sybil attack detection in Vehicular networks. In Proceedings of the 2017 Third International Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 11–12 February 2017.

[13] Helmi, Z.; Adriman, R.; TYArif Walidany, H.; Fatria, M. Sybil Attack Prediction on Vehicle Network Using Deep Learning|Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi). August 202).

[14] Laouiti, D.E.; Ayaida, M.; Messai, N.; Najeh, S.; Najjar, L.; Chaabane, F. Sybil Attack Detection in VANETs using an AdaBoost Classifier. In Proceedings of the 2022 International Wireless Communications and Mobile Computing (IWCMC), Dubrovnik, Croatia, 30 May–3 June 2022; pp. 217–222.

[15] Akshaya, K.; Sarath, T.V. Detecting Sybil Node in Intelligent Transport System. In Innovative Data Communication Technologies and Application; Springer: Singapore, 2022; pp. 595–607.

[16] Velayudhan, N.C.; Anitha, A.; Madanan, M. Sybil attack detection and secure data transmission in VANET using CMEHA-DNN and MD5-ECC. J. Ambient Intell. Humaniz. Comput. 2021.

[17] Nirbhay Kumar Chaubey & Dhananjay Yadav, "Detection of Sybil attack in vehicular ad hoc networks by analyzing network performance", International Journal of Electrical and Computer Engineering (IJECE)Vol. 12, No. 2, April2022, pp. 1703~1710[1] Bo Yu, Cheng-Zhong Xu, Bin Xiao "Detecting Sybil attacks in VANETs", Elsevier Inc, J. Parallel Distrib. Comput. 73 (2013) 746–756.

[18] Soni, G., Chandravanshi, K., Jhariya, M.K., Rajput, A. (2022). An IPS Approach to Secure V-RSU Communication from Blackhole and Wormhole Attacks in VANET. In: Sarma, H.K.D., Balas, V.E., Bhuyan, B., Dutta, N. (eds) Contemporary Issues in Communication, Cloud and Big Data Analytics. Lecture Notes in Networks and Systems, vol 281. Springer, Singapore. https://doi.org/10.1007/978-981-16-4244-9_5

[19] Soni, G., Chandravanshi, K. (2022). A Novel Privacy-Preserving and Denser Traffic Management System in 6G-VANET Routing Against Black Hole Attack. In: Karrupusamy, P., Balas, V.E., Shi, Y. (eds) Sustainable Communication Networks and Application. Lecture Notes on Data Engineering and Communications Technologies, vol 93. Springer, Singapore. https://doi.org/10.1007/978-981-16-6605-6_49

[20] Soni, G., Chandravanshi, K., Kaurav, A.S., Dutta, S.R. (2022). A Bandwidth-Efficient and Quick Response Traffic Congestion Control QoS Approach for VANET in 6G. In: Saini, H.S., Sayal, R., Govardhan, A., Buyya, R. (eds) Innovations in Computer Science and Engineering. Lecture Notes in Networks and Systems, vol 385. Springer, Singapore. https://doi.org/10.1007/978-981-16-8987-1_1