International Journal of Current Trendsin Engineering & Technology
ISSN: 2395-3152
Volume:8, Issue: 4, July-August 2022

Preventing Vehicular Ad-hoc Networks (VANET) from multiple attacks using Neighboring Information

Chinmayi Panicker, Pankaj Richhariya
Research Scholar, Deptt. of Computer Science,
Bhopal Institute of Technology & Science, Bhopal (MP), INDIA

Abstract—The advancement of wireless communication leads researchers to conceive and develop the idea of vehicular networks, also known as vehicular ad hoc networks (VANETs). In a Sybil attack, the WSN is destabilised by a malicious node which creates innumerable fraudulent identities in favour of disrupting network protocols. In this paper, a novel technique has been proposed to detect and isolate Sybil's attack on vehicles resulting in proficiency of the network. It will work in two phases. In the first phase, RSU registers the nodes by identifying their credentials. If they are successfully verified, the second phase starts and allows vehicle identification. Thus RSU gathers information from neighbouring nodes & define threshold speed limit to them & verifies that the threshold value exceeds the defined limit of speed. Multiple identities generated by Sybil's attack are very harmful to the network & can be misused to flood the wrong information over the network. Simulation results show that the proposed detection technique increases detection possibilities and reduces the percentage of Sybil attacks.

Keywords–MANET, VANET, Malicious node, Sybil Attack. Collision, V2V communication

I. INTRODUCTION

Mobile Ad hoc Network (MANET) is the formation of a network that connects mobile nodes wirelessly. It can be fabricated by mobile or fixed mobile nodes. Security described above attacks on VANETs is elevated to catastrophic results such as the fatality of lives or revenue for those value-added services. Therefore making VANETs secure has become a key objective for VANET designers. However, dealing with these nodes in VANET is more challenging due to the increased ambiguity in the detection caused by the high mobility of vehicles [1].

The level of security is defined in terms of requirements, such as confidentiality (preservation of private information), integrity (assertion of information is ethical and rigorous), availability (it is conscientious access to the information by authorised people), authenticity (confirming the identity of a person), freshness (message is new, not a replay message) and non-repudiation (used to settle disputes about the occurrence or non-occurrence of an event). Subsequently, a Sybil attacks from some threats, in which a malicious vehicle creates an illusion of traffic bottleneck by creating numerous identities. Therefore, Sybil attacks are a premeditated, deliberate security threat to Ad hoc Networks and Sensor Networks. Traditionally in ad hoc networks and sensor networks, there are three types of defences against Sybil attacks: radio resource testing, registration and position verification.

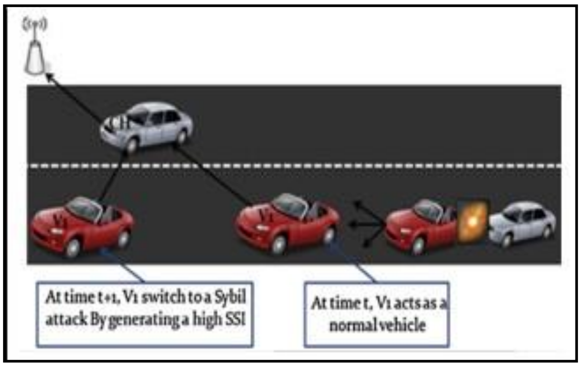
At time t+1, V1 switch to a Sybil attack By generating a high SSI
At time t, V1 acts as a normal vehicle

Figure 1. Attack's Scenario: Sybil Attacks [2].

Sybil's attacks might be ruinous to a variation of VANET applications. For example, a greedy driver can formulate that a number of vehicles are travelling nearby, which creates an illusion of traffic congestion. Then, other vehicles will choose an alternate route and evacuate the road for the greedy driver. Sybil's attacks may even cause serious safety threats. For example, in the application of deceleration warning systems [3], if a vehicle reduces its speed, it will broadcast a warning to the following vehicles.

The remainder of the paper is organised as follows. In Section 2, we define the Major Attacks in VANET. Section 3 presents the reviews of Sybil's attack-related work. Section 4 explains the proposed work. Section 5 approaches details of detecting potential Sybil nodes. Section 6 explains the method used for the simulation model & presents factual results. At last, Section 7 concludes the paper.

II. ATTACKS IN VANET

VANET has some issues with High Mobility, Real-time Guarantee, Privacy and Authentication, Location Awareness, and Delay in VANET [10]. VANET is facing many attacks. Some of them are described as follows.

Denial of Service Attacks: DOS attacks are a type of attack caused by network insiders and outsiders and provide a network that is unavailable to real users. It is done by flooding the control channel with a high amount of naturally generated messages, thus stopping the connection. It results in improper functioning of OBU and RSU [4].

Sybil Attack: Such attacks forge the identity of many vehicles, which are used to cast any type of attack on the system, and it is also used to ruin the connections of network, topologies, and network transmission expenditure.

Message Suppression Attack: In this kind of attack, the attacker discriminative drops the message packets. For the receiver, Critical Information might be held by these packets. So, this attack aims to prevent insurance authorities from learning about vehicular collisions.

Malicious Vehicle: Privacy is vehicular Adhoc networks' most crucial security obligation. To avoid being tracked, the use of randomly changing identities (also called pseudonyms) is suggested. It can lead to a situation where a malicious vehicle (M) can easily change its identity to node N without punishment [5].

Distributed Denial of Service Attack: DDOS is more harmful than DOS attacks because it is distributed. The attacker uses different types of locations to launch the attack. DDOS is possible at V2V and V2 I. Its main objective is to slow down and jam the network [4].

III.RELATED WORK

In VANET, it can be expressed by sending numerous intimation messages from one node with numerous identities. When any node creates multiple copies of itself, it creates confusion in the network. So all the illegal and fake IDs and Authority should be Claimed [6]. It can create a collision in the network. This kind of situation is known as a Sybil attack in the network.

A. Cluster-based approaches

In [7], the author proposed the VANET QoS-OLSR protocol to maintain the stability of VANET and Stable the Clusters of the communication in the network & overhead minimisation. They proposed a new Cluster-based protocol for VANET called VANET QoS-OLSR. To reduce the stability of the cluster, they add the parameters, including velocity & distance, that represent the mobility metrics to the QoS function. Select the optimal path, and select the MPR nodes so that they broadcast the three messages to at maximum 2- hop away nodes (Hello, Ant-Hello, Ack).

In [8], Authors have proposed a two-phase model of incentive and detection. After cluster formation, misbehaviour is detected by aggregating evidence and cooperative decision using the Dempster-Shafer-based cooperative watchdog model. Incentives are in the form of reputation, where network services are provided depending on reputation value. Watchdogs are appointed from the nodes in the network that monitor the behaviour of other nodes to ensure vehicles are cooperating.

B. Privacy Preserved-Based Approaches

In [9], they propose a security protocol to detect Sybil attacks for position-based applications in privacy-preserved vehicular ad hoc networks (VANETs). Vehicles in our protocol identify Sybil attacks locally in a cooperative way by examining the rationality of vehicles' positions to their neighbours.

Authors [10] developed to improve the lightweight Sybil attack detection technique. There is one disadvantage in the lightweight technique: Sybil nodes whose speed is less than 10m/s are also detected as legitimate nodes. To improve this, they enhanced the lightweight Sybil attack detection technique. When a new node enters a network, its RSS value is checked and verified concerning RSS upper bound value. If the received RSS value of the node exceeds the RSS upper bound value, then that node is recognised as a Sybil node; otherwise as a legitimate node.

IV. PROPOSED WORK

Here, an approach is used to localise the fake identities by analysing the consistent similarity in neighbourhood information. This work proposes a new scheme to detect malicious nodes from the network responsible for triggering Sybil's attack.

A. Assumptions

According to our approach, when a vehicle joins a road for travelling, it has to send "Hello Packets" in a network and in return, it gets certain information about its neighbour vehicle nodes. The returned packet contains information like vehicle speed, Last Info Station, Authentication Certificate given by RSU, Actual Position in a network, and Internet Protocol Address. By the use of this information, the vehicle calculates the approximate position of a particular vehicle by using this information.

We use some assumptions for implementing our approach, like Road Side Unit (RSU) providing the authentication certificate to each valid node by checking its electronic number plate. This information is already stored in RSUs from central road authorities. Every vehicle has a GPS by which they can calculate the approximate positions of their neighbour nodes. Detection of Sybil attack and barring communication: When vehicles get information, it calculates each neighbour node's approximate value. After that, it decides from whom it wants to communicate further based on the following cases: If the neighbour node's last info station is not the same and does not have an "Authentication Certificate," the receiving vehicle can refuse to receive its information and mark it as a suspicious attacker. If the last info station of the neighbour node is the same, but its location is not in the range of "last actual position" and "Approximate position", then that vehicle is marked as the suspected attacker. Number of approximate Position Calculator, Speed of Vehicle = S, Internet Protocol Address = IP , Last Info Station= LIS , Authentication Certificate= AC , Actual Position= P, Electronic Number Plate= ENP and Approximate Position= P'. At every 30 seconds, the neighbour table updates itself and deletes previous data in a neighbour table.

```
Step 1.  Send Hello Packets
Step 2.  Receive replies in format (IP, ENP, S, LIS, AC, P)
Step 3.  Calculate P' = (S* 0.0084) + P
Step 4.  Put values in Neighbor Table
Step 5.  End
```

# Road Side Unit Authentication Certificate Issuing:

```
Step 1.  Receive "Hello Packets"
Step 2.  if ENP = Stored ENP data goto Step 4
Step 3.  Else discard the packet. Step 4: if AC = Nil, go to step 6
Step 4.  Else Delete previous data.
Step 5.  Put new authentication certificate.
Step 6.  End
```

V. SYBIL ATTACK DETECTION

Sybil attacks refer to a malicious node illegally taking on numerous identities. So, detect potential Sybil nodes by verifying legitimate nodes. In this technique, a fixed speed is defined to vehicles. The threshold value is set in limits. The threshold value of speed is set to 60m/s. The nodes whose speed value is less than their corresponding threshold values are detected as legitimate nodes. Otherwise, if the speed limit exceeds the threshold set value, it is detected as a Sybil attack. The following detection & isolate algorithm mechanisms are described.

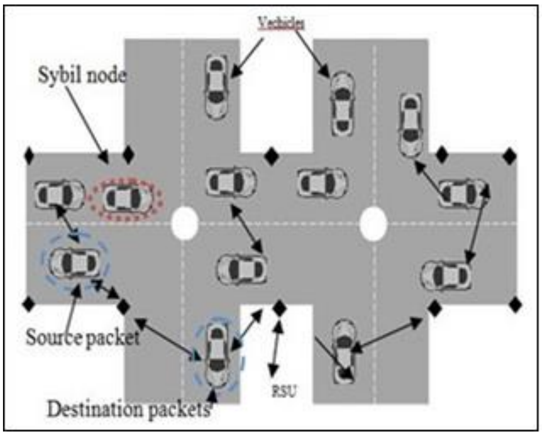

Figure 2. Neighbouring Nodes detect Sybil Node

# Algorithm:

```
Step 1.  Receives IP datagram
Step 2.  If IP= ST [30], go to Step 4 (Check IP with Suspicious Sybil Attacker Table)
Step 3.  Else Discard packet
Step 4.  If IP= NT [30], go to Step 8 (Check IP with Neighbor Table)
Step 5.  Else update the neighbour table
Step 6.  calculate the approximate position
Step 7.  Goto Step 4
Step 8.  If LIS= LIS' goto Step 14(Compare Last info station of incoming IP datagram (LIS)' with itself (LIS))
Step 9.  Else go to Step 10
Step 10. If the Authentication Certificate ≠ nil, go to Step13
Step 11. Else Discard data
Step 12. Put IP in Sybil Attacker Table goto Step18
Step 13. Accept Data goto Step 18
Step 14. If P<=P' go to Step17 (Actual Position should be less or equal to approximate position)
Step 15. Else Discard data
Step 16. Put IP in Sybil Attacker Table goto Step 18
Step 17. Accept Data
Step 18. End
```

VI. EXPERIMENTS

We used NS2 (Network Simulator - 2) for the experiments due to the variety of applicable models for Simulations. The Network Simulator version 2.34 is used, with the configured area of 1000 X 1000 m2.

Some nodes are configured to act as RSU, and others are configured as vehicles. In total, 60 nodes are used for this simulation purpose. RSU nodes are fixed nodes, whereas the other nodes move at a speed of 30m/s. To detect malicious nodes, we configured 2 to act as malicious nodes. AODV protocol is used for communications with 512 kiloBytes packet size and TCP packet Types. The movement type of the nodes is of random waypoint category. This whole configuration is summarised in Table 1.

Simulation Parameters	
Parameters	**Values**
Simulator	NS-2.34
Area	1000x1000
Number of Nodes	60
Vehicle Speed	30m/s
Malicious Node	2
Routing Protocol	AODV

A. Experimental Results

1. Monitoring Process: As shown in the figure 3, the roadside units start flooding the ICMP messages in the networks, which will start monitoring adjacent nodes.

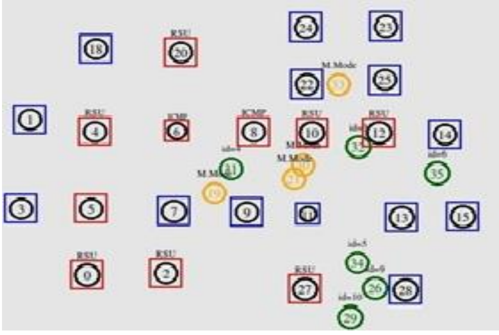

Figure 3 Monitoring Process of Malicious Nodes

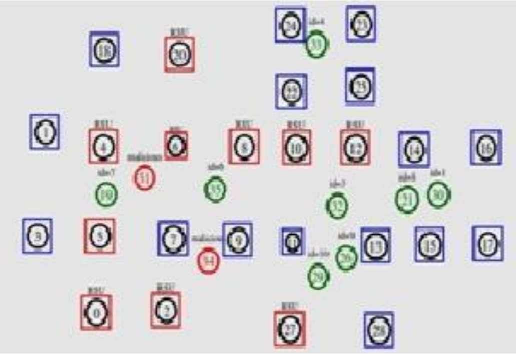

Figure 4 Detection of Malicious Nodes

2. Detection of Malicious Node: As shown in the figure 4, When the roadside units found that some malicious nodes exited the network, the roadside units flood ICMP messages in the network. Its adjacent nodes.

B. X-Graph Results

1. Throughput: Throughput is defined as

Throughput = P/T

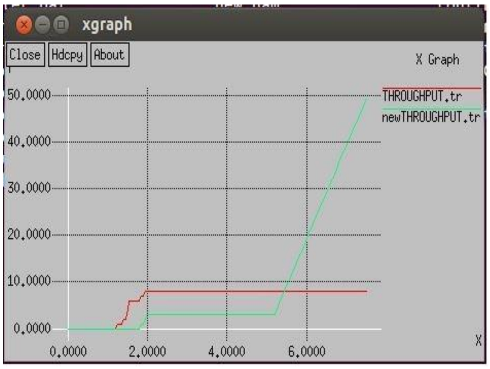

Figure 5. Throughput Comparison between new and old AODV Technique.

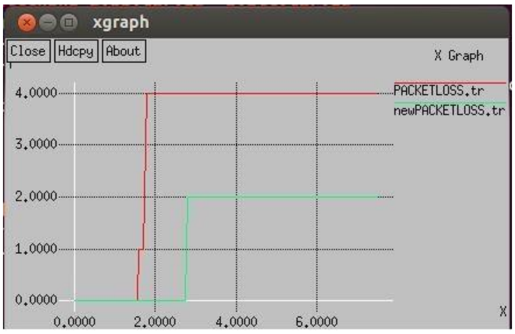

Figure 6. Packet Loss Ratio Comparison between new and old AODV Technique.

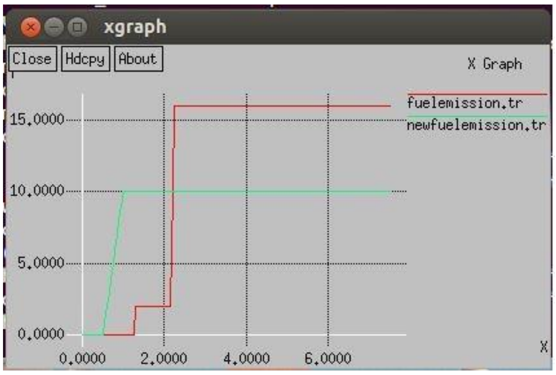

Figure 7. Comparison between old and new AODV Fuel Emission.

2. Packet Loss Ratio: The packet Loss Ratio is the number of packets that originated at the source and were received at the destination.

3. Fuel Emission: In the network Total fuel consumption that a vehicle consumes in an urban journey is fuel consumed while running and at a stop sign.

VII CONCLUSION

In VANET, many attacks are triggered by malicious nodes. Therefore keeping in view the above challenges, there is a need to improve the efficiency of the proposed protocol so that it may be able to control both the factors which make wireless communication unreliable and also support the above application challenges to a large extent. All the problems discussed in this paper can be raised if some of the wrong information can be flooding in the network. The wrong information can be flooding in the network by malicious vehicles that can degrade the network performance by triggering some security attacks will help to improve network performance.

REFERENCES

[1]. J.-A. Jang, K. Choi, and H. Cho, "A fixed sensor-based inter-section collision warning system in vulnerable line-of-sight and traffic-violation-prone environment," Intelligent Transportation Systems, IEEE Transactions on, vol. 13, no. 4, pp. 1880–1890, 2012.

[2]. H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," Computers & Electrical Engineering, vol. 43, pp. 33–47, 2015.

[3]. I. D. Chakeres and E. M. Belding-Royer, "The utility of hello messages for determining link connectivity," in Wireless Personal Multimedia Communications, 2002. The 5th International Symposium on, vol. 2. IEEE, 2002, pp. 504–508.

[4]. A. Rawat, S. Sharma, and R. Sushil, "Vanet: security attacks and its possible solutions," Journal of Information and Operations Management, vol. 3, no. 1, pp. 301–304, 2012.

[5]. B. Liu, Y.-P. Zhong, and S. Zhang, "Probabilistic isolation of malicious vehicles in pseudonym changing Vanets," in Computer and Information Technology, 2007. CIT 2007. 7th IEEE International Conference on. IEEE, 2007, pp. 967–972.

[6]. J. T. Isaac, S. Zeadally, and J. S. Camara, "Security attacks and solutions for vehicular ad hoc networks," Communications, IET, vol. 4, no. 7, pp. 894–903, 2010.

[7]. O. A. Wahab, H. Otrok, and A. Mourad, "A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles," Computer Communications, vol. 41, pp. 43–54, 2014.

[8]. "Vanet Qosolsr: Qos-based clustering protocol for vehicular ad hoc networks," Computer Communications, vol. 36, no. 13, pp. 1422–1435, 2013.

[9]. Y. Hao, J. Tang, and Y. Cheng, "Cooperative Sybil attack detection for position-based applications in privacy preserved Vanets," in Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE. IEEE, 2011, pp. 1–5.

[10]. H. Sharma and R. Garg, "Enhanced lightweight Sybil attack detection technique," in Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference-. IEEE, 2014, pp. 476–481.