International Journal of Current Trends in Engineering & Technology
www.ijctet.org, ISSN: 2395-3152
Volume: 05, Issue: 06 (November- December, 2019)

A Novel Approach to Protect Node in Vehicular Ad-Hoc Network from Sybil Attack

Azimuddin Ahmad
Department of Computer science and engineering
Bhopal Institute of Technology & Science, Bhopal, M.P., India

Dr. Satya Ranjan Patra
Department of Computer science and engineering, Bhopal Institute of Technology & Science
Bhopal, M.P., India

Abstract— *In Vehicular Ad-hoc Networks (VANET), Wireless device sends information to nearby vehicles, and messages can be transmitted from one vehicle to another vehicle. It is an important component of Intelligent Transportation Systems. In today's era of wireless communication, it is important to have a communication between nodes to be safe, secure and timely manner, In this respect, many types of research have been done recently in VANET technology to secure the communication between nodes. But day by day attackers are also being very smart and invented new ways to expose the network. In VANET passenger safety is a prime concern and for achieving this, nodes are exchanging safety messages at regular intervals to increase passenger safety on road. Since the network is open and accessible from everywhere in the radio range of nodes, it is expected to be an easy target for attackers. When any notorious vehicle comes into the network and for its profit, it sends false messages in a network and to protect itself from any type of penalty it uses fake identity, this attack is known as Sybil attack. In the previous approach, the researcher limits the speed of the vehicle and gives all the authority to roadside units to give permission regarding communication or detect Sybil attack. Due to this, places where RSU is not present like highways and rural areas, this approach is not compatible. To overcome this deficiency we are presenting our approach. The proposed detection technique increases the possibilities of detection and reduces the percentage of Sybil attack.*

I INTRODUCTION

Day by day increasing the reliability and dependence on wireless communication techniques, Vehicular Ad hoc Network has become a promising technology. It has the potential to improve the efficiency and safety level of the transportation system. Vehicular Ad hoc Network provides many facilities like traffic congestion control, the safety of passengers and vehicles, location-based services [1], etc. In Vehicular Ad hoc Network, there are two types of communication [2] as shown in figure 1.

- Vehicle to vehicle communication.
- Vehicle to RSU communication.

Being a wireless network, the network is open for all, this leads to the danger of malicious attacker attacks on the network, and thus the security of VANET is a major concern as it inherits all the security threats of the wireless network [3]. A lot of security threats have been discovered and introduced by many researchers in VANET. One of these threats, Sybil attack [4] is a serious threat to VANET security. In the Sybil attack, attacker node forges or creates fake identities. By using these fake identities, the attacker node creates an illusion [5], that there are some additional nodes in VANET. With the help of these fake identities, the attacker node communicates with other nodes [6] and sends false warnings to disturb the traffic on the highway. So, the detection of such nodes is the critical issue of VANET. An attacker node, which creates fake identities or forges the identities of other nodes, is known as Sybil attacker. Nodes, whose identities are forged by Sybil attacker, are known as Sybil nodes. Sybil nodes are used by an attacker to affect the proper functioning of any application in VANET like voting, routing, misbehavior detection, fair resource allocation, data aggregation [7], etc.

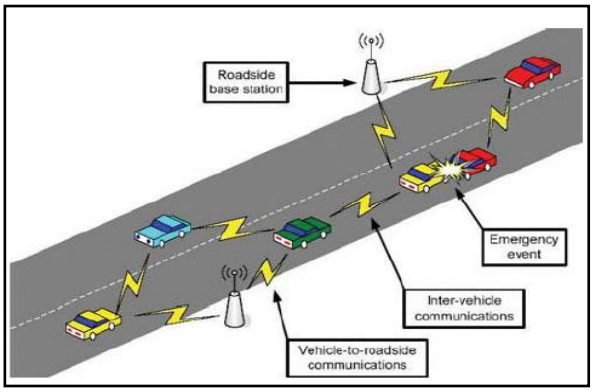

Figure 1 Schematic Representation of a Vehicular Ad-hoc Network

The proposed scheme is a way to detect Sybil attack and Sybil nodes respectively. To reduce the risk of Sybil attack, we used an electronic number plate as identities. To detect Sybil nodes, the neighboring list mechanism was introduced. The rest of the paper is organized as follows. Section II describes the attacks in VANET Section III presents the proposed prevention and detection

scheme. Section IV evaluates the performance and security related issues in the proposed scheme.

II ATTACKS IN VANET

A. Denial of Service Attack: In DOS attack the main objective is to prevent a legitimate user from accessing resources and services. This attack can be trigger by jamming the whole channel and network so that no authorized vehicle can access the network. It is a serious problem in which the user is unable to communicate with the user due to the DOS attack. At the basic level, the attacker forces node and make it busy to do unnecessary tasks by overwhelming it so that it could not do necessary tasks. So it is responsible for packet dropping [8].

B. Distributed Denial of Service Attack: DDOS is more harmful than a DOS attack because it is in a distributed manner. Different types of locations are used by the attacker to launch the attack. It might be possible that they use different time slots for sending messages. The nature of the message and time slot varied from vehicle to vehicle. DDOS is possible at V2V and V2 I. Its main objective is to slow down the network and jam the network [8].

C. GPS Spoofing: The table is maintained in the network to update all the information regarding the identity of the vehicle and the geographic location of the vehicle. The attacker generates GPS satellite signals to fool vehicles which are more effective than the original signals.

D. Timing Attack: There should be accuracy in the time for the best performance of the network so the delay should be less in any application. A timing attack is an issue in ITS safety applications. In this attack, the attacker instead of modifying the data; adds more content in the original data. Due to addition message takes more slot to reach to the destination rather than the required time. So ITS application is a crucial application which is dependent on time and it requires data transmission on time otherwise serious accident may happen [8].

E. Sybil Attack: It consists of sending multiple messages from one node with multiple identities. Sybil attack is always possible except for the extreme conditions and assumptions of the possibility of resource parity and coordination among entities. When any node creates multiple copies of itself then it creates confusion in the network. Claim all the illegal and fake ID and Authority. It can create a collision in the network [9]. This type of situation is known as the Sybil attack in the network. This system can attack both internally and externally in which external attacks can be restricted by authentication but not internal attacks. As there is one to one mapping between identity and entity in the network [10].

III PROPOSED APPROACH

According to our approach when a vehicle joins the road for traveling, it has to send "Hello Packets" in a network and in return of these packets it gets certain information of its neighbor vehicle nodes. Returned packet contains information like the speed of the vehicle, 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 for a particular vehicle.

a) Assumptions: We use some assumptions for implementing our approach like Road Side Unit (RSU) provides 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 approximate positions of their neighbor nodes.
b) Detection of Sybil attack and barring communication: When vehicles get information, then it calculates the approximate value of each neighbor node. After that it decides from whom it wants to communicate further, based on the following cases:

1) If the last info station of the neighbor node is not the same with itself and they did not have an "Authentication Certificate" then the receiving vehicle can refuse to receive its information and mark it as the suspected attacker.

2) If the last info station of the neighbor 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.

 # 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
Approximate Position= P'

At every 30 seconds, neighbor table updates itself and delete previous data in a neighbor table.
Step 1: Send Hello Packets
Step 2: Receive replies in format (IP, ENP, S, LIS, AC, P)
Step 3: Calculate P' = (S (30*(1/3600))) + 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 goto step 6
Step 5: Else Delete previous data.
Step 6: Put the new authentication certificate.
Step 7: End

 # Vehicle receives an IP datagram
Step1: Receives IP datagram
Step 2: If IP= ST [30] goto Step 4
Step 3: Else Discard packet
Step 4: If IP= NT [30] goto Step 8
Step 5: Else update neighbor table
Step 6: calculate the approximate position
Step 7: Go to Step 4
Step8: If LIS= LIS' goto Step 14
Step 9: Else goto Step 10
Step 10: If Authentication Certificate ≠ nil goto Step13
Step 11: Else Discard data
Step12: Put IP in Sybil Attacker Table goto Step18
Step13Accept Data goto Step 18
Step14: If P<=P' goto Step17
Step 15: Else Discard data
Step 16: Put IP in Sybil Attacker Table goto Step 18
Step17: Accept Data
Step 18: End

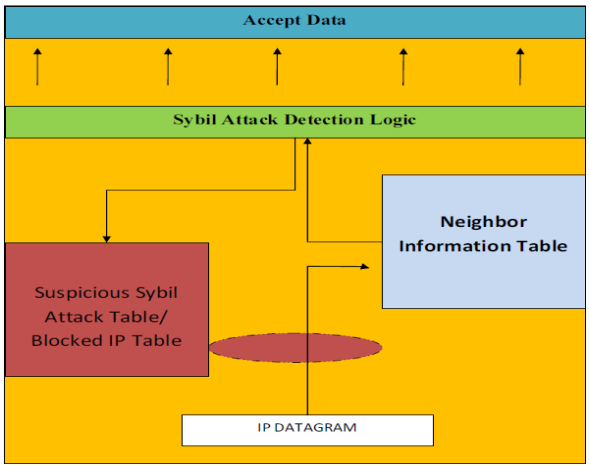

Figure 2 Logic Diagram

IV RESULTS

To validate the proposed approach several simulation experiments have been performed by using network simulator version 2.34. Table 5.1 shows the parameters used in the simulation experiments. The proposed approach is tested in busy traffic conditions using a rectangular scenario of 1000 × 1000 m square area; the network topology consists of the different number of vehicle nodes. There are two types of communication traffic are used in the NS2 (CBR and FTP), CBR (Constant Bit Rate) traffic is used to generate UDP packets for the simulation. In the simulation, start on 0ms and end on the 300ms. The Sybil detection algorithm will start at 0.001ms in the simulation and recheck on 0.5ms. There are different packets sizes are used in the NS-2, for this simulation 1024KB packets are used. There are four-way highways and they have two lines each direction. There are four crossings through which vehicles may cross each other on the highway. To have a fixed number of vehicles in the simulation, assume that the exit vehicles will enter the highway at the nearest highway end and immediately start to send messages. We have selected a single vehicle as to the attacker and remaining are normal vehicle nodes. A simulation has been carried out to evaluate the performance of the proposed method. Each vehicle is first randomly scattered on one intersection along the paths. Each vehicle is driven at a randomly fluctuating speed along different streets. Simulation parameters are listed in Table 1.

Table 1 Simulation Parameters

Parameter	Default Value
Simulation Area	1000m * 1000m
Simulation Time	300 minutes
Number of vehicles	60
Communication range	400m
Node Speed	60km/hr
Visualization Tool	NAM
MAC layer	IEEE 802.11 p

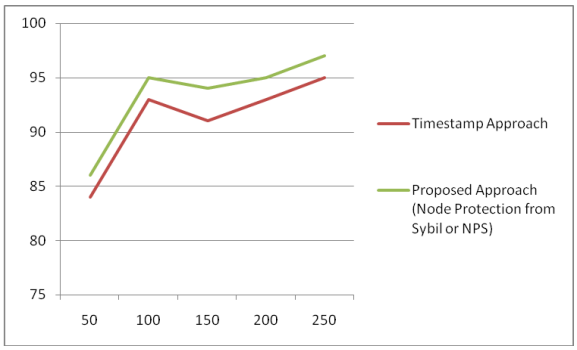

Figure 3 Graph-Packet delivery ratios of "Timestamp Approach" & "Node Protection Scheme"

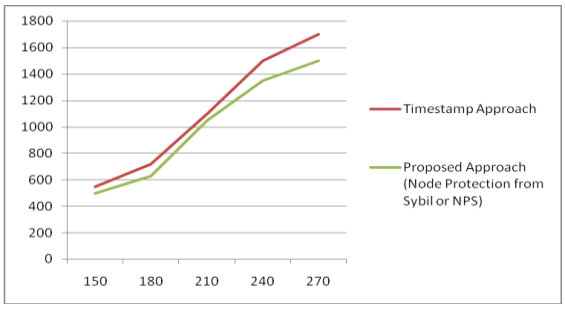

Figure 4 Routing overhead graphs, shows comparability of Timestamp Approach & Node Protection Scheme.

The performance of our approach is measured based on packet delivery ratio, routing overhead. There are two

different approaches for which we measure the packet delivery ratio. Those two approaches are 1) Timestamp Approach, 2) Node Protection Scheme. Simulation graphs are as follows:

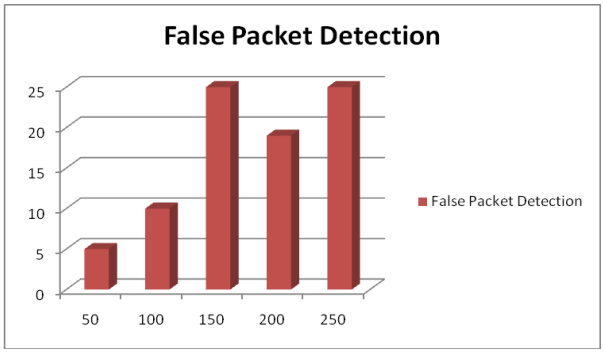

Figure 5 False Packet Detection by "Node Protection Scheme" over time.

V CONCLUSION

We have proposed a simple technique for Sybil attack detection by which any malicious node in a network shall be easily detected and barred from the network. This technique is very light because of this its basic necessary packets that are spread in a network without increasing a routing load in a network will do well without compromises with delay time. This method employs on each vehicle's on-board unit (OBU), in which OBU collects information regarding its neighbor and then only communicate with valid vehicles. The communication paradigm which is used in our approach is relay-based. The technique is localized, requires only a small overhead, and does not have special requirements such as special hardware, etc. The technique was tested through simulations for different distributions of vehicles in dynamic connectivity models. Under all the evaluated scenarios, the technique demonstrates excellent detection of the attacker. The results of the proposed approach are battered than the previous approaches to reduce routing load as well as decreasing a delay time of a packet in a network and detection of Sybil attack as well.

REFERENCE

[1]. Alimohammadi M., Pouyan A. A.; Vehicular Ad Hoc Networks: Introduction and a proposal for vehicle positioning; 13th International Conference on Traffic and Transportation Engineering; 2014.

[2]. Douceur J. The Sybil attack Proc. of International Workshop on Peer-to-Peer Systems 2002; 251–260.

[3]. Isaac, J. T., Zeadally, S., & Camara, J. S. Security attacks and solutions for vehicular ad hoc networks. Communications IET 2010; 4(7): 894

[4]. Alimohammadi M., Pouyan A. A.; Defense Mechanisms against Sybil Attack in Vehicular Ad hoc Network, Security and Communication Networks, John Wiley & Sons, 2014.

[5]. Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. Footprint: Detecting Sybil Attacks in Urban Vehicular Networks. IEEE Transactions on Parallel and Distributed Systems 2012; 23(6): 1103-1114.

[6]. Xiao, B., Yu, B., & Gao, C. Detection and localization of Sybil nodes in VANETs, Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks 2006; 1-8.

[7]. Abbas, S., Merabti, M., Llewellyn-Jones, D., & Kifayat, K. Lightweight Sybil Attack Detection in MANETs. IEEE, Systems Journal 2013; 7(2):36- 248.

[8]. Zhou, T., Choudhury, R. R., Ning, P., & Chakrabarty, K. P2DAP—Sybil Attacks Detection in Vehicular Ad Hoc Networks. Selected Areas in Communications, IEEE Journal 2011; 29(3): 582- 594.

[9]. Jaydeep P. Kateshiya and Anup Prakash Singh," Review To Detect and Isolate Malicious Vehicle in VANET", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 2, February 2015, pp: 127-132.

[10]. Komal Rani and Meenakshi," Prevention of Denial of Service Attack on Dynamic Source Routing vanet Protocol", IJRET: International Journal of Research in Engineering and Technology, Volume: 04 Issue: 09 | September2015, pp: 251-255