Proactive Defence Technique (PDT) For Vehicular Ad Hoc Network To Protect Against Sybil Attack

Poonam Pandey[#1], Ankit Mehto[*2]

[#1]M .Tech Scholar & C.S.E. Department, B.I.T.S., Bhopal

[#2]Assistant Professor & C.S.E. Department, B.I.T.S., Bhopal
Madhya Pradesh, 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). It enables value-added services such as road safety and managing traffic on the road. Security issues are the challenging problems in this network. Sybil attack is one of the serious security threats that attacker tries to forge some identities. One of the main purposes for creating invalid identities is disruption in voting based systems. In that we propose an algorithm for solving two conflicting goals privacy and Sybil attack in vehicle to vehicle (V2V) communications in VANET. Simulation results show that proposed detection technique increases the possibilities of detection and reduces the percentage of Sybil attack. document gives formatting instructions for authors preparing papers for publication in the Proceedings of an IJETT Journal. The authors must follow the instructions given in the document for the papers to be published. You can use this document as both an instruction set and as a template into which you can type your own text.*

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 a potential to improve efficiency and safety level of the transportation system. Vehicular Ad hoc Network provide many facilities like traffic congestion control, 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.

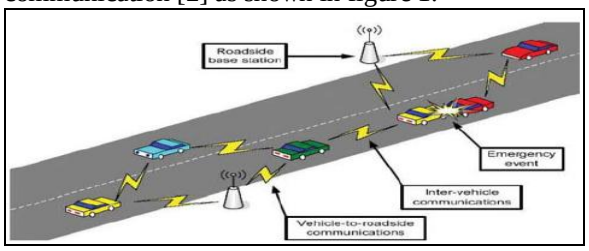

Figure 1 Schematic Representation of a Vehicular Ad-hoc Network

• Vehicle to vehicle communication.
• Vehicle to RSU communication.

Being a wireless network, network is open for all, this leads to danger of malicious attacker attacks on network, and thus security of VANET is a major concern as it inherits all the security threats of 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 for VANET security. In Sybil attack, attacker node forges or creates fake identities. By using these fake identities, attacker node creates an illusion [5], that there are some additional nodes in VANET. With the help of these fake identities, attacker node communicates with other nodes [6] and sends false warning to disturb the traffic on highway. So, detection of such nodes is the critical issues 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.

The proposed scheme is a way to detect Sybil attack and Sybil nodes respectively. To reduce the risk of Sybil attack, we used electronic number plate as identities. In order to detect Sybil nodes, neighboring list mechanism has 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 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 serious problem in which user is unable to communicate with the user due to DOS attack. At

the basic level, 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 DOS attack because it is in 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: Table is maintained in the network to update all the information regarding identify of the vehicle and geographic location of the vehicle. Attacker generate GPS satellite signal to fool vehicle 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 delay should be less in any application. Timing attack is an issue in ITS safety application. In this attack, attacker instead of modify the data; add more content in the original data. Due to addition message takes more slot to reach to the destination rather than required time. So ITS application is 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 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's and Authority. It can create collision in the network [9]. This type of situation is known as 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 vehicle join road for travelling, 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 speed of vehicle, Last Info Station, Authentication Certificate given by RSU, Actual Position in a network, and Internet Protocol Address. By the use of these information vehicle calculates approximate position for 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 GPS system by which they can calculate approximate positions of their neighbor nodes.

B. Detection of Sybil attack and barring communication: When vehicles gets information, then it calculates the approximate value of each neighbor node. After that it decides from whom it wants to communicate further, on the basis of following cases:

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

2) If last info station of neighbor node is same but its location is not in the range of "last actual position" and "Approximate position", then that vehicle is marked as suspicious 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 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 packet.
Step 4: if AC = Nil goto step 6
Step 5: Else Delete previous data.
Step 6: Put 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 approximate position

Step 7: Goto 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

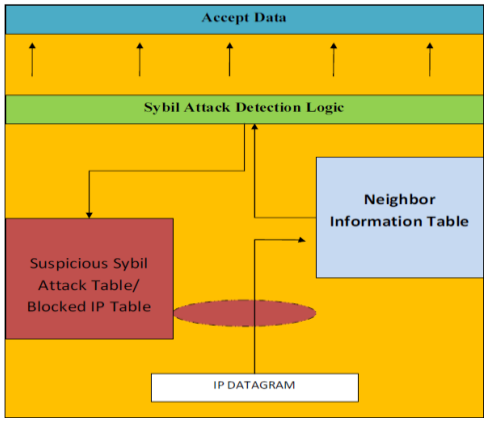

Figure 2 Logic Diagram

IV RESULTS

In order to validate the proposed approach a number of 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 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 on 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 in 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 single vehicle as attacker and remaining are normal vehicle node. 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

Performance of our approach is measured on the basis of packet delivery ratio, routing overhead. There are two different approaches for which we measure packet delivery ratio. Those two approaches are 1) Timestamp Approach, 2) Proactive Defence Technique. Simulation graphs are as follows:

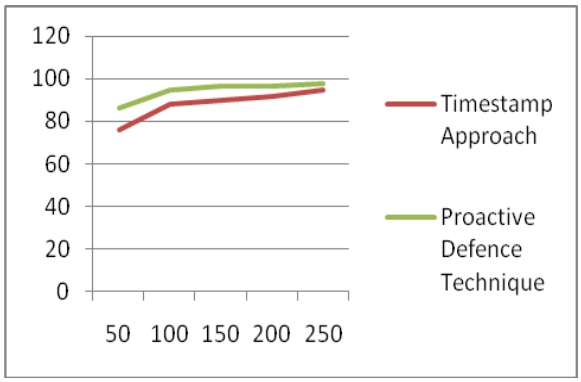

Figure 3 Graph-Packet delivery ratio of "Timestamp Approach" & "Proactive Defence Technique"

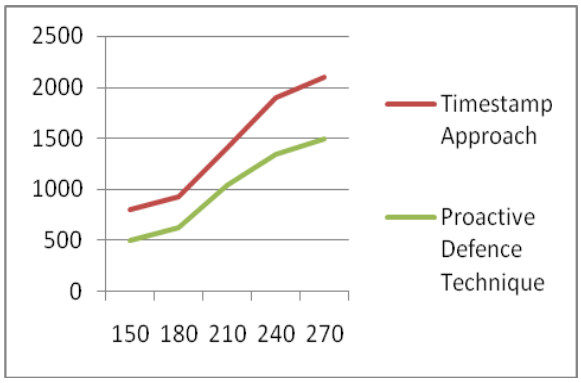

Figure 4 Routing overhead graph, shows comparability of "Timestamp Approach" & "Proactive Defence Technique"

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 which 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. 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 attacker. The results of the proposed approach are batter then the previous approaches in order to reduce routing load as well as decreasing a delay time of a packet in a network and in detection of Sybil attack as well.

REFERENCES

[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 Peerto-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 AnupPrakash 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 Routingvanet Protocol", IJRET: International Journal of Research in Engineering and Technology, Volume: 04 Issue: 09 | September2015,pp: 251-255