Protecting VANET from Sybil Attack & Denial of Service Attack (DoS) by Using ANF Scheme

Gaurav Shrivastava[1], Aditya Sinha[2]

[1]M. Tech. Scholar, [2]Assistant Professor, Department of CSE

Bhopal Institute of Technology & Science, Bhopal, Madhya Pradesh

Abstract— 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 researches has 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 network. In VANET passenger safety is a prime concern and for achieving this, nodes are exchanging safety messages at regular interval to increase the 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. The availability of the network is extremely needed when a vehicle sends any safety information to other one. In this regard, union of Sybil and Dos attack are very dangerous, because it is very difficult to detect it as well as they adversely affect the network availability. In this paper, we propose a Adjacent Node Faith Algorithm (ANF) which is an efficient method to defend against union of sybil and Denial of Service attack (DoS) attack.

Keywords- Adjacent Node Faith Algorithm (ANF), Denial of Service (DoS) Attacks, Sybil Attack.

I INTRODUCTION

Wireless network plays an important role in the field of inter-networking. Through wired media it is very difficult to fulfill the need for mobility, coverage of location and ad-hoc networking, therefore wireless networks relocation, have become and rise as the most important access network technology [1]. VANET (Vehicular Ad-hoc Network) is a subset of MANET (Mobile Ad-hoc Network) which is designed for vehicles. Both VANET and MANET support wireless technology. Nodes in MANET is moving slowly in the network therefore VANET is introduced by ITS in which nodes can move in network at high speed (up to 120 km/hrs) and they can communicate with each other at that is speed also. VANET are very helpful in developing an I T S which enhances the road safety and also add to need of driver and passenger to improve the overall transportation productivity.

In VANET nodes can communicate in two manner first one is vehicle to vehicle (V2V) and other one is vehicle to infrastructure (V2I) communication. DSRC (Dedicated Short Range Communication) is used as communication technology; range of communication between nodes is approx 100 to 300 meters. According to DSRC there are over 100 recommended applications of VANET some of them are Co-operative collision warning, Lane change warning, intersection collision warning, work zone warning, etc.

But as we know that every technology have its advantage and disadvantage, VANET also have some issues which yet has to be resolved some of them are as follows:

a) High mobility: - It is very difficult to have communication between nodes because they are travelling at very high speed and if notes were crossing each other then they have only few seconds to communicate and in those few seconds nodes have to learn about the behavior of other vehicles which decreases the efficiency of the system [2].

b) Guarantee of Real Time Communication: - VANET applications are bound to be having strict deadline for proper message delivery [3] because they deal with hazard warning, collision avoidance, accident avoidance, etc.

c) Proper Authentication: - Vehicles on road want to communicate without disclosing their personal information. Therefore there is a need of system which can authorize vehicle nodes on road without disclosing their personal information [4].

VANET is suffered from some attacks like spoofed id attacks and denial of service attack; framework of VANET permits the attacker to forge source addresses of the incoming IP packet by replacing the packet header with spoofed one as mentioned in 'proper authentication'. Attacker use IP spoofing with DoS attacks because it leads network to its worst place. Today in VANET environments, a Denial of Service attack is a serious problem and it may causes severe damages on the targeted node [12, 4]. By the study of related work, it was found that various approaches and applications are used for the prevention of DoS attacks.

This paper is organized as follows: Section 2 Describes about types of attacks in VANET, Section 3 Reviews a related work on DoS and Sybil attack, Section 4 Describes our proposed approach Section5 shows the results of proposed approach and finally, the paper concludes in Section 6.

II ATTACKS IN VANET

VANET is a technology which brings dynamic change in communications. It is very reliable with respect to save time as well as life of passengers on road. Dark side of VANET is, it is also suffering from different attacks, and some of them are discussed in the following subsections.

A. False massage Broadcasting

Attacker sends false massage to its adjacent vehicles; massages may contain false information regarding the blockage of roads, etc. Attacker can alter a safety massage to make diver life at risk. Due to this attack vehicle may crash on road; motive behind this attack is to manipulate the flow of traffic around a chosen route for attacker's interest [9].

B. Sybil attack

Sybil attack consists of sending multiple messages from a malicious node with multiple forge identities. Attacker makes fool of other available vehicle in the network, forge identities may be used by attacker to cast any type of attack in the VANET environment. The messages communicated in this type of attack include sending of false position as well as wrong direction information.

C. Suppresed massage attack

Attacker drops packets selectively in the network; those dropped packets may contain vital information for the receiver, attacker suppressed these packets for its personal use [10]. Generally aim of such attacks may be to prevent any specific node from insurance and registration authorities to knowing about accidents involving vehicle or to avoid sending collision reports to authorities.

D. Timing Attack

Attacker adds extra content in original data, instead of modify it. Because of adding extra data massage needs more slots then original one to send from one node to another; thus time of communication is increases or delay may increase. So ITS application is crucial application which is dependent on time and it requires data transmission on time otherwise serious accident may happen [9].

E. Denial of Service attack

Motive of this attack is to prevent network resources from legitimate users; this attack is really disastrous in VANET environment. In this attack flooding of packet in network is done by attacker due this large amount of messages so that either system may crash or it may be unable to operate accurately, which effectively denies the service to the valid users from its proper functioning [2]. The target resources which are affected in these attacks include CPU memory, and bandwidth.

III RELATED WORK

In this paper [1] authors suggested a new Job-Scheduling based online algorithm for VANET environment. In this scheme they shows that how proposed scheme reduces the delays experienced by the vehicles as they passed through the intersection under light and medium vehicular traffic loads.

In paper [15] author suggests a massage authentication scheme in VANET. For authentication non repudiation is used in system which allows to access personal information of the vehicle, by this reorganization of the vehicle can be done in case of any claims. Packets contain identity information of a vehicle, so it can be tracked whenever desired and non-repudiation can be done in the network.

In paper [7] authors suggested an approach to reduce the effect of denial of service attack. This approach wants to maintain a database by onboard unit. If OBU detects attack then database suggests node to use channels switching. Detailed approach is, according to paper switching technology has four options which are available to detect the received messages after making decision, and the appropriate decision will be sent to the next OBU in the network [7].

In paper [13] authors propose a method in which they use a special packet called Decision Packet. This packet is generated after the route has been established between source and destination. By using RREP packet, path former obtains required detailed information of all the intermediate nodes in the path. This information contains identity of all nodes which are forming route from source to destination node in recent identified path. Intermediate nodes has to computes the hash value of the decision packet at every node which is verified at the adjacent next Intermediate node, by this chances of alteration of vehicle secrets information shall be reduced.

In paper [8] authors try to solve the security issues of the Sybil attack detection methods, proposed scheme is hybrid, it consist of two techniques. The first one is a location identification technique; this technique is based on the strength of received signals from Adjacent Node nodes. In which node sends beacon packets to its Adjacent Node nodes on the basis of distance, speed, and direction, other node can determine and compare their geographical position in the network and verify the authenticity of sender node. Second technique is Sybil attack detection, in which nodes uses distinguishing ability degree metric by which they can identify origin of data. Every node can launch it in the network.

In paper [1] authors proposes a model based on reference broadcast synchronization by which they prevent VANET from DoS attacks and they named this approach as RBS protocol. This model is based on the master chock filter concept for filtration of packets during busy traffic. The protocol was also evaluated by the other two methods, which are blocking the source IP originator by the DoS attacks and checking the prevention of TCP/UDP flooding and IP sniffing attacks. This model can protect network from DoS attack as well as Sybil attack.

IV PROPOSED APPROACH

In a network a malicious node starts sending huge amount of massages to its adjacent nodes and for securing its original identity it uses multiple fake identities for this work, massages send through DSRC channels. In DSRC scheme safety massages has highest priority over other massages so when malicious node sends huge amount of safety massages they use all the bandwidth of the sufferer node along with this messages come from different IP address so it is very difficult to detect attack, as the result sufferer is not able to communicate with other vehicles nodes. Our Adjacent node faith scheme works on that, as per this scheme each vehicle keeps its Adjacent Node's IP address in a table and update it at regular interval and after that it checks all incoming traffic, if incoming packet is matched from "IP" present in a table than data will go through DoS detection module and then en-queue in a processing queue, else new queue will be created with a receiving limitation of massages and number of new queue shall be equal to the count of entries in Adjacent Node Table. Limitation of massage receiving from unknown IP will lead to protect network from union of Sybil and Denial of Service attack. When DoS attack starts all the internal queues of On Board Unit are filled with messages and all the resources of On Board Unit are busy in processing of these messages so communication with other vehicle is not possible. But if only limited numbers of safety message from valid user are received, On Board Unit will perform its task quite easily. Working of our scheme is described as follows:-

INPUT MODULE:

In input module checks the incoming packets at entry level with blocked IP table if entry is matched with it than module will discard that packet otherwise packet will send to control block module.

CONTROL BLOCK MODULE:

Control Block Module compare incoming packet's IP address with adjacent node table if they matched than it forwards that packet to DoS detection Module otherwise packet sends to limited queue module.

ADJACENT NODE TABLE:

This module will sends hello packets in network at regular interval and receives incoming replies from network, at the same time it will put all the entry of incoming packets in adjacent node table.

LIMITED QUEUE ALGORITHM:

This modules first checks that is queue already allocated for incoming entry if yes than it will put packet in that queue but if no then it will check control block module for free entry. If free space is not available than it will discard packets else it will allocate a new queue for that packet.

DENIAL OF SERVICE (DoS) MODULE:

In this module first count the number of packet has been processed in span of time in control block table ad by using this it calculates threshold if it is over than desired value then corresponding IP is sends towards blocked IP table else processed that massage.

V SIMULATION & RESULTS

Performance of ANF (Adjacent Node Faith) approach is measured on the basis of Throughput, end-to-end delay and Packet delivery ratio. In this section we are comparing our approach with two existing approaches on the basis of time. Previous approaches are IP-trackback and other one is referenced broadcast synchronization. Simulations parameter table is as follows:

Simulation Parameter

Parameter	Default Values
No. of Nodes	20
Node speed	50 m/sec
Simulation Time	300
Environment Size	800 x 800 meter
Packet Size	500 KB
Antenna Model	Omni-directional Antenna
Packet Type	TCP/UDP
Traffic Type	CBR
MAC Layer	IEEE 802.11p
Visualization Tools	NAM

Simulation graphs are as follows:

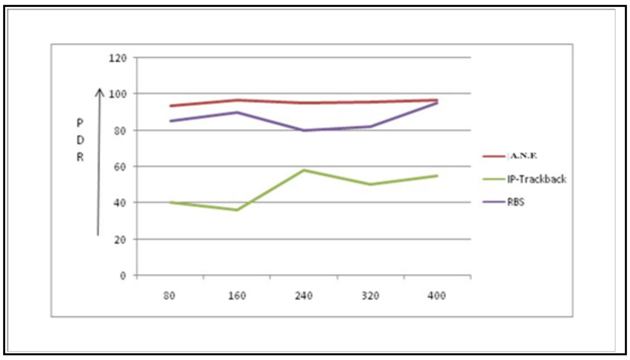

Figure 1 Comparison graph on the basis of PDR

In the Figure1 Horizontal plane represents time in seconds & vertical plane represents packet delivery in percentage. Red line represents our proposed approach "Adjacent Node Faith Algorithm" or ANF in the packet delivery ratio graph, blue line represents Reference Based Synchronization in the packet delivery ratio graph and green line represents IP-Trackback in the packet delivery ratio graph.

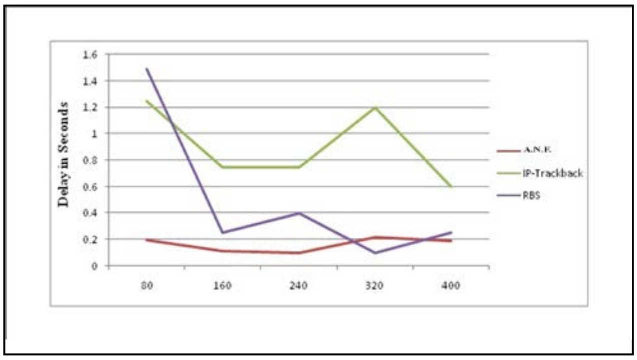

Figure 2 Comparison graph on the basis of delay

In the Figure2 Horizontal plane represents time in seconds and vertical plane Delay in seconds. Red line represents our proposed approach (ANF) in the end-to-end delay graph, blue line represents Reference Based Synchronization in the end-to-end delay graph & green line represents IP-Trackback in the end-to-end delay graph.

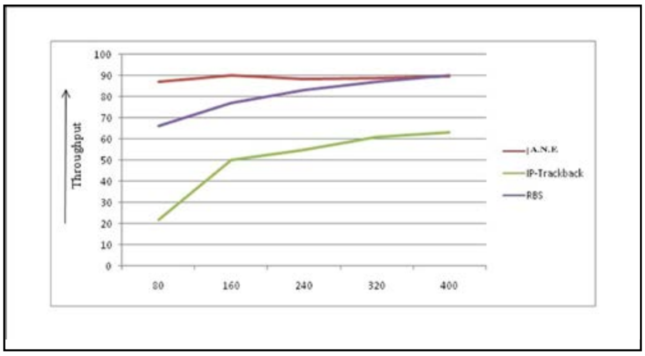

Figure 3 Comparison graph on the basis of throughput

In the Figure 3 Horizontal plane represents time in seconds and vertical plane shows throughput in bytes. Red line represents our proposed approach (ANF) in the Throughput graph, blue line represents Reference Based Synchronization in the Throughput graph & green line represents IP-Trackback in the Throughput graph.

VI CONCLUSION

ANF or Adjacent Node Faith scheme is able to protect VANET in concern of the security threats such as union of Sybil and DoS attacks. Dependence of this work is on the node's faith on its Adjacent Nodes for communication; by this we can protect VANET from fake IP problem. The proposed ANF (Adjacent Node Faith) model is work into two sections: one is for the known Adjacent Node nodes and the other is for the new nodes coming to its surroundings. For known Adjacent Nodes model implements DoS detection scheme and for new nodes, limited queuing is to be used. This approach is local and simple so it can be easily implemented in a network. Results of ANF are promising.

References

[1] K. Verma, H. Hasbullah and H. K. Saini, "Reference broadcast synchronization-based prevention to DoS attacks in VANET," *Contemporary Computing (IC3), 2014 Seventh International Conference on*, Noida, 2014, pp. 270-275. doi: 10.1109/IC3.2014.6897185

[2] Lyamin, Nikita, Alexey V. Vinel, Magnus Jonsson, and Jonathan Loo."Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11 pVehicular Networks", IEEE Communications Letters 18, no. 1, pp. 110-113, 2014.

[3] Macia-Fernandez G., Diaz-Verdejo E. J., and Garcia-Teodoro P.*"Mathematical foundations for the design of a low-rate DoS attack toiterative servers (short paper)"* Lecture Notes Computer science in Information and Communications security, pp. 282-291, vol. 4307,Dec. 2013.

[4] Lu. N., Zhang N., Cheng N., and Shen X. *"Vehicles meet infrastructure: toward capacity- cost tradeoffs for vehicular access networks"* IEEE Transactions Intelligent Transportation System, vol.14, Issue 3, pp. 1266-1277, July 2013.

[5] Spaho E., lkeda M., Barolli L., and Xhafa F. *"Performance Evaluation of OLSR and AODV protocols in a VANET crossroad scenario"* in proceeding of the *IEEE 27th Advanced Information Networking and Application (AINA) Conference* pp. 577- 582, 25-28 March 2013.

[6] Biswas S., Misic J., and Misic V. *"DDoS attack on WAVE- enabled VANET through synchronization"* in proceeding of the *IEEE Globalcommunications conference*, pp. 1079-1084, 3-7 Dec. 2012.

[7] Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan. "Vehicular ad hoc networks (VANETS): status, results, and challenges", Telecommunication Systems vol. 50, no. 4, pp. 217-241, 2012.

[8] Karagiannis, Georgios, Onur Altintas, Eylem Ekici, Geert Heijenk, Boangoat Jarupan, Kenneth Lin, and Timothy Weil. "Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions", IEEE Communications Surveys & Tutorials, 2011.

[9] Hasbullah, Halabi, Irshad Ahmed Soomro, and Jamalul-lail Ab Manan. "Denial of service (dos) attack and its possible solutions in

VANET.", World Academy of Science, Engineering and Technology (WASET), vol. 65, pp. 411-415, 2010.

[10]] José María de Fuentes, Ana Isabel González-Tablas, Arturo Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks", Handbook of Research on Mobility and Computing 2010.

[11]] Studer A., Bai F., Bellur B., and Perrig A "*Flexible, extensible, and efficient VANET authentication*" Journal Communications and. Trans.Networks, vol. 11, Issue 6, pp. 574-588, Dec. 2009.

[12] Rahim A., Ahmad I., Khan S. Z., Sher M., Shoaib A., Javed A., and Mahmood R. "*A comparative study of mobile and vehicular adhoc networks*" International Journal Recent Trends in Engineering, vol. 2, Issue 4, pp. 195-197, Nov. 2009.

[13] Hartenstein, Hannes, and Kenneth P. Laberteaux. "A tutorial survey on vehicular ad hoc networks", IEEE Communications Magazine, vol. 46, no. 6, pp. 164-171, 2008. [2] Gongjun Yan, Stephan Olariu, Michele C. Weigle, "Providing VANET Security through active position detection", ELSEVIER, Computer Communication 2008.

[14] Zhao J., Zhang Y., and Cao G. "*Data Pouring and buffering on the road: a new data dissemination paradigm for Vehicular Ad Hoc Networks*" IEEE Transactions on Vehicular Technology, vol. 56, Issue 6, pp. 3266–3277, Nov. 2007.

[15]]Harsch, Charles, Andreas Festag, and Panos Papadimitratos. "Secure position-based routing for VANETs.", IEEE 66th Vehicular Technology Conference, 2007.