Neighbor Trust Algorithm (NTA) to Protect VANET from Denial of Service Attack (DoS)

Varsha Raghuwanshi
M. Tech. Scholar, Department of CSE
NRI Institute of Information Science & Technology
Bhopal, Madhya Pradesh

Umesh Lilhore
Department of Computer Science & Engineering
NRI Institute of Information Science & Technology
Bhopal, Madhya Pradesh

ABSTRACT
In Vehicular Ad-hoc Networks (VANET), communication can be done with mutual understanding of vehicles. This communication is an important application of Intelligent Transportation Systems. In VANET, safety of user is a main concern, for achieving this vehicles are exchanging safety messages at regular interval to increase the passenger safety on road. But similar to other technology VANET is also suffering from some noticeable issues. From these issues one of the most important issues is security. Since the network is open and accessible from everywhere in the radio range of vehicle nodes, it is expected to be an easy target for malicious users. The availability of the network is extremely needed when a vehicle sends any safety information to other one. In this regard, Denial of Service (DoS) with spoofed IP attacks are very dangerous in VANET because they adversely affect the network availability and very difficult to detect. Oppress the node resources by flooding of messages to the victim vehicle is one of the most dangerous type of DoS attack, in which a malicious node sends a large number of message to the victim node and because attacker uses different ids for doing it, so it is very difficult for a victim to identify that sender of massages is a attacker or a legitimate VANET user. In this paper, we propose a Neighbor Trust Algorithm (NTA) which is an efficient method to defend against Denial of Service attack (DoS) with Spoofed IDs attacks.

Keywords
Neighbor Trust Algorithm (NTA), Denial of Service (DoS) Attacks, DSRC (Dedicated Short Range Communication).

1. INTRODUCTION
In the last few years, vehicles on road have been increasing rapidly, due to this keeping a safe distance between vehicles on urban areas is very difficult [11]. This situation led to accidents on road. To save the life of passengers many automobile manufacturers and international agencies has been worked together and develop a frame work called I.T.S. (Intelligent transportation system). I.T.S. is helpful for drivers, it can predict accidents or crash and can help them to suggest prefect route for their destinations, these routes are preferably less dense (or having less traffic). I.T.S. uses its own (Specially developed for VANET) wireless communication technology called Wireless Access to Vehicular Environment (WAVE), which is dedicated to vehicle to RSU and vehicle to vehicle communications [6]. This WAVE helps I.T.S. to ensure the passenger safety on road, by this the main goal of I.T.S. has been achieved on the aid to this on-board entertainment and information applications, such as online gaming, music & video streaming, etc are also supported by it. Manufacturers develops VANET enable vehicles, which are able to create wireless sensor network among each other, these vehicle have intelligence to self organized their network when need [3]. To achieve successful communication, a vehicle node needs efficient routing protocols which can deliver data packets from source to destination. Vehicle nodes must be equipped with computerized control modules, transmission and receiver equipments. Communication range of these vehicle nodes are not more than 300m, so when sender have to send data packets to the destination which is far away from it (may be distance between them in miles), it starts passing packets to its neighbor nodes and by the help of several intermediate nodes data packet shall be reached their destination successfully, by this process system can achieve end to end connectivity over a miles [14].

At the evolution of VANET people says that it is a part of Mobile ad-hoc Network. Reason behind this statement is both technologies have many similarities but when researchers have establishes VANET, people figure out some special characteristics in VANET which are different from MANET, and makes VANET a Special class of MANET. Those characteristics are: VANET posses' highly dynamic topology, frequently disconnected networks and hard delay constraints, these characteristics of VANET attract an attacker towards it. VANET is not able to prevent them self from those attackers because it has not been configured with security mechanism. In ad-hoc networks Denial of Service (DoS) is a well known attack. In VANET environment malicious vehicle node might launch a Denial of Service attack by consuming all the capacity of communication channel so that important safety massages do not reaches their destinations. The motive behind these attacks is to disable the whole network by selectively or continuously jamming the important transmissions. As we know that VANET is known for real time communication system, as a result of selectively or continuously losing a regular transmission could led to catastrophe [11]. Attacker may launch a direct attack in which he could simply synchronize to the corresponding providers and broadcast false messages at the same time as the service announcements, it could be delivered periodically. Frames which come simultaneously would collide and May a legitimate user unaware of the real messages which causes potentially disastrous result. Situation may become worse when, the device that sent the real message would never know that it had been lost, because broadcast communications are not accompanied by acknowledgements [12].

VANET is also suffered from the spoofed id attacks; architecture of VANET allows the attacker to forge source addresses of the incoming IP packet by replacing the header of packet with spoofed one. Generally IP spoofing is used by an attacker with DoS attacks in the VANET. Today in VANET environments, a Denial of Service attack is a major problem and it may causes major damages on the victim node [12, 4].

The remainder of this paper is organized as follows: Section 2 Describes about types of attacks in VANETs, Section 3

Reviews a related work on DoS and Sybil attack detection and protection, Section 4 Describes our proposed approach Section5 shows the performance evaluation and finally, the paper concludes in Section 6.

2. ATTACKS IN VANET

Every coin has its flipside, in case of VANET, It is very reliable and good technology to save life and time of passenger on road, but it also suffering from many attacks and these attacks are discussed in the following subsections.

2.1 Broadcasting of False massage

An attacker sends false massage to its neighbor vehicles; these massages may be, a wrong direction message, false information regarding the blockage of roads. Attacker may temper a safety massage, or it may send illegal and false information regarding huge jam on the roads. This attack led vehicle to a crash, the purpose of attacker behind this attack is to manipulate the flow of traffic around a chosen route for its own interest [9].

2.2 Malware

Malware may be used by attacker to get the information of victim vehicle node, malware such as viruses, Trojans, and worms may cause system failure of a victim node [7]. Viruses can infect system files of victim nodes by this it will unable to do it basic operations, Trojans may sends victim personal data to attackers such as passwords, worms can slows down the computation power of victim processor by starting un use full processes. This attacks are may be done by a fraud insider or outsider for their own benefit.

2.3 Sybil attack

Sybil attack deals with forge identities [13], attacker node may generate multiple identities of vehicles for its profit. Attacker creates multiple identities may be same as its neighbors to make fool of other available vehicle in the network, these identities may be used by attacker to cast attack in the VANET environment. The messages communicated in this type of attack include sending of false position as well as wrong direction information.

2.4 Message Suppression attack

In this attack attacker selectively drops packets from the network, these packets may bear important information for the receiver, so attacker suppressed these packets and use them again in when it wants [10]. The aim of such an attacker may be to prevent itself from insurance and registration authorities to knowing about collisions involving his vehicle or to avoid sending collision reports to RSU.

2.5 Alteration attack

In this attack attacker alters an existing data in a network [9]. It fetches the information from the network and changes the original body and header of the information, after some time it uses this changed information for its profit. This attack also includes replaying earlier transmission, delaying the transmission of the information, and also altering the actual entry of the transmitted data.

2.6 Denial of Service attack

This attack is very dangerous for VANET environment because it attacks on the availability of network resources. DoS attack blocks the availability of the networks through massage flooding, with excessive traffic through the channel with large amount of messages so that system may crash, by this victim system effectively denies the service to the valid users [2][9].

3. RELATED WORK

In paper [15] author suggests that in VANET, every vehicle should make sure of message transmitters authority and they have to authenticate it. Because if authentication is not provided by it, a malicious vehicle might do whatever it want and may cause a damage in a network. 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. Message contains identity information of a vehicle, so it can be tracked whenever desired and non-repudiation can be done in the network. Privacy of personal information about the vehicles is restricted from other vehicles.

In paper [7] authors suggested an approach to mitigate denial of service attack. In this approach onboard unit have a database and case studies by which OBU is able to understand that is attack happens on it or not. If it detects attack than its database suggests it to use channels switching by which OBU can protect itself from DoS attack. 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]. Switching options are FHSS, technology switching, channel switching, and multiple radio transceivers. Through which can we switch the information from one channel to another, so that it become possible that whenever attack will happen over there, then the traffic can be transferred to the another channel by using a secure mechanism.

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 neighbor nodes. In which node sends beacon packets to its neighbor 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.

4. PROPOSED APPROACH

Attacker sends multiple messages to the victim vehicle through DSRC channels as well as it may also use spoofed IP addresses for this. Because safety massages has highest priority over other massages they use all the bandwidth of the victim and messages come from different IP address also create problem to detect attack, thus victim is unable to communicate with other vehicles and denial of service with Sybil attack is occur. Our protection scheme works on that, in our scheme each vehicle keeps its neighbor's IP address in a table and update it at regular interval and after that it checks all incoming traffic, if coming packet is matched from IP present in a table than data will go through DoS detection module and then en-queue in a queue, otherwise 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 Neighbor's Table. By this way we shall able to protect network from Denial of Service with Sybil attack. Our Limited Queue Algorithm module create receiving limitation of massages as well as new queue allocation, this prevent the node from DoS attack as well as Sybil attack. When DoS attack starts all the internal queues of OBU are filled with messages and all the resources of OBU are busy in processing of these messages so communication with other vehicle is not possible. But if only limited numbers of messages (safety message) from legitimate user are received, OBU will perform its task quite easily.

INPUT MODULE:

i) Look Corresponding Entry in Blocked IP Table
ii) If Entry matched
iii) Discard Packet
iv) Else
v) Forward Packet to Control Block Module

CONTROL BLOCK MODULE:

I Look Corresponding Entry in Neighbor's Table
II If Entry matched
III Execute Denial of Service (DoS) detection Module
IV Else
V Execute Limited Queue Algorithm

NEIGHBOR'S TABLE:

i) Send Hello Packet in Network at regular interval
ii) Receive reply from network
iii) Put IP address of all received reply packet in Neighbor's Table.

LIMITED QUEUE ALGORITHM:

i) Check Queue is allocated for Corresponding Entry
ii) IF YES
iii) Put Packet in a Queue
iv) Else
v) Search the queue control table for a free entry.
vi) If (not found)
vii) Discard packet.
viii) Else
ix) Create a new entry with the state "IN-USE".
x) Enter the IP address in the queue control table.
*xi) If NC< =20 (*NC= Count of entries in Neighbor's Table)*
*xii) Create Queue with Length= (NC*10)*
xiii) En-queue data
xiv) ELSE
xv) Queue Length= (NC)
xvi) En-queue data

DENIAL OF SERVICE (DoS) MODULE:

i) Count Number of Packets for Corresponding IP in Control Table
*ii) Calculate C1 = (Count ÷ Max Queue Size) * 100*
iii) IF C1 > = Threshold (Where Threshold= 50)
iv) Put IP in Blocked IP Table
v) Else
vi) Put Entry in control table
vii) En-queue data

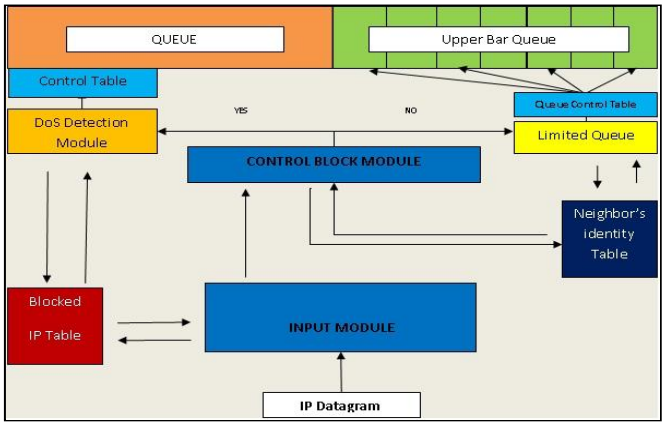

Figure 1 Logic Diagram

5. SIMULATION & RESULTS

Performance of our proposed approach is measured on the basis of Packet delivery ratio, Throughput and end-to-end delay. In this section we are going to compare our approach with two existing approaches on the basis of time. Those approaches are IP-trackback and other one is referenced broadcast synchronization. Simulations parameter table as follows:

1. Simulation Parameter

Parameter	Default Values
No. of Nodes	20
Node speed	60 m/sec
Simulation Time	400
Environment Size	1000 x 1000 meter
Packet Size	1 MB
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:

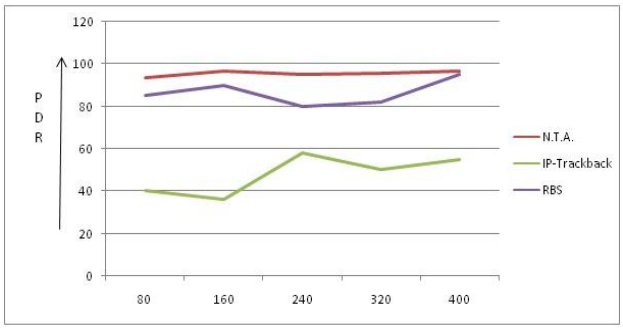

Figure 2 Comparison graph on the basis of PDR

In the Figure2 Red line represents our proposed approach (We named it "Neighbor Trust Algorithm" or NTA) in the packet delivery ratio graph, blue line represents Reference Based Synchronization (RBS) in the packet delivery ratio graph & green line represents IP-Trackback in the packet delivery ratio graph. Horizontal plane represents time in seconds and vertical plane represents packet delivery in percentage.

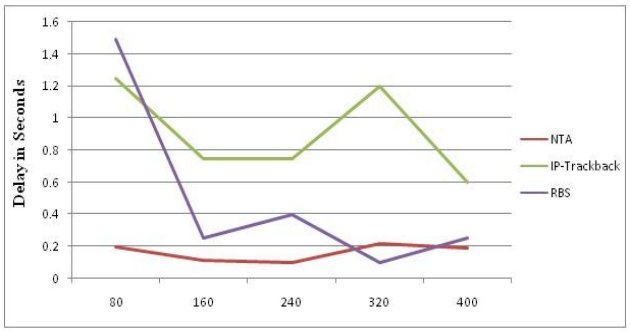

Figure 3 Comparison graph on the basis of delay

In the Figure3 Red line represents our proposed approach (NTA) in the end-to-end delay graph, blue line represents Reference Based Synchronization (RBS) in the end-to-end delay graph & green line represents IP-Trackback in the end-to-end delay graph. Horizontal plane represents time in seconds and vertical plane Delay in seconds.

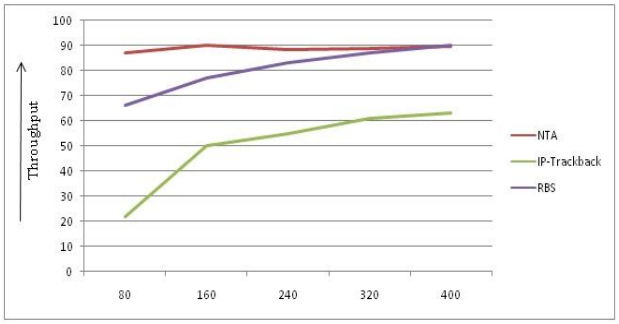

Figure 4 Comparison graph on the basis of throughput

In the Figure 4 Red line represents our proposed approach (NTA) in the Throughput graph, blue line represents Reference Based Synchronization (RBS) in the Throughput graph & green line represents IP-Trackback in the Throughput graph. Horizontal plane represents time in seconds and vertical plane shows throughput in bytes.

6. CONCLUSION

This work provides prevention mechanisms for VANET in concern of the security threats such as denial of service (DoS) attacks. The aim and contribution of this work is, node has to trust its neighbor for communication by this we can protect VANET from IP spoofing. The proposed NTA (Neighbor Trust Algorithm) model is work into two sections: one is for the known neighbor nodes and the other is for the new neighbor node. For known neighbors implements DoS detection scheme and for new neighbors limited queuing shall be used. This approach is local and simple so it can be easily implemented in a network. Results of this approach are promising.

7. 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.