International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Survey of Detection Techniques for DOS Attack in VANET

Jenis Shah[1], Deven Gol[2]

Department of Information & Technology, Silver Oak College of Engineering and Technology, Ahmedabad, India

Abstract: ***VANET is an application of mobile ad hoc network. More precisely a VANET is self-organised network that formed by connecting vehicle and aiming to improve driving safety and traffic management with internet access by drivers and programmers. So that security of the VANET is a critical issue. In VANET it is necessary that the network is mostly available all the time for the vehicles and RSU (Road Side Units). VANET faces several security issues due to which the network gets damaged and the services of the network may unavailable to the respective users or sometimes the wrong message of altered message passed during the communication. This type of security issues may lead in the failure of the network. Among all the attacks in the VANET, the DOS attack is very serious attack by which the services of the network get jammed and they cannot reach to the proper destination on time. Here, in this paper we analyze the different methods to detect the DOS attack in VANET.***

Keywords: VANET, DOS attack, Detection of DOS Attack, APDA, EAPDA, Security

1. Introduction

Nowadays according to the survey we analyze that the number of lives lost in motor vehicle crashes world-wide every year is by far the highest among all the categories of accidental deaths. With the increase in the no. of vehicle and humanpopulations as well as economic activities, roads will likely get busier. Thus, there is an urgent requirement to enhance road safety and reduce traffic congestion. Recently, with the advancement in technology more and more vehicles are being embedded with GPS and Wi-Fi devices that are connected in a self-organized way, this enables vehicle to vehicle (V2V) communication, forming a Vehicular Ad-hoc NETwork (VANET). VANET is a subset of the Mobile Ad-Hoc Network(MANET). Here, in VANET there are basically two types of communications. One is V2V (Vehicle to Vehicle) & another is V2I (Vehicle to Infrastructure).

VANET have no fixed infrastructure, and it is rely on the any network functionality. VANET can provide some safety related services like reporting the road conditions, information about the traffic on the road, weather conditions, warning of collision or accident. In VANET vehicles can communicate with each other by sending the messages and providing some other services like location based services, info related to jamming signals etc.

Vehicles may present some duplicate information to their drivers. If this information is dishonoured, the results of the control decision based on this information could be even catastrophic. In VANET each node is equipped with individual OBU (On Board Unit), to connect with RSU. GPS system is employed to identify the location of the nodes. The nodes can communicate with each other by sending messages at the distance of 100 to 300 meters.[4] Here the Roadside infrastructure units are used to support high mobility and bi-directional traffic on road. So that the RSU are installed on both sides of the road. The vehicles are communicated using dedicated radio signal of range 5.9 GHZ and 1 km range.

1.1 How VANET Work?

VANET is basically divided in to two parts. One is the access point which is usually fixed always connected to the internet, to act as a distribution points for vehicles. And another is the vehicle that works as a team spread on the road. As we know earlier that there are two types of communication takes place in VANET, V2V & V2I.

The V2V communication is further divided in to two types. i.e. single hop communication in which the vehicles directly communicate with each other, and one more is multihop communication in which vehicles relies on other vehicles to retransmit. The vehicles are also equipped with Temper Proof Devices (TPD) to hold the secret and confidential information such as trip details, speed, position and next route to be followed[1]. RSU determine the traffic condition and spread it widely over the longer distance and grant other traffic related services such as toll ticketing, monitoring, collision warning, accident information, road signal alarms and so on.

2. Security Requirements in VANET

a) Authentication
Authentication ensures that the message is generated by the proper user. In VANET a vehicle reacts upon the information came from the other vehicle hence authentication must be satisfied.

b) Availability
Availability requires that the information must be available to the legitimate users when it is needed, and sometimes it must have fast response time for specific applications. [8]

c) Confidentiality
It is needed that security must be provided to sensitive material being sent over the VANET.[8]

d) Integrity
Messages sent over the network should not be corrupted. Possible attacks that would compromise their integrity are

malicious attacks or signal failures producing errors in the transmission.[8]

e) Non-Repudiation
A sender cannot deny the fact of having sent the message and receiver cannot deny that not received the message.[8]

f) Privacy
The privacy of a node against the unauthorized node should be guaranteed. This is required to eliminate the massage delay attacks. The personal and private information of drivers and vehicles must not be available to unauthorized access.

g) Access control
It ensures that all the nodes in the network perform their functions according to the roles and privileges authorized to them.

3. Possible Attacks in VANET

1) Black Hole Attack
Nodes refuse to participate in the network or when an established node drops out. All network traffics are redirected to a specific node, which does not exist at all that causes those data to be lost.

2) Spamming
The presence of spam messages on VANETs increase the risk of transmission latency. The lack of centralized administration causes serious problems in VANET

3) Sybil Attack
Attacker creates large number of pseudonymous, and claims or acts like it is more than a hundred vehicle Threats to Confidentiality that to tell other vehicles that there is jam ahead, and force them to take alternate route.

4) Message Tampering
Any node acting as a relay can disrupt communications of other nodes. It can drop or corrupt messages, or meaningfully modify messages.

5) Timing Attack
Time is a crucial aspect in any application so users need accurate information on right time without any delay. In this attack attacker without manipulating the actual content add some time slot to create a delay in the message due to this user will receive the message after the required time, which leads to the unwanted accident on the route or the VANET network.

6) DOS Attack
In DoS attack the main objective is to prevent the legitimate user from accessing the services and from the resources. The attack occurs by jamming the network or channeling the system so that no vehicle can access it and aggressive injection of dummy messages. This avoids communication completely in the network which is devastating in real time applications.

Here, in this paper our main focus is on DOS attack, as it is very sensitive matter when this attack happens the intended receiver cannot get the real information from the sender and the receiver may affect from unwanted causes.

3.1 Situation of DOS Attack

The below cases describes what happens if DOS attack occur in the different situations of V2V (Vehicle to Vehicle) communication and V2I (Vehicle to Infrastructure) communication

Case: I
The V2V communication suffers by DOS attack where a victim node behind the attacker node receives a warning message “Accident at location Z” which is sent by an attacker. Same kind of message send by attacker continuously, keeps the victim node busy and it will completely deny to accessing the network

Case: II
Launch DOS Attack in V2I Communications. In this case, the attacker launches attack to Road Side Unit (RSU).
When RSU is continuously busy to verify the messages, any other nodes want to communicate with the RSU will not be able to get any response from it, thus the service is unavailable. Hence, sending critical life information in this situation is full of risk.

4. Existing Work on DOS Attack Detection

Among all the attacks we conclude that Detection of the DOS attack is very important for the security of VANET. So below are the details of the existing work of detecting the DOS attack.

In paper [2]author propose the security risk of DoS attack with the use of Onboard Units fit on each vehicle. The model relies on using OBU which resides on every vehicle node, so as to deter a DOS attack. The processing unit transfer information to the OBU, and suggest to change channels technology or to employ frequency hopping technique. OBU is provided with four preferences using which it can formulate decision based on the received malicious message. Subsequent to executing necessary processing and assessment, OBU send the information to next OBU in the network. The OBU can use available switching options such as channel switching, switching of technology, Frequency hopping spread Spectrum, multiple radio transceivers.

In the paper [6], author proposed detection scheme for detecting Sybil Attack using two techniques. The first one is a Localization scheme in which the vehicle’s location is verified on the basis of strength of received signal. A beacon signal is sent from one node to another on the basis of direction, speed, angle and distance of node to compare their geographical position in the network, perform verification and provide authentication to another node. And second technique is used for detecting Sybil attack, by means of distinguish ability degree metric. Every node can instigate it in the network.

In paper [3], proposed a Request Response Detection Algorithm (RRDA) which is used to detect DOS attack after APDA. By this the DoS attack detection has been extended

to multiple requests at a time in contrast to Attacked packet detection algorithm. Request Response Detection Algorithm has been implemented during the verification time. This method efficiently detects the attacks prior to the occurrence at node level. This increases the response time and maximizes the security in VANET.defining the rules associated with them has to be applied for control systems for improving system control performance.

In paper [4], author proposed Malicious and Irrelevant Packet Detection Algorithm (MIPDA) based on change in position, frequency and speed of the vehicle in order to detect the malicious vehicle posing DoS attack in the vehicular network. Thus the author reduced the delay overhead by detecting unwanted messages in early times.

In paper [5], author proposed an Attacked Packet Detection Algorithm (APDA) for detecting the DOS (Denial-of-Service) attacks before the verification time. The algorithm detects the invalid requests and attacked packets to avoid the delay that occurs while processing invalid requests and packets. This will not only minimize the overhead delay for processing but also enhances the security in VANET.

In paper [7], author represents Queue Limiting Algorithm that defines a limited capacity of each vehicle in anetwork for receiving safety message and defends against DoSattack without posing any security risk. The author classifiedthe messages into four classes and assigned priority to each class for accessing different DSRC channels of communication. An OBU on each vehicle is provided with a scheduler to control internal collision and allow high priority messages to be transmitted before low priority messages but the capacity of messages is decided by the QLA algorithm.

In paper [1], proposed Enhanced Attacked Packet Detection Algorithm which prohibits the deterioration of the network performance even under this attack. EAPDA not only verify the nodes and detect malicious nodes but also improves the throughput with minimized delay thus enhancing security. They proposed the solution to deal with Denial of service attack. DOS attack is being detected using timeslot so it is basically based on average communication time of the nodes as compared to earlier existing algorithm whose threshold was restricted by area. The proposed technique never falsely detect any node as a malicious node as done by existing schemes.

5. Conclusion

After analyzing the various approaches to detect the DOS attack in VANET we conclude that the EAPDA and APDA are very good methods to detect the DOS attack. In further, we will analyze the EAPDA method for the priority based vehicles and compare the results with the EAPDA methods.

References

[1] Amarpreet Singh, D. Priya Sharma,"A novel mechanism for detecting DOS Attack in VANET using Enhanced Attacked Packet Detection Algorithm", in International Conference RAECS UIET Panjab University Chandigarh 21-22nd December 2015978-1-4673-8253-3/15/ IEEE, 2015, pp. 850–855.

[2] HalabiHasbullah, Irshad Ahmed Soomro, Jamalul-lailAbManan, "Denial of Service (DOS) Attack and Its PossibleSolutions in VANET in International Scholarly and Scientific Research & Innovation 4(5) 2010

[3] Usha Devi Gandhi &R.M Keerthana, "Request Response Detection Algorithm for Detecting DoS Attack in VANET" International Conference on Reliability, Optimization and Information Technology - ICROIT 2014, MRIU, India, Feb 6-8 2014.

[4] Abdul Quyoom, Raja Ali , DevkiNandanGouttam and Harish Sharma, " A Novel Mechanism of Detection of Denial of Service Attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)" in International Conference on Computing, Communication and Automation (ICCCA2015).

[5] OS.Roselin Mary, M.Maheshwari, M.Thamaraiselvan, "Early detection of DOS attacks in VANET using Attacked packet detection algorithm (APDA)", ICICES, pp.237-243, 2013.

[6] Karagiannis, Georgios, OnurAltintas, EylemEkici, Geert Heijenk, BoangoatJarupan, Kenneth Lin, and Timothy Weil. "Vehicular networking:A survey and tutorial on requirements, architectures, challenges, standards and solutions", IEEE Communications Surveys &Tutorials, 2011.

[7] AdityaSinha&Santosh K. Mishra, "Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DoS) Attack" published in International Journal of Computer Applications (0975 – 8887) Volume 86 – No 8, January 2014..

[8] K.DeepaThilak "DoS Attack on VANET Routing and possibledefending solutions-A Survey" in International Conference On Information Communication And Embedded System(ICICES 2016)