ISSN:0975-9646

Analysis of Enhanced Request Response Detection Algorithm for Denial of Service attack in VANET: A Review

Deepali., Isha
Department of Computer Science and Engineering,
Lovely Professional University, Phagwara, Punjab-1444101

***Abstract*- Vehicular ad hoc networks are likely to be deployed in coming years and become the most relevant form of MANET. It is the special class of MANET i.e mobile ad hoc networks .In recent years not much work has to be done on security. So VANET is used for life saving of passengers .An attacker can change the behavior of other vehicle or infrastructure in the network and also try to challenge the network with their malicious attacks. . So in this review paper various detection methods for denial of service attack are discussed.**

Index Terms-MANET, VANET, MA, SA, TA.

I. INTRODUCTION

Now days vehicular ad hoc networks (VANET) are having more and more importance. It is used to enhance the protection of passengers and to reduce the occasion of traffic congestion. VANET is the class of MANET i.e mobile ad hoc networks. In this every node can move freely within the network and were stay connected, every node can communicate with other node. Now these days various accidents occur on the road, the estimated number of death is about 1.2 million in a year and various people are injured about 40 times of the number. So the aim of VANET is to provide safety. Its main potential is to improve vehicle and road safety, traffic efficiency and convergence as well as to provide comfort to both drivers and passengers. There are two types of nodes such as Road Side Units (RSUs) and On Board Units (OBUs). In case of road side unit there are fixed nodes along the routes where as on board unit refers to the mobile nodes which are equipped with radio interface that enables connecting to other nodes in wireless way. VANETs are dynamic in nature. Various numbers of nodes can communicate once as a group but they can change their own structure caused by leaving of member or joining with another node. Therefore it means nodes are "keeping in touch" with other nodes in a group to maintain the network.

1.1Various Classes of Attacks on VANET

Each class defines different types of attacks, their threat level and as well as attacks priority. The major aim of this model is to easily identify the attacks and their association to different class.

1).First Class: Network Attack: In this class attackers can affect directly other vehicles and infrastructure. These attacks are very dangerous because they affect the whole network. The main aim of these types of attacks is to create problem for legitimate users. In this class various attacks are come under like denial of service attack (DOS),Distributed denial of service attack(DDOS), Sybil attack, node impression attack.

2).Second Class: Application Attack: The main aim of this class is to change the content of the applications by attacker and he can use for their own benefits. In this the attacker can modify or change the actual message and send wrong messages or fake messages to other vehicles due to which various accidents occurs. For example Bogus information attack in which attacker send fake information to the network and these fake messages affects the behavior of users on the road.

3).Third Class: Timing Attack: In this case the main aim of attacker is to only add time slot in the original message due to which delay in the original message is to be created. It means the attacker does not disturb the other content of message , he just only creates the delay in message and the messages are received after it requires time.

4).Fourth Class: Social Attack: Its main aim is to indirectly create some problem in the network. The legitimate users show some angry behavior when they receive these types of messages. When the user heard some wrong message then he ultimately affects his driving behavior by increasing his speed of his vehicle. In this way the attack may occur.

5).Fifth Class: Monitoring Attack: The main aim of the attacker is to monitor the whole network and listen the communication between vehicle to vehicle and vehicle to infrastructure. Due to which if attacker find any related or useful information then he pass this information to the concern person.

There are three ways due to which the offender can achieve the denial of service attack:

1).Communication channel jamming
2).Overloading of network resource
3).Packet dropping

1).Communication Channel Jamming

In this type the attacker jams channel due to which users are not able to access or use the network. As its name indicate to jam the channel. In this a very high frequency are send the attacker and then jam the communication. Only when nodes leave the domain of attack it can able to send or receive.

2). Overloading of Network resources
As its name indicates in this the attacker can overload the node resources so that nodes cannot perform or does other work or tasks. All node resources are busy in message verification which comes from attacker node. In this RSU is engaged to check messages thus road side unit is not able to response to any other nodes and in this way service is not present or unavailable.
3).Packet dropping: In this type the various packets are to be dropped among various vehicles .Each were having their own IP address. False information is to be given to every vehicle due to which various accidents may occur. So this is all about the packet dropping.

II. RELATED WORK

In [1], authors proposed a model for detecting the dos attack by using attacked packet detection algorithm. The mechanism is attached to the road side unit (RSU).In this approach vehicle send various messages to the RSU by using APDA mechanism. It is used for detecting the position of vehicle. This ADPA algorithm is used before verification time. When the position is detected after that information is stored in the road side unit (RSU).The position or velocity of vehicle is identified by the on board unit. This algorithm is mainly used for detecting the vehicle's position and also detects the packet send by vehicle. If the packet was not attacked by attacker then vehicle cannot be tracked.
In [2], authors proposed a bloom filter based detection method which provides security service to the legitimate vehicles in VANET, this bloom filter method is used to detect the Denial of service attack.
A bloom filter based detection method is also used to defend against the IP spoofing of addresses in DOS attacks. It mainly focuses in increasing the systems connectivity as well as reliability. In this paper two techniques are used for detecting the denial of service attack:

1).Traffic capacity based Dos detection scheme: Now in first technique he generally shows that which flows are at victim attack and which are genuine. By using the packet detection mechanism various dos detection attacks are to be found. In this technique all packets are to be marked when the packet reaches its destination there should be a mark on packet by all of the RSU on the path that means the packet is traversed. It means the packets that traverse from that path are having same mark. So by using bloom filter packet it filters outs the packet. It means the packet which is having marked it means that packet is secure no attack on the packet.
2).IP-Chock (Filtering) Detection Algorithm: In this algorithm three phases are to be there Detection Engine Phase 1, Detection Engine Phase 2,Bloom Filter Phase. The detection engine phase1 collects the data which is to be processed in the next phase. While in detection engine phase 2 only process the information which is to be collected by the phase 1.If phase 2 does not found any malicious node then the information is to be stored in the data base. In third phase active bloom filter with a hash function is to be used. If in the decision engine malicious node is to be finding then alarms are generated and sends a link to all other nodes or vehicles that there should be a malicious node.
In [3], authors proposed a real time detection of dos attack. In this paper author mainly focus on the "jamming" of periodic messages called beacons which are exchanged by vehicles in platoon. In a platoon truck or leading vehicle is driven by person. In this the detector first only detects the event happening after that he computes hoe explainable occurring of collision is. It detects by using unicast method which is based on linear regression. This paper is based on two techniques:
1).A simple real time detector method for detecting the dos attack.
2). The detector is validated in terms of detection and false alarm probabilities within the limited time for two types of jamming attacks.

In [4], authors presented literature survey on security challenges in VANETs. In this paper various security issues are shown confidentiality, integrity, authentication, availability and non repudiation which are aimed to secure the vehicle to vehicle (V2V) and vehicle to infrastructure (V2I).Various attacks are shown in this paper which are as follows:
1).Sybil attack: In case of Sybil attack multiple fake nodes are to be present who broadcast the wrong information. In this the on board units are attached to the vehicles through which multiple copies are to be send to the other vehicles and every node contains the different identity. The problem starts when the malicious node is able to act as multiple vehicles and provides false data.
2).Node Impression attack: It is defined as the attack in which modified message is to be send by the node and act like that the message is come from the originator for the unknown purpose. In this case two techniques are used to detect the attack i.e greedy algorithm which is used for detection of malicious vehicle and the other algorithm is outlier detection algorithm which has been proposed for overcome this problem.
3).Sending False Information: As its name indicates it is defined as the attack in which wrong or fake information is send between the nodes to create a chaos scenario. The fake information is send by the attackers to vehicles for their own reasons. A technique is used to detect this attack is group signature technique. This technique is relies on password access.
4).ID Disclosure: In this case the identity is disclosed by the node and node's location is to be tracked. In this the target node is to be observed by the observer and virus is sending to the neighbors nodes.

In [5], authors proposed a technique to secure from denial of service attack and some solutions to overcome from attacks are also discussed in this paper. In VANET various attacks occur in the communication medium due to which channel jam. So to prevent from these kinds of attack or to save the legitimate nodes some techniques are to be used.

1).Oppress the node resources: In case of denial of service attack the attacker aim is to overwhelm the node such that they cannot perform any other tasks.
Case1:Vehicle to vehicle communication suffers by DOS attack; in this the attacker can send the wrong message to victim node that "Accident at location Z". Then after that this message is send again and again by attacker, to keep the victim node busy and he will properly deny to accessing the network.
Case2:In this vehicle to infrastructure communication suffers by DOS attack; whole attack is to be done on the road side unit (RSU), in this road side unit is engaged to check messages due to which RSU are unable to give response to other nodes and in this way service is unavailable.

In [6], authors proposed the queue limiting algorithm which will help to prevent or protect from denial of service attack. In this paper firstly described the system model which shows that every vehicle is having on board unit and for communicating with other vehicles they use DSRC channels. In this access points are present, vehicles send information about collision, crash and then after that access points send information to go that place. If access points are not present then information are passed by the vehicles. But if attacker knows then the things will be uncontrolled. Various false messages are sending to the victim node. Al channels are filled with CLASS 1 in this way victim node is not able to communicate with other vehicles due to which accident occurs.
Now the prevention mechanism includes that attacker send various false safety messages to victim node by using DSRC channel.

In [7], authors proposed techniques to detect and notify the attacks like "intrusion detection". Various attacks occur on vehicular ad hoc network such as Dos attack, black hole attack, Sybil attack etc. There are various characteristics of networks like highly dynamic network topology, shared wireless medium. In simple language intrusion is defined as any set of actions that done to compromise confidentiality, integrity or available of resource. The main work or goal of intrusion is to protect the system because if intrusion is detected then the attacks can be controlled.
In [8], authors proposed Bloom filter based IPCHOCKREFERENCE detection method to prevent from denial of service attack. The three goals of this paper are as follows:
1).The message delivery ratio is to be increased, by increasing the stability of link route message and also overhead is to be decreased, by reducing retransmission of message caused by drops occurring.
2).Reliability and connectivity of vehicle is also increased, by decreasing link breakage between communicating nodes and up to date information is to be provided by forwarding vehicle.
3).The overhead is also reduced which results from sending beacon between nodes.
The CUSUM technique is used which is based on IPCHOCKREFERENCE method. CUSUM is applied to detect the changes in digested traffic.
In [9], authors proposed Request Response Detection Algorithm after Attacked Packet Detection Algorithm which will be used for detecting the denial of service attack in VANET. Early detection algorithm is used before the verification. For the detection of attacked packet this algorithm considers mainly frequency and velocity of vehicle. Firstly the road side radio transductor (RSRT) sets the range and decides the range can form network which mainly depends on the transmission range. After that the vehicles request the RSDT with the help of attacked packet detection technique. Then the vehicles are verified by RSDT and make the database. Whole timestamp, location are shown by attacked packet algorithm.

After using attacked packet detection the vehicles are verified buffered in to RSRT. The jamming due to denial of service attack can again reduced by using Request Response detection Algorithm. Now in case of RRDA the vehicle which want to enter that are enter by request RSRT. Then it updates the counter. After that it checks the hop count. In this way RRDA algorithm works. The RRDA is used for further new request which wants to engage the network.

III. PROPOSED METHODOLOGY

In vehicular ad hoc networks, nodes are the vehicles which move at higher speeds as compared to nodes in mobile ad hoc networks. Since vehicles communicate wirelessly, they are prone to various attacks. In our work, we will focus on the denial of service attacks in vehicular ad hoc networks. Vehicles communicate with road side units to have access to information. Initially all the vehicles need to be registered prior to take part in the communication. We will use detection of the malicious vehicle in the network during the verification phase. The vehicles before entering in the network must pass the verification test defined by attacked packet detection algorithm. The difference between time at which vehicle sends the request and receiver receives the request must be less than threshold value for the vehicle to pass the verification test. According to APDA, the road side unit sets a range, so all the vehicles in its range can communicate with it, however any malicious node lying outside the range of the RSU can send the verification request so for that vehicle the difference of the sending and receiving the request at the RSU will be more than threshold value so it can be detected. However, if any node manages to pass the verification test and becomes a part of the network then we can detect it by allocating them time slots. After the node has passed the verification test and it becomes the part of the network. Road side units will allocate the time slots to the vehicles for communication. Since the malicious vehicle will continuously flood the control messages, so the RSU can easily detect which vehicle is sending more than average number of requests received by it in particular time slots assigned to the respective vehicles. The steps are shown on figure 1.

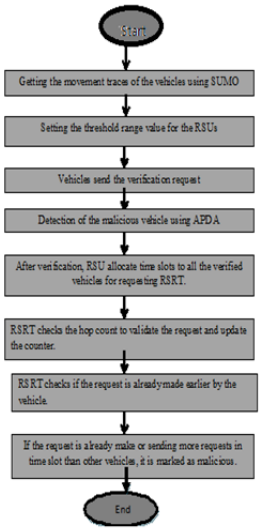

Figure 1: Steps to detect DoS attack in VANET

IV. CONCLUSION

The detection of Denial of service attack is very essential in case of vehicular ad hoc network. Till date various researches has been carried out but still at present the vehicular ad hoc network are not secured because of attacks occurring on the network. The main purpose of this review paper is to detect the Denial of service attack, by increasing the throughput by applying scheduling process. So this study proposes a scheme for providing an efficient mechanism to detect the attacks and reduce the accidents to a great extent.

REFERENCES

1. Roselin, M., & Mahsehwari, M.,(2013).Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA),.In *Engineering and Computational Sciences, 2013*. IEEE.
2. Verma, K. & Hasbullah, H., (2014).IP_CHOCK (filter)-Based Detection Scheme for Denial of Service (DOS) attacks in VANET,.In *Engineering and Computational Sciences, 2014*. IEEE.
3. Lyamin, N. & Vinel, A., (2014).Real-time detection of Denial-of-Service attacks *In802.11p vehicular networks, 2014*.IEEE.
4. Raw, R. &Kumar, M., (2013).Security Challenges, Issues and Their Solutions For VANET,*International Journal of Network Security,2013*.
5. Sinha, A. (2014) Technique to Secure DOS Attack,*International Journal on Ad Hoc Networking Systems,2014.*
6. Sinha, A. &Mishra, K,. (2014).Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DOS) Attack,2014.
7. Ouahidi, EL., (2014). A Review and Classification of Various VANET Intrusion Detection Systems, *Journal of Engineering Science and Technology, 2014*.
8 Verma, K. Hasbullah, H., (2012).An Efficient Defense method against UDP Spoofed flooding traffic of DOS Attack In VANET,.*Journal of Engineering Science and Technology, 2012.*
9 Gandhi.U,.(2014). Request Response detection algorithm for detecting DOS attack in VANET,*Journal of Engineering Science and Technology, 2014.*