Indian Journal of Science and Technology, *Vol 9(47), DOI: 10.17485/ijst/2016/v9i47/106865, December 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Detection of DoS Attack in VANETs

Deepak Rampaul[1*], Rajeev Kumar Patial[1] and Dilip Kumar[2]

[1]Department of Electronics and Communication, Lovely Professional University, Jalandhar-Delhi G.T Road NH1, Phagwara - 144411, Punjab, India; deepakrampal888@gmail.com, dilip.k78@gmail.com
[2]Department of Electronics and Communication, Sant Longowal Institute of Engineering and Technology, Longowal campus road, Longowal (Sangrur) - 148106, Punjab, India; rajeev.kumar@lpu.co.in

Abstract

VANET has number of applications like safety, comfort, efficient transportation services, entertainment and many more due to which it is growing in the present automotive industry. It is providing us a good resource for the Intelligent Transport System (ITS). But due to the mobile nature of the VANETs, a lot of problems in the actual implementation of this technology is arising. VANET uses wireless medium for its working, therefore, adding more difficulty to it. Because of this, it is easy to introduce security attacks by a malicious node. Such attacks can affect the proper working of the network. In this review paper, we have discussed about denial of service attack and its severity level. This paper analyses the different methods to combat denial of service.

Keywords: Attack, DDoS, DoS, Malicious Node, Security, VANET

1. Introduction

Vehicular Ad-hoc network comes under MANET which is further a part of ad hoc networks. An ad hoc network is a wireless connectivity which consists of individual devices having the ability to directly communicate with each other. It is a LAN (Local Area Network) which can be formed instantly rather than building a main serving access point. A Mobile Ad Hoc Network (MANET) can change its locations and can arrange itself wirelessly. VANET is a network in which vehicles can communicate with each other and can pass lifesaving messages. In others words, VANET is providing us a way of saving human lives as there is so much of traffic on roads now a days. Therefore, security of messages (information exchange) is a vital concern in VANETs due to its open access medium.

There are broadly two applications of the VANET i.e., non-safety and safety applications. First one includes drivers and passenger's comfort and improves the management of traffic system. Finding nearest filling station, availability of parking a car, weather information are some examples which comes under non-safety applications[1].

For safety applications, information should be error free and safely passed from sender to the target. Thus, security is very much needed because a little disconnection can create a big problem to the users. To gain this condition, network should be available to the users for all of the time.

Availability of the network is one of the major security requirements.

The inaccessibility or unavailability to the network caused by a malicious/fake node in the VANET system is known as denial of service.

2. Denial of Service (DoS)

DoS is done on the network for slowing down its working by introducing useless traffic. It makes network temporarily unavailable or suspends services of a host connected to the internet. In DoS attack, the faulty node transmits a large number of unneeded messages asking for the network to validate that requests which have incorrect return address. Therefore, the network will not be in a position to search for the address of the faulty node at the time

*Author for correspondence

when it has to send the authentication approval. It will cause the network to hold on for more time before ending the established communication link. When network shuts down the link, faulty node will send excessive messages for its authenticity, which have wrong return address. Therefore, the series of verification will run again and server has to wait for long time which keeps the network suspended.

Example of DoS attack is shown below:

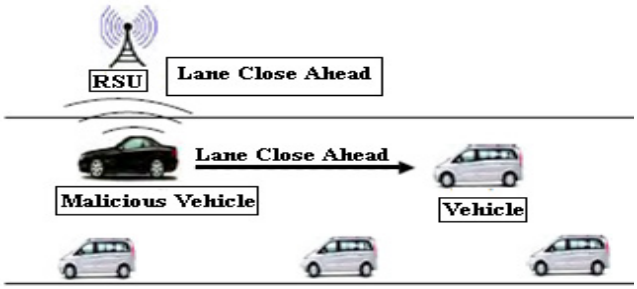

Figure 1. Example of DoS attack[2].

Categorizing the VANET system on the basis of its capacity, following attackers can be responsible for the DoS attack[3]:

- **Insider and outsider attacker:** If the attacker is the part of the communicating nodes then it will be an insider attacker. This type of attacker is harmful to the network in different possible ways. We can say an insider attacker is an authenticated person which is doing a wrong activity; hence, it is more dangerous to the network. On the other side, an outsider attacker is not an approved entity to directly transmit data with other users in the network. Therefore, it has less ways of attacking on the network.
- **Malicious and rational attacker:** Here the malicious attacker tries to interrupt the proper functioning of the network but not for his personal benefit while the rational attacker attacks on the network with a mind set of using several resources of the active network.
- **Active and passive attacker:** An active attacker has the ability of generating new messages so that they can harm the established network whereas passive attacker can just sense the network but cannot create new messages.
- **Local and extended attacker:** Local attacker holds a very limited scope on the network to attack even if it has control over the various nodes while the extended attacker can attack on a big area as it has control over several entities distributed across the network.

3. Security Attributes

For attaining the security in VANETs, we have to achieve some important requirements which are given below[3]:

- **Authentication:** In VANETs, it is necessary to authenticate the sender node so as to avoid the problem of impersonation. It tells us that the data is coming from a legitimate node of the network.
- **Availability:** In VANET system, it is important for the legitimate user to have the availability of the network all the time (even if there is an attack on the communicating nodes) by adopting some techniques which has less effect on the working of our network.
- **Integrity:** The intactness of the messages sent by the legitimate user should be so strong that an attacker cannot easily change the information contained in the message.
- **Confidentiality:** Privacy of every node must be protected. Information should be in encrypted form to check the attribute of confidentiality.
- **Privacy:** Privacy should be there for a legitimate node against any unauthorized node. Due to this, there will be a reduction in message delay attacks.
- **Data verification:** The chances of false messaging can be reduced by the regular & proper data verification.
- **Non-repudiation:** There should be a proper system for the users so that they cannot simply denies to send the message to the needed node.

4. Type of Attackers in DOS

Following are the ways from which an attacker can achieve DoS attack[4]:

4.1 Basic Level: Overwhelm the Node Resources

In this level, malicious node overwhelms the resources of valid nodes and leaves that node in a condition in which it cannot communicate with other nodes present in the VANET.

Case 1: DoS attack in Vehicle to Vehicle (V2V) communication

According to Figure 2, an attacker is sending a warning message 'accident at location Z". The entity which is at the back of the attacker node will receive this information. The attacker node will send this same message repeatedly and continuously to the victim node making it busier and denying it from accessing the network.

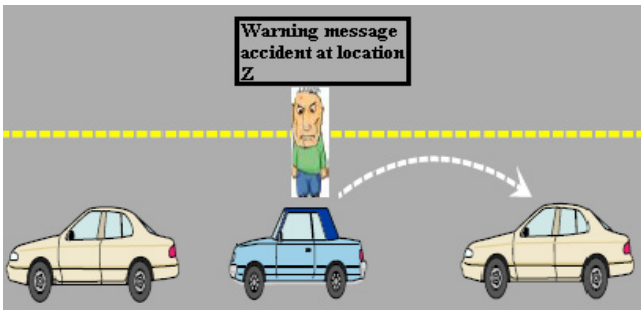

Figure 2. DoS attack in V2V communication.

Case 2:DoS attack in Vehicle to Infrastructure (V2I) communication

In this level of attack, attacker introduces attacks on the Road Side Unit. When the RSU is busy with checking the messages, any another node which wants to exchange information with the RSU will not get a reply. Hence, network services are unavailable to that node.

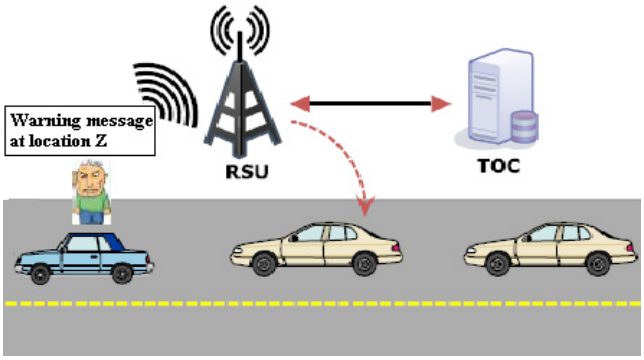

Figure 3. DoS attack in V2I communication.

4.2. Extended Level: Jamming the Channel

In the extended level, the attacker jams the channel. It completely eliminates the chance of information exchange in the VANET system. Therefore, extended level is more severe than overwhelming the node resources. There may be two possible conditions for this level:

Case 1: In this attack, attacker jams the whole channel in which a node has to communicate with the other node. From the Figure 4, it can be easily seen that the vehicles cannot receive or send information in the clouded part i.e., – services of the network will not be made available. The services are available to the authenticated node only when it leaves that attacked domain.

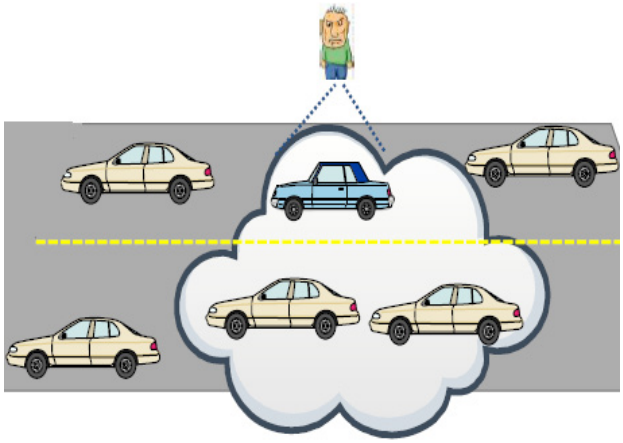

Figure 4. A domain of jammed channel for V2V communication.

Case 2: Next level of the attack is to block the communicating link between the infrastructure & the node so that there is no information exchange between them. In Figure 5, the attacker is launching an attack near to the road side unit which leads to the collapse of network.

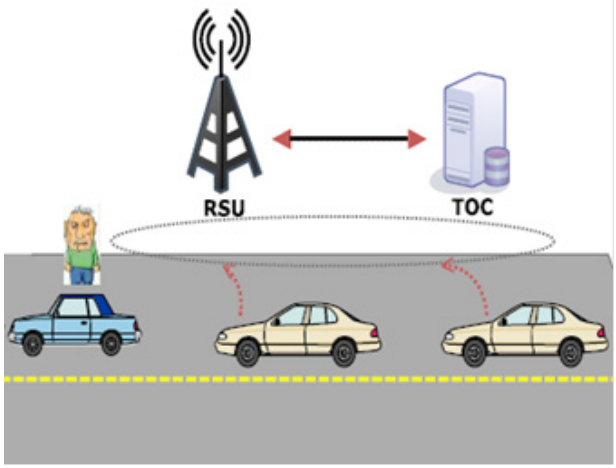

Figure 5. Jam the channel between V2I communication.

There is another worse condition in the DoS attack which is known as Distributed Denial of Service (DDoS). In DDoS, there is more than one attacker. So, this attack is dispersed in nature & more difficult to defend. Different geographical locations/sites are used by the attacker to launch this attack. Two conditions for this attack are:

Case 1: Here attacker attacks from various locations with various time slots. Therefore, the type of the message sent & the the time slot can vary from node to node.

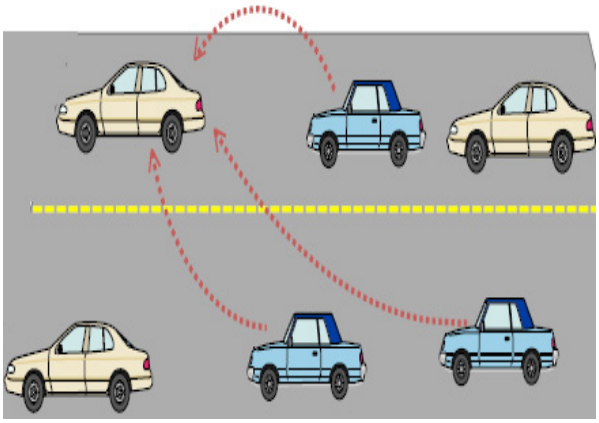

Figure 6. DDoS in V2V communication.

Case 2: In case 2, the attacker targets the infrastructure (RSU) of the VANET. In the Figure 7, it is shown that there are three attackers launching security threat on the VANET's infrastrucure with various sites. When node tries to communicate with RSU, it is found to be overloaded.

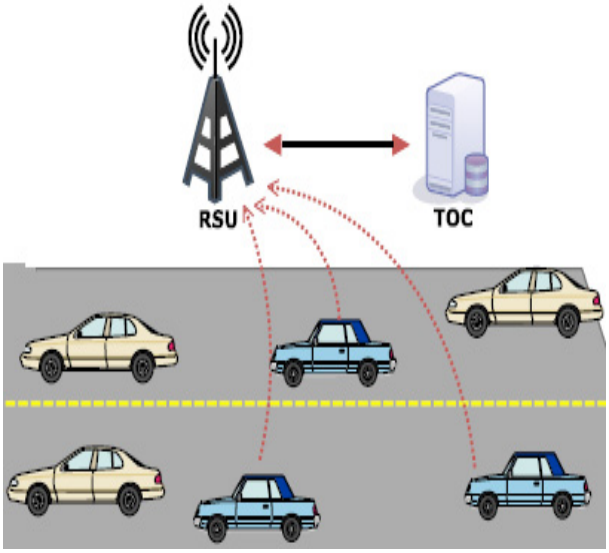

Figure 7. DDoS in V2I communication.

5. Work done in Defending DoS Attack

1. DJVAN: Detecting Jamming attacks in Vehicular Ad Hoc Networks proposed by[5] an algorithm called DJVAN for detecting jamming in VANETs using Packet Delivery Ratio (PDR). When jamming condition is true, an attacker will interrupt with the correspondence between two nodes. Therefore, the transmitter cannot find a free communication link for transmitting data. Even if the sender effectively transmits data, the receiving node will not get every one of the packet sent. Thus, its PDR is low and if its value is less than a threshold value we can judge whether there is a DoS attack or not.

Decrease in PDR is given by:

Down_PDR = (previous PDR - current PDR) ÷ (current time - previous time)

2. Mitigating Dos attacks against signature based authentication in VANET's proposed by[6] gives a pre-authentication process. In the DoS, a faulty node transmits fake data messages with wrong (unauthenticated) signatures to make the receiving node perform unnecessary signature verifications. Therefore, the gentle nodes will not verify the information from the valid user. They provided a pre-authentication process before signature verifying process to deal with DoS attack.

One-way hash chain and group rekeying scheme is used here.

3. Early detection of DoS attacks in VANET using Attacked Packet Detection Algorithm by[7]. In this paper, they applied a APDA (Attacked Packet Detection Algorithm) to defend DoS attack before the verification time. This technique is based on the position detection of the vehicles sending the false information.

AUTHORS	Techniques used (parameters)	Outcome
Lynda Mokdad et al.	DJVAN: Detecting jamming attacks in Vehicle Ad hoc Network	Detected jamming attacks in VANETs by the use of PDR (packet delivery ratio) and with performance analysis detected a threshold level that helps in differentiating between a poor link and an attacker.
Li He and Wen Tau Zhu	Signature-Based Authentication	Used pre-authentication process which involves one-way hash chain and a group rekeying scheme. Results shows the given scheme reduces DoS attack effectively.

S.Roselin Mary et al.	APDA: Attacked Packet Detection Algorithm	Detected DoS attacks before verification time which reduces the overhead delay for processing therefore enhancing the security.
Usha Devi Gandhi and R.V.S.M Keerthana	RRDA: Request Response Detection Algorithm	Detected DoS attack after APDA using RRDA which increases the response time (work is done on multiple requests)
Halabi Hasbullah et al.	Make use of OBU, Processing unit, Switching channels and technologies, Multiple radio transceiver, FHSS	DoS attack can be reduced by using any one of the technique i.e.-Channel switching, Technology switching, FHSS, Multiple radio transceivers
Karan Verma et al.	IP-CHOCK	Nodes with the same IP addresses in the database will be treated as attackers.
Hemanth Kumar .P et al.	Used a Transfer scheduler scheme along with Prototype analyzer	Distinguished the real/ authentic transfer with that of attack transfer and scheduled the transfer for better bandwidth usage.

Attacked packets are identified by change in position and change in frequency 'f', velocity 'v', 'α' is coefficient which is determined by the road characteristics and 'VMax' is the maximum speed =

$f = \alpha * | v - V_{Max} / 2 |$

'f' and 'v' are high because the position will change quickly. 'f' and 'v' are low because the vehicle positions will not change much.

It minimizes the delay overhead for processing & improves the security of VANET.

OUTPUT: 'v' and 'f' is high representing attacked packets or invalid request. Otherwise 'v' and 'f' is low representing to detect the attacked packets.

4. In Paper[8] paper makes advancement in the APDA discussed earlier. They give a new algorithm known as Request and Response Detection Algorithm (RRDA) to tackle with the problem of DoS after APDA. In this algorithm, the node which comes under the network range sends a request to the Road Side Radio Transducer (RSRT) which has the database of vehicles validation and hop count. The nodes can request the road side radio transducer by using APDA mechanism. In RRDA algorithm, the node which wants to enter in VANET can request RSRT and then RSRT updates its counter. After updating the counter, it checks the hop count made by a requested vehicle. If it matches the hop count then it updates the next hop and vehicle is assumed as an authenticated node and added to the network.

Furthermore RSRT checks if it made a request already and if it is there then it discards.

If request > max_cap_counter (maximum capacity of the packets) then show error message and transmit it.

5. Denial of Service (DoS) attack and its possible solutions in VANET by[9]. Here frequency hopping spread spectrum technique reduces the effect of DoS attack on VANET. When an attacker jams the communication channel, the message hops from one frequency to another. For hopping of one frequency to another they provided us with four switching technologies- UTRA-TDD, WI-MAX, WI-FI and Zig-Bee. Other techniques are also given in this paper to reduce DoS attack like channel switching, technology switching, and multiple radio transceivers. In multiple radio transceivers scheme an on board unit on a VANET node has multiple transceivers for receiving and sending messages (MIMO principle). Therefore, system will have the option to move from transceiver to another transceiver and the chance of total network collapse is eliminated.

6. Author in[10] proposed a method in which they made a model of product interaction for reducing DoS called 'IP-CHOCK'. It will be efficient to locate fake nodes without the need of any private information exchange. An efficient data structure is used for storage of consistent existing IP address information and a bloom filter based IPCHOCKREFERENCE (BFICR) detection method. They tried to make a communication link nodes and IP address 'IP-CHOCK' so as to maintain service abilities and DoS can be prevented. In this method, beacon messages are shared periodically with all the nodes to tell their existence in the network and to get aware about the next node. Each node saves a record of its database also. If any of the nodes finds a same IP address in the database, then the similar IP addresses can be said as DoS attacks.

7. Assuage bandwidth utilization DDoS attacks by using prototype analyzer and transfer scheduling scheme by[11]. In this paper, they tried to minimize the DDoS attack by using a transfer scheduler scheme with the combination of prototype analyzer. Their scheme further consists

of four modules i.e., - address verifier, session valuator, prototype analyzer and transfer scheduler. These modules have their own different functions which help in early stage mitigation of DoS and DDoS attacks. The main module is of address verifier which monitors transfer flow and drops any black listed attack packets if found.

Comparison of different schemes to mitigate DoS attack:

6. Conclusion

Safety is the first requisite to the road users. To fulfil this purpose VANET is introduced to the modern world. But it is the most challenging and promising research area to provide Intelligent Transportation System (ITS). Applications of the VANET may be categorized as safety, convenience and commercial applications. Due to the high mobility of the nodes, frequent disruptions in the link and security attacks implementation of VANET is a great but interesting challenge

For the proper functioning of the VANET system, network channel should be available to the needed user all the time. But due to the DoS attack, the availability of the channel can be obstructed. This attack has the highest level of risk as here the complete channel can be blocked and we cannot send our information to the other nodes.

There are different numbers of methods purposed for eliminating the DoS attack but at present we are not in a position in completely vanishing this attack and therefore a lot of research is going on this field. We can only reduce the severity level of DoS attack. In this review paper, we have discussed about the various possible solutions provided by different researchers that can reduce this attack including the DDoS attack also.

7. References

1. Hasbullah H, Soomro IA, Ab Manan J-L. Denial of Service (DoS) attack and its possible solutions in VANET. World Academy of Science, Engineering and Technology. 2010; 4.
2. Sirola P, Joshi A, Purohit KC. An analytical study of routing attacks in Vehicular Ad-Hoc Networks (VANETs). IJCSE. 2014; 3(4):210–8.
3. La VH, Cavalli A. Security Attacks and Solutions in Vehicular Ad-Hoc Networks: A Survey. IJANS. 2014 Apr; 4(2):
4. Pathre A, Agarwal C, Jain A. Identification of malicious vehicle in VANET environment from DDoS Attack. Journal of Global Research in Computer Science. 2013 Jun; 4(6).
5. Mokdad L, Ben-Othman J, Nguyen AT. DJVAN: Detecting Jamming attacks in Vedhicle Ad hoc Networks. Performance Evaluation; 2015.
6. He L, Zhu WT. Mitigating DoS attacks against signature-based authentication in VANETs. IEEE Inernational Conference on Computer Science and Automation Engineering (CSAE); Zhangjiajie, China. 2012.
7. Mary SR, Maheshwari M, Thamaraiselvan M. Early detection of DoS attacks in VANET using Attacked Packet Detection Algorithm (APDA). 2013 International Conference on Information Communication and Embedded Systems (ICICES); Chennai. P. 21–2.
8. Gandhi UD, Keerthana RVSM. Request response detection algorithm for detecting DoS attack in VANET. 2014 Internatinal Confernce on Reliability, Optimization and Information Technology – ICROIT 2014, MRIU; 2014 Feb. India. p. 6–8.
9. Hasbullah H, Soomro IA, Ab Manan J-L. Denial of Service (DoS) attack and its possible solutions in VANET. World Academy of Science, Engineering and Technology. 2010; 4.
10. Verma K, Hasbullah H, Kumar A. Prevention of DoS attacks in VANET. Wirerless Personal Communications. 2013 Nov; 73(1):95–126.
11. Kumar PH, Reddy KRA, Nagarjuna T. Assuage bandwidth utilization DDoS attacks using protoype analyzer and tranfer scheduling scheme. IOSRJEN. 2012 Aug; 2(8):187–18. ISSN: 2250-3021