Denial of Service Attack in VANET: A Survey

Varsha Raghuwanshi[#1], Simmi Jain[*2]

[#1]*M.Tech. Scholar, C.S.E. Department,*

[#2]*Assistant Professor, C.S.E. Department,*

NRI Institute of Information Science & Technology, Bhopal

ABSTRACT--- *Vehicular Ad-Hoc Networks (VANETs) isan indivisible component of I.T.S., where nodes are autonomous self-organizing and self-managing information in a distributed fashion. Its foundation is based on the co-ordination of vehicles and/or roadside units by which information is disseminated in network in organized way. In recent years, VANET has been taken more attention of automotive industries and researchers due to life saving factor. But always coin has two faces, when we know about its life saving factors at the same time security threats for VANET is also arises, so now VANET needs security to implement the ad hoc environment and serves users with commercial and safety applications. In this paper, we have done a survey of attack on network availability and its severity levels in VANET environment, which known as Denial of Service (DOS) attack, along with that different kind of hybrid Denial of Service attackis also present in it with their existing solutions.*

I. INTRODUCTION

In today's scenario congestion caused by vehicle crashes is considered to be an issue of great importance on the roads. Because of that, applications related to driver's safety are the focus of most researchers, who are working in the area of VANET systems. As a result efficiency of these applications is increases and has a good impact on network to limiting the number of accidents on road and providescomfortable, cleaner and safer travelling. Drivers on road have no ability to predict the conditions on the road coming ahead [1]. But now with the help of computer equipment, sensors and wireless communication devices along with a combination of advanced technically equipped devices it is possible to provide approach by which vehicles nodes on the roads can know the speed of its neighbor vehicles and predicts possible risk coming ahead [2]. By the use of such approach, vehicle could send warning messages periodically to its neighbor to predict their speed in order to avoidchances of accidents on road [3]. Because of high travelling speed of nodes in VANET network; dynamic network topology and high mobility are unique characteristics of VANET. Due to this some problem is faced by vehicle nodes in a network such as limitations of bandwidth due to the absence of central coordinator that manages and control communication between nodes, signal fading, and disconnection problems due to frequent fragmentation in the networks.

Security issues in VANET is an important prospective in today's scenario because of the rapid growth and increasing the utility of VANET. One of the most serious attacks in VANET is Denial-of-service (DoS) attack,because it attacks on the availability of network which causes life threatening effect on vehicle's drivers, a means of preventing such attacks must be found as soon as possible because the main objective of the attacker is to disturb the communication channel or overwhelms the vehicle's available services from the original users. Attack makes the system useless and this uselessness of the system in real-time vehicular networks even for a small instant of time is very dangerous.

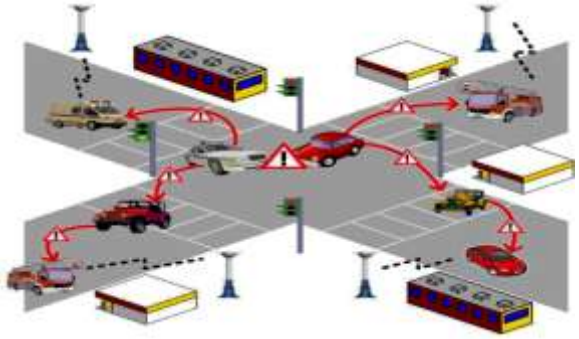

Figure-1 Vehicular Ad-hoc network

This paper is divided into six sections; Section II describes the work done in field of attacks in VANET. Section III explains the Denial of service attack and its level. In Section IV describe about HybridDOS attack. Section V provides the survey and critical review of existing solutions and conclusion is provided in section VI.

II. RELATED WORK

In 2010 HalabiHasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan published a paper on "Denial of Service (DOS) Attack and Its Possible Solutions in VANET" [4] In this paper, author presented a severity of denial of service attacks and its different level in VANET environment.. They have also suggests a model to secure the VANET from the DOS attacks in which they proposed a database of attackers by which their model can identify that is it attack or not and if yes then which kind of attack and according to that this model reacts.

In 2011 Hind AI Falasi, EzedinBarkapublished a paper on "Revocation in VANETs: A Survey" [5]in this paper author suggested a public key infrastructure (PKI) approach which was widely adopted by recent research efforts as a solution to security problems because of its usefulness. One part of a PKI solution is certificate revocation. It is one way to terminate the membership of a vehicle from the network who did some malicious activities in a network. Author suggests that revocation can also be conducted by the neighbor vehicles which areparticipating in the network. Survey of different revocation schemes developed for VANETs are done in this paper. According to author aim of this paper is to provide an overview of the extent of the research done in the area of revocation in VANETs.

In 2012 Subir Biswas, JelenaMiˇ si´ c, Vojislav Miˇ si´ c published a paper on "DDoS Attack on WAVE-enabled VANET through Synchronization" [6] in this paper author preset an attack scenario to reveal the deficiency in EDCA mechanism on the basis of synchronization-based DDoS attack bysmall contention window sizes and periodicity of transmissions. Things are going worse when, neither the receivers nor sender of periodic broadcasts will be aware of the attack since broadcast communications in VANET do not have acknowledgements., author analyze the prospect of a synchronization-based DDoS attacks on vehicular communications and also propose a solutionto avoid such attack.

In 2012 HalabiHasbullah, Karan Verma and Ashok Kumar published a paper on "An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VANET" [7]In this paper, author suggests an efficient method to detect UDP flooding attacks under different IP spoofing types. This method is depending upon use of a storage-efficient data structure and a Bloom filter based "IPCHOCKREFERENCE" detection method. This approach is not required any big changes in OBU that makes it relatively easy to deploy. Results of this approach is very promising which consistently showed that the method is both efficient and effective in defending against UDP flooding attacks under different IP spoofing types. Mainly, the method outperformed others in achieving a higher detection rate yet with lower storage and computational costs.

In 2014 Karan Verma, HalabiHasbullahpublished a paper on "IP-CHOCK (filter)-Based Detection Scheme for Denial of Service (DoS) attacks in VANET" [8] In this paper, author suggests the Bloom-filter-based detection method, which provides the availability of a service for the genuine vehicles in the VANET. This approach is used to detect and defend against the IP spoofing of addresses of the Denial of service attacks.This method is useful because it provides a secure communication as well as it also frees the bandwidth of the network. This approach requires a fewer resources and is easy to deploy. Results of this approach show that this method is efficient and effective to defend against and detect Denial of service attacks.

III. DENIAL OF SEVICE ATTACK

In VANET environment, usually the attacker attacks the communication medium to cause the channel jam or to make issues for the nodes from accessing the network. The main purpose is to prevent the genuine nodes from accessing the network services or from using the network resources. Because of this node will not be able to receive or send important information in network. Finally, the

networks are no longer available to authentic users. DOS could not be allowed to happen in VANET, because life critical information must reach its destination securely and timely. There are three ways the offender may achieve DOS attacks, namely communication channel jamming, overloading of network resource, and packets dropping [9].

A.Make Node Resource Uselesss

In this DOS attack, the attacker's goal is to overwhelm the node resources such that the nodes cannot perform other important and necessary tasks. All the resources of the nodes will continuously busy in message verification, which (messages) is coming from attacker nodes.

a) Case I: V2V Communication suffers by DOS attack as shown in Figure 2, a victim node behind the attacker node receives a warning message "Accident at location Z" which is send 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.

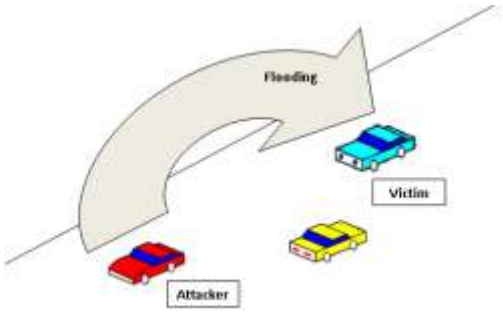

Fig 2 DOS attack in V-to-V communications

b) Case II: V2I Communications suffers fromDOS Attack; In this case, Road Side Unit is suffers from DOS attack; attacker directly attacks on it which is shown in Figure 3. RSU is continuously engage to check the messages, thus RSU is not able to give response to any other nodes, and thus the service is unavailable. Because of this, sending crucial life information in this situation is quite risky.

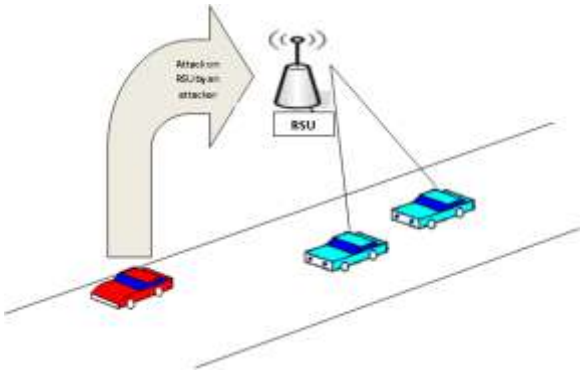

Fig. 3 DOS attack in V-to-I communications

B.Physical Layer attack: Channel Jamming

This is a worst level of DOS attack. In this attack, attacker jams the channel, because of that; other users are not able to access the network. The two possible cases are as follows:

a) Case I:In this case high frequencies are sending by an attacker and jam the communication between nodes in a particular domain, as shown in Figure 3. Nodes are not able to send or receive messages in that domain;thus, services are not available in that particular domain due to attack. Only when a node leaves the domain of attack it can able to send or receive messages. See figure 4.

b) Case II: The next level of attack is to jam the communication channel between the nodes and the Roadside unit (RSU). Which is illustrated in Figure 4; the situation is that, the attacker launches an attack near the RSU to jam out the channel, causing to network breakdown. Thus; nodes and RSU are notable to send or receive messages from each other, this cause network unavailability. See figure 5.

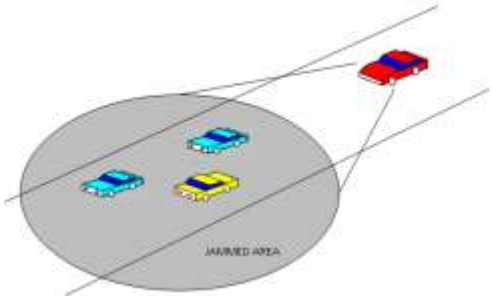

Fig.4 A domain of jammed channel for V-V communication.

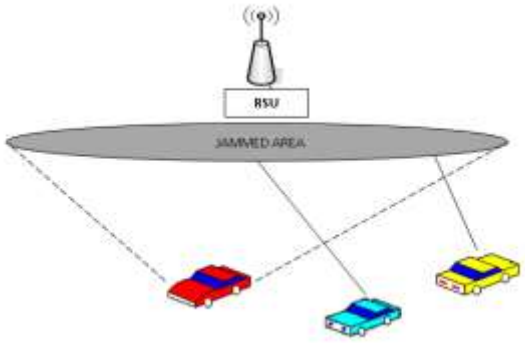

Fig. 5 Jam the channel in between vehicle-to-RSU

C. Distributed Denial of Services (DDOS)

DDOS attacks are very dangerous in the vehicular environment because the process of the attack is in distributed fashion where the impact is disseminating in the network. In this attack, the attacker takes control over the other nodes in a network and launches attack from different locations. Two possible cases are as follow:

***a) Case I*:** In this case, attacker sends message to victim from different locations and may be use different time slots for sending the messages. The attacker may change time slotsand the messages for different nodes. The goal of the attack is to make network unavailable for victim node by bringing the network breakdown. As shown in Figure 6.

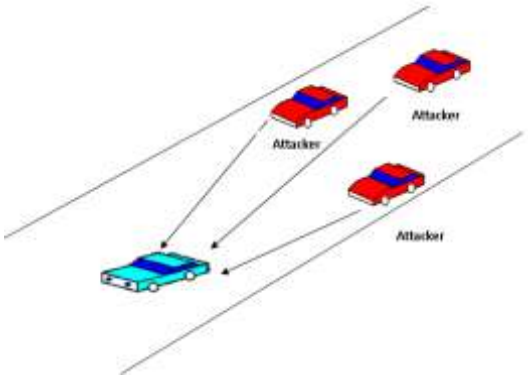

Fig. 6 DDOS in V-to-V communications

***b) Case II*:** In this case, VANET infrastructure (RSU) is the target for attacker as shown in Figure 7. Attacker launches attack on the infrastructure from different locations, because of that when other nodes in the network want to access the network, the road side unit is not able to respond them, thus it cause denial of service.

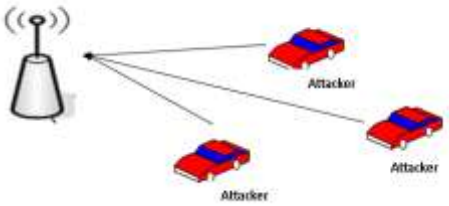

Fig. 7 DDOS in V to I communications

IV. HYBRID DOS ATTACK

As we explained above DoS attack is very dangerous for VANET networks, but what happen when it will be used by attacker with some other attack (eg. sybil, alteration, etc). This section presents hybrid dos attack in VANET.

A. Network Mode: The network mode of the Denial of Service attack creates a serious problem in VANET environment. Bandwidth of a node is blocked by the attacker and the network becomes jammed due to flooding. By using network layer attacker can produce enormous amount of packets and send them into a targeted vehicle known as flooding, in this way, attacker takes up a vehicle's computing resources and seizes genuine network traffic by overloading the communication channel. Because of this, lifesaving information can't be disseminating to other vehicles on time. Furthermore, it can cause danger to the driver if he make its decisions on the information giving by an application.

B.Application Mode:In this mode attacker broadcasts a wrong message to mobile vehicle drivers and diverts them to another path [12].

(a) Sybil Attack: This attack happens when an attacker creates a large number of fake identities and claims that more than a hundred vehicles tells other vehicles that there is a jam ahead and forces them to take an alternate route. This attack depends on some conditions such as how cheaply identities can be generated and depending on the way to which the

other nodes accepts inputs from entities that do not have a trusted chain linked them to a trusted entity,therefore the system treats all entities identically. For a period of time an attacker can act like hundred vehicles to agree the other vehicles on the road that there is congestion and instruct them to go to another route [12, 13].

(b) Message Suspension Attack:In this attack attacker selectively drops packets from the network. These packets contain some critical informationfor the receiver. Attacker save these packets and shall use them again at another time. Aim of such an attacker is to prevent insurance and registration authorities from knowing about involvement in collisionsof its vehicle and to avoid collision reports delivery to roadside access points [14, 15].

(c) Alteration Attack:In this attack, attacker alters the existing data of the network. This attack includes delaying the transmission of information, altering the actual entry of the data transmitted. For a period of time, attacker can alter a message sending other vehicles that the current road is clear while heavy traffic on road is present.

(d) Fabrication Attack: An attacker can implement this attack by transmitting incorrect information to the network. This information could be false or the sender can deny that he is responsible for it and put allegation on someone else. This attack includes fabricated messages, certificates, warnings and identities [16, 17].

(e) Replay Attack: In this attack attacker replays the transmission of earlier information to take advantage of the situation of the message at the time of sending [18].

(f) Black Hole Attack: In this type of attack, an unauthorized user broadcast its routing advertisements by using its own routing protocol. In these advertisements, it claims to have shortest path to the destination node.

(g)Jamming Attack:In this attack jammers deliberately generate interfering transmissions or signals to prevent communication across the network. Since the network coverage areas are well-defined in VANETs

V. SURVEY AND CRITICAL REVIEW OF EXISTING SOLUTION:

Table 1 summarizes the DoS attack protection schemes and classifies them according to scheme uses (i) Sybil attack protection, (ii) Message suspension protection, (iii) Replay attack,(iv) Fabrication attack, (v) BalckHole attack, (vi) Jamming attack, or (vii) Alteration attack protection**.**Table shows that different authors presented various schemes for VANET protection from different attacks and which scheme is more effective on different attacks.

In the following table Ali Hamieh's protection scheme is effective on Physical Jamming attack but it is not protect VANET from any other attack. As same as Grilles scheme is effective on message suspension and fabrication attack and if other than previous attack is happen this scheme is remain helpless.

Table 1DoS attacks protection schemes

Protection Schemes	Sybil Attack Protection	Message Suspension Protection	Replay Attack Protection	Fabrication Attack Protection	Black Hole Attack Protection	Jamming Attack Prevention	Alteration Attack Protection
Ali Hamieh et al (2009)	No	No	No	No	No	Yes	No
Gilles et al. (2007)	No	Yes	No	Yes	No	No	No
Ali et al. (2009)	No	No	No	No	No	No	Yes
Jyoti et al.	Yes	Yes	Yes	Yes	No	No	No

(2010)							
Irshad et al. (2011)	**Yes**	**Yes**	**Yes**	**Yes**	**No**	**No**	**No**
Nicole et al. (2012)	**Yes**	**No**	**No**	**No**	**No**	**No**	**Yes**
Hasbullah et al. (2014)	**Yes**	**No**	**Yes**	**No**	**No**	**No**	**No**
EmanFarag Ahmed Et al. (2014)	**No**	**No**	**No**	**No**	**Yes**	**No**	**No**

VI. CONCLUSION:

Safety is the primary aim for many road users. Therefore safety requirements should be well supported by many safety applications such as accident notification etc. Furthermore, life critical messages must be transmitted from node to node in the VANET network in reliable and timely manner. In this paper we have discussed the different types of attacks that may be applicable to VANET. We have done a survey on existing solutions, which the intention is to ensure network availability for secure communication between the nodes. We found that network availability has been directly affected in the case of DOS, DDOS attacks and their hybrid attacks, where the attacks has led to most severe impact by causing the network to break down.

REFERENCES

[1] Amadeo, M., C. Campolo, and A. Molinaro, Enhancing IEEE 802.11p/WAVE to provide infotainment applications in VANETs.Ad Hoc Networks, 2012. 10(2): p. 253-269.

[2] Blum, J.J., A. Eskandarian, and L.J. Hoffman, Challenges of intervehicle ad hoc networks. Intelligent Transportation Systems, IEEE Transactions on, 2004. 5(4): p. 347-351.

[3] J Raymond, D.R. and S.F. Midkiff, Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. Pervasive Computing, IEEE, 2008. 7(1): p. 74-81.

[4] HalabiHasbullah, Irshad Ahmed Soomro, Jamalul-lail Ab Manan, Denial of Service (DOS) Attack and Its Possible Solutions in VANET: World Academy of Science, Engineering and Technology 41 2010,p 411-415.

[5] Al Falasi, H.; Barka, Ezedin, "Revocation in VANETs: A survey," Innovations in Information Technology (IIT), 2011 International Conference on , vol., no., pp.214,219, 25-27 April 2011

[6] Subir Biswas, JelenaMi˘si´c, Vojislav Mi˘si´c "DDoS Attack on WAVE-enabled VANET Through Synchronization", Communication and Information System Security Symposium -Globecom 2012.

[7] HalabiHasbullah, Karan Verma and Ashok Kumar, "An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VANET"

[8] Karan Verma, HalabiHasbullah, "IP-CHOCK (filter)-Based Detection Scheme for Denial of Service (DoS) attacks in VANET"

[9] J. Blum, A. Eskandarian, "The Threat of Intelligent Collisions", IT Professional, IEEE Computer Society, 2004

[10] Khaleel, M., Hassan, A., & Mario, G., "ROAMER: Roadside units as message router in VANETs", Elsevier, Ad Hoc Networks, 10(3), 479–496, 2012.

[11] Congyi, L., &Chunxiao, C., "RPB-MD: Providing robust message dissemination for vehicular adhoc networks", Elsevier, Ad Hoc Networks, 10(3), 497–511.

[12] Karan Verma,HalabiHasbullah, e.al,"Prevention of DoS Attacks in VANET", Springer, 2013

[13] U.S. Department of Transportation, Intelligent TransportationSystem (ITS), November 1997.

[14] Wu, M., Yang, L., Li, C., & Jiang, H, "Capacity, collision and interference of VANET with IEEE 802.11 MAC", In 1st Intelligent networks and intelligent systems conference, ICINIS (pp. 251–254), Nov.1–3, 2008.

[15] Mishra, T., Garg, D., & Gore, M. M.," A publish/subscribe communication infrastructure for VANET applications", In IEEE advanced information networking and applications (WAINA) workshops (pp. 442–446), March 22–25, 2011.

[16] Isaac, J. T., Zeadally, S., &Camara, J. S, "Security attack and solutions for vehicular ad hoc networks". IET Communications Journal, 4(7), 894–903, 2010.

[17] Abedi, O., Barangi, R., &Azgomi, M. A," Improving route stability and overhead of the AODV routing protocol and make it usable for VANETs", In 29th IEEE distributed computing systems workshops (pp. 464–467), June 22–26, 2009.

[18] Kargl, F., Papadimitrators, P., Buttyan, L., Muter, M., Schoch, E., Wiedersheim, B., et al., "Secure vehicular communication systems: Implementation, performance, and research challenges",IEEE Communications Magazine, 46(11), 110–118, 2008.