Preventing VANET From DOS & DDOS Attack

Aditya Sinha[#1], Prof. Santosh K. Mishra[*2]

[#1]*Student of final year CSE dept., V.N.S. Group of institutions, Bhopal*

[#2]*Professor, CSE dept., V.N.S. Group of institutions, Bhopal*

Bhopal - MP - India

Abstract—.**VANET is an emerging technology; it is a special class of MANET. There are many challenges that must be addressed before it can be successfully deployed. In recent years, not much work is done in the field of security. For security, availability of network is must be obtained at every time since availability of the network is crucially needed when a node sends any important information to other nodes. Nevertheless, it can be expected that security attacks are likely to increase in the coming future because of more and more wireless applications being developed and deployed onto the well- known expose nature of the wireless medium. In this regard, the network availability is exposed to many types of attack. In this paper, Denial of Service (DOS) attack on network availability is presented with its severity level in VANET environment. A technique to secure the VANET from DOS attack has been introduced and some possible solutions to overcome the attacks have been discussed.**

Keywords: **VANET, DOS, Security, DDOS, DSRC.**

I. INTRODUCTION

VANET is a network in which vehicle nodes can communicate with each other on the road [3]. VANET applications have been widely divided into safety and commercial applications. Safety applications are very vital in nature as these are directly related to users and their lives. Post-crash, change of direction, etc notifications on a particular road is provided by these applications [2]. Commercial applications are to comfort the drivers and passengers. Examples of these applications are parking availability, traveling map and weather information. The purpose of both application categories is to provide actual information to users/drivers on the roads. Nevertheless, for safety applications, the information not only needs to be authentic but also securely transmitted from a source to a destination. Hence, security is a vital issue where little disturbance create problem to the users. This is particularly important if life critical information is being communicated between a sender and a receiver. To obtain this, availability of network is a basic requirement. It is defined as when any node wants to access the other node in the network or to access the infrastructure, the network should be available for user. The unavailability may be caused by any fault or attacks, such as Denial of Service (DOS).

This paper is divided into five sections; Section II describes the possible attacks in VANET. Section III explains the Denial of service attack and its level with possible use cases & their solution. In Section IV we discuss proposed solution to secure the network and Conclusion in Section V.

VANET is vulnerable to many attacks; these attacks are discussed in the following subsections:

II. ATTACKS IN VANET

A. Denial of Service attack

In this attack, attacker takes control over a vehicle's resources or jams the communication channel used by the VANET; by this it can prevent important information from arriving. For example, if a malicious node wants to create a traffic jam on the road, it can make an accident and use the DOS attack to prevent the warning notification from reach of the approaching vehicles [6], [12], [4], and [13].

B. Message Suppression Attack

This attack happens when the attacker selectively dropping packets from the network, packets may have bearing important information for the receiver, packets are suppress by the attacker and use them again in other time [12]. The aim of such an attacker would be to prevent insurance and registration authorities from knowing about collisions involving his vehicle and to avoid sending collision reports to RSU [14].

C. Fabrication Attack

In this attack, false information are transmitting into the network by an attacker, the transmitter could claim that somebody else are sending information and that information is false as well. Fabricate warnings, Identities, messages, certificates, etc are included in this attack [4], [12] [14].

D. Alteration Attack

An attacker alters an existing data in a network. This attack includes replaying earlier transmission, altering the actual entry of the data transmitted, or delaying the transmission of the information [12]. For instance, message is alter by an attacker that "Current road is clear" and send this to other nodes, but actually there is congestion on that place [14].

E. Sybil Attack

This attack happens when a node sends multiple messages to other nodes and every message contains a non identical

source in such a way that the originator is not known. The main goal of the attacker is to create confusion to other nodes by sending wrong messages and to emphasize other nodes to leave the road for the attacker's benefit [11].

III. Denial of Service 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 legitimate nodes from accessing the network services or from using the network resources. Network resources and node will not be able to receive or send important information because of this attack. Finally, the networks are no longer available to authentic users. DOS shall not be allowed to happen in VANET, because life critical information must reach its predestined destination securely and timely. There are 3 ways the offender may achieve DOS attacks, namely communication channel jamming, overloading of network resource, and packets dropping [7]. There are 3 kinds of DOS attacks as described below with their available solutions:

A. Oppress the Node Resources

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 1, 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.

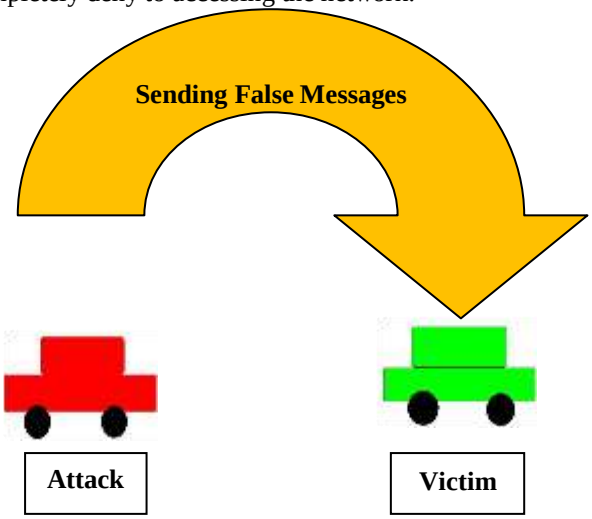

Fig 1 DOS attack in V-to-V communications

b) Case II: V2I Communications suffers from DOS Attack; In this case, Road Side Unit (RSU) is suffers from DOS attack; attacker directly attacks on it which is shown in Figure 2. 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. Therefore, sending crucial life information in this situation is quite risky.

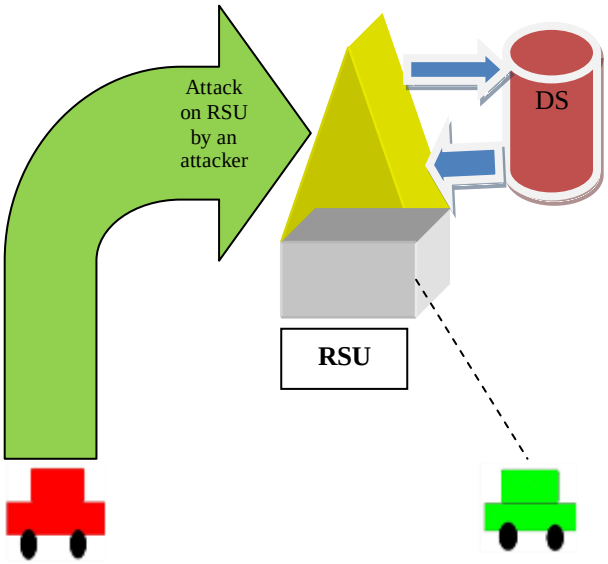

Fig. 2 DOS attack in V-to-I communications

Solution for this Attack is given below:

Author suggests [9] the solution for above kind of DOS attack by which node can protect itself from attack and if it happens then node is able to bear it. The model is depends on the use of On-Board-Unit (OBU) that is installed on each vehicle, to make decision as to block a DOS attack. If the DOS attack happens, the Processing Unit will suggest to the OBU to switch technology, channel, or to use frequency hopping technique. OBU have four options by which it can make decision based on the received malicious message. After necessary processing and decision, OBU send the information to next OBU in the network.

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 3.

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 4.

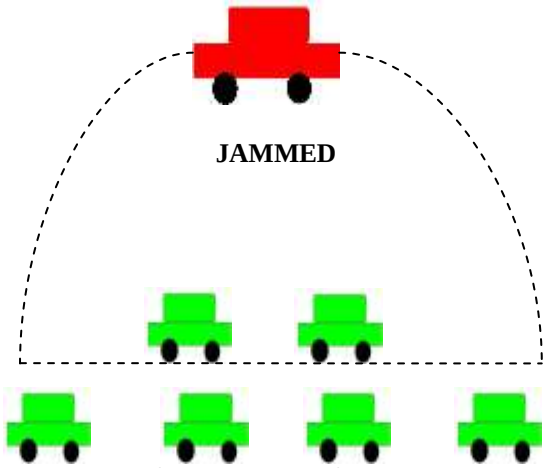

Fig. 3 A domain of jammed channel for V-V communication.

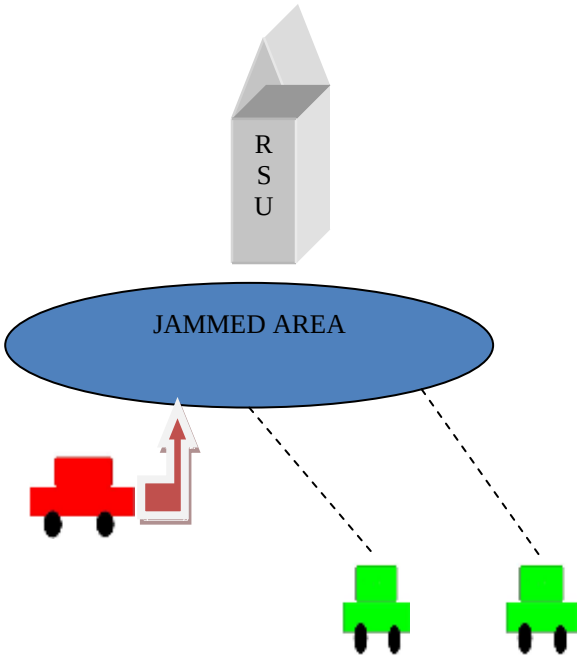

Fig. 4 Jam the channel in between vehicle-to-RSU

Possible Solution for this Attack is given below:

For the above problem author suggest [1] the solution, in which he assume that the jammer transmits only when valid radio activity is signaled from its radio hardware and the attacker jams the packet with *Pjam* probability. Using this strategy the attacker decreases its probability of detection. Thus, to differentiate this jamming scenario from legitimate scenarios, he has measured the dependence among the periods of error and correct reception times .In fact, the access to the channel of jammer is dependent of the access to the channel of active nodes. Thus, this dependence measure in jamming attack case is greater than in normal network activity. In order to measure this dependency, he has used the Correlation Coefficient which is a statistic measure of relation between two random variables. The simulation results of the model were quite promising.

$$cov(X, Y)/\sigma x \,.\, \sigma y$$

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 slots and 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 5.

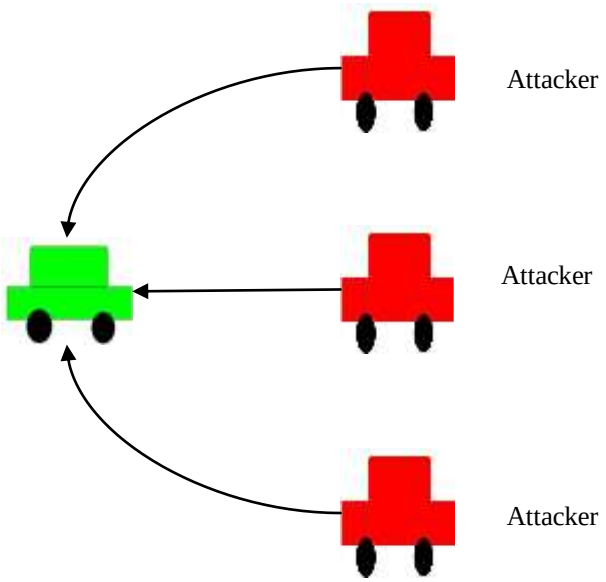

Fig. 5 DDOS in V-to-V communications

b) Case II: In this case, VANET infrastructure (RSU) is the target for attacker as shown in Figure 6. Attacker launches attack on the infrastructure from different locations, because of that when other nodes in the network want to access the network, the RSU is not able to respond them, thus it cause denial of service.

Possible Solution for this Attack is given below:

Author [8] addresses a security weakness of VANET where a group of malicious entities can launch a DDOS attack

exploiting the IEEE 802.11p's EDCA vulnerabilities based on small contention window, lack of acknowledgements in broadcast communications, and periodicity of service beacons. An attacker can easily synchronize to any periodic transmission in the network. He analyzed the prospect of launching such an attack, and also suggests different mitigating techniques including larger EDCA parameters for VANET entities. Such as randomizing the RSU schedule, increasing the Contention Window & Randomization with Increasing the Contention Window.

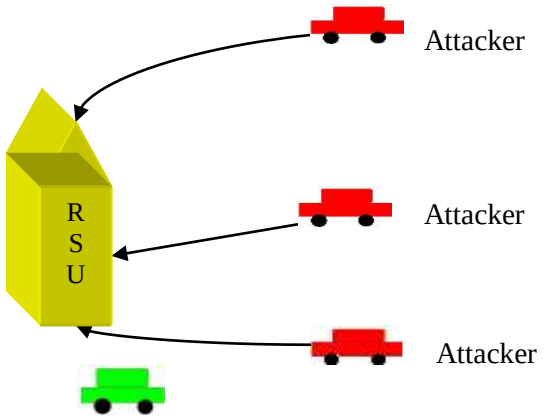

Fig. 6 DDOS in V to I communications

IV. PROPOSED APPROCH FOR SECURING NETWORK

In our proposed solution we use DSRC channels [5] & Revocation techniques [10]. As we know that, DSRC spectrum has seven channels which are used for sending different types of messages. In it, message is send or receives by their priorities [5]. There are four classes; Class1 and Class2 carry safety information whereas Class3 and Class4 carry commercial messages. Class1 has highest priority and second highest priority is given to Class2, Class3 & 4 has low priority. Proposed solution is that, any node in a network will receive limited number of security massages at given stamp of time. By this network will able to protect itself from DOS attack.

Now, consider any node 'A' who will receive message from another node if any safety massage is come, it will accept it, identify its IP address and start counting. Node 'A' will accept only 15 safety massages from same IP address in a time of 30 seconds. After this time node will again able to accept safety messages from the same IP. This 30 second time will starts when node 'A' receive first safety message from the IP address. If continuously safety messages are come from same IP address, OBU will report the RSU about it or if node is not in a range of RSU, it will send this report to its neighbor nodes by this, they will remove this attacker from the network. Thus our approach will protect vehicular network from denial of service attack.

V. *Conclusion*

The main goal of using VANET is to save the lives on the road. But if vehicle and roadside unit are not able to send or receive life critical information due to denial of service attack, VANET would be look as a useless technique. Therefore, protection from DOS attack is mandatory. We proposed a new technique by which network will be always available for the user. We expect that our approach will strongly opposes the DOS attack as well as DDOS attack. Because if node will stop accepting a garbage message from the attacker node, its processing resources will not be overwhelmed and always be available for other nodes. It can easily implemented in network without making a big change.

REFERENCES

[1] Ali Hamieh, Jalel Ben-Othman, Lynda Mokdad, "Detection of Radio Interference Attacks in VANET", IEEE "GLOBECOM" 2009

[2] J. Jakubiak, Y. Koucheryavy, "State of the Art and Research Challenges for VANETs", 5th IEEE Consumer Communications and Networking Conference, 10-12 Jan. 2008, pp. 912-916.

[3] Y. Qian, N. Moayeri, "Design of Secure and Application Oriented VANETs", IEEE Vehicular Technology Conference 2008, 11-14 May 2008, Singapore.

[4] I Aad, JP Hubaux, EW Knightly, "Impact of Denial of Service Attacks on Ad Hoc networks", Networking, IEEE/ACM Transactions on Volume 16, August, 2008.

[5] Yi Qian; Kejie Lu; Moayeri, N., "A Secure VANET MAC Protocol for DSRC applications," *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE* , vol., no., pp.1,5, Nov. 30 2008-Dec. 4 2008

[6] M Raya, P Papadimitratos, JP Hubaux, "Securing Vehicular Communications", IEEE Wireless Communications, Vol 13, October 2006.

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

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

[9] Sumra, I.A.; Ahmad, I.; Hasbullah, H.; bin Ab Manan, J.-L., "Classes of attacks in VANET," *Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International* , vol., no., pp.1,5, 24-26 April 2011

[10] 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

[11] GMT Abdalla, SM Senouci "Current Trends in Vehicular Ad Hoc Networks", Proceedings of UBIROADS workshop, 2007

[12] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks", Proc. of HotNets-IV, 2005.

[13] M Raya, J Pierre Hubaux," The security of VANETs", Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks, 2005.

[14] Security & Privacy for DSRC-based Automotive Collision Reporting.