Effects of DDoS Attacks on Inter-Vehicle Communication - A Survey

Gurjit Kaur[1], Ranjeet kaur Sandhu[2]
[1]M.Tech Student, Dept. of CSE, DAV University
[2]P.hD Research Scholar (CSE), PTU University
Punjab, India

Abstract *VANET is the special class of Mobile ad hoc networks (MANET). The main target of using VANET is to provide safeness or comfort for passengers and drivers on the road but now so many accidents occurs on the road due to attacks. If VANET cannot overcome the attacks and their network cannot provide correct information and safety to user then it would be unserviceable technology. In this review paper, we present various kind of attacks in VANET and also discussed DoS attack in network and presented with way in which they are occur in the communication medium and various detection method for network attacks are discuss.*

Keywords — *VANET, DoS, DDoS, Attacks in VANET, Protection Method.*

I. INTRODUCTION

VANET stands for vehicular ad hoc network. VANET have most attractive topic in recent years. It is special kind of mobile ad hoc network. In which, communication has been done in between vehicle to vehicle (V to V), Inter roadside communication, vehicle to roadside unit (V to RSU), in a range of 100 to 300 m as shown in figure 1. VANET are dynamic in nature and its topology is change very fast and frequently. In which, every node can move freely within the network and every node can communicate with other node. The aim of the VANET is to provide comfort to passengers and it is also used for life saving of passengers [10].

VANET has drawn boost concentration in recent years due to its broad range of application. VANET applications can be divided into two types. Safety application and non-safety applications. Application that increase vehicle or passenger's safety on the roads is called safety application. The example of safety applications are warning or instruction message to driver, road congestion etc. and the application that provide various services, such as entertainment, internet connectivity, peer to peer communication etc. are called the non-safety or user applications [16].

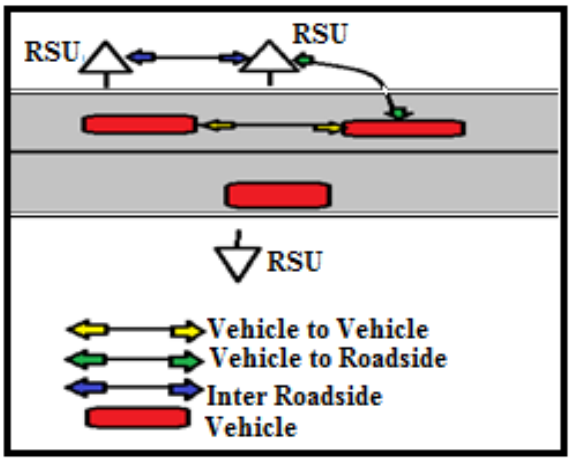


Fig. 1: Types of Communication in VANET

The pretension to secure the VANETS are the equal to the secure the other networks. The demand of secure the VANET is to protect the information by an unauthorized node and the information cannot be inserted or modified by an unauthorized person. The objective is to provide Authentication, Confidentiality, Integrity and Availability [10].

- **Authentication** is the process of verifying the identity of someone.
- **Confidentiality** is deals with the protection of data from unauthorized/malicious nodes. It ensures that information is not disclosed to unauthorized node.
- **Integrity** means information can be modified by authorized node only.
- **Availability** means that the network works properly and service should be available 24*7 [10].

II. ATTACKS IN VANETS

In this section, the different kinds of attacks in VANET are discussed. There are certain types of unauthorized messages are available in the VANET network. The following kinds of attacks are comes in the network.

Table No. 1:-Different Types of Attacks in VANET

Sr. No.	Types of Attack	Effects on network	Example
1.	Network attack	In this type, the attacker can directly attack on other vehicle or infrastructure. The main purpose of attacker is to create a problem for authorized users. This attack is very dangerous [15].	DoS, DDoS, Sybil attack etc.
2.	Application attack	In this type, the attacker may be outsider (intruder) or insider (authorized user). The attackers can be modify or change the correct message and send wrong or fake information to other vehicle for their own benefits [15].	Bogus information attack, GPS spoofing, hidden vehicle etc.
3.	Timing attack	In timing attack the attacker receive a message but they cannot forward this message. The attacker cannot modify the original message they added some timeslots in the message to create delay. The receive node may receive the message but the actual time constraint for receiving the information is over. So the information received by the node is not usefulness [3].	Timing attack
4.	Social attack	In this type of attack, attacker may create a problem in the network. so the authorized user confuse when they are receiving fake or wrong messages and these fake of wrong information change the behaviour of the users. Due to this various kind of accident are occurs [15].	Emotional and social attack
5.	Monitoring attack	In this type, Attacker is to monitor the overall network. The attacker plays a role like eavesdropper. In which, When two vehicles communicate with each other the attacker listen to their private conversation without their prior knowledge and the attacker gains access to the information and misuse it [15].	ID disclosure, Position attack

III. DENIAL OF SERVICE ATTACK (DOS) -A TYPE OF NETWORK ATTACK.

DoS is one of the most serious attacks in VANET network. An attempt to make service unavailable to its users is called denial of service (DoS) attack [1]. In which, attacker may send bogus messages to the channel thus reduce the productiveness of the network so network is not providing service to authorized users [3]. There are three ways to happen dos attacks.

First Class: Communication channel jamming: In this type, the attacker jams channel or other users cannot be enter in the network. This type of attacks are comes between the vehicle to vehicle (V-V) and vehicle to infrastructure (V-I) [11].

- ***Vehicle to Vehicle:*** In which, unauthorized node jams the channel by sends high frequency channel and create a domain. The nodes are present in the domain cannot communicate with each other when a node leaves the domain then they can communicate with each other [15].

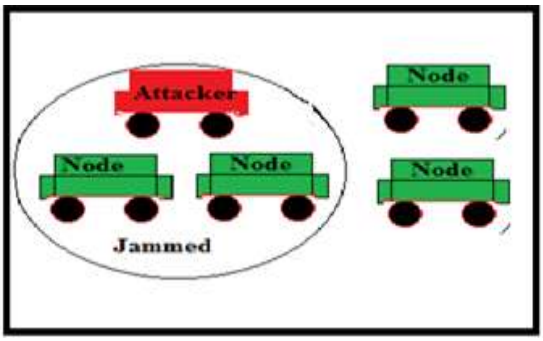


Fig. 2: Jamming between Vehicle to Vehicle

- ***Vehicle to Infrastructure*:** In which, unauthorized node jams the channel between the vehicle and the infrastructure by sending so many fake messages to infrastructure. The nodes lies between the infrastructures ranges cannot be communicate because the infrastructure can be busy to verify the preceding fake information [15].

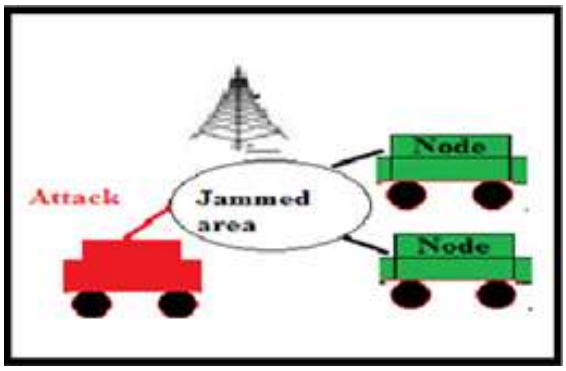


Fig. 3: Jamming between Vehicle to Infrastructure.

Second class: overloading of network resource: In this type, the attacker can overload the resources node such that resource node cannot perform task. In this type of attack all resource node become busy with overloaded message, due to this service is not available [11].

- ***Vehicle to Vehicle:*** A node behind the attacker and received various wrong messages which is send by

an attacker keeps the node busy. It will completely deny for accessing the network [15].

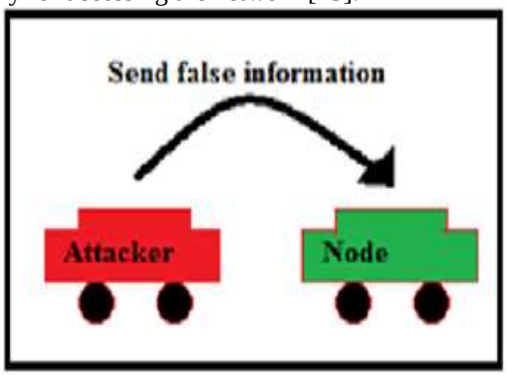
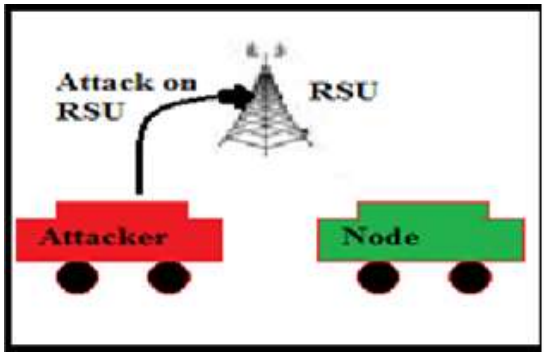


Fig. 4: DoS attack in Vehicle to Vehicle communication

- ***Vehicle to Infrastructure:*** In this class RSU is suffer from DoS attack and attacker directly attack on the RSU. So the RSU is busy to verify the attacker's messages. If any node wants to communicate, thus RSU is not providing service to



any other nodes. Due to this service is not available [15].

Fig. 5: DoS attack in Vehicle to Infrastructure Communication.

Third class: Distributed denial of service attack (DDoS):-In which attacker are placed at the different locations and the process of the attack is in distributed fashion. It is very dangerous attack in VANET [11].

- ***Vehicle to Vehicle:*** In this case the attacker is attack on victim node from different location and also sends messages in different timeslots. The purpose of the attacker is to make network unavailable for target node [15].

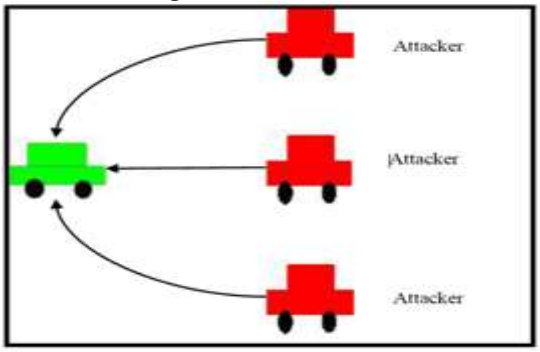


Fig6. DDoS: Attack in Vehicle to Vehicle communication

- ***Vehicle to Infrastructure:*** The target of the attacker is RSU. Attacker attack on the infrastructure from different locations. If any other node want to communicate with RSU the infrastructure is already overloaded thus the service is not available [15].

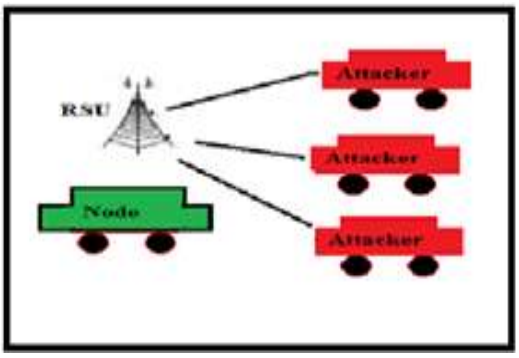


Fig. 7: DDoS attack in Vehicle to Infrastructure communication

We present three ways to occurs DoS attack in the network and also all the way of attacks can be further divided into two categories so we can discuss six types of attacks in communication. Due to this, service is no longer available to their authorized users.

IV. TECHNIQUES TO OVERCOME NETWORK ATTACKS IN VANETS.

In [1], Authors proposed a schemes for detecting the DoS attack by using bloom filter and traffic capacity method. Which provide security to the authorized node in VANETs. In this paper some techniques are used for detecting the DoS attack. 1) Bloom filter based detection scheme: It is used for provide safety against the IP spoofing of address in DoS attack. 2) Traffic capacity based DoS detection scheme. 3) IP-Chock (Filtering) Detection Algorithm: The algorithm is work on the three phases: Detection engine phase 1, Detection engine phase 2 and Bloom filter. The first phase is responsible for collecting data that is processed in the next phase. While second phase is only process the information that is collected by the phase 1. If phase 2 cannot found any malicious node then the information is stored in the database. The last phase is the active bloom filter with hash function. If any malicious node found by phase 2 then it generate an alarm and send a link to all other nodes.

In [2], Authors proposed a real time detection of DoS attacks. In this paper authors mainly concentrate on the jamming of periodic messages which are exchanged by vehicles in a platoon (a group of vehicles who are in network and communicate with each other). This paper is using

two techniques. 1) A simple real time detector method for detecting an attack. 2) Probabilities of attack detection and also estimate the false alarms for any jamming probabilities.

In [4], Authors proposed a technique to secure from DoS attacks. In VANETs so many type of attacks occur in the communication medium such as overload resource attack which can be overcome by using On Board Unit (OBU) technique. It is authentication method which allows the node to authenticate each other for vehicle to vehicle communication when there is insufficient security of infrastructure and also make decision as to block a DoS attacks. This technique will protect network from dos attack. In this paper, authors can also present various types of attacks and provide technique to secure the network from attacks.

In [5], Authors proposed a VIPER: a vehicle to infrastructure communication privacy enforcement protocol. It is used for deal with traffic analysis attack. The main aim of this protocol is to have vehicle does not send message directly to the RSU but RSU uses neighbor vehicle as intermediates. This protocol is also used for detecting three traffic analysis attacks: message coding attack, message volume attack and timing attack. The main purpose of this paper is to be providing secure communication between the vehicle and the infrastructure.

In [9], Authors proposed a registration method. According to this if user want to communicate with RSU in the first time, then vehicle should register with the nearby RSU. In the first time communication the user verified their identity to RSU. Authentication is in the form of username, password. If the verification is done then data is provided. If verification is not successful then the node is blocked by RSU. It should provide security to outside attacks.

In [8], Authors present an Intrusion Detection System (IDS), by applying genetic algorithm (GA) to efficiently detect various types of network intrusions. The intrusion means take action that compromise security resource and intrusion detection means protection strategy. The main purpose of this paper is to protect the network against the security attacks if intrusion is detected then the network would be safe and work properly. Therefore attacks can be controlled.

In [12], Authors proposed a cryptographic algorithm for distributed denial of service (DDoS) attack, defence against source IP address spoofing attacks. It can be identifying attack packets and dropping those attack packets. This algorithm can be give productive result against IP spoofing attack packet. In this paper, authors present a various previous proposed techniques for defending against DDoS attacks with source IP address spoofing. IP address spoofing is the way of introduce DDoS attack.

In [13], Authors present a technique called IPCHOCKREFERENCE for defence against UDP spoofed flooding traffic of denial of service (DoS) attacks in VANET. This method can be used storage efficient data structure and a bloom based IP-CHOCK detection method. This technique can be used for detecting abnormal traffic which is occurring due to flooding attacks. Authors can also involve two method i.e. random spoofing and non-parametric testing for classifying detected events. The network simulator result shows that this method gives an efficient and effective detection result with low cost.

In [14], Authors proposed a method based on cryptographic to detect Sybil attack in VANETs. This method can be use encryption mechanism to detects attack and involve four security phase such as authentication, non-repudiation, privacy and data integrity. The evaluation on network simulator can show that the execution time of this algorithm is low because most operations are done in certification authority.

Table No.2:- Summary of Detection Methods for Network attacks in VANETs.

Sr. no.	Technique	Procedure
1.	• Bloom filter based detection scheme. • Traffic capacity based DOS detection scheme. • IP-Chock (Filtering) Detection Algorithm [1].	Provide safety against the IP spoofing of address in DOS attack
2.	Real time detection of DOS attacks [2].	Focus on jamming of periodic message
3.	On Board Unit (OBU) technique [4].	This technique will protect network from DoS attack
4.	VIPER: vehicle to infrastructure communication privacy enforcement protocol [5].	Deal with traffic analysis attack and provide secure communication between V2I.
5.	Registration Method [9].	Provide security against the outside attacks
6.	Genetic Algorithm [8].	Detect the attacks like intrusion detections.
7.	Cryptographic Algorithm [12].	Defense against source IP address spoofing attacks in DDoS attack
8.	IPCHOCKREFERENCE [13].	Defense against UDP spoofed flooding traffic of DoS attack in VANET
9.	Encryption Method [14].	Using cryptographic method deal with Sybil attack. This method can be used four security phase.

V. CONCLUSION

Security in VANET is used for enhance road safety and save the lives on the road. If vehicle and RSU cannot receive correct information due to any type of attacks the VANET network is not secure. So detection of attacks especially DoS is very important for securing network. There are various type of method has been used for protecting the network to the DoS as well as DDoS attack. In this paper, we present various types of attacks and explain the DDoS attack. At last we present various methods to provide protection from attack and secure the network.

ACKNOWLEDGMENTS

The authors are grateful to those people who are gives farsighted opinions on the previous version of this document and for his/her recommendations related to this survey.

REFERENCES

[1] karan verma and Halabi hasbullah, "IP-CHOCK (filter) Based Detection scheme for Denial of service (DoS) attacks in VANET", In engineering and computer sciences ,vol. 8, issue 5, pp. 864-868, IEEE 2014.

[2] Nikita lyamin, Alexey vinel, Mognusjonsson and Jonathan loo, "Real-Time detection of denial of service attacks in IEEE 802.11p vehicular network" IEEE Communications Letters, vol. 18, no.1, pp.110-113, jan. 2014.

[3] VinhHoa La and Ana CAVALLI, "Security Attacks and solution in vehicular ad hoc network: A survey" International Journal on Ad hoc Networking system (IJANS). vol.4, No.2, 2014.

[4] Adityasinha, prof santosh k. Mishra, "Preventing VANET from DoS & DDoS Attack" International journal of engineering trends and technology. vol. 4, pp. 4373-4376, 2013

[5] P. Cencioni and Robert di Pietro, "A mechanism to enforce privacy in vehicle to infrastructure communication", Computer communication, pp. 2790–2802, 2008.

[6] Adil Mudasir Malla, Ravi Kant Sahu, "Security Attacks with an Effective Solution for DoS Attacks in VANET" International Journal of Computer Applications, Volume 1, Issue 2, ISSN: 2349-6002, 2013.

[7] Vikash Porwal, Rajeev Patel, and R.K.Kapoor, "Review of Internal Security Attacks in Vehicular Ad-hoc Networks (VANETs)" International Journal of Engineering Research & Technology, Vol. 3, Issue 8, 2014.

[8] Mohammad Sazzadul Hoque , Md. Abdul Mukit and Md. Abu Naser Bikas, "An Implementation Of Intrusion Detection System using Genetic Algorithm" International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.

[9] Shah Shruti k, "Secure and efficient data acquisition in service oriented VANET" International Journal of Engineering Development and Research, vol-2, issue 2, pp.1966-1970, 2014.

[10] Maria Elsa Mathew, Arun rai kumar "Threat Analysis and Defence Mechanisms in VANET" International Journal of Advanced Research in Computer Scienece and Software Engineering, vol. 3, issue 1, January 2013 .

[11] Halabi Hasbullah, 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 ,Vol. 4, No. 5, 2010.

[12] Archana S. Pimpalkar, Prof. A. R. Bhagat Patil " DDoS Attack Defense against Source IP Address Spoofing Attacks" International Journal of Science and Research (IJSR) , Vol. 4 , Issue 3, March 2015.

[13] Karan Verma, Halabi Hasbullah , Ashok Kumar , "An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VANET" International Advance Computing Conference(IACC)IEEE , 2013.

[14] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection of Sybil Attack Based on Cryptography in VANET," International Journal of Science and Research (IJNSA), Vol.3, No.6, November 2011.

[15] Irshad Ahmed Sumra,Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan , "Classes of Attacks in VANET" Conference: Electronics, Communications and Photonics Conference (SIECPC), 2011 .

[16] Vishal Kumar, Shailendra Mishra,Narottam Chand, " Applications of VANETs: Present & Future" Scientific Research : Communication and Network ,2013