# Overview of Various Attacks in VANET

Ujwal Parmar, Sharanjit Singh- Astt.Prof. M.tech (CSE)

Student - M.tech (CSE)  Guru Nanak Dev University RC Gurdaspur, India. 9256649894

ujwalparmar92@gmail.com

**Abstract**— VANET stands for Vehicular Ad-hoc Network. It is the sub category of MANET(Mobile Ad-hoc Network). It serves a critical infrastructure for road safety and traffic efficiency. It is an emerging technology to achieve intelligent inter vehicle communication that results in improved road safety and essential alerts.[1] Vehicular Ad hoc Network (VANET) serves user with safety and non safety applications but needs security to implement the wireless environment In VANET vehicles does not have fixed infrastructure because of the reasons that vehicles are nodes with mobility. It serves safe and non safe wireless applications due to which security is most important concern in VANET. In this paper we will present comprehensive study of various attacks in VANET and comparison of various attacks in VANET. "[1],[3]"

**Keywords**— Denial of Service Attacks, On-Board Units, Security Attacks, VANET, Sybill Attack, Integrity, Privacy.

## INTRODUCTION

In today's world transportation plays important role in our daily lives. From last few years transportation system that has come into era is VANET. It stands for vehicular Ad- hoc Network. A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network.[1] In VANET every participating car act as a wireless router that allows cars approximately 100 to 300 meters each other to connect in turn which creates a network with wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created."[2],[3]" It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. Automotive companies like General Motors, Toyota, Nissan, DaimlerChrysler, BMW and Ford promote this term.

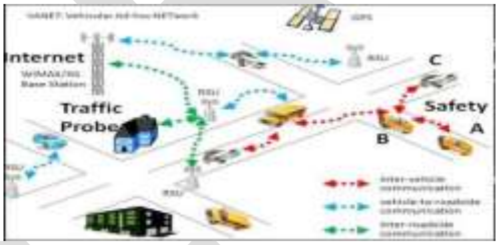

**Fig 1- VANET Structure**

In VANET each node act as a vehicle or  roadside unit which can move freely within the network range and stay connected. The communication is in single hop or multi hop between the nodes. It constitutes of short range radio that is installed inside vehicles and roadside units (RSUs) and central authorities which are responsible of identity registration and management. The security in VANET is most critical issue because the information is propagated in open access environment. VANET's  are exposed to various threats and attacks. It is necessary that all the data which is transmitted should not be changed by the attackers. Attacker may be the authenticated user of the network that has detail knowledge of the network that can be used for understanding the design and configuration of the network. The possible attacks that can occur in[5] the VANET are broadly categorized into three main groups firstly those that pose a threat to availability. Secondly those that pose a threat to authenticity. At last those that pose threat to driver confidentiality and miscellaneous.

## 2. VANET Characteristics

Though VANET is similar to ad hoc networks but it posses unique network characteristics which are as follows:[3]

(i) High Mobility
(ii) Rapidly changing network topology
(iii) Unbounded network size
(iv) Frequent exchange of information
(v) Wireless Communication

(vi) Time Critical
(vii) Sufficient Energy
(viii) Better Physical Protection.

## 3. Properties of Attacker

Attacker possess various properties which are mentioned below:

- **Insider:** This type of attacker is an authentic user of the network and have detail knowledge of the network. If the attacker is a member node who can communicate with other members of the network, it will be known as an Insider and able to attack in various ways.

- **Outsider:** The outsider attacker is a kind of intruder which aims to misuse the protocols of the network and range of such attacks are limited which means less variety of attacks.

- **Coverage Area:** When any kind of attack is being launched coverage area act as a main property of the attacker. It depends on the nature of the attacker it can cover the main area of the road. "[1],[4]"

- **Technical Expertise:** It is the most powerful property of the attacker that makes attacker more stronger for creating attacks in the network.

- **Resources:** The three main characteristics on which attacker depends to achieve their goal are budget manpower and tools.

## 4. Types Of Attacks

VANET suffer from various attacks; which are discussed in the following subsections.

**4.1 Denial of Service Attack:** It is the most serious level attack in vehicular network. In this attack attacker jams the main communication medium and network is no more available to legitimate user."[4],[5]"

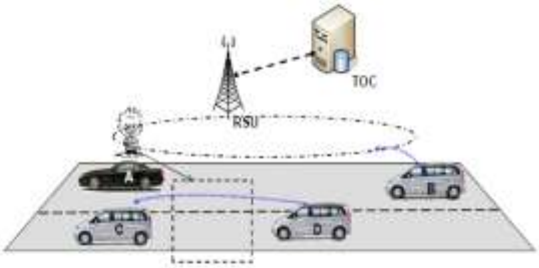

**Fig. 2- Denial of Service Attack between V2V and V21**

Fig. 2 shows the whole scenario when the attacker A launches DOS attack in vehicular network as a result it Jams the whole communication medium between V2V and V2I and the authentic users (B, C, and D) cannot communicate with each other.

**4.2 Distributed Denial of Service Attack (DDOS Attack):** DDOS attacks are those attacks in which attacker attacks in distributed manner from different locations. Attacker may use different timeslots for sending the messages. Nature and time slot of the message can be varied from vehicle to vehicle of the attackers. The aim of attacker is same as DOS attack. "[5],[7]"

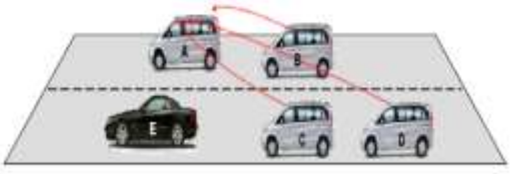

**Fig. 3- DDOS Attack in vehicle to vehicle communication**

Fig. 3 explains the vehicle to vehicle (V2V) DDOS attack scenario in which attackers (B,C,D) launches DDOS on vehicle A.

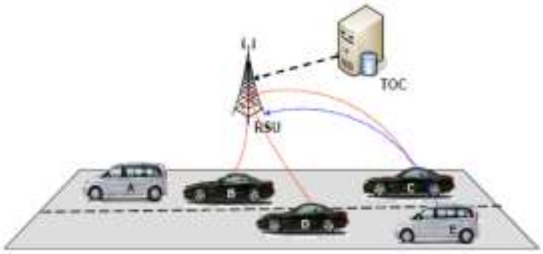

**Fig. 4- DDOS Attack in vehicle to Infrastructure communication**

Fig4 explains DDOS attack in vehicle to infrastructure communication. Here B,C,D are the attackers which attacks the infrastructure from different locations.
Whereas other vehicles (A,E) in the network want to access the network then the infrastructure is overloaded.

**4.3 Sybil Attack:** It is a critical attack. In this kind of attack attacker sends multiple messages to other vehicles. Each message contains different source identity. It creates confusion to other vehicles by sending wrong messages like traffic jam. So there is jam further and vehicles are forced to take another route."[7],[9]" The main aim of the attacker is to provide an illusion of multiple vehicles to other vehicles so that vehicles can choose another route.

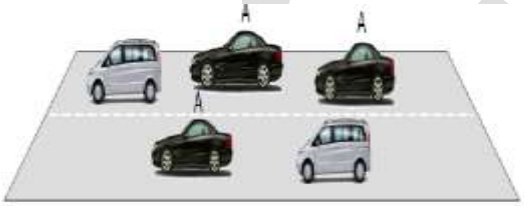

**Fig. 5- Sybil Attack**

**4.4 Node Impersonation Attack:** In vehicular network each vehicle has unique identifier which is used to verify the messages whenever the accident occurs by sending the wrong messages to other vehicles.

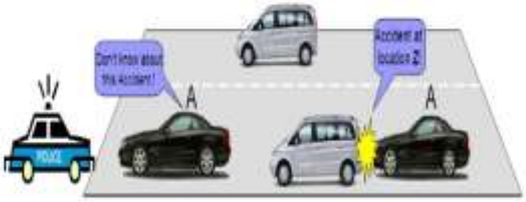

**Fig. 6- Node Impersonation Attack**

Figure 6 shows node impersonation attack scenario in which vehicle A is involved in the accident at location Z. When police identify the driver as it is associated with driver's identity, attacker changes his/her identity and simply refuses it.[8].

**4.6 Application Attack:** The main motive of attacker in this kind of attacker in this kind of attack is to content that are related to safety and non safety related applications. Safety applications play very important role as they provide warning messages to other users. In this attack the attackers alter the contents of the actual message and send wrong messages to other users."[11],[12]"

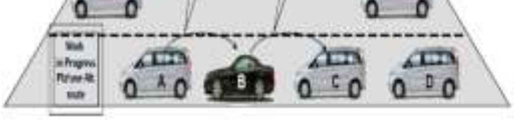

**Fig. 7- Application Safety Attack**

Figure 7 shows the example in which attacker B attacks on safety application. Attacker B receives one warning message “Work Zone Warning” from nearby vehicle. During attack he changes the content of the message and sends this message “Road is Clear” to other vehicle C.

**4.7 Non Safety Application Attack:** Non safety are related to users comfort during the journey. These do not disturbs the safety applications. The main role of non safety applications is to give comfort to passengers and to improve traffic system. One of the major non safety application is car parking

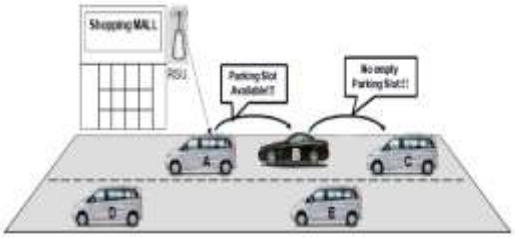

**Fig. 8 - Non safety Application Attack**

In the above figure Vehicle A is authentic user which receives information "Parking Slot Available" from road side unit near shopping mall. So he sends the message to other vehicle B. The vehicle B is the actual attacker who receives the message. Now vehicle B alters this message "Parking slot available to "No Empty Parking Slot" and passes this message to other vehicle C."[8],[9]"

**4.8 Timing Attack:** The main objective of attacker is to add some time slot in the original message that creates delay in the original message and these messages are received after these requires a time. AS we know safety applications are time critical applications if delay occurs in these applications then major objective of these applications is also finished.

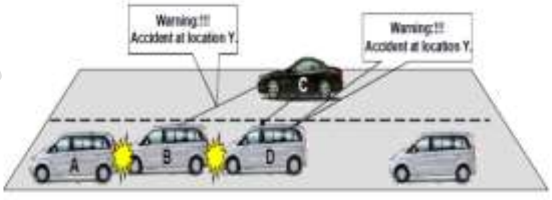

**Fig. 9- Timing Attack**

Fig.9 shows the complete scenario of the timing attack in which vehicle C is attacker which receives warning message from other vehicle B and then pass this message to other vehicle D by adding some time. Whenever the other D receives this message then accident actually occurs.

## 5. VANET Security Requirements: **The main three security requirements for VANET are as follows:**

1.**Confidentiality:** In VANET's the term confidentiality refers to the confidential communication. In a group no one except the group members are able to decrypt the messages that are broadcasted to every member of the group.

**2. Integrity:** This term refers that the data or information among nodes are not altered by attackers.[10]

**3. Availability:** It means network should be available to the users even if it is attacked by the attacker.

**4. Privacy: We consider privacy in following two cases:**
**1. Communication between vehicles and RSUs:** In this case privacy means that that an eavesdropper is impossible to decide whether two different messages come from the same vehicle.

**2. Communication between Vehicles:** In this case privacy means that determining whether message whether two different valid messages coming from the same vehicle is kind of burden for everyone except a legitimate vehicle.[10]

**6. Related Work:** In 2013, Adil Mudasir Malla, Ravi kant Sahu published paper on Security attacks with an efficient solution for DOS attack in VANET."[4],[5]" They discussed various types of attacks in their paper and security attack classification of irshad et al in more proper manner known by name Security Attack Pyramid in VANET. In 2014, Vinh Hoa LA, Ana Cavalli published paper on

Security attacks and solutions in vehicular Ad hoc networks: A survey. They discussed various types of attacks. They also presented main security requirements like confidentiality, integrity, availability, privacy. they proposed various attacks counter measures like sybill attack, Man in the middle attack, illusion attack. They also proposed Global Positioning spoofing, Hidden and Tunnel Attack. In 2011, Irshad Ahmed Sumra,Iftikhar Ahmad, Halabi Hasbullah , Jamalul-lail bin Ab Manan published paper on clases of attcaks on VANET. "[10],[11]"They discussed various classes of attacks of VANET. They explained attacks process mechanism. They also proposed solution that provides information about the attack whenever the attacker launches it. They presented a flowchart which shows process to identify attacks with respect to attack classes.[12] They also discussed attack classes with different time slots. In 2012, Ajay Rawat , Santosh Sharma and Rama sushil published paper on VANET security attacks and its popular solutions. He proposed various security attacks and their possible solutions. He also discussed the solution for DOS attack which is based on the use of OBU (On Board Unit)that is installed in vehicles."[12], [13] In case of DOS attack the processing unit will suggest to the OBU to switch channel, technology, or touse frequency hopping technique or multiple transceiver. He also proposed two solutions to prevent sybill attack, first is using a globally synchronized time for all nodes and other is using nonce. Another solution is to mitigate this attack is to verify the received data in correlation with the data received from other sources.

## 8. ACKNOWLEDGEMENT

We would like to thank Dr. Sandeep Sood and Mr. sharanjit singh Astt. Prof Mtech (CSE) for their guidance towards the work.

## 7. CONCLUSION

Vehicular Networks have received great attention in last few decades. These networks are mainly used for improving efficiency and safety of the transportation. As we know that wireless medium is used in VANET for transmission of data or information from vehicle to vehicle so there are chances of various attacks in VANET. This paper includes various attacks in VANET. It also includes various properties of attacker, what are the security requirements which are required for the safety of the VANET. As we know that users want safety and security on the road in future and it may be possible by implementing secure and safe VANET network for users. [11], [12], [13].

## REFERENCES:

**[1]** Usha Devi Gandhi and R.y'S.M Keerthana " Request Response Detection Algorithm for Detecting DoS Attack in VANET" in International Conference on Reliability, Optimization and Information Technology 2013.

[2] Irshad Ahmed Sumra,Iftikhar Ahmad, Halabi Hasbullah, Jamalul-lail bin Ab Manan "Classes of Attacks in VANET" in Advanced Information Security Cluster MIMOS Berhad in 2012.

[3] Megha Nema, Prof. Shalini Stalin2 and Prof. Vijay Lokhande " Analysis of Attacks and Challenges in VANET" in International Journal of Emerging Technology and Advanced Engineering , Volume 4, Issue 7, July 2014.

[4] Jose Maria de Fuentes, Ana Isabel Gonzalez-Tablas, ArturoRibagorda, "Overview of security issues in Vehicular Ad-hocNetworks", Handbook of Research on Mobility and Computing 2010.

[5] Karan Verma, Halabi Hasbullah, Ashok Kumar „An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacksin VANET‟ 2012 IEEE Deptt. of Computer & Information Sciences Universiti Teknologi PETRONAS, Malaysia.

[6] Y.Qian, N.Moayeri,"Design of Secure and Application oriented Vanets"Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE,11-14 May 2008, Singapore.
[7] D.Jiang,V.Taliwal, A.Meier, W.Holfelder and R.Herrtwich,"Design of 5.9GHz DSRC based vehicular safety communication", IEEE Wireless
Communication Magazine, Vol 13, No.05 Nov
2006.

[8] T.Leinmuller, E. Schoch, F. Kargl, C. Maihofer, "Improved security in Geographic ad hoc routing through autonomous Position Verification", ULM University.

[9] M. Raya, P. Papadimitratos, J.P. Hubaux," Secure vehicular communications",IEEE Wireless Communication Magazine,specail issue on inter-vehicular communication, Oct 2006.

[9] M. Raya, J. Pierre, Hubaux,"Securing vehicular ad hoc Networks" Journal of Computer Security,vol.15, january 2007.

[10] Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky, and Bertrand Ducourthial, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET," International Journal of Network Security, Vol.9, No.1, PP.22- 33, July 2009.

[11] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection of Sybil Attack Based on Cryptography in VANET," IJNSA, Vol.3, No.6, November 2011.

[12] Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): stastus results and challenges", springer science+ Business Media, LLC 2011.

[13] A. Khalili, J. Katz, and W. Arbaugh, (2003)"Toward secure key distribution in truly ad-hoc networks". IEEEWorkshop 2003 International Symposium on Applications and the Internet, Orlando, FL, January