IJCAT - International Journal of Computing and Technology, Volume 3, Issue 5, May 2016
ISSN : 2348 - 6090
www.IJCAT.org

A Review on Various Attacks in VANET

[1] Manpreet kaur , [2] Nitin Bhagat

[1,2] Department of CSE
Sri Sai College of Engg. & Technology, Manawala
Amritsar, Punjab, India

Abstract - Vehicular Ad-Hoc network or VANET is a subgroup of mobile Ad-Hoc network or MANET. VANET does not have fixed topology and the nodes move one location to another location. It is used for life saving of passengers. To transfer a packet from client to server it should follow a routing protocol. Many challenges and security attack are in VANET like DOS attack, DDOS attack, Sybil attack, Grayhole attack. So in this paper we discuss about different types of attack in VANET.

Keywords **- VANET, DOS, DDOS, Sybil, Greyhole, Blackhole, Wormhole.**

1. Introduction

VANET is basically a form of MANET. VANET is a mix of sensor networks and ad hoc networks. They use wireless channel, Satellite channel and transmission for communication. In VANET, vehicles act as nodes which can be exchange data between each other. VANET is mainly aimed at providing safety related information and traffic management [1][2]. The various types of communication in VANET are of following.

- Vehicle – to – Vehicle
- Vehicle – to – Infrastructure
- Inter roadside communication

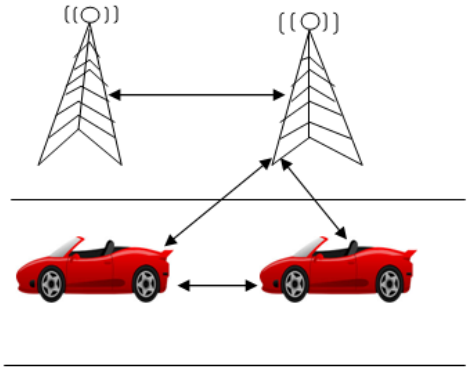

Fig.1 Vanets

2. Various Attacks

VANET suffer from various attacks; these attacks are discussed in the following subsections:

2.1 Denial of Service (DOS)

It is the most serious level attack in vehicular network. This type of attack is very simple but it's very harmful. It can prevent important information from arriving. In this attack its use other identity and block the services of other or it can stop also VANET communication service. These attacks done by attackers taking control of others and stop the communication services or jam the channel in network. This attack is very harmful to the drivers which are not communicating and also get false information [1][4].

2.2 Distributed Denial of Service Attack (DDOS Attack)

DDOS attacks are number of attackers in the network. That attacks from different location with different timing slots. It is dangerous than the DOS attack because these is only one attacker which can be easily find But in DDOS attack there are number of attacker in the network [4].

Case I: V2V communication:-

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 aim of attacks is to achieve network unavailability by bringing the network down at a target node.

for example There are three attackers nodes (blue color car) send some messages to a target node in front (yellow color car). After some time the target node cannot communication with any other nodes in the network [7].

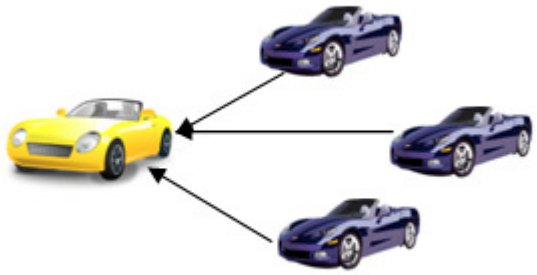

Fig.2 DDOS Attack in V to V communication

Case II: V2I communication:- In this case, the target of attack in the VANET infrastructure (RSU). There are three attackers in the network and lunch attack on the infrastructure from different location. When other nodes in the network want to access the network, the infrastructure is overloaded [7].

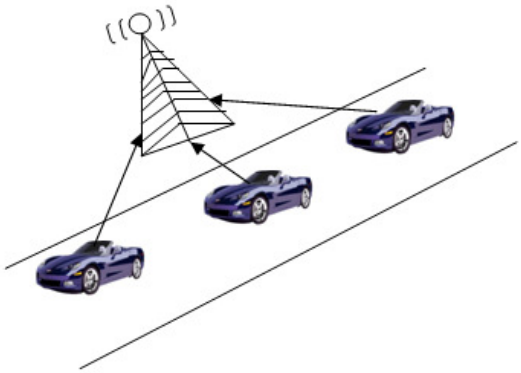

Fig.3 DDOS Attack in V to V communication

2.3 Sybil Attack

It is a critical attack. In this 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. This attack is very dangerous because a one node can give its various locations at the same time [4][6].

2.4 Black Hole Attack

Black hole attack is type of routing attack and can bring harm to whole network. When some malicious user enter into the network and stop forwarding messages to next nodes by dropping messages are called as black node [6].

2.5 Grey Hole Attack

Grey hole attack is the kind of denial of service attack. In this attack, the router which is mesh behave just not well and a subset of packets are forward and handle by receiver but leave by others [10].

2.6 Wormhole Attack

In wireless networking, the wormhole attack consists in tunneling packets between two remote nodes. In VANETs, an attacker that controls at least two entities remote from each other and a high speed communication link between them can tunnel packets broadcasted in one location to another location [9].

3. Conclusion

This paper concludes that many researchers provide their methodologies to solve this savior attack but still this is one of the major prone in VANETs, because this attack may also be the reason of other attacks like denial of service attack, distributed denial of service, Sybil attack, grey hole attack, black hole attack a name of few. 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 [4][6].

References

[1] Jaydip P. Kateshiya, Anup Prakash Singh "Review To Detect and Isolate Malicious Vehicle in VANET" International Journal of Innovative Research in Science, Engineering and Technology Vol. 4, Issue 2, February 2015.

[2] Divya Chadha, Reena "Vehicular Ad hoc Network (VANETs): A Review" International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 3, March 2015.

[3] Senthil Ganesh N. Ranjani S. "Security Threats on Vehicular Ad Hoc Networks (VANET): A Review Paper" International Journal of Electronics Communication and Computer Engineering Volume 4, Issue 6 2013.

[4] Ujwal Parmar, Sharanjit Singh "Overview of Various Attacks in VANET" International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015.

[5] Komal B. Sahare, DR. L.G.Malik. "Review - Technique for Detection of Attack in VANET" International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 2, February 2014.

[6] Priyanka Soni Abhilash Sharma "A Review of Impact of Sybil Attack in VANET's" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 5, May 2015.

[7] Varsha Raghuwanshi, Simmi Jain "Denial of Service Attack in VANET: A Survey" International Journal of Engineering Trends and Technology Volume 28, Number 1, October 2015.

[8] Harbir Kaur, Sanjay Batish & Arvind Kakaria " An Approach To Detect The Wormhole Attack In Vehicular Ad hoc Networks" International Journal of Smart Sensors and Ad Hoc Networks Volume 1, Issue 4, 2012.

[9] Er.Jagjit Singh, Er.Neha Sharma. "Wormhole Attack Detection by using Intrusion Detection System in VANET" International Journal of Computer Networks and Wireless Communications Vol 2, No 5, October 2012.

[10] Rupinder Kaur and Parminder Singh. "REVIEW OF BLACK HOLE AND GREYHOLE ATTACK" International Journal of Multimedia & Its Applications Vol 6, No 6, December 2014.

Author Profile:

Manpreet kaur is currently in the final year of degree course of Master's of engineering and technology from Sri Sai College of Engineering and Technology, Manawala, , Amritsar under I.K. Gujral Punjab Technical University, Jalandhar

Prof. Nitin Bhagat the guide and assistant professor in Sri Sai College of Engineering and Technology, Manawala Amritsar under I.K. Gujral Punjab Technical University, Jalandhar