International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-4, Issue-3, March 2016

Location Information Control Base Model for Secure Transmission in VANET

Manpreet kaur, Er.Nitin Bhagat

***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 Sybil attack prevention technique LICMB [1][2].**

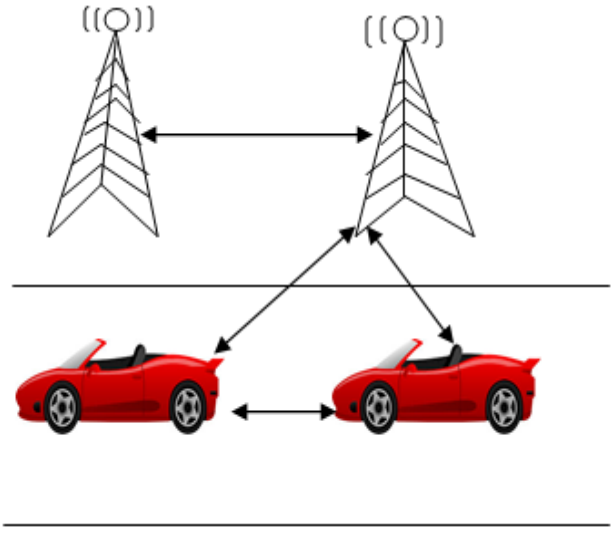
***Index Terms*— VANET, DOS, DDOS, Sybil, Greyhole, Blackhole, Wormhole.**

I. 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



VARIOUS ATTACKS

Manpreet kaur, Student (M.Tech), Department of CSE, Sri Sai College of Engg. & Technology, Manawala, Amritsar, Punjab, India.

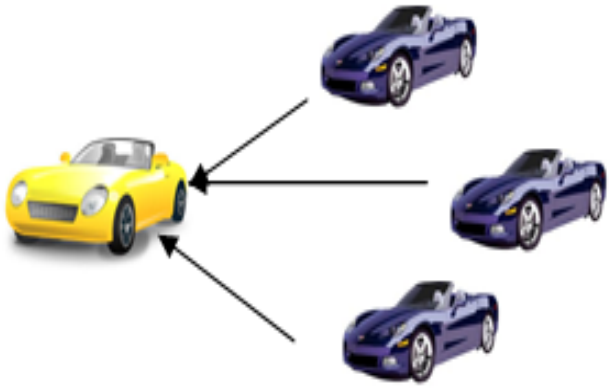
Er.Nitin Bhagat, Assistant Professor, Department of CSE, Sri Sai College of Engg. & Technology, Manawala, Amritsar, Punjab, India .

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

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].

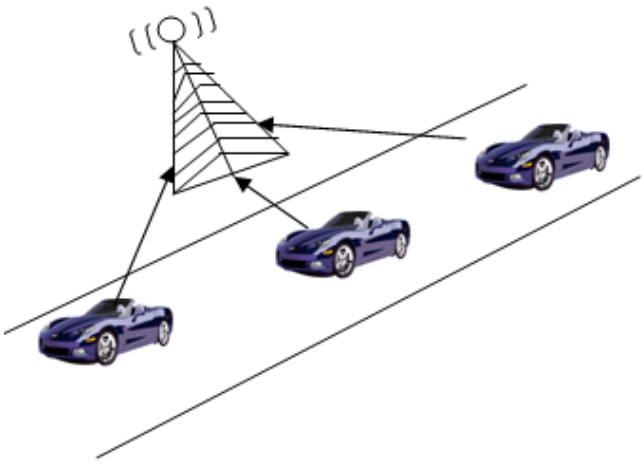
Distributed Denial of Service Attack (DDOS Attack): DDOS attacks are number of attackers in the network. That attacks from different location with different timing slots. It is dangerous than the DOS attack because these is only one attacker which can be easily find But in DDOS attack there are number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



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].



Attack in V to V communication

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].

II. Related work

Priyanka Soni et al. [6] VANET is a vehicular ad hoc network. This is a part of mobile ad hoc network. VANETs also called as intelligent transportation system (ITS) in which vehicles communicate to provide timely information. Their aim is to provide security, information and management of network. Instead of their many advantages vehicular network is prone to various attacks. Like prankster attack, denial of service attack, blackhole attack, alteration attack, fabrication attack, man in the middle attack, timing attack, illusion attack etc. In this we will use GPSR protocol to remove the Sybil attack. In GPSR protocol physical measurement of vehicle can be verified at any time and GPS coordinates will be compared. If GPS coordinate matched then there is no attack Abhilash Sharma et al. [7] Vehicular Ad hoc Networks (VANETs) have emerged recently as one of the most attractive topics for researchers and automotive industries due to their tremendous potential to improve traffic safety, efficiency and other added services. However, VANETs are themselves vulnerable against attacks that can directly lead to the corruption of networks and then possibly provoke big losses of time, money, and even lives. This paper presents a survey of VANETs attacks and solutions in carefully considering other similar works as well as updating new attacks and categorizing them into different classes.

Soyoung Park et al. [8] In this paper, we propose a timestamp series approach to defend against Sybil attack in a vehicular ad hoc network (VANET) based on roadside unit support. The proposed approach targets the initial deployment stage of VANET when basic roadside unit (RSU) support infrastructure is available and a small fraction of vehicles have network communication capability. Unlike previously proposed schemes that require a dedicated vehicular public key infrastructure to certify individual vehicles, in our approach RSUs are the only components issuing the certificates. Due to the differences of moving dynamics among vehicles, it is rare to have two vehicles passing by multiple RSUs at exactly the same time. By exploiting this spatial and temporal correlation between vehicles and RSUs, two messages will be treated as Sybil attack issued by one vehicle if they have the similar timestamp series issued by RSUs. The timestamp series approach needs neither vehicular-based public-key infrastructure nor Internet accessible RSUs, which makes it an economical solution suitable for the initial stage of VANET.

III. Proposed Algorithm

The proposed algorithm is for secure data transmission in a vnet

Step 1: Generate Network scenario using NS2

Step 2**:** Start with some initial elements like ‘no of nodes’, ‘neighbor node’, ‘Malicious node.

Step 3: Initialize with n no. of nodes.

Step 4: Implement LICBM technique.

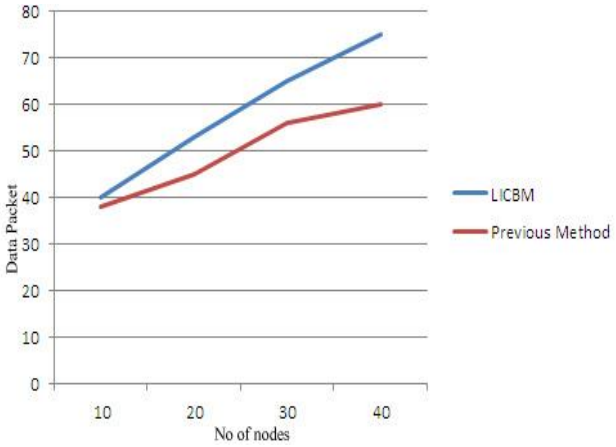
Step 5: initially Start LICBM algorithm for finding location and direction of nodes

Step 6: In LICBM finds the location for node is not changing and but is showing fake identity on various location without changing it position the technique will blacklist the and it will isolate the node

Step 7: Then finally With LICBM Algorithm secure transmission will be formed.

Step 8: This process continuation until the efficient and secure transmission is formed.

IV. Result and analysis



The result show proposed LICBM data transmission has better result than previous method

V. CONCLUSION

This paper concludes that many researchers provide their methodologies to solve sybil 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]5 A. Senthil Kumar S.Velmurugan. "ASecure distributed data discovery and dissemination in wireless sensor network Volume 5, july 2015.

[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]Priyanka Soni, Abhilash Sharma "Sybil Node Detection and Prevention Approach on Physical Location in VANET Volume 128, Number 1, October 2015.

[8]Soyoung Park, Baber Aslam, Damla Turgut,. "Defence against sybil attack in vehicular ad-hoc network based on road side unit Multimedia & Its Applications