Wormhole Attack Detection by using Intrusion Detection System in VANET

Er.Jagjit Singh
Student of Department (ECE), Amritsar College of Engineering & Technology
ACET, PTU, Kapurthala Punjab, Jallandhar, 144001, India
jagjitsingh_sandhu@yahoo.com

Er. Neha Sharma
Asst.Professor in ECE Department, Amritsar College of Engineering & Technology
ACET, PTU, Kapurthala Punjab, Jallandhar, 144001, India
er.neha.ruchi@gmail.com

***Abstract*: The use of self-driving vehicles is becoming more and more significant in last few years. The fact that the vehicles are self-driving can lead to greater difficulties in identifying failure and anomalous states, since the operator cannot rely on its own body perceptions to identify failures. VANET turns every participating vehicle into wireless sensor nodes and which allowing vehicles to communicate with each other, create a network with wide range. VANET is no centralized infrastructure due to which it is vulnerable to various security attacks. One of such of them most dangerous attack is wormhole attack which mainly occurs least two or more malicious nodes In this paper we mainly dicuss intrusion detection system to detect wormhole attack by evaluating the decision packet at destination node.**

Keywords— VANET, Inter-Vehicle Communication (IVC)

I. INTRODUCTION

Vehicular Network (VANET) is a form of Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as roadside equipment. It is a cornerstone of the envisioned Intelligent Transportation Systems (ITS). By enabling vehicles to communicate with each other via Inter-Vehicle Communication (IVC) as well as with roadside base stations via Roadside-to-Vehicle Communication (RVC), vehicular networks will contribute to safer and more efficient roads by providing timely information to drivers and concerned authorities. The interesting research area of Vehicular Networks is where ad hoc networks can be brought to their full potential. Both modern high-speed motorways and vehicles that drive upon them are becoming increasingly intelligent. In particular, communication devices are being installed in more and more cars and roadside infrastructure components. In the not-too-distant future, traveling Vehicles will be able to communicate while forming ephemeral, rapidly changing ad hoc networks. At the same time, they will have direct access to a fixed roadside network infrastructure with information flowing both ways. This network environment motivates the need for an infrastructure that will provide drivers with access to a variety of vital vehicular and roadside information. The resulting enhanced situational awareness has the potential to not only facilitate the decision making tasks of the drivers (e.g., trip planning based on traffic congestion on the road), but also to improve highway safety (by bringing information about catastrophic events and road conditions to the driver's attention) .The main goal of VANET is providing safety and comfort for passengers. To this end a special electronic device will be placed inside each vehicle which will provide Ad-Hoc Network connectivity for the passengers. This network tends to operate without any infra-structure or legacy client and server communication. Each vehicle equipped with VANET device will be a node in the Ad-Hoc network and can receive and relay others messages through the wireless network. Collision warning, road sign alarms and in-place traffic view will give the driver essential tools to decide the best path along the way.

II.TECHNOLOGY USED IN VEHICULAR NETWORK.

1) In VANET or Intelligent vehicular Ad-Hoc Networking, defines an intelligent way of using Vehicular Networking.

2). Both radio (very high frequency [VHF], micro, and millimeter waves) and infrared waves have been used in experimental V2V systems. Infrared and millimeter waves allow communication only in line of sight, VHF and microwaves allow broadcast communications. VHF can provide long links but at low speed; the mainstream is microwaves. In the United States, 75 MHz in the 5.9 GHz band is allocated for VANETs; in Europe and Japan, the spectrum allocated to VANETs is in the 5.8 GHz band. In Europe, 10 MHz also is available between 2010 and 2020 MHz for vehicle communications. In the PHY/MAC layer for a VANET, three difficult problems must be solved. The first is how to offer robust transmission between vehicles and an efficient sharing of the radio medium. This is a special case of the same problem in MANETs but with the peculiarity that VANETs are usually linear networks. The second problem comes from the fact that there may be a large variation in the density of nodes in a VANET. For instance, in traffic jams or just after an accident, the density of nodes may increase considerably. The third problem concerns the support of emergency applications; in fact ensuring quality of service (QoS) is difficult in a wireless environment.[1].

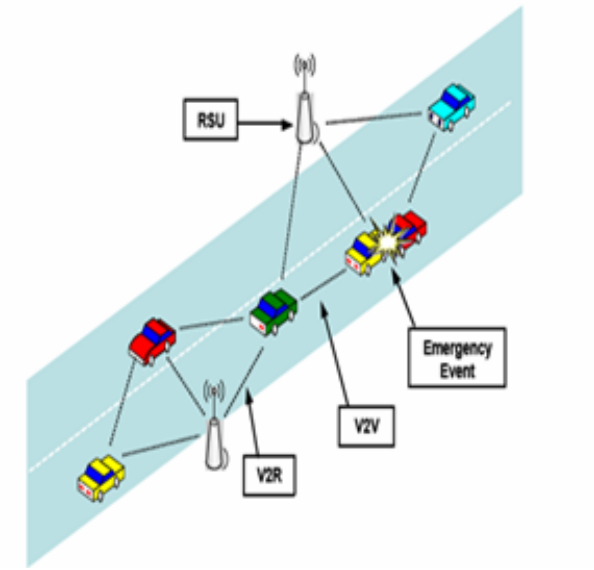

Fig: Example of vehicular network

III. TYPES OF ATTACKS IN VEHICULAR NETWORK ENVIROMENT.

Attacker create problem in the network by getting full access of communication medium DSRC. Here we are discussing some properties and capability of the attackers which has been mentioned in studies.

A. Insider

This type of attackers who is an authentic user of the network and have detail knowledge of network. Insider attacker might have access to insider knowledge and this knowledge will be used for understanding the design and configuration of network. When they have all information about the configuration then it's easy for them to launch attacks and create more problem as compare to outsider attacker. It can create problem in the network by changing the certificate keys. We can simply say that insider attacker is the right man doing the wrong job in the network.

B. Outsider

The outsider attacker is considered as an authentic user of the network. It is a kind of intruder which aims to misuse the protocols of the network and the range of such attacks are limited. Outsider attacker also has a limited diversity for launching different kind of attacks as compare to insider attacker.[2].

C. Wormhole Attack

In wireless networking, the wormhole attack consists in tunneling packets between two remote nodes.[3] Similarly, 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, thus disseminating erroneous (but correctly signed) messages in the destination area.

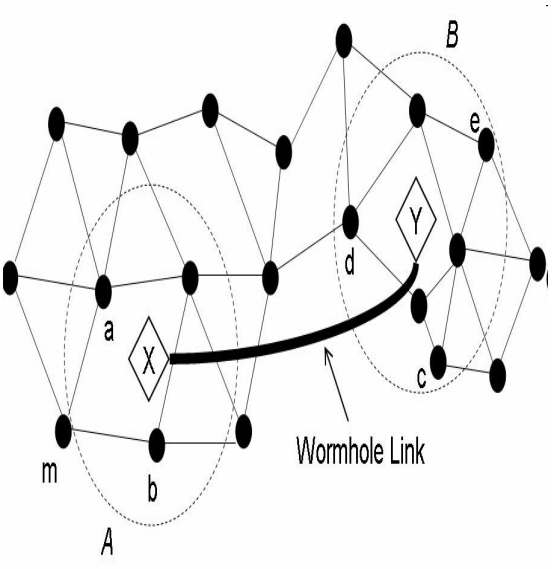

Fig: wormhole link

In case wormhole attack hacker tries to hack the network and form a tunnel between the legitimate nodes and disrupts the functioning of the network.[4]

IV. IDS APPROACH TO DETECT ATTACK.

An IDS is a device or software application that monitor network or system activities for malicious activities or policy violations and produce report to a management station. An IDS evaluates a suspected intrusion once it has taken place it also watches for attacks that originate from within system. Considering the malicious road side attacker that is sending incorrect emergency braking warnings, then IDS detection process could be as follows .A first event of a suspicious action within the active safety system would be discovered, if an emergency braking event is received from a previously unknown node. One would normally expect such an event to come from a previously known node. A second event might come from another vehicle that previously passed this area and also received the same warning message. After passing the respective area, this car's intrusion detection system recognizes, that for itself, there was no emergency braking event and transfers this analysis to follow up cars.
Combining these two events results in a strong evidence that the received warning message must be a fake warning. Thus, the intrusion detection system tells the active safety system to ignore the warning and communicates the detection results to other nodes, especially follow up nodes. In order to realize such an intrusion detection system in VANETs, we implement of a modular cross layer intrusion detection system. On every node, different modules are in charge of collecting audit data on different layers. A local decision module receives continuously audit data summaries from the other modules and analyses them with the aid of additional information, available from other non-network devices, such as radar, GPS and sensors.[5]

Expect from the central decision module, the different modules are: a monitoring module for the network and routing layer, a context information module, an application evaluation module, an action module and a module for communication with intrusion detection systems on other nodes.
The monitoring module for network activity and routing is responsible for collecting data on communication within the node's communication range. This includes monitoring the neighboring nodes' forwarding attitude, as well as the generation of a list of current and previous neighbors, including their positions and movements, i.e. the creation of a network topology development report. The current neighboring nodes' position data can be verified by active probing messages, or GPS and sensor data from the context information module, in order to help to identify abnormal node behavior. On the application layer, the received warning messages are first evaluated by the application evaluation module, which uses knowledge from applications, in combination with sensor data provided by the context information module. This verification could enable, for instance, the detection of false icy road warnings, which would be quite implausible when the outside temperature is above 11 degree..

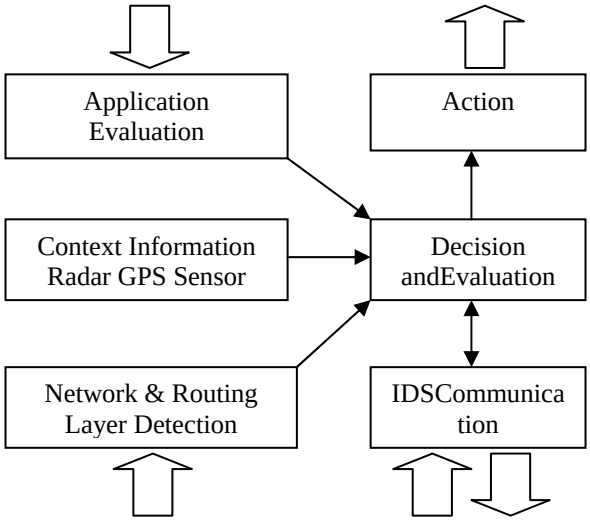

Fig: Modular Cross Layer Architecture

The intrusion detection communication module is used to share the evaluated audit data with other nodes and forward other nodes' audit results to the local decision module. Audit results are either exchanged directly, via multiple hops, or via a temporarily accessible road network infrastructure. Especially in case of sparse node density, a potentially accessible road network infrastructure will help to propagate intrusion alerts to follow up cars. On the other hand, cooperative detection requires some kind of trust between the participating nodes. Hence, we will use dynamic trust establishment between communicating nodes and establish first trust relations during a direct communication phase, to keep them for later usage.[6]

v. SIMULATION AND RESUTS.

In this section the resuts from various simulations is shown in from of graphs.

True Positive: True positive means that an attack is detected by the intrusion detection system and marked as abnormal activity.

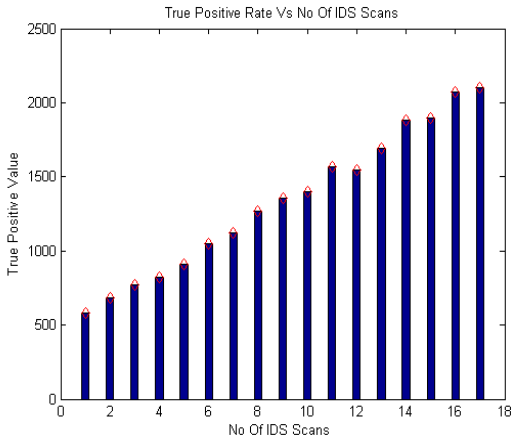

Fig: True Postive

True Negative: True negative means that the situation when there is no abnormal activity or attack in the network and IDS mark this activity as normal activity.

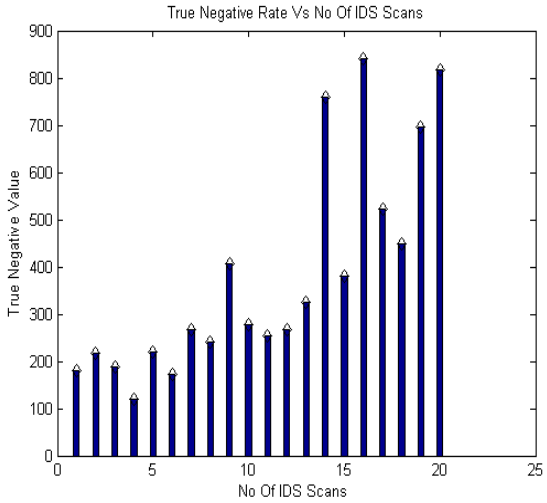

Fig: True Negative

VI. CONCLUSION

Safety is a primary concern to many road users. Securing VANET communication is a crucial and serious issue, since failure to do so will delay the deployment of technology on the road. The safety requirements can be powerfully supported by many safety applications, such as traffic report and accidents notifications. Wormhole is very severe attack in adhoc network and it is possible even if the attacker is not compromised ane types of any hosts. The wormhole attack can form a serious threat in wireless networks,especially in adhoc network. We present different methods like TP, TN to detect these types of attacks.

.

REFRENCES

[1] J.-P. Hubaux, S. Capkun and J. Luo, The security and privacy of smart vehicles, IEEE Security and Privacy Magazine **2**(3) (2004).

[2] Maxim Raya and Jean-Pierre Hubaux "Securing vehicular ad hoc networks", Journal of Computer security, IOS Press Amsterdam, The Netherlands, Volume 15, Issue 1(January 2007),

[3]. H. Kaur , S. Batish and A.Kakaria, An approach to detect the the wormhole attack in vehicular adhoc network in: International journal of smart sensors and adhoc networks,4,2012.

[4] Y.-C. Hu, A. Perrig and D.B. Johnson, Packet leashes: A defense against wormhole attacks in wireless networks, in: Proceedings of IEEE Infocom'03, 2003.

[5] Y. Zhang and W. Lee, “Intrusion detection in wireless ad-hoc networks,”in Proceedings of the 6th annual international conference on Mobile computing and networking. ACM Press, 2000, pp. 275–283.

[6] Y. Zhang, W. Lee, and Y.-A. Huang, “Intrusion detection techniques formobile wireless networks,” Wirel. Netw., vol. 9, no. 5, pp. 545–556, 2003