A Survey on Wormhole attack in VANET

Shreya Patel[1], Prof. Pratik Modi[2]

[1]*Research Scholar, Computer Engineering Department, LDRP Institute of Technology & Research, Gujarat, India*
[2] *Professor, LDRP Institute of Technology & Research, Gujarat, India*

ABSTRACT

Security of nodes is one of the major effects that exist in Vehicular Ad-hoc network. Vehicular Ad-hoc networks are increasingly used to avoid accidents, traffic control and management of toll stations and public areas. In this paper we will study about wormhole attack. Wormhole attack is the one of the dangerous attack in network layer. In wormhole attack two or more malicious nodes can create a tunnel and transmit the data from one malicious node to another malicious node through tunnel. This paper describes all routing attacks and briefly describes wormhole attack. In this paper also describes wormhole detection and prevention techniques by literature survey.

Keywords: - *VANET, Wormhole attack.*

---

1. INTRODUCTION:

A special type of mobile ad-hoc network in which nodes are vehicles is called Vehicular Ad-hoc Network (VANET). The network in VANET is movable nodes. The VANET can allows generally 100 to 300 meter distance to connect the vehicles. If the vehicle is not coming under the range, the signal will breaks and new vehicle can join if this vehicle is coming under the network range. [1]

Vanet is an Intelligent Transportation System in which vehicle act as router, sender receiver to broadcast the information of data to the vehicular network. Its purpose to provide suitable information, security, management of network. Vanets are dynamic in nature because connection between nodes is temporary. It is designed for vehicle to vehicle communication, vehicle to infrastructure communication and hybrid communication (both vehicle to vehicle and vehicle to infrastructure).Due to accidents of vehicles and road mortality increasing day by day, people are facing this type of problems need safety. So security in VANET is very essential, because the message sent by one vehicle to another vehicle might have important outcome such as accident avoidance. Its main objective of handle vanet is to reducing the level of accidents and provides safety to the passengers sitting in the vehicles. [2]

VANET is similar to MANET (Mobile ad-hoc network) along with some variations. VANET have the mobile nodes (MN) and road side units (RSU). Mobile nodes are the sensors embedded in the vehicles that are called as on board units (OBU) for the data sharing to and from RSUs. RSUs are decided installed units that are the gateway for the communication between Mobile nodes and the servers(internet). There are a lot of services granted by VANET but the very important among all is the road safety services for the decrease of road accidents by data sharing through internet. [3]

Comparisons table for mobile ad-hoc network, vehicle ad-hoc network and flying ad-hoc network.

MANET	VANET	FANET
MANET is an Ad-hoc network Of mobile nodes.	VANET is an Ad-hoc network of vehicle nodes.	FANET is an Ad-hoc network of flying nodes.
Node mobility of MANET is slower compared to VANET and FANET.	Node mobility of VANET is higher compared to MANET.	Node mobility of FANET node is much higher than MANET and VANET.
Node density is low in MANET.	Node density is high in VANET.	Node density is very low.
Topology change is slow in MANET compared to other network.	Topology change is fast in VANET.	Topology change is fast in FANET
MANET nodes can having the limited computational power because of the size of nodes.	VANET application specific devices with high computational power can be used.	FANET application specific devices with high computational power can be used. Most of the nodes can have enough energy and space to include high computational power.

Table 1: Comparison of MANET, VANET, FANET

2. ARCHITECTURE OF VANET:

The VANET architecture for communication between vehicles and road- side equipment's which can be broadly classified into 3 types. [4]
1. Vehicle to Vehicle communication
2. Vehicle to Infrastructure communication
3. Hybrid communication

1. Vehicle to Vehicle:-

In Vehicle to Vehicle, there will be direct communication between vehicles that are not depending on the infrastructure (road side units or internet). These types of communication are mainly used for security, safety and another application. Figure 1 shows the communication between vehicle to vehicle.

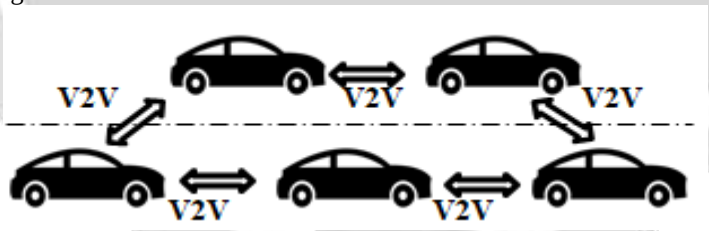

Figure 1 : Vehicle to vehicle

2. Vehicle to Infrastructure:-

In vehicle to infrastructure, this type of communication is mainly used for applications such as information application and data gathering application to communicate with road side in infrastructure. Figure 2 shows the communication between vehicle to infrastructure.

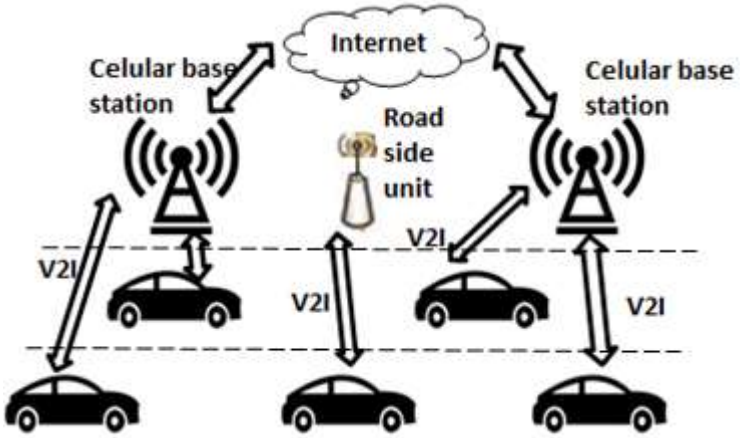

Figure 2 : Vehicle to infrastructure

3. Hybrid:-

In hybrid type, depending on the distance the vehicle can communicate between the vehicle to vehicle and vehicle to roadside infrastructure with single hop or multi hop fashion. This is possible because of the combination of vehicle to vehicle and vehicle to infrastructure. Figure 3 shows the communication between vehicle to vehicle and vehicle to infrastructure.

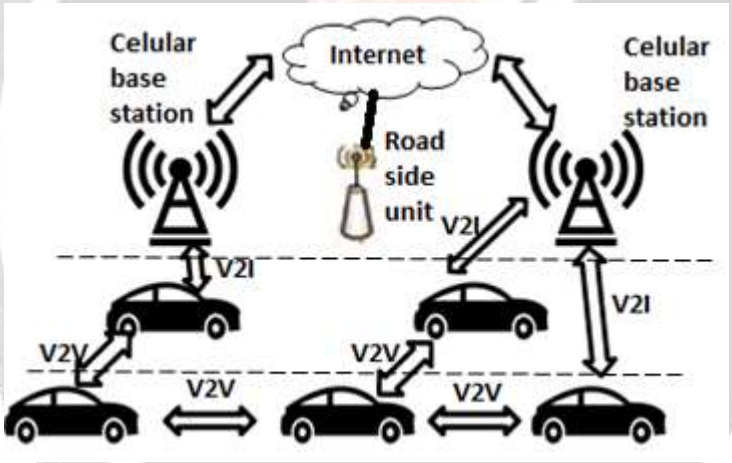

Figure 3 : Hybrid

3. ROUTING ATTACK:

1) Denial of Service (DoS) Attack:
DoS attack can be done by insiders and outsiders of the networks. An insider attacker can jam the channel after transmitting dummy messages and hence, stops the network connection. An outsider attacker can introduce a DoS attack by regularly disseminating fake messages with invalid signatures to consume the bandwidth or other resources of a targeted vehicle. The impact of DoS attack is that, VANET loss its ability to provide services to the proper. [9]

2) Black Hole Attack:

A malicious node can destroy all the packets that it receives for sequential transmission. In black hole attack is specifically effective when the node is also a collection point. This type of combination may be the reason for stopping the transfer of large amount of data.[6]

3) Grey Hole Attack:

In this type of attack, malicious node behavior is unpredictable such that a node will act as a malicious node for a little time, but in the next later on node act just like other normal nodes. In this attack an attacker drops the packet in the network and disturbs the route detection process which reduces the packet delivery ratio of the vanet network. [10]

4) Sinkhole Attack:

A malicious node can be the most optimal for all neighboring nodes from the point of view of the routing algorithm.[6] For example, the malicious node can send out routing messages, definite all neighboring nodes that it is the best node for sequential transmission of the packet to the base station. This allows node to become a hub and collect all the data packets from every nodes of his neighborhood going to the base station. This opens up great opportunities for subsequent types of attacks.

5) Sybil Attack:

In this type of attack, an attacker makes multiple identities to simulate multiple nodes and so creates an illusion of traffic congestion. The malicious nodes can misguide other vehicles, take part in voting security protocols and can even lead to loss of life. [14]

6) Wormhole Attack:-

Wormhole attack is a dangerous attack in VANET as well as in other Ad-hoc networks [1].This attack has one or more malicious node and a tunnel between them. The attacking node captures the data packets from one location and transmits them to other separate located node which scatters them locally. [5]
Malicious nodes are capable of generate a wormhole due to the wireless type of the network. The wormhole tunnels the packets to the colluding node at the other end of the wormhole. Wormhole provides the commanding role to the attacker in comparison to the other nodes. Wormhole can perform disrupting routing process, unauthorized access, breaking the security of data packets transmission. Wormhole attacks disturb the multi-cast and broadcast operations for transmitting messages in VANET. [1]

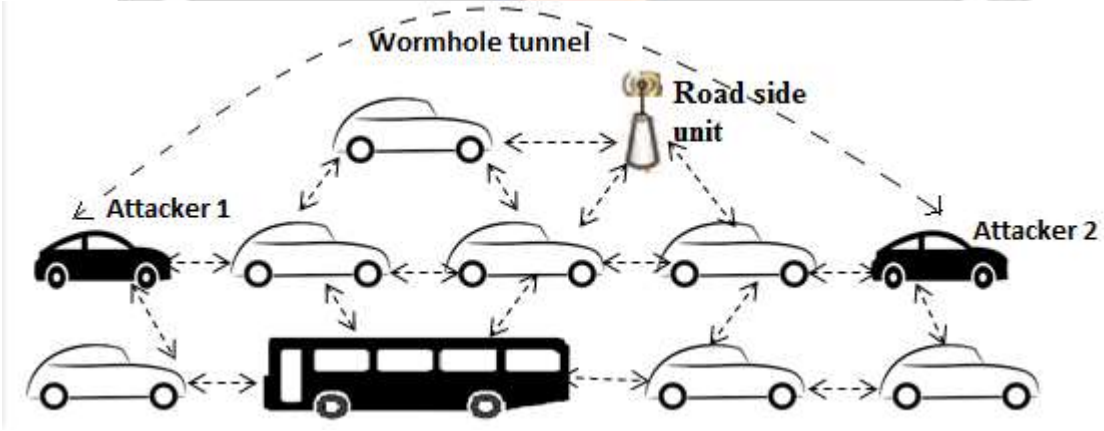

Figure 4 : Wormhole attack.

4. LITERATURE SURVEY:

4.1 Artificial swarm algorithm for VANET protection against routing attacks

Vasiliy Krundyshev, Maxim Kalinin, Peter Zegzhda [6] They are proposed a new approach to provide security for VANET and other types of transport relative networks using swarm algorithms of artificial intelligence. The article describes the algorithm itself, its characteristics and main advantages. The proposed swarm algorithm is used for detection of wormhole attack in vanet. The algorithm is based on IWD (intelligent water drops), and the algorithm uses the trust model. Trust is the key element in creating a trusted vehicular environment which promotes security in vehicular networks. The algorithm is designed for moving vehicular networks up to 1000 nodes, the speed of the nodes is 0-140 km/h, it is suitable for both urban and highway use scenarios. The algorithm has two types of parameters: static and dynamic parameters. Static parameters are constant during the process of the IWD algorithm. Dynamic parameters are reinitialized after each iteration of the IWD algorithm. The algorithm consists of 3 phases: build a route, maintain existing routes, and update a trust estimation to detect anomalies in routing and build a new route bypassing the suspicious node. Calculate the trust value of the neighbor node by using the formula. Average value of the pheromone per unit calculates and then checks to the threshold value if exceeded node secure either not secure. In this the two attack results are described here in the terms of throughput, packet delivery ratio and average end to end delay. Better results are shown in paper.

4.2 Secure Message Broadcasting in VANET over Wormhole Attack by using Cryptographic Technique

Shahjahan Ali ,Prof. Parma Nand ,Prof. Shailesh Tiwari[1] Broadcast secure message from source to destination using RSA algorithm and symmetric key combination(cryptographic technique).And proposed algorithm are used by which a message (in the form of packets) can be broadcasted from one node to other nodes securely and efficiently. In this technique RSA is used to distribute the shared key and identifier (ID) of nodes, and further broadcasting of messages with ID of node is carried out by the shared key encryption. And then prevent the wormhole attack by using the packet lease technique. It is uses for maximum transmission distance of the packet. It uses TIK protocol and it gives efficient authentication for broadcast communication in wireless networks by using the concept of temporal leashes. And proposed approach is described in the paper. Two time verification is required if sender uses public key and destination uses private key , so more secure approach. The limitation of this proposed approach is that if it applied on a Network having large number of nodes then more and more computations are required due to which more power will be consumed. In future work proposed approach can be simulated and the performance of proposed approach can also be compared with other approaches.

4.3 Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol

Parmar Amisha, V.B.Vaghela [5] In this paper, the techniques dealing with wormhole attack in WSN are surveyed and a method is proposed for detection and prevention of wormhole attack. AOMDV (Ad hoc On demand Multipath Distance Vector) routing protocol is incorporated into these method which is based on RTT (Round Trip Time) mechanism and other characteristics of wormhole attack. And then firstly sender node calculate the round trip time by using the hop count and threshold value and then compare the result with the normal AOMDV protocol and wormhole affected AOMDV protocol. In this improved result shown in paper that are end to end delay, packet fraction ratio and throughput.

4.4 Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks

Raja Waseem Anwar, Majid Bakhtaran, Anazida Zainal,Abdul Hanan Abdullah and Kashif Naseer Qureshi [7]To protect sensor network from routing attacks in the presence of malicious nodes is always a challenge. In this paper, They propose a trust aware distance vector routing protocol (T-AODV) to protect wireless sensor network from wormhole attacks .Neighbor node and actual node distance calculated and then by using this approach detect wormhole attack. propose scheme is better than AODV in the presence of malicious nodes. Number of hop, end to end delay and packet delivery ratio result are shown in this paper with the comparison.

4.5 A Detection and Prevention of Wormhole Attack in Homogeneous Wireless Sensor Network

Swati bhagat, Trishna Panse [8] In this paper they distinguish the wormhole by their powerful transmission of the node in the system furthermore put off the system from the wormhole by accomplishing privacy in our modified AODV.They produce a secure AODV protocol and it uses for detecting wormhole attack it checks transmission power .they are using parameters like throughput , packet delivery ratio and end to end delay. They also compare this parameter with the normal AODV protocol and better result are described in the paper.

5. CONCLUSION:

Vehicular Ad-hoc Networks is encouraging technology, which gives big chances for attackers, who will try to challenge the network with their harmful attacks. In this paper describes the overview of wormhole attack. And also describes some techniques for wormhole attack detection and prevention. In this paper the modified AODV protocol are used in the detection and prevention technique. In future work proposed approach can be simulated and the performance of proposed approach can also be compared with other approaches in the network.

6. REFERENCES:

[1]. Shahjahan Ali , Prof. Parma Nand , Prof. Shailesh Tiwari ," Secure Message Broadcasting in VANET over Wormhole Attack by using Cryptographic Technique ", International Conference on Computing, Communication and Automation (ICCCA2017) .

[2]. Shikha Sharma , Er.Shivani Sharma,"A Review: Analysis of Various Attacks in VANET ",Volume 7, No. 3, May-June 2016 International Journal of Advanced Research in Computer Science.

[3]. Muhammad Rizwan Ghori, Kamal Z. Zamli, Nik Quosthoni, Muhammad Hisyam, Mohamed Montaser ," Vehicular Ad-hoc Network (VANET): Review", 2018 IEEE International Conference on Innovative Research and Development (ICIRD).

[4]. Pramod Mutalik, Dr venakanguada C patil," A survey on vehicular adhoc network[VANET'S] protocols for improving safety in urban city" ,IEEE 2017.

[5]. Parmar Amisha ,V.B.Vaghelab ," Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol "ELSIVIER 2016.

[6]. Vasiliy Krundyshev , Maxim Kalinin , Peter Zegzhda," Artificial swarm algorithm for VANET protection against routing attacks ", IEEE 2018.

[7]. Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal,Abdul Hanan Abdullah and Kashif Naseer Qureshi,"Enhanced Trust Aware Routing against Wormhole Attacks in Wireless Sensor Networks ",IEEE 2015.

[8]. Swati Bhagat,Trisha panse," A Detection and Prevention of Wormhole Attack in Homogeneous Wireless Sensor Network ",IEEE2016.

[9]. Mithun Sahay Shrivastava , Ravi Khatri , Anand Singh Bisen ." Hybrid Approach for detecting and preventing DOS attack in VANET ", International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016.

[10]. Swati Verma , Bhawna Mallick , Poonam Verma ," Impact of Gray Hole Attack in V ANET ", 2015 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015.

[11]. Masayuki Arai, Chiba, Japan ,"Reliability Improvement of Multi-Path Routing for Wireless Sensor Networks and Its Application to Wormhole Attack Avoidance ",IEEE2015.

[12]. Ubaidullah Rajput1, Fizza Abbas2, Hasoo Eun1, and Heekuck Oh1," A Hybrid Approach for Efficient Privacy Preserving Authentication in VANET ", 2016 IEEE.

[13]. Bodhy Krishna. S ," Study of Ad hoc Networks with Reference to MANET, VANET, FANET ", International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-7,Issue7)

[14]. Anu S Lal ,Reena Nair," Region Authority Based Collaborative Scheme to Detect Sybil Attacks in VANET", 2015 International Conference on Control, Communication & Computing India (ICCC) | 19-21 November 2015.