An Approach To Detect The Wormhole Attack In Vehicular Adhoc Networks

Harbir Kaur, Sanjay Batish & Arvind Kakaria

Dept. of Comp. Science, PEC, University Of Tech, Chandigarh, India
E-mail : harbir37@gmail.com, sanjaybatish@gmail.com, & arvind_802@rediffmail.com

Abstract **-** In VANET there is no centralised infrastructure due to which it is vulnerable to various security attacks . One of such attack is wormhole attack, it enables an attacker to capture packets at one location and tunnels them to another location making a wormhole in-between the legitimate nodes of the network. In this paper we proposes a method in which we use decision packets to detect the wormhole nodes in the network and for maintaining the integrity of the packets we compute hash value of each packet. The source node broadcasts the decision packet to all the nodes after receiving the route reply message from the destination node which contains the list of the route forming nodes. The decision packets from the nodes are then evaluated by the destination node based on the hop count value. If the hop count exceeds the threshold value, it means a wormhole is formed between the nodes.

I. INTRODUCTION

Automobile traffic is the major problem in modern societies. Millions of hours and gallons of fuel are wasted everyday by vehicles stuck in traffic. Technology is at a point today in which vehicles themselves could be used to compile and analyze traffic conditions which would help the drivers to take smart decisions to avoid congestions on road due to traffic jams or accidents and drive safely and soundly. Vehicular Ad-hoc Networks (VANETs) can be considered as a subset of Mobile Ad hoc Networks (MANETs) with unique characteristics. It is a combination of wireless, adhoc and cellular network. It is a special type of adhoc network used to provide communication between vehicles. It allow the vehicles almost to connect 100 to 300 meters to each other and in order to create a wide range network , vehicles are connected to each other so the mobile internet is made .Vehicles are equipped with wireless communicating devices. They can communicate with other vehicles within their range leading to the formation of wireless adhoc network that can disseminate information in a peer to peer fashion. Each communicating vehicle act as a wireless router or node allowing vehicles within a particular range to form a network. As cars fallout of the range of the network and drops out other nodes or vehicles comes into play and start communicating creating a mobile network. A typical VANET[1] consists of vehicles and access points along the road. Vehicles move on the roads sharing information between themselves and with the Internet through the access points.

VANET has become an active area of research, standardization, and Development because it has tremendous potential to improve vehicle and road safety, traffic efficiency, and convenience as well as comfort to both drivers and passengers.

In VANET each vehicle, acting as a wireless router or node, is equipped with sensors that are connected to the computer that provides (1) measurements about the vehicle itself (speed, acceleration, tire slip), (2) the vehicle's location with the lane,(3) the relative speed between the vehicle and the vehicle in front. Most importantly , an inter vehicle communication system formed a local area network to exchange information with other vehicles in the neighborhood to support cooperative driving features like lane changing , congestion warning , rollover warning ,coupling decoupling , inert vehicle communication etc. The information transmitted during communication should be safeguarded as it contains the information about the driver's credentials so a threat to network would be a threat to driver's safety.

VANET, being a wireless network, inherits all the security threats that a wireless system has to deal with. A security system should be developed that should ensure that a transmission comes from trusted source and is not tampered in route by other sources. Our primary focus in VANET is on safety related applications because they require stringent time requirements as compared to non safety related applications. Due to the adhoc nature of the network any node can enter or leave the network at any time and

there is no prior trust relationship between nodes which makes it vulnerable to various types of attacks[2] like Sybil attack, denial of service attack, forging attack ,illusion attack[3] and wormhole attack. Wormhole attack is the most severe of these attacks as it can occur even if no node of the network is compromised. Wormhole attack can occur in every scenario where there is no centralized unit controlling all the nodes in the network.

II. RELATED WORK

In [5] Safi et. Al introduces a packet leashes method to defend against the wormhole attack. A leash[4] is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. Leashes are designed to protect against wormholes over a single wireless transmission; when packets are sent over multiple hops, each transmission requires the use of a new leash. Leashes prevent wormhole attack by limiting the distance of the packet to be travelled in a transmission. There are two types of leashes: geographical leashes[5] and temporal leashes. In a geographical packet leash each packet, upon transmission contains a credit which contains the location and time of the sending node and sent to the receiving node after digitally signed by the sending node. At the receiving end the receiving node compares it with its own location and timestamp and determines whether the sender is close enough to be a neighbour. Geographical packet leashes require accurate and verifiable location information. With temporal leashes[6], all nodes have tightly synchronized clocks. The sender stamps the packet with the current time, and signs it for later authentication. The receiver compares the time in the packet with its local clock. If the difference exceeds some small value, determined by the maximum transmission range of the radio in use, the packet is discarded. Temporal packet leashes require extremely tight global clock synchronization, making it infeasible for many applications.

An advantage of geographical leashes over packet leash is that the time synchronisation can be much looser and other advantage is that it provides non-repudiation of nodes so an attacker can be caught if it pretends to reside at multiple locations. . When a legitimate node overhears the attacker claiming to be in different locations that would only be possible if the attacker could travel at a velocity above the maximum node velocity, the legitimate node can use the signed locations to convince other legitimate nodes that the attacker is malicious.

In temporal leashes going through a wormhole means covering a longer distance than the normal distance between neighbouring nodes and this longer distance can be precisely measured due to the tightly synchronised clocks. The disadvantage of this approach is that they require either information of each node or tight clock synchronisation between nodes and these requirements cannot always be satisfied in VANET.

III. DIFFERENT ATTACKING MODES

Based on the launching techniques wormhole attack is classified into two types[10].

a) Wormhole using packet encapsulation

Wormhole attacks are particularly severe against many ad-hoc and sensor network routing protocols, such as ad-hoc on-demand routing protocols DSR [8] and AODV [9] protocols. First, we demonstrate how a generic wormhole attack is launched against such routing protocols, using DSR as an example. In DSR, if a node, say S, needs to discover a route to a destination, say D, S floods the network with a route request packet. Any node that hears the request packet transmission processes the packet, adds its identity to the source route, and rebroadcasts it. To limit the amount of flooding through the network, each node broadcasts only the first route request it receives and drops any further copies of the same request. For each route request D receives, it generates a route reply and sends it back to S. The source S then selects the best path from the route replies; the best path could be either the path with the shortest number of hops or the path associated with the first arrived reply. However, in a malicious environment, this protocol will fail. When a malicious node at one part of the network hears the route request packet, it tunnels it to a second colluding party at a distant location near the destination. The second party then rebroadcasts the route request. The neighbors of the second colluding party receive the route request and drop any further legitimate requests that may arrive later on legitimate multihop paths. The result is that the routes between the source and the destination go through the two colluding nodes that will be said to have formed a wormhole between them. This prevents nodes from discovering legitimate paths that are more than two hops away. One way for two colluding malicious nodes can involve themselves in a route is by simply giving the false illusion that the route through them is the shortest, even though they may be many hops away. Consider Figure 1 in which nodes A and B try to discover the shortest path between them, in the presence of the two malicious nodes X and Y. Node A broadcasts a route request (REQ), X gets the REQ and encapsulates it in a packet destined to Y through the path that exists between X and Y (U-V-W-Z). Node Y demarshalls the packet, and rebroadcasts it again, which reaches B. Note that due to the packet encapsulation, the hop count does

not increase during the traversal through U-V-W-Z. Concurrently, the REQ travels from A to B through C-D-E. Node B now has two routes, the first is four hops long (A-C-D-E-B), and the second is apparently three hops long (A-X-Y-B). Node B will choose the second route since it appears to be the shortest while in reality it is seven hops long. So X and Y succeed in involving themselves in the route between A and B. Any routing protocol that uses the metric of shortest path to choose the best route is vulnerable to this mode of wormhole attack. This mode of the wormhole attack is easy to launch since the two ends of the wormhole do not need to have any cryptographic information.

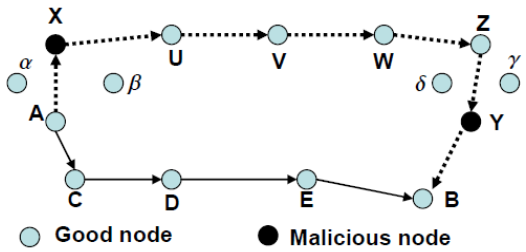


Figure:1 Wormhole through packet encapsulation

b) Wormhole using out-of-band Channel

This mode of the wormhole attack is launched by having an out-of-band high-bandwidth channel between the malicious nodes[7]. This channel can be achieved, for example, by using a long-range directional wireless link or a direct wired link. This mode of attack is more difficult to launch than the previous one since it needs specialized hardware capability. Consider the scenario depicted in Figure 2. Node A is sending a route request to node B, nodes X and Y are malicious having an out-of-band channel between them. Node X tunnels the route request to Y, which is a legitimate neighbor of B. Node Y broadcasts the packet to its neighbors, including B. Node B gets two route requests — A-X-Y-B and A-C-D-E-F-B.

The first route is both shorter and faster than the second, and is thus chosen by B. This results in a wormhole being established between X and Y on the route between A and B.

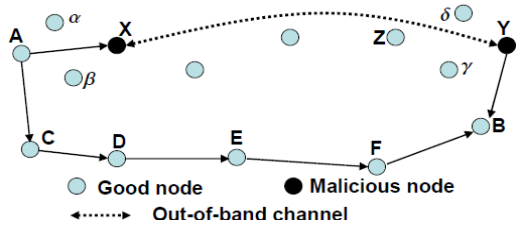
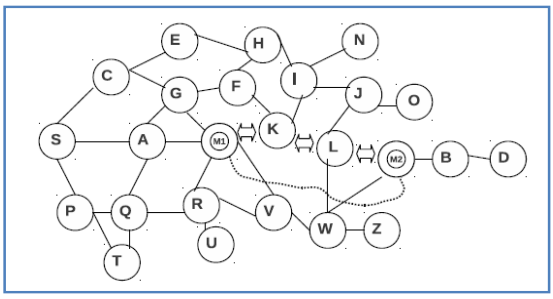


Figure : 2 Wormhole through out-of-band channel

IV. PROPOSED SOLUTION

In order to avoid wormhole attack, the nodes participating in the VANET communication have to be registered in the network. Each node is provided with the unique id which would help in maintaining the record of each and every node participating in the network. The authenticated users or nodes decrease the possibility of the out-of- band channel wormhole attack as attackers would not be able to disrupt the route. Each packet or message sent between two nodes should be protected using hashing algorithms which would maintain the integrity of the packet at every node. If the attacker modifies the value of the message and tries to disrupt the communication then that modification results in change of hash value which would alarm the network against the attacker. The attacker forms the wormhole during the route discovery phase. In order to avoid the formation of wormhole in the route this paper proposes a method in which after the route reply from the destination the source has a complete list of the intermediate nodes forming the route[11]. As we know the complete network consists of only authenticated users so it is difficult for the outside attacker to disrupt the route but there is a possibility that the attacker compromises the legitimate users and then form their own network in between two legitimate nodes hiding their network from the rest of the nodes.



Out-of–band channel normal channel
In band channel malicious node
Figure 3: wormhole attack

eg .in fig 3 the malicious nodes compromises the legitimate nodes to form their own network.

In this we propose a scheme in which we use a special packet called decision packet .After the route has been set up between source node and destination node, source node got the information about all nodes in the path from RREP packet[11]. To identify wormhole in the path sender node creates decision packet as shown in fig 4. which contain all nodes identity whose has been forming route from source to destination node in recently identified path. Each node in the network forwards the decision packet instead of nodes which take part in the route formation from source to destination. The rest of neighboring nodes process the nodes and updates the decision packet information by incrementing the hop count of the nodes listed in packet that are its neighbor. This would help in calculating the distance between the nodes.

Node	Hop count

Fig. 4 decision packet

The nodes send these packets to the destination node and the destination node perform a check on these packets by evaluating the hop counts and make a decision table.

Node	next node	Hop count

Fig 5. Decision table

If the hop count exceeds the threshold value ,let it be 5, it means a wormhole is formed between nodes.

Every node computes the hash value of the decision packet which is verified at the next node, so there is no chance of alteration of the hop count by the attacker. If any attacker by somehow changes the hop count value then it would result in change in hash value of the packet which would result in discarding of the packet.

V. CONCLUSION AND FUTURE WORK

This paper proposes a solution for wormhole attack in VANET. Wormhole attack is the most dangerous attack as it can also become a cause of other attacks like sinkhole attack as it creates a sinkhole in the network by falsifying the route information, DOS attack as by discarding the packet in the wormhole results in permanent denial of service. By introducing the decision packets the occurrence of the wormhole reduces to a great extent. Moreover, it does not require any additional hardware to be installed on the nodes.

As future work, we intend to implement the proposed solution in the real environment so that the processing delay and efficiency of the VANET can be tested.

REFERENCES

[1.] Panagiotis Papadimitratos, Elmar Schoch, Julien Freudiger and Maxim Raya, Jean-Pierre Hubaux. Secure Vehicular Communication Systems: Design and Architecture. IEEE Communications Magazine.2008

[2.] J.T. Isaac, S. Zeadally, J.S. Ca´mara, Security attacks and solutions for vehicular adhoc networks (2010).

[3.] G. Guett, C. Bryce, ”Using TPMs to Secure Vehicular Ad-Hoc Networks (VANETs)”, WISTP 2008, LNCS 5019, pp.106-116

[4.] Farid Na¨ıt-Abdesselam, Brahim Bensaou, and Tarik Taleb. Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks.(2006).

[5.] Seyed Mohammad Safi Ali Movaghar Misagh Mohammadizadeh. A Novel Approach for Avoiding Wormhole Attacks in VANET. (2009).

[6.] Y. Hu, A. Perrig, and D. Johnson, “Packet leashes: A defence against wormhole attacks in wireless networks,” in INFOCOM, 2003.

[7.] Ming -Yang Su,”WARP:a warmhole avoidance routing protocol by anamoly detection in mobile adhoc networks”,in Computer and security 29(2010).

[8.] D. Johnson, D. Maltz, and J. Broch, “The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks,” in Ad Hoc Networking, C. Perkins, Ed., Addison-Wesley, 2001.

[9.] C. E. Perkins and E. M. Royer, “Ad-Hoc On-Demand Distance Vector Routing,” in Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’99), pp. 90-100, February 1990.

[10.] Issa Khalil, Saurabh Bagchi, Ness B. Shroff “LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks”,Proc.Int’lConf. Dependable Sys.and Networks, Yokohama,japan,July 2005.

[11.] Saurabh Gupta,Subrat Kar,S Dharmaraja “WHOP: Wormhole Attack Detection Protocol using Hound Packet” ,in 2011 international conference on innovation in Information Technology.