A Survey of Wormhole Detection and Prevention Technique in DSR Protocol

Hitesh Kumari, Giriraj Vyas, Sunil Dhankar

Abstract—Security is an important issue in network communication. A wormhole attack is one of the hardest problems in mobile ad-hoc network. In wormhole attack a malicious node captures packets from one location in the network, and tunnels them to another malicious node at a distant point, which replays them locally. There are many techniques to detect and prevent them. In this survey paper we find some detection techniques and classify the proposed solution in which prevent the routing protocol against the wormhole attack. In this paper we present a security enhancement to dynamic source routing (DSR) protocol against wormhole attacks for ad hoc networks.

Index Terms—MANET, Wormhole, DSR, Network Security.

I. INTRODUCTION

Nowadays Mobile ad-hoc network is becoming more popular platform. An ad-hoc network is a self-organized network system without any infrastructure [1]. A mobile ad hoc network (MANET) consists of a collection of wireless mobile nodes that are capable of communicating with each other without the use of any centralized administration or network infrastructure [2]. Security is an important issue in mobile ad-hoc network communication. There are different types of attacks. Some of them active attacks and passive attacks. In active attacks do perform some actions in addition to listening of data. Active attackers can perform Modification, Impersonation or Fabrication. On the other hand passive attackers only listen to network traffic and do not perform any modification of traffic [3]. Other type of attack is wormhole attack. During this attack, a malicious node captures packets from one location in the network and “tunnels” them to another malicious node at a distant point which replays them locally. The tunnel can be established in many ways e.g. in-band and out-of-band channel. This makes the tunneled packet arrive either earlier or with a lesser number of hops compared to the packets transmitted over normal multi hop routes. This creates the illusion that the two end points of the tunnel are very close to each other. However, it is used by malicious nodes to disrupt the correct operation of ad hoc routing protocols. They can then launch a variety of attacks against the data traffic flow such as selective dropping, replay attack, eavesdropping etc [1].

Here Fig.1 shows an example of wormhole attack. A network under a wormhole attack. Intruders A and B are connected by an off-channel link (i.e. wired or satellite link), which they use to tunnel network data from one end of the network to the other. Without a wormhole, nodes 7and 3 are 4 hops apart their messages to each other should go through nodes 2, 6, and 5. When intruders A and B activate a wormhole, nodes 7 and 3 are able to directly overhear each other’s messages, and are lead to believe they are immediate neighbors. Once this happens, all further communications between nodes 3 and 7 will be going through the wormhole link introduced by A and B [4].

II. BACKGROUND

Wormhole attack is a type of severe attack which has been introduced in the context of ad hoc networks. In this paper we use DSR protocol. In this section first we define DSR protocol Second define wormhole attack after that discuss about the how to launch the wormhole attack.

1) Dynamic source routing (DSR)

Dynamic source routing (DSR) protocol, is an on-demand routing protocol based on the concept of source routing, which means that the initiator knows the complete hop-by-hop route to the destination. This specific feature brings efficiency, but also results in the scaling of routing message overhead. To perform DSR, each node is required to maintain a route cache which contains the topology information of the network. The route cache is consistently updated to reflect the current status of the network. DSR consists of two major phases: route discovery and route maintenance. In case of route recovery, source node generates routing request (RREQ) and broadcasts it’s to neighbors. The receiving node will append its own address to the RREQ packet and rebroadcasts it, if it is not the destination. On
reception of RREQ packet at destination, node generates route reply (RREP) packet and forward back to the source [5].

2) Wormhole Attacks
In a wormhole attack two nodes are connected with one another with the help of a medium which is not available to normal nodes, with the help of this out of band channel the nodes are able to communicate with one another over a range in which normal nodes cannot. The two colluding nodes act in a way that they appear to be neighbors to all the other nodes [3].

3) Modes of wormhole attacks
a) Wormhole using high power transmission
In this mode, a single malicious node can create a wormhole attack without the help of any colluding node. When a malicious node gets a route request, it broadcasts the request with high power as compared to normal nodes. Any node that hears the high-power broadcast re broad casts it towards the destination. By this method, the malicious node increases its chance to be in the routes established between the source and the destination.

b) Wormhole tunnel using encapsulation
In this mode of attack, two or more malicious nodes participate to create a tunnel between the mend give false illusion that the route through the miss the shortest, even though they may be far away. They create a tunnel with the help of normal nodes using encapsulation. Due to encapsulation, hop count does not increase during the traverse although intermediate nodes of tunnel, which launches wormhole attack between source and destination.

c) Wormhole tunnel using out-of-band channel
In this mode of attack, an out-of-band high-bandwidth channel between the malicious nodes is used to create a wormhole tunnel. These channels can belong-range directional wireless link or a direct wired link. This type of attack requires specialized hardware, therefore, it is more difficult to launch as compared to encapsulation attack.

d) Worm hole using packet relay
In this mode of attack, a malicious node tries to convince two far nodes that they are neighbors by relaying packets between them. Even one malicious node can do this and if more malicious nodes are available then this can expand the neighbor list of victim nodes to several hops.

III. LITERATURE SURVEY

a) Detection Techniques:-
The methods proposed in the previous researches can be broadly classified into two categories. First, methods which has modified a well-known routing protocols such as Adhoc on Demand Distance vector, Dynamic Source routing, Optimized Link Sate routing to avoid/detect wormhole attack during route request [7],[8]. Second, methods which has adopted an extra hardware or monitoring system such as positioning system, a time synchronization mechanism, directed antenna or intrusion detection system.
Hu et al.[9] introduced Packet Leashes method to defend against the wormhole attack. Two types of leash information were used Geographical Leash and Temporal Leach. In geographical leases each node must have its accurate location information and loose clock synchronization. When node receives a packet, it calculates distance between previous node and itself by using send/receive timestamp. For temporal leashes, each node should have accurate clock synchronization. Every packet should be delivered to the next node within computed life time of a packet. Otherwise, the next node regards the path as a wormhole the packet leashes do not identify malicious nodes.

Chu et al.[11] introduce a delay analysis approach called DELPHI. It calculates mean delay per hop of every possible route. DELPHI applied a multi-path approach, and recorded the delay and hop counts in transmitting RREQ and RREP through the paths. After collecting all response, the sender computes mean delay per hop of each route. The path with wormhole attacks, the delay would be obviously longer than a normal path with the same hop count. Hence, the path with longer delays would not be selected to transmit data packet and wormhole nodes could be avoided.

Khalil et al. [10] introduce a LITEWORP in which they used the notion of guard node. The guard node can detect the wormhole if one of its neighbors is behaving maliciously. The guard node is a common neighbor of two nodes to detect a legitimate link between them. In a sparse network, however, it is not always possible to find a guard node for a particular link.

Su et al. [7] proposed a modified AODV routing protocol called WARP to defend against wormhole nodes by adopting link disjoint multi-path routing between source and destination. In WARP each node records its entire neighbor’s anomaly values (number of times it forms path from different source to destination). Due to wormhole node’s great ability to grab routing paths, if the occurrence of one links exceeds the threshold value, the two ends of this link may be wormhole nodes. If anomaly values of a node exceed a threshold value then its neighbor will discard all requests for forming route containing that node in the path.

b) Proposed solutions:-
Several solutions have been proposed in the literature for the wormhole attack, the solutions can be categorized into location based, time based, key based, statistics, and graph based solutions. In this section we give a brief overview of these solutions.

Location and Time Based Solutions: Most of the proposed wormhole solutions in the literature are based on location or time. Packet leashes have been proposed and specifically two types of packet leashes: geographical and temporal were considered in [12]. The main idea is that by authenticating either an extremely precise timestamp or location information combined with a loose timestamp, a receiver can determine if the packet has traversed an unrealistic distance for the specific network technology used. Packet leashing was added to each packet on each link to restrict the transmission distance of the packet. Two types of packet leashes could be added into the packet. One is geographical leash in which the sender inserts its own position and sending time into the packet, the receiver will estimate the maximum distance between the sender and itself based on its own position and receiving time. If the distance exceeds the transmission range, the packet will be discarded. The other type is temporal leash. This mechanism assumes that the maximum transmission speed of radio signal is the speed of light, thus the expiration time of a packet can be estimated using the maximum transmission range and the speed of light. The expiration time of the packet is inserted into the packet,
and then the receiver can check whether the received packet has expired or not based on its receiving time. A drawback of packet leases is that it requires extremely tight time synchronization and GPS.

In [13], secure tracking of node encounters (SECTOR) was proposed. It applied similar principle as packet leases, with the difference that it measured the distance at a single hop and it required special hardware at each node. Directional antennas can be considered as location based solutions and were used in to prevent the wormhole attack.

A mechanism based on signal strength and geographical information for detecting malicious nodes staging HELLO flood and wormhole attacks was proposed in [12]. The idea is to compare the signal strength of a reception with its expected value, calculated using geographical information and the predefined transceiver specification. A protocol for disseminating information about detection of malicious nodes was also proposed.

In [12], another method was suggested in which the sender sets the Destination-only flag such that only the destination can respond to the RREQ packet. Once the RREQ packet reaches the destination, it responds with a RREP with its current position. The sender retrieves the receiver’s position from the RREP packet and estimates the lower bound of hops between the sender and the receiver. If the received route is shorter than the estimated shortest path, the corresponding route will be discarded. Otherwise, the sender will select the shortest path corresponding to the estimation. Once a wormhole is detected by the sender, the sender temporarily enables the path with wormhole and sends out a TRACE packet to the receiver. This TRACE packet is forwarded by each intermediate node through the route with wormhole. When a node on the route receives the TRACE packet, it replies the source with its current position and its hop count to the destination. Then, the sender can estimate the increase of hop count at each node using the received position. If the increase of hop count at one node is not one comparing to its previous hop, then this node and its previous hop node are identified as the wormhole. This approach was illustrated with more details in [12], where an end-to-end detection of wormhole attack (EDWA) in wireless ad-hoc networks was explained in details. In addition analysis and simulation results have shown that the end-to-end wormhole detection method is effective when the source and destination are not too far away.

Key Based Solutions:

For the key based solutions, a scheme was proposed in, and [12] depending on location-based keys, a node-to-node authentication scheme, which is not only able to localize the impact of compromised nodes within their vicinity, but also to facilitate the establishment of pairwise keys between neighboring nodes was developed. These schemes only accept messages from authenticated neighbors and discard those messages tunneled from multi-hop-away locations preventing thus the wormhole attack. Statistical Based Solutions:

In [12], a statistical based solution was proposed. The main idea of the proposed scheme SAM (Statistical Analysis of Multipath) was based on the observation that certain statistics of the discovered routes by routing protocols will change dramatically under wormhole attacks. Hence, it was possible to examine such statistics to detect this type of routing attacks and pinpoint the attackers if enough routing information is available (obtained by multi-path routing). Some other schemes use statistical testing to measure the distribution of the number of neighbors or the distance of all pairs of nodes [12].

Graph-Based Solution:

One type of wormhole detection involves graph theories. In Multi-Dimensional Scaling Visualization of Wormhole (MDS-VOW) [12] multi-dimensional scaling in graph theory was used to reconstruct the topology of the network. A wormhole attack could cause distortion of network topology which could be detected using graph visualization. Another solution based on attack graphs was proposed in [12], its main idea was the development of the wormhole attack graph and the use of adjacency matrices characteristics to predict and detect the wormhole attack.

IV. CONCLUSION

In this paper, we focused on the wormhole attack in ad hoc networks. In this paper we define the modes of wormhole attack. A wormhole attack can be launched in ad-hoc network and what technique we use to detect the wormhole attack. The wormhole attack was introduced and its proposed solutions classified into location based, time based, key based, statistics, and graph based solutions.

In future we can detect the wormhole attack and prevent the ad-hoc network using different techniques.

REFERENCES

[10] I. Khalil S. Bagchi and N.B. Shroff. LITEWORP: “a lightweight countermeasure for the wormhole attack in multihop wireless
networks”. International Conference on Dependable Systems and Networks, 2005

