Comparative Study of Various Methods of Detection of Wormhole Attack in MANET

Rashmi Vijaywargiya¹, Prof. Kamlesh Chopra²

¹ M.Tech Scholar, CSE, Acropolis Technical Campus, Indore, MP, India, rashmi.vijaywargiya89@gmail.com
² Professor, CSE, Acropolis Technical Campus, Indore, MP, India., atc.cse@gmail.com

Abstract

This paper presents survey analysis which aims at comparing various methods of detection of wormhole attack in MANET. Mobile Ad Hoc Network makes it exposed to a variety of network attacks. MANET due to its wireless transmission nature contains more security issues as compared to wired networks. These security issues are very important to deal with so as to make network secure. Wormhole attack also called as tunnelling attack is very difficult to detect, wormhole generally possess two properties In this paper we have studied the wormhole attack along with its properties and various method have been discussed for identification, removal, and prevention of wormhole attack and then they have been compared to one another so that effective methods should come forward. This study aims to combine some methods or to modify the one [1].

Keywords: Mobile Ad Hoc networks (MANET), Wormhole Attack, Vehicular Ad Hoc network (VANET).

1. INTRODUCTION

MANET’s, A Collection of Mobile Hosts with Wireless Network Interfaces Form a Temporary Network without the Aid of Any Fixed Infrastructure or Centralized Administration. These Nodes, Such as Laptop Computers, Pdas and Wireless Phones, have a Limited Transmission Range. Hence, Each Node has the ability to Communicate Directly with another Node and Forward Messages to Neighbors until the Messages Arrive at the Destination Nodes. Security of Such Network is a Major Concern[2]

MANET is an autonomous transitory association of mobile nodes that communicate with each other over wireless links. Nodes that lie within each other’s send range can communicate directly and are responsible for dynamically discovering each other In MANET, every device works as a router and free to move in any direction. Using this property, we can send data over a long distance. It provides high mobility and device portability” that enable to node connect network and communicate to each other. Connections among nodes are limited to their transmission range, and cooperation with intermediate nodes is required for nodes to forward the packets to other node outside of their transmission range.

These properties make security of MANET vulnerable to attackers, and an attacker can modify the routing protocol and disrupt the network operations such as packet drop, selective forwarding, and data fabricating. Most previous ad hoc networks research has focused on problems such as routing and communication, assuming a trusted environment. However, many applications run in untrusted environments and require secure communication and routing such as military or police networks, emergency response operations like a flood, tornado, hurricane or earthquake. However, the open nature of the wireless communication channels, the lack of infrastructure, the fast deployment, and

the Environment where they may be deployed, make them vulnerable to a wide range of security attacks[1].

2. WORMHOLE ATTACK

A particularly severe security attack, called the wormhole attack, has been introduced in the context of ad hoc networks. 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 tunnelled packet arrive either sooner 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. Wormhole can be formed using, first, in-band channel where malicious node m1 tunnels the received route request packet to another malicious node m2 using encapsulation even though there is one or more nodes between two malicious nodes, the nodes following m2 nodes believe that there is no node between m1 and m2. Second, out-of-band channel where two malicious nodes m1 and m2 employ a physical channel between them by either dedicated wired link or long range wireless link shown in Fig. 1
3. WORMHOLE DETECTION TECHNIQUES

3.1. Geographical Leashes
A geographical leash [3] is a method that is implemented in 2003 by Hu to protect ad hoc network from wormhole attack. It is based on this feature that the receiver of the packet is located within a certain distance from the sender. In order to implement geographical leash in the ad hoc networks, firstly some requirements should be provided such as each node must know its own location (using GPS), all nodes must have loosely synchronized clocks and digital signature (RSA) in order to checking the authentication of the location and time of sender. When a packet is sent by a node, it inserts its own location (ps) and the time that the packet is sent (ts) in the header of packet. When the packet arrives to the next node, the location of the receptor (pr) and the time of receive packet (tr) is compared with the values of sender. As regards to the sender and receiver are used synchronized clocks, if the clocks of them are synchronized to within Δ, so, an upper bound distance between the sender and receiver (dsr) is computable by receptor.

3.2. Temporal Leashes
The next method that is designed to protect sensor networks against wormhole attack is called temporal leash [9] in which an expiration time is considered to each transmitted packet. According to this time restriction in temporal leash, a sender of packet should prevent broadcasting packet more than distance L (Lmin = Δ/c, where c is the propagation speed of light). Before a packet is sent at ts by sender the packet expiration time is calculate (te = ts + L/c - Δ) and it is added to packet. So, when the packet received by the next node at its local time (tr), this time is compared with the time of expire packet (te). Then, the packet is drop if tr > te. One of the important requirements of this method is checking the authentication of nodes. According to the existence issue in HMAC and RSA authentication and the side effects of them like the number of keys, the TIK protocol is considered for temporal packet. TIK is constructed based on TESLA, using a symmetric cryptographic [3]. One of the important weak-point of this method is that it is important to mention TIK has some impractical assumptions. It relies on synchronized time between all nodes and there are no delay when the packet sending and receiving. These assumptions are weak points of packet leash method to detect wormhole [4].

3.3. Graph Theoretic Approach
L. Lazos [5] designed a model to characterize wormhole attack in ad hoc networks that called “a graph theoretic approach”. According to this method, to secure an ad hoc network from wormhole attacks a Local Broadcast Key (LBK) was considered and provided a distributed mechanism for establishing them in randomly deployed networks. To succeed these approach its need to use a GPS and special localization equipment. This method is not readily applicable to mobile networks.

3.4. Localized Encryption and Authentication Protocol (LEAP)
“Localized Encryption and Authentication Protocol (LEAP)” is a method which is suggested by Zhu [6]. This model is based on clustering and it requires defining 4 type key for each sensor node such as: an individual key shared with the base station, a pair wise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network. This method is implemented for static or immobile sensor networks. This model is based on clustering and it requires defining 4 type key for each sensor node such as,

a. Individual key that is shared with the base Station.

b. Pair wise key that is shared with another sensor node.

c. Cluster key that is shared with multiple neighbouring nodes.

d. Group key that is shared by all the nodes in the network.

This method is implemented for static or immobile sensor networks.

3.5. Multipath Hop-count Analysis
According to the nature of wireless transmission, the security issues in MANET are more than wired environments. Among all possible attack on wireless sensor networks, one of the specific types is wormhole attack in which the attacker does not need to exploit any nodes in the network and it can be done by the route establishment process. MHA is a method based on hop-count analysis in order to avoid this attack in MANETs from the standpoint of users without any special environment assumptions. Recently a new model [4] is prepared by Jen which is called “Multipath Hop-count Analysis” to prevent wormhole attack for MANETs. The MHA method is contained the following steps: Firstly, the hop-count values of all routes are calculated. In the next step, a safe set of routes are chosen for data transmission.
Ultimately, the packet is transmitted to destination through the safe routes due to decreasing the rate of packet that is sent by wormhole. One of the features of this method is that it does not require any specific hardware to well-done. It utilizes control packets as in RFC3561 and tries to modify it. Therefore, it used the RREQ packet is used for route discovery and the RREP packet is used for route reply. Generally, the main idea of this method is that when the wormhole attacks happen, the number of hops will be smaller than normal situation. As a result of this rule, the wormhole attack is detected and by using multipath method, the packet is transferred from another path.

3.6. An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks
EDWA [7] is a method that is suggested to detect wormhole attack in DSR routing protocol based on hop-count scenario. There are some assumptions which should be considered in order to use this method such as all nodes have to find their geographical information by using Global Positioning System (GPS) and also, all network nodes record each other’s authentic public keys (using TESLA for authentication). EDWA is consisted of following step which is explained sequentially

3.6.1. Detecting a wormhole by using estimate shortest path
When the destination receives a Route Request packet, it prepares a Route Reply packet to broadcast it to sender. Once a packet reaches to source node, firstly, it authenticates this packet then it extracts the location of destination from the Route Reply packet. Finally, the source estimates the shortest path through goal in terms of hop count by using Euclidean distance estimation model.

3.6.2. Identifying the malicious nodes
In order to discover a malicious node and the tunnel between them in this method, a Tracking packet is sent through destination. When each one of intermediate nodes receives the packet, they transmit the Track-Response to the first node. Finally, the source will compute shortest path to each intermediate node to identify the two malicious nodes.

The last step is involved selecting a shortest path to destination from the trusted routes that will be performed when the malicious nodes are identified and eliminated from the path [7].

3.7. Detecting Wormhole Attack in OLSR
This method [8] contain three approaches such as detecting Suspicious Links, wormhole Verification and timeouts that they are explained in the following respectively.

3.7.1. Detecting Suspicious Links
The detection approach in this method is based on that the packet latency. One of the important side effects of wormhole attack on the network is increasing delay compared to normal wireless propagation latency on a single hop. In order to find suspicious links in OLSR protocol, it is needed to apply two new control packets HELLOreq and HELLOrep. A source node transmits one HELLOreq message and set a time for expiry of this packet. When a node receives aHELLOreq, firstly save the address of sender then due to avoid overloading the network with too many HELLO answers, it holds the packet for Ni until it is scheduled for transmitting its next HELLO message. It is important to mention that the default transmission interval time for HELLO message is 2 seconds in OLSR and piggybacks the replies to this HELLO message (HELLOrep). When a requester node receives a HELLOrep, it checks an in arrival time of this packet in order to determine that whether it has arrived within its scheduled timeout interval or not. If the packet did not arrive within its scheduled timeout, the source node supposes this link as an untrusted link and not allows communicating with that node until the wormhole verification procedure archive to the end point.

3.7.2. Wormhole Verification
The mechanism that is used to detect wormhole attack is similar to HELLOreq and HELLOrep procedure in which the source node broadcasts another packet that is called Probe to all of its suspect nodes and it is waiting to receive ACKprobe from them. When the ACKprobe packet is arrived to the originator of Probe, the source node compares its evaluation from the reputation of the other end-point in the suspicious link with the evaluation of other nodes from its own reputation status. It is important to mention that the Suspicious link is not a trusted link if and only if the reputation of the remote node or the contents of the ACKprobe or both of them [8].

DAWWSN [9] is method that is designed to prevent wormhole attack in WSNs with constructing a hierarchical tree by base station - via transmitting a request packet due to find its children nodes - in which the base station is the root of tree, and the rest of sensor nodes are located in the intermediate or the leaf nodes of the tree. This method
consists of three major components such as request packet, replay packet and hopcount. When the request packet is originated by the source node, the hop-count and IDs is determined by the source node then this packet is transmitted. Each intermediate node that receives this packet should not replay it immediately. So, this packet is entered in the waiting list based on its hop-count. Once a replay timer is expired, the replay packet is prepared and sent through source node. This packet includes these fields like: The id address of the generator the replay packet (IDs), The id address of the source node that is equal to IDs request packet (IDd), The number of hop-count, The number of replayed packets (Num_Rep), The acceptance flag (Recv_Accept). Upon the replay packet is received by any nodes, each node firstly runs a timer that is called accept timer and before this timer expire, it checks its replay wait-list that is contain the id address of sender, hop-count and number of reply (Num_reply). If an entry is discovered that its ID is similar to the ID of received packet, its num_reply field will be enhanced by one else a new entry will be created and insert to the list (Num_reply=1). When the timer expires, this node prepares a packet (accept packet) that is contained its id (IDs), destination id that is equal to IDs of replay wait-list, and the Num_reply field and then it sends this packet to each entry in its reply list. Once a node receives an accept packet, it checks its replay list to find an entry that its id is similar to the received packet id. If this node finds a related entry, its feature in the list should update (Num_reply = Num_Rep + 1) otherwise the wormhole attack is detected and the following steps should be performed:

1. The received accept packet should be deleted.
2. Add the ID of the sender of the accept packet should be inserted into its (Not Accepted Packets (NAP) list.
3. Update its replay wait-list by resetting all values to zero.
4. In last step, the node should wait for another request packet or it can send another reply that is similar to the second item in its request list.

As a consequence, based on this method a hierarchical 3-way handshake routing tree can be made easily in order to detect wormhole attack for a multi-hop wireless sensor networks [9].

3.9. Wormhole Geographic Distributed Detection
Another model to detect the wormhole attack dependent on the existence of disorder in the network due to this attack is called “Wormhole Geographic Distributed Detection” [10] which is designed in 2008 by Xu. In this model to detect wormhole attack is used hop-count technic Then, the local map is re-built finally; a method is utilized to identify the irregularity in the network which is named “diameter”. The main advantage of using a distributed wormhole detection algorithm is that the proposed algorithm can approximately detect the location of a wormhole.

3.10. Special Hardware Based Approaches
The Secure Tracking of Node Encounters in Multi-hop Wireless Networks (SECTOR) is a wormhole detection technique that does not depend on time synchronization (Srdjan Capkun et.al., 2003) [3]. In this SECTOR method we uses Mutual Authentication with Distance-bounding (MAD) protocol for the estimation of distance between 2 nodes or users. MAD operates in the assumption that every node is appended with transceiver as extra Hardware. It accepts a single bit, carry out 2 bit XOR process over it and broadcast it.

3.11. DELPHI Technique
DELPHI provides a solution to the exposed wormhole attacks [11]. In this mechanism, delay per hop is determined in every path and it is proved that delay per hop for the genuine path is shorter than the wormhole path. If the path has noticeably high delay per hop, then the corresponding path is affected by wormhole.
By observing the delays of different paths to the receiver, the sender is able to detect both kinds of wormhole attacks. This method requires neither synchronized clocks nor special hardware equipped mobile nodes. The performance of DelPHI is justified by simulations. DELPHI allows the sender to check the whether there are any malicious nodes sitting along its path to the receiver and trying to launch wormhole attacks. Thus obtain the delay and the hop count information of some disjoint paths between the sender and the receiver and use this information to indicate whether a certain path among these disjoint paths is subjected to worm hole attacks.
The advantages of DELPHI are that it does not require clock synchronization and position information and it does not require the mobile nodes to be equipped with some special hardware, which in turns provides higher power efficiency.

4. SUMMARY OF WORMHOLE DETECTION METHODS
In the following Table I, there are all wormhole detection methods that are explained previously. Also, the requirements of each method are listed
<table>
<thead>
<tr>
<th>Methods</th>
<th>Synchronization</th>
<th>Authentication</th>
<th>Hop Count</th>
<th>Localization Information</th>
<th>Protocol Used for authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geographical Leashes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>RSA</td>
</tr>
<tr>
<td>Temporal Leashes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>TIK</td>
</tr>
<tr>
<td>Graph Theoretic Approach</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>LBK</td>
</tr>
<tr>
<td>Localized Encryption &amp; Authentication Protocol</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Four Type Keys</td>
</tr>
<tr>
<td>Multipath Hop Count Analysis</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>End to End Detection of Wormhole Attack in Wireless Ad Hoc Network</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>TESLA</td>
</tr>
<tr>
<td>Detecting Wormhole Attack in OLSR</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Defense Mechanism Against Wormhole Attack in Wireless Sensor Network</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>RC5</td>
</tr>
<tr>
<td>Worm Hole Geographic Distributed Detection</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Special Hardware based approach</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>MAD</td>
</tr>
<tr>
<td>DELPHI</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Table-1: Qualitative Comparison of Wormhole Detection Methods**

5. CONCLUSIONS

In this paper, we reviewed the various detection mechanisms against wormhole attacks in Mobile Ad-hoc networks. Along with the explanation of these methods we had done qualitative comparison of all the wormhole detection techniques and give a brief view of all the techniques in Table 1. Overall, a significant amount of work has been done on solving wormhole attack problem. We can’t say one solution is applicable to all situations. So there is choice of solutions available based on cost, need of security, type of network. Implementing more hardware for increasing security may lead better result, but can be costly, which may affect other networks need.
6. ACKNOWLEDGEMENT

I would like to sincerely acknowledge the encouraging efforts of all faculty members and friends. Special thanks to our guide Prof. Kamlesh Chopra for giving me the opportunity to learn.

7. REFERENCES


