Detection and Prevention of Wormhole Attack in MANET: A Survey

Shreya V Shah

Student, Computer Science & Technology,

Parul Institute of Engineering and Technology, Limda, Vadodara, India

***Abstract**:* A Mobile Ad-Hoc Network (MANET) is defined as an arrangement of wireless mobile nodes which creates a temporary network for the communication. MANET doesn't having any access point. Due to high availability of wireless devices infrastructure-less networks are using every day's life. MANET is suffering from both kinds of attacks, active and passive attacks at all the layers of network model. The lack in security measures of their routing protocols is number of attackers to intrude the network. Wormhole, attack is generated by tunnels creation and it results in complete disruption of routing paths on MANET. This attack can form a serious threat in wireless networks, especially against many wireless ad-hoc networks and location-based wireless security systems. There is several wormhole detection and Prevention methods in the wireless ad-hoc networks which some of them are reviewed in this paper.

Keywords: Adhoc Networks, MANET Attacks, Wormhole Attack

I. INTRODUCTION

A wireless network is the any type of computer network that uses wireless data connections for connecting network nodes. Wireless communications networks are implemented by using radio communication channels. Infra-Structure Based and Infrastructure Less Are two types of Wireless network [1-13]. The main research problem is how to provide security protection to the network topology and the routing in a MANET. The major challenges includes dynamic topology, decentralized control, limited resources, and the lack of information dissemination control.

Many Applications runs in untrusted environments which requires secure communication and routing such as, Military Arena, Provincial level, Personal Area Network, Bluetooth and Commercial Sector etc [13].There are some challenges of MANETs like Quality of Service (QoS), security, scalability, power control and performance measurement[16].

There are two different kind of attacks in MANET, External Attack: External attacks are carried out by nodes that do not belong to the network. It causes congestion and sends false routing information. It also causes unavailability of services. Internal Attack: Internal attacks occurred from the nodes that are part of the network. In this attack the malicious node gains unauthorized access and pretend as a genuine node. It can also analyze traffic between other nodes and may participate in other network activities [16]. wormhole attack, black hole attack, grey hole attack, flooding, replay attack, DoS (Denial of Service) attack, Man-in-middle attack and evas dropping attack[16] are different types of attacks form in MANET and create trouble in network topology which trouble upper layer Applications.

II. WORMHOLE ATTACK

Figure 1 shows the working of wormhole attack. At one end of the tunnel, a malicious node captures a control packet and sends it to another collaborating node at the other end through a private channel, which rebroadcasts the packet locally. Communication between source and destination is selected through the private channel because of having better metrics e.g., less number of hops or less time, as compared to packets transmitted over other normal routes. There are mainly two phases which describes working of wormhole attack. In the first phase, the wormhole nodes involved themselves in several routes. In the last phase, these malicious nodes start exploiting the packets they receive. These nodes can confuse the protocols that depend upon location or geographic proximity of nodes, or the colluding nodes may forward data packets back and forth to each other in case of virtual tunnel so as to exhaust the battery of other intermediate nodes. Wormhole nodes can drop, modify, or send data to a third party for malicious purposes.

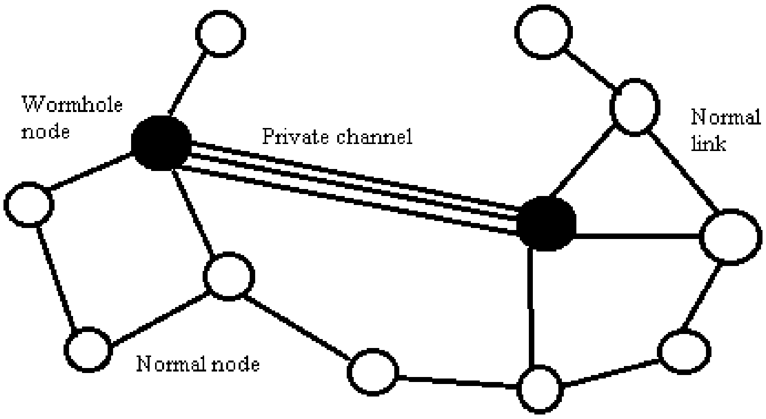

Figure 1: Wormhole attack

Tunnel in the wormhole attack can be established in many ways: in-band and out-of-band channel. This creates illusion that two end points of tunnel are very close to each other. It can be used by malicious nodes to interrupt the correct operation of ad hoc routing protocols. They can then launch a variety of attacks against like selective dropping, replay attack, eavesdropping etc.

III. WORMHOLE DETECTION TECHNIQUES:

A. *Packet Leashes* [10]

Numerous methods were proposed using a packet leash technique for the detection of the wormhole attack. The packet leash is the method that defends against the wormhole attack. The leashes can be grouped either into geographical or temporal. In geographical leashes, all nodes should have knowledge of its own location in the network and secure synchronized clock. Whenever a sender sends the data packet, it includes its own recent location and transmission time Directional antenna detects the existence of wormhole nodes. In this method, directional information is shared between source and destination. The destination can detect the wormhole by comparing the received signal from the malicious nodes and directional information from the source. If the both the signals from the source and intermediate nodes are different, then the wormhole link is detected.

B. *Using Directional Antennas* [10]

This method used an special hardware called directional antenna at each mobile nodes antennas to defend against wormholes and maintain an directional scheme ie sender node sends packets in a given direction and receiver packet will get that packet from the opposite direction whole communication will performed only when the directions of both pairs match, the neighboring relation is confirmed .

This approach work only when system has only two end points does not prevent multiple endpoint attacks. Directional errors are possible.

C. *Wormhole Geographic Distribution Technique* [8]

WGDD algorithm detects the wormhole attack based on the damage caused by them and the parameter used for wormhole detection is hop count. According to the hop count measured, it reconstructs the mapping details in each node and finally it exploits diameter feature to detect distortions caused by malicious nodes. WGDD algorithm is effective in finding the exact location of the wormholes.

D. *True Link: A Time Based Mechanism*[8]

True Link verifies whether there is a direct link for a node to its adjacent neighbor. Wormhole detection using TrueLink involves 2 phases namely rendezvous and validation. The first phase is performed with firm timing factors in which nonce exchange between two nodes takes place. In the second phase, both the nodes authenticate each other to prove that they are the originator of corresponding nonce. The major disadvantage is that TrueLink works only on IEEE 802.11 devices that are backward compatible with a firmware update. A round trip time (RTT) approach is emerged to overcome the problems in using additional hardware. The RTT is the time taken for a source node to send RREQ and receive RREP from destination. A node must calculate the RTT between itself and its neighboring nodes. The malicious nodes have higher RTT value than other nodes. In this way, the source can identify its genuine and misbehaving neighbors. This detection technique is efficient only in the case of hidden attacks.

E. *Beacon Nodes scheme* [10]

Beacon node scheme based on a special type of node ie Beacon Node that’s behave like wormhole detector. Beacon node generate alarm message to each of base station if its catch a wormhole node within their range .Main disadvantage of beacon node scheme that its use GPS system to find location of another beacon node.

F. *Hop Count Analysis Scheme* [10]

This method selects routes and "avoids" rather than "identify" the wormhole. This method first examines the hop-count values of all routes. Then they choose a safe set of routes for data transmission.

G. Neighbor node analysis approach

Neighbor node analysis approach analyze the neighboring nodes so as to check the authenticity of the nodes for secure transmission of data over the network. According to this approach a node will request to its neighboring nodes and perform a request and response mechanism. The node will maintain the table to track the timeout. If the reply time is not accurate there is an attack in the network. All the intermediate nodes are analyzed to detect the presence of wormhole attack using AODV protocol in MANET.

H. *Watchdog Technique* [8]

To identifies misbehaving nodes and avoids routing through theses nodes, watchdog and path rater. In this technique, watchdog identifies misbehavior of nodes by copying packets and maintained a buffer for recently sent packets. The overheard packet is compared with the sent packet, if there is a match then discards that packet. If the packet is timeout, increment the failure tally for the node. And if the tally exceeds the thresholds, then node will misbehave.

IV. WORMHOLE PREVENTION TECHNIQUES:

A. *Path tracing Approach:*

There are two phases in Path tracing approach as described below.

Phase I

The source node floods the route request (RREQ) packets through immediate neighbours towards destination. When it reaches the destination, it sends back route reply (RREP) in the reverse path. The path details are stored in the DSR routing cache. In order to detect the wormhole, we optimize the general DSR header by adding extra fields. Prior per hop distance field, per hop distance field and timestamp fields are added to the header of each packet. We consider both prior per hop distance and per hop distance so as to compare the difference between the two distances. If the difference is too large that exceeds the maximum threshold value, then wormhole is detected. All nodes that participate in the routing mechanism perform this operation.

Phase II

Each node in the network has to perform four major operations to detect the wormhole attack.

1. Compute per hop distance and compare it with the prior per hop distance.

2. Check whether the difference between prior per hop distance and per hop distance is larger than the maximum threshold value.

3. If it is larger, then the wormhole is detected and it is informed to all other nodes in the networks to provide wormhole alertness.

4. For the confirmation of wormhole attack, the number of time a link is used in a path is also checked in addition to comparison of per hop distance.

5. If DBC - DAB > RTh and FAcount > FATh then it is a wormhole link.

B. *Defense Mechanism Against Wormhole Attack*

DAWWSEN 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 willbe 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 waitlist, 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.

V. CONCLUSION AND FUTURE WORK

In this paper, we reviewed the various detection and prevention mechanisms against wormhole attacks in wireless 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.

Conflict of interest: I declare that I have no conflict of interest.

Ethical statement: I declare that I have followed ethical responsibilities.

REFERENCES

[1] Anal Patel, Nimisha Patel, Rajan Patel "Defending Against Wormhole Attack in MANET", Fifth International Conference on Communication Systems and Network Technologies, 978-1-4799-1797-6/15 $31.00 © 2015 IEEE, 2015

[2] Muhammad Imrana, Farrukh Aslam Khanb, Tauseef Jamala, Muhammad Hanif Durada "Analysis of Detection Features for Wormhole Attacks in MANETs", ScienceDirect, 2015

[3] Aarfa Khan, Prof. Shweta Shrivastava, Prof. Vineet Richariya "Normalized Wormhole Local Intrusion Detection Algorithm (NWLIDA)", International Conference on Computer Communication and Informatics, 978-1-4799-2352-6/14/$31.00 ©2014 IEEE,2014

[4] Neha Agrawal,Nitin Mishra "RTT based Wormhole Detection using NS-3", Sixth International Conference on Computational Intelligence and Communication Networks, 978-1-4799-6929-6/14 $31.00 © 2014 IEEE,2014

[5] Ms Neha Choudhary, Dr Sudhir Agrawal "Analysis of Worm-Hole Attack in MANET using AODV Routing Protocol", SSRG International Journal of Electronics and Communication Engineering (SSRG-IJECE) – volume1 issue10, Dec 2014

[6] Devendra Singh Kushwaha, Ashish Khare, J. L .Rana "Improved Trustful Routing Protocol to Detect Wormhole Attack in MANET", International Journal of Computer Applications (0975 – 8887) Volume 62– No.7, January 2013

[7] Sweety Goyal, Harish Rohil, "Securing MANET against Wormhole Attack using Neighbor Node Analysis", International Journal of Computer Applications (0975 – 8887) Volume 81 – No 18, November 2013

[8] Yashpalsinh Gohil, Sumegha Sakhreliya, Sumitra Menaria "A Review On: Detection and Prevention of Wormhole Attacks in MANET", International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013

[9] Yudhvir Singh, Avni Khatkar, Prabha Rani, Deepika, Dheer Dhwaj Barak "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks", Third International Conference on Advanced Computing & Communication Technologies 978-0-7695-4941-5/12 $26.00 © 2013 IEEE, 2013

[10] Vikaskumar Upadhyay,Rajesh Shukla "An Assessment of Worm Hole attack over Mobile Ad-Hoc Network as serious threats", Int. J. Advanced Networking and Applications Volume: 05 Issue: 01,2013

[11] Vandana C. P, Dr. A. Francis Saviour Devaraj "WAD-HLA: Wormhole Attack Detection Using Hop Latency and Adjoining Node Analysis in MANET", International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 3, March – 2013

[12] Teerawat Issariyakul, Ekram Hossain, "Introduction to Network Simulator NS2", ISBN 978-1-4614-1405-6, DOI 10.1007/978-1-4614-1406-3, © Springer Science+Business Media, LLC 2012

[13] D. Helen, D. Arivazhagan "Applications, Advantages and Challenges of Ad Hoc Networks", Journal of Academia and Industrial Research (JAIR) Volume 2, Issue 8 January 2014

[14] Nidhi Nigam,Vishal Sharma,Mahesh Malviya "A Novel Approach for Wormhole Detection in MANET", International Journal of Computer Applications (0975 – 8887) Vol.63(7), 2013

[15] Priyank Nayak, Akshay Sahay, Yogadhar Pandey"Detection and Prevention of Wormhole Attacks in MANETs using Detection Packet", International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013

[16] Priyanka Goyal, Vinti Parmar, Rahul Rishi "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, January 2011