A Method for Preventing Wormhole in MANET

Pardeep Singh[1] Hemant Sethi[2]

[1]Research Scholar

[2]Department of Computer Science & Engineering

[1,2]Maharishi Markandeshwar University, Ambala

Abstract— *A Mobile Ad hoc Network (MANET) is a collection of self-configurable mobile nodes that connected through wireless links. Each node in MANET can work as a sender or receiver or as a router. Communication in the network depends upon the trust on each other. Security in MANET is the most important aspect for the basic functionality of network. The dynamic topology of MANET's allows any node to join and leave network at any point. In wormhole attack, illegal node tunnels the packets from its location to the other illegal node. To detect the wormhole in network I use the digital signature. Digital signature is the verification technique.*

Keywords— MANET, AODV, Wormhole, Digital Signature, Directional Antennas

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a collection of mobile nodes that form a temporary network without the aid of any fixed infrastructure. Due to absence of any kind of fixed infrastructure and open wireless medium security implementation is difficult. In MANET each node functions as a host as well as router, forwarding packets to another node in the network. MANET is vulnerable to various kinds of attacks. Wormhole attack is one of them. In this attack two malicious nodes that are far apart from each other are connected by nodes, called a tunnel and giving an wrong information that they are neighbors.

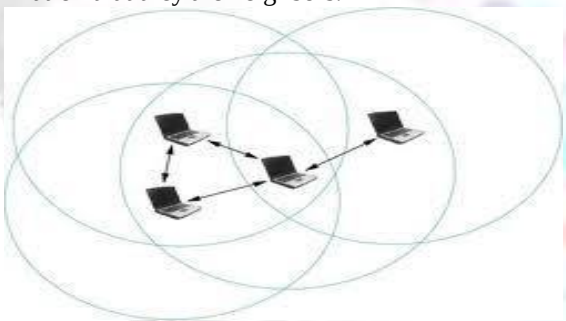

Fig. 1: MANET Network [7]

AODV is an on demand distance vector routing protocol. In on demand routing a route is established between nodes only. There is no fixed existing route. Whenever a node needs to send data it has to initiate route discovery process. Route discovery process consists of two messages: Route Request (RREQ) and Route Reply (RREP). The source node broadcasts the RREQ messages to its neighbors. In response to RREQ, either the destination node replies or intermediate node having the route to destination. Validity and freshness of route is decided by destination sequence number. If destination sequence number is higher than earlier (before) than route is considered valid. Source node selects the path for data packets transmission from which it received RREP first. Further received RREPs are discarded.

II. WORMHOLE

Wormhole attack is where a pair of colluding nodes that are located at distance are connected by a tunnel and giving an illusion that they are linked nodes. Each of these nodes receive route request and sends it to the other destination colluding node via tunnel. By using this extra tunnel, these nodes advertise that they have the shortest path through them. Once this link is connected, the attackers may choose each other, which then lead to an exchange of data packets through the wormhole tunnel. In this attack, two separate node located at distance can collude together using either wired link or directional antenna and give an impression that there are only one hop away.

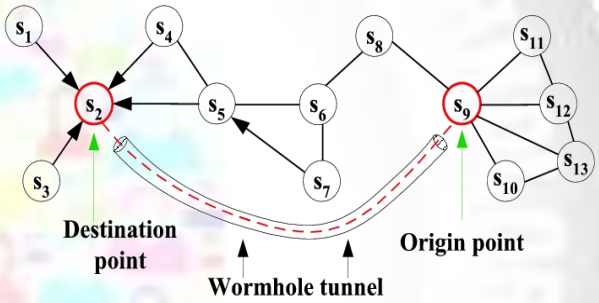

Fig. 2: Wormhole in Network [10]

Wormhole attack can be launched in hidden or in participation mode. Attack in participating mode is more difficult, yet once it is launched, itis also hard to detect. MANET faces several challenges.

They include: 1) Multicast Routing – Designing of multicast routing protocol for a constantly changing MANET environment.2) Quality of service (QoS) – Providing constant QoS for different multimedia services in frequently changing environment.3) Internetworking – Maintain communication between wired network and MANET.4) Power Consumption – The necessity of conservation of power and discovery of power saving routing protocol.

III. LITERATURE SURVEY

In [2] the existing system implements EAACK scheme which involves digital signature for safer exchange of packets. This is implemented by both Digital Signature Algorithm (DSA) and RSA. EAACK scheme depends on acknowledged packets. So, it's necessary to reduce the network overhead caused by digital signature. Network overhead increases when number of malicious node in network increases, because the count of acknowledged packet increases. Thus to reduce network overhead Hybrid key cryptography technique is used.

In [3] authors presented two phase mechanism, the first phase delay/hop count and verification of digital signature information is collected. In the second phase analyzes the collected information obtained in first phase to detect whether there is any wormhole attack present or not. The reason behind is that under normal situation ,the delay a packet experiences in propagating one hop should be similar along each hop along the path. However, under a wormhole attack the delay may unreasonably high or low, since there are in fact many or no hops between them.

In [5] authors protect from wormhole attack used the scheme called multihop count analysis with verification of legitimate nodes in network through its digital signature. Destination node analyzes the number of hop count of every path and selects the best path for replying. For checking the authenticity of the selected path, used verification of digital signature of all sending nodes by receiving node. If there is no malicious node between the path, from source to destination, then source node creates a path for secure data transfer.

In [7] authors developed a protocol using directional antennas to prevent wormhole attacks. Directional antennas are able to detect the angle of arrival of a signal. In this protocol, two nodes communicate knowing that one node should be receiving messages from one angle and the other should be receiving it at the opposite angle i.e. one from west and the other at east.

In [9] Khalil et. al. propose a protocol "LiteWorp" for wormhole attack discovery in static networks. In this protocol once deployed, nodes obtain full two-hop routing information from their neighbors. While in a standard ad hoc routing protocol nodes usually keep track of who their neighbors are, in LiteWorp they also know who the neighbors of neighbors are. This information can be exploited to detect wormhole attacks. After authentication, nodes do not accept messages from those they did not originally register as neighbors. Also, nodes observe their neighbors behavior to determine whether data packets are being properly forward by the neighbor, a so-called watchdog approach. The adds an interesting wormhole specific twist to the standard watchdog behavior. Nodes verify that all packets are forwarded properly.

In [11] authors presented the wormhole detection which is based on the smallest hop count estimation between source and destination. If the hop count of a received shortest route is much smaller than the estimated value an alert wormhole attack is raised at the source node. Then the source node will start a wormhole tracing procedure to identify the two end points of the wormhole. Finally, a legitimate route is selected for data communication.

IV. PROBLEM STATEMENT

Directional antennas are able to detect the angle of arrival of signal. In this, two nodes communicate knowing that one node should be receiving messages from one direction and the other should be receiving it from the opposite direction. The protocol fails if the attacker is placed very tactfully between two directional antennas.

V. PROPOSED SOLUTION

To avoid the wormhole attack in directional antenna, digital signatures are used. In mobile ad hoc network it is assumed that each legitimate node shares the digital signature of every node in the network and malicious node does not have its own digital signature. If a sender wants to send the data to destination then it firstly checks the direction. If direction is ok then broadcast the route request (RREQ) packet in the network. The route request (RREQ) packet header contains the information of visiting node (node-id) in node information column and hop count column which contains the number of visiting nodes used in path. When the sender broadcasts a route request packet, every time direction is checked, then it adds its node-id in node information column and starts its hop counter with one. All the intermediate nodes add its node id and increment the number of hop count by one until it reached at destination. The intermediate nodes use the forwarding route request (FRR) technique. Intermediate nodes do not broadcast the route request. The destination node used a scheme called multi path hop count analysis (MHA) in which destination node received all route requests following different path within a certain time period called time to live (TTL) period and discard all RREQ which reached after TTL get expired. Now, destination node analysis the number of hops used by different paths and selects the optimal route for unicasting the route reply packet (RREP). To check the authentication of selected path, Destination node unicasts the (RREP) packet, whose header contains the id of all nodes traversed on that path and the digital signature of the receiving node received route reply (RREP) packet, it checks the direction if direction is ok and then compare the digital signatures of previous node, which are in the signature column of RREP header, from its database which contains the signatures of all nodes in the network. If the sending node is legitimate then the digital signature of sending node should be identical to the digital signatures which are in the database of receiving node. Digital signature of two nodes in signature column of packet-header should not be identical and there is no blank space in place of signature in signature column of packet header. If all conditions do satisfy then the sending node is a legitimate node so receiving node also add its signature in signature column of header and again unicast route reply (RREP) packet to next node. The process is repeated again and again. When the RREP packet reached at source node, source node also verifies the signature of previous nodes. If the route reply reached at source is legal then source node creates a secure and authenticated path between source and destination. If the packet header contains the duplicate digital signature of previous node or black space in signature column then there is malicious node in the path and node which receives the reply from malicious nodes inform to all other nodes about malicious node and discarded the route reply. All other nodes which receive the information about malicious node need to update their database.

A. Algorithm

Algo(Wormhole_attack_detection)
Input: Number of nodes n, Source node, Destination Node;

Output: Detection of Wormhole attack, Find the Best Path for routing;
Begin
Create the network for the input node
Define Source node & Destination Node
Find the Direction of each mobile node and their neighbor's node
For source to destination
Send Route Request to next neighbor
End for
For destination to source
Send RREP to pervious node
Verify directions
Verify digital signature
End for
End

VI. Simulation and Result

For the simulation MATLAB 7.10.0.499 simulator is used. Here the network of 50 nodes is created (as shown in Figure 3). All the nodes are randomly placed in network.

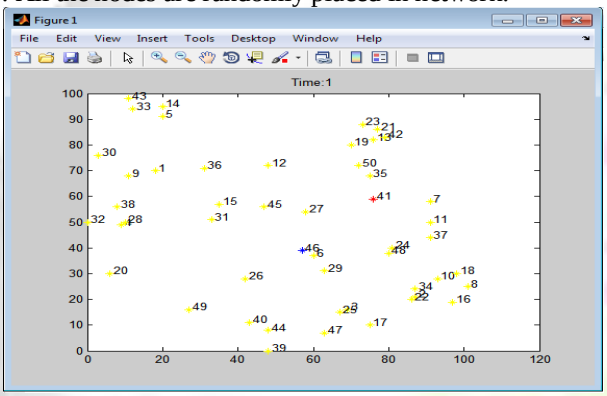

Fig. 3: Dynamic Networks

In this figure 35 is the source node and 7 is the destination node. The 35 node broadcasts the route request to all neighbor nodes. There is a region 100*120 and in this region 1 to 50 nodes placed randomly. The node id 7 is a source node that wants to send the data to node 35. The node 7 broadcasts the route requestpacket with in communication range. The neighbor nodes received that route request packet and if its destination node then it will do RREP to source node, otherwise that node adds its id in packet header column and hop count increments by 1 and forwards it to next neighbor node. This process is going on when the packet reaches at the destination node.

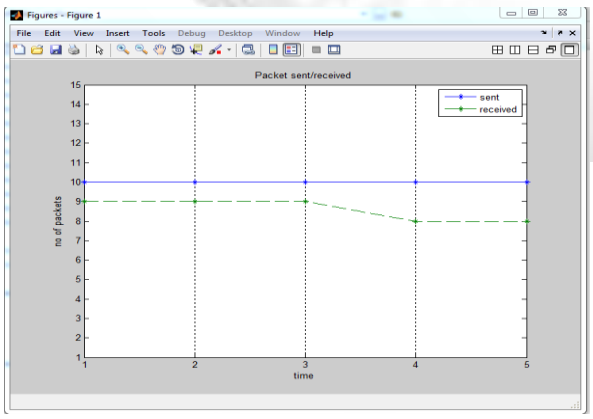

Fig. 4: Proposed Scheme with digital signature

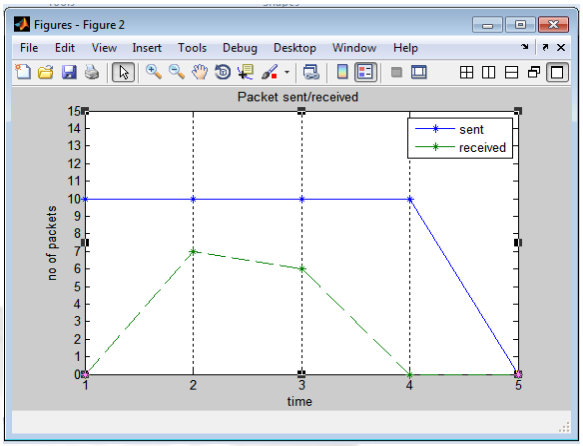

Fig. 5: Existing scheme without digital signature

Table 1 (given below) describes the above both graphs (i.e Existing scheme without digital signature and Proposed scheme with digital signatures) in terms of packets sent/received by the destination when the simulation runs for 5 number of rounds and 10 packets have been sent in each round.

Round Number	Packets Received (with Digital Signature)	Packets Received (without Digital Signature)
1	9	0
2	9	7
3	9	6
4	8	0
5	8	No path found

Table 1: Packet Received Scenario (10 Packets sent in each round)

VII. Conclusion and Future Work

Mobility is the main and common issue in network. Due to their dynamic nature, it will require higher security. As digital Signature is used to secure a connection in MANET. But this research provides an efficient scheme that detects the malicious node in the network using digital signature as well as by finding the direction of each mobile node and the neighbor's nodes. Abest path is chosen from the given paths and connection is established between nodes.

Security has become a primary concern in order to provide secure communication between mobile nodes in an aggressive environment so that MANET is more vulnerable to attacks and more chances to path break so there is more work need to be done on routing and security considered.

References

[1] Tapan P. Gondaliya et.al. Intrusion detection system for Attack prevention in Mobile Ad hoc network. IJARCSSE, vol 3, April 2013.
[2] B. Suruthiet. al. An Enhanced Intrusion Detection System for MANET using Hybrid Key Cryptography. IJCSIT, vol.5(2), 2014.
[3] Anil kumarfatehpuria et.al. An Efficient Wormhole Prevention in MANET through Digital Signature. IJETAE, volume 3, Issue 3, March 2013.
[4] PoonamDabas et.al. A Novel Technique for the Prevention of Wormhole Attack. IJARCSSE, volume 3,Issue 6,june 2013

[5] Rutvij H. Jhaveri et.al. MANET Routing Protocol and Wormhole Attack against AODV. IJCSNS vol. 10, Issue 4, April 2010.
[6] Sjalinijain et.al. Detection and Prevention of wormhole attack in mobile ad hoc networks. IJCTE, vol 2 No.1, February 2010.
[7] SweetyGoyal et.al. Securing MANET against Wormhole Attack using Neighbor Node Analysis. IJCA, volume 81, Issue 18, Nov 2013.
[8] L. Hu, D. Evans Using Directional Antennas to Prevent Wormhole Attacks, Proceedings of the 11th Network and Distributed System Security Symposium, pp. 131-141, 2003.
[9] Pallavi Sharma et.al. Prevention of Wormhole Attack in Ad hoc Network. ICEICE, No 5, Dec 2011.
[10] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach, IEEE Communication Society, WCNC 2005.
[11] Xia Wang, Johnny Wong, "An End-to-end Detection of Wormhole Attack in Wireless Ad hoc Networks", 31st Annual International Computer Software and Applications Conference IEEE, 2007.