Prevention of Wormhole Attack in Ad-Hoc Network

Pallavi Sharma Prof. Aditya Trivedi

ABV-IIITM, Indian Institute of Information Technology and Management, Gwalior - India

ABSTRACT

Ad hoc networks are vulnerable due to their structure less property. A Mobile Ad-Hoc Network (MANET) is an infrastructure less collection of mobile nodes that can arbitrarily change their geographic locations such that these networks have dynamic topologies and random mobility with constrained resources. They also have capability of network partition. The Wormhole attack is the most attention seeking attack in ad hoc networks; it consists of two malicious nodes and a tunnel between malicious nodes. In wormhole attack, attacker records the packets at one location and tunnels them in another location in same network or in different network. In this paper, we present a mechanism which is helpful for detection and defend against wormhole attack in ad hoc network is"multipath hop counting analysis" (MHA) in which accepting all route request at destination node with in a fixed time period called time to live (TTL) period and then verification of digital signature of sending node by receiving node because each legitimate node in the network contains the digital signature of every other legitimate nodes of same network. In proposed solution, if sender wants to send the data to destination, firstly it creates a secure path between sender and receiver with the help of multipath hop count analysis with verification of digital signature. If there is presence of any malicious node in between the path then it is identified because malicious node does not have its own legal digital signature.

Keywords

Mobile ad hoc network, wormhole attack, routing Protocols, digital signatures, multipath hop count analysis (MHA).

1. INTRODUCTION

All The promise of mobile ad hoc networks to solve or disputing real world problems continues to seek the attention from industrial and academic research projects. The most focus area of research in mobile ad hoc networks is to provide a trusted environment and secure communication. There are several applications of ad hoc network which need highly secure communication. Some of the example of these applications are: military or police networks, business operations like oil drilling platforms or mining operations and emergency response operation such as after natural disaster like a flood, tornado, hurricane and earthquakes.

There are basically three types of routing protocols: reactive routing protocol, proactive routing protocol and hybrid routing protocol. Here, we emphasis on AODV and DSR routing protocols which are the part of reactive routing.

In this paper we define the wormhole attack and a new general and effective mechanism for detection and then defend against wormhole attack. In wormhole attack the attacker record the packets (bits) at one location and tunnel them in another location in same network or in different networks. The attacker can transfer each bit directly, without waiting the entire packet. It is very difficult to find out the location of wormhole attack without having the cryptographic key or without knowing the infrastructure of routing protocols. Here, we focus on defend against wormhole attack in routing protocols.

In our proposed solution, it is assumed that all legitimate nodes must know the digital signature of every other legitimate node in the network. If a sender wants to send the data to destination then it firstly broadcast the route request (RREQ) packet in the network. The route request (RREQ) packet header contains the information of visiting nod (node-id) in node information column and hop count which contains the number of nodes used in path. When the sender broadcast a route request packet then it adds its node-id in node information column and starts its hop counter with one. All the intermediate node add its node id and increment the number of hop count by one until it reached at destination. The destination node received all route requests which arrived using different path within a certain time period is called time to live (TTL) period and discard all RREQ which reached after TTL. Now, Destination node analyze the number of hops used in every route and select the route for unicast which used average number of hops in route request (RREQ), this process is called multipath hop count analysis (MHA). Destination node avoid to select the route which have minimum hop count because the route using minimum number of hop count may contains malicious node due to their encapsulation and tunneling property. To check the authentication of path selected by destination node for replying route request we used verification of digital signature in which destination node unicast the route reply (RREP) packet, whose header contains the column of node id and the digital signature column in which each visiting node adds its digital signature. when receiving node received route reply (RREP) packet, it verifies the digital signature of previous node, if the signature of previous nodes are legal, there is no identical signature of two previous nodes and there is no blank space in signature column of header, then receiving nodes verified that received reply RREP packet is genuine and adds its own digital signature in signature column of packet header and unicast the reply to next node. The process is repeated until the route reply reached till source. When route reply packet (RREP) reached at source, source node also verifies the signatures of all previous nodes. It creates an authenticated path between source and destination for data transfer.

The organization of this paper is as follow: Section II describes the related work. Section III explains wormhole attack in routing protocols. Section IV explains proposed scheme. Section V describes simulation and results and section VI describes the conclusion and future work.

2. RELATED WORK

A. Packet Leashes

It is the excellent mechanism for detection of wormhole attack [2]. There are two types of packet leashes: One is temporal leashes which are related to time of sending and receiving packets from one node to another node. Another one is geographical leashes which are related to geographical location of nodes.

1) Geographical Leashes: It requires location determination (eg. GPS hardware) and all nodes contains a clock which is loosely synchronized. In geographical leashes when one node sends a packet to another node then it includes its own location *ps* and time on which it sends a packet *ts*. The receiving node compare the value of sending packet with its own location *pr* and time at which it receives packet *tr*.

2) *Temporal Leashes:* In temporal leashes all nodes must required a tightly synchronized clock. The time synchronization can be achieved now with off-the-shelf hardware based on LORAN-C [3], WWVS [4], and GPS [5][6].

But the problem faced in packet leashes is that it is inaccurate due to unpredictable processing time and channel availability. It does not prevent DoS attack against route establishment.

B. Lite Worp

Liteworp [7] also provides a defense mechanism against wormhole attack; it uses secure two hop neighbor discovery and local monitoring of traffic by using guard node. It also has additional features that provide a technique to isolate the malicious node from the network. But there is some restriction in liteworp that it requires extremely accurate clock, assuming no delay in network apart from propagation delay and exact measurement of angle of reception.

C . Womeros

Womeros [8] is the framework for defending against worm-hole attack which contains two phase: one is suspicious and another is conformation. The first phase applies inexpensive techniques and utilizes local information that is available during the normal operation of wireless nodes. Advance techniques in the second phase are adapted only when wormhole attack is suspected. If there is no presence of malicious node in the network after applying suspicious phase technique then there is no need to waste consumption and communication resources by applying conformation technique.

D. MobiWorp

The works in Mobiworp [9] focus on the problem of locally isolating the malicious node. It uses a secure central authority for global tracking of node position, but if the mobility of nodes increases then it degrades the performance of Mobiworp.

E. Directional Antennas

These antennas [10] are used to prevent wormhole attack. Each node in the network shares a secret key with every other node and broadcasts HELLO messages to discover its neighbor using directional antenna in each direction.

E. Worm-IT

Worm-IT [11] is a new intrusion tolerant group communication system with a membership service and a view synchronous atomic multi cast primitive. The system is intrusion tolerant in the sense that it behaves correctly even if some nodes are corrupted and become malicious. It is based on novel approach that enhances the environment with special secure distributed component used by protocols to execute surely a few crucial operations.

3. WORMHOLE ATTACK IN ROUTING PROTOCOL

Mobile ad hoc routing protocol divide into two major categories [1]:

Table driven routing protocol:

In these protocols all nodes consists up-to date routing information, so they update their table with in a fixed time period. The OLSR is the example of these proactive routing protocols.

On-Demand routing protocol:

In these routing protocols, the route is created only if required. Nodes do not update their information within a fixed time interval. These protocols find route on demand by flooding the network with route request packets from source to destination. AODV and DSR are the example of reactive routing protocols.

Figure 1 shows the scenario of the wormhole attack. There are two malicious nodes which are far apart from each other in a similar network or may be in different networks which are connected with each other through a tunnel and pass the data packets through tunnel where they are replayed [14]. The tunnel is either the wired link or a high frequency links. The wormhole attack can actually be helpful if used for forwarding all packets. It can be launched without having the cryptographic keys. Some harmful effects of wormhole are as follow: selectively drop data packets, routing disruption in which attackers prevent discovery of legitimate route and traffic analysis for information leaking. Now, let us discuss that how wormhole attack can be launched in wireless network: It can be launched by four ways [12]:

1) *Packet Encapsulation:* In which one malicious node encapsulates the route request and sends it to colliding node which decapsulate it and forwards the route request (RREQ) packet.

2) *Out-of-Band:* In Out-of-Band, two malicious nodes sends route request (RREQ) between them by using the long range directional wireless link or direct wired link.

3) *High-Power-Transmission:* In high power transmission a malicious node get a route request (RREQ) and broadcast that request with high power level. Any other node that hears the high power broadcast must be a malicious node so it receives that route request and again rebroadcast towards the destination.

4) *Packet Relay:* In packet relay two malicious nodes relay packet between two nodes which are far apart from each other and convenience these nodes that they are neighbor.

4. PROPOSED SOLUTION

To avoid the wormhole attack 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 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 broadcast a route request packet then it adds its node-id in node information column and starts its hop counter with one. All the intermediate node add its node id and increment the number of hop count by one until it reached at destination. The destination node used a scheme called multi path hop count analysis (MHA) in which destination node received all route requests which reached at destination following different path within a certain time period is called time to live (TTL) period and discard all RREQ which reached after TTL. Now, destination node analysis the number of hops used by different path and select the route for unicast route reply packet (RREP) which used average number of hops because the route using minimum number of hop count may contains malicious node due to their encapsulation and tunneling property. To check the authentication of selected path, Destination node unicast the (RREP) packet, whose header contains the column of

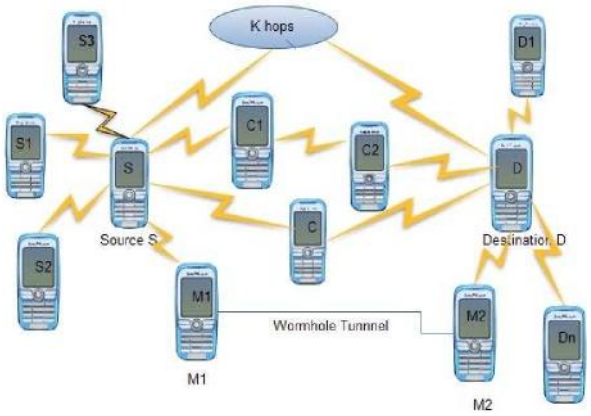

Fig.1 Wormhole attack in mobile ad hoc network

node id, which contains the id of all nodes used in that path and the digital signature column in which each visiting node adds its digital signature. When receiving node received route reply (RREP) packet, it compare the digital
signatures of previous nodes, 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 condition is satisfy then 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 until that route reply (RREP) reached till source node. 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 there is presence of any malicious node in the path which receives route reply (RREP) packet and unicast it to next node, the node that received packet from malicious node found that signature column of packet header either contains duplicate digital signature of any previous node or a blank space in place of digital signature because the malicious node does not have its own digital signature. So the node that received the RREP packet from malicious node discard the reply and inform to all node in the network about the malicious node and all other nodes update their database.

Here, let us discuss how to find out average number of hop count. Let take an example, destination node received five route request which followed different path from source to destination with in a fixed time period called time to live period (TTL). The hop counts of first to five routes are three five six five seven respectively. Now, destination node used a scheme called multipath hope count analysis (MHA) in which it analysis the minimum average number of hop counts. Here, the average number of hop count is five, so it used the path which have five hop counts and discard all other requests. It does not used the route which have hop count less than the average number of hop count like route one have only three hop count, it may contain malicious node because malicious nodes used encapsulation and tunneling property.

A. Algorithm:

At Source: -
If (Send any packet P)
a. Add node information (node-id) of visiting node in node id column of packet header.
b. Starts hop count with number one in hop count column.
If (any malicious node in route)
Add malicious node information.
Broadcast packet P by using routing protocol;
Call routing protocol.
If (Received acknowledgment (RREP))
Verify the digital signature of all nodes which are used in unicasting of route reply (RREP).
If (all signatures are legal and different column of packet header)
Establish a path for data transfer.
If (Any intermediate or destination node is malicious node)
Then add the malicious node information in malicious node column in the packet header and again rebroadcast Route request (RREQ)

At Intermediate node 'I':-
If ('I' is not a destination)
If (Received a route request (RREQ) packet P in broadcasting process)
a. Add its node id in node id column and increment the hop counter by one in hop count column of header
If (Received a route reply (RREP) packet P in unicasting process)
Verify the digital signature of previous node
a. If (legal signature)
Then it also add its signature in signature column of packet header and unicast it to next node using routing protocol.
Call routing protocol.
b. If (signature of two previous node is identical or absence of signature of any previous node)
Drop request packet and inform to all nodes about the malicious node

At Destination: -
If (received a packet P)
1. Received all route request (RREQ) packet which arrived by followed different paths and having different number of hops in a particular time interval called TTL.
2. select a path for unicasting route reply, which have average number of hops, because the root which contains less hop count than average number of hops may contain malicious nodes due to their encapsulation and tunneling property.
3. Then, add its digital signature in signature column and reply to source through same path through which it received a route request.
4. Establish a path for data transfer.

Assumption: It is assumed that every legal node in network must have digital signature of every other node in same network [13].

When a new node enters in network it exchanges its digital signature with every nodes of the network with the help of central authority which works ass offline.

5. SIMULATION AND RESULTS

To evaluate the effectiveness of proposed scheme, we simulate the scheme using qualnet version 5.0. In simulation we vary the number of nodes from 20 to 70, carried out simulation 20 times on every scenario and get the results.

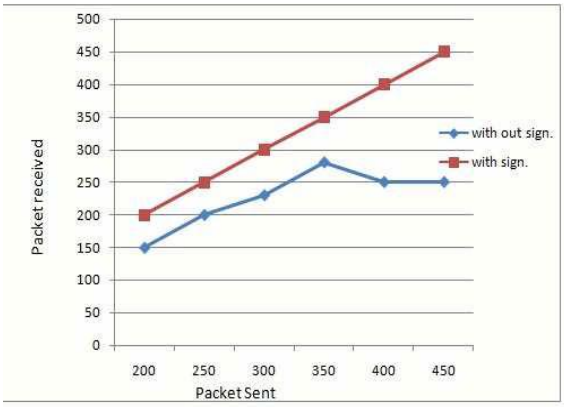

Fig. 2 comparing number of packet send and packet received with and without using digital signature.

We implement the random way point movement model for simulation in which nodes start at random position. with simulation time 600 seconds, 100*100 simulation area, maximum speed 20m/s, pause time is 10 seconds, traffic type is CBR, payload size 512 bytes, two malicious node with a tunnel.

Figure 2 shows that when there is the malicious node in the network then number of packet received by receiver is less than the packet sends by sender. When we apply digital signature scheme then packet received by receiver is equal to the packet send by sender.

Figure 3 shows the comparison of throughput, when we apply the digital signature scheme then the throughput level is increased than the previous scenario when there is no digital signature and presence of malicious node in the network. The throughput is increase with digital signature scheme because it does not allow any malicious node in between the path of data transfer. The throughput level is also increased when we increase the number of nodes.

Figure 4 shows the comparison of overhead level when we apply digital signature. The overhead is increased as we increase the number of nodes because it increases the packets in the network due to broadcast of route request RREQ again and again. All nodes contain the digital signature of every other node due to which overhead is increased.

6. CONCLUSION AND FUTURE WORK

A wormhole is one of prominent attack which is formed by two malicious nodes and a tunnel. In order to protect from wormhole attack we used the scheme called multihop count analysis (MHA) 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 authentication of selected path, we used verification of digital signature of all sending node by receiving node. If there is no malicious node between the paths from source to destination, then source node creates a path for secure data transfer.

7. ACKNOWLEDGMENT

I am thankful to ABV-Indian Institute of Information Technology and Management Gwalior, India for providing facilities and resources for this paper.

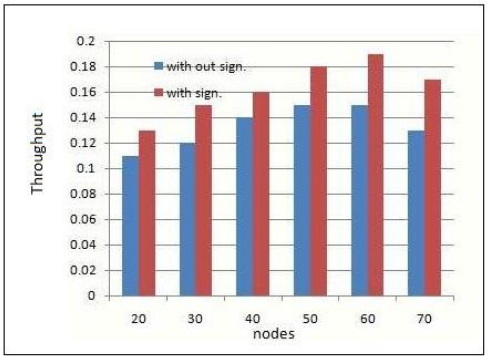

Fig. 3 Comparing throghput versus number of nodes with and without digital signature

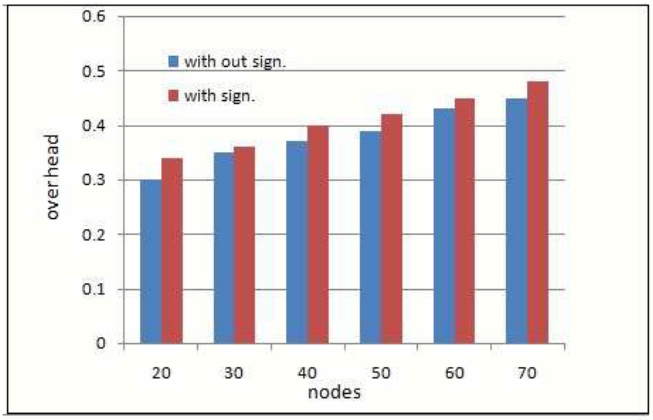

Fig. 4 comparing overhead versus number of nodes with and without applying digital signature.

8. REFERENCES

[1] M. Bouhorma, H. Bentaouit and A. Boudhir, "Performance Comparison of Ad-Hoc Routing Protocols AODV and DSR," *in Multimedia Computing and Systems, 2009. ICMCS'09,* pp. 511-514, 2009.

[2] Y.C Hu, A. Perrig and D. Johnson, "Wormhole Attack in Wireless Networks," *IEEE JSAC,* vol. 24, no. 2, Feb. 2006.

[3] David L. Mills, "A Computer-Controlled LORAN-C Receiver for Precision Time Keeping," *Technical Report 92-3-1, Department of Electrical and Computer Engineering,* University of Delaware, DE, March 1992.

[4] David L. Mills, "A Precision Radio Clock for WWV Transmissions", Technical Report 97-8-1, *Department of Electrical and Computer Engineering, university of Dalware, DE,* August 1997.

[5] Tom Clark, "Tom Clark's Totally Accurate Clock FTP Site. Greenbelt, Maryland." ftp://aleph.gsfc.nasa.gov/GPS/totally.accurate.clock/.

[6] Defense Advanced Research Projects Agency www.mil/ato/solicit/baa01-01faqv4.doc, October (2000).

[7] I. Khalil, S. Bagchi, N.B. shroff, "LiteWorp: Detection and isolation of the wormhole in static mulihop wireless network. Journal," *Acm: The international Journal of Computer and Telecommunications Networking Archive,* Vol. 51, Issue 13, September 2007.

[8] H. Vu, A. Kulkarni, N. Mittal, "WOMEROS: A new

framework for defending against wormhole attacks on wireless ad hoc networks," *in WASA 2008, LNCS 5258*, pp. 491-502, 2008.

[9] I. Khalil, S. Bagchi, N.B. Shroff, "MOBIWORP: Mitigation of wormhole attack in mobile multihop wireless networks," *in Direct Science: Ad Hoc Networks6 (2008)*, pp. 344-362, Feb. 2007.

[10] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," in *Proc. Network and Distributed System Symposium (NDSS), San Diego, USA*, Feb 2004.

[11] M. Correia, N. Ferreira, L.C. Lung, "Worm-IT -A Wormhole based intrusion-tolerant group communication system," *in Science Direct: The Journal of system and Software 80, 2007*, pp. 178-197, March 2006.

[12] M. Jain, H. Kandwal, "A Survey on Complex Wormhole Attack in Wireless Ad-Hoc Network," *in Advances in Computing, Control & Telecommunication Technologies*, pp. 555-558, 2009.

[13] E. Poornima, C. S. Bindu, SK. Munwar, "Detection and a prevention of Layer-3 Wormhole Attack on Boundary State Routing in Ad Hoc Networks," *In International Conference on Advances in Computer Engineering (ACE), Banglore, Karnataka, India*, pp. 48-53, June 2010.

[14] Azer, M. A. El-Kassas, S.M. El-Soudani, M.S, " Immuning Routing Protocols from the Wormhole Attack in Wireless Ad Hoc Networks," *Systems and Networks Communications, ICSNC '09,* pp. 30-35, 2009.