Security in AODV against Wormhole attack in MANET

Priyanka B. Patel[#], Purvi N. Ramanuj* Dr. J.S. Shah[&]

[#]*Department of Computer Science & Technology, L.D.College of Engineering, Gujarat Technological University*
Ahmedabad
Piyu_patel18@yahoo.com

[*]*Assistant Professor, L.D.College of Engineering, Gujarat Technological University*
Ahmedabad
purviramanuj@yahoo.com

[&]*Principle GEC, Gujarat Technological University*
Patan
jssld@yahoo.com

Abstract — **A mobile ad hoc networks (MANETs) is a dynamic mobile wireless network that can be formed without the need for any pre-existing wired or wireless infrastructure. Security takes crucial part in several application of MANET basic implementation of protocols used in MANET does not involve security solutions. Due to dynamic infrastructure-less nature and lack of centralized monitoring points, the ad hoc networks are vulnerable to attacks. The network performance and reliability is break by attacks on ad hoc network routing protocols. AODV is a important on-demand reactive routing protocol for mobile ad hoc networks. In Mobile ad hoc networks there are many types of attacks. Like, Spoofing attack, Sybil attack, Black hole attack, denial of service attack, and wormhole attack. We are studying Wormhole attack. In wormhole attacks, one malicious node tunnels packets from its location to the other malicious node. If source node chooses this fake route, malicious nodes have the option of delivering the packets or dropping them. In a wormhole attack, intruders tunnel the data from one end of the network to the other, leading distant network nodes to trust they are neighbours' and making them communicate through the wormhole link.**

Keywords— **Wormhole attack, ad hoc network, tunnelling, AODV, RREQ.**

I. Introduction

A mobile ad hoc network (MANET) consists of a collection of wireless mobile nodes without the use of any established infrastructure or centralised administration. Individual nodes can communicate directly only with their immediate neighbour nodes within a limited transmission range. Any communication beyond the direct transmission range relies upon the collaboration of the nodes involved. Nodes may play different roles in a communication as, for example, a source node, destination node, and intermediate node. The intermediate nodes need to forward packets for other nodes while the source node initialises a communication to the Destination. A mobile ad hoc network is an infrastructure less Network because the mobile nodes configure by themselves as paths are set by mobile nodes for transmission. [1].

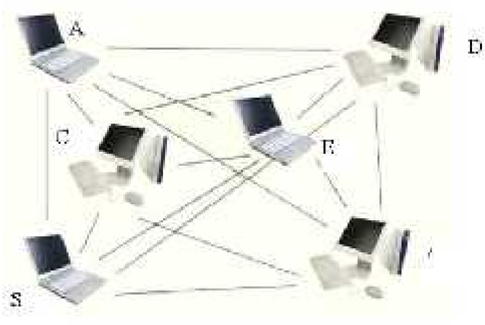

Fig.1 mobile adhoc network

Wireless ad-hoc network is promising to solve many challenging real-world problems, for example, communication in emergency response system, military field operation and oil drilling and mining Operation [2]. This paper provides analysis of wormhole attacks.

II. Routing Protocols

Many routing protocols are available for MANET. In this section, some of the frequently used routing protocols are reviewed and the threat of wormhole attacks to such protocols is considered. These routing protocols can be categorized into two types: table-driven/proactive and demand-driven/reactive [3]. DSDV, OLSR are proactive routing protocols and DSR, AODV are reactive routing protocols.

1. *AODV (Ad-hoc On-demand Distance Vector) :*

It is a pure on-demand routing protocol. For sending messages to destination, it broadcasts RREQ messages to its immediate neighbours. These neighbours in turn rebroadcast them to their neighbours. This process continues unless the RREQ message reaches the destination. Upon receiving the first RREQ message from the source node, it sends a RREP to the source node following the same reverse path [4]. All the intermediate nodes also set up forward route entries in their table. Upon detecting error in any link to a node, the neighbouring nodes forward route error message to all its neighbours using the link. These again initiate a route discovery process to replace the broken link. The AODV routing protocol is vulnerable to wormhole attack. Since the colluding nodes involved in wormhole attack uses a high speed channel to send messages, it is possible that the RREQ packet through them reaches the destination faster compared to usual path. According to this protocol, the destination discards all the later RREQ packets received, even though they are from authenticated node. The destination therefore chooses the false path through wormhole for RREP.

III. SECURITY ISSUE IN MANET

Due to the issues such as shared physical medium, lack of central management, limited resources and highly dynamic topology, ad hoc networks are much more vulnerable to security attacks [5]. Hence it is very necessary to find security solutions. In the following sections we first address attacks in ad hoc networks, and list several typical special attacks.

1) *Wormhole attack:* In wormhole attack, a malicious node in the network with the help of an external node which is far away from the malicious one establishes a tunnel between them.
In [4], the tunnel can be established in many ways e.g. in-band and out-of-band channel. By creating a tunnel between nodes they create a false impression that the two nodes are quite near to each other.

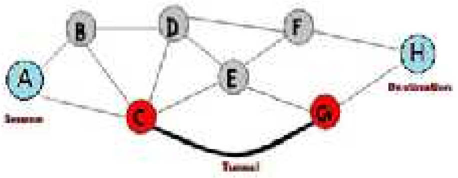

Fig. 2 Wormhole attack

Wormhole can be formed using, first, *in-band channel* where malicious node tunnels the received route request packet to another malicious node using encapsulation. Second, *out-of-band channel* where two malicious nodes employ a physical channel between them by either dedicated wired link or long range wireless link. [4]

Fig 2 indicates that node X and Y are malicious nodes and they form a tunnel between nodes. Source S sends the RREQ to A and P. Node A and Node P will forward RREQ to their immediate neighbors respectively i.e. B and X .Thereafter Node X will forward RREQ's to Y as both are malicious nodes and there is tunnel between these two nodes .The route requests will reach quickly towards destination D with route S-P-R-D. So the route with malicious node is selected rather than optimal path i.e. S-A-B-D.

2) Black hole attack: It is also known as sinkhole attack. In this attack, a malicious node attempts to suggest false path to the destination. An adversary could prevent the source from finding path to destination, or forward all messages through a certain node.

3) *Spoofing attack:* Spoofing attacks are also called impersonation attack. The adversary pretends to have the identity of another node in the network, thus receiving messages directed to the node it fakes. One of these attacks is man-in-the-middle attack. In this attack, attackers place their own node between two other nodes communicating with each other and forward the communication.

4) Denial of service attack: In this type of attack, the attacker attempts to prevent the authorized users from accessing the services. Due to the disadvantage of ad hoc networks, it is much easier to launch Dos attacks. For example, an adversary could disrupt the on-going transmissions on the wireless channel by employing jamming signals on the physical and MAC layers.

5) *Sybil attack:* The Sybil attack especially aims at distributed system environments [11]. The attacker tries to act as several different identities/nodes rather than one. This allows him to forge the result of a voting used for threshold security methods. Since ad hoc networks depend on the communication between nodes, many systems apply redundant algorithms to ensure that the data gets from source to destination. A consequence of this is that attackers have a harder time to destroy the integrity of information.

IV. WORMHOLE ATTACK IN AODV:

Wormhole attack [10] commonly associates two remote malicious nodes shown as X and Y in Fig-3. X and Y both are attached via a wormhole link and they target to attack the source node S. During path finding process, S broadcasts RREQ to a destination node D. Thus, A and C, neighbors of S, accept RREQ and transmit RREQ to their neighbors. Now the malicious node X that receives RREQ forwarded by A. It records and tunnels the RREQ via the high-speed wormhole link to its partner Y. Malicious node Y forwards RREQ to its neighbor B. Finally, B forwards it to destination D. Thus, RREQ is forwarded via S-A-X-Y-B-D. On the other hand, other RREQ packet is also forwarded through the path S-C-D-E-F-G-D. However, as X and Y are connected via a high speed bus, RREQ from S-A-X-Y-B-D reaches fist to D. Therefore, destination D ignores the RREQ that reaches later and chooses D-B-

A-S to unicast an RREP packet to the source node S. As a result, S chooses S-A-B-D route to send data that indeed passes through X and Y malicious nodes that are very well placed compared to other nodes in the network. Thus, a wormhole attack is not that difficult to set up, but still can be immensely harmful for a MANET. Moreover, finding better techniques for detection of wormhole attacks and securing AODV against them still remains a big challenge in Mobile Ad-hoc Networks.

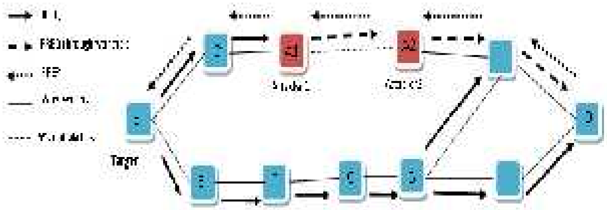

Fig :3 wormhole attack on AODV in MANET

V. PROPOSED WORK FOR FUTURE WORK

We propose an approach to detect wormhole in MANET by using average time delay to detect anomalies based on statistical information of packets in the networks. Three features of the network are monitored including: the number of incoming packets, the number of outgoing packets and the average route discovery time related to each node, throughput of the network, retransmission attempts and load on the network. The network is having wormhole attacks if any abrupt change of one of these features is reported. The proposed algorithm is light weight and low computation overhead.

In this method we specifically consider Wormhole attack which does not require exploiting any nodes in the network and interfere with the route establishment process. Instead of detecting suspicious routes as in previous methods. We implement a new method which detects the attacker nodes and works without modification of protocol, using a hop-count and time delay analysis from the viewpoint of users without any special environment assumptions. The proposed work is simulated using NS2 and results showing the advantages of proposed work. The basic idea behind this work is that the wormhole attack reduces the length of hops and the data transmission delay.

The steps of proposed algorithm are as follows.

- step 1: Randomly generate a Number in between 0 to maximum number of nodes.
- step 2: The randomly generated number in step 1 will be the transmitted node.
- step 3: Routs are generated from selecting transmitting node to any destination node.
- step 4: Start Counter and send RREQ using reactive routing technique
- step 5: Receive the RREP packet from the each path; associate it in route list with time delay.
- step 6: Now calculate the average time delay.
- step 7: Select the route within covariance range of average delay.
- step 8: If the routes that are not within the covariance range are black listed hence they are not involved in future routes discovery.
- step 9: Whole process (from step1 to step 8) is repeated for limited assumed time.

VI. CONCLUSIONS

MANET is easily vulnerable to security attacks than wired networks. MANET is highly vulnerable to attacks due to its characteristics like dynamic topology and infrastructure less etc. Efficient Security mechanisms must be applied to different types of attack to provide protection and stability in MANET. Various existing Techniques are reviewed with its detection mechanisms. Developing detection scheme against the wormhole attack. The detection scheme removes the malicious node and increases the performance. Our proposed detection is designed to detect the malicious node in the WORMHOLE attack. Proposed approach provides detection scheme at route discovery as well as at packet transmissions.

The future scope is to implement the detection algorithm in ns2 simulator. This proposed scheme will reduce the length of hop and data transmission delay.

ACKNOWLEDGEMENT

I (Priyanka B. Patel) would like to thank to my thesis guide Prof. Purvi N Ramanuj for her great effort and instructive comments in this paper work. I would also like to thank my family. Lastly, I offer my regards and blessings to all of those who supported me in any respect during the completion of this paper.

REFERENCES

[1]. Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks” in springerlink 2006.

[2]. A.VANI and D.Sreenivasa Rao “A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing In Ad Hoc Wireless Networks” *International Journal on Computer Science and Engineering (IJCSE) Vol*. 3 No. 6 June 2011.

[3] Reshmi Maulik1 and Nabendu Chaki.” A Study on Wormhole Attacks in MANET” *International Journal of Computer Information Systems and Industrial Management Applications* (2011).

[4]. Saurabh Gupta, Subrat Kar, S Dharmaraja “WHOP: Wormhole Attack Detection Protocol using Hound Packet “in 2011 International Conference on Innovations in Information Technology.

[5] Shalini Jain, Dr.Satbir Jain "Detection and prevention of wormhole attack in mobile adhoc networks". *in International Journal of Computer Theory and Engineering*, February, 2010.

[6] M. Sookhak, M. R. Eslaminejad, M. Haghparast and I. FauziISnin "Detection wormhole in wireless ad hoc network" International Journal of Computer Science and Telecommunications [October 2011]

[7] Xia Wang, Johnny Wong "An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks"

[8] Shilpa Jaiswal#1, Sumeet Agrawal"A Novel Paradigm: Detection & Prevention of Wormhole Attack in Mobile Ad Hoc Networks" *International Journal of Engineering Trends and Technology* (2012).

[9] Ajay Prakash Rai, Vineet Srivastava, Rinkoo Bhatia "Wormhole Attack Detection in Mobile Ad Hoc Networks " in *International Journal of Engineering and Innovative Technology (IJEIT) Volume 2*, Issue 2, August 2012.

[10]. T. Sakthivel, R. M. Chandrasekaran "Detection and Prevention of Wormhole Attacks in MANETs using Path Tracing Approach" *European Journal of Scientific Research* (2012).

[11]. Priyanka Goyal, Sahil Batra Ajit Singh "*A Literature Review* of Security Attack in Mobile Ad-hoc Networks"

[12] Dong-Uk Kim, Hyo-Won Kim, and Sehun Kim "A Two Phase Wormhole Detection Method against Attacker's Countermeasure"*International Conference on Computer Science and Information Technology* (ICCSIT'2011)

[13] T. V. Phuong, N. T. Canh, Y.-K. Lee, S. Lee, and H. Lee, "Transmission time-based mechanism to detect wormhole attack," *In the proceedings of the IEEE Asia-Pacific service computing conference*, 2007

[14] Latha Tamilselvan and Dr. V Sankaranarayanan,"Prevention of wormhole attack in MANET"