International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 30441-30448
© Research India Publications
http://www.ripublication.com

Wormhole Attack Efforts on Manets Challenge on The Mobile

S. Sathish Raja* S. Saravana Kumar
**Research Scholar, Department of CSE, Vels University, Chennai,*
***Professor, Department Of Information technology, Panimalar Institute of Technology, Chennai*
**ssathishraja@gmail.com, **saravanakumars81@gmail.com*

Abstract

The ad-hoc networks are the temporarily established wireless networks which does not require fixed infrastructure it is also called as infrastructure less network. Because of some flaws of ad-hoc network such as shared wireless medium and lack of any central coordination makes them more prone to attacks in comparison with the wired network. Among all the attacks wormhole attack is the most severe attack. In this attack an attacker capture the packets at one location in the network and send it two another attacker at a distant location through tunnels which is established through different ways like packet encapsulation, using high power transmission or by using direct antennas. This tunnel between two colluding attackers is virtual and it is called as a wormhole. The wormhole attack is possible even if the attacker has not comprised any hosts, and all communication provides authenticity and confidentiality. By using the various approaches for finding the solution over wormhole attack, the dynamic information of the packets could still be modified. So in order to give more robust protection in some special scenario like battlefields, which requires highly secured information, there is need of developing some secured mechanism for wormhole detection. Taking into consideration this problem the proposed scheme is developed. This paper discusses proposed works on wormhole attack along with comparison of different wormhole detection techniques in ad-hoc wireless network.

Keywords: ad-hoc, protection, packets, attacker

Introduction

A wireless ad hoc network is a decentralized type of wireless network . The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks.

Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data. An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. Very often, ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks.

The earliest wireless ad hoc networks were the "packet radio" networks (PRNETs) from the 1970s, sponsored by DARPA after the ALOHA net project.

Wireless ad hoc networks can be further classified by their application

- mobile ad hoc networks (MANET)
- wireless mesh networks (WMN)
- wireless Sensor networks (WSN)

An ad-hoc network is made up of multiple “nodes” connected by “links”. Links are influenced by the node's resources (e.g. transmitter power, computing power and memory) and by behavioral properties (e.g. reliability), as well as by link properties (e.g. length-of-link and signal loss, interference and noise).

Since links can be connected or disconnected at any time, a functioning network must be able to cope with this dynamic restructuring, preferably in a way that is timely, efficient, reliable, robust and scalable.

The network must allow any two nodes to communicate, by relaying the information via other nodes. A “path” is a series of links that connects two nodes. Various routing methods use one or two paths between any two nodes; flooding methods use all or most of the available paths

Worm Hole Attack

In this section we explain the wormhole attacks modes and classes while pointing to the impact of the wormhole attack and the efforts that have been done in the literature to detect and prevent this attack.

These attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. Schematics of various attacks as described by Al-Shakib Khan [15] on individual layer are as under.

- Application Layer: Malicious code, Repudiation
- Transport Layer: Session hijacking, Flooding
- Network Layer: Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.
- Data Link/MAC: Malicious Behavior, Selfish Behavior, Active, Passive, Internal External
- Physical: Interference, Traffic Jamming, Eavesdropping

Wormhole Attack Modes

Wormhole attacks can be launched using several modes, among these modes, we mention

1) Wormhole using encapsulation
2) Wormhole Out-of-Band Channel
3) Wormhole with High Power Transmission
4) Wormhole using Packet Relay
5) Wormhole using Protocol Deviations

1) Wormhole Using Encapsulation:

In this mode a malicious node at one part of the network [10] and hears the RREQ packet. It tunnels it to a second colluding party at a distant location near the destination. The second party then rebroadcasts the RREQ. The neighbors of the second colluding party receive the RREQ and drop any further legitimate requests that may arrive later on legitimate multi hop paths. The result is that the routes between the source and the destination go through the two colluding nodes that will be said to have formed a wormhole between them. This prevents nodes from discovering legitimate paths that are more than two hops away.

This mode of the wormhole attack is easy to launch since the two ends of the wormhole do not need to have any cryptographic information, nor do they need any special capabilities, such as a high speed wire line link or a high power source.

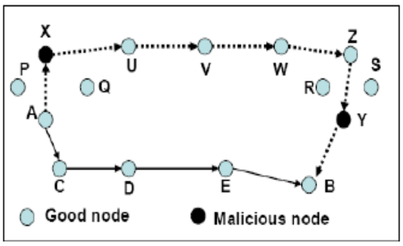

Figure 1: Wormhole Through Out of Band

2) Wormhole Out-of-Band Channel:

The second mode for this attack is the use of an out of band channel. This channel can be achieved, for example, by using a longrange directional wireless link or a direct wired link. This mode of attack is more difficult to launch than the previous one since it needs specialized hardware capability. Consider the scenario depicted in Figure . Wormhole through out-of-band channel Node A sends a RREQ to node B, and nodes X and Y are malicious nodes having an out-of-band channel between them. Node X tunnels the RREQ to Y, which is a legitimate neighbor of B. Node Y broadcasts the packet to its neighbors, including B. B gets two RREQs—A-X-Y-B and A-C-D-E-F-B. The first is both shorter and faster than the second, and is thus chosen by B.

3) Wormhole With High Power Transmission:

Another method is the use of high power transmission. In this mode, when a single malicious node gets a RREQ, it broadcasts the request at a high power level, a capability which is not available to other nodes in the network. Any node that hears the high-power broadcast rebroadcasts it towards the destination. By this method, the malicious node increases its chance to be in the routes established between the source and the destination even without the participation of a colluding node.

4) Wormhole Using Packet Relay :

Wormhole using Packet Relay is another mode of the wormhole attack in which a malicious node relays packets between two distant nodes to convince them that they are neighbors. It can be launched by even one malicious node. Cooperation by a greater number of malicious nodes serves to expand the neighbor list of a victim node to several hops. It is carried out by an intruder node X located within transmission range of legitimate nodes A and B, where A and B are not themselves within transmission range of each other. Intruder node X merely tunnels control traffic between A and B (and vice versa), without the modification presumed by the routing protocol e.g. without stating its address as the source in the packets header so that X is virtually invisible. Node X can afterwards drop tunneled packets or break this link at will. Two intruder nodes X and X′, connected by a wireless or wired private medium, can also collude to create a longer (and more harmful) wormhole, as shown in Figure 4. An extraneous A - B link can be artificially created by an intruder node X by wormholing control messages between A and B. A longer wormhole can also be created by two colluding intruders X and X′ as in

To accessfully exploit the wormhole, the attacker must wait until A and B have exchanged sufficient HELLO messages (through the wormhole) to establish a symmetric link. Until that moment, other tunneled control messages would be rejected, because the OLSR protocol specifies that TC/MID/HNA messages should not be processed if the relayer node (the last hop) is not a symmetric neighbor. However, once created, the A – B link is at the mercy of the attacker.Figure . A longer wormhole created by two colluding nodes.

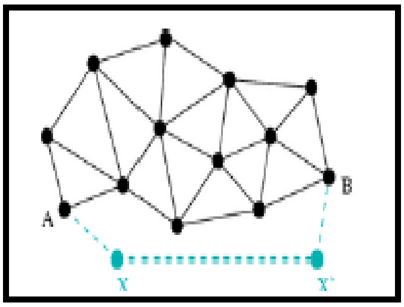

Figure 2: Packet Relay

5) Wormhole Using Protocol Deviations:

A wormhole attack can also be done through protocol deviations. During the RREQ forwarding, the nodes typically back off for a random amount of time before forwarding reduce MAC layer collisions. A malicious node can create a wormhole by simply not complying with the protocol and broadcasting without backing off. The purpose is to let the request packet it forwards arrive first at the destination. The classification of such an attack facilitates the design of prevention and detection methods. According to whetherthe attackers are visible on the route, we classify the wormholes into three types: closed, half open, and open. Following illustrates the three types of wormhole attack.

A) Open Wormhole Attack:

In this type of wormhole, the attackers include themselves in the RREQ packet header following the route discovery procedure. Other nodes are aware that the malicious nodes lie on the path but they would think that the malicious nodes are direct neighbors.

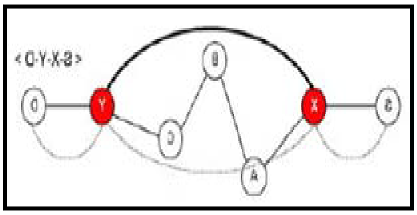

Figure 3: Open Wormhole Attack

B) Half Open Wormhole Attack:

One side of wormhole does not modify the packet and only another side modifies the packet, following the route discovery procedure.

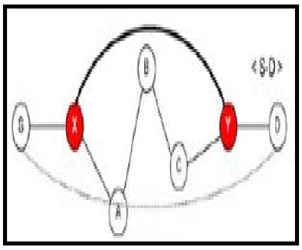

Figure 4: Half Open Wormhole Attack

C) Closed Wormhole Attack:

The attackers do not modify the content of the packet, even the packet in a route discovery packet. Instead, they simply tunnel the packet form one side of wormhole to another side and it rebroadcasts the packet.

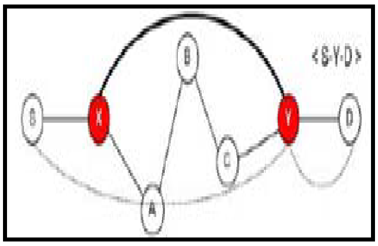

Figure 5: Closed Wormhole Attack

Wormhole Attack In Ad-Hoc Networks

A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a high-speed off-channel link, are strategically placed at different ends of a network, as shown in figure +1. These attackers then record the wireless data they overhear, forward it to each other, and replay the packets at the other end of the network. Replaying valid network messages at improper places, wormhole attackers can make far apart nodes believe they are immediate neighbors, and force all communications between affected nodes to go through them. In general, ad hoc routing protocols fall into two categories: proactive routing protocol that relies on periodic transmission of routing packets updates, and on-demand routing protocols that search for routes only when necessary. A wormhole attack is equally worse a threat for both proactive and on-demand routing protocols [25, 28, 26,29]. When a proactive routing protocol [30] is used, ad hoc network nodes send periodic HELLO messages to each other indicating their participation in the network. when node S sends a HELLO message, intruder M1 forwards it to the other end of the network, and node H hears this HELLO message. Since H can hear a HELLO message from S, it assumes itself and node S to be direct neighbors. Thus, if H wants to forward anything to S, it may do so unknowingly through the wormhole link. This effectively allows the wormhole attackers full control of the communication link.

In case of on-demand routing protocols, such as AODV [17], when a node wants to communicate with another node, it floods its neighbors with requests, trying to determine a path to the destination. if S wants to communicate with H, it sends out a request. A wormhole, once again, forwards such request without change to the other end of the network, may be directly to node H. A request also travels along the network in a proper way, so H is lead to believe it has a possible route to node S thru the wormhole attacker nodes. If this route is selected by the route discovery protocol, once a gain wormhole attackers get full control of the traffic between S and H. Once the wormhole attackers have control of a link, attackers can drop the packets to be forwarded by their link. They can drop all packets, a random portion of packets, or specifically targeted packets1. Attackers can also forward packets out of order or ‘switch’ their link on and off [16].

Conclusion

In order to give more robust protection in some special scenario, where highly secured information is required there is a need of developing some secured.

The main objectives of this approach are as follows

- To prevent eavesdropping
- To avoid packet modification
- To provide authentication & confidentiality.
- To reduce the packet overhead.
- To minimize computation

In this section, a new group based wormhole detection method has been proposed. In multi-hop wireless systems, the need for cooperation among nodes to relay each other's packets exposes them to a wide range of security threats including the wormhole attack. A number of recent works have been studied before proposing this new methodology. The proposed solution unlike some of its predecessors does not require any specialized hardware like directional antennas, etc for detecting the attackers. or extremely accurate clocks, etc. Currently more studies are being done to analyze the performance of the proposed algorithm in presence of multiple attacker node.

References

[1] Wormhole Attacks in Wireless Networks Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, and David B. Johnson, Member, IEEE IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006

[2] IN THE PAPER Detection and Prevention of Layer-3 Wormhole Attacks on Boundary State Routing in Ad hoc Networks. 2010 International Conference on Advances in Computer Engineering

[3] Y.C. Hu A. Perrig and D. B. Johnson. PACKET LEASHES: A defense against wormhole attacks in wireless ad hoc networks. IEEE INFOCOM, pages 1976–1986, 2003. 612–621, 2005

[4] H.S. Chiu and K.S. Lui. DELPHI: wormhole detection mechanism for ad hoc wireless networks. 1st International Symposium on Wireless Pervasive Computing, pages 6–11, January 2006.

[5] Ming-Yang Su. Warp: A wormhole-avoidance routing protocol by anamoly detection in mobile ad hoc networks. Computer Security, vol.29, March 2010.

[6] S Dharmaraja and Subrat kar:WHOP: Wormhole Attack Detection Protocol using Hound Packet. 2011 international conferenceon innovation in information technology

[7] On the Survivability of Routing Protocols in Ad Hoc Wireless Networks, A. Baruch, R. Curmola, C. Nita-Rotaru, D. Holmer, H. Rubens, Converence onSecurity and Privacy for Emerging Areas Communications, SecureComm 2005, September2005.

[8] I. Khalil S. Bagchi and N.B. Shroff. LITEWORP: a lightweightcounter measure for the wormhole attack in multihop wireless networks. International Conference on Dependable Systems and Networks, pages 612–621, 2005.

[9] Issa Khalil, Saurabh Bagchi & Ness B. Shroff, “MOBIWORP: Mitigation of the Wormhole Attack in Mobile Multihop Wireless Networks”. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4198824

[10] A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies.1

[11] C K Toh, Ad Hoc Mobile Wireless Networks, Prentice Hall Publishers , 2002.

[12] P. Gupta and P.R. Kumar. Capacity of wireless networks. IEEE Transactions on Information Theory, Volume 46, Issue 2, March 2000, doi:10.1109/18.82579.

[13] Jinyang Li, Charles Blake, Douglas S. J. De Couto, Hu Imm Lee, and Robert Morris, Capacity of Ad Hoc Wireless Networks, in the proceedings of the 7th ACM International Conference on Mobile Computing and Networking, Rome, Italy, July 2001.

[14] Wu S.L., Tseng Y.C., "Wireless Ad Hoc Networking, Auerbach Publications", 2007 ISBN 978-0-8493-9254-2.

[15] Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking". O'Reilly Wireless Dev Center. Retrieved 2009-01-20.

[16] Y.-C. Hu, A. Perrig, D. B. Johnson, “Wormhole Attacks in Wireless Networks,” Selected Areas of Communications, IEEE Journal on, vol. 24, numb. 2,pp. 370- 380, 2006.

[17] Y. Hu, A. Perrig, and D. Johnson, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks”, in *proceedings of INFOCOM*, 2004.