ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

A Review: Wormhole attack In Mobile Ad Hoc Network.

Chandraprabha Rawat
Master's in Software system, Department of computer application, Samrat Ashok Technological Institute, Vidisha, India [1]

ABSTRACT: The Mobile Ad hoc Network (MANET) is a Infrastructure-less Network. And lack of centralized co-ordination in ad hoc network that make Susceptible to various attacks. Various attacks in the network that are effect in the network performance one of the most important attack called wormhole that is create complex problem within the mobile ad hoc network. Wormhole attack makes some malicious node in the network that disrupts to delivery of Packets. In this paper provides some important information about wormhole and its detection methods.

Keywords: Routing Protocal, Mobile ad ho network, Wormhole attack, security requirement.

I INTRODUCTION

Mobile Ad-hoc Network (MANET) is a collection of wireless mobile hosts without fixed network infrastructure and also no centralized administration. Communication in MANET is done via multi-hop paths. There are Lots of challenges (MANET) contains that different resources. Typically, the nodes act as both host and router at the same time i.e. each node participates in routing by forwarding data for other nodes and deciding to which nodes forward data next based on the network connectivity. Most previous ad hoc networks research has focused on problems such as routing and communication, assuming a trusted environment. However, many applications run in untrusted environments and require secure communication and routing such as military or police networks, emergency response operations like a flood, tornado, hurricane or earthquake. However, the open nature of the wireless communication channels, the lack of infrastructure, the fast deployment, and the Environment where they may be deployed, make them vulnerable to a wide range of security attacks.

The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a stand-alone fashion, or may be connected to the Internet. Multi hop, mobility, large network size combined with device heterogeneity, Bandwidth and battery power constraints make the design of adequate routing protocols a major challenge.

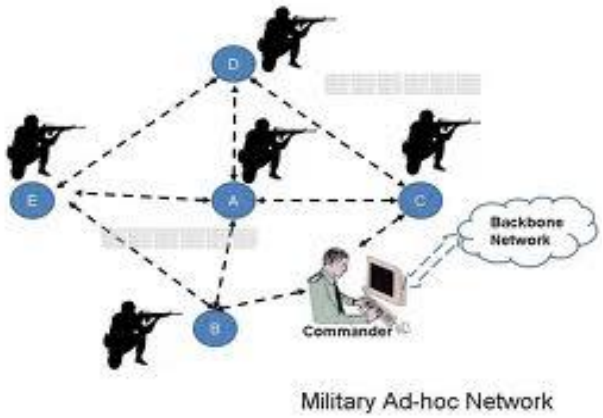


Figure1-ad hoc network.

II Routing protocols

Wireless mobile ad hoc networks without fixed infrastructure consist of mobile hosts that travel randomly in and out of each other in a communication range resulting in frequent connection breaks and topology varies stochastically. Traditional table-driven routing protocols also called Proactive routing protocol cannot perform in such environment because of its work with wired network in resulting than development of on-demand routing protocols also called Reactive routing protocol for wireless ad hoc networks. The two highly on-demand routing protocols are AODV(Ad hoc on-demand distance vector) and DSR(Dynamic Source Routing).An ad hoc routing protocol is a convention, that controls how nodes decide which way

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

to route packets in between source destination in a mobile ad hoc network.

AODV

(Ad hoc on-demand distance vector)[15] routing protocol that is proposed for wireless network .mobile ad hoc network doesn't require prior infrastructure. A route is established only when source node need to send data packets in the network which is in transition range. Most important think in AODV routing it work on destination sequence number for identify recent path in between transmitting nodes. A major difference in between ad hoc on- demand distance vector routing protocol and other routing protocol is that it uses destination sequence number for determine an most recent path to destination. A RouteRequest carries the source identifier (SrcID,), the source sequence number (SrcSeqNum), destination identifier (DestID), the broadcast identifier (BcastID),the time to live field.This protocol performs Route Discovery process using route request(RREQ) messages to send packet to destination node and route reply(RREP) messages send by destination node to the source node for confirmation of received packet that send by the so messages source node.

The route discovery process is use broadcasts of RREQs, the source node use an mounting search technique. The forward path sets up in intermediate nodes in its route table and intermediate node forward RREQ its next node all intermediate which are included in route discovery contain information of our next node that is RRP packet also use send by the destination node. When either destination or intermediate node moves, a route error (RERR) is sent to the affected source nodes. When source node receives the (RERR), it can reinitiate route discovery if the route is still needed.

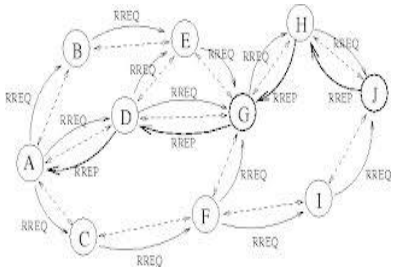
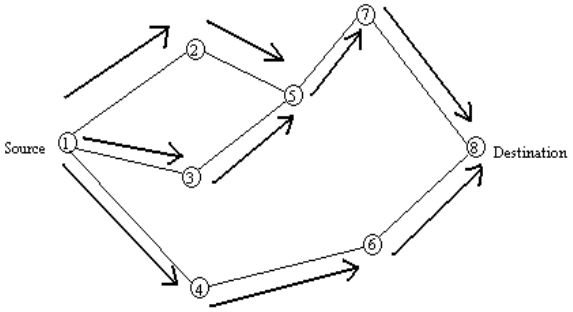


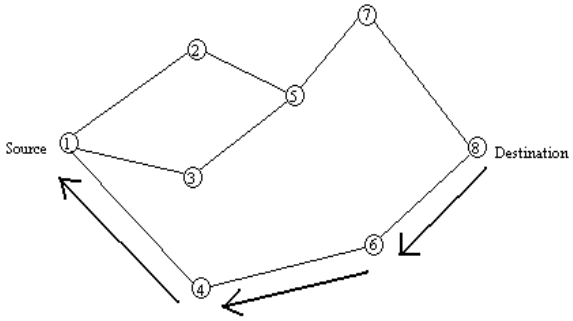
Figure2-Process of AODV routing Protocol

DSR

DSR(Dynamic Source Routing Protocol)[14] is an Ad Hoc routing protocol also called on-demand routing protocol it's work on source routing can't table-driven approach.DSR is design for restrict the bandwidth consumed by control packet in ad hoc wireless protocol which is requied in table-driven approach. Dynamic Source Routing Protocol use source sequence number to prevent for looping in the network. This Protocol is composed of two essential parts of route discovery and route maintenance phase. In route discovery phase it use source sequence number from the source node and destination address source node. In the route discovery phase source node establish flooding RouteRequest Packet in the wireless network. And when destination node receiving this flooding packet it send a RouteReply packet back to the source node using reverse path which contain in the RouteRequest packet that receive by the destination node.DSR carries whole path between the source to destination.



(a) Propogation of Route Request (RREQ) Packet



(b) Path taken by the Route Reply (RREP) Packet

Figure3- DSR routing Protocol

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

III ISSUE INAD HOC WIRELESS NETWORK

There are some major Issues that is need to be focused on it when an ad hoc network is to design because of that affect on performance, design ,deployment of an ad hoc wireless mobile system. We describe as follows:-

1.Distributed Operation- The lack of centralized co-ordination system in ad hoc wireless network so that the MAC protocol design should be fully distributed which is include minimum control of overhead.

2.Throughput-ad hoc wireless network involve the MAC protocol should effort to maximize throughput of the system. Improve throughput of the system important deliberation are reduce the incidence of collision, minimizing channel consumption, minimizing control overhead.

3. Access delay-Access delay refers to the average delay of any packet that experience to get transmitted. In ad hoc network include the MAC layer should attempt to minimizing the packet delay.

4.multicasting- the multicast routing protocol must able to recovery and reconfigure rapidly from any links break in the network. It is making suitable for highly dynamic environment.

5.Scalability- ad hoc wireless network multicasting routing protocol must be able to scale for network for larger amount of nodes.

6.Quality of service- QoS is a essential part of the multicasting routing protocol just because of use time - sensitive environment.

7.Security-in the ad hoc wireless network security of communication is very important part especially in military application. In the network attack effect on use of service that is useful for the node which are working in the ad hoc network by either consuming bandwidth or by overloading the system, is called denial of service(DoS).

IV NETWORK SECURITY REQUIREMENT

In ad hoc wireless network security protocol must be satisfy some requirement.
Confidentiality, Integrity, Availability, Non-repudiation.

A. Confidentiality-Whenever starts communication between the source and destination node. the data send by the source node and received by the indented destination node. Only intruder might get hold of the data but other he/she can't able to access any useful information out of the data packet. In the ad hoc network proposed one most popular technique is that ensuring confidentiality is data encryption.

B. Integrity-most important think is Integrity in the network, means that the date sent by the source node should reach accurately to destination node. No missing, and fault data must be reach. But it is not possible if any malicious node is present in the network that is tamper with the data during transmission.

C. Availability-if any link is failure in the network but the network should remains operational all time. It always must be able to works various attacks are mounted in it. Network always provides necessary service that is required by an authorized user.

D. Non-repudiation-the mechanism of Non-repudiation is provide guarantee that source of message can't deny later having sent massage and that the destination can't deny having receiving the message.

V WORMHOLE ATTACK IN AD HOC NETWORK

The ad hoc wireless network is infrastructure-less network or lack of centralized coordination that is vulnerable of various attacks, one the wormhole attack is discuss here. Wormhole attack can form a serious threat in wireless networks especially against many ad hoc network routing protocols. Wireless ad-hoc networks are usually vulnerable to different defense threats and wormhole attack is one of these. In this type of attack, the malicious node participates in the network communication forming a short path tunnel and transmitting traffic flow through this high speed wormhole tunnel. Then the malicious nodes create problem during data transferring. it just because of dynamic routing environment. Wormhole attack make malicious node in the network one node does not make wormhole two or more than two nodes make wormhole. One malicious node catches the data packet and "tunnels" them to another malicious node at a distant point which replays them locally by wormhole link .The tunnel (packet transmit on one malicious node another malicious node) can be established in many ways e.g. in-band and out-of-band channel. This makes the tunneled packet arrive either quicker or with a

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

minimum number of hops compared to the packets transmitted over normal multi hop routes. This creates the illusion that the two end points of the tunnel are very close to each other. However, it is used by malicious nodes to disrupt the correct operation of ad hoc routing protocols. They can then launch a variety of attacks against the data traffic flow such as selective dropping, replay attack, eavesdropping etc. Wormhole can be formed using, first, *in-band channel* where malicious node m1 tunnels the received route request packet to another malicious node m2 using encapsulation even though there is one or more nodes between two malicious nodes, the nodes following m2 nodes believe that there is no node between m1 and m2. Second, *out-of-band channel* where two malicious nodes m1 and m2 employ a physical channel between them by either dedicated wired link or long range wireless link .show in figue4.

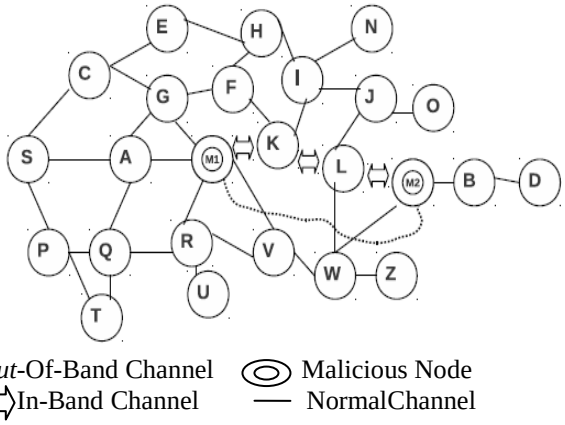


Figure4. Wormhole Attack

When malicious nodes form a wormhole they can reveal themselves or hide themselves in a routing path. The former is an *exposed* or *open* wormhole attack, while the latter is a *hidden* or *close* one. In Fig. 4, the destination *D* notice that a packet from the source *S* is transferred through node *A* and *B* under hidden wormhole attack, while it believes that the packet is delivered via node *A,m1,m2*, and *B* under exposed wormhole attack.

VI RELATED WORK

In the previous research can be broadly classified in two categories. First method which is known as routing protocols such as Adhoc on-demand vector, Dynamic source routing , Optimizing Link State Routing to avoid/detecting wormhole attack .Second, methods which has adopted an extra hardware or monitoring system such as positioning system, a time synchronization . In [5] WHIDS, a cluster based counter-measure isproposed for the wormhole attack. Simulation results using MATLAB exhibit the effectiveness of WHIDS for detecting wormhole attack. The method, however, has notbeen tested in presence of multiple wormhole attacks. In (Shang-Ming Jen, Chi-Sung Laih and Weh-Chung Kuo, 2009), a hop count based scheme is used to present wormhole attack. A route with a hop-count value, that is significantly smaller than the others, is most likely a wormhole. The proposed scheme uses simulator of C and Matlab to get results.

Farooq Anjum et al. [1] have proposed an initial approach to detect intrusions in ad hoc networks. Anand Patwardhan et al. [2] have proposed a secure routing protocol based on AODV over IPv6, further reinforced by a routing protocol independent Intrusion Detection and Response system for adhoc networks. Chin-Yang Henry Tseng [3] has proposed a complete distributed intrusion detection system has consisted of four models for MANETs with formal reasoning.

In [4] a new protocol called Multi-path Hop-count Analysis (MHA) is introduced based on hop-count analysis to avoid wormhole attack. It is assumed that too low or too high hop-count is not healthy for the network. The novelty of the hop-count analysis in detecting wormholes is however questionable. Similar works have also been reported earlier. As an example, Djenouri et al. [8] may be considered.

Hu et al.[6] introduced *Packet Leashes* method to defenda gainst the wormhole attack. Two types of leash information was used *Geographical Leash and Temporal Leash*. In geographical leashes each node must have its accurate location information and loose clock synchronization. When node

Receives a packet, it calculates distance between previous node and itself by using send/receive timestamp. For temporal leashes, each node should have accurate clock synchronization. Every packet should be delivered to the next node within computed life time of a packet. Otherwise, the next node regards the path as a wormhole the packet leashes do not identify malicious nodes.

Khalil et al. [10] introduces LITEWORP in which they used the notion of *guard node*. The guard node can detect the wormhole if one of its neighbours is behaving maliciously. The guard node is a common neighbour of two nodes to detect a legitimate link between them. In a sparse network, however, it is not always possible to find a guard node for a particular link.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

REFERENCES

1. Farooq Anjum, Dhanant Subhadrabandhu and Saswati Sarkar "Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols" inproceedings of IEEE 58th Conference on Vehicular Technology, 2003.
2.Anand Patwardhan, Jim Parker, Anupam Joshi, Michaela Iorga and Tom Karygiannis "Secure Routing and Intrusion Detection in Ad Hoc Networks" Third IEEE International Conference on PervasiveComputing and Communications, March 2005.
3.Chin-Yang Henry Tseng, "Distributed Intrusion Detection Models for Mobile Ad Hoc Networks University of California at Davis Davis, CA, USA , 2006.
4.Shang-Ming Jen, Chi-Sung Laih, Wen-Chung Kuo. "*A Hop-Count Analysis Scheme for Avoiding Wormhole Attacks inMANET*", 9 (6), pp. 5022-5039, (2009).
5.D.B. Roy, R. Chaki, N. Chaki. "A New Cluster-based Wormhole Intrusion Detection Algorithm for Mobile Ad-hoc Networks", *IJNSA*, 1 , pp. 44-52, (2009)
6.Y.C. Hu, A. Perrig and D. B. Johnson "*Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks*. "In IEEE INFOCOM, vol.3, pp. 1976 – 1986, (Apr.2003).
7.L. Hu and D. Evans. *Using Directional Antennas to Prevent Wormhole Attacks*. In Network and Distributed System Security Symposium, San Diego California, USA,(5-6
February 2004) for the wormhole attack in multihop wireless networks.
8.International Conference on Dependable Systems and Networks, pages 612 Farid Na¨ıt-Abdesselam, Brahim Bensaou, and Tarik Taleb. Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks.(2006).
9.Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defence against wormhole attacks in wireless networks," in INFOCOM, 2003.
10.I. Khalil S. Bagchi and N.B. Shroff. LITEWORP: a lightweight countermeasure –621, 2005.
11.S.R.Das,C.E.Perkins, and E.M.Royer, "Performance comparison of two on-demand routing protocols for ad hoc networks, in Proc. INFOCOM 2000, pp3-12.
12. Yuan Sun, Elizabeth M. Belding-Royer, and Charles E. Perkins. Internet connectivity for ad hoc mobile networks. International Journal of Wireless Information Networks, special issue on Mobile Ad hoc Networks, 2002
13.A. Boukerche, B. Turgut, N. Aydin, M. Z. Ahmad, L. Bölöni, and D.Turgut, "Routing protocols in ad hoc networks:A survey," Journal Computer Networks:The International Journal of Computer and Telecommunications Networking archive, vol. 55, no. 13, September, 2011, pp. 3032-3080.
14.Johnson D.B., Maltz D.A. and Broch J. (2001) Ad Hoc Net-working. Boston, Addison-Wesley, 139-72.
15. C. Perkins, E. B. Royer, S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing - Internet Draft", RFC 3561, IETF Network Working Group, July 2003

BIOGRAPHY

Chndraprabha Rawat have complete bachelor degree with Information Technology in 2009 from Rajiv Gandhi Proudyogiki Vishwavidyalaya Bhopal and Master's with Software System from Samrat Ashok technological Institute Vidisha India. Reseach in Mobile Ad Hoc Wireless Network.