International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Review on Detection and Prevention Techniques of Wormhole Attack in MANETs

Darshana Sorathiya[1], Haresh Rathod[2]

[1]PG Scholar Computer Engineering, RK University, Rajkot, Gujarat, India

[2]Assiatant Professor, Computer Engineering, RK University, Rajkot, Gujarat, India

Abstract: ***A Mobile Ad-Hoc Network (MANET) is an infrastructure less or a self-configured collection of mobile nodes that can randomly change their geographic locations such that these networks have dynamic topologies and random mobility with constrained resources. It usually works by broadcasting the information. Its nature is broadcasting so there is a chance to disrupt network by attacker. The number of attack can be done in Mobile Ad Hoc Network. This paper analysed different technique to detect and prevent wormhole attack and compare them.***

Keywords: MANET, Wormhole attack, Wormhole detection techniques

1. Introduction

MANETs dynamically form a temporary infrastructureless network of mobile nodes. In this network, intermediate nodes cooperate and act as a router and send messages from one node to another. It is quite useful in situations where we have lack of fixed network infrastructure, such as an emergency situations or rescue operation, medical assistance, disaster relief services, mine site operations, and military mobile network in battlefields.

Figure 1: Mobile Ad Hoc Network [11]

Security is providing protected communication between mobile nodes in wireless network. There are many routing protocols for MANET. It has been proposed to facilitate rapid and efficient network design and restructuring.

MANET has several challenges. They include:

1. Multicast routing: Designing of multicast routing protocol for a constantly changing MANET environment.
2. Power consumption: Since the nodes in MANET network usually run on batteries and are deployed in unfriendly terrains, they have inflexible power requirements.
3. Dynamic Topology: The nodes are move free in network and hence the network topology is changed.
4. Quality of service (QOS): Providing constant QoS for different multimedia services in frequently changing environment.
5. Security: The eventual goal of the security solutions for MANET is to provide a framework covering availability, confidentially, integrity, and authentication to insure the services to the mobile user.

2. Routing Protocols

Routing protocol in MANET can be classified as

A. Proactive Routing Protocol

In proactive routing [1], mobile nodes periodically broadcast their routing information to the next node. Each node needs to maintain the records of the adjacent and reachable nodes with a number of hops. Nodes have to evaluate their neighbourhood as per the network topology change. It is also called table-driven routing protocol. These types of protocols are Destination Sequenced Distance Vector (DSDV) routing protocol and Optimized Link State Routing (OLSR) protocol. Wireless Routing Protocol (WRP), Global State Routing (GSR), Zone Based Hierarchical Link State Routing Protocol (ZHLS) and Clustered Gateway Switch Routing Protocol (CGSR) are also proactive routing protocols.

B. Reactive Routing Protocol

Reactive routing [1] protocol is called on-demand routing protocol. If there is no communication then it is not maintaining routing information. If a node wants to send packet to another node then the protocol has to searches for the route in on demand. It has to establish the connection in order to transmit and receive the packet. It is simply started when nodes desire to transmit data packets. On-demand routing protocols or reactive routing protocols are Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR). Clustered Based Routing Protocols (CBRP), Temporally Ordered Routing Algorithm (TORA), Associatively Based Routing (ABR) and Signal Stability Routing (SSR) are also reactive routing protocols.

C. Hybrid Routing Protocol

Hybrid routing [1] protocol is combination of proactive and reactive routing protocol's advantages. It overcomes on the disadvantages of these protocols. This protocol is based on hierarchical or layered network framework. There are two Hybrid routing protocol zone routing protocol (ZRP) and temporally-ordered routing algorithm (TORA).

D. AODV Routing Protocol

Ad hoc on-demand distance vector (AODV) routing protocol is an on demand routing protocol for searching routes and a route is established only when it is required by source node for transmission of data packets [5]. AODV uses a sequence number. It applies a destination sequence numbers to identify the fresher path. AODV has three tyes of message RREQ, RREP, RERR. In an AODV, the source node broadcast the Route Request (RREQ) packet in the network when the route is not available for the preferred destination. A node updates its path information only if the DesSeqNum (destination sequence number) of the current packet received is greater than the last DesSeqNum (destination sequence number) stored at the node.

A Route Request (RREQ) [4] has six parameter, (1)The source identifier (SrcID), (2)The destination identifier (DesID), (3)The source sequence number (SrcSeqNum), (4)The destination sequence number (DesSeqNum), (5)The broadcast identifier (BcastID), and (6)The time to live (TTL) field. When an intermediate node receives a Route Request (RREQ), it either forwards it or provides a Route Reply (RREP) if it has a valid route to the destination. The route is correct or not at the middle node is determined by comparing the sequence number (Seq) at the intermediate node with the destination sequence number (DesSeqNum) in the route request (RREQ) packet.

All middle nodes having legal routes to the destination or the destination node itself, only those nodes are permitted to send Route Reply (RREP) packets to the source. When a node receives a Route Reply (RREP) packet, information or data about the prior node from which the packet is received is also reserved in order to forward the data packet to this next node as the next hop against the destination.

AODV does not rebuild a not working path locally but at the same time of link breaks. It is determined by observe the periodical beacons or through link-level acknowledgements, the end nodes are announced. Hence, source node came to know about the path break and it rebuild a route to the destination if required by higher layers. If path break is detected at an intermediate node, the node warns the end nodes by sending a voluntary Route Reply with the hop count set as infinity.

3. Security Attacks

A. Flooding Attack

In a flooding attack, a malicious node takes an advantage of the route discovery process of the AODV routing protocol. The malicious node aims to flood the network with a large number of RREQs to missing destinations in the network which takes a lot of the network resources. Since the destination does not present in the network, a RREP packet cannot be generated by any node in the network and all the nodes keep on flooding the RREQ packet. When large number of fake RREQ packets is broadcast into the network, new routes can no longer be added to the network. And the network is not capable to transmit data packets, which leads to congestion in the network and flood the route table in the intermediate nodes so that the nodes are unable to receive new RREQ packet, which resulting in a DoS attack.

B. Black hole Attack

In a black hole attack, a malicious node absorbs the network traffic and drops all packets. To accomplish with a black hole attack, a malicious node waits for incoming RREQ packets from other nodes. When RREQ message received at the malicious node, without checking its routing table, the malicious node instantly sends a false RREP with a high sequence number with zero hop count to spoof its neighbours that it has the best route to the destination. The malicious node reply will be received by the source node before any reply is received from other nodes. When source node receives multiple RREP, it selects the RREP with the largest destination sequence number and the minimum hop count. Then the source node ignores other RREP packets and starts sending data packets over the malicious node. When the data packets transmitted by the source node and it are reached to the black hole node, at that time it drops the packets before transfer them to the destination node.

C. Gray hole Attack

A gray hole [3] may forward all the packets to certain nodes but may drop those packets coming from or destined to some specific nodes. In another variation of this attack, a node may behave maliciously for some time but later on it behaves normally. Sometimes, a node may combine the behaviour of attacks discussed above. Due to this uncertainty in behaviour of gray hole, this type of attacks are more difficult to detect/prevent compared to black hole attack. Like black holes, cooperative gray hole attacks may be possible against AODV.

D. Worm hole Attack

A security attack, called the wormhole attack [9], has been introduced in the background of ad hoc networks. In this type of attack, a malicious node takes packets from one location in the network. Malicious node tunnels this packet to another malicious node at a distant point which replays this packet locally. The tunnel can be recognized in many ways e.g. In-band and Out-of-band channel. This make the tunnelled packet get there either faster or with a slighter number of hops compared to the packets transmitted over normal multi hop routes. This creates a false impression that the two end points of the tunnel are very close to each other means that that one is a shorter route. But it is used by malicious nodes to interrupt 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 RREQ 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 shown in Fig.

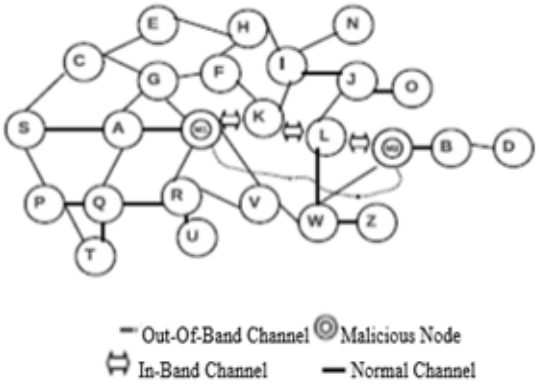

Figure 2: Wormhole attack [9]

4. Literature Survey

The various techniques used for the prevention and detection of wormhole attack in MANET is described below:

A. Packet Leashes

In this paper [6], the method is used to detect wormhole attack. Two types of Leashes: Temporal Leashes and Geographical Leashes. Temporal Leashes is based on time of sending and receiving packets from 1 node to another node. Geographical Leashes is based on location of nodes.

1. *Temporal Leashes:* All modes must need strongly synchronized clock. It is based on off- the -shelf hardware.
2. *Geographical Leashes:* There is no requirement of clock synchronization. It requires GPS hardware. In this method when one node send a packet to another node then it add its own location ps and time on which it sends a packet ts. The receiver compare the value of sending packet with its own location pr and time at which it receives packet tr.

B. Directional Antennas

It is a hardware based approach [7] in which each nodes are equipped with directional antennas that communicate with each other, nodes use specific sectors of antennas and observe the direction of received signal. If the directions of both the pairs match than relation is set. This approach fails if an attacker intentionally places the wormhole between the communicating nodes.

C. Digital Signature

This paper [8] is presented a method which is useful to prevent a wormhole attack in ad hoc network is verify a digital signature of a sending nodes by receiving node. All nodes contain digital signature of every other legitimate nodes of current network. Create a trusted path between sender and receiver with the help of verifying of digital signature. If malicious node present it is identify because that node does not have legal digital signature.

D. Neighbour Node Analysis

In this paper [10] neighbour node approach analyse the entire neighbour node for the purpose of authentication, so that secure transmission can be occur over the wireless network. This method is use request and response mechanism. Node will send a request to its all neighbour nodes. The node will maintain a table which store a reply time. If reply time is not accurate there is a harmful node in the current network. The response time of RREP message is compare to the response time of actual message sent. If response time of actual message is greater than the response time of RREP + threshold value than we can say that wormhole link is present in the route. Comparison of this process is repeated till the destination reached.

E. DelPHI technique

Delay Per Hop Indication [9] is based on the calculation of (delay per hop) value of disjoint paths. It is based on the fact that under normal condition, the delay a packet experiences in propagates one hop should be comparable along each hop path. While in wormhole attack, the delay for propagating across fake neighbours are high as there are many hops between them. It doesn't need any extra hardware or tight time synchronization and has high power efficiency [9]. It works for both In-Band and Out of –Band mode.

F. WHOP technique

This paper [12] proposes a routing protocol WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on AODV. In WHOP, a hound packet will be send after the route has been exposed using AODV routing protocol, the hound packet will be processed by every node except nodes who were involved in route from source to destination during path set up. WHOP contains other three column address of node processing bit (PB) and count to reach next hop (CRNH). CRNH represents the hop difference between neighbors of one hop separated node; its value will be increment by each node for the first node entry whose processing bit is zero in the packet.

5. Discussion

Method	*Advantages*	*Disadvantages*
Geographical Leashes	Used when tight clock synchronization not needed	Limitation of GPS technology. Increase Computation and network Overhead
Temporal Leashes	Do not rely on GPS information, highly efficient when client used TIK	All nodes require Tight synchronization.
Directional Antennas	Less expensive, efficient use of energy and better special use of bandwidth	Needs for directional antenna.
Digital Signature	Packet delivery ratio is high. Through put level is increased when increase the number of nodes in network	Network overhead is also increased.
Neighbour node analysis	Through put is increase Also Provide better efficiency.	Not use for large network
DelPHI Technique	Synchronization doesn't need.	Qos is low because of delay is there.
WHOP Technique	Not requires any hardware support and clock synchronization. And to avoid/detect both types of wormhole attack in-band and out-band.	Network overhead is increase

6. Conclusions

MANET is a wide area in which security is major challenge.In this paper, we have analysed the different types of attacks and protocols which degrade the performance of the network. Also various techniques are compared to detect and prevent wormhole attack. WHOP doesn't required significant change in AODV. It only adds extra packet called hound packet. Detection is done without support of any hardware.

Reference

[1] Robinpreet Kaur and Mritunjay Kumar Rai , "A Novel Review on Routing Protocols in MANETs" , *Undergraduate Academic Research Journal (UARJ)*, Volume-1, Issue-1, 2012.
[2] PRADIP M. JAWANDHIYA and MANGESH M. GHONGE, "A Survey of Mobile Ad Hoc Network Attacks", *International Journal of Engineering Science and Technology*, Vol. 2(9), pp.- 4063-4071, 2010.
[3] m.h. davda, s.r.javid "A review paper on the study of attacks in MANET with its detection and mitigation scheams " *IJARCSMS*, april 2014.
[4] C. Siva Ram Murthy and B.S.Manoj, "Ad hoc Wireless Networks" (Chapter 7), 2014.
[5] E.M.Royer and C.E.Perkins, "Adhoc On-Demand Distance Vector Routing", *IEEE*, pp. 90-100, February 1999.
[6] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad Hoc Networks", *IEEE* 2003.
[7] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks". In the *Proceedings of network & distributed system Security Symposium*,, February 2004.
[8] Pallavi Sharma, Prof. Aditya Trivedi, "An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature", *IEEE*, 2011.
[9] Lui K.-S., sChiu H.S., "DelPHI: Wormhole Detection mechanism for *Adhoc* Wireless Networks" Proceedings of the 1st International Symposium on Wireless Pervasive Computing; Phuket, Thailand. 16–18 January 2006.
[10] sweety goyai, harish rohil, "Securing MANET against Wormhole Attacl using Neighbour Node Analysis" *IJCA* volume 81,November 2013.
[11] Saleh Ali K.Al-Omari1, Putra Sumari2 "An overview of a mobile ad hoc networks for the existing protocols and application", International journal of graph theory in wireless Adhoc network, March-2012.
[12] Saurabh Gupta, Subrat Kar, S Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", *IEEE*, 2011.