ISSN:0975-9646

A Survey of Different Approaches to Detect Wormhole attack

Baltej Kaur Saluja[1], Prof A.K.Gupta[2]

[1]Research Scholar, Department of Computer Science, JSPM COE College ,411024,
Hadapsar, pune,Maharashtra, India.
[2]Associate Professor, Department of Information Technology,JSPM COE College,411024,
Hadapsar, pune,Maharashtra, India.

Abstract- **Mobile ad-hoc networks (MANETs) are collection of wireless mobile computers (or nodes) having no Pre existing infrastructure or centralized management and which are connected by wireless links automatically .Securing Mobile Adhoc Network is essential for network communications. Success of mobile networks (MANET) strongly depends on people's confidence in its security. As Ad hoc networks are vulnerable to security attacks, among them Wormhole Attack is big menace to the mobile ad hoc network. In this paper we specifically considering Wormhole attack which does not require exploiting any nodes in the network and can interfere with the route establishment process by capturing packet from one point in the network, and tunnels the recorded packets to another point which is a malicious node and later on packets in the network can be transmitted again locally .In wireless ad hoc networks, it is difficult to trace out wormhole attacks because malicious nodes behaves as legitimate nodes. Many of the scheme have been proposed for wormhole attack like location and time depended end to end solutions. In this paper we present different routing attack and followed by wormhole attack with its different preventive techniques.**

Keywords:**Wormholeattack, Tunnelling ,Malicious Node, Blackhole, Spoofing.**

I. Introduction

Most attractive Wireless Ad hoc network solve many problems in real world due to which it continues to gain attraction from industrialists and researchers. However the widespread progress of deployment of Wireless Adhoc network faces many challenges. Previously Network was assumed as trusted and focus was on routing and communication. Whereas secure communication is vital demand of networks in this era. Military or police Network and Safety critical business operations such as oil drilling platforms or mining operations are the type of applications that may require secure communication.[1] Wireless Ad hoc Network work in the license free frequency band and do not require any investment in infrastructure making them very attractive. For example, in emergency crisis like natural disaster like a, earthquake, hurricane or tornado, ad hoc network could be useful for further regular Communication .As everything has two sides similarly there are many unsolved problems in ad hoc network Where securing the network is major concern. wormhole attack, easily launches in spontaneous network i.e mobile ad hoc networks .The Wormhole attack is one of the most severe security attacks which may troubled the communications and try to gain sensitive information across the network [2].

Security comes after attacks. If no attacks are there, there is no need for security. Section II describes Major Attacks on Mobile Ad hoc Networks Section III describes various possible countermeasures for wormhole attack in MANET. Finally, conclusion is presented in section IV.

II. Major Attacks On Mobile Ad Hoc Networks

A) Spoofing

Among various types of attacks, identity-based spoofing attacks[3] are especially easy to launch,attacker attempts to acquire identity of legitimate user and can cause significant damage to network performance. For instance, in an 802.11 network, it is easy for an attacker to gather useful MAC address information during passive monitoring and then modify its MAC address by simply issuing an ifconfig command to masquerade as another device.After Masquerading as a legitimate user, the malicious node can access the services are normally restricted to legitimate node only.Because MAC addresses associated with wireless cards are usually used to identify individuals in 802.11 networks, masquerading attacks typically work by spoofing these MAC addresses. The goal of this attack is to establish a connection that will allow the attacker to gain access to the other hosts and their sensitive data (Gayathri et al., 2009; Latha et al., 2007; Priyanka etal., 2010).

B*)Flooding Attack*

Flooding of Attack can be launched by using either by using RREQ or Data flooding [4].The flooding attack causes the most damage and also easy to implement. In flooding through RREQ the network is flooded with the RREQ, due to which lots of network resources get exhausted. The Malicious node select such I.P addresses that do not exist in the network. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding the attacker set up paths between all the nodes in the network by getting into the network. The malicious nodes after establishment of paths will inject lots of useless data packets into the network which will be forwarded to all other nodes in the network. These immense unwanted data packets in the network congest the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time.

C) Packet Dropping

A node may advertise routes through it to many other nodes and may start dropping the received packets rather than forwarding them to the next hop based on the routes advertised. Another variation of this attack is when a node drops packets containing routing messages. These types of attacks are a specific case of the more general packet dropping attacks. In a packet dropping attack a misbehaving node simply destroys or discards data or routing packets without taking responsibility. The packet dropping attack[5] is also known as an ignorance attack and has the following variations regarding frequency and selectiveness. Random or constant dropping concerns the period of time that the malicious node drops the packets. In selective dropping, packets are dropped according to some specific criteria. Selective dropping is also known as a gray hole attack.

D) Sleep Depravation:

In sleep deprivation attack, the resources of the specific node/nodes of the network are consumed by constantly keeping them engaged in routing decisions. The attacker node continually requests for either existing or non-existing destinations, forcing the neighbouring nodes to process and forward these packets and therefore consume batteries and network bandwidth obstructing the normal operation of the network.

E) Impersonation Attack:

The attacker nodes impersonates a legitimate node and joins the network undetectable, sends false routing information, masked as some other trusted node.

F*)BlackHole*

MANETs are vulnerable to various attacks among them the black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. A black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path by sending fake RREP with higher sequence number to the source node in order to pretend like a destination node, So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the RREP packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself, due to this actual source and destination nodes are unable to communicate .It drops the packets or do not allows forwarding of packets to neighbours. This attack is known as blackhole as it swallow the data packets. [6]

G*)Grayhole*

A variation of black hole attack is the gray hole attack, in which the nodes will drop the packets selectively. Selective forward attack is of two types they are :-

- Dropping all UDP packets while forwarding TCP packets and another may be Dropping 50% of the packets or dropping them with a probabilistic distribution. These are the attacks that seek to disrupt the network without being detected by the security measures.
- Gray hole is a node that can switch from behaving correctly to behaving like a black hole that is it is actually an attacker and it will act as a normal node.[7] So we can't identify easily the attacker since it behaves as a normal node. Every node maintains a routing table that stores the next hop node information which is a route packet to destination node . If a source node is in need to route a packet to the destination node it uses a specific route and it will be checked in the routing table whether it is available or not. If a node initiates a route discovery process by broadcasting Route Request (RREQ) message to its neighbour, by receiving the route request message the intermediate nodes will update their routing tables for reverse route to the source . A route reply message is sent back to the source node when the RREQ query reaches either to the destination node or to any other node which has a current route to destination.

H)Wormhole :-A wormhole attack is considered dangerous as it is independendent of Mac Layer . Wormhole attack is also known by name of tunneling attack. In this paper we specifically considering Tunneling attack which does not require exploiting any nodes in the network and can interfere with the route establishment process by capturing packet from one point in the network, and tunnels the recorded packets to another point which is a malicious node and later on packets in the network can be transmitted again locally [8].In wireless ad hoc networks, it is difficult to trace out wormhole attacks because malicious nodes behaves as legitimate nodes.

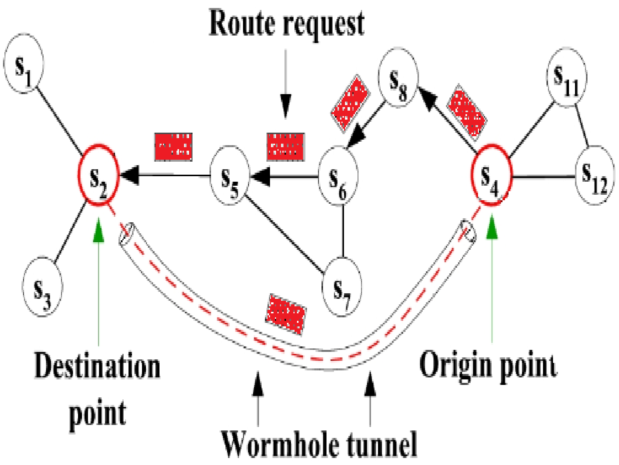

Fig. 1 Wormhole Attack depiction

In Fig-1. Node s9 wants to send data to node s2. The malicious node forwards the RREQ broadcasted from node s9 through the wormhole link to node s2 in return it replies with a route reply via the wormhole link. Thus by creating tunnel , these hops pretend to be neighbours.

III. Related Work

A)*Packet* Leashes

Packet Leashes is any information that is added to a packet designed to restrict the packets maximum allowed transmission distance. Leashes are designed to protect against a wormhole over a single wireless transmission, when packets are send over multiple hops each transmission requires a new leashes.[9] A Temporal Leash ensures that the packet has an upper bound on its lifetime, which restrict the maximum travel distance, since the packet can travel atmost at the speed of light. To construct a temporal leash in general all 'nodes must have tightly synchronized clocks, such that the maximum diference between any two nodes clock .The value of the parameter must be known By all nodes in the network, and for temporal leashes ,generally must be on the order of a few Microseconds or even hundreds of a nanoseconds.This level of time synchronization can be achieved now with the hardware based on LORAN-C, GPS or on Chip atomic clocks.

A geographical Leash ensures that a recipient of the packet is within a certain distance from are sender.To construct a geographical leash, in general, each node must know its own location, and all nodes must loosely synchronized clocks. when sending a packet ,the sending node includes in the packet its own location and the time at which it sent the packet. When receiving a packet , the receiving node compares these values to its own location and the time at which it received the packet. If the clock of sender and receiver are synchronized to within some specific value, and V is the upper bound on velocity of any node,then the receiver can compute an upper bound on the distance between the sender and itself, dsr.Standard digital signature or other authentication techniques can be used to enable a receiver to authenticate location and timestamp in the received packet.In certain circumstances, bounding the distance between the sender and receiver dsr cannot prevent wormhole attack . For example when obstacles prevent communication between two nodes that would otherwise be in a transmission range, a distance based scheme would still allow wormhole between sender and receiver.

B)Location based end to end detection

Location Based End to End Wormhole Detection: In this scheme node estimates the minimum Hop count to the destination node based on the geographical information of two end hosts in which receiver information is present at source end by Route Reply packet during the Route discovery [10]. Now source compares the hop count value received from the receiver from route reply and the estimated value. If received value is less than estimation, the route which corresponds to a particular reply is marked as if wormhole is detected.Then after that source launches wormhole TRACING in which wormhole two end points are identifed in a small area provided that there are multipath exists between source destinations[. In Location based scheme, taking into assumption that geographical location can be measured through global positioning system(GPS) and all network nodes have to share pair wise key which are secret or hold both sender and receiver authentic public key which are secret or hold both sender and receiver authentic public keys. Thus end to end wormhole detection requires extremely tight time synchronization and GPS.

C) SECTOR

IN[11],secure(SECTOR) approach i.e tracking of node encounters was presented. It applied similar principle as packet leashes, with the difference that it measured the distance at a single hop and it required special hardware at each node.

The main idea of the proposed protocol is that the distance between two sensor nodes can be measured accurately based on the speed of data transmitted between them. SECTOR using mutual authentication with distance bounding (MADB) protocol does not require any clock synchronization and location information .with this protocol the nodes can determine their mutual distance at the time of encounter. They proposed a technique that enables a party to determine a practical upper-bound on its physical distance to another party. By measuring the time between sending out the challenges and receiving the responses, the first party can compute an upper-bound on the distance to the other party. Capkun et al. modified the distance-bounding protocol proposed by Brands and Chaum. The protocol allows both parties to measure the distance to the other party simultaneously. At the same time, it is considered that each pair of parties share a symmetric key, that the nodes are established before running the distance-bounding protocol between them.

D) Directional antennas

Directional antennas are employed for access restriction and neighbor discover in WSNs. Neighboring nodes are identified by zones where each zones are defined by directional antennas. The zones around each sensor are numbered 1 to N clockwise starting with zone 1 facing east. When a sensor node receives a signal from a sensor node for the first time, the sensor node can get the approximate direction of the signal and identify the unknown sensor node by its zone. After that the sensor node cooperates with its neighbouring nodes to verify the legitimacy of the unknown node, for example, by checking whether the unknown node is known by the neighbouring nodes. Directional Antennas can be considered as location based solutions and were used in [12] to prevent the wormhole attack.In DirectionalAntennas all nodes should be omni directional i.e in same direction,which itself is complex requirement.

E) Concept of Diffusion of Innovation

Diffusion of innovation is a social science concept with respect to adoption or rejection of a innovation by population. This Social Science Concept has different stages in the process of adopting or rejecting a idea and even consist of roles played by the individuals in the diffusing process .and Whereas roles played in the process are Innovators, Early Adopters,Early Majority,Late Majority and Laggards. The adoption of innovation begin with the early adopter in the system which is then followed by early majority and then late majority.The nodes which are early majority are highly suspected nodes for forming wormhole link. In the detection and prevention approaches based on actors, malicious nodes are avoided by network nodes even without previous direct interaction because of the penalties added to them by actors. Even if the early adopters are not involved in routing, the other network nodes have other actors to help protecting them._This method has the advantage of being simple with no computational complexity, which makes it suitable to a ad hoc networks with limited resources.

IV. CONCULSION

Ad Hoc Networks is an area that is being widely researched these days and is a very fast growing area.Power Control is a major area of improvement and also they need to be made more secure. Ad Hoc Networks have started to be implemented in the field today in battle_fields and also in disaster struck areas. As time goes by we can see more applications of Ad Hoc Networks various schemes of detection and prevention of the wormhole attack has been discussed. In wormhole attacks, as adversaries usually replay the genuine data packets, detection of these attacks is quite complicated.In this paper we have discussed what wormhole attack is actually and how to detect them in wireless environment. All the detection procedures have their own benefits and drawbacks. But there is no detection procedure which detects wormhole attack perfectly. Here we have basically surveyed the existing approaches which will help us in future to design a new approach for detecting the wormhole attack in wireless sensor network and MANET .

REFERENCES

[1] *MARIANNE A. AZER, SHERIF M. EL-KASSAS, AND MAGDY S. ELSOUDANI, "AN INNOVATIVE APPROACH TO WORMHOLE DETECTION AND PREVENTION".*

[2] *I. Guler, M. Meghdadi, and S. Ozdemir, "A survey of wormhole based attacks and their countermeasures in wireless sensor Networks," IETE Technical Review, vol. 28, no. 2, pp. 89–102, 2011.*

[3] Security against Spoofing Attack in Mobile Ad Hoc Network by Dr. Wesam Bhaya from European Journal of Scientific ResearchISSN 1450-216X Vol.64 No.4 (2011), pp. 634-643

[4] M.T.Refaei, V.Srivastava, L.Dasilva, M.Eltoweissy, "A Reputation-Based Mechanism for Isolating Selfish nodes in Ad-Hoc Networks," Second Annual International Conference on Mobile and Ubiquitous Systems, Networking and Services, pp.3-11, July, 2005.

[5] Intrusion Detection of Packet Dropping Attacks in Mobile AdHoc Networks Aikaterini Mitrokotsa, Rosa Mavropodi, Christos Douligeris Ayia Napa, Cyprus, July 6-7, 2006

[6] Mangesh Ghonge, Prof. S. U. Nimbhorkar "Simulation of AODV under Blackhole Attack in MANET, International Journal of Advanced Research in Computer Science and Software Engineering Volume 2, Issue 2, February 2012 ISSN: 2277 128X

[7] Onkar V.Chandure, Prof V.T.Gaikwad " A Mechanism for recognition & Eradication of Gray Hole attack using AODV Routing Protocol in MANET" IJCSIT , Vol.2,No.6, Jul 2011.

[8] Ritesh Maheshwari, Jie Gao and Samir R Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity In-formation", Department of Computer Science, Stony BrookUniversity Stony Brook, NY 11794-4400, USA

[9] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks," in 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), 2003, pp. 1976-1986.

[10] Xia Wang, JohnnyWong," An End -to-end Detection ofWorm-hole Attack in Wireless Ad-hoc Networks", Department of Computer Science Iowa State University Ames, Iowa 50011

[11] S. Capkun, L. Buttyan, and J. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks," in ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN) Washington, USA October 2003, pp. 1-12.

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