ISSN:0975-9646

Detection and Prevention Techniques for Wormhole Attacks

Chandandeep kaur
M.Tech Student
Department of Computer Science & Engg.
Sri Guru Granth Sahib World University
Fatehgarh Sahib,Punjab,India

Dr.Navdeep Kaur
Associate Professor & Head
Department of Computer Science & Engg.
Sri Guru Granth Sahib World University
Fatehgarh Sahib,Punjab,India

Abstract - Mobile Adhoc Networks(MANET's) are refers to self organizing in nature. In MANET's communication is done through multi hops with dynamic topology. Mobile nodes send data through wireless links, which means less secure environment and vulnerable to various attacks. There are various types of attacks which effect the data when it transfers from the source node to the destination node but wormhole attacks are most dangerous attacks and very frequently occurred in the wireless environment. In this paper we discuss the various detecting and preventing techniques for wormhole attacks.

Keywords- MANET,AODV, QOS, Wormhole Attack, Dynamic Topology,OLSR.

I. INTRODUCTION

AdHoc networks are infrastructure less and have no fixed routers .All nodes are capable of movement and connected dynamically in an arbitrary manner .Each node in this network function as router which maintains and discover the routers to other nodes in the network. These networks also called multi hop networks .In these networks every node has a fixed area in that particular area a node can send and receive data .The particular area defined by allocating the range in which the mobile node can send data and receive data .Due to this defined range nodes communicate through the multiple hops.Figure 1.1 represents mobile AdHoc network in which source node connected to destination node through multiple hops and dotted circles represents the area of each node.

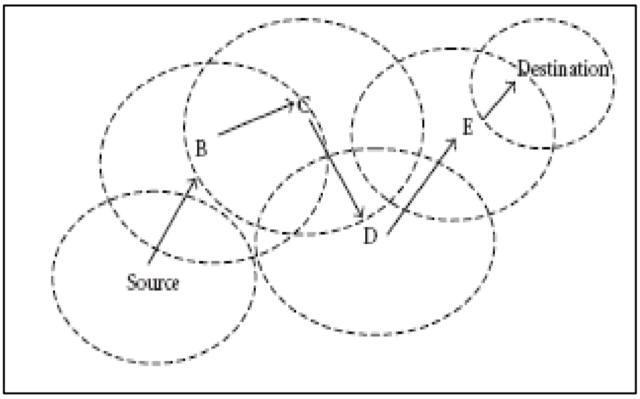

Figure. 1.1 Mobile AdHoc Network Model

Current challenges in the MANETS includes:-

1) Quality of service (QOS) :- Providing a stable QoS for different multimedia services in dynamically changing environment.
2) Dynamic Topology : - Due to the movement of nodes MANETS are highly dynamic in nature.
3) Multicast routing :- Designing of multicast routing protocol for a dynamically changing MANET environment.
4) Power consumption :- Since the nodes in MANET network has Limited battery life and limited processing power so ,they have rigorous power requirements.

II. WORMHOLE ATTACK

A wireless mobile ad hoc network consists of wireless nodes communicating without the need for a centralized admin. A collection of autonomous nodes that communicate with each other by forming a multi-hop radio network and maintaining connectivity in a decentralized manner is called an ad hoc network. There is not a static infrastructure for the network, such as a coordinator node or an administrate. The idea of such networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes .Due to wireless network attacks are more vulnerable to the network .The wormhole attack is the most vulnerable attack to wireless network. Routing is the act of moving information from a source to a destination in a network. During this process, at least one intermediate node within the network is encountered .Wormhole attack effect routing activities with the help of Malicious node and Wormhole tunnel .Malicious node is the false node which acts as the part of the network .Malicious nodes degrade the performance of the network or analyze the network traffic. These malicious nodes constitute the end points of the wormhole. The endpoints are connected using a high-speed link called a wormhole tunnel .Figure 1.2 represents the wormhole tunnel which is formed by two malicious nodes x and y. When malicious nodes form a wormhole they can reveal themselves or hide themselves in a routing path.

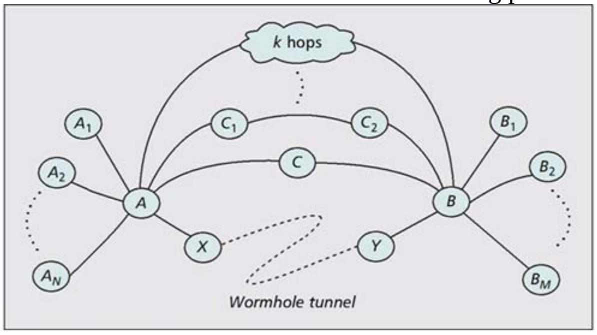

Figure1.2 Wormhole tunnel

Wormhole attack having two types 1).In band wormhole attack :-In this attack malicious node involve the mobile nodes which are the part of a valid network. Figure1.3(b) represents the in band attack in which all the network node are involved in the wormhole attack .This attack also called exposed attack [2] and Out of band wormhole attack:- In this attack only malicious nodes takes participation none of the node involved from the network .The figure 1.3(a) represents the out off band attack .This attack is also called as hidden attack[2]

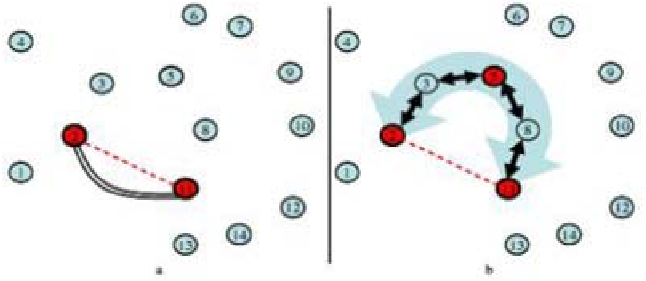

Figure1.3 (a) Out-of-band wormhole, (b) in-band wormhole

III. Detection And Prevention Techniques For Wormhole Attack

Zhou et al[5] proposed a new algorithm called Neighbor-Probe-Acknowledge (NPA) for detection of wormhole attacks. NPA does not require time synchronization or any other hardware. Moreover, it accomplish higher detection rate and lower false alarm rate than the methods using RTT under different background traffic load conditions. By theoretical analysis and comprehensive experiments, wormhole attacks links are easy to detect, standard deviation of *RTT* (*stdev*(*RTT*)) is a more effective metric than per-hop *RTT* to detect wormhole attacks.

Dhurandher et al[7] proposed an energy efficient scheme to detect the wormhole attack called Energy efficient scheme to immune the wormhole attack (E2IW). This protocol use the location information of the mobile nodes to find the presence of a wormhole, and in case a wormhole exists in the path, it discovers another routes involving the nodes of the selected path so as to get a more secure route to terminus. The protocol is capable of detecting wormhole attacks employing either hidden or participating malicious nodes. E2SIW can find wormholes with a high detection rate, less overhead, and can consume less energy in less time. This protocol keep down the overhead related with the control packets.

Abdesselam et al[3] presented an effective method for detecting and preventing wormhole attacks in OLSR.To find wormhole tunnels a simple four-way handshaking message exchange method is used. The proposed solution is easy to deploy: it does not need the time synchronization or any location information .It does not require any complex computation or special hardware requirement. The performance of this approach shows a high detection rate under various scenarios. This method first attempts to pinpoint links that may potentially be part of a wormhole tunnel, then after a proper wormhole detection method is applied to suspicious links by means of an exchange of encrypted probing packets between the two supposed neighbours (end points of the wormhole).

S. Gupta et al [8] proposed an approach, called WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on the AODV protocol and considered to detect wormhole attack with the help of hound packets. In this approach a hound packet is sent after the route discovery process that means after the route has been discovered. This hound packet is processed by all the nodes except that nodes which are involve in the path setup process. Basically the path discovery is done by the help of the two types of packet, called RREQ and RREP. When the sender gets the message, it creates a hound packet and computes its message digest and signed this message digest with its own private key and attached all this information with the hound packet. But processing delay of the packet becomes high[4].

Yih-Chun Hu et al [9] described that the wormhole attack can form a serious threat in the wireless network security, specially against many ad hoc network routing protocols and location-based wireless security systems. To detect and defend against the wormhole attack ,two types of leash information were used Geographical Leash and Temporal Leash. Geographical leashes presents that each node must have accurate location information and loose clock synchronization. Whenever a node receives a packet, it calculates distance between previous node and itself by using send/receive time stamp. In 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 node.

Chiu et al[4] identified two types of attacks:

- Malicious node does not involved in finding routes
- Authorized nodes aware of the existence of malicious nodes

[4] proposed an efficient detection method called Delay Per Hop Indication (DelPHI). There are different paths to the destination node so, by observing delays per hop the source node is capable to detect both kinds of wormhole attacks. This method does not require any synchronized clocks or any special hardware for mobile nodes. Advantages of DelPHI are following:

- DelPHI does not require clock synchronization an position information.
- some special hardware's are not required in the DelPHI scheme, thus it provides higher power efficiency.

Mary et al[1] examined the performance of reactive multicast routing protocol Multicast Ad hoc On demand Distance Vector Protocol (MAODV) under the influence of worm hole nodes under different scenarios and design a Worm Hole Secure MAODV (WHS-MAODV) by applying certificate based authentication mechanism in the route discovery process. The proposed technique can greatly enhance network performance in the presence of attacking nodes. WHS-MAODV is as effective as MAODV in discovering and maintaining routes in addition to providing the required secure environment. The proposed protocol reduces the packet loss due to malicious nodes to a considerable extent thereby improve the performance.

Mary et al[2] analyzed the performance of reactive multicast routing protocol On Demand Multicast Routing Protocol (ODMRP) under the influence of worm hole nodes under different scenarios and design a Worm Hole Secure ODMRP (WHS-ODMRP) by applying certificate based authentication mechanism in the route discovery process. The proposed protocol reduces the packet loss due to malicious nodes to a considerable extent thereby enhancing the performance.

Lazos et al[6] proposed the use of geometric random graphs induced by the communication range constraint of mobile nodes, this paper present the necessary and sufficient conditions for detecting and defending against wormhole attacks. This theory also presents a defence mechanism based on local broadcast keys. In this cryptography based solution relaying on local broadcast keys.

Yang Su et al[11] proposed a WARP(Wormhole Avoidance Routing Protocol).This is a secure routing protocol which is based on AODV(Ad Hoc On demand Distance Vector) routing protocol .During path discovery phase ,WARP considers link joint multipath and provides secure path .Based on the characteristics that wormhole nodes can easily take information of routing from source node to the destination node.

Khalil et al[12] presented a lightweight protocol called LITEWORP to detect thee malicious nodes and remove the wormhole attacks in AdHoc networks .This proposed protocol uses secure two hop neighbour discovery and information about the whole traffic to detect the malicious nodes which are part of the wormhole attack .This technique isolate the malicious nodes and provides the secure network for future routing.

Gambhir et al[13] proposed a PPN(Prime Product Number) for detection and removal of wormhole attack .In this scheme every cluster head node maintains a neighbor table which is used for the information about every node which will create a route that does not go through a node whose replied information is wrong and PPN is not fully divisible .Therefore malicious nodes will be gradually avoided by other non malicious node in the network

IV. COMPARISON OF DIFFERENT WORMHOLE DETECTION AND PREVENTION TECNIQUES

METHOD	BASED ON	EXTRA HARDWARE REQUIREMENT	SYNCHRONIATION
NPA		No	NPA does not require time synchronization
E2IW	AODV	Yes	No Need
Simple Four-way Handshaking	OLSR	No	No Need
WHOP	AODV	Yes	No Need
Temporal Leash Technique	AODV	No	Medium synchronization
Geographical Leash	AODV	Yes	Low synchronization
DelPHI	AODV	No	No Need
LITEWORM	AODV		No Need
PPN	AODV	No	No Need

V. CONCLUSION

The Mobile Ad Hoc network is greatly influenced by wormhole attack .These attacks degrade the network performance and menace to network security .In this paper various techniques are presented for detection and prevention of wormhole attacks .In future these approaches will help to efficiently remove the malicious nodes from the Mobile Ad Hoc networks .All above techniques based on different factors like cost ,need of security ,Quality of Service may lead better result but can be costly . So we cannot say that one solution is perfectly deal with all conditions .One factor may have effect on the other factor .Like some networks need more security like whether forecasting and military area may increase the cost. From all above solutions we can find the efficient method to prevent the wormhole attacks by equating all factors.

REFERENCES

[1] E.A.Mary Anita,V.Vasudevan and A.Ashwini, “A Certificate-Based Scheme to Defend Against Worm Hole Attacks in Multicast Routing Protocols for MANETs” *IEEE*,pp.407-412,2010.

[2] E.A.Mary Anita, V.Thulasi Bai, E.L.Kiran Raj and B.Prabhu, “Defending against Worm Hole Attacks in Multicast Routing Protocols for Mobile Ad hoc Networks”, *IEEE*,2011.

[3] Farid Nait Abdesselam, Brahim Bensaou and Tarik Taleb**,** “Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks*”, IEEE Communications Magazine* , pp.127-133,April 2008.

[4] H.S. Chiu, K.S. Lui,“DELPHI: Warmhole Detection Mechanism for Adhoc Wireless Networks”, *1st International Symposium on Wireless Pervasive Computing*, pp.6–11, January 2006.

[5] Jie Zhou, Jiannong Cao, Jun Zhang, Chisheng Zhang and Yao Yu, “Analysis and Countermeasure for Wormhole Attacks in Wireless Mesh Networks on a Real Testbed”, *IEEE International Conference on Advanced Information Networking and Applications*,pp.59-66,2012.

[6] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L. W. Chang, “Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic”, *Collaborative Technology Alliance (CTA)*,2010.

[7] S.K. Dhurandher and I. Woungang ,"E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks",*26th International Conference on Advanced Information Networking and Applications Workshops*, pp.472-477, 2012.

[8] S. Gupta, S. Kar and S.Dharmaraja, “WHOP: Wormhole Attack Detection Protocol using Hound Packet”, *International Conference on Innovations in Information Technology”,IEEE Transactions*, pp.226-231, 2011.

[9] Y.C. Hu, A. Perrig and D. B. Johnson, “PACKET LEASHES: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks”, *IEEE INFOCOM*, pp.1976–1986, 2003.

[11] Ming-Yang Su, “WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile ad hoc networks”, *Elsevier Ltd*,pp. 208-224,2010.

[12] Issa Khalil, Saurabh Bagchi and Ness B. Shroff, “LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks”, *International Conference on Dependable Systems and Networks,IEEE*,pp.1-10,2005.

[13] Sapna Gambhir and Saurabh Sharma, “PPN: Prime Product Number based Malicious Node Detection Scheme for MANETs”, *3rd IEEE International Advance Computing Conference (IACC)*,pp. 335-340,2012.