IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Surveying Wormhole Attack and Their Different Existing Detection Techniques

Niharika Shrivastava[1], Prof. Tilotma Sharma[2]

M. Tech Student, Department of CSE&IT, Mahakal Institute of Technology, Ujjain[1]

Reader, Department of CSE& IT, Mahakal Institute of Technology, Ujjain[2]

Abstract: In recent scenario, as the technology increasing communication and computing service are in demand, these services are operating under MANET. MANET is a self organizing wireless network which required more security than other networks. In wireless network the probability of attack is very high and in MANET security becomes one of the major issues of this type of network. Among several type of attack, wormhole attack is one of the most threatening and severe attack in routing. In wormhole attack it establish a tunnel shaped link between the network in which one malicious node will transfer packet from tunnel to another malicious node in a network and replays them locally .to prevent and detect this attack many researchers have proposed the solution and methods for attack. This paper will focus on the different aspects of the prevention and detection technique of wormhole attack.

Keywords: MANET, Wormhole Attack, Detection Technique.

1. INTRODUCTION

Now a day's mobile adhoc network become one of the most popular and way for communication because it has no boundation regarding to the network like topology, infrastructure and centralization of network. This makes the MANET different from other network , it determine the feasibility of achievement in solving many real world problems for e.g. in emergency system, military network etc[6].MANET has power to self configuring its node in a network and each device is moving independently in network. There is no fixed base station for communication MANET does not have any static network, its topological changes are unpredictable, because of its dynamic nature vulnerability towards attack increases, and this makes the network in secured who affect the network integrity, confidentiality accuracy and performance of the network. Due to this the overall efficiency of the network gets affected and disgraces the performance of Manet.

2. WORM HOLE ATTACK

The wormhole attack is one of the most severe and threatening attack. This is network layer and routing attack and it is particularly challenging to prevent it .In wormhole attack an adversary receives packets at one end location in network and tunnel them into the another end location in a network. The link through which the packets are sent via tunnel is low latency link between the nodes and replays them to each other in a network. In fig X and y are two wormhole nodes connected via wormhole link. X replays neighbor in one area Y hear in another area of network and vice-versa.

The overall results drawn from the attack is that all nodes one area assumes to be in another area. This result creates routing and connectivity problem in a network. After the attack, once new route started using shortcut wormhole node starts dropping packets and causing disruption in network [8] .Wormhole attack also cause denial of service by unauthorized access, create congestion and route disruption. Denial of service prevents the discovery of legitimate route and unauthorized access allowed to access wireless control system which is based on the physical proximity [1]. Wormhole can be created by using in-band out-band channel. In-band channel [6] where malicious node forward the request packet to another malicious node via other nodes of the network, other is out-band channel where one malicious node which is directly connected via other malicious node. These two methods are used to get the confidential data from the network.

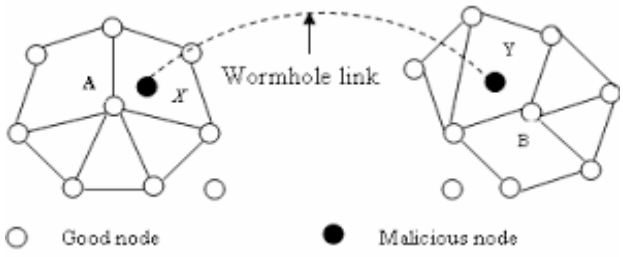


FIG.1

2.1 TYPES OF WORMHOLE ATTACK

S.No	Attacks	Description
1.	OPEN WORM HOLE	The source and destination nodes area visible. Attacker includes themselves in packet header and nodes are aware about the presence of malicious node.
2.	HALF-OPEN WORM HOLE	One side of the network is visible and other is hidden. One side in a network is modified by malicious node and rebroadcasted.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

3.	CLOSED WORM HOLE	In this attack all intermediate nodes are in between malicious nodes and their identity is hidden. The attacker does not modify the packet tunnel them from one side to another & rebroadcast.

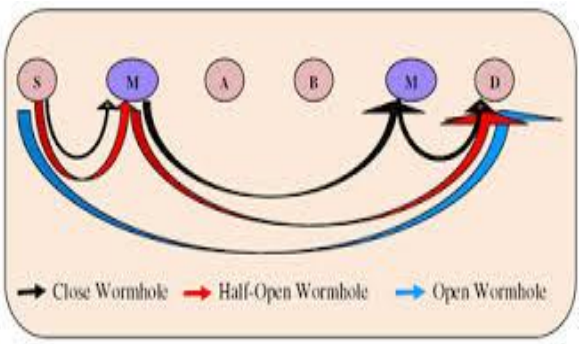


FIG.2

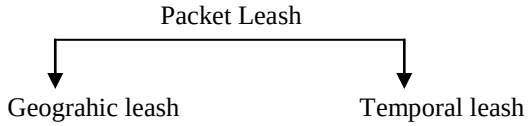
The different modes of wormhole attack is discussed above the prediction of such attack is very difficult & they are invisible forms of attacks where end points are not visible in the network path .so, there detection also become complicated.

3. DETECTION METHOD/MECHANISM OF WORMHOLE ATTACK

In this section different method of detecting wormhole attack is described.

3.1 PACKET LEASHES

In packet leashes the detection of wormhole is done with help of geographic location which will measure distance between nodes. Clock synchronization is strictly required to perform the practical solution. The packet leashes method is further classified in two type's i.e Geographic and Temporal leashes. In geographic leash each node knows its position and all nodes is loosely synchronized. In this time between the sender and receiver is calculated that how much it will take to travel across the network. Second one is temporal leash in this the difference between the sending time and receiver time is calculate and it will required fine synchronization.[5]



3.2 SECTOR (secure tracking of node encounter)

In this method one bit challenges respond with no delay in packet leash. SECTOR is one of the hardware based approach which is used for secure tracking. In secure tracking, directional antenna is used for sending message. It will bound the maximum distance between neighbor nodes. The use of particular hardware like directional antenna may become complicated to implement for hand held services in network [7].

3.3 LITEWORP

It is used to recognize wormhole attack in adhoc network , based on local traffic observation at some selected nodes in a network this furnish a counter measure procedure that isolate the malicious node from network there by removing there ability to cause future damage . Liteworp has several features that make it especially suitable for resource-constraint wireless habitat. Liteworp does not require particular hardware and time synchronization in a network[12].This [1]detection method may introduce other attack such as blackmail attack through imitation .

3.4 DELPHI (delay per hop indicator)

Delphi was proposed by Hon sun chiu and king shan lui . this method used protocol delay per hop indicator, and it is able to detect both hidden and exposed wormhole attack . Delphi is designed to find out every available disjoint route between source and destination .To indicate wormhole , hop count and delay per hop is monitored . The greater delay per hop will justify the presence of wormhole but the location of wormhole can not be identify by delphi method .[7]

3.5 TRUST BASED APPROACH

The goal of this approach is to finding out the trust level of each neighbor node . The trust based model will calculate the reliable path to particular destination .The level in this approach decides the presence of wormhole attack, lower the level of trust the presence of wormhole is identify. assume that all packets drop by wormhole in system it have the least trust level easily eliminated[7] .

3.6 SECURE NEIGHBOR DISCOVERY

Secure discovery approach is effective for counter wormhole attack. [13] introduced about detection and isolation protocol against wormhole attack . They give a method that is applicable for detection of attack except protocol divergence .This method consist of two step -In first step list of neighbor node is prepared and in second step where a node monitor the traffic going in and out of neighbor node , this removes the malicious node and ability to cause future damage in the network.

4. PREVENTION AGAINST WORMHOLE ATTACK

In prevention of wormhole assume that all nodes will monitor the behavior of its neighbor. Every node will send a RREQ at receiver. If source will received a message within particular time It detect the occurrence of wormhole and add route to list .The node maintain its each neighbor node table that contain the serial no. of the neighbor node id ,sending time ,receiving time RREQ and count. the source have set the wormhole prevention time after sending request message wait until neighbor confirm its transmission. So that delay per hop value must not exceed estimated wormhole prevention time and support distance source routing based on the end to end, signature authentication of routing.

Time of flight is another prevention method found which is used to prevent attack in mobile adhoc network. In this the total journey roundtrip time of message is calculated

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

between all nodes. The estimated distance of node is calculated and check it is in possible available communication range or If wormhole attack is identified packet travelling time is increased and will not returned in particular estimated time.[2]

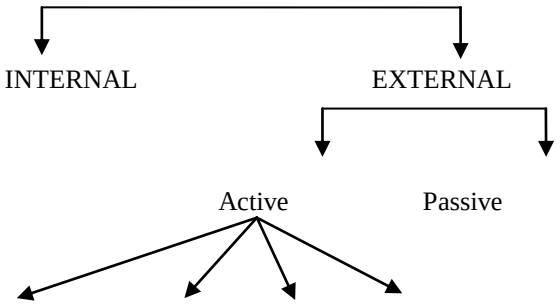
5. SECURITY ATTACKS IN MANET

MANET is a class of wireless network which have mobile nodes, they are more vulnerable to attack due to their properties such as disperse node, decentralization .security in adhoc network become big challenge in the field of wireless network. The attack in network may be external or internal. The nature and structure of this type of network makes it attractive towards different types of attackers. Different types of attackers will try to decrease the performance of the network. The different categories of attack and attackers against MANET are classified.

A. Categories of attacker in MANET

TYPES OF ATTACKER	TYPES OF ATTACK PERFORMED
Emission	Active , Passive
Location	Insider, Outsider
Quantity	Single, Multiple
Motivation	Confidentiality, integrity, selfishness, privacy, unauthorised
Rationality	Naïve, irrational , rational
Mobile	Fixed , Mobile

B. TYPES OF ATTACKS



Internal attacks – **Internal** attacks are direct attack on the node present in the network and the links which are present in between them.

External attack - External attacks are carried out by nodes that are not the part of the network. These attacks will try to create congestion in congestion in network and intercept the normal communication. The external attacks are classified in two categories.

a. Active attacks - Active attacks are very grievous attack on network. That prevents the message to flows between the nodes. This attack may be internal or external. Active external attacks are from node outside the network and internal active attack in which node is malicious and part of network. The detection of the active attack is harder then external attack. Active attacks are further classified as **dropping, modification, fabrication, timing attacks** [10]

b. Passive attack – MANET are most vulnerable to passive attack. It does not change the data transmitted within the network. But it involved unauthicated listening to network traffic and collects data from it. The attacker will not disrupt the operation from the routing protocol attempt to fetch the important information from the traffic. Detection is difficult in this type of attack. To control this attack some encryption techniques have to be used to encrypt the data being transmitted [10]

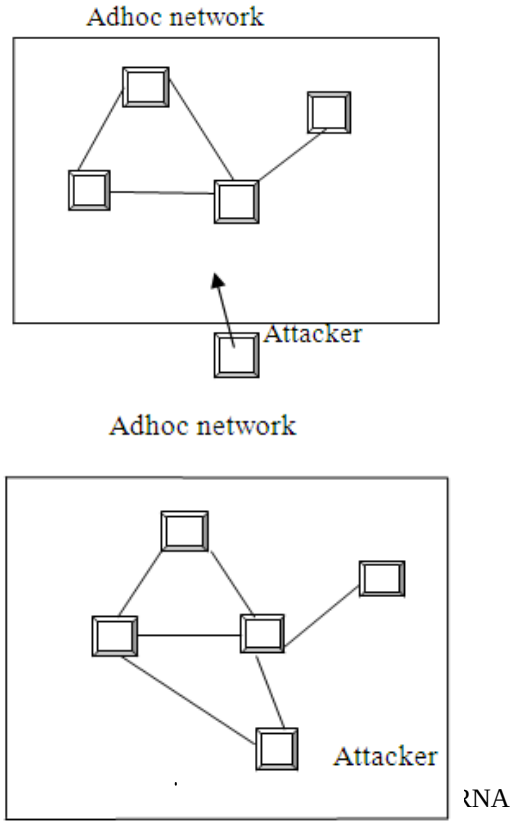


Fig. 3 External & Internal attack

6. CONCLUSION

In this paper, the existing methods and wormhole attack has been introduced with different types and its attacking modes. Also some detection and prevention technique of wormhole attacks has been discussed. With the help of them new effective approach can be designed to detect the attack in MANET. This survey is beneficial for various challenges in research field of wormhole attack. The different type of attack by wormhole is discussed. There is still need of some effective method to diminish the attacks in adhoc network.

REFERENCES

1. Shilpa jaiswal , sumeet agrawal , A novel paradigam : detection and prevention of wormhole attack in mobile adhoc network, International journal of engineering trends and technology,vol3 Issue 5,2012
2. Jyoti thalor , ms.Monika ,detection and prevention technique in mobile adhoc network: review,International journal of advanced research in computer science and software engineering ,vol 3 Issue 2, february 2013

3. Vandana c p ,Dr. A. francis savior devaraj ,A multilayered detection mechanism for wormhole attack in AODV based MANET ,International journal of security and trust management vol 2 NO.3 , june 2012
4. K.sivakumar ,Dr. g. selvaraj ,Analysis of wormhole attack in MANET and avoidance using robust secure routing method , International journal of advanced research in computer science and software engineering vol 3 issue 1, January 2013
5. Maria Sebastian , Arun raj kumar, A novel solution for discriminating wormhole attack in MANET from congested traffic using RTT and transitory buffer , International journal of computer network and information securityy , 8, 28-38 , aug 2013
6. Umesh kumar chaurasia ,Mrs. varsha singh, MOified wormhole detection AODV protocol
7. Nishant Sharma , Upinderpal singh ,Vrious approaches to detect wormhole attack in wireless sensor networks , international journal of computer science and mobile computing vol 3 issue 2 february 2014
8. Moutushi singh , Rupayan das, A survey of different technique for detection of wormhole attack in wireless sensor network , International journal of scientific & engineering research vol 3 issue 10 october 2012
9. Priyanka Sharma , H.P. sinha , Abhay bindal, detection and prevention against wormhole attack in AODV for mobile adhoc network , International journal of computer application vol 95 ,NO.13,june 2014
10. Gagandeep, Aashima , Pawan kumar,Analysis of different security attacks in MANET on protocol stack: Review , International journal of engineering and advance technology, vol 1 ,issue 5, june 2012
11. Ali Dorri and Seyed Reza Kamel and Esmail kheyrkhah, Security Challenge in mobile adhoc networks: A Survey, International journal of computer science &E ngineering Survey (IJCSES) Vol.6, No.1, February 2015
12. J.Erickson, S. krishnamurthy, M. faloutsos. True link: A practical countermeasure to the wormhole attack. In the 14 th ieee international conference.
13. Issa Khalil , Saurabh bagachi , Ness B.Shroff ,Liteworp: Detection & isolation of wormhole in static multihop wireless network