



A Comparision Of Wormhole Dtection Methods in MANETS

Sonia Ohri
Computer science department
Maharishi Markandeshwar university, Mullana
Ambala , India
Soniaohri818@gmail.com

Sapna Boora
Computer science department
Maharishi Markandeshwar University, Mullana
Ambala, India
Sapnaboora@gmail.com

Abstract: MANET due to its wireless transmission nature contains more security issues as compared to wired networks .These security issues are very important to deal with so as to make network secure. Wormhole attack also called as tunnelling attack is very difficult to detect. wormhole generally possess two properties In this paper we have studied the wormhole attack along with its properties and various method have been discussed for identification , removal, and prevention of wormhole attack and then they have been compared to one another so that effective methods should come forward .This study aims to combine some methods or to modify the one.

Keywords: MANETS, VANETS , wormhole attack

I. INTRODUCTION

Mobile adhoc networks is a collection of nodes that do not rely on predefined infrastructure to keep network connected. It is also called mobile mesh network or wireless ad hoc network. In MANET, every device works as a router and free to move in any direction. Using this property, we can send data over a long distance. It provides high mobility and device portability's that enable to node connect network and communicate to each other. connections among nodes are limited to their transmission range, and cooperation with intermediate nodes is required for nodes to forward the packets to other node outside of their transmission range. These properties make security of MANET vulnerable to attackers, and an attacker can modify the routing protocol and disrupt the network operations such as packet drop, selective forwarding, and data fabricating. 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 Security attacks are basically classified as follows :

a. Active and Passive Attacks: In passive attack there is not any alteration in the message which is transmitted. There is an attacker (intermediated node) between sender & receiver which reads the message. This intermediate attacker node is also doing the task of network monitoring to analyse which type of communication is going on.

The information which is routing through the nodes in MANET is altered by an attacker node. Attacker node also streams some false information in the network. Attacker node also do the task of RREQ (re request) though it is not an authenticated node so the other node rejecting its request due these RREQs the bandwidth is consumed and network is jammed.

b. Internal and External attacks: Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

External attacks are carried out by nodes that do not belong to the domain of the network.

c. Layer Specific attacks: The attacks can be further classified according to the five layers of the Internet model.

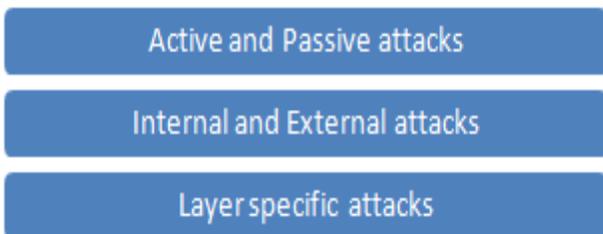


Figure 1 Types of attacks

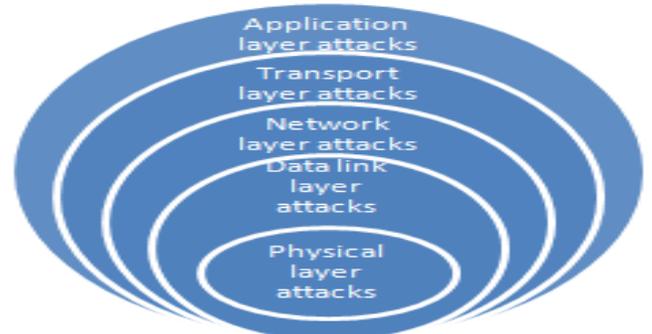


Figure 2 layer specific attacks

- a) **Application layer attacks:** Repudiation , Data corruption
- b) **Transport layer attacks:** Session hijacking, syn flooding
- c) **Network layer attacks:** Worm hole , Black hole , Byzantine attacks
- d) **Data link layer attacks:** Traffic Analysis ,WEP weakness
- e) **Physical layer attacks:** Jamming , Eavesdropping

The foremost concerned security issue in mobile ad hoc networks is to protect the network layer from malicious attacks, thereby identifying and preventing malicious nodes. A unified security solution is in very much needed for such networks to protect both route and data forwarding operations in the network layer. There are various attacks at network layer out of them Worm hole attacks is difficult to detect and deal with so in this paper we are listing various methods that can be used for the detection and removal of worm hole attacks.

This paper we are firstly discuss the vulenrabilities of mobile adhoc networks then introduce details of worm hole attack, then list various methods for detection of worm hole attack and finally removal methods.

II. VULENRABILITIES OF MANETS

- a. **Dynamic topology:** In MANETs, nodes can join and leave the network dynamically and can move independently. Due to such type nature there is no fixed set of topology works in MANETs. The nodes with inadequate physical protection may become malicious node and reduce the network performance
- b. **Wireless links:** As the nodes in such networks are interconnected through wireless interface that makes it highly susceptible to link attacks. The bandwidths of wireless networks are less as compared to wired networks which attracts many attackers to prevent normal communication among nodes.
- c. **Cooperativeness:** In MANETs, all routing protocols assume that nodes provide secure communication. But some nodes may become malicious nodes which disrupt the network operation by changing routing information etc
- d. **Lack of clear line of defence:** There is no clear line of defence mechanism available in the MANETs; attacks can come from any directions. Attackers can attack the network either internally or externally
- e. **Limited resources:** The MANETs consists of different set of devices such as laptops, computers, mobile phones etc. All of such devices having different storage capacity, processing speed, computational power etc. This may attracts the attackers to focus on new attacks.

III. WORMHOLE ATTACK

Network layer is the third lowest layer of OSI reference model. The function of network layer in OSI layer model is to provide the services for exchanging the individual piece of data/information over the network between identified end devices. The network layer in MANET uses ad hoc routing

and does packet forwarding. In MANET nodes act as host and router. Therefore router discovery and router maintains in the MANET is effectively concern. Thus attacking on MANET routing protocol not only disrupt the communication on the network even worst it paralyzed the whole communication all over the network. Therefore, a security in network layer plays a vital role to ensure the secure data communication in the network. The wormhole attack is one of the most efficient and merciless attacks, which can be executed within MANET. Therefore two collaborating attackers should establish the so called wormhole link connection via a direct low-latency communication link between two separated distant points within MANET[12]. As soon as this direct bridge (wormhole link) is built up one of the attackers captures data exchange packets, sends them via the wormhole link to the second one and he replays them.

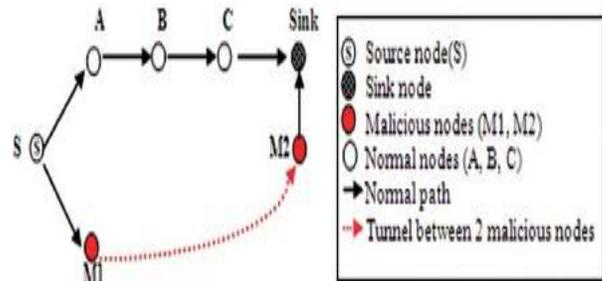


Figure 3 Description of wormhole attack

In a wormhole attack, malicious node m1 first captures routing message from a neighboring node, and then sends the message to another malicious node, m2, by means of a secret tunnel, m2 then broadcasts or propagates the message received. In this way, a tunnel-like channel is formed between the two malicious nodes.

Even though the tunnel has a very long distance, other normal nodes may mistakenly think that there is only a distance of a one-hop count.

A. Wormhole Attacks Types :

By categorizing the attacks into its types makes it easier for its prevention and detection so here wormhole attack has been classified as

- a. **Open Wormhole attack:** In this type of wormhole, the attackers include themselves in the RREQ packet header following the route discovery procedure. Other nodes are aware that the malicious nodes lie on the path but they would think that the malicious nodes are direct neighbours.
- b. **Closed Wormhole Attack:** The attackers do not modify the content of the packet, even the packet in a route discovery packet. Instead, they simply tunnel the packet form one side of wormhole to another side and it rebroadcasts the packet.
- c. **Half open wormhole attack:** One side of wormhole does not modify the packet and only another side modifies the packet, following the route discovery procedure.

B. Wormhole Attacks Modes:

Worm hole attack can be launched using several modes they are described as under

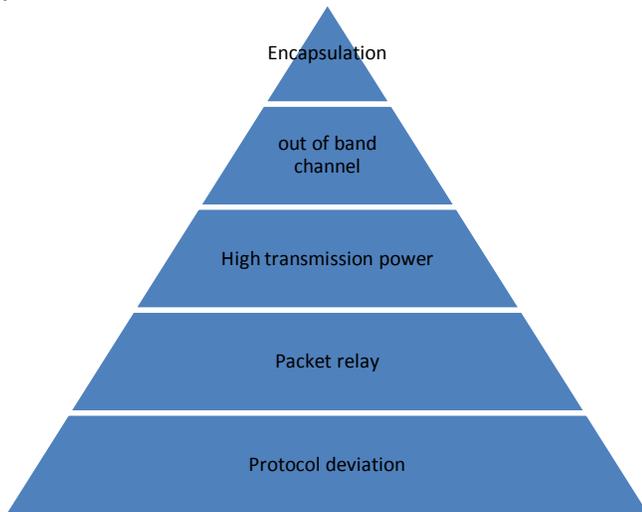


Figure 4 Description of wormhole attack modes

- a. **Worm hole attack using Encapsulation:** When the source node broadcast the RREQ packet, a malicious node which is at one part of the network receives the RREQ packet. It tunnels that packet to a second colluding party which is at a distant location near the destination, it then rebroadcasts the RREQ. The neighbours of the second colluding party receive the RREQ and drop any further legitimate requests that may arrive later on legitimate multihop paths. The result is that the routes between the source and the destination go through the two colluding nodes that will be said to have formed a wormhole between them. This prevents nodes from discovering legitimate paths that are more than two hops away.
- b. **Worm hole attack using out of band channel:** This channel can be achieved, for example, by using a long range directional wireless link or a direct wired link. This mode of attack is more difficult to launch than the previous one since it needs specialized hardware capability.
- c. **Worm hole attack using high transmission power:** Another method is the use of high power transmission. In this mode, when a single malicious node gets a RREQ, it broadcasts the request at a high power level, a capability which is not available to other nodes in the network. Any node that hears the high-power broadcast rebroadcasts it towards the destination. By this method, the malicious node increases its chance to be in the routes established between the source and the destination even without the participation of a colluding node.
- d. **Worm hole attack using packet relay:** Another mode of the wormhole attack is by using packet relay. In this mode a malicious node relays packets between two distant nodes to convince them that they are neighbours. This mode can be launched by even one malicious

node. It involves the cooperation by a greater number of malicious nodes, which serves to expand the neighbour list of a victim node to several hops

- e. **Worm hole attack using protocol deviation:** During the route request forwarding, the nodes typically back off for a random amount of time before forwarding. This is motivated by the fact that the request forwarding is done by broadcasting and hence, reducing MAC layer collisions is important. A malicious node can create a wormhole by simply not complying with the protocol and broadcasting without backing off. The purpose is to let the request packet it forwards arrive first at the destination and sit is therefore included in the path to the destination. The advantage of this mode is that the control packet arrive faster. The challenge for this mode is that there is a possibility of collision to occur between transmissions of malicious nodes

IV. METHODS FOR WORMHOLE DETECTION

This section represents the various methods to detect and remove wormhole attack.

In [1] debdutta barman roy proposed a method based on countermeasures for clusters. In this method a two layer approach is used for detecting whether a node is participating. The layered approach is introduced to reduce the load of processing on each cluster heads. From security point of view, this will also reduce the risk of a cluster head being compromised. The presented algorithm states that initially network is divided into clusters then cluster with minimum id is chosen as cluster head. once the cluster head for both clusters is selected then node nearest to the both cluster heads is chosen as guard node. source sends hello packet to the destination and the time is calculated then source sends the data and calculates the time then both the timers are compared. depending upon these calculations wormhole attack is detected. This technique is implemented on AODV.

In [2] Anil kumar proposed an approach to prevent the wormhole attack using digital signatures. This method is divided into two phases. In the first phase delay/hop count and verification of digital signature information is collected. And in the second phase analyzes the collected information obtained in first phase to detect whether there is any wormhole attack present or not. The reason behind is that under normal situation, the delay a packet experiences in propagating one hop should be similar along each hop along the path. However, under a wormhole attack the delay may unreasonably high or low, since there are in fact many or no hops between them. Therefore, if we compare the delay per hop of a legitimate path with the delay per hop of a path that is under wormhole attack, we should find that the delay of the legitimate path is smaller. Therefore, if path has distinguishable high or low delay value, it is likely to be subjected to a wormhole and another technique is used for pin point detection of wormhole digital signature technique, it is assumed that each legitimate node shares the digital signature of every node in the network and the malicious node does not have its own digital signature.

Our mechanism is designed specifically for AODV routing protocol in mobile ad hoc network.

In [3] P.anitha proposed an approach based on path tracing method. Path Tracing (PT) algorithm for detection and prevention of wormhole attack as an extension of AODV protocol. The PT algorithm runs on each node in a path during the AODV route discovery process. It calculates per hop distance based on the RTT value and wormhole link using frequency appearance count. MASK is based on a special type of public key cryptosystem, the pairing based cryptosystem to achieve anonymous communication in MANET.

In [4] Once the route is defined in between source node and destination node, the next step is to authenticate the sender and receiver. To authenticate the sender and receiver, here we use the double encryption technique to increase the security level against the wormhole attack. In proposed technique, session key and generated time will be stored in the token. This token is issued by the issuer, if issuer is convinced about the security level of sender or subject node. This token is encrypted with the Receiver's public key and the whole token is encrypted with Sender's Private key, if the sender's private key is authorized that token will be decrypted by the sender's public key. Now the whole token is decrypted by the receiver's private key. Session Key[10] is one time Key, if there is any delay in the transmission that key will be expired and packet will be loosed. At that time the subject node will record the activity of next node, if the RREQ is hold by the node more than the time interval, session key is expired at that node, that node is treated as suspicious node. The response of expire token is automatically generated and received by the receiver with the suspected id. The Token will be encrypted by the private key of sender so that we called token as digital signature certificate.

In [5] Shalabh jain proposed a method based on channel characteristics In this paper, we devise a novel scheme for detecting a wormhole by utilizing the inherent symmetry of electromagnetic wave propagation in the wireless medium. We demonstrate the loss of this symmetry in case of a wormhole attack and propose a method to detect and flag the adversary. We modify the insecure neighborhood discovery to incorporate authentication.

In [6] Phuon Van Tran proposed an approach based on Transmission time based mechanisms. In our mechanism, when a node establishes a route to another node, we will try to check whether there is a wormhole link in that route or not by calculating every Round Trip Time (RTT) between two successive nodes along the route. Each node in the established route will compute the RTT between it and the destination, then send this value back to the source node. The source node collects all of these RTT values, calculating RTTs between two successive nodes and identifying wormhole based on the fact that RTT between two fake neighbors or two wormhole links will be considerably higher than that between two real neighbors.

In [7] Saurabh Upadhyay proposed an approach for avoiding wormhole attack using statistical analysis. The proposed wormhole attack model method works without any extra hardware requirements, the basic idea behind this work is

that the wormhole attack reduces the length of hops and the data transmission delay.

In [8] A.Vani et al. proposed 3 different methods for detection and removal of the wormhole attack. proposed scheme has three techniques based on hop count, decision anomaly, neighbor list count methods are combined to detect and isolate wormhole attacks in ad hoc networks. That manages how the nodes are going to behave and which to route the packets in secured way. Hybrid routing algorithm is used to provide the common solution to three different techniques. This protocol is based on On-demand ad hoc routing protocol (AODV). In hop count based method one hop neighbors are calculated. Based on the received replies, he will create a list of his one-hop neighbors that excludes the next hop along the route. In anomaly based detection method

The principle of WARRDP is to allow neighboring nodes of a wormhole node to notice that the wormhole node has extreme capacity of competition in path discovery. In the path discovery of WARRDP, an intermediate node will attempt to create a route that does not go through a hot neighbor node, which has a route-building rate higher than the threshold. Thus, not only are wormhole nodes gradually identified and isolated by their normal neighboring nodes. In neighbor discovery method secure neighbor discovery from source to destination obtained by neighbor list and detect the anomaly if attack is present. The steps are

- a. One-hop neighbor discovery;
- b. Initial route discovery
- c. Data dissemination and wormhole detection, and
- d. Secure route discovery against a wormhole attack.

Each node sends a hello message for the neighbor discovery immediately after the deployment of the mobile nodes. Each node that receives a hello message sends a reply. Each node builds its neighbor list which could include remote neighbors connected by a wormhole. The neighboring nodes exchange their neighbor lists. Each node will compare its neighbor list with its neighbors' neighbor list. If they are similar, either these nodes are close enough or are connected by a wormhole. Next, both of these nodes and their neighbors will reconstruct their neighbor lists which will remove these two nodes and their neighbors. Finally, to secure the data

In [9] Vandana CP proposed a method for detecting wormhole attack based on hop count latency and adjoining node analysis. In this method wormhole detection is two step process :

- a. Observation phase
- b. Confirmation phase

In observation phase round trip time of all nodes is calculated which are between source and the destination and the link with maximum round trip time is marked as wormhole link (which exceeds the threshold value) and corresponding nodes are marked as suspicious nodes. Here round trip time is defined as the difference between request and reply packet propagation node. In confirmation phase the suspicious wormhole peers identified in the previous stage are confirmed by verifying if any adjoining node (intermediate node) exists between the wormhole peers.

In [10] khin sandar win proposed a new technique based on link frequency analysis and trust based model. The

algorithm states that whenever a when a node needs to route the data to other node then it broadcasts the request and appends trust vector with it. Every node in the intermediate path also adds the trust vector in request message. As destination receives the request message it copies all trust vector values into rely message and sends it. If source receives the reply message through different paths then it checks for the presence of the wormhole by checking high frequency link and also by comparing with the threshold value. if value is greater than that of the threshold value wormhole is present.

Table 1 comparison of methods that detect the wormhole attack

METHOD	FEATURES	ADVANTAGES
Cluster based method	Two layered approach	Does not require any special hardware and synchronization clocks
Digital signature based method	Secure as cryptography comes into play	detect both hidden and exposed wormhole with pinpoint location of wormhole and prevent them
Path tracing based method	Can only detect wormhole but cannot prevent	Good and satisfactory performance in terms of packet delivery ratio
Token based method	Detect and avoid wormhole	Double encryption makes it secure
Method based on channel characteristics	Detects and flags wormhole	Low cost method using inherent symmetry in wireless channel
Transmission time based mechanism	Detects the exact location of wormhole	Detects hidden and Exposed Attacks
Statistical based approach	Algorithm is light weight and detects wormhole successfully	Efficient and useful results
3 different methods combined together	Detection and isolation of wormhole	Better performance as 3 different methods are combined together
Hop count latency and adjoining node analysis based method	Combination of two approaches	Includes early detection of wormhole
Link frequency analysis and trust model based method	Detection and defense	Achieves low delay

V. CONCLUSION

As wormhole attack is one of the harmful attack in MANETS so we have studied many methods for its detection, removal and the prevention. Also we have compared these methods .Wormhole attack or tunneling attack can also occur in the VANETS so we can discuss various methods for the detection of wormhole in VANETS .we can also compare the two that is wormhole attack in MANET to that of VANET .The other scope can be to study and compare various other attacks and evaluate there performance metrics accordingly. other attacks that can be studied similar to this context are jellyfish attack, sinkhole attack, gray hole attack and many more.

VI. REFERENCES

[1]. ¹ Debdutta Barman Roy, ² Rituparna Chaki ³ Nabendu Chaki. "A new cluster based intrusion detection algorithm for mobile

ad hoc networks" International Journal of Network Security & Its Application (IJNSA), Vol 1, No 1, April 2009.

[2]. Anil Kumar Fatehpuria, SandeepRaghuwanshi "An Efficient Wormhole Prevention in MANETS through digital signatures " International journal of Emerging Technology And Advance Engineering (IJETAE) Vol 3 Issue march 2013

[3]. P. Anitha, M. Sivaganesh "Detection and Prevention of Wormhole Attack in MANETS using Path Tracing" International Journal of communications and networking systems, vol 1 issue 2 december 2012

[4]. Mohit Kumar, Nidhi shayla "Securing AODV Against Wormhole Attack Using Token Based Approach" International Journal of Applied Information Systems ,Vol 4 Issue 10 December 2012.

[5]. Shalabh Jain, Tuan Ta, John S. Baras "Wormhole Detection using Channel Characteristics"

[6]. Phuong Van Tran¹, Le Xuan Hung¹, Young- Koo Lee, Sungyoung Lee, and Heejo Lee "TTM :Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad hoc Networks" 1-4244-0667-6/07/\$25.00 © 2007 IEEE

[7]. Saurabh Upadhyay¹ and Aruna Bajpai² "Avoiding Wormhole attack in MANET using statistical analysis approach" International Journal on Cryptography And Information Security , Vol 2 Issue 1 March 2012

[8]. A.VANI , D.Sreenivasa Rao "An Algorithm For Detection And Removal Of Wormhole Attack for Secure Routing in Ad hoc Wireless Networks" International Journal on Computer science And Engineering.

[9]. Vandana C. P , Dr. A. Francis Saviour Devaraj "WAD-HLA:Wormhole Attack Detection Using Hop Latency and Adjoining Node Analysis In MANETS" International Journal of Engineering Research And Technology Vol 2 Issue 3 March 2013

[10]. Khin Sandar Win "Analysis of DetectingWormhole in Wireless Networks", World Academy of Science ,Engineering And technology 2008

[11]. Yahya Ghanbarzadeh, Ahmad Heidari, and Jaber Karimpour ,"Wormhole Attack in Wireless Ad hoc Networks " ,International Journal of Computer Theory And Engineering, Vol 4,Issue 2 April 2012

[12]. Pradip .M.Jawandhiya, Mangesh .M.Ghonghe, Dr. MS Ali, "A survey of Mobile Ad hoc Network Attacks",International Journal of Engineering Science And Technology,Vol 2 ,Issue 9 2010

[13]. Dr.Satya Prakash Singh, Ramveer Singh, "Security Challenges in Mobile Adhoc Networks", International Journal of Applied Engineering Research, Vol 7 ,Issue 11 , 2012

[14]. Jaiswal P,Kumar R, "Preventing MANETS From Attacks "International Journal of Neural Networks" ,Vol 2 ,Issue 1, 2012

- [15]. G.S. Mamatha, Dr. S.C. Sharma, “Network Layer Attacks And Defence Mechanism in Manets” International Journal of Computer Applications, Vol9 , Issue 9 , 2010
- [16]. Priya Maidamwar¹ and Nekita Chavhan², “A Survey On Security Issues to Detect Wormhole Attack in Wireless sensor Network ”,International Journal on Ad hoc Networking Systems, vol 2, Issue 4 , October 2012
- [17]. Gagandeep, Aashima, Pawan Kumar ,”Analysis of Different Security Attacks In Manets on Protocol Stack-A Review ” International Journal of Engineering And Advanced Technology , Vol 1 Issue 5 June 2012