Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 2; January-March, 2015 pp. 156-161
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/acsit.html

A Survey of Wormhole Attack Detection in MANET

Isha Harode[1] and Preeti Saxena[2]

[1]School of computer science and information technology, DAVV Indore Madhya Pradesh, India
[2]School of computer science and information technology, DAVV Indore Madhya Pradesh, India
E-mail: [1]ishaharode14@gmail.com, [2]preeti_ms@rediffmail.com

Abstract—*The Mobile Ad hoc Networks (MANETs) is a collection of wireless devices or nodes that communicate by dispatching packets to one another or on behalf of another device or node. It does not have any central network authority or infrastructure which controls data routing. The lack of centralized infrastructure and security measures of their routing protocols in ad-hoc network are allowing a number of attackers to intrude the network.*
Wormhole attack is one of the most severe attacks with mobile ad-hoc networks which is launched by creation of tunnels and it results in complete disruption of routing paths on MANET. It attracts a huge amount of network traffic which is done by giving a shortest route through wormhole tunnel to destination in the network. Once the path is established between the source and the destination through wormhole link, they misbehave in many ways in the network like, continuously dropping the packets, selective dropping the packets, analyzing the traffic and performing Denial of Service attack. There have been many researches in past to detect and prevent the wormhole attack. However there are still some limitations to handle wormhole attack properly. In this paper, a comprehensive review is done on the very recent state of the research results on wormhole attacks. It also presents some relevant mitigation measures.

1. INTRODUCTION

Mobile Ad Hoc Network (MANET) is created in a self-organizing manner when the mobile devices come close enough within radio communication range. In a MANET, each node can act both as a host and as a router. It doesn't require any fixed central authority for routing messages from one node to another. Thus it has a low maintenance cost [8]. Due to the infrastructure less network, MANET is widely used in remote areas, emergency response operations like a flood, tornado, hurricane or earthquake and military or police networks. But, the open nature of the wireless communication channels, the fast deployment, the lack of infrastructure, and the environment where they may be deployed making security more challenging task during transmission [17].

There are various routing protocols for discovering routes between source and destination. These routing protocols are not very secure that makes network vulnerable to various attacks. Wormhole attack is one major attack in ad hoc network, which has very adverse effect in the network. Routing protocols in MANET are categorized into two types.

1.1 Proactive or Table driven routing protocol

In proactive protocol each node maintains the network topology information in routing tables periodically. When topology changes then by exchanging routing information maintains the consistency and up-to-date view of the network. When the node requires a path to destination it can directly access through the table. Some existing proactive protocols are Destination Sequence Distance Vector (DSDV), Global State Routing (GSR) and Clustered Gateway Switch Routing (CGSR).

1.2 Reactive or On-demand routing protocol

Reactive Protocols do not maintain topology information and known as a lazy approach to routing. Route discovery is performing on demand of sender; they do not maintain any routing information periodically. The route remains valid until the route is no longer needed. Dynamic Source Routing (DSR), Ad-hoc On-demand Distance Vector Routing (AODV) are routing protocols of this category.

1.3 Hybrid routing protocol

Hybrid routing protocol combines best features of above two protocol categories. Intra-domain use table driven approach and inter-domain apply on-demand approach. Examples are Zone Routing Protocol (ZRP), Wireless Ad hoc Routing Protocol (WARP).

2. WORMHOLE ATTACK

Wormhole is an attack on the routing protocol of a Mobile Ad-hoc Network (MANET). It is a kind of active attack and is hard to defend against. Wormhole can be possible due to single long range wireless or wired link between two colluding node. In this attack, two colluding nodes that are far apart are connected by a tunnel and give an illusion that they are neighbors [2]. Malicious node captures route request messages, topology control messages and data packets from the network and send it to the other malicious node by tunnel which replays them into the network from there. By using this additional tunnel these malicious nodes provide false route information during route discovery and are able to advertise that they have the shortest path through them. So this shortest path can attract the maximum traffic through this tunnel for fast delivery.

2.1 Types of Wormhole Attack

Hidden Attacks

In hidden attacks, attacker nodes do not update packets headers. Other nodes do not realize the existence of them [12], a packet P sent by node S is overheard by node W1, node W1 transmits that packet to node W2 (worm-hole 2) which in turn replays the packet into the communication network. In this way it seems D & S are neighbors although they are out of radio range. In this kind of attack, a path from S to D via wormhole attacker link will be:

S → A1 → B1 → D

Exposed Attacks

In exposed attacks, wormhole nodes do not change the content of packets but they include their identities in the packet header as a trustworthy node. Therefore, other nodes get alert of wormhole node existence but they do not recognize the actual wormhole nodes [12]. In case of exposed attacks, the path from S to D via wormhole will be:

S → A1 → W1 → W2 → B1 → D

2.2 Wormhole Attack modes

Wormhole attacks can be achieved using several modes.

2.2.1. Wormhole with high power transmission. In this mode, when an attacker node gets a route request message, it broadcasts the message at a high power level towards the destination. By this method, the malicious mode attracts the packets to follow path passing from it.

2.2.2. Wormhole using encapsulation. A malicious node which is at one part of the network receives the RREQ (route request) packet from source. Then it encapsulate packet as payload and tunnels that packet to a second malicious node via legitimate path. The intermediate nodes can’t be able to increment the hop count field of RREQ packet. When another colluding node receive the RREQ, it removes the header appended by first colluding node from the packet and send further in the network towards destination. The result is that the routes between source and the destination go through the two malicious nodes that will be said to have formed a wormhole or the tunnel between them. This prevents the other nodes from discovering any other legitimate path that are more than two hops away. Here Fig. 1 shows [19] that X encapsulates the RREQ packet as payload and sends it to next malicious node to Y. Y remove the header appended by X and rebroadcast it to next neighbor node B. So B thinks that there are only 2 nodes between A and B.

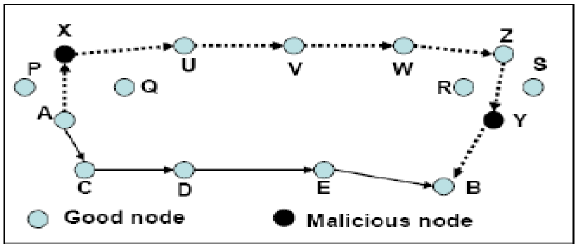


Fig. 1: Wormhole attack in Encapsulation mode

2.2.3. Wormhole using out of band channel. In this mode, an out-of-band high bandwidth channel is placed between two end points to create a wormhole link. This mode of attack is more difficult to launch than the previous one since it needs specialized hardware capability.

Fig. 2 shows [19] that node A sends a RREQ to node B, and nodes X and Y are malicious nodes having an out-of-band channel between them. Node X tunnels the RREQ to Y, which is a legitimate neighbor of B. Node Y broadcasts the packet to its neighbors, including B. B gets two RREQs A-X-Y-B and A-C-D-E-F-B. The first is both shorter and faster than the second, and is thus chosen by B.

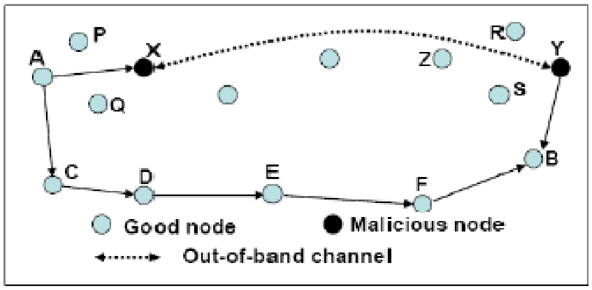
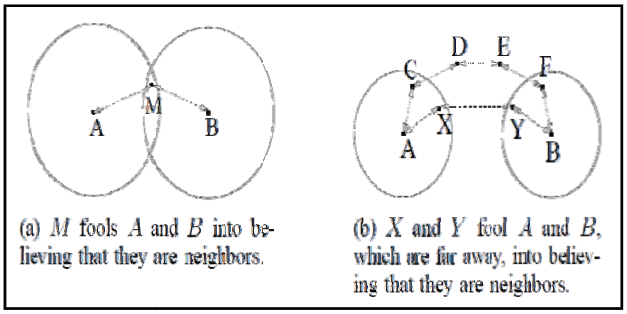


Fig. 2. Wormhole attack in out of band mode

2.2.4. Wormhole using Packet Relay. A malicious node relays packets between two distant nodes to convince them that they are neighbors. It can be launched by even one malicious node. Using more than one malicious node serves to expand the neighbor list of a victim node to several hops. In Fig. 3 it is carried out by an intruder node X located within transmission range of legitimate nodes A and B, where A and B are not themselves within transmission range of each other. Intruder node X tunnels control traffic between A and B, without any modification presumed by the routing protocol e.g. without stating its address as the source in the packets header so that X is virtually invisible. Node X can afterwards drop tunneled packets or break this link.

2.2.5. Wormhole using Protocol deviation. During the RREQ forwarding, the nodes typically back off for a random amount of time before forwarding to reduce MAC layer collisions. A malicious node can create a wormhole and broadcasting without backing off. The purpose is to let the request packet it forwards arrive first at the destination.



(a) *M* fools *A* and *B* into believing that they are neighbors.

(b) *X* and *Y* fool *A* and *B*, which are far away, into believing that they are neighbors.

Fig. 3: Wormhole attack in packet relay mode

3. RELATED WORK

Viren Mahajan *et al.* proposed various characteristics that can be observed in a network in the presence of a wormhole attack [1]. The paper explains the self-contained in-band Wormhole phenomenon. The various characteristics that are observed are. First is Path length distribution. It suggests the abrupt decrease in the path lengths which can be used as a possible symptom of the wormhole attack.

The other is Delay. Due to the wormhole, the hop delay of tunnel nodes would increase. It leads to increase in the end-to-end delay of the routes that do not get attracted by the wormhole but pass through some of the tunnel nodes. In this approach there is no concept of authentication of individual node. Through this approach we can find the route on which wormhole is present but can't detect that particular node compromised by attacker.

Another research paper presented a novel approach to secure against wormhole attack in MANET using neighbor node analysis [2]. The neighbor node analysis approach analyzes the neighboring nodes so as to check the authenticity of the nodes for secure transmission of data over the network. According to this approach a node will request to its neighboring nodes and perform a request and response mechanism i.e. source node send the route request packet encrypted with its public key to all of its neighbor and the neighbor can decrypt the packet through their private key. The legitimate node can only be able to decrypt that node and send the route response message as acknowledgement to source node. Source node keeps record of response time of route response message. The node will maintain the tracking table for the timeout. It suggests that if the route reply time is smaller than the response time of actually message send, then an attack is present in that route of the network. It was observed that the intermediate nodes can be analyzed to detect the presence of wormhole attack in MANET. This approach can't be able to detect the exposed wormhole attack.

Author found the spurious links by sending hello request and hello response message to all its neighbors [3]. However, in a wormhole attack this HELLO message can be replayed from a far. To detect the wormhole tunnel, the sender sends a Probing packet to all of its suspect nodes. When neighbor node receives the Probing packet, it sends back an ACKprob message to the originator of the Probing packet after stopping all transmissions of data packets. The reputation state of a node that has been inferred in the exchange of HELLO procedure can be justified on the basis of conclusions derived from the suspicious link detection procedure.

Gunhee Lee *et al.* proposed [5] monitoring of both the exposed (open) wormhole attack and hidden (close) wormhole attack. This approach will be helpful to remove impractical assumptions. The author mainly focus on the check whether a node forwards the packet is a real neighborhood or not. However, for the exposed wormhole attacks, the node does not detect a wormhole with direct neighbour information, since one of wormhole node can be a real neighbour of it [5]. Each node must have to maintain one hop and two hop neighbour list. Each newly joined node to the network broadcast an announcement being valid until next two hops. It is called as two hop broadcast. TTL of newly joined node is 2 and the packet consist the identity of the announcer and an encrypted identity with its secret key. When a first hop neighbour receives the announcement, it checks the TTL value. If it is 2, then the receiver decreases it by 1, and it keeps the sender's identity and encrypted value. After that, it forwards the announcement by broadcasting it and sends an acknowledgement (ACK) including its identity, parameters for Diffie-Hellman key exchange algorithm, and an encrypted identity with its own secret key [5].

When a second hop neighbour receives the announcement, it checks the TTL value first. If the value is 1, then it saves the announcer's identity and the encrypted one and sends an ACK as the first hop neighbour does [5]. Each neighbour receiving the response from the announcer generates a session key, which is the same as the announcer's one. With the key, it obtains sender's secret key and the nonce. By using the secret key, it verifies whether both the identity of the sender and the encrypted identity, which is kept in previous step, are the same or not. If they are identical, then the node updates its neighbour list with the announcer's identity.

Each message in this approach should arrive at the destination within a predefined time intervals. There are two intervals such as ti,1 = 2(d/v) + δ for one-hop neighbours and ti,2 = 2ti,1 for two-hop neighbours, where v is the velocity of the light, d is the maximum transmission range, and δ is the processing time on the receiver. If a one-hop neighbour node and any other malicious node form a wormhole, the delay of the message between them is longer than that between normal neighbours. Thus, each node, which participates in the process of building a list, will discard any message that arrives after the interval. There are 2 testing i.e. one hop and two hop node. Identity verification can successfully detect the exposed wormhole attack.

Umesh kumar chaurasia and Varsha singh [6] proposed a modified wormhole detection AODV protocol (MAODV) which is based on the working strategy of AODV protocol. To detect wormhole attacks in the Network MAODV suggests collecting information regarding numbers of hop count and delay per hop for different paths from source to destination. The reason behind is that under legitimate situation the delay for each packet is similar along each hop in the path and the delay for each packet should be excessive for those nodes which are involved in the wormhole attack. Therefore, if there is a comparison of the delay per hop of every node in the normal path and a path that is under wormhole attack. It finds that delay per hop of a path that is under wormhole attack is larger in comparison of normal path.

A potential wormhole is identified by examining the routing table, any link with highest density of usage is suspected as wormhole [7]. Once suspected paths are identified locally by sending request to the neighbors to confirm the existence of the same path with high percentage of usage. When a node receives processing request, it checks its own table and if the same pattern exists, it replies as true to the requesting node. If a confirmation reply is received, but still cannot be sure if it is a wormhole or the physical location of nodes have caused such routing structure, there are another confirmation step, and in this step the nodes at the two ends of wormhole send some encrypted messages to one another. Every legitimate node on the path will be able to process those messages and adds their signatures/stamps/flags to the encrypt packet pay load.

When a destination node receives the encrypted message [7], it looks for signatures for all nodes along the path, if every node has added its signature to the encrypted payload; it considers the node as normal. If the signature of any node along the path is missing, it is considered as a wormhole. Isolate the colluder nodes so that no further communication takes place with them and hence are black listed. Upon the confirmation of wormhole, both end nodes broadcasts a blacklisting message. This message contains list of colluder nodes to be excluded from communication.

Normalized wormhole local intrusion detection algorithm [12] has an intermediate neighbour node discovery mechanism, packet drop calculator. Individual node can perform isolation technique for conformed wormhole nodes. Except RREQ and REEP there are 2 more types of packet used which are FRREQ and FRREP. In this approach every node sends FHellow packet to consecutive neighbour of its next node. In reply every node gets a preclusion ratio (PR). If PR is greater than 50% then the node is trustworthy otherwise it is wormhole node. This method transmits more number of packets per route so it can cause link congestion.

4. COMPARATIVE STUDY

We have reviewed various research studies related to wormhole attack detection methods in section 3. Now a comparative study of various techniques is presented in Table 1.

Table 1: Comparison of various research papers

Techniques	Description	QOS Parameter	False detection	Drawbacks
Neighbour node analysis[2]	Preparing neighbour list and check the response time.	Response time	Response time vary due to traffic, node interference and line congestion.	Cannot able to handle all variants of wormhole attack
Two hop neighbour list [5]	Preparing neighbour list up to 2 hops. Check the legitimate user present in the route.	none	none	The trail of attack can be neutralized properly but does not identify the entrance of the wormhole
NWLIDA [12]	Algorithm has an intermediate neighbour node discovery mechanism, packet drop calculator; individual node can perform isolation technique for conformed wormhole nodes.	Preclusion ratio	none	This method transmits more number of packets per route so it can cause link congestion.
Hybrid approach [13]	This approach has 3 steps training, detection and updating. There are 2 algorithms NicheMGA and NEGA algorithm.	none	none	Genetic algorithm and artificial immune system is able to adapt itself when network topology changes.

Routes redundancy and time-based hop calculation [14]	This approach is based on 3 combinational steps i.e. route redundancy, route aggregation, RTT.	Average time per hop, RTT	none	This technique is only able to detect exposed attack and failed to detect hidden attack
Timed and Secured Monitoring [11]	Combination of AODV-WADR-AES and E-HSAM schemes.	RTT, hop count	RTT causes false alarm	
path tracing approach [9]	The detection of wormhole using per hop length over a fixed routing path. As the wormhole node is detected, an alarm message is passed to the entire network	per hop distance using round trip time (RTT)	RTT cause false detection	
MAODV [6]	This MAODV protocol Collect number of hop count or delay per hop. Delay per hop of a path that is under wormhole attack is larger in comparison of normal path.	Number of hop count, delay per hop	none	Detection ratio of shortest tunneled path is less because this path is similar to normal path
LiteWorp[10]	LITEWORP assumes a pre-distribution pair-wise key management protocol for ad hoc networks. Sender contains the neighbour list up to two hop. It uses a collaborative detection strategy.	none	none	Applicable only to static stationary network
Trust based approach [20]	It is a cluster based approach. This approach uses a monitoring server for calculating trust value.	Trust value, packet delivery ratio, end to end delay	none	Authentication process of node is week. Malicious node can easily skip from it and used in transmission path.
AODV-WADR[21]	It helps a node to confirm whether a neighbor has created a wormhole tunnel within the MANET or not, using a combination of timing and cryptography.	NetTT, NodeTT, ATT, ATT WADR, MTT	none	Restricted to analyzing 3 hop route only.

5. CONCLUSION

This paper aims to analyze the wormhole attack patterns. It will identify the conditions that are necessary for wormhole attack to persist. It would help to find some metrics to judge a wormhole attack. The identified metrics will help for proposing the strategy useful for the detection of such an attack. Wormhole attracts all the network traffic by advertising false shortest path through it. Wormhole attack decreases the throughput. Presence of wormhole can be detected by abruptly decrease in path length from source to destination and increase delay. We believe that the analysis on different types of wormhole attacks and their detections presented in this paper would be useful to devise stronger intrusion detection technique that would work on any wireless network including the mesh networks and sensor network.

REFERENCES

[1] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, “Analysis of wormhole intrusion attacks in manets” IEEE communication magazine, 2008.

[2] Sweety Goyal and Harish Rohil, “Securing MANET against Wormhole Attack using Neighbor Node Analysis” International Journal of Computer Applications (0975 – 8887) Volume 81 – No 18, November 2013.

[3] Farid Naït-Abdesselam and Brahim Bensaou, “detecting and avoiding wormhole attacks in wireless ad hoc networks”, IEEE Communications Magazine, April 2008.

[4] Poonam Dabas and Prateek Thakral,“detection and prevention of wormhole attack in manet: a review”, International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 3, March 2013.

[5] Gunhee Lee and Dong-kyoo Kim, Jungtaek Seo, “An Approach to MitigateWormhole Attack in Wireless Ad Hoc Networks”, International Conference on Information Security and Assurance 2008.

[6] Umesh kumar chaurasia and Mrs. Varsha singh,” MAODV: Modified Wormhole Detection AODV Protocol” IEEE explore 2013.

[7] Zubair Ahmed Khan and M. Hasan Islam,” Wormhole Attack: A new detection technique” IEEE explore 2012.

[8] Reshmi maulik and Nabendu chaki, ”A comprehensive review on wormhole attack in MANET”, IEEE explore 2010.

[9] T.sakthivel and R.M chandrashekran, “Detection and prevention of wormhole attack in MANET using path tracing approch”, European journal of scientific research vol.71 EuroJurnals publication, Inc 2012.

[10] Issa Khalil, Saurabh Bagchi and Ness B. Shroff, “LITEWORP: Detection and isolation of the wormhole attack in static multihop wireless networks” Science Direct Computer Networks 51, 2007.

[11] Isaac woungang and sanjay kumar dhurandher, “A Timed and Secured Monitoring Implementation AgainstWormhole Attacks in AODV-Based

Mobile Ad Hoc Networks" computer, information and telecommunication systems,(CITS), international conference 2013.

[12] Aarfa khan and shweta shrivastava, "Normalized Worm-hole Local Intrusion Detection Algorithm (NWLIDA)" International Conference on Computer Communication and Informatics (ICCCI -2014), Coimbatore, INDIA, Jan. 03 – 05, 2014.

[13] Fatemeh Barani," A Hybrid Approach for Dynamic Intrusion Detection in Ad Hoc Networks Using Genetic Algorithm and Artificial Immune System" Intelligent Systems (ICIS), Iranian Conference 2014.

[14] Soo-young shin and Eddy Hartono Halim, "Wormhole attacks detection in MANETs using routes redundancy and time-based hop calculation", ICT Convergence (ICTC), International Conference 2012.

[15] Gaurav garg, sakshi kaushal and akashdeep Sharma, " Reactive Protocol analysis with wormhole attack in ad hoc network" 5th ICCCNT 2014 hefei, chaina, July 11-13, 2014.

[16] Zolidah Kasiran and Juliza Mohamad "Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV", Digital Information and Communication Technology and it's Applications (DICTAP), Fourth International Conference 2014.

[17] Kamini Singh,Gyan Singh and Arpit Agrawal "A Trust based Approach for Detection and Prevention of Wormhole Attack in MANET", International Journal of Computer Applications Volume 94 – No.20, May 2014.

[18] Priyanka Sharma, H.P. Sinha and Abhay Bindal,"Detection and Prevention against Wormhole Attack in AODV for Mobile Ad-Hoc Networks", International Journal of Computer Applications (0975 – 8887) Volume 95– No. 13, June 2014.

[19] Mohit Jain and Himanshu Kandwal, "A Survey on Complex Wormhole Attack in Wireless Ad Hoc Networks", International Conference on Advances in Computing, Control, and Telecommunication Technologies, IEEE 2009.

[20] Kamini Singh, Gyan Singh and Arpit Agrawal," A Trust based Approach for Detection and Prevention of Wormhole Attack in MANET", International Journal of Computer Applications Volume 94 – No.20, May 2014.

[21] E. A. Panaousis, L. Nazaryan, and C. Politis, "Securing AODV against wormhole attacks in emergency manet multimedia communications," 5th Intl. ICST Mobile Multimedia Communications Conference (Mobimedia 2009), Brussels, Belgium, 2009.