Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.980 – 984

REVIEW ARTICLE

Wormhole Detection and Prevention in MANET: A Review

Shraddha S. Mahajan[1], Dr. Hitendra D.Patil[2]

[1]Master Student, Computer Engineering, SSVPS'S B.S.Deore College of Engineering, India

[2]Professor and Head, Computer Engineering, SSVPS'S B.S.Deore College of Engineering, India

[1] itsshraddhamahajan2@gmail.com; [2] hitendradpatil@gmail.com

Abstract— *As Mobile Ad-hoc Network (MANET) doesn't require pre-existing infrastructure, thus every node is active in data transmission and reception. In MANET various attacks are created by unauthorized transmitter in the network, which may affects on the performance of the network. Wormhole attack is created by collaborative attackers. So confrontation is take place between discoveries and dislodges this threat from network. Various techniques have developed to detect & intercept wormhole. The concern on this work is to perusal various methods of wormhole attacks detection and prevention and take some comparative measurements against these methods by considering with pros and cons.*

Keywords— *Mobile Ad-hoc Network, Wormhole Attack, AODV protocol, DSR protocol*

I. INTRODUCTION

Ad-hoc network is infrastructure less network in which each node can take part in the process of data sending and receiving. Ad-hoc is Latin word. The meaning of it is "Due to this reason". Day by day issues related to the network performance and security has increase while uses of network take big part in the society. There is no guaranty that nodes in the network can communicate without affection of malicious node. Most of the routing protocol also get failed to comply with such malicious nodes or attackers. The purpose of ad-hoc network is to provide secured communication in hostile environment. As MANET is infrastructure less network, each node can establish routing. There are many routing protocols which are used in mobile ad-hoc network. Routing protocols such as Ad-hoc On-demand Distance Vector Routing (AODV), Destination Sequence Distance Vector (DSDV) and Dynamic Source Routing (DSR) [1].

II. DIFFERENT ROUTING PROTOCOLS

1. Ad hoc On Demand Distance Vector Routing (AODV)

AODV is basically an improvement of DSDV (Destination Sequence Distance Vector). As DSDV is proactive in nature, AODV is not so. Ad hoc On Demand Distance Vector Routing (AODV) is reactive routing protocol. Based on demand, it minimizes the number of broadcasts by making routes available. This thing is not done in DSDV routing protocol. Source node broadcast a RREQ, if source node wants to send a packet to a destination. Neighboring nodes in turn broadcast the packet to their neighbors and the process continues until the packet reaches to destination. Intermediate nodes record the address of the neighbor during the route request forwarding from which first copy of the broadcast packets is received at destination. Route table is used to store that record, and reverse path is established with the help of that route table record. These packets are discarded if duplicate copies of the RREQ are received. RREP (Route Reply) is then sent back using unicasting through the reverse path of the network. When sender moves from one node to another, a route discovery process is reinitiated for route maintenance since MANET support nodes mobility [11].

2. Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a reactive protocol based on the source route approach. Dynamic Source Routing (DSR) protocol is based on the link state algorithm in which source initiates route discovery on demand basis. The RREQ sender determines the route from source to destination and it includes the address of intermediate nodes to the route record in the packet. Dynamic Source Routing (DSR) was designed for multi hop networks. In Dynamic Source Routing (DSR), no HELLO messages are exchanged between nodes to notify them of their neighbors in the network. A group of different mobile wireless device is formed by mobile ad-hoc network. Mobile wireless device like desktop, laptop, wireless phone, etc. have capability to communicate with each other co-operatively. As MANET works with infrastructure less network that is untrusted environment, various attackers tries to reduce the performance of the network [12].

III. ANALYSIS OF PROBLEM

Data transmission and reception is risky process since MANET is infrastructure less network and here each node can take participation in this process. Various types of hackers try to hack the data during the process of data travelling from one node to other. Wormhole attack is one from those which is created by two or more attackers. Here two unauthorized node or malicious node create a large tunnel between each other and passes unauthorized data through it otherwise it increase the size of the network or create unnecessary delay in the data transmission process which indirectly degrade the overall performance of the network.

IV. VARIOUS ATTACKS IN MANET

As use of networking is grown up, security related issue is also increases. During utilization of network for data transmission and reception process, it is responsibility of the user to take care that performance of the network should not degrade. Hackers always try to add intrusion into authorized data in the network. Black hole attacks, white hole attacks, wormhole attack is attacks which affects on the performance of the network. In white hole attack, large amount of traffic floods in the network which creates collusion inside the network. In black hole attack, attacker drops the traffic which is passing through it. Black hole attack and white hole attack s created by single attacker.

V. COMPARATIVE TECHNIQUES FOR WORMHOLE ATTACK DETECTION AND PREVENTION

Wormhole attack is created by two or more attackers which work together to fabricate serious threats in the network. Such attack is also called as collaborative attack. The name wormhole indicates tunnelling which is created by collaborative attackers. It means that attacker create tunnel between two unauthorized attacker, so that they can increase the size of network. Attackers can easily transfer unauthorized data through this tunnel. As delay and hope count is increase due to this tunnelling, performance of the network can simply decreases. Wormhole attack can be categorised into two groups.

1. Hidden wormhole attack
2. Exposed wormhole attack

Hidden attack is also called as out of band wormhole in which authorized nodes doesn't know the existence of malicious nodes. Exposed attack is also called as in band wormhole in which authorized nodes are aware about existence of malicious nodes. Various researches had been done to detect and prevent wormhole or tunnelling in the network. In ad-hoc network, multihop wireless mobile nodes can transmit and receive data to each other without having any centralized control of the network. Routing protocol like Ad-Hoc On Demand Distance Vector Routing Protocol (AODV) Dynamic Source Routing (DSR), have been develop to perform routing in MANET, since it is critical task because of highly dynamic environment. This protocol helps to increase the performance of the network. Different technique like DelPHI (Delay Per Hope Indication), DAW (Distributed Antiworm Detection), WAP (Wormhole Attack Prevention), Packet Leashes has developed which work effectively against wormhole attack by using different routing protocols like, AODV, DSR, DSDV etc.

Number of techniques has developed to detect the wormhole and to take preventive measurement against wormhole. Here just see two comparative techniques of wormhole detection and prevention [1].

A. AODV based wormhole detection (DelPHI)
B. DSR based wormhole detection (WAP)

Both methods which mention above are work effectively in the process of wormhole detection. But both methods have different environment. Let see this two comparative methods in detail.

A. **AODV based wormhole detection (DelPHI)**

Hon Sun Chiu & King Shan Lui presented this new algorithm called as DelPHI (Delay Per Hope Indication). Wormhole attack affects on the network performance. It forms serious threats in the wireless network security mechanism. This method can detect the wormhole by just observing delay and hope count information from each node. It is observed that path in which wormhole is located has a larger network size than normal path. That means that the path in which wormhole is resides, its hope count and delay value has increases than normal path. So that it may be indirectly degrade the performance of the network. DelPHI is an effective mechanism to detect a wormhole in the network. As the name suggest AODV, it used AODV (Ad-hoc On Demand Distance Vector) routing protocol to set up the route procedure. This method can detect both that is hidden and exposed attack [1].

DelPHI works with two phases which is as follows.

1. Data Collection
2. Data Analysis and Wormhole Detection

In first phase, route related information like delay, hope count etc. is collected. In second phase collected information is analysed by the sender that is whether wormhole is located in the path or not. Two possible disjoint paths are created here that is DREQ roadmap and DREP roadmap. These two disjoint paths helps to detect wormhole easily. DREQ (Data request) is broadcasted from sender to receiver with timestamp field, hope count field and node id. These all fields are updated by each node during DREQ transmission. The principle of DREQ is to collect route information at each node. When request (DREQ) reach at destination then acknowledgment is given by receiver using data reply (DREP) roadmap. Receiver first update each field and then unicasts DREP request through exactly reverse path from destination to source. Here receiver must have to reply for each DREQ request. Round Trip Time (RTT) is a time required for sending packets from source to destination. In this method, delay/hope and RTT value is calculated by sender and according to the difference value of it, sender analysed that whether wormhole is located or not. According to the network simulator, it is observed that delay per hope value in normal path is smaller than tunnelled/wormhole path.

Advantage of DelPHI is that it does not required clock synchronization and special hardware. It also has higher power efficiency. Biggest drawback of DelPHI is that if wormhole is located at all side, DelPHI get failed to locate it. It cannot find pin point location of wormhole. It cannot take preventive measurement against wormhole attack [1].

B. **DSR based wormhole detection (WAP)**

Sun Choi, Kim, Lee & Jung introduced a new technique called WAP (Wormhole attack Prevention). By the comparison of the DelPHI it works effectively against wormhole attack. WAP method is not only for wormhole detection but also for wormhole prevention. As the name suggest DSR based, it used DSR (Dynamic Source Routing) routing protocol to set up the route procedure. This method has ability to take some preventive measurement against wormhole so that it will not appear again in the network while discovery of the route. As like DelPHI, WAP also stores wormhole information at source node.

WAP also works with two phases which is given as follows [2].

1. Neighbour Node Monitoring
2. Wormhole Route Detection

1. Neighbour Node Monitoring

Special list of neighbour node list is created in which all nodes monitors the neighbour behaviour after sending RREQ message to the receiver. By using this neighbour node list, observation is taken out and wormhole is detected which is then stored in the wormhole node list. This phase work as wormhole prevention so that it cannot be appears in the network again. As like DelPHI, it also stores wormhole information at the sender side so these are less number of chances to appear it again. Neighbour node table contain neighbour Node ID, RREQ sequence, sending time, receiving time and count etc. Each node in the network must have to update this table. To avoid the clock synchronization, WPT (wormhole prevention timer) is used here. WPT means that maximum time required sending packet from source node to neighbour node.

$$\text{WPT} = \frac{2 \times \text{Transmission Range (TR)}}{\text{Vp}} \qquad (1)$$

Where TR = Distance in which packet can travel.
VP = Denotes propagation speed of a packet.

2. Wormhole Route Detection

In wormhole route detection phase, route in which wormhole is located is detected. Here wormhole route is detected using wormhole node list [2].

VI. DISCUSSION

DelPHI & WAP both methods are effective to detect wormhole attack. Since both methods have some differences. Both methods work with different routing protocols, DelPHI works with AODV routing protocol which is suitable for infrastructure less network. AODV does not broadcast packet unless not necessary. Whereas WAP works with DSR routing protocol this is based on two mechanisms like route discovery and route maintenance. Broadcast route discovery mechanism in which source node broadcast the request to all nodes is used by AODV and DSR.

VII. COMPARISON

TABLE I

Comparison Factor	**DelPHI**	**WAP**
Routing Protocol	AODV	DSR
Properties	Wormhole Detection	Wormhole Detection & Prevention
Mechanism	Broadcast Discovery	Broadcast Discovery
Simulator	NS2	Qualnet
Performance Parameter	Delay & Hope count	Throughput & speed
Cost	High	High

VIII. CONCLUSION

With the comparison of both (WAP & DelPHI) method it can be concluded that wormhole detection and prevention is difficult and essential task in order to increase the performance of the network and decrease the risk in the network. Both method works effectively against the process of wormhole detection. Both methods have some pros and cons which are discussed above. Standard solution to detect and prevent wormhole is yet to be covered.

REFERENCES

[1] Hon Sun Chiu and King Shan Lui, "DelPHI : The Efficient Wormhole Detection Mechanism for Ad Hoc Wireless Network," 1st International Symposium on Wireless Pervasive Computing IEEE Transaction on Mobile Computing, pp. 1-6, 16 Jan 2007.

[2] Sun Choi, Doo-young Kim, Do-hyeon and Jae-il Jung, "WAP : Wormhole Attack Prevention Algorithm in Mobile Ad-hoc Networks," IEEE International Conference on Sensor Network, Ubiquitous and Trustworthy Computing, pp. 343-348, 2008.

[3] Deepesh Namdev and Shikha Singhal, "Wormhole Attack Detection and Prevention Mechanism for Mobile Adhoc Nework," Quest Journal of Electronics and Communication Engineering Research, vol. 2, no. 6, pp. 7-16, 7-July 2014.

[4] Anil Kumar Fathepura and Sandeep Raghuwanshi, "An Efficient Wormhole Prevention in MANET through Digital Signature," Inteand Advancedrnational Journal of Emerging Technology anced Engineeringnd Adv, vol. 2, no. 6, pp. 360-367, March 2013.

[5] Motjaba Ghanaatpisheh Sanaei, Babak Emami Abarghouei, Hadi Zamani and Miranda Dabiranzohouri, "An Overview on Wormhole Attack Detection in Ad-Hoc Network," Journal of Theorotical and Apllied Information Technology, vol. 5, no. 3, pp. 291-300, 30 Jun 2013.

[6] Shigang Chen and Yong Tang , "DAW : A Distributed Antiworm System," IEEE parallel an Distributed System, vol. 18, no. 7, pp. 893-906, July 2007.

[7] Yih-Chun, Adrian Perrig and Daavid B. Johnson, "Packet Leashes : A Defense against Wormhole Attacks in Wireless Networks," in In Proceeding of IEEE INFOCOM, April 2003, pp. 1976-1986.

[8] S. Capcum and I. Buttyan, "SECTOR : Secure Tracking of Node Encounters in Multihop Wireless Network," in In Proceeding of the ACM Workshop on Security of Ad-hoc and Sensor Network, 2003, pp. 21-31.

[9] Pushpendra Niranjan, Prashant Srivastav, Rajkumar Soni & Ram Pratap, "Detection of Wormhole using Hope-count and Time delay Analysis," International Journal of Scientific & Research Publication, vol. 2, no. 4, pp. 1-4, April 2012.

[10] Saurabh Gupta, Subrat Kar & S. Dharmaraha, "WHOP : Wormhole Attack Detection using Hound Packet," in International Conference on Innovation in Information Technology, 2011, pp. 226-231.

[11] C. E. Perkins & E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," in Proc. of hte 2nd IEEE

Workshp on Mobile Computing System, New Orleans, LA, Feb-1999, pp. 90-100.

[12] D.B. Johnson, D.A. Maltz & J. Broch, DSR : The dynamic source routing protocol for multihop wireless ad hoc networks. Boston, Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc. , 2001.