IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.6, Special Issue.11, Dec 2018 E-ISSN: 2347-2693

The Indexing Strategy to Prevent Worm Holes in Manet - An Analysis

J.Nithyapriya[1*], V. Pazhanisamy[2]

[1]Alagappa University, Karaikudi,Tamilnadu,India
[2]Dept.of CA, Alagappa University, Karaikudi,Tamilnadu,India

[*]*Corresponding Author: nithyapriyajj@gmail.com, Tel.: 7339093757*

Available online at: www.ijcseonline.org

***Abstract*—** A temporary network of wireless mobile hosts without the assistance of standard administration form mobile ad hoc network (MANET). It has a dynamic topology because mobiles can enter and leave the network continuously. As MANET are wireless, dynamic and have no central administration, maintaining security in this network is difficult. The wireless nature of the communication makes nodes susceptible to various kinds of attacks such as black hole attack, worm hole attacks, DoS attacks etc. In present work, we aim at detection and prevention of the wormhole attack.

***Keywords*—** MANET, Wormhole

I. INTRODUCTION

Advancement in the Wireless network technologies have resulted many new applications in the internet discipline. Recently, due to the prestige of portable device and wireless networks Mobile ad Hoc network has become one of the most Vibrant and driving area of communication. A mobile ad Hoc network is an independent system of movable devices like smart phones, laptops and sensors. These devices can communicate and join each other at any time and any place through wireless links. Each device act as a router because each device forward traffic which is not related to it. MANET has some special characteristics like open network boundary, dynamic topology, distributed network, fast and quick implementation and hop-by-hop communication. These special features made the MANET popular for the military purpose and for the use of emergency relief situation. There is two types of communication: direct and indirect; in direct communication, nodes that are in radio range of one another can interact with each other directly while in indirect communication, nodes interact with each other with the help of intermediate nodes in order to route their packets. Wireless interface is used through which each node communicates. Because the network is fully distributed, so no fixed infrastructure is used as access points and base stations i.e. it can work without any fixed infrastructure. The topology of the network keeps on changing as nodes used are mobile nodes, so they enter and leave the network continuously.

II. WORMHOLE ATTACK

The wormhole attack is the most severe attacks of MANET. It is a kind of DOS attack which is very effective in network layer. Network routing is being affected by this attack along with this location based security of Ad-hoc is also compromised. "Wormhole attack" is a co-operative attack because there is a need of two nodes that will act in co-operation. In this attack, at two different edges of the network, two collaborating attacker nodes will occupy their strong strategic locations. In this way they are occupying dominant positions in a network so that they (nodes) can cover complete network and present to have the smallest path for transferring data. By using direct wireless link these two attacker nodes are linked together which is known as wormhole tunnel. At one end of wormhole tunnel, one node will collect packets in its local area and then those packets are transmitted to the other node at the other end of tunnel then this node will play again with those packets. The attacker nodes are connected together via tunnel that is created using high speed transmission links such as Ethernet cables or wireless optical links. If this pair of nodes will forward every packet legitimately then it means that they are supporting the faster communication and routing within the network. However, this is not the case as these attacker nodes, either drop all packets which are intended to them, alter those packets or selectively transfer some packets. In wormhole attack, malicious nodes give misconception to both sender and receiver of being close neighbors but they are actually far distant away by tunneling packets between two attackers. Wormhole can be established by using a single long-range wireless link or through wired link between two colluding attackers.

Communication is between malicious nodes, that is malicious node at a point in network receives data packets and bridges them to another one which is also malicious. These bridges exists between two malicious are known as wormhole. These wormholes create severe extortions to routing protocols in MANET. The attackers which use

wormholes are able to make their nodes more attractive to other nodes for sending packets [1].

The following Fig. 1 depicts that X and Y are forming tunnel that means these are malicious nodes in network. After initiation of PREQ from source node S to find route to destination D, nodes 1 and 2 transfers request to 5 and X. X which is malicious when finds PREQ, shares it with Y the other node of tunnel, so they start delivering PREQ through node 8 to D. Because it is a high speed link so it can force source node in selection of route to destination that can result in D ignoring PREQ that can arrive in later time and so it undermines the genuine route <S->2->5->7->D>.

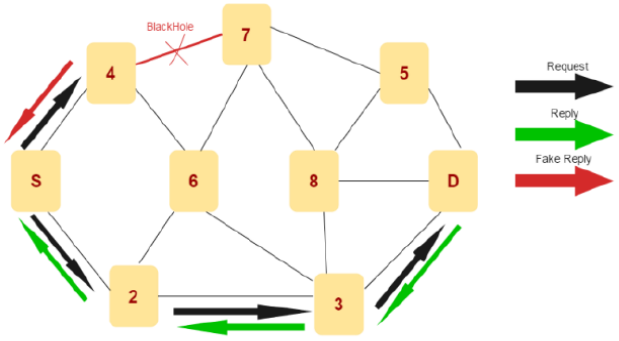

Fig.(1)

S-1-X-Y-8-D is opted instead S-2-5-7-D

A. *Types of Wormhole Attack*

- **Wormhole using Encapsulation (In-band channel):**In this, one malicious node will transfer the route request packets to another malicious node via one or more nodes present in the network
- **Wormhole using out of band channel:** In this, by using either wired link or long range wireless link two malicious nodes are directly connected to each other.
- **Open wormhole attack:** In this attack, for discovering the

RREQ packets malicious nodes keep on examining the wireless medium. If the malicious nodes are present in the network, it is supposed that malicious nodes are present on path by other nodes on the network and they are their direct neighbours.

- **Closed wormhole attack:** In this attack, neither capture packet nor packet field head are modified by the attacker instead attackers take advantage from processing packets in order to find a route known as route discovery. In route discovery process, attacker tunnels the packet from one side of the network to another side of the network and re-broadcast packets.
- **Half open wormhole attack:** In this attack, malicious node will modify only one side of packet and the other side of the packet will not be modified in subsequently route discovery procedure.
- **Wormhole with high power transmission:** In this attack, in order to broadcast a packet, malicious node will use maximum level of energy transmission. With the help of route discovery process malicious node will get a Route Request (RREQ), after that, it will broadcast the Route Request (RREQ) at a maximum level of energy of it power so the other node on the network which are on the normal power transmission and lack of high power capability hears the maximum energy power broadcast they rebroadcast the packet towards the destination. By doing this malicious node can get more chances to create a route between source and destination without using colluding. Our work is to face this wormhole attack.

III. EXISTING SYSTEM

The existing scheme for preventing this wormhole is bait. This is finding out malicious nodes by requesting route and sending packets to the suspicious nodes.

The nodes in mobile ad hoc networks communicate wirelessly with each other. The wireless nature of the communication makes nodes susceptible to various kinds of attacks such as black hole attack, worm hole attacks, denial of service attacks etc. In present work, we aim at detection and prevention of the wormhole attack. In wormhole attack, the attacker nodes form a tunnel. As a result the length of the path between source and destination is shortened in terms of the hop count. The source node has to select the path containing lowest hop count, and when the data is received by the wormhole nodes on the path the nodes drop the packets coming to them. This hampers the performance of the network in terms of packet drops, packet delivery ratio and throughput. In past many researchers have designed many algorithms and techniques to detect and prevent such kind of attacks in mobile ad hoc networks.

One of the researches done in the past by the authors in [2] describes the concept of bait destination node to detect the black hole attack in the network. The source node chooses one of its neighbours as the bait destination and broadcasts a route request in the network to find a path to it. Since the source node already has directly reachable ability to the bait destination, any reply from other nodes in the network would put them into the suspected nodes category. This bait detection technique helps to put all the nodes in the suspected list that would give a false reply to source node. Once the nodes are suspected in the network, the scheme defines the reverse tracing step that would be sending of test packets to the suspected nodes in the network. If the replies by the nodes are not true, then the test packets will be dropped in the network. This would verify the nodes as malicious. The authors in their future work have proposed to detect other attacks in networks such as wormhole attack by using the bait detection approach. In this work, the bait scheme will be modified according to the wormhole attacks.

IV. PROPOSED ALGORITHM

The proposed algorithm is based on the index values of individual nodes. All the nodes of wireless ad-hoc network have zero index value. The algorithm encompasses the following steps:

[A] Initialization:

1. Index values of all the participating nodes are initializing with zero.
2. Initialize the threshold value of the index value with 100.
3. Assumption: 1 index value = 10 packets dropped.

[B] Updating of index values:

1. If the packets are correctly transmitted from one node to another node:

(a) If the correctly transmitted no of packets is between 1 to 10, then index values of the respective nodes will be incremented by one time.

(b) If the correctly transmitted number of packets is greater than 10, then the updated index value will be:

Updated index value = old index value + (correctly transmitted packets / 10);

2. If the packets are dropped/delayed :

(a) The number of dropped or delayed packets is between 1 to 10, and then index value of that particular node is decremented by one.

(b) The number of dropped or delayed packets are greater than 10, then index value of that particular node will be, Updated index value = old index value – (Packet dropped or delayed / 10);

3. If the index value of particular node is negative, then print "Invalid node".

[C] Isolating the Packet drop node from the network:

1. If (Updated index value <<< Threshold index value)
   Then the particular node is treated as malicious node
2. If (Updated index value > Threshold index value)
   Then the particular node is treated as legitimate node.
3. Stop comparing the index values of nodes with threshold value.

V. CONCLUSION

Wormhole is a severely damaging attack to a MANET. If wormholes are not attended properly they will cause immense damages like lose of packets, wrong routing, information theft and uncooperative network etc. In this paper we have tried out a scheme that has been discussed and applied for black holes of MANET and even now we apply it for wormholes. In future this algorithm may be further improved by accompanying the routing concept.

REFERENCES

[1] "Prevention of BLACK HOLE attack in MANET Using Indexing Algorithm", Monika Shivhare1 , Prof. Praveen Kumar , Gautam Department of Computer Science and Engineering Sagar Institute of Research & Technology, Indore, India, IJESC,Volume 7,IssueNo. 5,2017

[2] Dhruvi Sharma, Vimal Kumar, Rakesh Kumar, " Prevention of Wormhole Attack Using Identity Based Signature Scheme in MANET " , Computational Intelligence in Data Mining. Volume 2. Volume 411 of the series "Advances in Intelligent Systems and Computing" pp 475-485. 10 December 2015, Springer.

[3] "Wormhole Attack Detection and Prevention in MANET Using Bait Scheme" Harjinder Kaur , Sukhjit Singh ,Department of Electronics Golden College, Gurdaspur, India,IJESC,Volume 7,IssueNo. 5,2017

[4] " Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach" , IEEE Systems Journal, Vol. 9, No. 1, March 2015

[5] "Security issues in MANET",Rashid Sheikh,Mahakal Singh Chandel,Durgesh Kumar Mishra, 978-1-4244-7202-4/10 IEEE 2010.

[6] P. Basu, N. Khan, and T. D. C. Little, "A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks," in proceedings of IEEE ICDCSW‟ 01, pp. 413–18, Apr. 2001

[7] T. Hara, "Effective Replica Allocation in Ad Hoc Networks for Improving Data Accessibility," Proc. IEEE INFOCOM, pp. 1568-1576, 2001.

[8] Wireless sensor Network security by Intrusion Detection in Energy Efficient Way by P N Rajitha et al,International Journal of Science Engineering and Technology Research,Vol 5,Issue 4, April 2016.

[9] Honeypot-An external layer of security against advanced attacks on Networks by Aaditya Jain et al. ,3rd International Conference on Recent Trends in Engineering Science and Management,April 2016. [10] A. P. K. Gagandeep, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 1, no. 5, 2012

