ISSN:0975-9646

A Novel Scheme to Detect Wormhole Attacks in Wireless Mesh Network

Priti Gupta[#1], Suveg Moudgil[*2]

[#]*CSE Department, KUK University*
Haryana, India

[*]*CSE Department, KUK University*
Haryana, India

***Abstract*— Wireless Mesh Networking is an emerging technology in order to provide a possibility to build a network that can grow in terms of coverage to offer service access (i.e. internet access) for a large number of people with different needs. Wireless mesh networks are more vulnerable to wormhole attack (one out of many kind of attacks). In a typical wormhole attack, two or more malicious nodes plan together by establishing a tunnel using an efficient communication medium. The aim of this paper is to describe a wormhole detection algorithm for wireless mesh networks which detect the wormholes by calculating neighbour list and directional neighbour list of the source node. The main goal of the algorithm is that it can provide approximate location of nodes and effect of wormhole attack on all nodes which is useful in implementing countermeasures. The performance evaluation is done by varying no. of wormholes in the network.**

***Keywords*— Wireless Mesh Networks, Wormhole attack, Wormhole Detection, AODV**

I. INTRODUCTION

Wireless LAN (WLAN) Technology is currently experiencing tremendous growth in popularity, offering secure, seamless mobile access into corporate environments, residential areas, and public spaces. Wireless technologies represent rapidly emerging area of growth and for providing ubiquitous access to the network for the campus community. Wireless is being adopted for many new applications to, eg. Connect computers, to allow remote monitoring, to provide access control and security, and to provide solution for environments where wires may not be the best solution. Wireless Mesh Network[1] solution offers a different solution that can be deployed as an integrated solution to existing infrastructure to extend and expand WLAN access beyond traditional hotspot areas, enhancing coverage and offering seamless mobility. The wireless mesh networking has emerged as a promising technology for future broadband wireless access. A wireless mesh network (WMN) consists of mesh nodes which form the backbone of the network. Wireless mesh networks provide reduced infrastructural costs for access networks spanning up to hundreds of square miles by reducing the use of costly wired entry points that supply access to the Internet. Moreover, self-healing property of WMN enables it to route around network faults using multiple, redundant wireless routes. We define such networks as two-tier mesh networks, consisting of a backhaul tier (mesh node to mesh node also called network access) and user access tier (mesh node to client). Instead of the typical wire line backhaul, the wireless mesh nodes forward data to and from wire line entry points. Clients or access nodes throughout the coverage area then connect to local mesh nodes to receive connectivity back to the wire line network.

WMN[2] consist of mesh clients, mesh gateways, and mesh routers where mesh routers have minimal mobility and form the backbone of WMNs (Figure 1.1). They provide network access for both mesh and conventional clients.

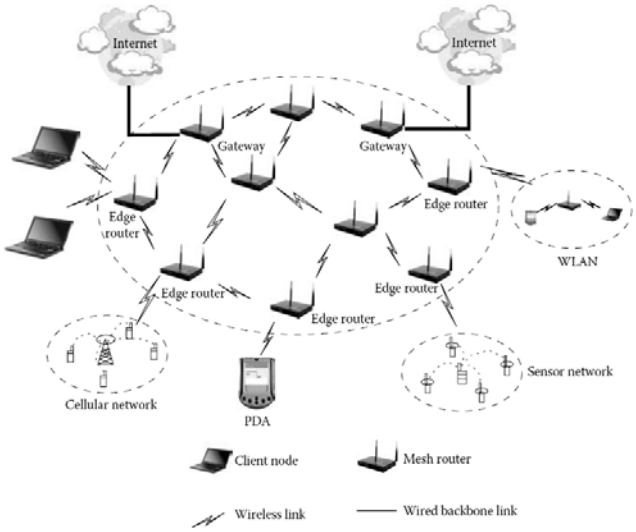

Fig.1.1 A Typical Infrastructure Wireless Mesh Network

In wireless mesh networks (WMNs) wireless mesh routers form densely interconnected multi-hop topologies. For local communication and routing to a wired access network the routers automatically configure a wireless broadband backbone. Three kinds of wireless mesh networks can be identified:

1) In infrastructure WMNs [1] mesh routers form a network offering connectivity to clients. The network is meant to be self-configuring and self-healing and to offer gateway functionality for connections to wired networks.

2) Client WMNs are ad-hoc networks formed by clients amongst themselves. None of the dedicated routers or infrastructure exists, so that the clients have to be self-configuring and act as routers for the traffic in the client WMN (if mobility is there then Client WMNs are very similar to MANETs). In this type of architecture, client nodes constitute the actual network to perform routing and

configuration functionalities as well as providing end-user applications to customers.

3) Hybrid WMNs [1] combine the advantages of the two other WMNs. The infrastructure provides connectivity to other networks such as the Wi-Fi, Internet, cellular, and sensor networks and inside WMNs the routing capabilities of clients provide improved connectivity and coverage.

II. WORMHOLE ATTACK

For introducing a wormhole attack [4], two distant points in the network are connected by an adversary by using a direct low-latency communication link named as the wormhole link. By a variety of means the wormhole link can be established e.g., by using a Ethernet cable, a long range wireless transmission, or an optical link and many more. Once the wormhole link is established, wireless transmissions captured by an adversary on one end, send them through the wormhole link and replay them at the other end or simply drop some amount of data or the whole data. Several vulnerabilities exist in the protocols for WMNs that can be exploited by the attackers to degrade the performance of the network. The assumed trust and the lack of accountability make the MAC layer protocols and the routing protocols vulnerable to various active attacks, such as black hole attacks, wormhole attacks, and rushing attacks. In a typical wormhole scenario [3], two or more malicious nodes collude together by establishing a tunnel using an efficient communication medium. During the route discovery phase of on-demand routing protocols like AODV, the Route Request messages are forwarded using the established tunnel between the malicious nodes. Therefore, the first Route Request message that reaches the destination node is the one forwarded by the malicious nodes which results in the fact that, the malicious nodes are added in the path from source to destination. Once the malicious nodes are included in the routing path, either they drop all the packets which results in complete denial of service, or drop selected packets to avoid detection.

An example is shown in Fig 2.1. Here X and Y are the two end-points of the wormhole link (called as wormholes). X replays in its neighbourhood (in area A) everything that Y hears in its own neighbourhood (area B) and vice versa. After analysing this the effect of such an attack is that all the nodes in area A assume that nodes in area B are their neighbours and vice versa. As a result, affects routing and other connectivity in the network (because according to the X and Y's reply the other node changes their routing information that is not real). Once the new routes are established and the traffic in the network starts using the X-Y shortcut, the wormhole nodes can start dropping packets and cause network disruption.

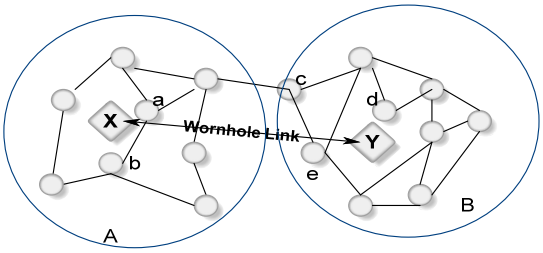

Fig 2.1: A typical wormhole scenario

A) Types of Wormhole Attack

Wormhole attacks can be classified as:-

1) Wormhole using Packet Encapsulation

In encapsulation-based wormhole attacks[11], some nodes exist between two malicious nodes and the data packets are encapsulated. Since encapsulated data packets are sent between the malicious nodes, the actual hop count does not increase during the traversal. So routing protocols that use hop count for path selection are particularly susceptible to encapsulation-based wormhole attacks.

2) Wormhole Using Packet Relay

Packet-relay-based wormhole attacks[11] can be launched by one or more malicious nodes. According to this type of attack, a malicious node relays data packets of two distant sensor nodes to convince them that they are neighbors. This kind of attack is also called "replay-based attack" in the literature.

3) Wormhole Using Protocol Distortion

In this, one malicious node tries to attract network traffic by distorting the routing protocol. Instead of the smallest hop count routing protocols which are based on the 'shortest delay' is at the risk of wormhole attacks by using protocol distortion.

4) *Wormhole Using High-quality/Out-of-band Channel*

In this mode, the wormhole attack is launched by having a high-quality, single-hop, out-of-band link (called tunnel) between the malicious nodes. By using a direct wired link or a long-range directional wireless link this tunnel can be achieved. This mode of attack is more difficult to launch than the packet encapsulation method since it needs specialized hardware.

III. RELATED STUDY

Hu, et al.[4] use the packet leashes approach to detect wormhole attacks. A leash is the information that is added to a packet and designed to restrict the packet maximum allowed transmission distance. Geographical or temporal information is contained in the packet leashes to bound the distance or the lifetime of an end-to-end transmitted packet. When a sender delivers packets, a domain in the packet contains geographical leash or temporal leash. A receiver checks if it's out of bound. A a result GPS must be used to acquire geographical information and tight clock synchronization are needed for temporal information.

A Lightweight Countermeasure for the Wormhole Attack in Multi-hop Wireless Networks (LITEWORP) is proposed by Khalil, et al. [5]. LITEWORP uses secure two-hop neighbor discovery and local monitoring of control traffic to detect nodes involved in the wormhole attack. It provides a countermeasure that isolates the wormhole nodes from the network therefore removing their ability to cause future damage..

In [6], a method that uses directional antennas to detect wormhole attacks is proposed. Each node gets approximate direction information based on received signals. And each node maintains a neighbor list using a protocol called neighbor discovery. As directional information is added, attacks become increasingly difficult to execute successfully.

V.S .Shankar Sriram [7] proposed architecture and analyzed the possibility of wormhole attack along with a countermeasure to avoid such an attack. The proposed work involves the shared information between communicating access points to prevent Rouge Access Points from

masquerading as false neighbours. The author's defence greatly diminishes the threat of wormhole attacks and requires no location information or clock synchronization. In initial research it has been focused that wormhole attack is possible only on adhoc networks, but now-a-days wormhole attack is possible on infrastructure based wireless LANs also.

Pushpendra Niranjan[8] implemented a new method which detects the attacker nodes and works without modification of protocol, using a hop-count and time delay analysis from the viewpoint of users without any special environment assumptions instead of detecting suspicious routes by specifically considering Tunneling attack which does not require exploiting any nodes in the network and can interfere with the route establishment process.

Huaiyu Wen and Guangchun Luo [9] proposed a high efficiency wormhole detection algorithm based on 2-hop neighbor in WMNs, which is called Wormhole Detection based on Neighbour's Neighbour scheme (WDNN) to enhance the efficiency and facility of wormhole detection .Then a simple Random Walk Route scheme (RWR) is proposed to prevent routes from wormholes in which the route is chosen without using the low latency link which is created by wormholes.

P Subhash and S Ramchandram[10] proposed a mechanism to prevent byzantine wormhole attack in WMNs. The proposed work relies on digital signatures and prevents formation of wormholes during route discovery process and it is designed for an on-demand hop-by-hop routing protocol like HWMP (Hybrid Wireless Mesh Protocol-the default routing protocol for WMN). This is also applicable to source routing protocols like DSR(Dynamic Source Routing). This is a software based solution and does not require additional (or) specialized hardware.

Nishant Sharma[11] proposed scheme that detects and further prevents wormhole attack in wireless sensor networks. Location information of nodes in network were used in proposed scheme and uses Euclidean Distance Formula to further detect and prevent wormhole attack and make the communication between sensor nodes more secure and reliable.

IV. PROPOSED OBJECTIVES AND WORMHOLE ATTACK DETECTION ALGORITHM

The objective is to propose a scheme for wormhole detection in wireless mesh network and performance evaluation of proposed scheme by varying no. of wormholes in the network.

The wormhole attack detection algorithm is proposed:

Step 1: Set the values of X_Range and Y_Range of terrain area,,Node_Num,Antenna_Num,Radio_Range,Directional_ Range , Iteration,pi

Step 2: Two functions are defined i.e distance and direction

Step 3: Calculate density and directional density.

Step 4: Initialize the position of randomly distributed nodes.

Step 5: Initialize the neighbor list and directional neighbor list of nodes

Step 6: For each node, initialize the array and for each direction apply the following conditions:

Condition 1: No node in this direction of wormhole so the attack is not meaningful

Condition 2: Atleast one node in other direction can detect anomaly

Try out in different five directions

Step7:Calculateavg_neighbor_num,avg_trust_neighbor_num,disconnected_num

Step 8:Free the Key_list and Neighbor_list

Step 9:Set the distance from one node to another node.

V. RESULTS AND DISCUSSIONS

Simulations are performed in GloMoSim which stands for Global Mobile information systems, a network simulator that provides support for simulating multi-hop wireless networks complete with physical and IEEE 802.11 MAC layer models. The whole scenario consist of 50 nodes in which one wormhole is present and 100 nodes in which two wormholes are present. The parameters set up for our simulation are described below:

PARAMETER	VALUE
Number of Nodes	50,100
Terrain range	(800,800) (1000,1000)
Bandwidth	2Mbps
Simulation Time	15 m
Node-placement	Uniform
Mobility	Random Waypoint Motion
Traffic Model	CBR
MAC Protocol	802.11
Routing Protocol	AODV
Wormholes	1,2

Table 1:- Simulation Parameters

The wormhole detection algorithm helps to provide the effect of wormhole attack on total nodes by describing how many nodes are partially affected,disconnected and unaffected in diffrent wormhole scenario.

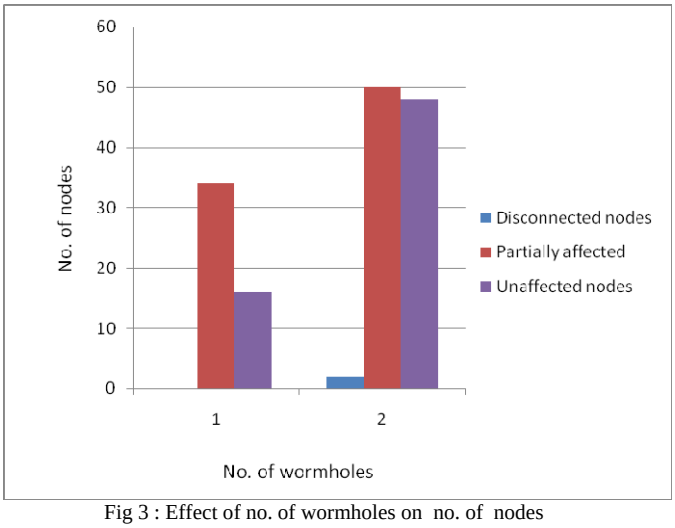

Fig 3 : Effect of no. of wormholes on no. of nodes

Figure 3 shows that when there is one wormhole in the network, there is no disconnected node having 15 unaffected nodes and 35 partially affected nodes out of total 50 nodes.When there is two wormholes in the network there

are limited no. of disconnected nodes having 50 partially affected nodes and 48 unaffected nodes out of total 100 nodes

A)Performance Analysis

The parameters used in our simulation to compare results of network by varying the no. of wormholes are Throughput and Packets Delivery ratio.

1)Throughput is defined as the average rate of successful message delivery over a communication channel. The throughput is measured in kilo bits per second (kbps or kbit/s). Greater the value of throughput means better the performance of the protocol.

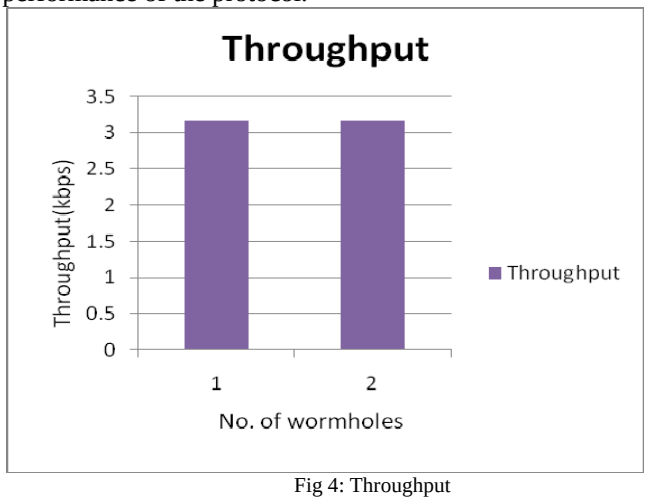

Fig 4: Throughput

Figure 4 shows that when there is one and two wormhole in the network the throughput is same for both i.e consistent.

2) Packet delivery ratio is defined as the ratio of the number of packets actually delivered without duplicates to the destinations versus the number of data packets supposed to be received.

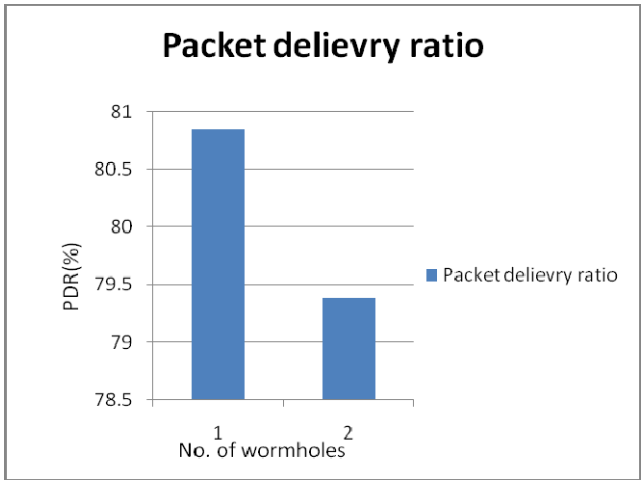

Fig 5 : Packet Delivery Ratio

VI. CONCLUSION

The wireless mesh networking has emerged as a promising technology for future broadband wireless access but we have shown that wireless Mesh Networks are more vulnerable to wormhole attacks (out of many kind of attacks).In this paper wormhole attack is detected using proposed algorithm. The algorithm is simple and easy to understand. Our simulation results have shown the effect of wormhole attack on the network. We expect this algorithm will help to prevent wireless mesh network against wormhole attacks. The performance is analysed by varying no. of wormholes showing consistent results.

REFERENCES

[1] Safak Durukan Odabasi et al. ,"A Survey on Wireless Mesh Networks,Routing Metrics and Protocols" ,International Journal Of Electronics,Mechanical and Mechatronics Engineering, Vol.2 Num.1 pp.(92-104)

[2] Ian F. Akyildiz, Xudong Wang, Weilin Wang, Wireless mesh networks: A survey, in Computer Networks, IEEE , September 2005, 445-487

[3] Moutushi Singh et al.," A Survey of Different Techniques for Detection of Wormhole Attack in Wireless Sensor Network" , International Journal of Scientific & Engineering Research Volume 3, Issue 10, October-2012

[4] Y. C. Hu, A. Perrig, D. B. Johnson, Packet leashes: A defense against wormhole attacks in wireless networks, in INFOCOM 22th IEEE 2003, Vol. 3, April 2003, 1976-1986

[5] I. Khalil, S. Bagchi, N. B. Shroff, LITEWORP: A lightweight countermeasure for the wormhole attack in multihop wireless networks, Proc. IEEE DSN'05, (New York, USA), June 2004, 612-621

[6] L. Hu, D. Evans, Using directional antennas to prevent wormhole attacks, NDSS, Feb. 2004, 1-11

[7] V.S.Shankar Sriram, Ashish Pratap Singh, G.Sahoo, "Methodology for Securing Wireless LANs Against Wormhole Attack", International Journal of Recent Trends in Engineering, Issue. 1, Vol. 1, May 2009

[8] Pushpendra Niranjan et al., "Detection of Wormhole Attack using Hop-Count and Time-Delay analysis", International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 1 ISSN 2250-3153

[9] P Subhash and S Ramachandram, "Preventing Wormholes in Multi-hop Wireless Mesh Networks",Third International Conference on Advanced Computing & Communication Technologies,IEEE 2013

[10] Huaiyu Wen and Guangchun Luo, "Wormhole Attacks Detection and Prevention Based on 2-Hop Neighbour in Wireless Mesh Networks" Journal of Information & Computational Science 10:14 (2013) 4461–4476, September 20, 2013

[11] Nishant Sharma et al., "A Location Based Approach to Prevent Wormhole Attack in WSN" ,IJARCSSE Vol4 , Issue 1, January 2014,pp 840-845