Wormhole Attack Detection for Wireless Mesh Networks

Rohit Jain, Kamal kumar

***Abstract*— The ability of wireless mesh networking cannot be exploited without considering and adequately addressing the involved security issues. Wireless Mesh Networks are a promising and gradually maturing technology that cannot be ignored anymore when considering various wireless networking technologies for deployment. This paper proposes authentication and authorization implementation for increasing the security in Wireless Mesh Networks, which would make their deployment more efficient and resistant to possible kinds of attacks. The simulation is done using GlomoSim, to analyze the performance of wireless mesh network with wormhole attack. Two CBR (Constant Bit Rate) application, UDP/IP, IEEE 802.11b MAC and physical channel based on statistical propagation model. Insuring robust authentication and authorization would give confidence for any customers in the security aspect of Wireless Mesh Network.**

***General Terms*—Wireless mesh networks, routing protocols, Wormhole attacks, out-of-band link.**

***Index Terms*— Wormhole using Packet Encapsulation, Wormhole Using Packet Relay, Wormhole Using Protocol Distortion, Wormhole attack detection mechanism.**

I. INTRODUCTION

The wireless technology is low cost, low maintenance and speedily installable. Thus a number of indoor and outdoor network technologies are developed to serve according to the need of services. Among a number of different technologies the wireless mesh network is one of the essential technologies. The (WMNs) wireless mesh networks are very useful because of its self-healing and self-configuring nature. That can be used for cellular mobile networks, business networks, community networks [1].

Typical WMN as shown in Figure 1 is constitute of a set of stationary mesh routers (MRs) that form the mesh backbone and a set of mesh clients that interacted via mesh routers. Security is a critical component that contributes to the performance of WMN. The utmost challenges that need to be dealt with in addressing security issues mainly arise due to open nature of the wireless medium and multi-hop cooperative transmission environment. These factors make network services more vulnerable, specifically due to attacks coming from within the network [2] .

Rohit Jain, MVVEC, JAGADHRI.

Kamal kumar, Assistant Professor, ECE epartment, MVVEC, JAGADHRI.

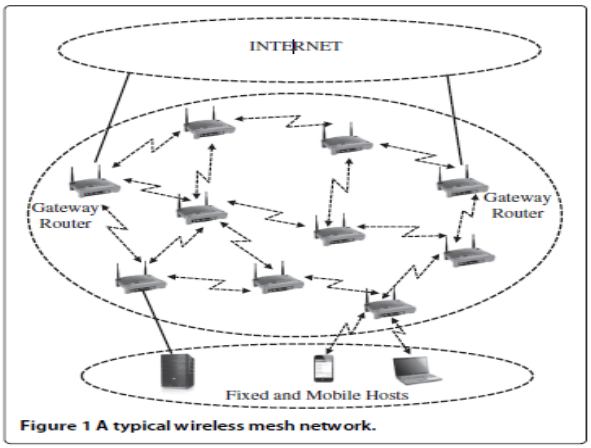

Figure 1 A typical wireless mesh network.

1.1 Types of wormhole attacked:

Wormhole attacks can be classified as:-

1.1.1 Wormhole using Packet Encapsulation:

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

1.1.2 Wormhole Using Packet Relay

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

1.1.3 Wormhole Using Protocol Distortion:

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

1.1.4 Wormhole Using High-quality/Out-of-band Channel:

In this mode, the wormhole attack is initiated by having a high-quality, single-hop, out-of-band link (called tunnel) between the destructive nodes. By using a direct wired link or a long-range directional wireless link this tunnel can be attained. This mode of attack is more difficult to launch than

the packet encapsulation method since it needs specialized hardware [3].

1.2 Wormhole attack detection mechanism:

Broadly the different detection mechanism falls into the described two types:

1.2.1 Centralized mechanisms: In the centralized approach, data collected from the local neighborhood of each node are sent to a central entity. The central entity uses the received data to construct a model of the full network, & tries to detect inconsistencies in this model that are potential indicators of the wormholes. This entity tried to trap the wormholes by identifying all the inconsistencies in the main structured model. Various types of instabilities that might get appeared in the model, due to wormholes, mainly depend on the nature of the local information provided by the nodes. The following techniques come under it are:-

- Statistical Wormhole Detection
- Wormhole Detection using different multi-dimensional Scaling approaches

1.2.2 Decentralized mechanisms:- In this approach, every node keeps on creating a model of its own neighbourhood using locally composed data, hence no central entity is required ,which is surely a big advantage of this technique. The advantage of decentralized wormhole detection mechanisms is that they do not need a central entity to be employed, and thus it can be used in a wider range of applications .The various main approaches used for observing wormholes that comes under it are:

- Wormhole detection based on estimating the distance
- Wormhole detection based anchors positional information
- Wormhole detection using directional range information [4].

1.3 Routing approach for preventing wormhole attack:

1.3.1WRSR (wormhole-resistant secure routing):

This protocol prevents the selection of route demand traversing the wormhole link. WRSR is based on HWMP and therefore inherits majority of its characteristics. The operating principle of WRSR is to permit nodes to monitor the two-hop sub-path on a (RREQ) received route request and identify a RREQ that traverses a wormhole. A route demand that traverses via a wormhole link would not satisfy the required wormhole-free path criterion, which can be observed at the neighbors of a wormhole node and can easily be quarantined [5].

1.3.2 WHOP: WHOP is very secure protocol against any malicious action being done by node under scan of hound packet. Hidden wormhole attack cannot be feasible in WHOP as a result of if node hides its identity whereas forwarding RREQ or RREP, the node who receives such packet once it, would discard the packet as a result of it might not realize the last hop entry within the packet as its adjacent node. So, malicious node must reveal its identity while forming the route from source node to destination node. Figure 2 shows m1 is a malicious node forming wormhole with m2 in the path [6].

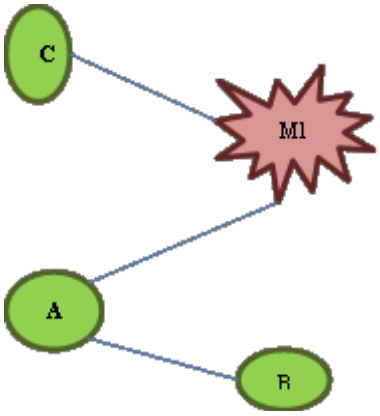

Figure 2: Security Analysis[6]

II. LITERATURE SURVEY

The research work performed in this field by different researchers is presented as follows:

Virendra Dani et al. (2015) this paper locates the wormhole link in network and tries to recover the network performance during the attack conditions. Thus, the method detects the malevolent nodes and prevents formation of wormholes. The Proposed mechanism based on two stage solution. In first stage the threshold value is computed using the different routing scenarios, the threshold value occupy the network transmission delay in network and in second phase the threshold value is used to observe the malevolent link in the network. The implementation of the proposed concept is provided using the Ad-hoc on Demand Distance Vector routing protocol updating in network simulator 2 i.e. NS-2.

Rakesh Matam et al.(2013) this paper suggest WRSR, a wormhole-resistant secure routing algorithm that detects the presence of wormhole during route finding process and quarantines it. Unlike other existing approches that initiate wormhole detection process after observing packet loss, WRSR identifies route requests visiting a wormhole and prevents such routes from being established. WRSR uses unit disk graph model to determine the required and sufficient condition for identifying a wormhole-free path. The most attractive features of the WRSR consists its ability to defend against all forms of wormhole (hidden and Byzantine) attacks without depending on any extra hardware like global positioning system, synchronized clocks or timing information, and computational intensive conventional cryptographic mechanisms**.**

Priti Gupta et al. (2014) The aim of this paper is to narrate a wormhole observation algorithm for wireless mesh networks which detect the wormholes by calculating neighbour index and directional neighbour index of the source node. The main goal of the algorithm is that it can provide approximate location of nodes and result of wormhole attack on all nodes which is useful in implementing countermeasures. The performance evaluation is done by different no. of wormholes in the network.

Huaiyu Wen et al.(2013) a simple (RWR) Random Walk Route scheme is proposed to prevent routes from wormholes, which attract traffic of the routing protocols depends on min cost. In WDNN, through enlarging the transmission range of the 2-hop neighbor, the faked network topology obtained by wormholes can be detected without utilize extra hardware or clock synchronization. In RWR, the route is selected without using the low latency link which is created by wormholes. Security analysis shows that the wormhole attacks can be observed and also be prevented using our schemes efficiently. And our simulation results also indicate that our schemes can produce a 100% wormhole detection rate and prevent routes from being attacked by the adversary against traditional routing protocols.

Pushpendra Niranjan et al.(2012) In this paper author specifically considering Tunneling attack which does not require utilizing any nodes in the network and can interfere with the route establishment process. Instead of detecting suspicious paths as in previous methods, author implement a new method which detects the attacker nodes and works without renovate of protocol, using a hop-count and time delay analysis from the viewpoint of users without any special environment assumptions. The suggested work is simulated using OPNET and results showing the advantages of proposed work**.**

III. PROPOSED WORK

3.1 Problem Formulation

The detection and prevention of wormhole attack are complicated by the network. In wormhole attack, the adversary connects two distant points in the network using a exact low-latency link which is called the wormhole link Once the wormhole link is established, the two colluding malicious nodes begin to launch wormhole attack. The adversary eaves drops messages at one end of the link and relays messages at the other end of the link. Thus, nodes choose to transmit messages through this wormhole link since this route needs fewer hops to destination than normal routes. During this period, the wormhole nodes can launch other kinds of attacks, such as selective forwarding attack. If the wormhole link is short, it may not attract much traffic, and hence will not do much damage to the network hole attack, etc. There is significant effect of wormhole attack on network performance.

A simulation is implemented using GlomoSim, to analyze the performance of wireless mesh network with wormhole attack.

3.2 Proposed Work

The proposed architecture is decentralized and partially distributed. It is particularly designed for Wireless Mesh Networks. We have implemented Wormhole attack in a GlomoSim. For our simulations, we used two (Constant Bit Rate) CBR application, UDP/IP,IEEE 802.11b MAC and physical channel based on statistical propagation model. The simulated network consists of 50 and 100 randomly allocated wireless nodes in 800 by 800 square meter flat space. The node transmission range is 250- meter power range. The size of data payload is 512 bytes. In both scenarios some node nodes are normal and some are connected with the wireless subnet having wormhole property. The simulation is done using GlomoSim, to analyze the performance of wireless mesh network with wormhole attack.

IV. RESULTS AND ANALYSIS

4.1 Simulation Environment

GloMoSim which named as Global Mobile information systems, a network simulator that provides support for simulating multi-hop wireless networks finished with physical and IEEE 802.11 MAC layer models. Two scenarios are used first scenario consists of 50 nodes in which one wormhole is present and second scenario consists of 100 nodes in which two wormholes are present. The parameters used for simulation are described in table 4.1

PARAMETER	VALUE
Number of Nodes	50,100
Terrain range	(800,800) (1000,1000)
Bandwidth	4Mbps
Simulation Time	15-60 S
Node-placement	Random
Mobility	Random Waypoint Motion
Traffic Model	CBR
MAC Protocol	802.11
Routing Protocol	DSR
Wormholes	1,2

Table 4.1 Simulation Parameters

4.2 Simulation Evaluation

We have taken two scenarios of network. One consisting of 50 nodes in the network and other consists of 100 nodes in the network. In scenario consisting of 50 nodes we have inserted one wormhole in the network and in scenario consisting of 100 nodes we have inserted two wormholes in the network. Now we are detecting the wormhole attack which shows the effect of wormhole attack on the nodes of network and provides their locations in the network which can help in preventing the wormhole attack. The effect of wormhole attack on the nodes of network is shown below

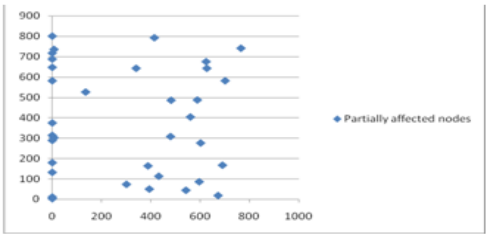

Fig 4.1 partially affected nodes in 50 nodes scenario

In fig 4.1 partially affected nodes in 50 nodes scenario has been shown in the form of graph.

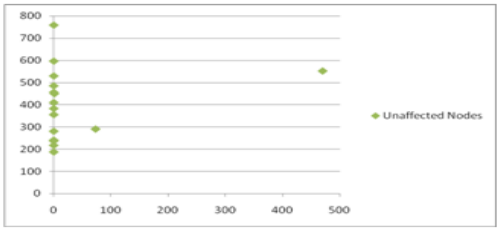

Fig 4.2 Unaffected nodes in 50 nodes scenario

In fig 4.2 unaffected nodes in 50 nodes scenario has been shown in the form of graph.

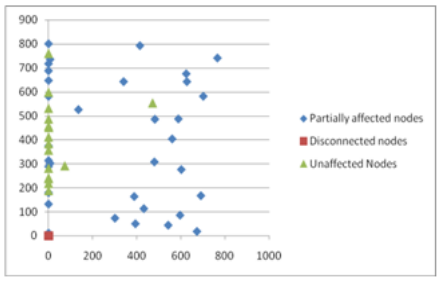

Fig 4.3 Complete network in 50 nodes scenario

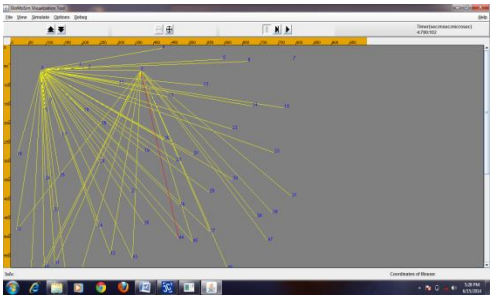

Fig 4.4 50 nodes scenario in glomosim visualization tool

In fig 4.4 50 nodes scenario in glomosim visualization tool has been shown.

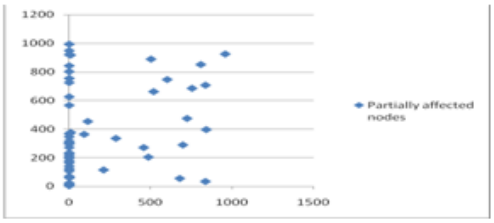

Fig 4.5 Partially affected nodes in 100 nodes scenario

In fig 4.5 partially affected nodes in 100 nodes scenario has been shown in the form of graph.

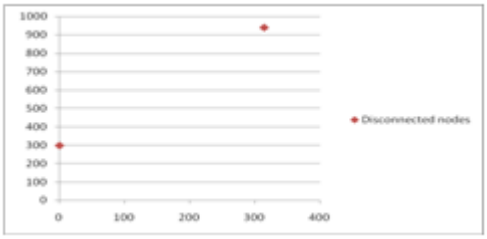

Fig 4.6 Disconnected nodes in 100 nodes scenario

In fig 4.6 disconnected nodes in 100 nodes scenario has been shown in the form of graph.

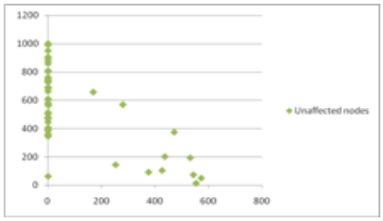

Fig 4.7 Unaffected nodes in 100 nodes scenario

In fig 4.7 unaffected nodes in 100 nodes scenario has been shown in the form of graph.

The complete scenario for 100 nodes is shown in the form of graph as below:

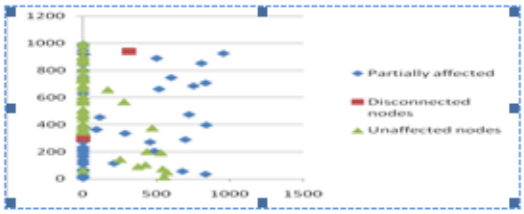

Fig 4.8 Complete network in 100 nodes scenario

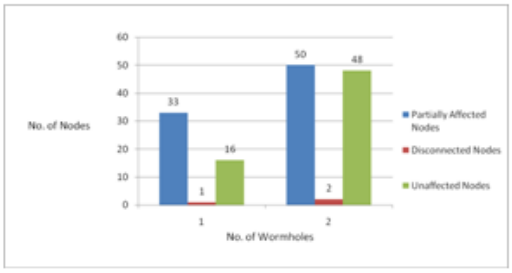

Fig 4.9 Effect of no. of wormholes on 50 & 100 Nodes

In fig 4.9 the effect of no. of wormholes on no. of nodes of the network in both the scenarios has been shown.

The 100 nodes scenario in glomosim visualization tool has been shown in the fig 4.10

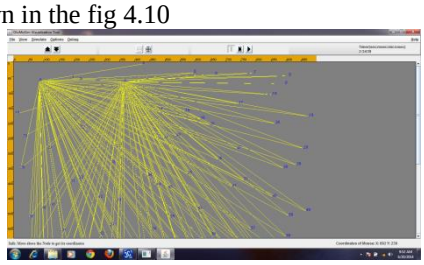

Fig 4.10 : 100 nodes scenario in glomosim visualization tool

4.3 Performance evaluation:

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

1) **Packet delivery ratio** is defined as the ratio of the number of packets literally delivered without duplicates to the destinations versus the number of data packets assumed to be received.

2) **Throughput** is termed as the average rate of successful message delivery over a communication channel. The throughput is calculated in kilo bits per second (kbps or kbit/s). Greater the value of throughput means better the potential of the protocol.

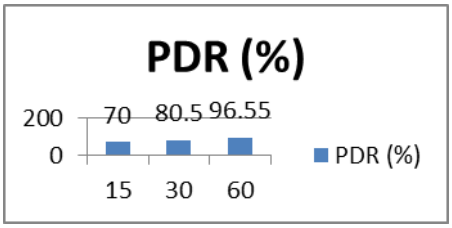

Fig 4.11: PDR (15-60 S) for 50 nodes

In Fig 4.11 Packet delivery ratio (15-60 S) for 50 nodes has been shown.

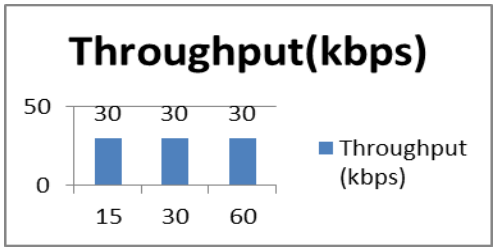

Fig 4.12 : Throughput (15-60 S) for 50 nodes

In Fig 4.12 Throughput (15-60 S) for 50 nodes has been shown.

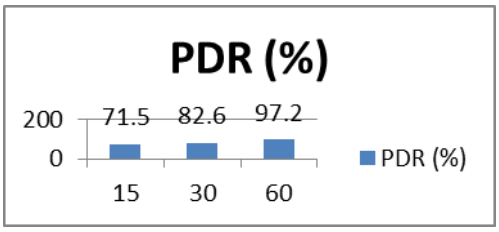

Fig 4.13: Packet Delivery Ratio (15-60 S) using 100 nodes.

In Fig 4.13 Packet delivery ratio (15-60 S) for 100 nodes has been shown

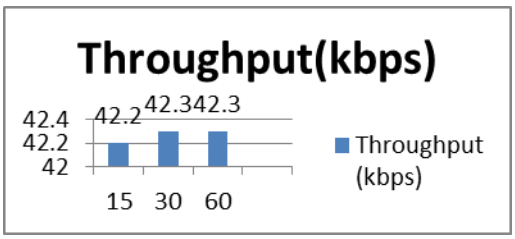

Fig 4.14: Throughput (15-30 s) for 100 nodes

In Fig 4.14 Throughput (15-30 S) for 100 nodes has been shown.

V. CONCLUSION

The proposed architecture is decentralized and partially distributed. In this work, we evaluated the affect of wormhole attack on the mesh network topology (one with 50 nodes and other with 100 nodes). Performance is evaluated which explores the throughput and packet delivery ratio for both scenarios. Work mainly focused on the connectivity information without any additional requirement of special hardware devices (GPS).

REFERENCES

[1] Virendra Dani1, Vijay Birchha ,"An Improved Wormhole Attack Detection and Prevention Method for Wireless Mesh Networks", Vol. 4, Issue 12, December 2015.
[2] Rakesh Matam and Somanath Tripathy,"WRSR: wormhole-resistant secure routing for wireless mesh networks", 2013.
[3] Priti Gupta, Suveg Moudgil,"A Novel Scheme to Detect Wormhole Attacks in Wireless Mesh Network", Vol. 5 (3), 2014.
[4] Er. Pinki Tanwar Himani Gupta," Partially Distributed Authentication Solution for Securing WMN against Wormhole Attacks", Volume 5, Issue 5, May 2015.
[5] Huaiyu Wen, Guangchun Luo, "Wormhole Attacks Detection and Prevention Based on 2-Hop Neighbor in Wireless Mesh Networks", September 20, 2013.
[6] Miss Neha Jain, Ashish Kr. Shrivastava,"Reactive Routing approach for preventing wormhole attack using hybridized WHOP", Volume 13, Issue 3 (Jul. - Aug. 2013).
[7] Pushpendra Niranjan, Prashant Srivastava, Raj kumar Soni, Ram Pratap," Detection of Wormhole Attack using Hop-count and Time delay Analysis",Volume 2, Issue 4, April 2012.
[8] Mohan Seth,"Detection of Wormhole Attacks in Wireless Sensor Networks", May 11, 2013.