International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 08 | Aug -2017 www.irjet.net p-ISSN: 2395-0072

To Design a Hybrid Algorithm to Detect and Eliminate Wormhole Attack in Wireless Mesh Network

Pranita Lende[1], Abhay Satmohankar[2]

[1]*Research Scholar, Department of Electronics, Wainganga College of Engineering and Management, Maharashtra ,india*
[2]*Assistant Professor, Department of Electronics, Wainganga College of Engineering and Management, Maharashtra, india*

Abstract –*Wireless mesh networking is an emerging technology in order to provide low-cost, high bandwidth. Wireless access services for a large number of people with different needs. One out of many kinds of attacks in Wireless mesh networks is more vulnerable to wormhole attack. There are two different nodes in wireless communication between which are dynamically self-organized and self-configured. In a wormhole attack, two or more malicious nodes plan together by establishing a tunnel and they are using an effective communication medium. At the same time, most of the existing wormhole defense mechanisms are not secure at the same time and wormhole attacks that are launched in participation mode also at the same time. In this paper is described a wormhole detection algorithm for wireless mesh networks and they detect the wormhole by calculating neighbor list and the directional neighbor list of the source node. it can provide an approximate location of nodes and effect of wormhole attack on all nodes which is useful in implementing counter measures this is the main goal of this paper. The performance evaluation is done by varying number of wormholes in the network.*

Key Words: **Wireless mesh network, Wormhole attack, Cryptographic mechanism, Wormhole detection, WSN**

1. INTRODUCTION

A different solution that can be deployed as an integrated solution to existing infrastructure to extend solution offers wireless mesh network [1]. and also wireless mesh network solution offers to expand WLAN access beyond traditional hotspot areas, enhancing coverage and offering seamless mobility. Promising technology is in wireless mesh networking have emerged for future broadband wireless access. Mesh nodes which form the backbone of the network are consisting of in wireless mesh network (WMN).

Wireless mesh networks by reducing the use of costly wired entry point that supply access to the Internet and also reduced infrastructural costs for access networks spanning up to hundreds of square miles. Moreover, WMN enables it to route around network faults using multiple, redundant wireless routes this is self-healing property.

We define such wireless 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 a client).The wireless mesh nodes forward data to and from wire line entry points instead of the typical wire line backhaul. Local mesh nodes to receive connectivity back to the wire line network to connected and Clients or access nodes throughout the coverage area.

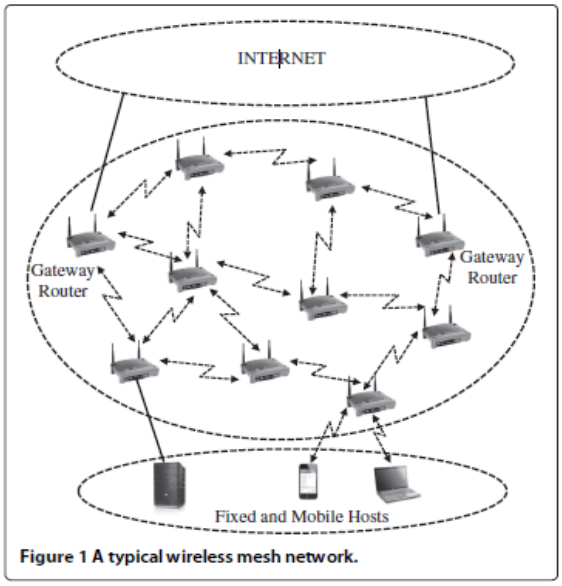


Figure 1 A typical wireless mesh network.

Wireless mesh network[2] consist of mesh clients, mesh gateways, and mesh routers where mesh routers have minimal mobility and form the backbone of WMNs. Wormhole attacks categorized into two types depending on the type of adversary involved.

Hidden wormhole attack is wormhole attack launched by colluding external adversaries. Similarly, an exposed/Byzantine wormhole attack is called a wormhole attack launched by malicious colluding internal nodes.

1.1 Typical Infrastructure Wireless Mesh Network

In wireless mesh routers and wireless mesh networks (WMNs) form densely interconnected multi-hop topologies. In wireless mesh networks, to a wired access network the router automatically configures a wireless broadband backbone for routing and local communication. Three types of wireless mesh networks can be identified

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

2) ad-hoc networks formed by clients amongst themselves are client WMNs. The clients have to be self-configuring none of the dedicated routers or infrastructure exists and act as routers for the traffic in the client WMN. Perform routing and configuration functionalities as well as providing end-user applications to customers to client nodes constitute the actual network this type of architecture.

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

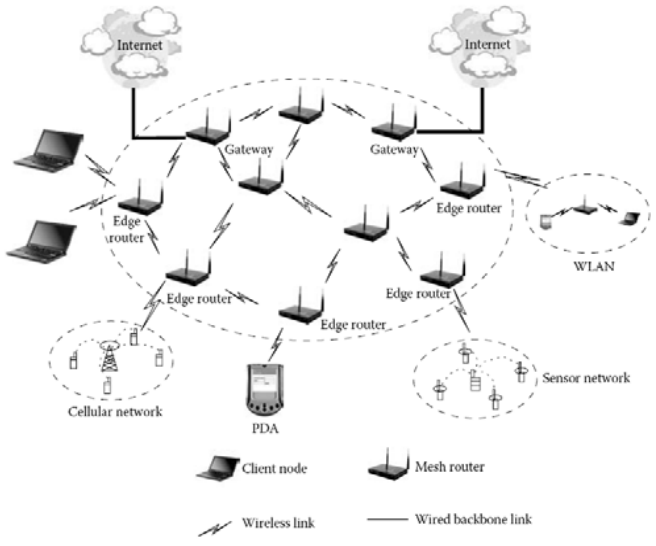
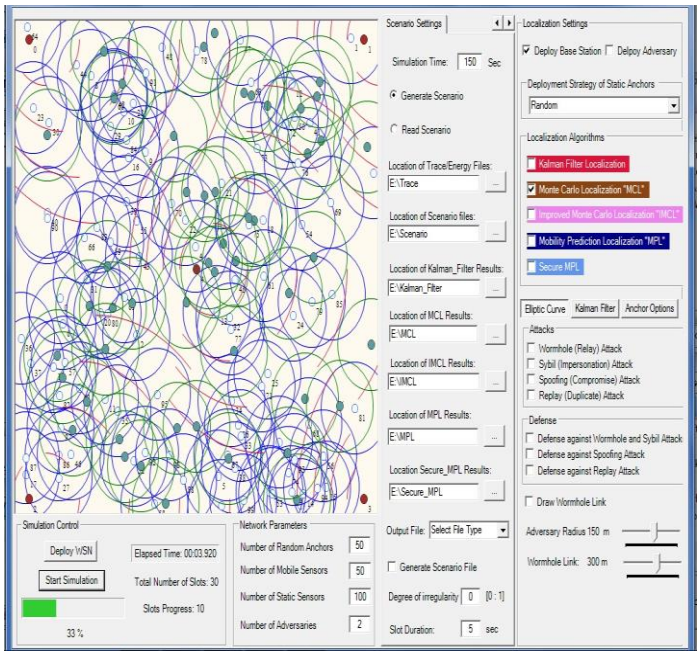


Fig.1.1 A Typical Infrastructure Wireless Mesh Network

1.2 Wormhole Attack

By a variety of means, the wormhole link can be established two distant points in the network are connected by an adversary by using a direct low-latency communication link named as the wormhole link e.g., by using an Ethernet cable, a long range wireless transmission, or an optical link and much more for introducing a wormhole attack [3].

wireless transmissions captured by an adversary on one end Once the wormhole link is established, send them through the wormhole link and replay them at the other end or simply drop some amount of data or the whole data. the packet leashes approach to detect wormhole attack used by Hu, et al.[3]. To restrict the packet maximum allowed transmission distance is designed and a leash is an information that is added to a packet. The lifetime of an end-to-end transmitted packet in the packet leashes to bound the distance geographical or temporal information is contained.

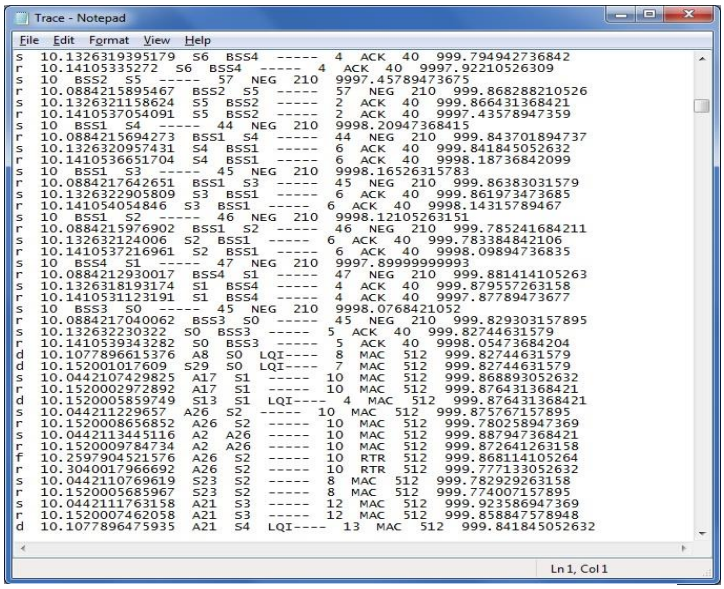


2. WSN Localization

The effect of these alterations on the model's behavior can be observed can be simulated such as a channel noise and sensor modes (i.e. wake up and sleep), Modeling the localization problem is virtually impossible to solve mathematically.How variables interact valuable insight may be obtained into by which variables are most important observing the resulting outputs and by changing simulation inputs.

Cryptographic techniques are the study of the technique for secure communication in the presence of third parties called adversaries. In cryptography, a message authentication code (MAC) is a short piece of information used to authenticate a message. RTR means network layer, AGT means application layer and MAC means media access control layer. The packets from one location and transmits them to other distant located node which distributes them locally captured from attacking node.

The attacker without having knowledge of the network or cryptographic mechanism wormhole attack launched or compromising any legitimate nodes. Oracle Database creates to help you diagnose and resolve operating problems that trace File is trace (or dump) file. A trace file Each server and background process writes. it writes information about the error to its trace file When a process detects an internal error. For debugging the database or when diagnosing errors used in TRC files.

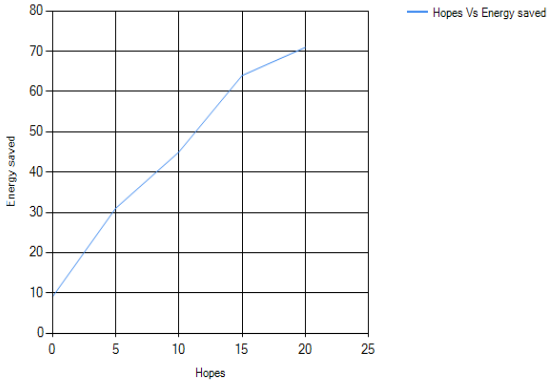


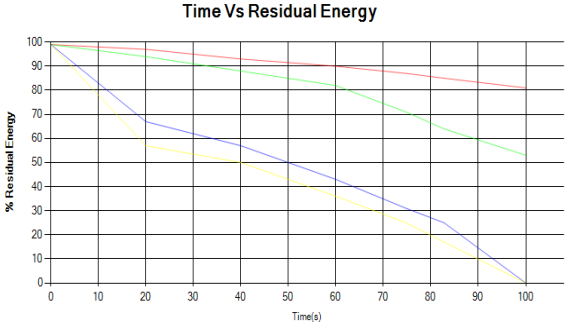
3. RESULTS AND ANALYSIS

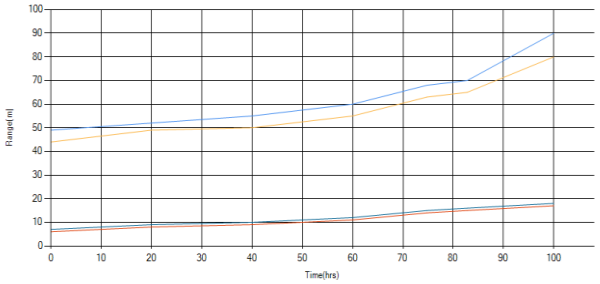
The aim of this paper is performed on WSN localization simulator- Microsoft visual studio. first, if we are deploying the network and create nodes and start simulation using algorithms. After creating the trace file and then attack defense and detection. Import trace file using cryptographic technique MAC used. node is sender or receiver. The time stamp is given duration to send information. Node ID means entry node is having one unique ID.

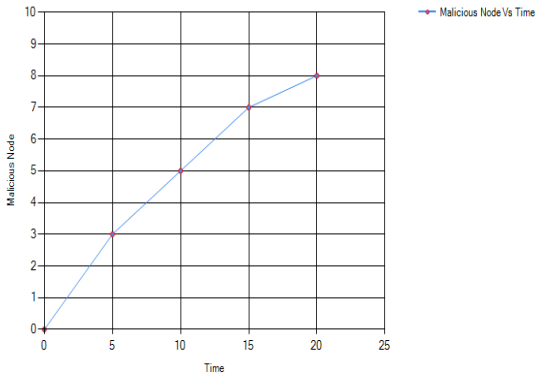
Three layers are used in this project which are RTR, AGT. Hop count is we pass the information by dividing it is packets. Each of this packet is called hop and no. of packets created is called hop count. Message ID is a message from each node is denoted by unique ID called message ID. RTR layer is a network layer, AGT layer is application layer and MAC layer is a media access control layer.

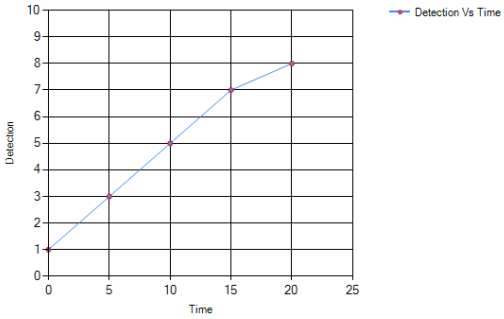
1. Energy save vs hopes
2. Residual Energy vs time
3. Range vs time
4. Malicious node vs time
5. Detection vs time











4. CONCLUSION

A promising technology is the wireless mesh networking has emerged for future broadband wireless access but wireless mesh networks are more vulnerable to wormhole attacks. The hybrid algorithm is simple and easy to understand. Our simulation results have shown the effect of wormhole attack on the network. this hybrid algorithm will help to prevent wireless mesh network against wormhole attacks and to performance is analyzed by varying no. of wormholes showing consistent results

ACKNOWLEDGEMENT

The author is thankful to Professor Abhay Satmohankar, faculty of Electronics /Electronics and telecommunication for providing necessary guidance to prepare this paper

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, Wireless Mesh networks: A survey, in Computer Networks, IEEE, September 2005, 445-487

[3] 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

BIOGRAPHIES

Miss. Pranita lende is a M.tech student of Electronics branch at Wainganga college of Engineering and Management, Nagpur, Maharashtra, India. She completed B.E in Electronics and Telecommunication branch from smt. Radhikatai pandav college of engineering now renamed SRPCE, from Rashtrasant Tukadoji Maharaj Nagpur University, Maharashtra in 2014. Her areas of interest are communication, Digital Design and image processing.

Prof. Abhay Satmohankar, M.Tech in Communication Electronics(2013), Nagpur B.E. in Electronics and communication (2008), Nagpur Faculty of Electronics and Telecommunication department, Wainganga College of Engineering and Management, Nagpur.