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

***Abstract*-A WMN is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves characteristics of WMN Dynamic self-configuration and self-organization. The nodes in a WMN automatically detect neighbor nodes and establish and maintain network connectivity in an ad hoc fashion. Wireless Mesh Network (WMN) is one of the most vibrant fields of different wireless communication network technologies. WMN can replace wireless infrastructure network. Self-organization, self-configuring and self-healing natures of WMN dynamically provide a solution for high-speed internet access. WMN is highly cost-effective and provides scalability and flexibility. As a result of its open medium nature, distributed architecture and dynamic topology, it is highly prone to a security vulnerability. Wormhole attack is the most vulnerable attack in WMN, where two malicious nodes at different locations establish a tunnel between them and can selectively drop data packets. Passed by. Detection and prevention of wormhole attack are very difficult. In this present work, a hybrid algorithm is proposed that can detect and prevent the wormhole attack and also wormhole link is successfully isolated from the concerned network.**

***Index Terms*- Cryptographic mechanism, Wireless mesh network, Wormhole attack, Cryptographic mechanism, Wormhole detection, WSN**

I. INTRODUCTION

The Recently, several new and marketable applications, such as broadband home networking, community networks, battlefield surveillance, VoIP etc and many others very important wireless technology has become in WMN. Most importantly, wireless broadband service access at minimum cost to provides it helps in WMNs. nodes automatically establish and maintain network connectivity in WMN. e.g., low up-front cost, robust, easy network configuration, and maintenance, reliable network coverage etc. end users the advantages of this feature are many in WMNs.

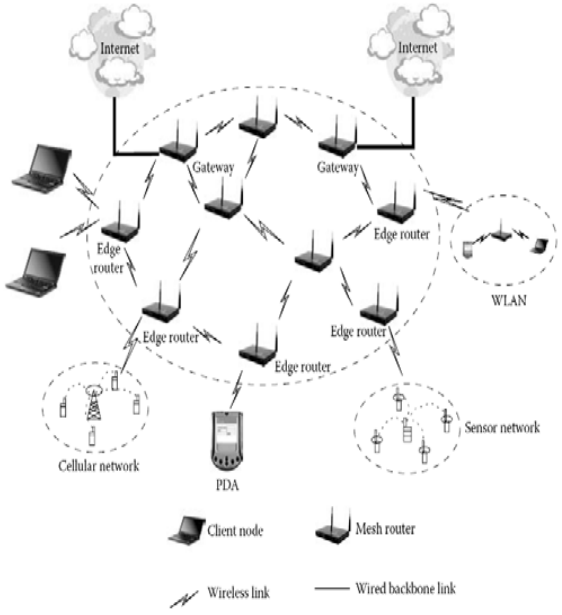

Fig.1.1 A Typical Infrastructure Wireless Mesh Network

The wormhole attack can be launched regardless of the MAC, routing, or cryptographic protocols used in the network and are thus difficult to defend against. Defense mechanisms against this attack are either very complex or very expensive. Most of the wormhole defense mechanisms aim to detect wormholes successfully with minimal false positives.

II. WSN SIMULATOR

Mathematically Modeling the localization problem is virtually impossible and many environmental changes can be simulated such as a channel noise and sensor modes (i.e. wakeup and sleep), and the effect

of these alterations on the model's behavior can be observed. The resulting outputs, valuable insight may be obtained into which variables are most important and how variables interact observing the simulation inputs by changing.

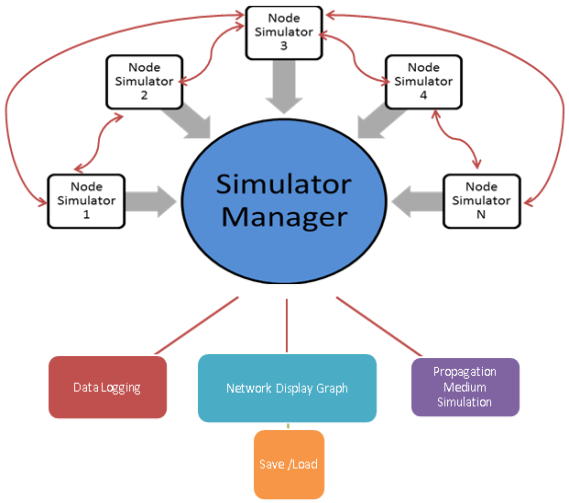

Figure 3.2: WSN Simulator manager

Reconfigured and experimented a simulation is the operation of a system model. too expensive or impractical to do in the system it represents this operation is impossible. properties concerning the behavior of the actual system or its subsystem can be inferred the operation of the model can be studied and henced. existing or proposed, under different configurations of interest and over long periods of real-time simulation is a tool to evaluate the performance of a system in its broadest sense.

III. WORMHOLE ATTACK

The main objectives of deploying the Wireless Sensor Network (WSN) are remote monitoring and gathering information and the A Wireless Sensor Network (WSN) is composed of a group of tiny sensor devices which can be networked together and deployed in a wide spectrum of applications in various military and civil domains.

In this attack, an attacker records a packet orbits of the packet at one location in the network, tunnels the packet to another location, and replays it there. The wormhole attack places the attackers in a very powerful position, allowing them to gain unauthorized access, disrupt routing, or perform a Denial-of-Service (DoS) attack.

IV. DEFINITIONS, STRATEGIES AND EFFECTS OF NETWORK LAYER ATTACKS ON WSN

Attack/Criteria	Attack definition	Attack Effects
Wormhole	A wormhole attack requires two or more adversaries. These adversaries have better communication resources (e.g. power memory) than normal nodes and can establish better communication channels (called ”tunnels”)between them.	• False/forged routing information • Change the network topology • Packet destruction/alteration by wormhole nodes • Changing normal message stream
Sybil	In Sybil attack, a malicious node attacks network traffic by representing multiple identities to the network.	• Confusion and WSN disruption • Enable other Attack • Exploiting the routing race conditions

Wireless mesh networking is used in a layered form.and this a layered architectures of makes these networks vulnerable and to damage against kinds of attacks. Various attacks and their defensive mechanisms are defined and of each layer. Thus, WSNs are vulnerable to different network layer attacks, such as black hole, gray hole, wormhole, sinkhole, selective forwarding, hello flood, acknowledgment spoofing, false routing, packet replication and other attacks to network layer protocols used in this paper.

Now, the following above table shows network layer attacks on WSNs, its classification, and comparison based on their strategies and effects.

V. RESULTS & DISCUSSION

5.1. Deploy Base Station Using Algorithms

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. It consists of 512 nodes and 30 slots.

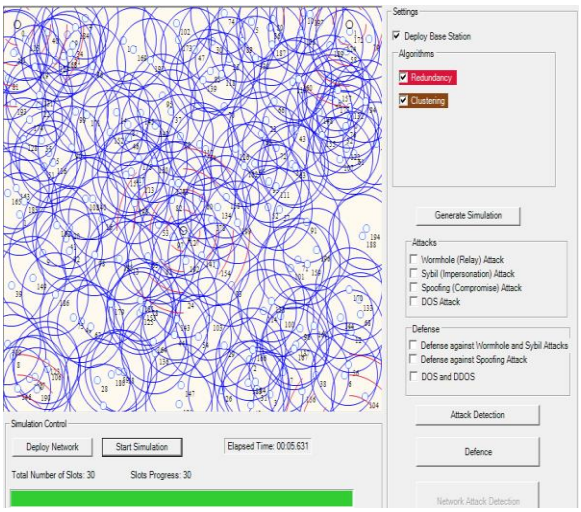

Figure 5.1 Deploy Network

5.2.Create the Trace File

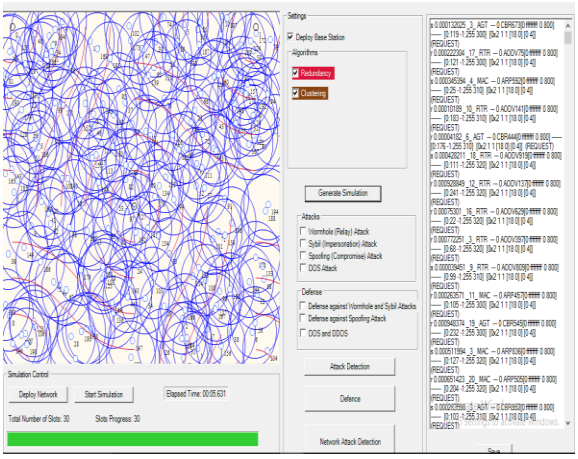

Figure 5.2. Create Trace File

5.3. Attack Detection

Figure 5.3. Attack Detection

5.4 Attack Defence

Figure 5.4 Attack defence

VI. OUTPUT RESULT

To design a hybrid algorithm to detect and eliminate wormhole attack in WMN is performed on WSN localization simulator- Microsoft visual studio. First, if we are deploying the network and create nodes and start simulation using algorithms and After creating the trace file and then attack defense and detection. Import trace file using cryptographic technique MAC used and the node is sender or receiver. Output result shows the time stamp is given duration to send information and Node ID means entry node is having one unique ID and also Three layers are used in this project which is RTR, AGT.

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

6.1 Network Attack Detection

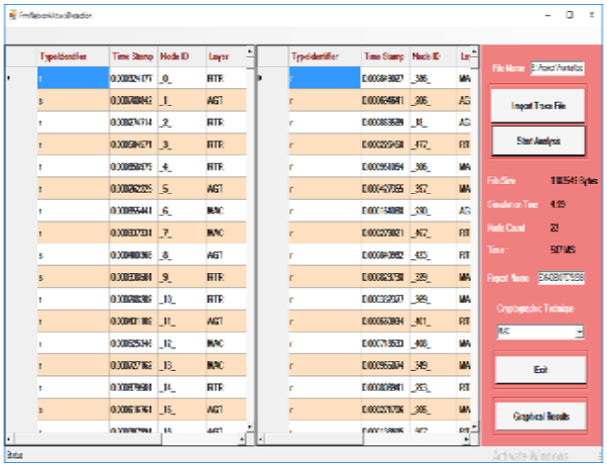

Figure 6.1 Network Attack Detection

VII. GRAPHICAL RESULTS

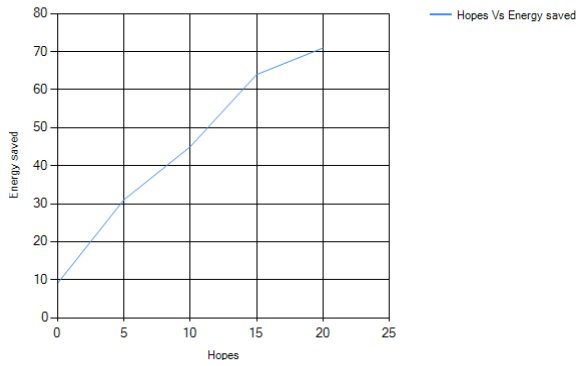

Fig 7.1 Energy save vs hopes

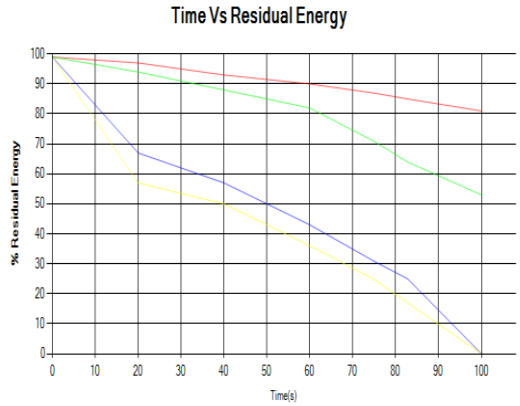

Fig 7.2 Residual Energy vs time

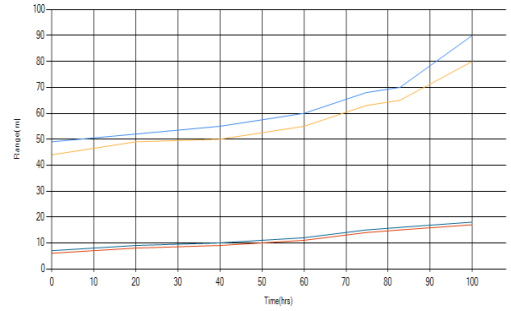

Fig 7.3. Range vs time

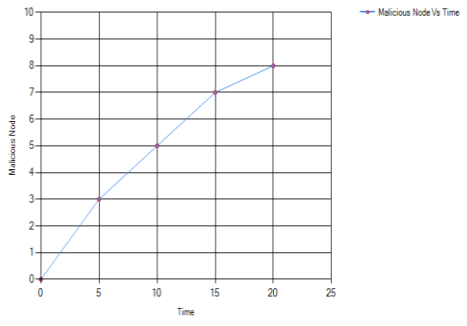

Fig 7.4 Malicious node vs time

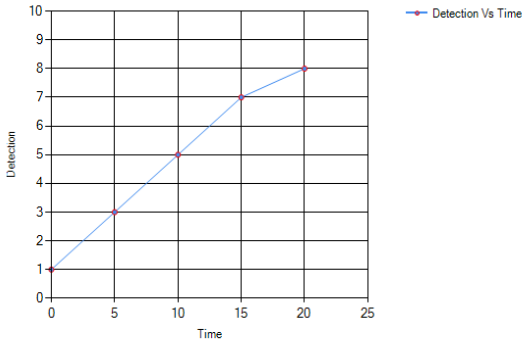

Fig 7.5. Detection vs time

VIII. CONCLUSION

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. The hybrid routing algorithm is used to provide the common solution to three different techniques.

IX. ACKNOWLEDGEMENT

I have been bestowed the privilege of expressing my gratitude to everyone who helped me in completing the dissertation work. The sense of Contentment and elation that accompanies the successful completion of my project and its report would be incomplete without mentioning the names of the people who helped me in accomplishing this work.

I express my sincere gratitude to my guide Prof. Abhay Satmohankar faculty of Electronics /Electronics and telecommunication for his valuable guidance .Without his advice and cooperation I would not have succeeded in my endeavor. His thoughtfulness and understanding were vast and thoroughly helpful in successful completion of my Project.

REFERENCES

[1] Priti Gupta et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4798-4801

[2] Monika / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4516-452

[3] Y. C. Hu, A. Perrig, D. B. Johnson, Packet leashes: A defense against wormhole attacks in wireless networks, in INFOCOM 22th IEEE

[4] 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).
[5] Fayaz ahamed shaikh, uttam patil " Efficient Detection and prevention of Wormhole Attacks in Wireless Mesh Network" IRJET May-2017