

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

Pranita Lende ¹, Abhay Satmohankar ²,

¹Research Scholar, Department of Electronics, Wainganga College of Engineering and Management, Maharashtra, India

²Assistant Professor, Department of Electronics, Wainganga College of Engineering and Management, Maharashtra, India

Abstract - In this paper, we specifically considering any nodes in the network considering Tunneling attack which does not require exploiting and can interfere with the route establishment process. Instead of detecting suspicious routes, which detects the attacker nodes using a hop-count and time delay analysis from the viewpoint of users without any special environment assumptions and works without modification of protocol. The aim of this paper is to explain a wormhole detection algorithm for WMNs which detect the wormholes by calculating neighbor list as well as a directional neighbor list of the source node. The main aim of the algorithm is that it can offer approximate location of nodes and effect of wormhole attack on all nodes which is helpful in implementing countermeasures. The performance evaluation is complete in varying no. 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.

Less maintenance, low price and speedily installable is wireless technology. A number of indoor and outdoor network technologies are designed and according to the need of services. One of the essential technologies among different technologies is Wireless Mesh network. The (WMNs) wireless mesh networks are very valuable because of its self-configuring and self-healing nature. Community networks, cellular mobile networks, and business networks used in WMN.

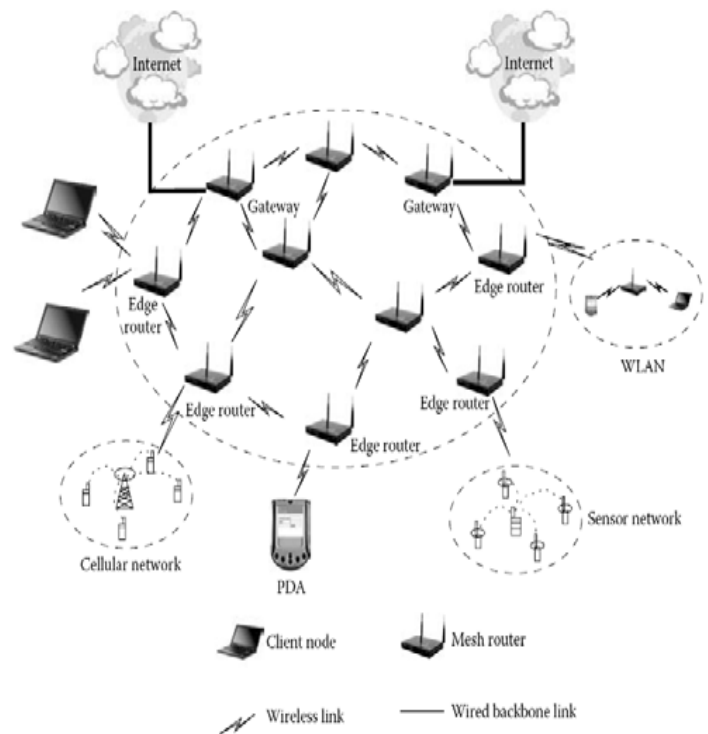


Fig.1.1 A Typical Infrastructure Wireless Mesh Network

Optimistic technology as well as will play an ever more significant part in upcoming invention wireless mobile networks are said to be WMN (Wireless Mesh Networks). Active self-configuration, self-organization, and self-healing by characterized in Wireless Mesh Network. Speedy deployment, low cost, simple maintenance, reliable services, high scalability as well as attractive network facility, connectivity, and flexibility allows in self-healing.

1.1 Overview of WMNs Potential Attacks

A Network failure can cause by various types of attacks and threats in addition to they be able to change, disturb the routing data, updates as well as reduce the performance of the network. This project is supposed to simulate probable wormhole attack against WMNs with the present counter trial against such attacks in a WMN.

To WMNs there are two sources of threats. First, external attackers do not belong to the mesh network can add erroneous information or jam the communication. Second, from internal compromised nodes there are additional harsh threats come since internal attacks are not as simple to stop as external attacks.

The network eavesdrop on the communication of active attacks, the attacker injects as well as into the network modifies packets.

1.2 Aim and Objective of the Project

As the WMN's are deployed in several places and need to be protected from attacks. WMN is vulnerable to many attacks because of the several constraints. Providing security and understanding the attacks in the network is of great need. By using the Mat Lab Simulation program, the attacks can be simulated.

Correct measures to identify and avoid the attacks can be taken by the simulation of the attack can be understood obviously in the attacks.

Wormhole detection in wireless mesh network as well as performance estimation of projected method in the network by varying number of wormholes is the goal is to recommend a method for wormhole detection.

2. Definitions, Strategies and Effects of Network Layer Attacks on WSN:

WSNs are organized in layered form. This layered architecture makes these networks vulnerable and leads to damage against various kinds of attacks. For each layer, various attacks and their defensive mechanisms are defined. 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.

Now, the following table shows the attack, attack definition, and attack effects.

Table -1: Classification 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

3. RESULTS & DISCUSSION

3.1. Deploy Base Station Using Algorithms

To design a hybrid algorithm to detect and eliminate wormhole attack in wireless mesh network 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.

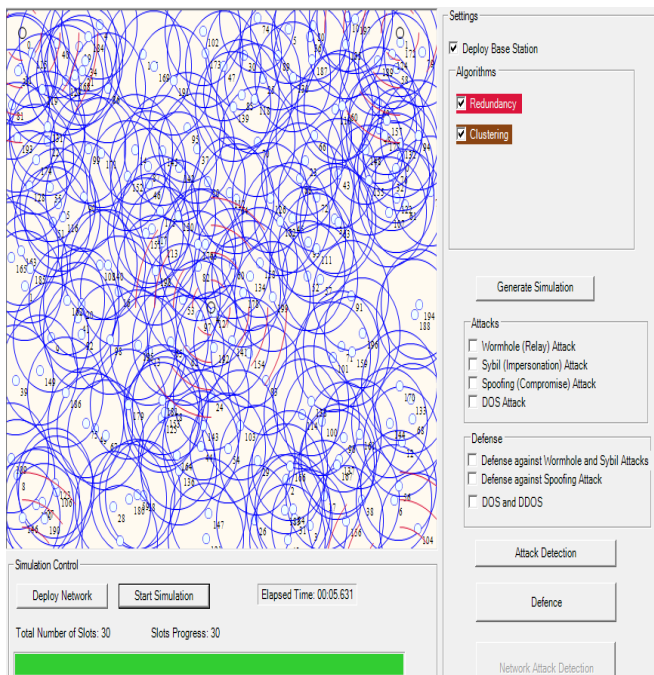


Figure 3.1 Deploy Network

3.2. Create the Trace File

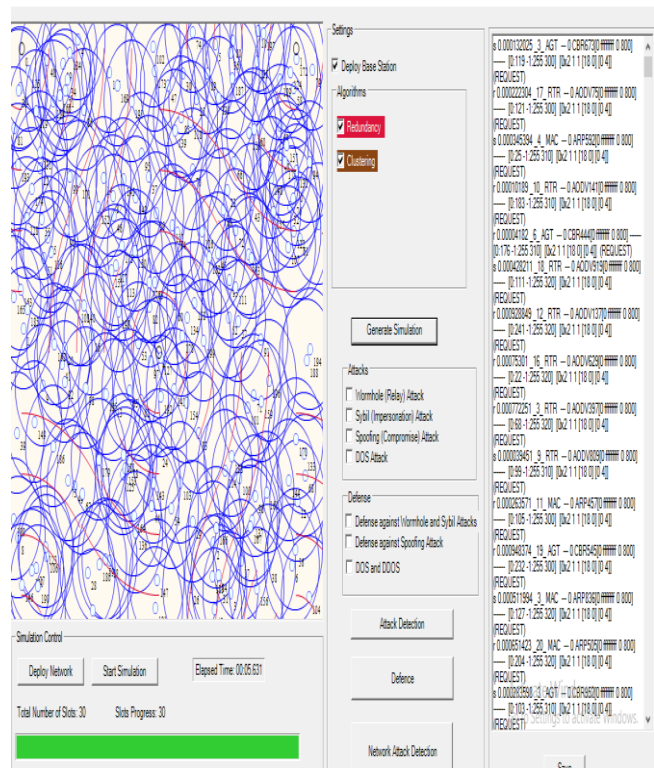


Figure 3.2. Create Trace File

3.3. Attack Detection

Nodes	Attack Type
5	Sybil (Impersonation) Attack
17	Wormhole (Relay) Attack
18	Sybil (Impersonation) Attack
27	Wormhole (Relay) Attack
44	Wormhole (Relay) Attack
58	Wormhole (Relay) Attack
51	Sybil (Impersonation) Attack
58	Wormhole (Relay) Attack
33	Sybil (Impersonation) Attack
94	Wormhole (Relay) Attack
96	Wormhole (Relay) Attack
105	Wormhole (Relay) Attack
108	Wormhole (Relay) Attack
113	Sybil (Impersonation) Attack
113	Sybil (Impersonation) Attack
124	Wormhole (Relay) Attack

Figure 3.3. Attack Detection

3.4 Attack Defence

Total Nodes : 612 Total attacked Nodes : 48 Total Recovered Nodes : 45

Nodes	Attack Type	Nodes	Attack Type
5	Sybil (Impersonation) Attack	5	Sybil (Impersonation) Attack
17	Wormhole (Relay) Attack	17	Wormhole (Relay) Attack
18	Sybil (Impersonation) Attack	18	Sybil (Impersonation) Attack
27	Wormhole (Relay) Attack	27	Wormhole (Relay) Attack
44	Wormhole (Relay) Attack	44	Wormhole (Relay) Attack
58	Wormhole (Relay) Attack	58	Wormhole (Relay) Attack
51	Sybil (Impersonation) Attack	51	Sybil (Impersonation) Attack
58	Wormhole (Relay) Attack	58	Wormhole (Relay) Attack
61	Sybil (Impersonation) Attack	61	Sybil (Impersonation) Attack
66	Wormhole (Relay) Attack	66	Wormhole (Relay) Attack
63	Sybil (Impersonation) Attack	63	Sybil (Impersonation) Attack
94	Wormhole (Relay) Attack	94	Wormhole (Relay) Attack
96	Wormhole (Relay) Attack	96	Wormhole (Relay) Attack
105	Wormhole (Relay) Attack	105	Wormhole (Relay) Attack
108	Wormhole (Relay) Attack	108	Wormhole (Relay) Attack
113	Sybil (Impersonation) Attack	113	Sybil (Impersonation) Attack
113	Sybil (Impersonation) Attack	113	Sybil (Impersonation) Attack
124	Wormhole (Relay) Attack	124	Wormhole (Relay) Attack
129	Sybil (Impersonation) Attack	129	Sybil (Impersonation) Attack
143	Sybil (Impersonation) Attack	143	Sybil (Impersonation) Attack

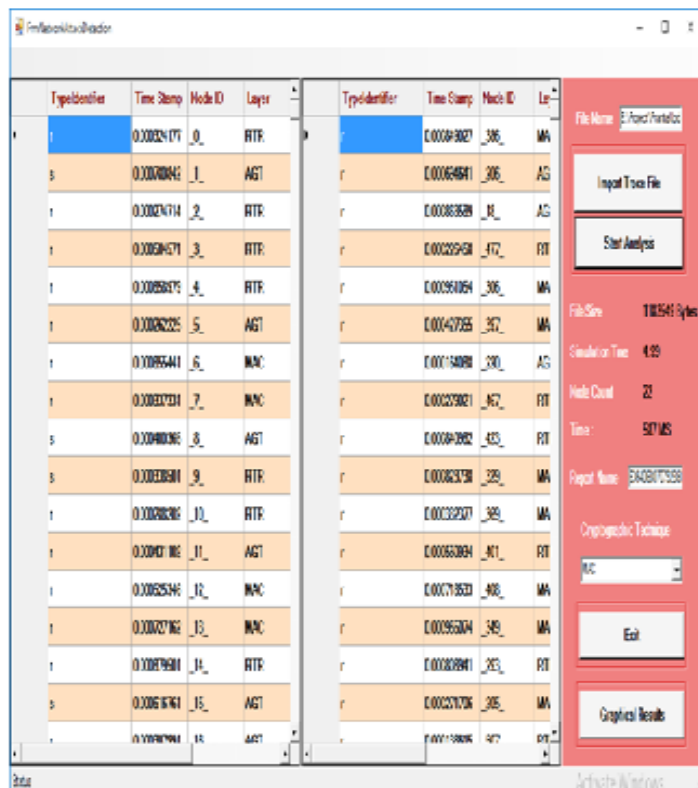
Figure 3.4 Attack defence

4. 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. 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. In output result shows Message ID as a message from each node is denoted by unique ID called message ID and 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

4.1 Network Attack Detection



TypeIdentifier	Time Stamp	Node ID	Layer	TypeIdentifier	Time Stamp	Node ID	Layer
1	0.00024171	0_0	RTR	r	0.00049027	306	MA
s	0.00070842	1_1	AGT	r	0.00064881	306	AG
r	0.00074714	2_2	RTR	r	0.00083629	31_1	AG
r	0.00094571	3_3	RTR	r	0.00022958	472	RTR
r	0.00098375	4_4	RTR	r	0.00091054	306	MA
r	0.00082205	5_5	AGT	r	0.00147325	357	MA
r	0.00095641	6_6	MAC	r	0.00154094	390	AG
r	0.00033734	7_7	MAC	r	0.00233021	467	RTR
s	0.00040336	8_8	AGT	r	0.00042892	433	RTR
s	0.00038384	9_9	RTR	r	0.00082958	329	MA
r	0.00040286	10_10	RTR	r	0.00022927	389	MA
r	0.00071082	11_11	AGT	r	0.00055094	461	RTR
r	0.00055346	12_12	MAC	r	0.00071853	498	MA
r	0.00070786	13_13	MAC	r	0.00095674	349	MA
r	0.00076941	14_14	RTR	r	0.00082881	283	RTR
s	0.00061674	15_15	AGT	r	0.00027076	305	MA
r	0.00040944	16_16	AGT	r	0.00115806	467	AG

Figure 4.1 Network Attack Detection

5. Graphical Results

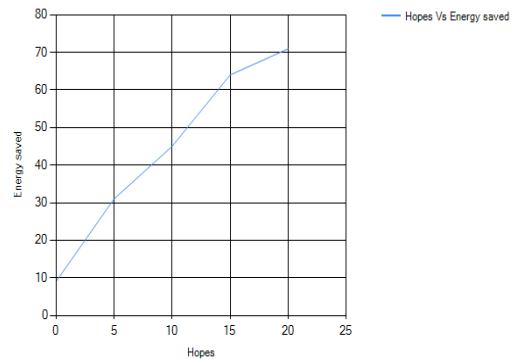


Fig 5.1 Energy save vs hopes

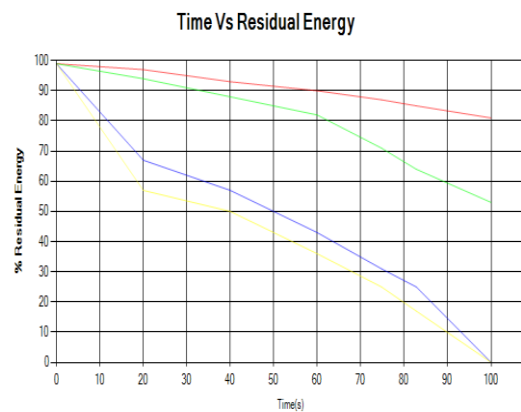


Fig 5.2 Residual Energy vs time

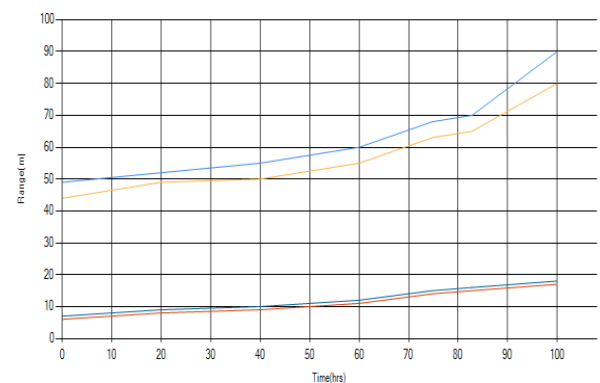


Fig 5.3. Range vs time

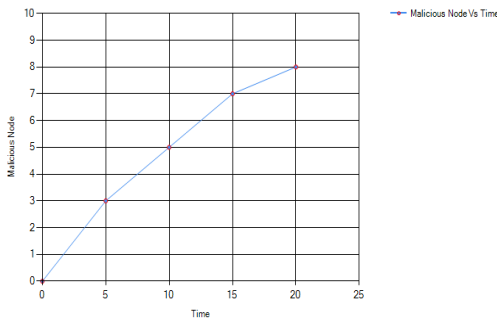


Fig 5.4 Malicious node vs time

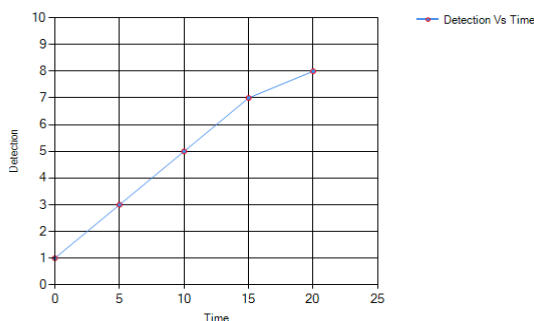


Fig 5.5. Detection vs time

6. CONCLUSION

The wormhole attack is a major setback of wireless sensor technology. Hence, there is an utmost significance of overcoming this problem. The wormhole attack is a powerful attack that is able to have serious consequences on WMN protocols. An attacker who can carry out a victorious wormhole attack can reject service to big segments; disturb routing of a network, creation of unconnected component within a network. 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

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

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.