International Journal of Networks and Applications.
ISSN 0976-5859 Volume 6, Number 1 (2015), pp. 11-18

http://www.irphouse.com

An Evaluation on the Performance of Wireless Sensor Network with Wormhole Attack

N.Sugirtham [1*] and R.Sherine Jenny[2]

[1&2]Department of Electronics and Communication Engineering*
Dr.Mahalingam College of Engineering and Technology, Pollachi.
An autonomous Institution affiliated to Anna University, Chennai.
Email:nsugirtham@gmail.com,sjenny98@gmail.com

Abstract

A Wireless sensor network (WSN) is a fast developing technology which can monitor, calculate and communicate wirelessly thereby finding it's place in areas such as defense, home medical care and environmental sciences which demands better security, throughput, power efficiency and cost effectiveness. WSN's provide endless opportunities and at the same time pose formidable challenges due to the existence of enormous number of sensor nodes which are by default insecure, hence places few challenges on the network. This paper discusses the possible attacks and highlights the inefficiencies when wormhole is introduced in the network. This paper is centered on how the zigbee network performs when an intruder spoofs the information from the communication medium and a comparison is made on the performance of zigbee nodes. Simulations were performed on a tree based network under three different scenarios with and without attack. The entire network performance is simulated through OPNET simulator. The results obtained through inference from the simulation will help us to have a better understanding on the impact of these attacks, thus leading to more secure systems and thereby increasing user's confidence.

Keywords*: - Wireless Sensor Networks, wormhole attack, zigbee,Opnet.*

1 Introduction

A WSN consists of wireless sensors, which are capable of collecting, storing, processing and sharing information with neighboring nodes. Zigbee is a specification for a suite of high-level communication protocols used to create personal area networks built from small, low-power digital radios based on IEEE802.15.4 standard. It supports protocols above the data link layer for connecting IEEE 802.15.4 devices

together. Zigbee is the name for a short-range, low-power, low-cost, low-data-rate wireless multi-hop networking technology standard [2]. The features of Zigbee networks include self-organization, support for multi-hop routed networking topologies, interoperable application profiles, and security based on the Advanced Encryption Standard (AES). Zigbee standard defines the higher-level Network and Application layers as well as the security services. The Security Services Provider establishes the trust infrastructure of the network and offers essential security services such as cryptographic key management and admission control for nodes joining the network. Enabling security incorporates an authentication step to the joining process. Network layer provides reliable and secure transmissions among devices [1]. This paper begins with the role that Zigbee protocol plays in the secured deployment of ZigBee networks using a tree based approach. The following section describes the technical overview on the scenarios included in the paper. Finally, a section that discusses about the impact of wormhole attack on the network including various parameters for the purpose of analysis. A concluding section summarizes key points and is followed by a list of technical references related to the topics presented in this document.

2 Technology Overview

The primary components that comprise a Zigbee network are Zigbee Coordinator also referred as PAN Coordinator which is capable of assigning device address and controlling PAN formation and operation, Zigbee Router that is capable of establishing and maintaining multiple connections to children and parent nodes, Zigbee End Device (ZED) and a Zigbee Gateway that serves as a bridge between a Zigbee network and a wired Ethernet network. An end device can be an Reduced Function Device (RFD) or Full function Device (FFD) but is a leaf node in the network and does not perform any of the other Zigbee device functions of router, coordinator, trust center, or gateway [2]. The number and type of each device in a Zigbee network will vary depending on the size, complexity, and type of applications supported. Zigbee Routers forward packets in a simplified routing scheme among their parent and child nodes. The Zigbee Network Layer supports the formation of three types of topologies namely Star, Peer-To-Peer and tree. Here in this paper we have chosen a tree based approach taking into consideration the low routing cost, ability to collect data quickly [7] and allows multihop communication.

A Tree network consists of a central node called the coordinator that initializes the network, and is the top (root) of the tree. The coordinator can have either routers or end devices connected to it as shown in figure 1. Router helps in extending the network coverage. For every router connected, there is a possibility for connection of more child nodes to each router. Child nodes cannot connect to end devices as it does not have the ability to relay messages. This topology allows different levels of nodes, with the coordinator being at the highest level. In order the messages to be passed to other nodes in the same network, the source node must pass the messages to its parent, and is continually relayed higher up in the tree until it is passed back down to the destination node.

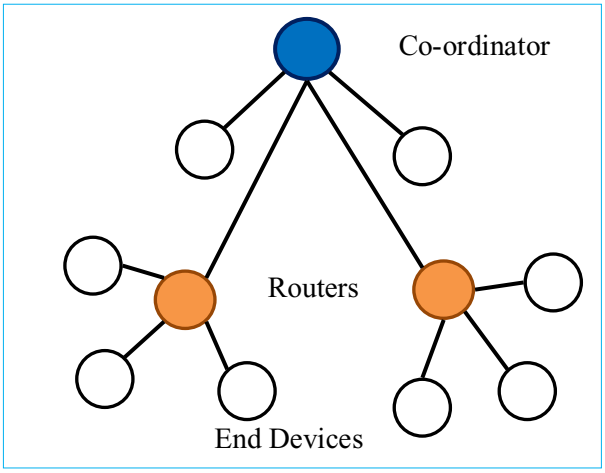

Figure 1: Tree Topology

3 Attacks on Wireless Sensor Network

In networks an attack is an unauthorized attempt to alter, destroy or steal the content of a user. It is a threat which uses different techniques to deceive the security mechanisms intelligently. Attacks in Wireless Sensor networks are classified as active and passive attack. Modification of data in the communication channel by unauthorized intruder is classified as active attack. Major attacks that come under active attack are Denial of service, Sink Hole, Worm Hole, Sybil etc... Passive attacks are ubiquitous in nature where the intruder monitors and listens to the network traffic to gather information. Some examples of passive attack are traffic analysis, network analysis, and eavesdropping [4].Our paper explores the effect of wormhole attack and studies the behaviour under different parameters using simulation software. Wormhole attack is one of the most severe attacks in WSN where two or more malicious nodes combine and form a low latency channel between them as shown in figure 2. As this channel is of low latency nodes try to send the packets through this channel [5].

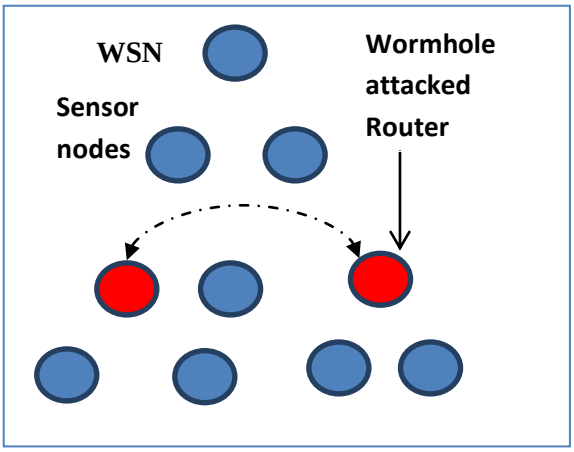

Figure 2: Wormhole attacked router placed in between normal sensor nodes

Wormhole attack is very difficult to detect as they use a separate band which is invisible to WSN [6]. A node that is attacked by a wormhole is termed as malicious node and such nodes transfer the packets to other nodes by encapsulation or through a wired medium or through a directional antenna [3]. Wormhole attack possibly works in two modes, hidden mode and participation mode. In hidden mode, it can be launched even if the network maintains high confidentiality and authentication. Here the malicious node will not modify the routing information instead it forwards them through the channel. In participation mode it is difficult to launch as it needs to modify the routing packets. Once launched it is very difficult to detect this attack as they simply ignore all the security mechanisms employed [8, 10]. Here in our scenario we have assumed the malicious node to be bidirectional in functionality.

4 Simulation and Results

This section describes the different scenarios, attributes and parameters used for simulation. This paper mainly focuses on the impact of the wormhole attack on a Zigbee network. In order to study the effects of this attack on a WSN, simulation is carried out using Opnet-Riverbed Modeler academic edition 17.5. We have considered three different scenarios for the purpose of analysis and compilation. The three scenarios being normal operations without attack, wormhole attack without mobility and wormhole attack with mobility. The reason for simulating scenario-1 where no malicious node is used is to identify the state of the network under normal conditions and to use the data to compare and differentiate the impact of wormhole attacks on the network. Wormhole attack is introduced by proper modification in the scenario -1 as shown in figure-3. Global Parameters that are chosen for the analysis are data dropped, delay, load and the nodal parameter is traffic received at the routers. Table 1 below shows the detailed information about scenario parameters.

Table 1: Simulation Parameters for the Scenario

Simulation Parameter	**Value**
Scale	Office
Size	100m*100m
Model Family	Zigbee
PAN ID	Auto assigned
Trajectory	X clock_circle_south
Simulation Time	One hour
Application Traffic for Coordinator, End device and Router	
Destination	Random
Packet Interval Time	Constant(1,0)
Packet Size	Constant(1024)
Start Time	Uniform(20,21)
Stop Time	Infinity

The sample shown in figure 3 is the scenario for an attacker with a trajectory. The duration for which the simulation is carried out is 1 hour. For a better clarity graph, around 15 values are considered. The following observations were made for the global parameters.

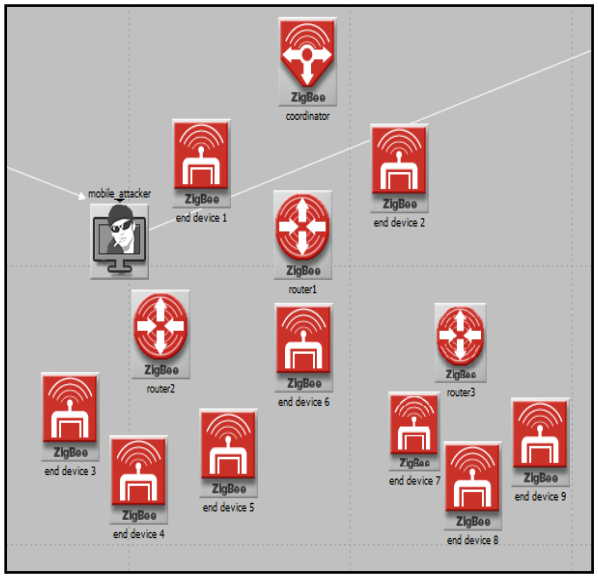

Figure 3: Scenario - 3 that includes a mobile attacker with trajectory

Data Dropped: It is the average number of packets dropped by the MAC layer due to failure in transmissions or retransmission of packets. This statistics also reports the outstanding packets in the buffers that are dropped during roaming as shown in Figure 4.

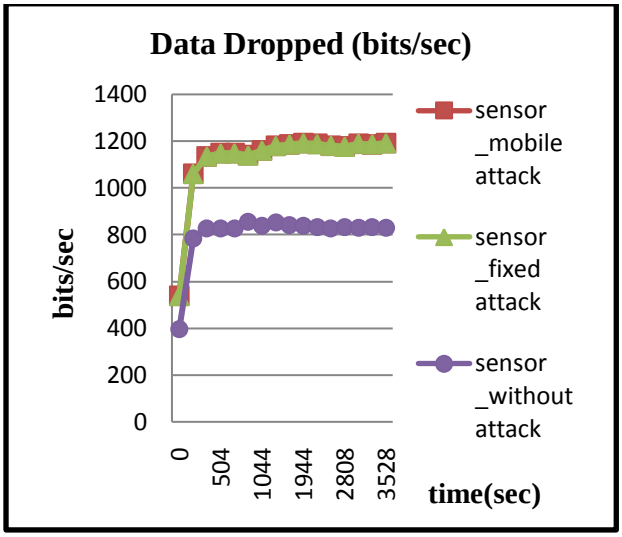

Figure 4: The curve of data dropped during mobile attack, fixed attack and without attack on the network

Delay: This represents the end to end delay of all the packets received by the 802.15.4 MACs of all WPAN nodes in the network and forwarded to the higher layer. Lower the value of end-to-end delay better is the network performance [9].

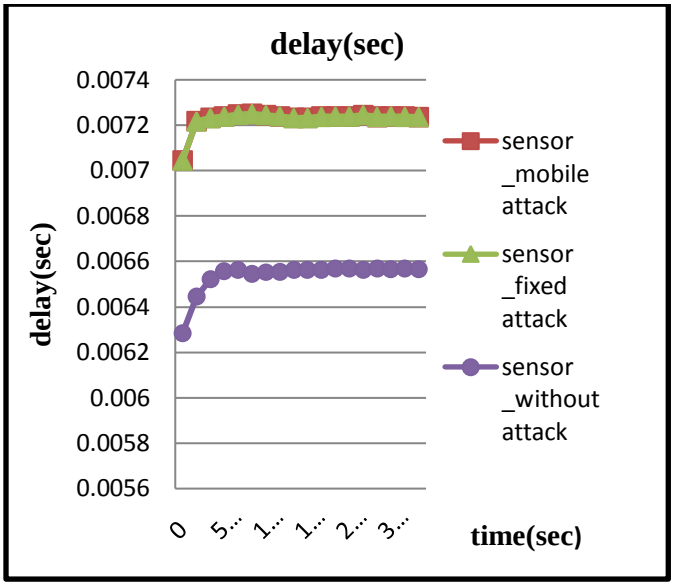

Figure 5: The curve of delay produced in the network during different conditions imposed on the router

It is clear from figure 5 that the WSN without attack experiences an end to end delay of 0.0066 Sec and with attack it is increased to 0.0072.

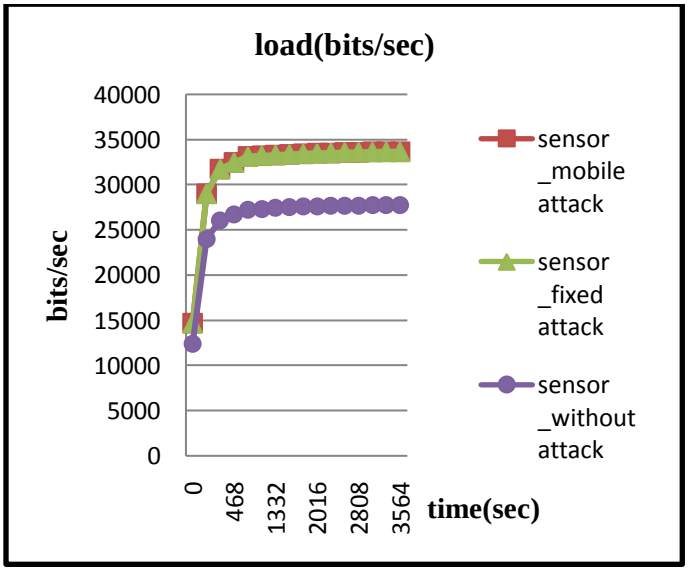

Figure 6: Curve obtained with respect to the load

Load: This represents the total load (in bits/sec) submitted to 802.15.4 MAC by all higher layers in all WPAN nodes of the network .It is observed that the network load is more during the attacks and is getting reduced during normal operation. Figure 6 shows the curve obtained with respect to the load that a network can handle when the router includes an attacker, a mobile attacker and with no attack. However in spite of the nature of an attacker the load is found to be the same in both the cases.

The nodal parameter, traffic received by the routers is observed. Here the behavior of the three routers is studied.

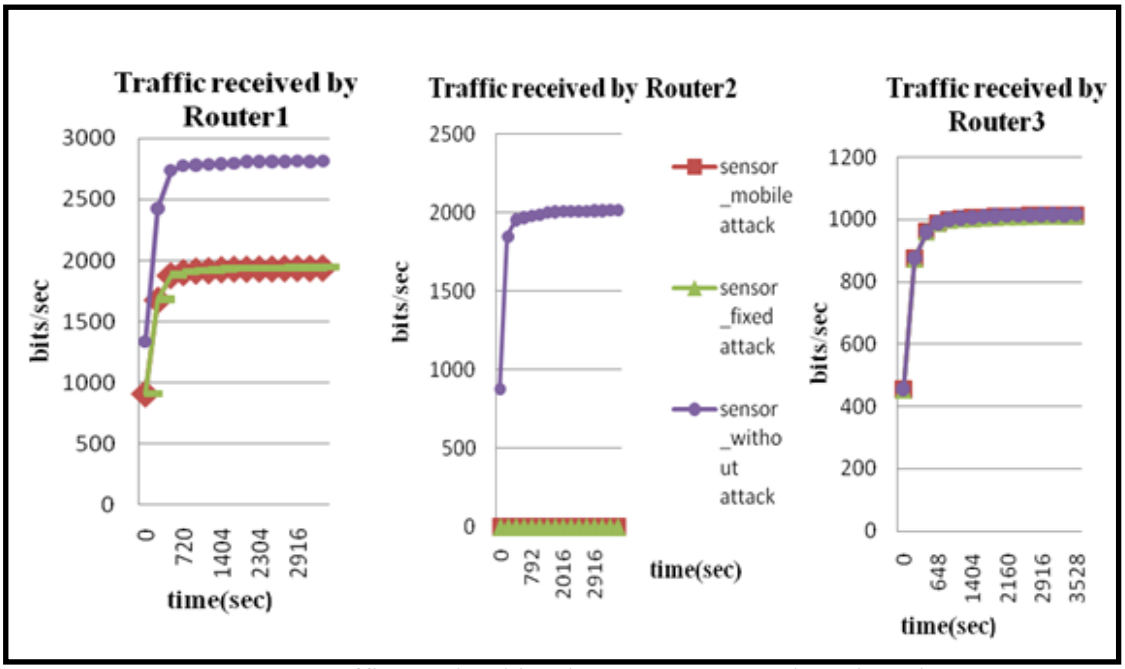

Figure 7: Traffic received by the router 1, 2, and 3 when the attacker is fixed, mobile and without attack

The disruption in traffic is inversely proportional to the distance between the location of the attacker and the router, (i.e.) less the distance between the attacker and the router more the impact and vice-versa. In Figure 3 the attacker is situated nearer to router-2 hence the traffic received is next to zero, where as the router -3 situated a further distance has no or minimal impact hence the traffic does not show any significant change.

5 Conclusions

Wormhole attack is a prominent attack that forms a serious threat in a wireless Network. Detecting and eliminating such an attack is a very challenging task till now. It is to be noted that the results obtained and analyzed here are specific to particular scenarios. On analyzing the simulation results it is observed that the average end to end delay in the scenario with attack is increased by 9%. Similarly the data dropped also shows a significant increase of 50%. From the simulation results it is evident that the performance of the sensor network under study with wormhole attack is getting

degraded. It is obvious that the load offered on the network with an attacker is more compared to the network without an attacker. Router-2 which is in close proximity to the attacker receives very low traffic which is almost zero. The above conclusion is clear from the simulated results.

References:

[1] Adrian Perrig, John Stankovic, and David Wagner, "Security in wireless sensor network.", Communications of the ACM, Vol.47, No.6, June 2004, pp.53-57.

[2] Boris Mihajlov and Mitko Bogdanoski "Overview and Analysis of the Performances of ZigBee based Wireless Sensor Networks' International Journal of Computer Applications (0975 – 8887) ,Volume 29– No.12, September 2011,pp.28-35.

[3] Er. Gurjot Singh, Er. Gurpreet Kaur, "Analyzing the Impact of Wormhole Attack on Routing Protocol in Wireless Sensor Network on Behalf of packet tunnel, dropped and intercepted", International Journal of Engineering Development and Research, ISSN: 2321-9939,Vol.1,No.1, 2013,pp.42- 48.

[4] Hong-Ning Dai, QiuWang, Dong Li,1 and Raymond Chi-Wing Wong ,"Research Article On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas" Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, 2013, Article ID 760834,13 pages.

[5] Huang Wen hua, "Research on Security of Routing Protocols Against Wormhole Attack in the Ad hoc Networks" WSEAS Transactions on Computers, E-ISSN: 2224-2872, Vol.12, Issue 6, June 2013,pp.255-264.

6] Lukman Sharif and Munir Ahmed, "The Wormhole Routing Attack in Wireless Sensor Networks (WSN)", Journal of Information Processing Systems, Vol. 6, No. 2, 2010, pp.177-184.

[7] Ozlem Durmaz Incel, Amitabha Ghosh, Bhaskar Krishnamachari, and Krishnakant Chintalapudi, "Fast data collection in tree-based wireless sensor networks", IEEE Transactions on Mobile Computing, Vol.11, No.1, 2012, pp.86-99.

[8] Reshmi Maulik and Nabendu Chaki ," A Study on Wormhole Attacks in MANET",International Journal of Computer Information Systems and Industrial Management Applications, ISSN 2150-7988, Vol.3 , 2011, pp. 271-279.

[9] R.Sherine Jenny, N.Sugirtham, "Simulation based performance comparison of AODV, DSR, FSR routing protocol with wormhole attack", International Journal of Computer Networks and Wireless Communications,ISSN: 2250-3501 Vol.3, No.1, February 2013,pp.45-49.

[10] Susheel Kumar, Vishal Pahal , Sachin Garg, " Wormhole attack in Mobile Ad Hoc Networks: A Review" IRACST – Engineering Science and Technology: An International Journal (ESTIJ), ISSN: 2250-3498,Vol.2, No. 2, April 2012, pp.268-275.