

Exploring Impacts of Random Proactive Jamming Attack in Wireless Sensor Network

Ali Mohammed Hussen*

*Department of Information Technology, Collage of informatics, Werabe University; P.O.Box 46, Werabe;
Ethiopia*

Email: ali.mohammed324@gmail.com

Abstract

Wireless Sensor networks are one of the most extensively used technologies in our day to day lives; they can provide communication without needing a fixed infrastructure, which makes them suitable for communication in disaster areas or when quick deployment is needed. However, this kinds of network technology uses the wireless medium for communication. It is vulnerable to malicious attacks. One of the most frequently used attacks is a random jamming attacks which is Denial of Service attack. Random Jamming attacks disturb the communication between Sink and legitimate nodes. In rough environments where there is constant traffic, Random jamming attack can cause serious problems. Because of this, a study of random jamming attacks and how to prevent them is necessary. In this research the random jamming attacks were simulated using Riverbed Modeler software, in order to provide a better understanding of effects of random jamming attacks. This study will be helpful for future research and development of a practical, effective way to avoid random jamming attacks. The objectives of this thesis were to simulate and analysis wireless sensor network (ZigBee) under random jamming attacks; launch different kinds of (fixed, mobile) random jamming attacks in order to test how much influence on performance of wireless sensor network. Riverbed Modeler Based simulation which have five scenarios were created and the simulation was run and the results were collected, which shows that the throughput of the wireless sensor network decrease and increase the delay ,data drop when the network is affected by the random Jammers. Finally, thesis describe the open issues in this field, such as adding more than one random jammer and sink in wireless sensor network.

Keywords: Wireless Sensor Network; Jamming attacks; Random Jammer; Jamming Detection; Jamming Isolation.

* Corresponding author.

1. Introduction

In Wireless Sensor Network (WSN), the radio communication ranges were restricted to small areas dictated by the transmission power of a central authority called the Base Station (BS). The BS also had the responsibility of controlling all the activity in the network and often required a fixed infrastructure. Wireless Sensor networks emerged as a possible alternative for scenarios where a fixed infrastructure does not exist and the environment is not suitable to build a fixed network. Wireless Sensor network is a kind of network that is easily deployed; the nodes only need to enter each other's radio range; this is particularly important for communication in disaster environment. WSNs are a particular type of ad hoc networks, which consist of large number of deployed sensor nodes with limited resources and one or more base stations (BSs) or sink, typically serves as the access point for the user or as a gateway to another network. Nodes can collect and transmit environmental data (temperature, pressure, humidity, noise levels, etc.) in autonomous manner. The node in WSN plays two roles: collect data and route data back to the base station [1]. WSNs are vulnerable to various kinds of attacks because of its use shared medium and install in open environments. Security is big issues in different application areas of WSNs. So, it requires to deal with numerous security issues especially jamming attacks. Some of the common jamming attacks in WSNs are: Constant, Reactive, Deceptive, and Random. Random jamming attack, this type of attack which is categorized under proactive jamming attacks. Attackers with a transceiver can be able to hinder wireless transmission, insert unwanted messages, or jam messages of high importance. This kind of attack known as random jamming attacks. Random jamming can be considered as one of the fundamental ways of degrading network performance and totally blocks packet transmission. In Random jamming, the attacker corrupts the content of the original message by transmitting radio frequency signals in the network or by blocking the message so that it cannot be able to reach to the intended destination. Random jamming causes many problems for real world applications. For example, in border security, an intruder can jam the communication and cross the border without being detected. Thus, in hostile environments, it is essential to be able to detect the place where the channel is jammed or deliver the messages out of the jammed area [2]. In Random jamming attack, the jammer alternates between periods of continuous jamming and inactivity. After jamming for t_1 units of time, it stops emitting radio signals and enters into sleep mode. This type of jamming attacks highly affect the performance of WSN. There are many researches which are focused on reactive jamming attacks in the last 10 years, but in this thesis concentrate on random jamming attacks. This thesis mainly focuses on random jamming attack types. This kind of attack prevents genuine users from accessing the channel or by disrupting the communication between a sender and a receiver. Nowadays random jamming attack is a serious problem for many users and organizations. Random jamming attacks affect the performance of WSN in the sense that they disturb all kinds of information exchange. This problem remains an open problem in the WSN communications field. This is the reason why this research focuses on the exploration of the level of impact of random jamming attacks on WSN. Security problems are something that cannot be eradicated completely. So, it is necessary to understand the level of impact of fixed random jammer and mobile jammers in WSN to design a well-structured prevention mechanism because 50% of the solution is clearly identifying the level of impact/problems.

2. Literature Review

Literature review is a research method that is mainly intended to identify the literature that is relevant to a

particular research area and to gather the information such as the extent to which the research was conducted, the dominant research gap in the area and the scope of the current research topic. It also acts as a standard for a comparison between the intended research study and other studies. It helps in defining a benchmark for identifying the contributions of remaining authors in the research area. With the development of the internet, security has more important aspect in network area. In WSN, security is the one of the essential and the serious aspect. Because the broadcast nature of the communication and the sensing tiny device that is called sensor node [52].Sensors node have some constraint such as lack of processing power, small storage area, lack of lifetime and too much energy consumption [44]. WSN are used in many applications and in some applications, security negotiations may lead to threat to national security, commercial lose [7]. WSNs use radio frequency (share medium) for communication between sensors and sink nodes, this is by default a shared medium, in this environment security becomes a serious issue [8]. There are different kinds of attacks against WSN, among them jamming attacks are the most common and widely used attacks that threaten WSNs. Jamming attacks are relatively cheap and easy to implement than other attack types [9]. Compromise of the secure information by an enemy is an act that cannot be neglected. Hence, appropriate security measures need to be taken at every layer of a protocol design. Many attacks are caused by intruders who have complete knowledge of the protocol. There has been 8 research on the different kinds of possible DoS attacks on sensor network especially reactive jamming attacks. In [14] the researcher represented a very important mapping service to detect jamming attacks. Jamming Area Mapping is a service that provides quick and accurate jamming attack response, which alerts the WSN for a possible jamming attack in effect. As geographic information is imperative for WSNs, knowing where exactly the jamming is and what sensors does it effect, certainly will help in modifying its effects. Random jammers often, attack specific areas like sink or sensor nodes. Finding where the jamming are coming from and what sensors are currently cut-off, is very essential in the next step which is avoiding or challenging the jammer. The authors advised that cost of other solutions like spread spectrum techniques [15] is high, and only practical in military WSN, were security compromise is not an option. Wood and his colleagues in [11] had brief identify different kinds DoS attack and its effect on the wireless sensor network. However no defense mechanism is proposed in this survey but different possibilities to reduce the attacks are given. In the physical layer, using spread spectrum is often used to reduce jammer attacks because this technique used to resist smart jammer, example reactive jammer. This paper concludes that due to the limited resources code spread as used in mobile networks cannot be used in WSN. Generally in this paper author did not mention which kinds of jamming attack highly affect the performance WSN and it is not clearly show which parameters are used in order to measure its effects. Ramya Shivanagu et in [22] had clearly discuss its application and security. Among different types of threats, Jamming attack has been considered a severe security threat. These jamming attacks cause the overutilization of scarce resources like the battery power. Further, high computations require lot of memory. Such problems cause the reduction in the lifetime of the sensor nodes in WSNs. There are four types of jamming attacks in which the most difficult type of attack is the reactive jammer as it is easy to launch by the adversary but very difficult to detect and defend. In this paper author present a brief survey of kinds of jamming attacks, methods used to detect and defend the jammers. the big issues which is not covered in thesis is amount of each jamming attacks impact level on WSN performance and did not mention about mobile/fixed jammer effects on WSN in the form of delay , data drop and throughput. Thamilarasu and his colleagues [20]: improve Reliability of Jamming Attack Detection in Ad Hoc Network

using the GloMoSim network simulator and CBR application simulation framework. For simulation purpose authors had taken few metrics like Detection Rate, False Positive Rate. Effects of Jamming at Physical and MAC layers in a wireless ad hoc network and presented a detection algorithm to reliably detect jamming attacks are not different from collision due to hidden terminal and network congestion. For improving Detection accuracy utilized the channel utilization metric for evaluating network congestion state and performed tests to find out collision is due to jamming or network traffic conditions. After the simulation result authors conclude the effectiveness of scheme and also demonstrated that it can be used to detect attack with enhanced reliability and accuracy. Ajana J. and his colleagues [23]: mitigate inside jammers in MANET using Localized Detection Scheme. For performance evaluation author's had taken NS2 Simulation tool for simulation purpose with taking various parameters such as 200 by 200 meters grid size, 10 nodes, simulation time 200 sec. , antenna Omni-directional with unity gain, No fading radio model with range of 376 meters, routing protocol.

3. Methodologies

In this chapter the way the experiment was designed is explained. It starts by stating the required tools for this research, discussing WSN Simulation parameters and explanation of steps that are required to design in each layouts. Later in each section the layouts for each of the scenarios is shown including a description of each of them.

3.1 Software and Hardware tools used

In this research, Riverbed Modeler Academic Edition 17.5 was used as the simulation tool. Riverbed Modeler Academic Edition 17.5 is broad and very powerful simulation software with large variety of possibilities. The whole different networks with several jamming attacks can be modeled utilizing Riverbed Modeler Academic Edition 17.5. High level of user interface is employed in Riverbed Modeler Academic Edition 17.5 which is made from C and C++ source code blocks. The simulation concentrates on evaluate of WSNs performance with and without random (fixed and mobile) jamming attack. Thus an Integrated method is utilized to analysis the network performance under jamming attack. This method involves: Sensor, sink and jammer nodes may or may not change their locations after deployment, High data rate of 1024bit/sec and all the nodes have limited supply of energy.

3.2 Simulation Parameter

In order to evaluate a network performance, important parameters were used for analysis. Including throughput, delay, and data dropped. Following important parameters used in this thesis are presented for a better understanding of this thesis.

Table 1: WSN Simulation Parameters

Parameters	Value
Number of end device	20
Simulation Area	60*60 Meter
Simulation Time	1200 seconds
Data rate	Auto calculate
Performance Parameters	Throughput, Delay and data drop
Frequency band	2450 MHZ
No. of coordinator(Sink)	1
Traffic destination	coordinator
No. of retransmissions	5
Packet size	Constant (1024)
ACK wait duration	0.05
Packet interval time	Constant(1.0)
Mobility type	Fixed/mobile
ACK status	Enable
Transmit Power	0.005

Throughput

Throughput (bits/sec) of a network or device is the total amount of data traffic that was successfully received and forwarded to the higher layer by the IEEE 802.15.4 Media Access Control (MAC). It is the rate of successful message delivery of the network communication channel. For example, assume two nodes are transmitting data in a network. If the average data delivery in this network is 100 bits/sec, the throughput of the network is 100 bits/sec.

Delay

Delay (sec) represents the end-to-end delay of all the data packets that are successfully received by the IEEE 802.15.4 MAC and forwarded to the higher layer. This delay includes the delays at the source, reception of all the individual fragments.

Data dropped

Data dropped (bits/sec) is the data traffic in higher layer dropped by the IEEE 802.15.4 MAC due to consistently failing retransmissions. This statistic reports the number of the higher layer packets that are dropped because the MAC cannot receive any ACKs of those packets or their fragments for the retransmissions. In this simulation experiment, five different scenarios are will be generate and illustrated by the Riverbed Modeler Academic Edition 17.5 simulation package and flow of the scenarios have been shown in each figures.

3.3 Simulation procedures

In this thesis, Riverbed Modeler Academic Edition 17.5 simulation scenario can be basically divided into two groups:

A) Scenarios of WSN without random jamming attacks Simulation have the following steps:

1. Create WSN Scenario 60*60 meter width on Riverbed Modeler Academic Edition 17.5 software
2. Initialize No. of Nodes (20 sensor nodes)
3. Apply Simulation Statistics for 1200sec on each scenarios
4. Formation of Cluster
5. Run and Record the behavior (values) each parameters
6. Analyze Result of Throughput, delay and data dropped
7. Stop Simulations

B) Scenarios of WSN with random (fixed and mobile) jamming attacks Simulation have the following steps:

1. Design WSN Scenario 60*60 meter width on Riverbed Modeler Academic Edition 17.5 software using 20 sensor nodes
2. Apply Simulation Statistics 1200sec
3. Run and Analyze Results
4. Compare Results with Normal Scenario
5. Is performance is too much degrade?
6. There is movable Random Jamming Attacks on WSN

Or if the performance is small amount of degrade?

7. There is fixed Random Jamming Attacks on WSN
8. Else there is no fixed or mobile Random Jamming Attacks on WSN
9. Stop Simulations

For this study for measure the effect of random jamming attacks on WSN the research will use average of 10 sample size on 120 sec time interval

3.4.1 Scenario 1 :(Fixed Sensor, Sink node without Random jammer node)

Scenario 1 :(Fixed Sensor, Sink node without Random jammer node) simulates the simplest of the WSN without Random jamming attacks. This scenario consists of a number of transmitter (sensor node) sending valid traffic to a receiver (Sink). This scenario consists of number of wireless stations this scenario shown in Figure 2.

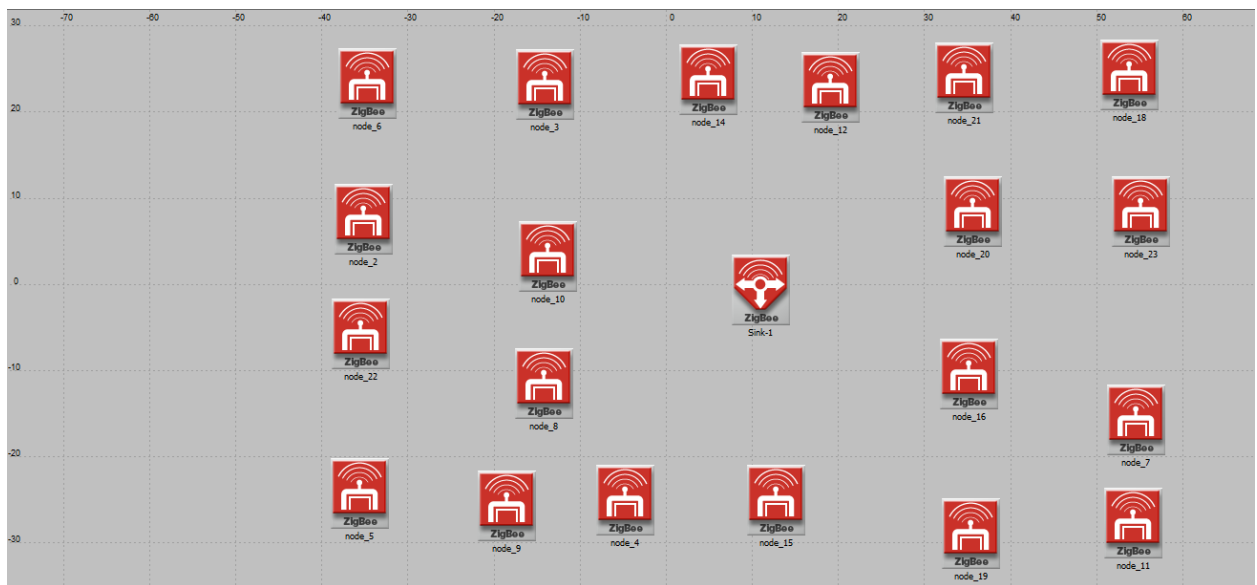


Figure 2: Scenario 1 (Fixed Sensor, Sink node without Random jammer node) layout

In Figure 2 it is shown that the Sink nodes receive packets with a constant length of 1024 bits at a constant rate of 1 packet per second. When those packets arrive at the wireless modulator they are converted into a suitable form to be transmitted by the antenna at a rate of 1024 bps with a transmission power of 0.05 watts ,number of transmission will be 5 ,and transmission band 2450MHZ. The wireless modulator also specifies that the modulation scheme is ‘zigbee_coordinator’ and all the processes that will apply to that packet.

3.4.2 Scenario 2: (Fixed Sensor, Sink and Random jammer node)

Scenario 2 is a variation of Scenario 1 .While there is no a random jammer is used in Scenario 1. in Scenario 2 a

random jammer (also known as pulse jammer) is used. For this thesis, the pulse jammer was *modified* to jam for a random period of time and sleep for another random period of time instead of using fixed periods as is done in the default OPNET model. One fixed pulsed Jammers named (jam_pulsed) added to Scenario 2 as shown in Figure 5. No. of wireless stations= 20, No. of Jammers = 1 and No. of coordinator = 1.

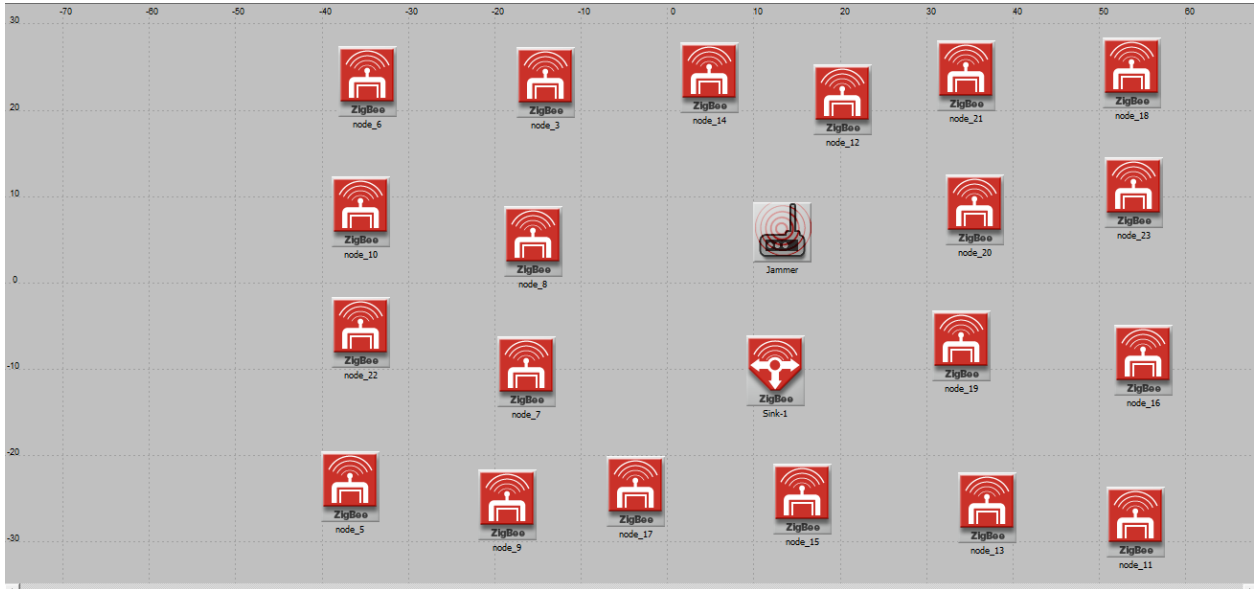


Figure 5: Scenario 2 layout

In Figure 5 it is shown that the jammer sends jamming packets with a constant length of 1024 bits at a constant rate of 1 packet per second. When those packets arrive at the wireless modulator they are converted into a suitable form to be transmitted by the antenna at a rate of 1024 bps with a power of 0.05 watts. The wireless modulator also specifies that the modulation scheme is '*jam_pulsed*' and all the processes that will apply to that packet.

3.4.3 Scenario 3 layout (mobile sensor, sink and random jammer)

Scenario 3 simulates the simplest of the WSN with mobile Random jamming attacks. This nodes consists of a number of transmitter (End device) sending valid traffic to a receiver (Sink). This scenario consists of number of mobile wireless stations this scenario shown in Figure 6. No. of wireless stations= 18, one Coordinator (sink-1) and one jammer.

The simulation setup is as follows:

The scenario has a size of 60×60 meters, which is the average coverage provided by Sink using the standard IEEE 802.15.4 and simulation time is 20 minutes.

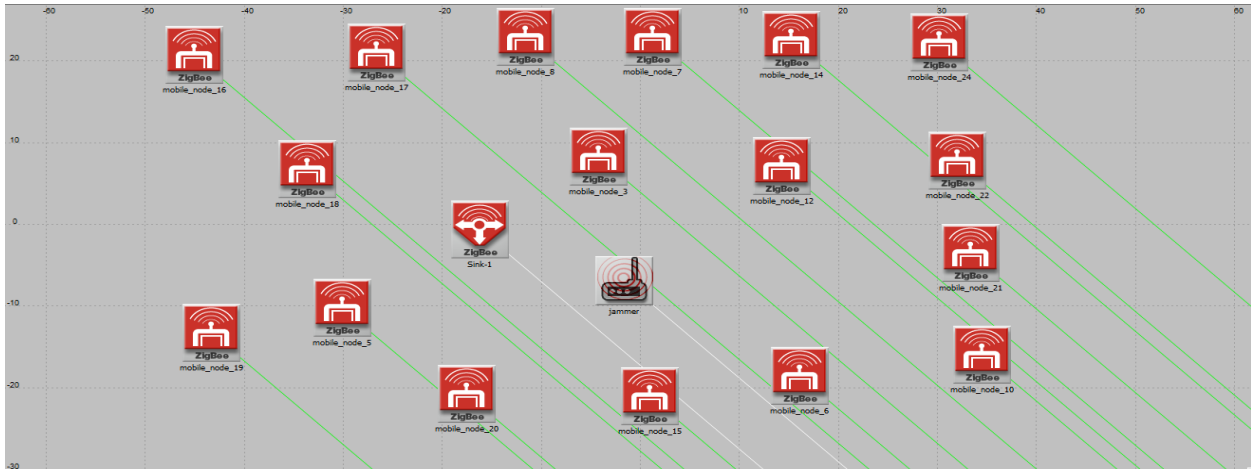


Figure 6: Scenario 3 layout (mobile sensor, sink and random jammer)

In this Scenario, a mobile pulse jammer was added to the network used in the Scenario-1. All the models of the end nodes were mobile. The jammer was represented by the model ‘jam_pulsed’ in OPNET Modeler. In Figure 6 it is shown that the mobile sensor nodes sends packets with a constant length of 1024 bits at a constant rate of 1 packet per second. When those packets arrive at the wireless modulator they are converted into a suitable form to be transmitted by the antenna at a rate of 1024 bps with a transmission power of 0.05 watts, number of transmission will be 5, and transmission band 2450MHZ. The wireless modulator also specifies that the modulation scheme is ‘zigbee_end_device’ and all the processes that will apply to that packet. Generally after creating those scenarios the result will be collect by running each scenarios for each parameters in tabular form and graph form and taking average of 10 samples of on 120sec time interval.

4. Result and Discussion

This section analyzes the results obtained from each of the scenarios described in the section 3. The simulation results are shown in plots, each of them supplemented by a detailed explanation.

Throughput Analysis

Discrete Event Statistics were chosen for each scenario, these statistics include (throughput, delay, data dropped). The simulation was run for 20 minutes and the results were collected as follows: Transmission Power of random Jammer=0.005 W

Throughput: Represents the total number of bits (in bits/sec) forwarded from 802.15.4 MAC layers to higher layers in all WPAN nodes of the network. Throughput for five scenarios (WSN without Jammers, WSN with fixed random Jammers, WSN with mobile random Jammers, WSN with fixed random jammer and mobile sensor node and WSN with mobile random jammer and mobile sensor) were shown in Figure 7. In the graph the x-axis indicate the simulation time in minutes and the y-axis represents throughput in bits per seconds.

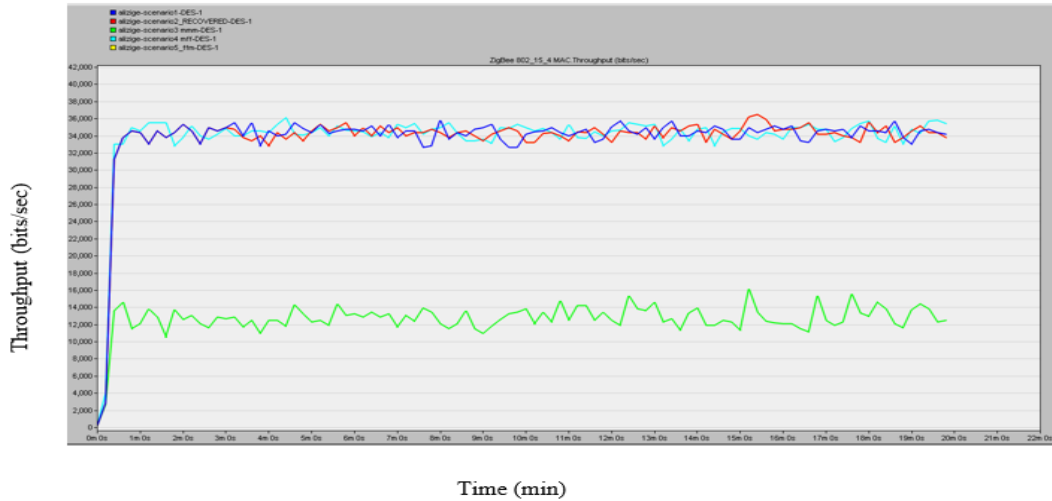


Figure 7: Analysis of throughput in all scenario

As shown previously, the existence of Jammers would reduce throughput from 36175.33333 bits/sec to 10544 bits/sec.

Table 2: Throughput of all Scenario in bits/sec

Time (sec)	Scenario 1 :Fixed Sensor, Sink node without Random jammer node	Scenario 2: Fixed Sensor, Sink and Random jammer node	Scenario 3: Mobile Sensor, Sink and Random jammer node	Scenario 4: Mobile Sensor, Fixed Sink and random jammer node	Scenario 5: Fixed Sensor and Sink node, mobile Random jammer node
0	160	160	160	160	160
120	35312	35312	12559.33333	33776	35312
240	34544	32816	12464	34352	32816
360	34736	33968	13232	34544	33968
480	35792	34352	12080	34928	34352
600	34160	33200	13808	34928	33200
720	35023.33333	33200	12464	34544	33200
840	34544	35312	13903.33333	34736	35312
960	34736	34736	12080	33584	34736
1080	34544	35599.33333	12943.33333	35696	35599.33333

As shown in the table average throughput values differ from scenario to scenario :scenario1: (Fixed Sensor, Sink node without Random jammer node):31355.133 bit/sec, Scenario 2: (Fixed Sensor, Sink and Random jammer node): 30865.533 bit/sec, scenario 3: (Mobile Sensor, Sink and Random jammer node): 11569.39 bit/sec, scenario 4: (Mobile Sensor, Fixed Sink and random jammer node): 31124.8 bit/sec and scenario 5: (Fixed Sensor and Sink node, mobile Random jammer node): 30865.533 bit/sec). Throughput values in each scenario

have different values, for example scenario one average 31355.133 bit/sec and scenario three 11569.39 bit/sec, as we seen scenario one throughput value is normal because there is no random jamming attacks ,but throughput values in scenario three is highly affected by mobile random jamming attacks.

Data Dropped Analysis

Data Drop: represent the data traffic in higher layer dropped by the 802.15.4 MAC due to consistently failing retransmissions. This statistic reports the number of the higher layer packets that are dropped because the MAC cannot receive any ACKs of those packets or their fragments for the retransmissions. Data Drop for five scenarios (WSN without Jammers, WSN with fixed random Jammers, WSN with mobile random Jammers, WSN with fixed random jammer and mobile sensor node and WSN with mobile random jammer and mobile sensor) were shown in Figure 39. In the graph the x-axis indicate the simulation time in minutes and the y-axis represents data traffic dropped in bits per seconds.

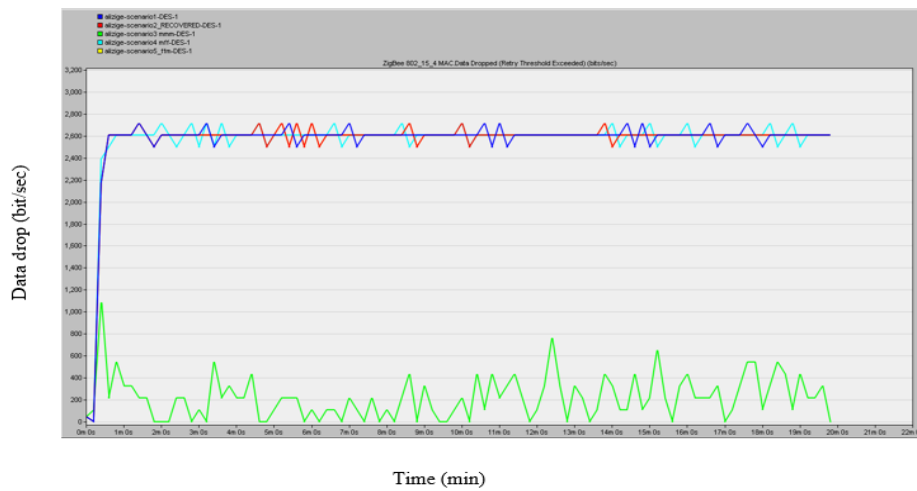


Figure 8: Analysis of data drop in all scenario

Table 3: Data drop of all Scenario in bits/sec

Time (sec)	Scenario 1	Scenario 2	Scenario 3	Scenario 4	Scenario 5
0	45.33333333	45.33333333	45.33333333	45.33333333	45.33333333
120	2608	2608	0	2716.66667	2608
240	2608	2608	217.333333	2608	2608
360	2608	2716.66667	108.666667	2608	2716.66667
480	2608	2608	108.666667	2608	2608
600	2608	2716.66667	217.333333	2716.66667	2716.66667
720	2608	2608	108.666667	2608	2608
840	2608	2499.333333	326	2716.66667	2499.33333
960	2608	2608	434.666667	2716.66667	2608
1080	2499.333333	2608	108.666667	2608	2608

As shown in the table average Data Drop values differ from scenario to scenario, scenario1: (Fixed Sensor, Sink node without Random jammer node); 2340.866 bit/sec, Scenario 2: (Fixed Sensor, Sink and Random jammer node); 2362.6 bit/sec, scenario 3: (Mobile Sensor, Sink and Random jammer node); 167.532 bit/sec, scenario 4: (Mobile Sensor, Fixed Sink and random jammer node); 2395.12 bit/sec and scenario 5: (Fixed Sensor and Sink node, mobile Random jammer node); 2362.6 bit/sec. With Jammers, the data drop was increased from 0 bits/sec to 2716.666667 bits/sec. 0 bit/sec indicate that at that time random jammer is in sleep mode which means there is no effect on WSN. Average data drop value (2395.12 bit/sec) on scenario four is high because fixed random jammer drop large number of bit/sec as compare to scenario one which is without random jamming attacks.

End-to-End Delay Analysis

Delay: Represents the end to end delay of all the packets received by the IEEE 8.2.15.4 MACs of all WPAN nodes in the network and forwarded to the higher layer. Delay for five scenarios (WSN without Jammers, WSN with fixed random Jammers, WSN with mobile random Jammers, WSN with fixed random jammer and mobile sensor node and WSN with mobile random jammer and mobile sensor) were shown in Figure 40. In the graph the x-axis indicate the simulation time in minutes and the y-axis represents delay in second.

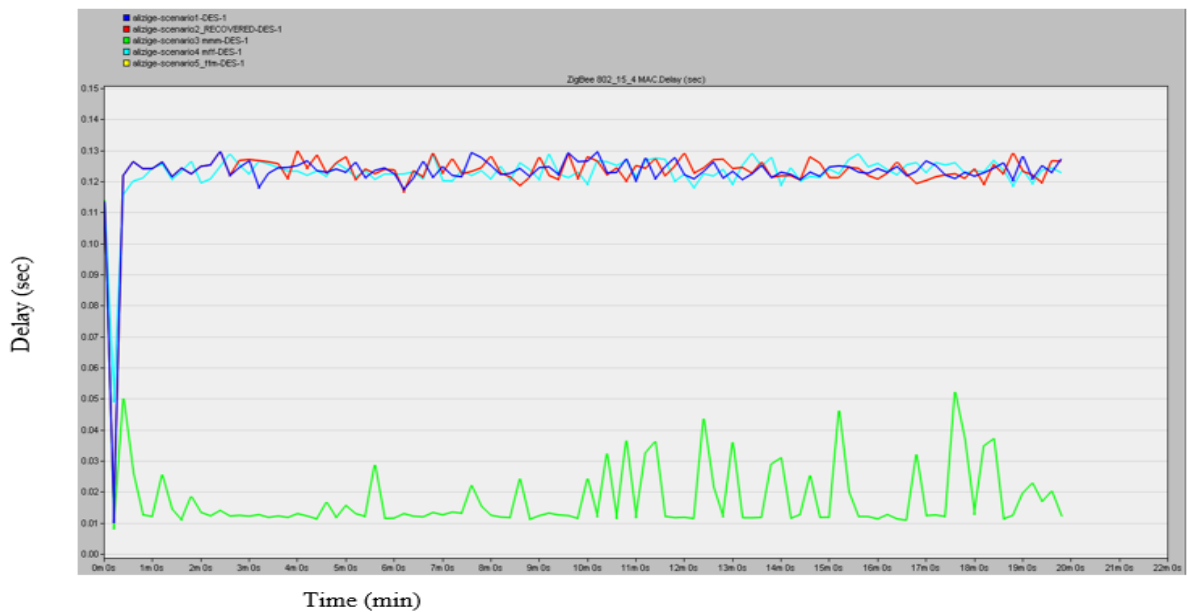


Figure 9: Analysis of Delay

With Jammers, the delay was increased from 0.00815601sec to 0.12982051sec.

Table 4: End-to-End Delay of all Scenario in Sec

Time (sec)	Scenario 1	Scenario 2:	Scenario 3:	Scenario 4	Scenario 5
0	0.113533818	0.11353378	0.11394538	0.113625247	0.11353378
120	0.124822892	0.12482285	0.01338898	0.119466305	0.12482285
240	0.12510051	0.12982051	0.01297095	0.123265799	0.12982051
360	0.122470164	0.12370465	0.01153738	0.122274352	0.12370465
480	0.125065718	0.12815492	0.01246652	0.120775195	0.12815492
600	0.126535075	0.12793218	0.02435962	0.119019699	0.12793218
720	0.122142796	0.12913523	0.01177984	0.122290984	0.12913523
840	0.122935753	0.12178441	0.03094476	0.118668517	0.12178441
960	0.124099469	0.12073646	0.01127438	0.12577665	0.12073646
1080	0.121662821	0.12404496	0.01289518	0.123384798	0.12404496
1080	0.121662821	0.12404496	0.01289518	0.123384798	0.12404496

As shown in the table average Delay values differ from scenario to scenario scenario1: (Fixed Sensor, Sink node without Random jammer node); 0.1228369016 Sec, Scenario 2: (Fixed Sensor, Sink and Random jammer node): 0.124366995 Sec, scenario 3: (Mobile Sensor, Sink and Random jammer node); 0.025556299 Sec, scenario 4: (Mobile Sensor, Fixed Sink and random jammer node); 0.1208547546 Sec and scenario 5: (Fixed Sensor and Sink node, mobile Random jammer node); 0.124366995 Sec. As show in the above table the average delay (sec) high when there is random jammer in WSN environment as compare to WSN without random jammer because if there is random jammer in WSN total amount time high in order to transfer packet from sender to receiver.

5. Conclusion

Experiments conducted to explore the performance level impacts of Random jamming attacks on WSN with fixed/mobile jammers, showed that a notable degradation in throughput, high data drop and end to end delay. With fixed sensor, fixed sink node and without jammer node scenario, the results clearly show that the communication between sensor node and sink node was normal which yields normal average throughput (31355.133 bits/sec), average delay (0.1228369016 in sec) and average data drop (2340.866 bits/sec). Whereas, In the scenario of With Mobile Sensor, mobile Sink and mobile Random jammer node, the traffic does not fall to zero, still it has a great impact on the overall average throughput (11569.39 bit/sec), average delay (0.025556299 in sec) and average data drop (167.532 bits/sec) on wireless sensor network. the performance of wireless sensor network would be highly affected the throughput up to 63.1% but even if there is mobile random jamming attacks on WSN environment decrease delay by 80.09% and data drop up to 92.84%, because of node mobility as compared to fixed sensor, fixed sink node without random jammer node in WSN. In Fixed Sensor, Sink and Random jammer scenario, the discoveries of the research clearly describes that, the traffic takes long

time. It still has a great influence on the overall wireless sensor network environment with average delay (0.124366995 sec), average throughput (30865.533 bits/sec) and average data drop (2362.56 bits/sec). When there is fixed sensor /sink node there would not be any distance variation among sensor/sink node time to time .it leads to less impacts compare to mobile random jammer relatively. Fixed random jammer causes 1.56% drop throughputs, increase delay by 1.245% and 0.927% of data drop as compared to fixed sensor and sink node without random jammer.

6. Recommendation

This performance study was studied in terms of some parameter such as (Throughput, Delay, Data Drop) could be taken with other parameters for further studies such as (load, Data traffic sent, control traffic sent, control traffic Rcvd, load per PAN).Some future work includes analyzing the effects of more than one mobile jammer in each scenario. future work consist of proposing an algorithm to cope with jamming attacks and evaluating it through simulations. Random Jamming attack IDS/IPS: It was demonstrated that random jamming attacks in WSN always could not avoided by changing transmissions, jamming attacks are still a big problem in WSNs. I believe that a method of detection can be found by developing a Random jamming attack IDS in the future. Real world system random jamming attacks: Random jamming attacks were tested in this research, but other factors, such as physical obstructions, other magnetic field, Radio transmitting towers, and weather in real world can also influence the function of devices. Physical equipment based random jamming attacks deserve to be tested.

Reference

- [1] Abdulaziz Rashid Alazemi. Defending WSNs against Jamming Attacks, American Journal of Networks and Communications. Vol. 2, No. 2, 2013.
- [2] G. Padmavathi, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," vol. 4, no. 1, pp. 1–9, 2009.
- [3] LV Bo, ZHANG Xiao-fa, WANG Chao, YUAN Nai-chang, " Study of Channelized Noise Frequency spot Jamming Techniques", 2008.
- [4] XI you-you, CHENG Nai-ping, "Performance Analysis of Multi-tone Frequency Sweeping Jamming for Direct Sequence Spread Spectrum Systems", 2011.
- [5] Ramya Shivanagu1 and Deepti C2 "A Security Mechanism against Reactive Jammer Attack in Wireless Sensor Networks Using Trigger Identification Service" International Journal of Security, Privacy and Trust Management (IJSPTM) vol 2, No 2, April 2013.
- [6] Lewis, Frank L; "Wireless Sensor Networks," Smart Environments: Technologies, Protocols, and Applications, pp. 11-46, c 2005 John Wiley & Sons, Inc.
- [7] Wenyuan Xu; Ke Ma; Trappe, W.; Yanyong Zhang; "Jamming sensor networks: attack and defense

- strategies," *Network*, IEEE, vol.20, no.3, pp. 41- 47, May-June 2006.
- [8] Alzaid, Hani; Park, Dong Gook; Nieto, Juan Gonzalez; Boyd, Colin; Foo, Ernest; "A Forward and Backward Secure Key Management in Wireless Sensor Networks for PCS/SCADA," *Sensor Systems and Software, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp. 66-82, Vol.24, c 2010, Springer Berlin Heidelberg.
- [9] Xin Liu, Guevara Noubir, Ravi Sundaram, San Tan, "SPREAD: Foiling Smart Jammers using Multi-layer Agility" IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2007 proceedings, IEEE 2007.
- [10] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses," in *IPSN '04: Proceedings of the third international symposium on Information processing in sensor networks*. ACM Press, 2004, pp. 259–268.
- [11] Wood, A.D. and J.A. Stankovic. "Denial of Service in Sensor Networks". *IEEE Computer*, Volume: 35, Issue: 10, Oct. 2002, pp.48- 56.
- [12] Williams united states," *Multi-Directional Barrage Jamming System*", 1975.
- [13] J. Schuerger, "Deceptive Jamming Modelling in Radar Sensor Networks," pp.1–7.
- [14] W. Xu et al., "Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service,"*Proc. 2004 ACM Wksp. Wireless Security*, 2004, pp. 80–89.
- [15] W. Xu et al., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," *MobiHoc '05: Proc. 6th ACM Int'l. Symp. Mobile Ad Hoc Net. And Comp.*, 2005, pp.46–57.
- [16] J.Pike,"*Sound Surveillance System (SOSUS)*"
[Online].Available:<http://www.globalsecurity.org/intell/systems/sosus.html>, March 2017.
- [17] C. E. Nishimura and D. M. Conlon, "IUSS dual use: Monitoring whales and earthquakes using SOSUS", *Mar. Technol. Soc. J.*, vol. 27, no. 4, pp. 13-21, 1994.
- [18] Y. Law et al., "Link-Layer Jamming Attacks on S-Mac," *Proc. 2nd Euro. Wksp. Wireless Sensor Networks*, 2005, pp. 217–25.
- [19] D. Report, C. Science, and J. Bacaj, "Detecting Attacks in Wireless Sensor Networks," 2011.
- [20] Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar," *Improving Reliability of Jamming Attack Detection in Ad-Hoc Networks*", *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol. 3, No.1, April 2011, pp. 57-66.

- [21] S. Raja Ratna, R. Ravi and Dr. Beulah Shekhar, "Mitigating Denial of Service Attacks in Wireless Networks", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, Volume 2, No.5, May 2013, pp. 1716-1719.
- [22] Ramya Shivanagu "An Assessment of Security Mechanisms Against Reactive Jammer Attack In Wireless Sensor Networks" *International Journal in Foundations of Computer Science & Technology (IJFCST)*, Vol. 3, No.3, May 2013.
- [23] Ajana J., Helen K.J, "Mitigating Inside Jammers in MANET Using Localized Detection Scheme", *International Journal of Engineering Science Invention*, Volume 2, Issue 7, July 2013, pp. 13-19.
- [23] Sklar B. et al. (1997). Rayleigh Fading Channels in Mobile Digital communication Systems Part I: Characterization. *IEEE communications magazine*, vol. 35.
- [24] Okumara, Y. et al. (1968). Field Strength And Its Variability In VHF And UHF Land Mobile Radio Service. *Rev. Elec. Commun. Lab*, vol 16.
- [25] Hata, M. (1980). Empirical Formulae for Propagation Loss in Land Mobile Radio Services. *IEEE trans. Vehic. Tech.* vol. VT-29, no. 3
- [26] Cox, D.C. et al. (1984). 800 MHz Attenuation measured in and around suburban houses. *AT&T Bell Lab Tech. J.*, vol. 673, no. 6
- [27] Rappaport, T.S.(1996). *Wireless communications*. NJ: Prentice Hall.
- [28] IEEE. (2007). 802.11 working group for wireless local area networks. Retrieved January 15,2017, from <http://standards.ieee.org/wireless/overview.html>
- [29] Bernard Sklar, "Digital Communications: Fundamentals and Applications", Chapter 12. Spread Spectrum Techniques, Englewood Cliffs, NJ: Prentice Hall, 1988.
- [30] Lisa Ann Osadciw and John F. Slocum "Clutter Processing Using K-Distribution for Digital Radars with Increased Sensitivity", *International Radar Conference*. 2002.