Arab American University

Faculty of Graduate Studies

Wireless Sensor Networks Analysis for Connectivity and Reliability Enhancement

By

Mariam Adwan Yasin

Supervisor

Prof. Adwan Yasin

Co- Supervisor

Dr. Mohammad Hamarsheh

This thesis was submitted in partial fulfillment of the

requirements for the Master`s degree in

Computer Science

January/ 2019

Wireless Sensor Networks Analysis for Connectivity and Reliability Enhancement

By

Mariam Adwan Yasin

This thesis was defended successfully on. 23/2/2019 and approved by:

Committee members	Signature
1. Supervisor Name: Prof. Adwan Yasin	……..……
2. Co- Supervisor Name : Dr. Mohammad Hamarsheh	…...……
3. Internal Examiner Name: Dr. Amjad Ratrout	……..……
4. External Examiner Name: Dr. Wasel Ganem	…….……

Declaration

This is to declare that the thesis entitled “A Novel Wireless Sensor Networks Anti-jamming Technique Based on a Hybrid DS-CDMA/ OFDM/ FH" under the supervision of Prof. Adwan Yasin is my own work and does not contain any unacknowledged work or material previously published or written by another person, except where due reference is made in the text of the document.

Date: 1/1/2019

Name: Mariam Adwan Yasin Signature:

Dedication

I dedicate this thesis to my great father and mother who never stop giving themselves in many countless ways; they have successfully made me the person I am proud to be now.

To my beloved husband who stood by my side all the time, who has been a constant source of support and encouragement.

To my beloved brothers who lightened my world.

Acknowledgments

First of all, many thanks to my supervisor Prof. Adwan Yasin for his incessant encouragement and support.

Also, I would like to thank and express my love to my beloved family; my father, my mother and my husband for giving me the power, support and to lighten my way in order to be able to finish this thesis.

Finally, huge thanks to my friend Ruba Ahmad who gave me much support.

Thanks for all your encouragement

Abstract

Because of the huge growing in wireless sensor networks (WSN) it became an important research area field. Wireless sensor networks are small devices that have restricted power energy and memory. In general they are easy reachable from the outside world they are also easy to attack from the outside attackers. So there are many methods are built to prevent these attacks.

So preventing outside attackers from attacking the WSN is a must, security measures are one of the important technique that each WSN must have. One of the most popular attacks are the Jamming attacks, they attend to prevent nodes from transforming data or send false one. This type of attacks has many attacking types and also many preventing technique also.

In this thesis securing WSN is studied to provide dependable, robust and lightweight security mechanisms that guarantee the system ability to be strong against foreign attacks. Different types of security attacks and the appropriate security mechanisms are deeply discussed, taking in to account the resources constraints in WSN.

Our proposed model investigates the combination of Direct Sequence-Code Division Multiple Accesses (DS-CDMA) with Orthogonal Frequency Division Multiplexing (OFDM) and Frequency Hopping (FH)

as a promising anti-jamming technique in wireless sensor networks (WSN).

The DS-CDMA component provides user discrimination based on coding at the same carrier frequency and simultaneously.

The OFDM component removes Inter-Symbol Interference (ISI) and provides resistance to multipath effect. The FH component solves the near-far problem inherent in DS-CDMA.

Table of Content

DECLARATION ..... **II**

DEDICATION ..... **III**

ACKNOWLEDGMENTS ..... **IV**

ABSTRACT ..... **V**

1 INTRODUCTION **1**

1.1 MOTIVATION 2

1.2 PROBLEM STATEMENT AND RESEARCH QUESTION 3

1.3 CONTRIBUTION 4

1.4 STRUCTURE OF THE THESIS 5

2 BACKGROUND **6**

2.1 CHARACTERISTIC OF WSN 8

2.2 WSN ARCHITECTURE 11

2.3 WSN APPLICATION 15

2.4 CHALLENGES OF WSN 16

2.5 SECURITY SCHEMES IN WSNS 17

2.6 SECURITY REQUIREMENTS OF WSN 18

2.7 WIRELESS SENSOR NETWORKS SECURITY THREATS 20

2.7.1 Wireless Sensor Networks Attacks 20

3 JAMMING **26**

3.1 INTRODUCTIONS TO JAMMING 26

3.2 JAMMING ATTACKS TYPES 28

3.3 JAMMERS TYPES 29

3.4 JAMMING ATTACK DETECTION METRICS 34

3.5 JAMMING DETECTION TECHNIQUES AND ALGORITHMS 36

4 PROPOSED MODEL 45

4.1 ALGORITHMS USED IN THE PROPOSED MODEL 45

4.1.1 Frequency Hopping (FH) 45

4.1.2 Code Division Multiple Access (CDMA) 47

4.1.2.1 CDMA in Wireless Sensor Networks 48

4.1.2.2 CDMA and FH 49

4.1.3 Orthogonal Frequency Division Multiplexing (OFDM) 50

4.1.3.1 OFDM and CDMA 53

4.1.3.2OFDM, CDMA and FH 54

4.2 SYSTEM MODEL FOR DS-CDMA/OFDNM/FH [86] 55

4.2.1 Bandwidth and number of OFDM sub-channels 55

4.2.2 Modulation 58

4.2.3 Frequency Sequence Generator 59

4.2.4 PERFORMANCE EVALUATION 62

4.2.4.1 Performance of the hybrid DS-CDMA/ OFDM/ FH system 62

5. SIMULATION AND FINAL RESULTS 64

5.1 CONCLUSION AND FUTURE WORK 70

REFERENCES 71

الخلاصة 82

List of Figures

Figure 1: Main Blocks for the Sensor Node 13

Figure 2: Types of jammers in wireless networks 30

Figure 3: Difference between FDM and OFDM..... 50

Figure 4: OFDM Transmitter and Receiver..... 53

Figure 5: Block Diagram of DS-CDMA /OFDM/FH System 55

Figure 6: IEEE 802.15.14 Channel Selection 56

Figure 7: OFDM Orthogonal Sub-Channels..... 56

Figure 8: Set of Used Frequencies 58

Figure 9: Frequency Generator 61

Figure 10: Block Diagram of the Proposed System..... 62

List of Tables

Table 1: Security Attacks on WSN 24

Table 2: Comparison between channels number and matching percentage 66

Table 3: Matching percentage for our proposed model 67

Table 4: Matching percentage for 16,32,64,128,256 and 512 sub-channels 68

Table 5: Fast hopping comparison 69

List of Abbreviations

BPR- Bad Packet Ratio

CDMA - Code Division Multiple Access

CSMA - Carrier Sense Multiple Access

CTS - Clear to Send

DS - Direct Sequence

DS CDMA - Direct Sequence-Code Division Multiple Accesses

DSSS - Direct Sequence Spread Spectrum

FH - Frequency Hopping

FHSS - Frequency Hopping Spread Spectrum

ISI – Inter Symbol Interference

OFDM - Orthogonal Frequency Division Multiplexing

PDR - Packet Delivery Ratio

PN - Pseudo Noise

RTS - Request to Send

SNR - Signal to Noise Ratio

WSN - Wireless Sensor Networks

1 INTRODUCTION

Wireless communication transmits data among the nodes that are connected with each other using radio waves. WSN is an example of the wireless communications; it's a large network contains group of sensor nodes that communicate with each other using multi-hope communication [1]. These sensors could be used for sensing temperature, light, sound and many other things. WSN have wide range of applications from military to daily life, for example WSN provide alerts for natural disasters, monitoring and controlling information from cities and provide public services for citizen.

The first use of sensor networks was in the cold war period. When they used distributed networks of radars and hydrophones in order to observe skies and oceans [2].

The most important feature in WSN is that it must afford security for the data that are being transmitted all over its network nodes, such that no intruder can affect the data. Starting from the earlier beginnings of WSN applications, they have been under attack by intruders that have interest in interrupting the transmitted data.

Jamming attacks are the most common methods that are being used by the intruders in order to disturb the transmission and reception between the nodes, which cause data loss or at least affect the transmitted data in order to inhibit them from reaching its destination [2].

Jammers have developed many types of jamming methods in order to insert false data through the communication between the nodes to distress the data during transmission. Jammers also distribute the data transmission in many different ways, for example; overutilization of the resources, for example, memory and the power in

its own batteries. As the jammers continue to improve their methods in order to distribute the transmission causing data loss, many defense techniques have improved to minimize the jammers affection. Jamming defense techniques are in an area of large attention in both the academic field and the industry field [3][4].

In general, most of the defense techniques aims to a specific type of jammers, so they are not an all purpose use for all jamming methods. In order to prevent most of jamming techniques, our thesis has proposed a significant algorithm that tries as possible to prevent all jammers from getting into the network, by minimizing the probability of jamming the used frequency between the nodes as minimum as possible, taking into consideration the amount of transmitted data in sensor nodes and keeping the used channels for transmission safe from jamming.

The rest of this chapter is organized as follows. In Section 1.1, we introduced the Motivations of our proposed work. Problem Statement is presented in Section 1.2. Our main contributions outlined in 1.3 and also discussed our future work. Finally, the last Section 1.4 contains the Structure of our thesis.

1.1 Motivation

The most essential requirement that the network have to achieve is security, by providing availability, integrity and confidentiality. Each eligible receiver node has to receive all the sent data and also to be able to confirm the integrity of the entire message as well as the identity of the sender. The content of the messages must not be interfered by any intruders. The main goal that WSN has to achieve is delivering the information in the right time without being exposed to the end user.

WSN - as they use the wireless communication technology - faces many challenges measured to the fixed wired network, because they are more vulnerable to jamming

attacks that's why efficient security methods are necessary to use for WSNs in order to overcome the security challenges that they face.

Jamming attacks as mentioned previously aims to interrupt the communication among the nodes in the network which cause data loss. Many defense and detect algorithms have been discussed and proposed in order to minimize the affect of jammers. But the main problems of most of the previous studies are, first the proposed techniques are not a general technique that stops all type of jammers or even detect all types of jammers, they are designed to stop or at least minimize the effect of a specific type. So, the main goal that we focused on it is to provide a secure mechanism that minimize the jamming effect as minimum as possible, by making the probability to access the network for the jammer as minimum as possible. Secondly, the previously used mechanisms are complex, most of them require some parameters like for example, Packet Delivery ratio (PDR) to catch the jammer that have already jammed the network and some data have been lost. Thus, we tried to find a new algorithm that doesn't require complex action in order to prevent the jammer from jamming the network and also doesn't use complicated parameters that takes time in order to be calculated. Our proposed algorithm makes less chance for most types of jammer to enter the wireless network.

1.2 Problem Statement and Research Question

In previous researches, the authors have shown the bad effects of the jammers and how they affect the WSN performance in general. Most of the previous researchers proposed defense technique for specific types of jammers, as we mentioned before not for most of jammers types. The proposed methods are complex and take some time to detect the jammer because of using some parameters from the wireless network. So

data will be lost for (n) time until the proposed algorithms start detecting jammers or stopping the jammers from affecting the communications between the sensor nodes. This all because jammers are different and can change their characteristic. So in order to minimize the overall jamming effect some steps and questions had to be answered.

First of all, we studied all jammers types and discussed all their used techniques in order to access the network.

Secondly, we also studied all the main defense techniques that have been used in the previous works in order to find the main problem that prevent most of the previous research from finding a new methodology that stops the jammers from jamming the WSN.

Thirdly, we had to answer this question:

How could we minimize the probability of being jammed as minimum as possible without affecting the data transmitted between the nodes?

The answer to this question was by using some other techniques in order to achieve our main goal.

1.3 Contribution

It is important to mention our work contribution as follows:

- Our thesis has provided a better understanding for jamming types and their behavior in WSN.
- Compared between the most important and famous used defense techniques.
- Proposed a new methodology in protecting the WSN from most jammers types by minimizing their overall probability of entering the wireless network.

- FH, CDMA and OFDM have been used in order to enhance our proposed scheme.

1.4 Structure of the Thesis

The rest of thesis is organized as follow: Chapter 2 is an overview of the WSN. Chapter 3 discuses and illustrates the jamming problem in the WSN, it also presents jammers types and the main defense techniques. Chapter 4, we present our proposed system and viewed an overview of the used techniques. In Chapter 5 we discuss the results and simulation of the proposed method.

2 Background

One of the most critical problems the US navy had through the cold war in the 1950's is to locate the enemies' submarines and that’s because underwater visibility was needed, so they developed a new system to help them locate the enemy, it was called Sound Surveillance System (SOSUS). This system was used to detect the closest submarine by using underwater sound microphone, this is considers the first level of WSNs [6].

In the 1980's the Defense Advanced Research Projects Agency (DARPA) began using The Advanced Research Projects Agency Network (ARPANET) in order to communicate between the nodes [7]. In the 1990's US navy started using a new system that sense data close ships to be aware of the target. In the 2000's, new software was built by the Defense Advanced Research Projects Agency using very small sensors in order to create a network with ad hoc connection.

These enhancements during the years have leaded us to the present WSNs that are used in many various applications. The world we are living in have many different type of information's like temperature, motion, light and many others. So for advanced understanding of this world, it had become important to us get all the information from different sources, and WSN was the best solution to capture all these information.

Every node contains the following parts, power supply component, sensors, microprocessor, communication device, analog convertor, and data storage [8-9]. These nodes are self organized and the data is sent out to neighbor nodes until it arrives at the destination.

WSNs used and still being used in many different applications, observing the environment and monitor it for example [10-15].

One of the basic concerns in WSN is node deployment method to implement in the network scenario; many aspects should be taken into consideration like types of devices, their numbers and their locations to see the network impact on many of WSN properties like lifetime, cost connectivity and many others. There are in general two types of deployments; it's either dense or spare. The first type, the sparse deployment is used when we need to cover the whole network using fewer amounts of sensors or else when the price of sensors is high [16]. The second type, dense deployment is the opposite it has large amount of sensor nodes in the network area.

WSNs have some challenges/issues that must be addressed before doing any implementations for any WSN. One of the most important issues that WSN face, is a very serious challenge that must be taken into account, it’s the *security mechanisms* used in WSNs. It's important to mention that there are many security mechanisms employed in ad hoc network that can't be used in WSNs.

WSN contains large number of spatially independent distributed sensors to observe different environment also to transmit the data among the network until it reaches the main sensor node or the base station.

WSN now days are bidirectional and it indicates that the network allows transmission from base station to nodes and from node to base station, so every node can actually transmit and receive data.

WSN started to be in use starting from military applications and that motivated us to use it in million different applications later, like industrial and environmental application for example. Sensors could be in different sizes from the size of cereal of dust or even like laptop size. Also sensors are different in cost, it could be from hundreds of dollars to few dollars and this depends on the functionality and complexity of the sensor.

Many applications use the WSNs to accomplish their tasks, we mention here some:

1- Observing regions, in other word monitoring them.

2- Observing environment and dangerous events like fire [8].

3- Data collections, WSNs are used widely to collect data for many other purposes [6- 7].

WSNs have many benefits including self-organization, easy deployment, high reliability in sensing and low cost [7]. Even though WSNs have many benefits it also suffers from serious challenges that decrease their performance. The following are some of the challenges that WSNs have:

1. The power consumption for each node since they use batteries.
2. Some nodes could be moving around like mobiles.
3. Sometimes nodes have problems in their communication in a way that causes a failure.
4. Ability to manage node failures.
5. Ability to survive during any environmental condition.
6. Security during communication between nodes.

2.1 Characteristic of WSN

Characteristics of WSNs have to be taken into consideration while building and designing the networks in order to achieve efficiency and reliability. The WSN nodes are able and responsible for gathering, arranging, processing, accumulating and sending the information to the sink. Robustness of any WSN is reached by the distributed sensing.

Sensor nodes can stop working for battery weariness or different conditions. Used communication channels can be also be distributed with the extra nodes that might be added in the network. All the above circumstances cause the frequent change in the network topology.

WSNs characteristics are defined from two perceptions: either the nodes that structure the network or from the network itself. The following points illustrate the most important characteristics of WSNs [17] [18]:

1) Low cost:

In general, to measure particular physical environment, large numbers of sensor nodes are being used. So to minimize the complete cost of the entire network, the cost of sensor nodes has to be as minimum as possible.

2) Energy efficient:

WSNs are used in many fields like communications and computation. That's why in general; wireless nodes consume energy way too more than any other type of nodes. Wireless sensor nodes try not to run out of energy because if they did they become useless since they also don't have the chance to recharge again.

3) Computational power:

In general nodes in WSNs have constrained computational capacities as the cost and vitality should be taking into consideration.

4) Communication capabilities:

WSN nodes use usually radio waves on its wireless channels in their communications. This type of communications can be done in two ways; either bidirectional or unidirectional with limited and dynamic bandwidth.

5) Security and Privacy:

All sensor nodes should have some kind of security mechanism to avert unapproved access, assaults, and inadvertent harm of the data within the sensor node.

6) Distributed processing and sensing:

All the nodes work in distributed manners.

7) Self organized:

WSN nodes should be able to arrange and organize themselves as they exist in an unattended environment. The nodes must work in association in order to modify them self automatically in their changeable network.

8) Multihop communication:

Each sensor node in the network should have a feasible connection way with the sink node in a direct way or indirect by using help from intermediate node through the routing path. In case a node had to communicate with nodes that are beyond their radio frequency, this communication should be done through the Multihop rout.

9) Application oriented:

Sensor nodes are different from other nodes in any other network according to their nature, they depend on the application type they are used in; the nodes are planned randomly in the environment depending on the type of use, either they are in military, environmental, health or any other type of use.

10) Robust operations:

Sensor nodes are planned in a very large and hostile area. Because of this, the WSN nodes must be fault and error tolerant by having the capability to self-test adjust and self repair.

2.2 WSN Architecture

Because of the WSN characteristics, many challenges have shown up and in the same time many development have been accrued for the WSN. But before addressing the challenges, the architecture of WSN have to be taken into consideration [19]. The WSN should be designed and implemented in a flexible way.

To facilitate doing that, some significant purposes of WSNs architecture design are as per the following:

1) WSNs application requirements should be identified:

Depending on the application requirements, special analytical study should be done in order to identify the relevant technology trends and

application necessities. Since WSNs are known as complex systems, it becomes important to take into consideration the designing cost and also finding the best fit for the WSNs using highest power optimization depending on the preferred application.

2) Optimized design:

It becomes a necessary task to design a WSN that greatest use of the sensor nodes by using smallest amount resources because of the resources constraints in the sensor nodes.

3) Designing Techniques and technology:

The architecture of WSNs should be designed based on existing and upcoming technology. The most important components that must be taken into consideration in this point are the power supply and storage, because of their important role and use in the sensors. So, in the designing phase the technologies that are used must be identified.

Because of the dynamic nature of the WSNs there are many sorts of sensor nodes. WSN nodes should focus on minimizing the cost, maximizing the flexibility and affording fault tolerance.

Sensor nodes structure contains sensing unit which is divided into sensors and analog digital converter (ADC), processing unit which is also divided into processor and storage, transceiver as a communication unit and

finally a power supply unit [17]. The main components for the sensor node are shown in Figure 1.

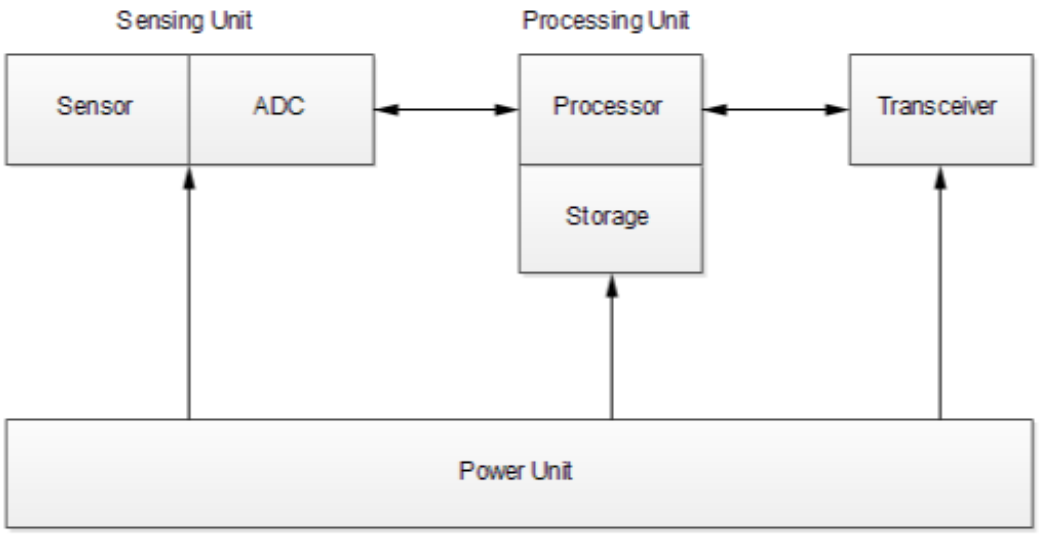

Figure 1: Main Blocks for the Sensor Node

Below is the description of the different units:

1) Sensing Unit:

It contains a group of diverse sorts of sensors that are required for measuring different phenomenon of the real environment. The sensors are chosen derived from the application that they work in. The outcome from the sensors are electrical signal for this reason, an analog to digital convertor (ADC) is being employed, in order to transform the signal into digital to communicate with the microcontroller.

2) Processing Unit:

This unit contains a microcontroller and storage; also it has an operating system. The main role of this unit is to collect data from different sources after that it processes and stores them.

3) Communication Unit:

Depends mainly on its transceiver that consists of both a transmitter and a receiver, it uses network protocol in order to communicate through a special communication channel.

4) Power Unit:

The main duty of this unit is to offer the needed energy for the sensor nodes in order to observe the environment with minimum cost and time. Sensor life time depends on the power supply that is attached with the power unit. This unite is necessary to perform proficient use of the battery.

WSNs are generally known as group of distributed sensors able to do many functions in general, they process and gather information and connect sensor node with each other by establishing a connection between them. Sensor nodes can also be defined as specialized sensors that process raw critical information that observe and record situations for example like temperature, sound, chemical concentration, and many others.

Wireless sensor nodes are field devices that are in charge of routing the packets. Each one of them has three other subsystems; processing subsystem, communication subsystem and sensor subsystem.

The transmission among sensors is made by using wireless transceivers. Because of the broadcast nature in WSN, it's more exposed to attacks more than the wired networks. Nodes in WSNs are randomly arranged in the network area that make them

easy target to be attacked. Even though routing algorithms, mechanisms and WSN modeling are getting more attention, the security threats are receiving much more focus because of the great damage that can be caused by violating it.

In this part, we look at the security threats and challenges for WSN and discussing the main solutions that are being used. in general, the biggest problem for developing any professional security scheme in WSN is based on the sensor size, the processing power, memory size and tasks type that are expected to be done from the sensor.

2.3 WSN Application

Equally to all other technologies sensor networks were initiated aiming military applications. The Sound Surveillance System (SOSUS) was the first known sensor network application [20].

In the 1980s, the Distributed Sensor Networks (DSNs) was created by the Defense Advanced Research Projects Agency (DARPA) [21]. Small and low-cost sensors founded on micro-electromechanical system (MEMS) technology [22], wireless networking, and with a reasonable cost low-power processors permitted the disposition of WSNs for various uses.

Some examples of WSNs applications*:*

1. Security: there are many applications for WSNs in security for example; the observation of dangerous and sensitive regions [23].

2. Environment observing: WSNs can propose better elasticity in this field as they have the ability to observe regions that don’t have infrastructure [24].

3. Medical monitoring: doctors are able to monitor their patients using proper WSNs.

4. Object Tracking: WSN can be used for trailing moving objects or persons if it was prepared with the suitable sensors [25].

5. Assistive environments: functional capabilities of individuals with disabilities can be improved using WSN technology in such environments. Illustrative samples of assistive environments that employ WSNs are [26] and [27].

2.4 Challenges of WSN

Looking at WSN uniqueness many challenges are considered especially regarding security issues. Without understanding these challenges, security aims cannot be met.

We mention some of the most well-known challenges that WSN face:

1) Customization

2) Resource limitations [29].

3) Absence of Central Control

4) Isolated Location [30].

5) Hardware constraint [30]

6) *Energy Constraint* [29, 30].

7) Time Synchronization [29].

8) *WSN Node* [30]

2.5 Security Schemes in WSNs

Security is a general term that contains the four main elements of it, Authentication, Integrity, Confidentiality and Availability.

For a secure transmission of all information types among the wireless networks, several techniques have been used to ensure a secure and reliable arrive of data as it is discussed below:

1) Cryptography

The method of using encryption-decryption is not feasible in wired networks; it's applied widely in wireless networks. Using encryption techniques require extra bits to be transmitted, processing, memory and battery power which are essential components for sensor nodes [31]. Also delay and packet loss is increased in WSN. Many important questions have to been asked while using encryption methods and algorithms in WSNs. For example, generation and managing processes for the keys is considered an important and questionable area that has to be addressed carefully, also trying to minimize the human interaction with the sensors.

2) Steganography

While cryptography tries to conceal the message content, Steganography tries to conceal the message existence. Steganography in general is the art of concealing information within another carrier.

The major purpose of steganography is to adjust the carrier not to look differently from the original one. It conceals the existence of the secret channel and data.

3) Securing the Access to the physical layer

This method can be reached in WSN by applying frequency hopping techniques. By using a group of significant parameters like hopping set, time interval for each hop and hopping pattern, this method will be effectively useful but also with small amount of disbursement of processing, memory and power resources.

2.6 Security Requirements of WSN

Security in WSN must be a vital requirement [32]. Protection of data, information and resources from intruders, attacks and misbehaviors is the ultimate goal of the security services in WSNs. The security needs in WSNs include:

1. Confidentiality: in WSN the information is firstly diffused starting with one hub then onto the next hub, followed by directing information through numerous hubs, and finally the information or data is delivered to the main station. It is critical for all messages directed through the remote sensor network is to be private and closed to the unapproved client. A given message cannot be understood by anyone other than the desired recipients is guaranteed by WSNs confidentiality [33].

2. Authentication: some defect hub -caused by an unapproved access- may drop a few bundles from the system or some false parcels into the system. Such unwelcome influences can be kept away if intended to identify the first sensor hubs. Intruder node cannot pretend to be as a trusted sensor node, as the authentication certifies that the transmission from one node to another node is unaffected [34].

3. Integrity: the idea of honesty is abused if some variation occurs in the information parcels by a malignant hub. Therefore, Integrity assures the rightness of the information and guarantees the sent message from one node to another and not altered by any malicious intermediate nodes. Leading to have the recipient hub getting the same information as the sender hub [32].

4. Availability: A defected hub may lead to a defected base station, which could lead to the whole WSN system to get defected. Sensor nodes and sink are ought to be reliable to be accessible for giving administrations of WSN. Availability makes sure that the chosen network services are accessible even in the presence of denial-of-service (DoS) attacks [32].

5. Authorization: Authorization guarantees that only a certified sensor node can deliver information to a WSN system [32].

6. Freshness: old data must not be replayed by malicious nodes. Each message data must be updated (fresh) [32].

7. Time Synchronization: the delay between packets in a pair of two nodes is calculated using time synchronization done by most Wireless sensor network.

8. Access control: Access control inhibits illegal access to a resource. It fails unauthorized contribution in the network.

2.7 Wireless Sensor Networks Security Threats

In general, Security threats in WSN are nearly the same as wired networks, but also worse in case of wireless connections. As known, wireless networks are in general vulnerable to diverse kinds of security attacks as the transmission medium is unguided and more liable to security attacks. Wireless communications have broadcast characteristics which mean that they exposed to eavesdropping. Generally, most of security problems and attacks that are related to wireless networks are as well for the WSN.

It's important to mention that the used techniques for ad hoc wireless networks can't be applied directly for WSNs due to the architectural difference between the two. Mean while wireless ad hoc networks are dynamic topology, self organize, peer to peer networks shaped by a group of nodes without a base station [33], the WSNs have a centralized node. The architecture of WSNs makes implanting the security models and techniques easier because of the existence of the centralized base station that is used widely. However, the biggest challenge is brought from the limitation of recourses of its teeny sensors. In general, sensors are supposed to be deployed randomly in critical or important areas like enemy regions. So, even though the sink node (base station) is placed in a safe or friendly area, the sensor nodes have to be secluded from the attacks.

2.7.1 Wireless Sensor Networks Attacks

Wireless sensor networks attacks are in general measured from two diverse points of view. The first is the attack on the security mechanisms and the second is against the main mechanisms methods like routing mechanisms. Below are mentioned the main attacks in WSNs.

1- Denial of Service attacks

Denial of service attacks are one of the famous types of active attacks [34] [35] [36], it is caused by malicious nodes or actions that harm the authenticated sensor nodes by making them fail. In general this attack is done by sending random packets to the legitimate nodes to prevent the users from accessing network services and resources. Denial of Service attacks has many types and it affects each network layer differently, below are mentioned some of the attacks for each layer [37];

a. Physical Layer:

- Jamming Attacks [34] [35] [36], this type of attacks aim to interfere the radio channels by sending wrong or random packets to the frequency band to disturb the network and intervene the transmission. Jamming attacks have many other types that try in general to disturb the transmission channel and affect the resources of the sensor nodes by minimizing their effectiveness.

- Node tempering [34] this attack happens when an attacker access the physical layer, all the important and sensitive information can be accessed by the outsider, also he'll be able to change or modify the nodes by using a malicious nodes to produce a node that he can control.

b. Data Link Layer:

- Collision: when two nodes send in the same frequency at the same period of time, this attack appears. When the transmitted packets run into each other, the data will be modified because of the attack. This will make the data packets invalid.

- Exhaustion: The attacker in this type tries to exhaust the WSN by repeating the transmission of data packets continuously. In general, this attack targets the close nodes by sending them many of join requests until exhausting the nodes batteries.

- Unfairness: this is the simplest and weakest type of DoS attacks; the attacker attempts to minimize the performance of the WSN instead of fully stopping the access to the network services. So the main aim of this technique to reduce network efficiency.

- Interrogation: the attackers try to exhaust the sensor nodes resources by using the communication among two nodes before the data transmission to send repeatedly the messages.

c. Network Layer:

- Blackhole attacks [34] [35][36] this attack is caused by an outsider element on the WSN, the intruder tries to prevent the nodes from transmitting data packets by using his special nodes which called blackhole nodes that cover special specific area called blackhole area. So, any data that goes into the blackhole area will be taken over and will not reach the base station. This attack increase in general the end to end delay and also decrease the throughput.

- Selective forwarding: the attacker tries to drop the data packets during the transition into the base station. The attacker can't be simply detected even though he'll be somewhere around the base station.

d. Transport Layer:

- Synchronization Flooding: the attacker tries to exhaust the network resources by making repeatedly new connections request. This attack generally exhausts the memory through flooding. Other way is used by the attacker is by sending huge number of random packets into one destination, this traffic makes the network not able to differentiate between authorized packets and malicious ones.

- De-synchronization: this attack aims to dry the nodes energy by disrupting the connection. The attack is done by continuously spoofing the sent messages to make the nodes retransmit the missing packets.

2- Attacks in information

In WSN the sensor nodes observe any changes according to its main functions and send this observation into the sink node, during the transmission process the sent data can be modified, spoofed or disappear. Any attacker can also observe the traffic and interrupt, alter or fabricate packets therefore, give false information to the sink nodes.

3- Wormhole attack

This is one of the dangerous types of attacks in WSN security attacks, the attacker tries to record most of the packets in a particular location, after that he sends them into another location.

4- Black-hole attack

In this sort of attacks, the attacker uses a node that acts like a black-hole in order to attract all the traffic in the WSN. The malicious node pay attention to all requests for routes after that it answers the node which has best quality or has the shortest path to the sink node.

Table 1: Security Attacks on WSN

Main Attacks	Description
Denial Of Service	Physical Layer: • Node tempering • Jamming Attacks
	Data Link Layer: • Interrogation • Unfairness • Exhaustion • Collision
	Network Layer: • Black-hole attacks • Selective forwarding

	Transport Layer: • Synchronization Flooding • De-synchronization
Attacks on Information	Modify, interrupt and spoof the transmitted data.
Wormhole	To record most of the packets in a one location in order to send them into another location
Blackhole	Attract all the traffic in the WSN

3 Jamming

3.1 Introductions to Jamming

Wireless Sensor Networks (WSN) now are very important and one of the most leading technologies that are used nowadays in many fields. This is one f the most important reasons that make the researchers put huge efforts in order to reach perfection.

WSN applications are wide and various, it covers large field of applications; it starting from home applications to military applications, as known about WSN, they are a group of tiny devices usually called nodes which have limited power and processing capability. These small devices are used to observe the environment and also for multidimensional information collecting purposes. The data collected from the area are delivered to the main node which called sink node via wireless links; these wireless communications in the WSNs can be directly to the main node or can use multiple hopes to reach its destination. As soon as the data is collected in the sink node they can be used by the user [38].

As the communications in the WSNs are done wirelessly, it became a huge security anxiety, because the communications are uncovered and exhibition for different types of attacks. Another drawback of WSN its limited resources and size, so building a secure network has become a must and that makes it one of the hot topics in research specially when WSN has become one of the most important areas in industry [39].

In order to guarantee the reliability of the WSNs, many techniques are needed to be used in order to make sure that WSNs can manage handling all types of jamming attack.

Jamming attacks cause distribution to WSNs and also arise accidentally because of collisions, noise or interference at the receiver side. Jamming attacks are an efficient

attacks since there is no particular hardware is needed to launch them, also jamming attacks can be easily implemented just by listening to sensors transition and broadcast at the same frequency [40].

The major two types of attacks that makes the researchers concern about the security of WSN are; active attacks and passive attacks [41]. Passive attacks aims to interrupt the radio frequencies and don't change any information transmitted in the WSN. As for the Active attacks, the data are modified and the most known and dangerous type from the category are the jamming attacks.

They can be defined in wireless sensor network as interrupting the wireless communications by interfering the communication of wireless signals [42]. Jamming attacks are diverse from other types of attacks since it aims to interfere the communication in the wireless sensors among sensor nodes in the same wireless network or using other devices.

Jamming attacks are mainly categorized as an external risk type of security threats, where the attackers are not physically placed in the network. Jamming attacks have a specific drawback from the jammer's viewpoint, the jammer has to use a huge amount of power (energy) in order to jam the frequency band in the victims, also jamming in general is very easy to notice due to the sudden raise in the energy of the victims channel. Jamming attacks reduce link reliability, also cause in packet transmission some delay [41]. Jammers in general aims to destroy the victim's network by making problems in the transmitted data between the nodes, also it aims to benefit from the victims network by increasing its capacity.

The main targets of jamming attacks are the physical layer and the MAC layer.

Jamming attacks in wireless sensor networks are disastrous attacks since they don't require any hardware devices or any software [43]. It can simply be done by just listening passively to the wireless devices so as to broadcast at the same frequency. Jamming attacks are typified by low detection probability, high energy efficiency and anti jamming resistance [44].

3.2 Jamming Attacks types

- **Low-level type:** Wireless communications are blocked when noise signal is cultivated. This is applicable to all typical designs of wireless communication, this sort is reacting or not. According to non-reacting one, the transmission is always blocked whereas the other one (reacting) the transmission is adjusted after a jammer's examination. Here are the three alternatives for the jammer to follow in an attack: constant, carding, and indiscriminate.

  The jammer doesn't leave the blocked channel regardless of time passes (constant); when blocking the cycles, the jammer selects which channel respectively to hop and block for a while (carding); After blocking channels respectively for a specific period, the jammer chooses the channel which needs to be altered indiscriminately.

- **High-level responsive type:** As the jammer follows a trace of the receiver to define the pseudo-random leaping pattern source, it commences this type to block the dispatch transmission. The both reacting types intend to FH from varied angles; the bundle transmitted can never be recovered in any hop when it is blocked (low level), whereas obstructing the dispatch transmitted happens through clutching the source when using the pseudo-random hopping pattern

- **Hybrid type:** It is an advanced type through which the jammer simultaneously utilizes low and high levels reacting types

3.3 Jammers Types

Attacker plant malicious devices usually wireless nodes in order to cause interference in the WSN. Jamming attacks interfere with radio signal in order to harm the communications in WSN, by keeping the nodes communication busy, and that makes the transmitter to back off when it senses the receiver side busy. In general, jamming attack targets the physical layer, however it sometimes affect and attack other layers. In this section; different types of attacks will be explained. Jamming attacks can give the attacker the same capabilities as the valid nodes or it can give them different ones, that's all depends on the attacking strategy. Based on the radio transmission power and position of the intruder, this attack influences the wireless network.

Figure 2 shows jamming types according to their characteristic in attacking the networks, the attacks could be elementary or advanced attacks and that depend on the jammer functionality. The elementary is divided into two categorize, the proactive and reactive. For the advanced attacks are classified to function specific and to smart hybrid [45].

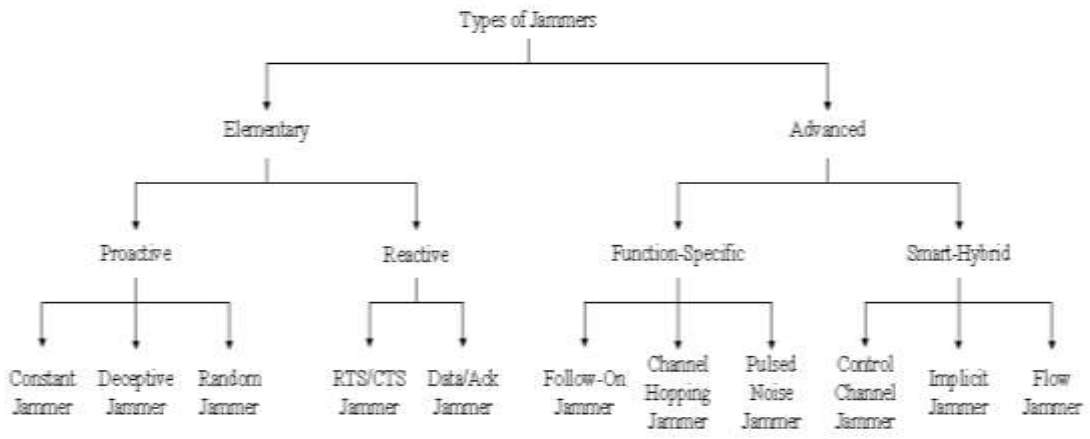

Figure 2: Types of jammers in wireless networks [45]

3.3.1.1 Proactive Jammer:

This type of jamming attack transmits their interruption signal among the target nodes whether there is a data communication or not in the network. The jammer sends random bits or even packets to the channel the network transmitting on, and by doing this it makes the transmission channel busy by transmitting jammers random bits or packets making all the target nodes in the network in non operating mode. But the jammer keeps his jamming signals in only one channel and doesn't switch to other channels until it exhaust all its energy. This type of jamming has three basic forms, the constant, deceptive and finally the random.

a. Constant Jammer:

The first type of proactive jamming is a type that doesn't follow the Carrier Sense Multiple Access (CSMA) protocol, this means that it doesn’t listen or sense the network before transmitting any data. The nodes use this protocol to sense the channel if they found it busy, the nodes postpone the transmission. The constant jammer prevents the target nodes in the network from communicating along with other nodes by keeping the channel busy. However, this type of jamming cause power exhausting

since it keeps transmitting data to the target network in order to keep the channel busy, also it's easy to detect. Even though it has a huge disadvantages, this type is easy to initiate and can cause a serious problem to the target network by making the nodes not able to communicate with each other.

b. Deceptive Jammer:

In this type of proactive jamming types, the jammer transmits regular packets continuously rather than producing random bits like the constant jammer. This type of jamming misleads the other nodes to think of them as legitimate and valid transmission so the target nodes will remain believing that the attacker node is a legal node. This type of jamming is not easy to detect than the constant jammer since it transmits legal packets not just random ones. This type is energy inefficient because it keeps transmitting data continuously.

c. Random Jammer:

Random jammer transmits either regular packets like the deceptive jammer or random bite like the constant jammer into the network. But dislike the previous two mentioned types it tries to not exhaust the power energy by saving it. Random jammer has two main phases, the sleep phase and the second one is the jamming phase. This type keep switching between these two phases by sleeping for some time and after that it start jamming by becoming active. The time of the two phases depends on the jammer to decide it if it's fixed or random. This type of jamming has a trade off among energy saving during its sleep phase and jamming effectiveness during the jamming phase.

3.3.1.2 Reactive Jammer:

In this type the jammer begins to jam just when it senses that the network became active in some channels. This type of jamming can interrupt small packets and large ones. Reactive jamming monitors the network continuously so it's less power conserving than proactive jammer but it's harder to detect. Reactive jammer has the following two types.

a. Reactive Jammer type RTS/ CTS

This type of reactive jamming jams only when the jammer start sensing request to send (RTS) packets from the sender node, so as soon as the these messages are sensed in the channel, the attacker start to jam. By using this technique a clear to send (CT S) message will not be sent by the receiver because it didn’t receive the RTC packet due to the interference of the jammer that destroyed it. The sender in his turn will not send the data packets because it didn’t receive the CTS message from the receiver thinking that it is busy.

b. Reactive Jamming type Data /ACK

In this type the jammer interferes the transmission in the network of the data or even acknowledgment packets. The attacker will not be interfering the transmission until the data transmission starts. So, its main goal is to corrupt the data packets or it even corrupt the acknowledgment packets after it waits the data packets to reach its destination. So in both cases the node will keep retransmitting the data due to not receiving an acknowledgment from the receiver.

3.3.2.1 Function Specific Jammers

This type of jamming can choose either jamming single channel in order to preserve energy or it can choose to jam more than one channel at the same time so as to maximize the throughput of jamming. If the jammer chooses to jam single channel it can change the jammed channel along with their special functionality. The following are the main classification of this type of jamming.

a. Follow on Jammer

The attacker in this type jams all the obtainable channels very often for example, thousands of times per second, and the intruder jams every one for a small period of time. If the target node could detect these jammers and change its channel, the attacker will scan again all the band width searching for a new channel to jam. Because this jammer has great frequency hopping rate, it is efficient against many types of anti jamming techniques.

b. Channel hopping Jammer:

This attacker hops among diverse channels proactively. By superseding the Carrier Sense Multiple Access algorithm it access directly the channels. Also it can jam more than one channel at the same time.

c. Pulsed Noise Jammer:

The jammer in this type can change channels and jam each one at different times on different bandwidths. This type has two phases, on and off, in order to save energy. This type can jam more than one channel.

3.3.2.2 Smart Hybrid Jammers:

This type of jammers are efficient in jamming also power conserving, that why they are called smart. The major goal of this type is to increase its jamming effect in the targeted network. Also, they are power efficient. The following are the main classification of this type.

a. Control Channel Jammers:

This type of Jamming aims to target the control channel in the network, by control channel we mean the channel that organize networks operations. Random jammer can decrease network performance if it attacks the control channel. As for the constant jammer it causes denying of access in the network.

b. Implicit Jammer:

This type of jamming tries to stop the target functionality, causing Denial of Service condition to all nodes in the targeted network.

c. Flow Jamming Attacks:

The attacker use more than one jammers, it uses many jammers all over the network in order to reduce traffic flow when it jams the packet. This type uses the information that exists in the network layer.

3.4 Jamming Attack Detection Metrics

Jammer Main goal is to interrupt the wireless communications in the target network. It's done by either stopping the sender node in the network from sending its own

packets, or by stopping the receiver side from receiving the sent packet. The following are some basic method called metrics that are used to detect the jammer.

1. Signal to Noise Ratio (SNR):

This metric describes the ratio of the received signal power at a citrine sensor node to the received noise power [46] in the same node. It's a very effective metric used in order to recognize jamming attacks in the physical layer.

2. Bad Packet Ratio (BPR):

This type of metric describes the ratio between numbers of bad data packets received by the sensor node to the whole number of packets received to the same node in a given period of time [46]. This is also a very important metric that must be calculated during the transmission of packets because it can give an indication if there is a jamming attack. Its calculation is easy and simple due to the availability of the numbers of bad packets and the total received packets.

3. Packet Send Ratio (PSR):

This metric describes the ratio between the successfully sent packets by the legal nodes and the number of packets the node plans to send out the MAC layer [46]. This is also easy calculated by tracing the number of successfully sent and the packets that the node plans to send.

4. Packet Delivery Ratio (PDR):

This metric calculate the ratio between the successfully sent packets and the packet that are also successfully delivered to destination.

3.5 Jamming Detection Techniques and Algorithms

3.5.1. Jamming Detection for elementary jamming

As mentioned earlier, elementary jamming are categorized into two groups, the proactive jamming and the reactive jamming. In the first group, the jammer strangles the bandwidth to make the transmitter not capable of transmitting its own packets. As a result, jammers type can be detected using carrier sensing thresholds. After that, the jammed region will be able to be mapped by networks nodes and perform different activates in order to overcome the situation, like switching the channel, reroute the traffic and other actions. For the second group of elementary jamming, the jamming attacks aims mainly for the sender end side, in these situations, the jamming attacks can be detected by checking SNR, PDR and the received signal strength. These defense techniques and many others are discussed below for detecting elementary jamming attacks.

a. Jammed Area mapping protocol (JAM)

In [59] the authors developed a new algorithm for mapping out jammed region in the wireless sensor network (WSN) and give a rout outside the jammed area to rout its packets. This algorithm (JAM) can finish mapping the jammed area in about 1 to 5 seconds.

If the effectiveness dropped under a predefined threshold, then jammer presence is detected. After that, the detection system in each node gives an alert message if it's Jammed or un-jammed and send it to its own neighbor.

Once the nodes get the jammed message, it starts the procedure of mapping the jammed area. It starts by initiating a group that has its own group id also it has a normalized rout vector points to the node that emits jamming attacks. After that, the

nodes begin to aggregate the jammed messages in era of time called the announce time.

Following the expiring of the announce time, a new message called the Build message starts to be sent by the nodes to its own neighbours, this message have a group Id and the membership list. The node checks for compatibility by comparing the rout vector of group. The vectors combined with each other if they are compatible. After that build message is sent by the mapping nodes which contains the leading group id and also the combined member list. All the mapping nodes will update their own list after receiving a new build message.

If the jammer quit the network, an un-jammed message will be sent by the earlier jammed nodes to the neighbours. By getting this message, a teardown message will be sent to the nodes by the mapping nodes so as to reverse the membership possessions of the build message. After finishing the mapping procedure the transmitted message will go to a different rout in order to avoid the mapped area.

b. Ant system

In [60] the authors have proposed a new evolutionary method of detecting jamming attacks in the physical layer. The algorithm uses an agent in order to iteratively traverse the network. A new list is created called the tabu list used to save the information gathered like energy and distance by the previous agent in order to be used later for different routes to destination. This procedure is done to detect if there is a jamming or not.

Four sorts of jammers are being used, specific tone, numerous tone, pulsed noise and electronic intelligence (ELINT). Resources availability are essential to detect a node, resources like number of hops, distance, energy, SNR, PDR and packet loss.

After examining these resource metrics, they'll be put in a model called the decision model that is responsible for detecting whether there is a jamming or not. The output of this model could be in two forms based on an acceptance rate, high and that's means the jamming has accurse or false a one and that means there is no jamming been detected. The algorithm keeps calculating the metrics repeatedly to check if a jamming accurse or not. When the algorithm discovers a jamming attack in a particular rout, this rout will not be used by the nodes and they'll try to explore another one.

c. Hybrid System

A new anti jamming system has been proposed in [61], the authors combined three defense models, the base station replication, base station evasion and finally the multipath routing among base stations. The model suggested that the first model will present and introduce the network; the second model will point to the spatial retreat in the base station if a jamming accurse.

When there are more than one data rout among the node and the base station, the multipath routing starts functioning. These entire countermeasures models are used in case of jamming in the base station.

d. Channel surfing

This detecting technique affords migration for another channel when jamming accurse and blocks the communication used between the nodes for some channel [62]. On the other hand, after that a special technique called spatial retreat is used to deal with moving the nodes into another safe area in case they have been attacked by jamming attacks.

e. Packet Delivery Ratio (PDR):

In [63], the authors have proposed a new jamming detection model employing nodes location or using the signal strength consistency check with PDR determination.

Low PDR can cause jamming, but it is not only jamming, other factors can cause it too. To make sure that jamming isn't the one that is caused by low PDR, we use consistency checks. Once the PDR is dropped below the threshold, the consistency check will reactivate the signal strength. Signal strength will be high if PDR is high and vice versa, but this doesn't mean that a low PDR means low signal strength. The PDRs' neighbors will need to be checked if signal strength is high and PDR isn't. Jamming will not be found if this kind of situation occurs.

Regardless of what the PDR value will be, the proactive area will determine the location. A node checks the stability of its PDR with its neighbors in order to figure out its jamming status. If nodes nearby have low PDR, jamming will occur. But, if these nodes don't have neighbors, jamming will not occur.

f. Channel hopping:

Changing the channel (channel hopping) is the best neutralizer to jamming. The simplest thing to do is proactive channel hopping. The different kinds of channel hopping are explained in [66-73].

The corresponding channel in proactive channel hopping is changed at a specific timing. It happens whether jamming has occurred or not.

IEEE 80211n has a limited amount of orthogonal channels to hop Since it forces channel bonding to use 40MHz channels which will mean that channel hopping is a bad choice for jamming countermeasure in IEEE 802.11n networks. The obstacle of

proactive frequency hopping is the limited amount of orthogonal channels and the smaller frequency separation between channels [74]. Support the fact that if and only if and only if the numbers of orthogonal channels are large, frequency hopping will become an effective technique.

There is a slight difference to the simple proactive form which is a reactive scheme that depends on sensing a channel to detect jamming. A threshold value needs to be fixed. If accessing a channel's waiting time surpasses a given threshold value, jamming will be assumed and channel is changed to a different one. Otherwise, it will be chosen according to a pre-defined strategy or to a random one.

When a chosen channel from a set of the unused ones is being hopped onto, it is considered as straightforward channel hopping. The set of used and unused channels are included in the selection when it comes to the deceptive scheme. And for that, if the history of channel hopping is known by an attacker, it will jam the next channel easily by tracking the selected channel that was hopped onto. Among all the mentioned variations, pseudo random channel hopping scheme is the best one. It chooses channels that are unknown to jammers by using the pseudo number generation [69] A communication is switched to another channel is called an adaptive scheme. It does so ones every k slot- which is described as a fixed time interval.

Communication is switched back to the first channel after the packet delivery ratio (PDR) is computed for the channel that has been switched before. And when the present channel's performance falls below a threshold it will give the best PDR value because communications are switched to another channel. A code-controlled message-driven frequent hopping mechanism has recently been put forward by [72]. Each time a channel is changed, a dynamic hopping pattern is generated. In [72] the authors use a sequence coding technique called pseudo noise (PN). This technique

also helps detect jammed channels using spectrum sensing capabilities. The sender and receiver are the reason to this design. When nodes are able to sense the spectrum and the jammer is not that complicated, the hopping technique will become effective.

3.5.2. Detection and countermeasure of advanced jamming

The function-specific jammer and the smart-hybrid jammer are both in an advanced level. They combine proactive and reactive methods to jam a network as they use smart applications to save energy. This discussion is going to be all about the different types of anti-jamming techniques that have to do specifically with advanced jammers. For example, in Hermes node countermeasure against follow-on jammers, when using a control channel hopping sequence, the control-channel jammer will be seen as useless. Also, there is a multi-channel that defends against channel-hopping jammer called MULEPRO (MULti-channel Exfiltration PROtocol). The FIJI system disables complete jamming as the cross-layer approach fights against flow jamming.

a. Hermes node (hybrid DSSS and FHSS):

In [77] use the direct-sequence spread spectrum (DSSS) that uses a wider bandwidth to transmit signals and the frequency-hopping spread spectrum (FHSS) helps avoid any interference in order to defend jamming attacks by fast-following jammers for their corresponding processing gains. Hermes node is a hybrid DSSS and FHSS scheme that deals with jamming attacks in sensing networks. It performs 1,000,000 hops per second (FHSS) to get away from fast-following jammers. DSSS is for making attackers sense the data signals as white noise. This white noise stops attackers from sensing the communication radio band.

For the spread spectrum in DSSS, Hermes node uses 55 frequency channels for FHSS and 275 MHz of bandwidth in order to recover the original signal, the FHSS' frequency, and DSSS' pseudo noise (PN) code needs to be available. A secret word, which is more likely to be hard-coded for a particular network, is used for continuous reproduction of channel sequence and PN code. This is done in order that a new code getting in the network can be seen it the available nodes between other nodes. The sink will make the Hermes node work properly, which is very important.

b. Control channel attack prevention:

In a wireless network, the control channel adjusts channel usage where numerous channels are being used in order to expand the space within the network. In [78] introduce some clusters that avoid jamming. Each cluster keeps its own control channel with a particular hopping sequence. The control channel can be jammed within the highest level by taking information from a compromised node about the protocol procedures and cryptographic quantities. The evasion entropy measures a jammer's ability to decide the future control channel from the previously observed data.

The nodes that are compromised are determined by calculating the distance of the hopping sequence of the jammer and the actual one. The recognition of the nodes involved leads to the control channel that is being restored by using frequency hopping by updating the hopping sequence. The delay of the evasion measures the latency of the new control channel's successful restoration. The evasion ratio makes the communication available whenever jamming is present.

3.6 Anti-Jamming Countermeasures

This section present some of the main anti-jamming methods that deals with jamming attacks, these anti-jamming techniques are referred to them as countermeasures.

A. Regulated Transmitted Power

Usually sensor nodes try to minimize the used transition power in order to increase their life time power, since they are placed separated in an outside environment far away from the base station. Also minimizing transition power will reduce the probability of being discovered by the jammer as it must know the location of the sensor node before starting to jam. One of the used anti-jamming techniques is to increase the transition power as high as possible in order to increase the nodes confrontation against the intruder. The jammer happened to need a very strong signal to overcome the sensor nodes one. An important percentage of sensor nodes are used in modern WSNs (e.g., Sunspots [47] which hold the capability to alter the output power of their transmitter.

B. Frequency-Hopping Spread Spectrum

Frequency Hopping Spread Spectrum (FHSS) [48][49], is a very well-known and used method as anti-jamming technique. The main idea behind it is the rapid switching on the frequency channels among many.

This method has many advantages in the WSN:

- By switching among the frequency channels it works as an anti-jamming technique by reducing the intruder interception.
- By using larger range of frequencies to transmit data among the sensor node, Signal to Noise Ratio (SNR) is decreased.

- More than one WSN can work in the same area without interfering each other since each one hops to different frequency channel.

So, as mentioned earlier, this method has been used in many algorithms to decrease the jammer effect, although it has a major drawback of this technique that the needed bandwidth is a lot wider than the one needed to transmit the same data by using single one.

C. Directional Transmission

In general, WSNs use antennas that are omni-directional [53], Jamming tolerance in WSNs could dramatically improve because of the use of directional antennas [53]. Better protection are provided using directional antennas against jamming, the nodes receive or transmit data just from one specific direction, and that's the opposite of how the Omni-antennas work since they receive and transmit data at the same time in all the directions. Using the directional type provides better transmission performance and minimizes the interference from the outsiders like jammers. directional antennas suffers from main disadvantage, transmitting the radio waves into only one direction each time makes multipath routing a complex task to do.

4 Proposed Model

4.1 Algorithms Used In the Proposed Model

4.1.1 Frequency Hopping (FH)

When two nods are rapidly adjusted and connected by signal communication of FH radio, the receiver and sender define the sequence of a pseudorandom channel according to the following procedure:

1. The control channel receives a the transmitter's initiated demand

2. A seed (number order) is emitted by a receiver which may not match the point of the sender's one, therefore, the process won't be completed

3. This seed is used by a transmitter as algorithm number in a haphazard way to determine communication frequencies through a channel consequence.

4. The consequence of all channels has the same time to emit by a transmitter who considers the time of starting data transmission.

5. The transmitter and receiver, at the beginning of a communication simultaneously, consider a channel consequence to adjust frequencies suitably.

The authors in [82] takes a FH template to study its key features insisting on availability of filtration and un-foresee ability through a haphazard digits order; he also assures that the hopping template seed in a suitable linear span in a tiered number and channel efficiency emerge from a constant long-term distribution of channels frequency.

He states the fact that assures that the a hopping sequence detained fraction leads to inability to rebuilding it since the linear span, which has to be tiny and a tiered sequence, is huge. Whether FH template is slow or fast, every generator of a haphazard number has a similar number to that drawn according to an extent with proper features, this number has a varied frequency defining what kind of FH template is.

When the altered frequency level has much data than needed, a fast FH symbol will be transmitted on one more hop. Whereas it will be transmitted during a period of a hop channel in slow FH. The low switching time rate makes WSNs slow FH is sufficient in a system of single carrier when it consumes little energy in a transmission waveform. FH saves itself from jamming and confusion signal which is at the receiver regathered after its spreading.

A distinctive feature of FH is to object information that are interacted. As its signal received as a noise, there are two alternatives for eavesdropper to capture FH communication, pseudorandom consequence objection and pseudorandom consequence creation frequency band in FH template work with technologies applying wireless tool. An applicable bandwidth of FH signals resulted from creating a noise in communication of designated frequency

FH has two advantages, It has a preventive method when interfering channel frequency and advanced fading frequency. It is useless in thermal noise which is wideband. Boosting FH potential and processing interferers of narrowband require using channels of separated frequency which are close to one another and protect bands in between through removing constant interference or selectivity of frequency from a hop set for a while. The difference between FH and uncompounded system of

channels emerges when FH uses more a bandwidth for similar information than the other one which allows a bandwidth of active interference applied at urgent time to communication.

Accurate synchronizing both the transmitter and receiver, who simultaneously apply channels, is a must to start FH. When a demand of channels usage at a time for a transmitter whose data has to be comply with validity after they are examined by the receiver who selects the channel randomly to do this. These data mainly needs to process through nodes using reliable channel sequence charts for both a transmitter reciting existing channel place and network communication. This is one method.

The other method, applied according to this study, as follows: Accurate synchronizing periodically both the transmitter and receiver in algorithms to initially save frequency hopping

4.1.2 Code Division Multiple Access (CDMA)

The definition of CDMA: it is a group of applied methodical polices for second and third mobile generations, and wireless communications allowing a bandwidth utility improvement and channel transmission individually. Its proficiency of avoiding blocking with indefinite amplitude is considerable.

Modulation two types: DS direct sequence in which PSK signal phase is changed by the arrangement of pseudo-random and FH frequency hopping which is created through using PN sequence for transmitted signal frequency of PN.

Scrutinize two instances of modulation: PSK and FSK. If the pseudo-random (PN) arrangement at the modulator is applied to change the phase of PSK signal, the

resulting modulated signal is called a *direct sequence* (DS) spread spectrum signal. On the other hand, if the PN sequence is used to select the frequency of the transmitted signal pseudo-randomly, the resulting signal is called a *frequency hopping* (FH) spread spectrum signal

4.1.2.1 CDMA in Wireless Sensor Networks

CDMA is a methodical way through which the synchronized channel data is coded with PN. Its three elements:

1. Sending information needs much bandwidth for (a signal) to use.

2. PN code distributes unrestricted (data).

3. Synchronizing the transmitter PN code with recipient to coded data deciphered.

4. Different motives apply PN for a security nature and saving data..

5. PN comes to a recipient in order not randomly to rebuild contemporaneous examination code.

A signal for expanding energy is adjusted by Spread spectrum communication across a range of frequency wider than its bandwidth un-modulated through DS and FH.

The absence of root station creates hinders of WSN which depends on CDMA solutions, one of these hinders is that a terminal even its messages must have an appointed code according to a protocol assigned. Honestly, these hinders come the scene when we deal with vast networks (unlike small ones) which need a lot of

protocols of code assign leading to work done more functionally through examining whether the neighbors nodes have the same code.

Depending on what is mentioned before, collisions may happen in two forms: When the coding data resulted from utilizing the same PN by at least two nodes, there will be collision which is called main collision and has to be either diminished or subdued by competent protocol of code assignment. The previous protocol requires a topology control (algorithms) to be effective for both WSN and the other one (without algorithm) with WSN as a basis of CDMA .According to other form of collisions: Two nodes of CDMA, in a shape not synchronized, use PN codes not similar to each other, a collision here is unavoidable and called minor.

4.1.2.2 CDMA and FH

The transmission of spread spectrum signal requires an adjustment fundamentally done by FH-CDMA; a transmission of radio happens at the same time when FH-CDMA switches the frequency repeatedly.

It is a helpful tool decreasing jamming strength or telecommunications objection. A signal is permitted to be held by spread spectrum over a band frequency which is normally more than bandwidth required. The transmitter, hopping algorithmically frequencies used randomly or in an organized manner, dispersing energy over frequencies of channels band on a spectrum.

There is a synchronization of a transmitter working with a receiver which is responsible for core frequency tuned accurately. The narrowband where less burst data is implemented and tuned to a different frequency by the transmitter to retransmitted for the second time. A receiver’s capability of having frequency hopped

infinitely through an indicated bandwidth to transmit if correctly by hopping and transmitting another frequency respectively. DS-CDMA is a technique for spread spectrum and FH-CDMA's choice spreading data after being split over a sphere of frequency. Unlike FH-CDMA, the system of DS-CDMA is better in influence and cost, and is more practicable

4.1.3 Orthogonal Frequency Division Multiplexing (OFDM)

Orthogonality:

- OFDM is an expert FDM; carrier signals are orthogonal to one another Figure 3 shows the difference between OFDM and FDM.

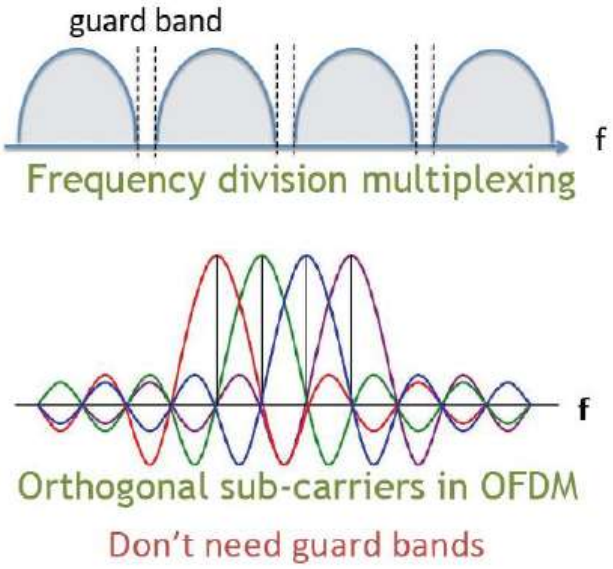

Figure 3: Difference between FDM and OFDM [85]

- The controversial discussion about the sub-channels is vanished and inter-carrier protecting bands are not needed.

OFDM is methodical convenient technology, against fading eclectic frequency, transmitting a course of a divided data high rated simultaneously into courses of ranks

over subcarriers to boost its rate and dissipation amount due to a reduction of spreading delayed multipath. A subcarrier spectrum's interference with spacing of a frequency base to be ranked in putting a subcarrier to one another in an orthogonal way. Indeed, it is splendid instance of transmission of so many carriers where a course of data over normal subcarriers simultaneously transmitted; one of them, a carrier's connotation in which user's course of data transmitted and received by a carrier regardless of time, transmission of a single carrier. However, when there are carriers for the previous process, it is called Multicarrier transmission.

OFDM advantages:

- **Inviolability to chosen fading:**

OFDM has much immunity to a chosen frequency fading than a system of one carrier does since the splitted channel into many signals on narrowband are accessible and influenced through branched channels faded.

- **Flexibility to interference:**

Channel Interference is not affected branched channels on restricted bandwidth to save the left data from being lost.

- **Spectrum competence**:

OFDM exploits spectrum dynamic utility when nipping up branched carrier implemented in nearer spaces.

- **Pliable to ISI**:

The OFDM pliability to symbol and interference frame in between for both because of data lowness rate on branched channels.

- **Simpler channel settlement**:

To avoid the settlement of channel complication (CDMA), OFDM gets simplicity of many branched channels and a settlement of channel.

OFDM drawback

- **Towering summit to normal power ratio**:

An amplifier RF, which has a narrow indigence and limited ability, is incompetent to operate at an extent because of a noisy signal of OFDM, dynamic ample extent, and variety in amplitude.

- **Sensitive to carrier offset and drift:**

An inaccuracy in target and substitute for frequency of one carrier system.

OFDM is a procedure of adjusting multi-carrier by implementing the information of data according to subcarrier one. It is strong to process a prevalence of channel and facilitates a channel phase to be estimated. Moreover, it is competent to an interference of symbol in between resulted from channel dispersion (83). Dividing the stream ratio data through the system of OFDM into other streams equally so that a design of adjustment is used for each one. Even adjusting symbols to minor carriers by IDFT which alter a symbol of OFDM through a specific frequency. However,

IFFT does the same process as the previous procedure but with effective ability; the symbol of OFDM converted digitally or analogously (DAC = digital to analogue converter): it processes a signal in analogous baseband to convert this into a digit (in the receiver). Before examining the data, instances departed the interval which is defended to be fed through DFT, and changed according to defined frequency [83-85]. Figure 4 shows how OFDM transmit data and how the receiver deals with received data.

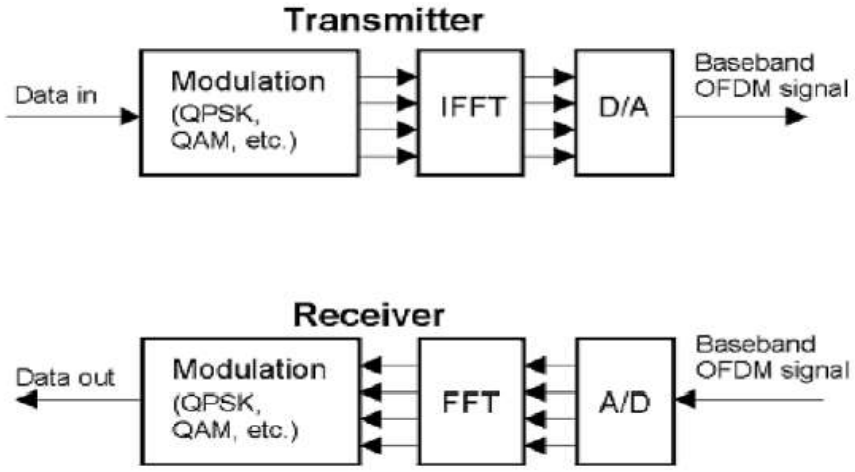

Figure 4: OFDM Transmitter and Receiver [84]

4.1.3.1 OFDM and CDMA

It encircles many multi-path interference happen in a broadband channel by applying various low symbol rate sub-carriers and by making full application of the frequency multiformity result using the dispense and coded signals over similar sub-carriers. Although OFCDM obtain better throughput performance in a broadband channel, it suffers from the reduction caused by inter-code interference due to loss of orthogonality among code multiplexed channels. So dispreading the signal in

frequency domain is a key technique in order to compensate for the devastation of orthogonality

4.1.3.2OFDM, CDMA and FH

This hybrid method is formed of a straight consequence altered signal that its main frequency is prepared to hop chronologically in a pseudorandom manner. This guarantees that, even within the same cell, no two mobiles are operating at the same frequency. There was, however, an industrial request for very high bit rates, regardless of the style of access plan applied. This gave an increase to OFDM systems. In such systems very lofty data rates are adjusted to very low similar data rates using a sequence-to similar converter. This guarantees vast fading for all the sub-carriers.

4.2 System Model For DS-CDMA/OFDNM/FH [86]

The overall block diagram of DS-CDMA /OFDM/FH system is shown in Figure 5.

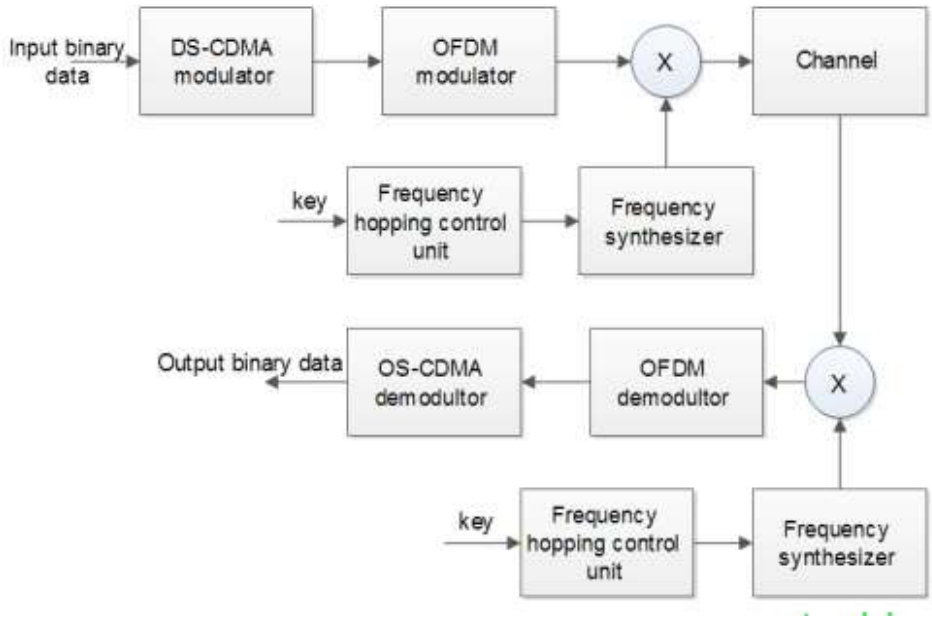

Figure 5: Block Diagram of DS-CDMA /OFDM/FH System

The generation of DS-CDMA /OFDM/FH signal can be considered as three sequential steps as shown in Figure8. The input binary data is first spread with a unique spreading code of length N and when applied to OFDM modulator which uses multiple subcarriers, equal in number to the length of the spreading code. The output of the OFDM modulator is applied to frequency hopping section which consists of multiplier, frequency synthesizer and frequency hopping control unit.

There are few points to be noticed:

4.2.1 Bandwidth and number of OFDM sub-channels

Orthogonal frequency-division multiplexing (OFDM) has been used in this model in order to increase number of sub-channels in the 2.4 band that is been used in the WSN,

as shown in Figure 6 the IEEE 802.15.4 has a standard division for the used channel. The number of sub-channels that IEEE proposed is 16 sub-channels, and channels capacities are defined as 2 MHz for each.

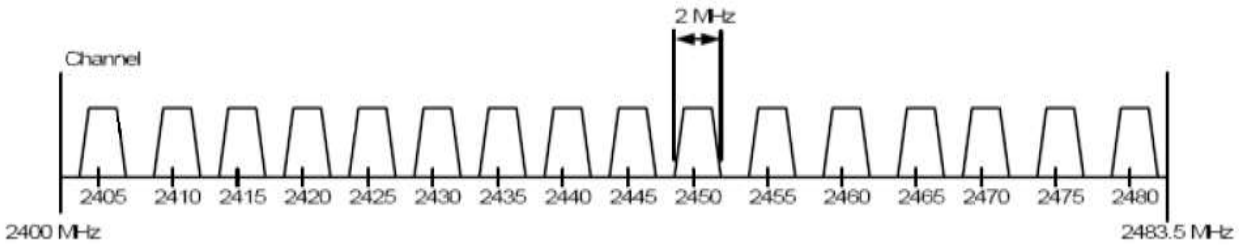

Figure 6: IEEE 802.15.14 Channel Selection

OFDM divides the channels into many sub-channels that are orthogonal to each other Figure 7 shows how sub channels are orthogonal in OFDM; previously the division of the channel was done using normal FDM, which caused using lots of guard bands in order to prevent interference between transmitted signals. By using OFDM we can double the number of channels of original FDM and by this we save great bandwidth and spectral effectiveness in addition mitigatation ISI and delay.

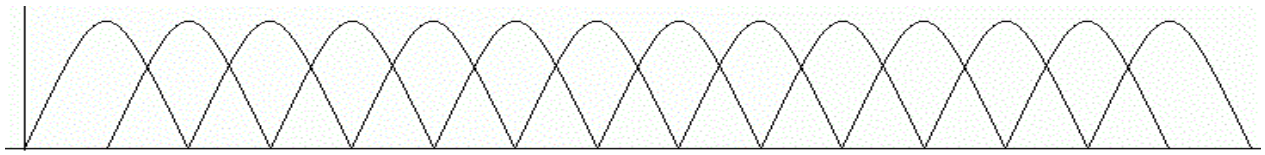

Figure 7: Orthogonal Sub-Channels

In case of frequency hopping that is been used to avoid jamming, 16 channel to hope among them have large probability to be exposed by the jammer, so probability P for jammer to guess the used channel will be $P=\frac{1}{\text{number of channels}}$, in IEEE case $P=\frac{1}{16} \cong$ 0.06, this number make lots of troubles during data transmission and makes lots of data loss. To overcome this issue our proposed model aims to minimize P to minimum in order to increase the complexity of our suggested anti-jamming technique by

increasing number of channels. In order to achieve this goal we employed OFDM, and we decrease the capacity of each sub-channel to satisfy the required data transmission rate in most WSNs.

In our proposed work, we are interested in the unlicensed frequency band (2.4 GHz-2.5 GHz) with a total bandwidth of 100 MHz. The number of OFDM sub-channels is determined by the channel coherence bandwidth (Bc) which in turn is determined by the rms delay spread (Trms). Suppose that the rms delay spread Trms =0.266 ms which is suitable for open area and suburban area.

The coherence bandwidth is determined as:

$$Bc=\frac{1}{5\ Trms} \qquad (1)$$

$$Bc=\frac{1}{5 \times 0.266} = 750\ KHz$$

Usually the OFDM sub channel bandwidth (Bsc) is much less than the coherence bandwidth

$$Bsc << Bc \qquad (2)$$

$$Bsc \approx 0.1\ Bc$$

$$Bsc = 0.1 \times 750\ KHz = 75\ KHz$$

Suppose the signal to noise ratio ($\frac{S}{N}$) is equal to 0.8, then according to Shannon capacity theorem, the channel capacity (C) is determined as:

$$C=BW \log2 \left(1+\frac{S}{N}\right) \qquad (3)$$

$$C= 75\ KHz \log2 (1+0.8) = 64\ Kbps$$

The number of sub channels for sub carriers (Nsc) is equal to:

$$Nsc= \frac{100\ MHz}{75\ KHz} \cong 1328 \text{ sub channels}$$

In our work we will take the Nsc= 1024 for data because according to IFFT, the number of IFFT points must be equal to a number that is a power of 2.

The rest of sub-channels will be divided as shown in Figure 8, 256 sub-channels will be used as control channel and the rest will be left without particular use as guard channels in case of interference while transmitting high data rate. The sub channels are not fixed, for example, data can be transmitted at any channel from the 1327 sub-channels but number of channels that is used to transmit data mustn't exceed 1024 sub-channels.

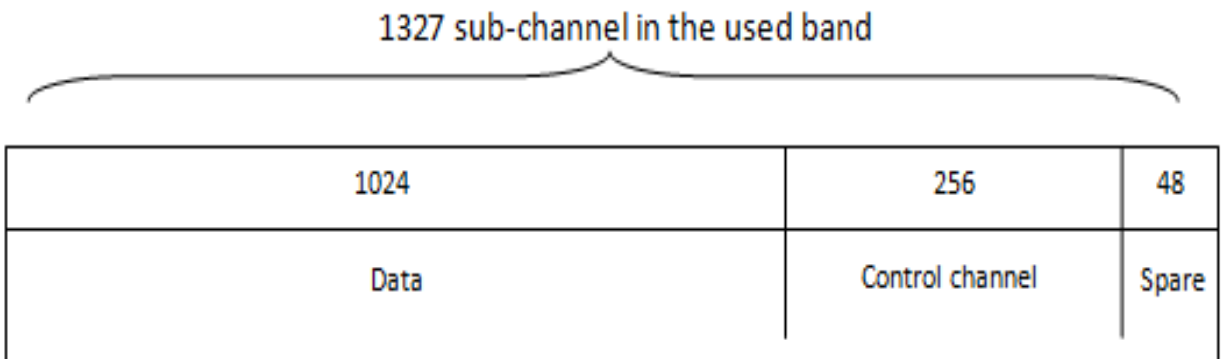

Figure 8: Set of Used Frequencies

4.2.2 Modulation

In our case, the CDMA sequence is modulated in the OFDM transmitter as M-QAM or any other type of modulation. CDMA multiplexing technique is used to make large number of users access the network in the same time by giving each user a unique code sequence called pseudo noise (PN), this code will be like a signature for any transmitted data bit. This technique doesn't divide the transmission according to time or other methods; instead the division will be using the assigned code for each user. The code is transformed in a wide band signal collecting user's signals. The user code is used to extract the user's signal from the wide band signal, in order to recover his data.

CDMA suffers mainly from near-far problem where the signal travels in different paths in order to reach the destination, but combining it with proposed FH technique

solves this problem. This makes sure that there are no two sensors operating in the same frequency.

Since jamming attacks may have different levels of complexity we adapt our proposed model to deal with all jamming levels. In CDMA technique we suggest using different Walsh code size where each bit of data will be sent along with the used code. Size of Walsh code depends on the level of jamming, suggested model divides the jamming attack level into four categories: low jamming level (J_0), medium jamming level (J_1), high jamming level (J_2) and very high jamming level (J_3). Where we use 8, 16, 32 and 64 bits sequentially Walsh code on each data bit takes. Number of sub channels (NSC) needed to transfer data throughput of 8 Kb/s will be defined according to the following Equation 4.

$$NSC = \frac{\text{data T} \times \text{chips}}{\text{SC}} \qquad (4)$$

Such that

Data T = 8 Kb

Chips= number of Walsh code bits will be used according to the jamming level

SC= Sub channel bandwidth and it equals 64 Kb/s

For example, if the network suffered from jamming attack from level j_3, number of sub channels needed to transfer 8 Kb/s will be= $\frac{8 \times 64}{64}$ = 8 sub- channels

4.2.3 Frequency Sequence Generator

Stringent synchronization is still needed as the PN order significance to be completely coincided. However, in such instances, the load of synchronization is converted to the OFDM system. The OFDM system has a more complicated synchronization system than the CDMA. According to this, the OFDM system uses the cyclic prefixes for synchronization. Therefore, the PN sequences springing from the OFDM system and

shifting on to the CDMA system are coincided more precisely than in case of a clear CDMA system. It is realized that synchronization is one of the defining elements in CDMA systems for gaining high data rates. It is predicted that in our intended system, such crucial problems will be effectively minimized.

Synchronization is achieved by using cyclic prefix in OFDM modulator. In order to generate frequencies, a random number generator (RNG) has been used; it generates a sequence of numbers that represents sub-channels, which are used in order to hope among the frequencies. Every channel band width will be given a number from {0,1,2, …., 1327}, taking into consideration that our suggested bandwidth will be 75KHz, so number 0 will express the 2.400 MHz channel bandwidth, number 1 will express the 2,400075 MHz channel bandwidth and so on. Each number will be converted into carrier i using the following Equation 5.

$$\text{Carrier } i = i * f_0 + \text{base} + \frac{f0}{2} \qquad (5)$$

Such that

i: the output number from the random number generator

f_0: 75 KHz, sub-channel bandwidth

Base: 2.4 MHz

At the beginning a special key that exists in each authorized node is used to generate the initial frequency sequence using the random number generator, when all frequencies in the sequence is used, the synch node sends a new seed to be used as an input instead of the key for the RNG as shown in Figure 9.

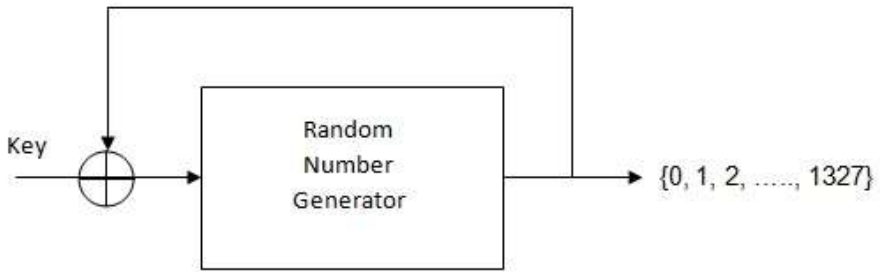

Figure 9: Frequency Generator

In order to deal with the case of repetitions among the output numbers, the following steps are done:

- After the sequence is generated each node checks the sequence numbers
- It fills 1's inside an array, each number on its place, and fills the missing number places with zero.
- After arranging the array with zeros and ones, it lays each number from the sequence on its order.
- Whenever it sees a duplicated number that is already exists it replace it with the first missing number from the array, then the second and so on.

Synchronization is mainly needed when we add a new node to the WSN, adding a new node to the network will make confusion to the new node since the used frequency is not fixed and the nodes keep hopping among the channels.

Using the random number generator and a special key that exists in each authorized node as shown in Figure 9, any new node can guess the frequency hopping sequence and it will start transmitting data on the right channel as soon as it implemented in the network.

4.2.4 PERFORMANCE EVALUATION

4.2.4.1 Performance of the hybrid DS-CDMA/ OFDM/ FH system

The proposed system is essentially an OFDM-FH system. This is because the transmission and reception is carried out by the OFDM-FH system. The DS-CDMA component only generates data stream, but in more complex way.

Advantages:

• Anti multipath capability.

• Multiple access due to FH needs very wide bandwidths relying upon a number of users.

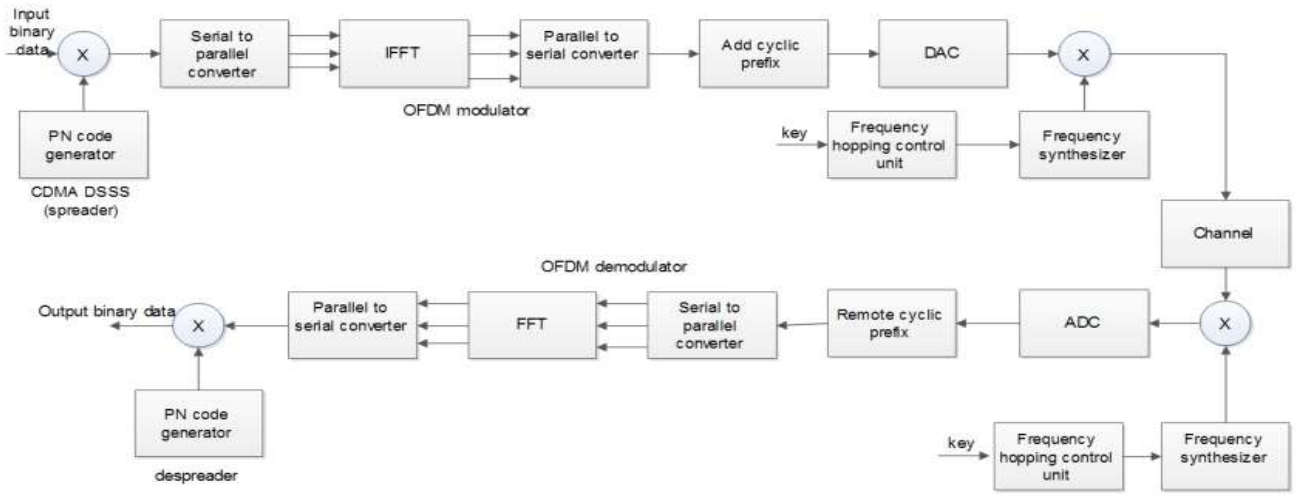

Figure 10: Block Diagram of the Proposed System

The Final proposed model is illustrated in Figure 10; this figure shows in detail how our system works using the three models of CDMA, OFDM and FH.

The core of CDMA system is the spread spectrum method, which uses high data rate pulses in order to improve the signal bandwidth for the used data rate. Spreading is achieved by using a spreading sequence of pseudo random signs that we call the

pseudo noise (PN) code. These codes are used to differentiate different users, so orthogonality is needed to avoid interference between the users.

After that the joint data with the PN code from CDMA model enters OFDM model. The input data is derived to serial to parallel converter in order to convert the high rate data symbol into parallel low rate sub stream before spreading the data symbols on each sub channel with a user specific spreading code. After that, the parallel output from the serial to parallel convertor block goes as input to the inverse Fourier transform (IFFT) block to produce the OFDM symbol,

After computing the IFFT, the complex output of the IFFT block are sent to the parallel to serial convertor block P/S, which is used to convert computation result which is in parallel to serial before being sent to other module for processing. The output from P/S block is inserted into the cyclic prefix block to resist the inter-symbol interference (ISI) and inter carrier interference (ICI) that is caused by the multipath channel.

Lastly, the output of the cyclic prefix block goes as input to the digital to analog convertor (DAC) block. The output of the last block will be combined with the frequency synthesizer and sent to the antenna for transmission.

As for the receiver side, First of all the received signals will be converted by the analog to digital converter (ADC). After that, remote cyclic prefix convolution will remove the cyclic prefix and the rest of the signals are sent to as an input to the serial to parallel convertor. Then FFT block performs demodulation so as to achieve the transmitted symbols with the amplitude. The output of the FFT block goes to the final block the parallel to serial convertor in order to obtain the final output bit stream.

5. Simulation and Final Results

In this chapter, we have simulated the proposed model in order to find the "Matching Percentage" and the probability of jammer to hit the used channels.

The main goal of the proposed model is to minimize the matching probability to as possible in order to minimize the affected amount of data transmitted in each channel which preserve the WSN transmission environment and bandwidth.

Our simulation is evaluated in a condition where an intruder is trying to catch used channels all the time. This work focuses on preventing the intruder/ jammer from catching any used channel by our system.

We design our own system using C# in order to verify the correctness of our proposed system and we consider this is sufficient as we are focusing on probability and randomness as they are can be implemented and tested in C#.

In order to achieve our goal we have generated two large datasets of random frequencies, the first one is a jammer and the second is our system dataset which is a key dependent.

The simulation is done to achieve the following:

1) The Matching Percentage of the proposed model and all the possible channel number.

2) The difference between Matching Percentage in fast hopping and Matching Percentage in slow hopping.

Our proposed model focused on the idea of preventing all jammers types from accessing the network regardless of the used mechanism by the jammer in order to interrupt our signal. The main idea was to increase number of channels without affecting the data bandwidth.

The simulation was done by generating two data sets that are random, for our own system and for the jammers; our own data set depends on a secret key that can be changes by the user. We built a special random number generator that doesn't repeat any number among the channels numbers, each number represents a sub-channel as we mentioned earlier.

After generating the two data sets a comparison was done to calculate the matching percentage between the jammers set and our own set which are both random sets and we assumed that the jammer also has the same number of channels.

IEEE 802.11 use number of channels that are usually equal to 16, most of the proposed works that use frequency hopping mechanism divides the channels into 16 channel and hop among them. Using a small number of channels hopping increases the probability of being hit by the jammer. Table2 shows a comparison analysis between different channel number and their Matching percentage.

As shown, the matching percentage of techniques that divides the whole channel into a 16 channels in order to hop between them have a higher probability of being hit by a jammer, every ten hops the jammer catch one channel of them. Mean while our proposed method which uses 1327 channels has the least chance to of being caught by the jammer, The probability of being hit by a jammer in average is 0.003 which is three channels from every 1000 Channels. As a result the chance of being hit by the jammer is reduced. In addition the proposed model uses CDMA technique to overcome this situation even if the jammer catch accidentally on of used channels, data will not be lost and the users will continue to work properly without any loss or interference. The table 2 shows the matching percentage while we increase the number of channels used.

Table 2: Comparison between channels number and matching percentage

channels number	Matching Per.
16	0.1014813
32	0.05112656
64	0.02846719
128	0.01656875
256	0.009967187
512	0.005917285
1327	0.003212671

Hopping among the frequencies can be divided into two categories, fast hopping and slow hopping. The jammer can use any type of them in order to catch the used frequency. Since our hopping sequence is randomly chosen between all channels, we supposed that also the jammer is randomly hopping to the same number of channels that we proposed. This step was done in order to calculate the Matching Percentage at its worst case. So we also supposed the ability of the jammer to change his status from slow hopping mode which compares one of his channels with only one user channel to status where the intruder can compare from 1 to 8 channels each channel from the user side. At first when the jammer use slow hopping the matching percentage is 0.003 but when we rise the hopping speed of the jammer the matching percentage increase to reach 0.023.

Table 3: Matching percentage for our proposed model

Hop speed	channels number	Matching Per.
1	1327	0.003212671
2	1327	0.006252542
3	1327	0.009040462
4	1327	0.01195873
5	1327	0.01471519
6	1327	0.01737708
7	1327	0.0200445
8	1327	0.02274638

The tables 4 shows the Matching Percentages with jammer where channels number are 16, 32, 64, 128, 256, 512. The hop speed increased in order to show the matching percentage differences between slow and fast hopping and how they affect our proposed countermeasure. As seen from the tables our proposed model has the least matching percentage and this is considered acceptable as the second level of protection (CDMA) will eliminate the effect of jammed frequencies even if the jammer hopping speed dozens of times faster than the hopping speed of our proposed system.

Table 4: Matching percentage for 16,32,64,128,256 and 512 sub cahnnels

Hop speed	Matching Per. for 16 sub channel	Matching Per. for 32 sub channel	Matching Per. for 64 sub channel	Matching Per. for 128 sub channel	Matching Per. for 256 sub channel	Matching Per. for 512 sub channel
1	0.1014813	0.05112656	0.02846719	0.01656875	0.009967187	0.005917285
2	0.18305	0.1003172	0.05448125	0.03157422	0.01905352	0.01145586
3	0.2710187	0.1415516	0.07816875	0.04440469	0.02695391	0.01633174
4	0.3174094	0.1797688	0.1000953	0.05811445	0.03536777	0.02162744
5	0.4592719	0.2307844	0.1198336	0.07057422	0.04303496	0.02626885
6	0.483875	0.2767391	0.1434922	0.08444805	0.05036445	0.03116523
7	0.638475	0.3044	0.172482	0.09687969	0.05777773	0.03587402
8	0.5606625	0.3148219	0.1802352	0.1061133	0.06481699	0.04035849

Finally, we showed in table 5 a comparison between different suggested channel numbers and our proposed model in fast hopping mode, where the jammer hopping speed is 8 times faster than the users hopping speed. The IEEE standard divisions of channels that divide them into 16 channels have a very dangerous probability of being caught by a jammer that reaches at almost 6 out of 10 channels. The matching Percentage decrease while we increase the channel number. Our proposed number of channel have the minimum matching percentage among them all, taking into consideration the right bandwidth that have been carefully calculated.

Table 5: Fast hopping comparison

Channel number	Matching Per.
16	0.5606625
32	0.3148219
64	0.1802352
128	0.1061133
256	0.06481699
512	0.04035849
1327	0.02274638

5.1 Conclusion and Future Work

We proposed a model that integrates CDMA/OFDMA/FH in order to increase jamming resistance; we extend the number of used frequencies by reducing the sub-channels bandwidth to 75 KHz which is sufficient in many applications for WSN. As a result we achieved 1327 sub-channels that can be used during the frequency hopping which make it very difficult for jammer to predict the used frequency during data transmission. We developed a frequency generator which is key dependent that enables the nodes to synchronize and coordinate frequencies.

Our simulation results showed that our proposed model minimize jamming probability to 0.003 mean while the most used models have a probability of being jammed reaches 0.1 which is very high. Also our simulation results showed the difference between jamming hit probability in fast and slow hopping and a comparisons between different channel numbers are done .

In future work we will enhance our proposed model to be able to minimize the jamming probability and increase the channel bandwidth to be able to handle multimedia data.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[2] A. Bagula, M. Zennaro, G. Inggs, S. Scott, and D. Gascon, “Ubiquitous Sensor Networking for Development (USN4D): An Application to Pollution Monitoring,” Sensors, vol. 12, no. 1, pp. 391–414, Jan. 2012.

[3] J. Jeong and Z. J. Haas, “An integrated security framework for open wireless networking architecture,” IEEE Wireless Communications, vol. 14, no. 2, pp. 10–18, 2007.

[4] X. Guo and J. Zhu, “Research on security issues in Wireless Sensor Networks,” in 2011 International Conference on Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011, vol. 2, pp. 636–639.

[5] A. Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks,” Communications of the ACM, vol. 47, no. 6, p. 53, Jun. 2004.

[6] C.-Y. Chong and S. P. Kumar, “Sensor networks: evolution, opportunities, and challenges,” Proceedings of the IEEE, vol. 91, no. 8, pp. 1247–1256, Aug.

[7] W. D. O’Neil, “The Cooperative Engagement Capability (CEC)Transforming Naval Anti-air Warfare,” the Center for Technology and National Security Policy, the National Defense University,, U.S.A, Case Studies in National Security Transformation 11, Aug. 2007.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Communications Magazine, vol. 40, no. 8, pp. 102– 114, Aug. 2002.

[9] A. Hoskins and J. McCann, “Beasties: Simple wireless sensor nodes,” in 33rd IEEE Conference on Local Computer Networks, 2008. LCN 2008, 2008, pp. 707–714.

[10] D. Li, K. D. Wong, Y. H. Hu, and A. M. Sayeed, “Detection, classification, and tracking of targets,” IEEE Signal Processing Magazine, vol. 19, no. 2, pp.17 –29, Mar. 2002.

[11] C. Meesookho, S. Narayanan, and C. S. Raghavendra, “Collaborative classification applications in sensor networks,” in Sensor Array and Multichannel Signal Processing Workshop Proceedings, 2002, 2002, pp. 370 – 374.

[12] T. He, S. Krishnamurthy, J. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, and L. Gu, “Energy Efficient Surveillance System Using Wireless Sensor Networks,” presented at the The 2nd Annual International Conference on Mobile Systems, Applications and Services (MobiSys), 2004.

[13] B. Sinopoli, C. Sharp, L. Schenato, S. Schaffert, and S. S. Sastry, “Distributed control applications within sensor networks,” Proceedings of the IEEE, vol. 91, no. 8, pp. 1235 – 1246, Aug. 2003.

[14] P. Sikka, P. Corke, P. Valencia, C. Crossman, D. Swain, and G. Bishop- Hurley, “Wireless ad hoc sensor and actuator networks on the farm,” in The Fifth International Conference on Information Processing in Sensor Networks, 2006. IPSN 2006, 0-0, pp. 492–499.

[15] F. Zhao, “Wireless sensor networks: a new computing platform for tomorrow’s Internet,” in Proceedings of the IEEE 6th Circuits and Systems Symposium on Emerging Technologies: Frontiers of Mobile and Wireless Communication, 2004, 2004, vol. 1, pp. I – 27 Vol.1.

[16] R. Mulligan and H. M. Ammari, “Coverage in Wireless Sensor Networks: A Survey,” Network Protocol and Algorithms,, vol. 2, no. 2, pp. 27–53, 2010.

[17] M. Ahmed, X. Huang, D. Sharma, and H. Cui, “Wireless Sensor Network: Cherecterestics and Architectures,” in World Academy of Science, Engineering and Technology, Penang, Malaysia, 2012, vol. 72, pp. 660–663.

[18] C. Buratti, A. Conti, D. Dardari, and R. Verdone, “An Overview on Wireless Sensor Networks Technology and Evolution,” Sensors, vol. 9, no. 9, pp. 6869–6896, Aug. 2009.

[19] J. Feng, F. Koushanfar, and M. Potkonjak, “Sensor Network Architecture,”Computer Science Department, University of California,, Los Angeles, U.S.A, Research Report for National Science Foundation, Grant No. ANI-0085773, 2005.

[20] 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.

[21] C.Y. Chong, and S.P. Kumar, “Sensor Networks: Evolution, Opportunities, and Challenges”, in Proc. IEEE, vol. 91, no.8, August 2003.

[22] J.W. Gardner, V. K Varadan, and O. O. Awadelkarim, “Microsensors, MEMS and Smart Devices”, New York: Wiley, 2001.

[23] R. Hills, “Sensing for danger”, Science Technology Rep. July/Aug. 2001. [Online] Available: http://www.llnl.gov/str/JulAug01/Hills.html

[24] D. Jensen, “SIVAM: Communication, navigation and surveillance for the Amazon”, Avionics Mag., June 2002. [Online]Available: http://www.aviationtoday.com/reports/avionics/previous/0602/0602sivam.html

[25] J. A. Stankovic, Q. Cao, T. Doan, L. Fang, Z. He, R. Kiran, S. Lin, S. Son, R. Stoleru, A. Wood, “Wireless Sensor Networks for In-Home Healthcare: Potential and

Challenges", in High Confidence Medical Device Software and Systems (HCMDSS) Workshop, June 2-3 Philadelphia, PA, 2005.

[26] R.R. Brooks, A.M. Sayeed, "Distributed Target Classification and Tracking in Sensor Networks", Proc. IEEE, vol. 91 (8), pp. 1163-1171, August 2003.

[27] L. Ran, S. Helal, S. Moore, "Drishti: an integrated indoor/outdoor blind navigation system and service", in Proc. Second IEEE Annual Conference on Pervasive Computing and Communications (PerCom 2004), pp. 23-30, 14-17 March 2004.

[28] S.Ram and J. Sharf, "The people sensor: A mobility aid for the visually impaired", in Second International Symposium on Wearable Computers, Digest of Papers, pp. 166-167, 1998.

[29] K. Chelli, "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures," Proceedings of the World Congress on Engineering 2015, vol. I WCE 2015, July 1-3, 2015, London, U.K.

[30] S. Patil, V. Kumar B P, S. Singha, and R. Jamil, "A Survey on Authentication techniques for Wireless Sensor Networks," International Journal of Applied Research, ISSN 0973-4562, vol. 7, no.11, 2012.

[31] Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference (Vol. 2, pp. 6-pp). IEEE..

[32]. N Alajmi, „WSN attacks and solutions" International Journal of Computer Science and Information Security, Vol. 12, No. 7, July 2014

[33]. Abhishek Jain, Kamal Kant, and M. R. Tripathy, "Security Solutions for Wireless Sensor Networks", to appear in IEEE ICACCT 2012.

[34]. Mayank Saraogi, “Security in Wireless Sensor Networks”, University of Tennessee, Knoxville.

[35]. D Buch, D. C. Jinwala, „Denial os service attcaks in WSN“ INSTITUTE OF TECHNOLOGY, NIRMA UNIVERSITY, AHMEDABAD – 382 481, 09-11 DECEMBER, 2010

[36]. P Rolla, M Kaur,“Review of prevention technique for DoS attacks in WSN“ NTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 5, ISSUE 07, JULY 2016

[37] Vashisht, E. H., Bharadwaj, S., & Sharma, S. (2018). Analysis of DoS attack in various layers of Wireless Sensor Network.

[38] O. Althobaiti, M. Al-Rodhaan, and A. Al-Dhelaan, “An Efficient Biometric Authentication Protocol forWireless Sensor Networks,” *International Journal of Distributed Sensor Networks*, v. 2013, Article ID 407971, 13 pages.

[39] M. A. Khan, G. A. Shah, “Muhammad Sher "Challenges for Security in Wireless sensor Networks (WSNs),” *International Journal of Computer and Information Engineering,* vol. 5, no. 8, 2011

[40] Gunda, P., & Boyapati, R. (2018). ANTI-JAMMING STRATEGY FOR WIRELESS NETWORK.

[41] Jaitly, S., Malhotra, H., & Bhushan, B. (2017, July). Security vulnerabilities and countermeasures against jamming attacks in Wireless Sensor Networks: A survey. In *Computer, Communications and Electronics (Comptelix), 2017 International Conference on* (pp. 559-564). IEEE.

[42] Grover, K., Lim, A., & Yang, Q. (2014). Jamming and anti-jamming techniques in wireless networks: A survey. *International Journal of Ad Hoc and Ubiquitous Computing*, *17*(4), 197-215.

[43] Osanaiye, O.; Choo, K.K.R.; Dlodlo, M. Distributed denial of service (DDoS) resilience in cloud: Review and conceptual cloud DDoS mitigation framework. J. Netw. Comput. Appl. **2016**, 67, 147–165. [CrossRef]

[44] Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. Denial of service attacks in wireless networks: The case of jammers. IEEE Commun. Surv. Tutor. **2011**, 13, 245–257. [CrossRef]

[45] Grover, K., Lim, A., & Yang, Q. (2014). Jamming and anti-jamming techniques in wireless networks: a survey. International Journal of Ad Hoc and Ubiquitous Computing, 17(4), 197-215.

[46] Gunda, P., & Boyapati, R. (2018). ANTI-JAMMING STRATEGY FOR WIRELESS NETWORK.

[47] SunSpotWorld. https://www.sunspotworld.com/

[48] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein, "Theory of spread spectrum communications-a tutorial", IEEE Trans. Commun., vol. 20, no. 5, pp. 855-884, 1982.

[49] FHSS-wikipedia.http://en.wikipedia.org/wiki/Frequency-hoppingspread-spectrum

[50] A.F Mohammed, "Near-far problem in direct-sequence code-division multiple-access systems", in Proc. 7th IEEE European conference on Mobile and Personal Communications, pp. 151-154, 1993.

[51] UWB-wikipedia. http://en.wikipedia.org/wiki/Ultra wideband.

[52] I. Oppermann, L. Stoica, A. Rabbachin, Z. Shelby, and J. Haapola, "Uwb wireless sensor networks: Uwen- a practical example", IEEE Communications Magazine, vol. 42, no. 12, pp. 27-32, Dec. 2004.

[53] W. Stutzman and G. Thiele, "Antenna Theory and Design", (2nd edition), John Wiley & Sons, 1997.

[54] C. S. R. Murthy and B. S. Manoj. “Transport Layer and Security Protocols for Ad Hoc Wireless Networks”, in Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall PTR, May 2004.

[55] A. Spyropoulos and C. S. Raghavendra. “Energy Efficient Communications in Ad Hoc Networks Using Directional Antennas”, IEEE Conference on Computer Communications (INFOCOM’02), NY, USA, June 2002.

[56] S. Bandyopadhyay, K. Hasuike, S. Horisawa, S. Tawara, “An Adaptive MAC and Directional Routing Protocol for Ad Hoc Wireless Network Using Directional ESPAR Antenna”, in Proc. ACM Symposium on Mobile Ad Hoc Networking & Computing 2001 (MOBIHOC 2001), Long Beach, California, USA, October 2001.

[57] Y. Li, H. Man, “Analysis of multipath routing for ad hoc networks using directional antennas” Vehicular Technology Conference, IEEE 60th, vol. 4, pp. 2759 - 2763, September 2004.

[58] F.B. Gross, “Smart Antennas for Wireless Communications with Matlab”, McGraw-Hill, 2005.

[59] Wood A, Stankovic J, Son S (2003) JAM: a jammed-area mapping service for sensor networks. In: 24th IEEE Real-Time Systems Symposium, pp 286–297

[60] Muraleedharan R, Osadciw LA (2006) Jamming attack detection and countermeasures in wireless sensor network using ant system. In: SPIE the International Society for Optical Engineering, vol 6248, p 62480G

[61] Jain SK, Garg K (2009) A hybrid model of defense techniques against base station jamming attack in wireless sensor networks. In: Proceedings of the 2009 First International Conference on Computational Intelligence, Communication Systems and Networks, pp 102–107

[62] Xu W, Wood T, Trappe W, Zhang Y (2004) Channel surfing and spatial retreats: defenses against wireless denial of service. In: Proceedings of the 3rd ACM Workshop on Wireless Security, pp 80–89

[63] Xu W, Trappe W, Zhang Y, Wood T (2005) The feasibility of launching and detecting jamming attacks in wireless networks. In: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp 46–57

[64] Misra S, Singh R, Mohan SVR (2010) Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system. Sensors 10:3444–3479

[65] Thamilarasu G, Sridhar R (2009) Game theoretic modeling of jamming attacks in ad hoc networks. In: Proceedings of 18th Internatonal Conference on Computer Communications and Networks, pp 1–6

[66] Khattab S, Mosse D, Melhem R (2008a) Jamming mitigation in multi-radio wireless networks: Reactive or proactive? In: Proceedings of the 4th International Conference on Security and privacy in communication netowrks, pp 27:1–27:10

[67] Khattab S, Mosse D, Melhem R (2008b) Modeling of the channel-hopping anti-jamming defense in multi-radio wireless networks. In: Proceedings of the 5th Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services, pp 25:1–25:10

[68] Wood A, Stankovic J, Zhou G (2007) DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4- based wireless networks. In: 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp 60–69

[69] Navda V, Bohra A, Ganguly S, Rubenstein D (2007) Using channel hopping to increase 802.11 resilience to jamming attacks. In: IEEE 26th IEEE International Conference on Computer Communications, pp 2526– 2530

[70] Gummadi R, Wetherall D, Greenstein B, Seshan S (2007) Understanding and mitigating the impact of RF interference on 802.11 networks. In: Proceedings of the 2007 Conference on Applications, technologies, architectures, and protocols for omputer communications, pp 385–396

[71] Kerkez B, Watteyne T, Magliocco M, Glaser S, Pister K (2009) Feasibility analysis of controller design for adaptive channel hopping. In: Proceedings of the Fourth International ICST Conference on Performance Evaluation Methodologies and Tools, pp 76:1–76:6

[72] Wang H, Zhang L, Li T, Tugnait J (2011) Spectrally efficient jamming mitigation based on code-controlled frequency hopping. IEEE Transactions on Wireless Communications 10(3):728–732

[73] Yoon SU, Murawski R, Ekici E, Park S, Mir Z (2010) Adaptive channel hopping for interference robust wireless sensor networks. In: 2010 IEEE International Conference on Communications, pp 1–5

[74] Pelechrinis K, Koutsopoulos I, Broustis I, Krishnamurthy S (2009b) Lightweight jammer localization in wireless networks: System design and implementation. In: IEEE Global Telecommunications Conference, pp 1–6

[75] Strasser M, Danev B,˘Capkun S (2010) Detection of reactive jamming in sensor networks. ACM Transactions on Sensor Networks 7(2):16:1–16:29

[76] Shin I, Shen Y, Xuan Y, Thai MT, Znati T (2009) Reactive jamming attacks in multi-radio wireless sensor networks: an efficient mitigating measure by identifying

trigger nodes. In: Proceedings of the 2nd ACM International Workshop on Foundations of Wireless Ad Hoc and Sensor Networking and Computing, pp 87–96

[77] Mpitziopoulos A, Gavalas D, Pantziou G, Konstantopoulos C (2007) Defending wireless sensor networks from jamming attacks. In: IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, pp 1 –5

[78] Lazos L, Liu S, Krunz M (2009) Mitigating control- channel jamming attacks in multi-channel ad hoc networks. In: Proceedings of the 2nd ACM Conference on Wireless Network Security, pp 169–180

[79] Alnifie G, Simon R (2010) MULEPRO: a multi- channel response to jamming attacks in wireless sensor networks. Wireless Communications and Mobile Computing 10(5):704–721

[80] Chiang JT, Hu YC (2011) Cross-layer jamming detection and mitigation in wireless broadcast networks. IEEE/ACM Transactions on Networking 19(1):286– 298

[81] Broustis I, Pelechrinis K, Syrivelis D, Krishnamurthy SV, Tassiulas L (2009) FIJI: Fighting implicit jamming in 802.11 WLANs. Security and Privacy in Communication Networks 19:21–40

[82] Don Torrieri. Principles of spread-spectrum communication systems. Boston: Springer Science+Business Media, Inc, 2005. 129-134.

[83] E. P. Lawrey, “Adaptive techniques for multiuser OFDM,” PhD diss., James Cook University, 2001.

[84] Y. G. Li, “Orthogonal frequency division multiplexing for wireless communications,” Springer-Verlag, 2009.

[85] J. Jang and KB Lee, ”Transmit Power Adaptation for Multiuser OFDM Systems”, IEEE Journal on Selected Areas in Communications, vol. 21, no. 2, pp. 171-178, Feb. 2003.

[86] Yasin, M., Yasin, A., Jazar, A. A., & Hamarsheh, M. (2018). A Novel Wireless Sensor Networks Anti-jamming Technique Based on a Hybrid DS-CDMA/OFDM/FH. International Journal of Applied Engineering Research, 13(14), 11454-11460.

الخلاصة

لقد ادى النمو الهائل في شبكات الاستشعار اللاسلكية الى جعلها احدى اهم مجالات البحوث العلمية. ان شبكات المستشعرات اللاسلكية هي عبارة عن أجهزة صغيرة تحتوي على طاقة وذاكرة محدودة .بشكل عام ، حيث يمكن الوصول إليها بسهولة من العالم الخارجي ، كما أنها تعتبر احد الاهداف السهلة من قبل المهاجمين الخارجيين .لذلك هناك العديد من الطرق التي بنيت لمنع هذه الهجمات.، ان منع المهاجمين من مهاجمة والتأثير على عمل شبكات المستشعرات اللاسلكية أمر لا بد منه ،حيث ان التدابير الأمنية و التقنيات الحديثة لتعتبرمن اهم الأشياء التي يجب أن تمتلكها كل شبكات المجسات اللاسلكية .ان من أكثر الهجمات انتشارا هي هجمات التشويش الاكتروني ، حيث تهدف هذه النوع من الهجمات الى منع وصول البيانات من المرسل الى المستقبل أو تحريفها .هذا النوع من الهجمات له العديد من الأشكال وأيضا العديد من تقنيات الوقاية.

في هذه الأطروحة تمت دراسة عدة انواع مختلفة من الهجمات على الشبكات الاسلكية وكذلك آليات الأمان المناسبة لهذه الانواع من الهجمات بهدف توفير آليات أمان موثوقة وقوية وخفيفة تضمن قدرة النظام على الصمود امام الهجمات الخارجية ذات العلاقة بالتشويش .

تم اقتراح نموذج بني على اساس دمج ثلاث تقنيات مختلفة وهي تقسيم التردد التعامدي(OFDM) , القفز الترددي(FH) و التقسيم الشفري(CDMA) , حيث يقوم النموذج المقترح لدينا بتحقيق توليفة من هذه التقنيات الثلاثة للحصول على نموذج مضاد للتشويش في شبكات الاستشعار اللاسلكية.(WSN) . ان كل تقنية من هذه التقنيات المستخدمة لها اهميتها فالتقسيم الشفري يسمح لاكثر من مستخدم في الارسال على نفس التردد و تقسيم التردد التعامدي يقوم بإزالة التداخل بين الرموز(ISI) ويوفر مقاومة لتأثير المسارات المتعددة كما يقوم القفز الترددي بالتقليل من اثر التشويش.

ان النموذج المقترح قلل اثر هجمات التشويش الى اقل ما يمكن مع الحفاظ على سعة البيانات المنقولة بين المرسل والمستقبل. قمنا بتطبيق النمذج المقترح على الشبكات الاسلكية حيث قمنا بتقسيم القنوات الى 1327 قناة مع الحفاظ على سعة كافية لكل قناة لاستخدامها في شبكات الاستشعار اللاسلكية. قمنا باختبار نظريتنا من خلال محاكات النموذج المقترح وحصلنا على نتائج ايجابية تظهر تقليل احتمالية التشويش من 0.1 في الشبكات الاسلكية (WIFI)الى 0.003

.