Analysis of Jamming attacks on Wireless Sensor Networks

by

Saif Saeed

Submitted to the University of Hertfordshire in partial fulfilment of the requirements of the degree of Master of Science by Research

University of Hertfordshire.

Abstract

Wireless Sensor Network (WSN) is a wireless-oriented form of communication largely used for outdoor applications, such as environmental monitoring and military surveillance. Therefore, a jamming attack is one of the denial of service attacks (DOS) that may take place by jamming the communication channel, making communication between genuine sensor nodes difficult or even impossible. Several studies have been carried out to develop countermeasures against jamming attacks, utilising parameters such as Packet Delivery Ratio (PDR), Packet Send Ratio (PSR), Received Signal Strength Indication (RSSI) and Clear Channel Assessment (CCA). The accuracy of the parameters used is very important for developing successful countermeasures against jamming attacks. Consequently, the focus in this study is to examine the effect of a jamming attack that was generated by one or more wireless sensor network nodes on PDR, PSR and RSSI, and look at the enhancements that can be made on Packet Delivery Ratio by altering the value of CCA on sender nodes. The experiment was performed using XBee RF and K-mote devices configured as jammers by disabling the CSMA protocol. It was performed in a non-isolated room in order to emulate a real-life environment.

Two scenarios were carried out in this study. The first scenario aimed to study RSSI, PSR and PDR values with a fixed CCA value, and the second scenario studied the effect of CCA on PDR value.

The experiment showed that the RSSI value measured by XBee RF inflated in the presence of noise. This fact has to be considered when RSSI is utilised in jamming attack counter measures. Further, it has been observed that the PDR value is distressed by jamming because genuine packets collide with jammers’ packets and increase the power of the sent packets without considering that the distance will not be enough to enhance the PDR value. This study demonstrates that changing the CCA threshold value on the XBee RF module influences the Packet Delivery Ratio (PDR) value in the presence of jamming.

Acknowledgements

I would like to thank specially my supervisor Johann Siau, for his support and patience. Without his guidance and persistent help this dissertation would not have been possible.

I would like to thank my wonderful family my wife Rasha and my lovely kids Sama , Ayad they were always supporting me and stood by me in good and bad.

I would also like to thank my parents, two sisters. They were always supporting me and encouraging me with their best wishes.

Contents

Table of Figures

Glossary

API	Application Program Interface
CCA	Clear Channel Assessment
CSMA	Carrier Sense Multiple Access
CTS	Clear to Send
dBm	Decibel-milliwatts
DOS	Denial of Service Attack
DSSS	Direct Sequence Spread Spectrum
GUI	Graphical User Interface
IDE	Integrated Development Environment
ISM	Industrial, Scientific and Medical
JM	Jammer Transmit
LR-WPAN	Low Rate Wireless Personal Area Network
LSS	Spread Spectrum Loss
MAC	Medium Access Control
PDR	Packet Delivery Ratio
PER	Packet Error Ratio
PN	Pseudorandom Noise
PSD	Power Spectral Density
PSR	Packet Send Ratio
RF	Radio Frequency
RSSI	Received Signal Strength Indication
RTS	Request to Send
SNR	Signal to Noise Ratio
UART	Universal Asynchronous Receiver/ Transmitter
USRP	Universal Software Radio Peripheral
WSN	Wireless Sensor Network
WPAN	wireless personal area network

1. Introduction:

Wireless Sensor Networks (WSN) is a type of ad-hoc networks that consist of limited energy, tiny and low cost sensor nodes. The main purpose of WSN is to provide an interface for the computer system to the real world by providing physical information such as temperature, light, radiation, etc. The functionality of WSN differs from any other wireless network in that all devices in WSN are totally independent, not controlled by human users, and these devices are limited in terms of battery life and processing power. Therefore, they can only offer simple and predefined tasks (Acs and Buttyan, 2008).

As in all computing environments, it is essential to ensure the appropriate functionality of WSN to achieve correct service. WSN should comply with certain security requirements, such as confidentiality, integrity and authentication. However, to achieve the security requirement on WSN is not an easy task, due to the constraints in resources in sensor nodes.

Since WSN is a wireless-oriented infrastructure, denial of service attacks (DOS) - for example, a jamming attack - may take place by jamming the communication channel and preventing the member of the network from sending or receiving packets. The attacks can take place against the internal routing protocol (Acs and Buttyan, 2008).

Several studies have been carried out to develop countermeasures against jamming attacks. The accuracy of the parameters that are used in countermeasures is very important for developing a successful countermeasure against jamming attacks, therefore the focus in this study is to examine PDR, PSR, RSSI and the enhancement that can be made to Packet Delivery Ratio by altering the value of CCA on sender nodes. This paper is organised as follows. In Section 2, the literature review and background of WSN and jamming attacks. Section 3 describes the materials and methodology of the experiment. Section 4 analyses the experiment results. This paper concludes with Section 5.

2. Literature review

2.1 Electronic Spectrum

Jamming attack is a physical layer attack therefore it is very important to study the physical layer of wireless communication in order to protect the WSN from jamming attack, the most common wireless technologies use electromagnetic wireless telecommunications. Electromagnetic spectrum is the broad range of frequencies. Radio is only one slice of the electromagnetic spectrum, as shown in figure (2.1). Radio waves can travel through solid materials such as clothing, furniture and brick walls because radio energy requires no medium. Radio waves affect conductors like metal and form different types of energy electrical signals, which means that radio waves cannot travel through metal walls but this also means that metal can be used in radio antennas on wireless modules (Faludi, 2011).

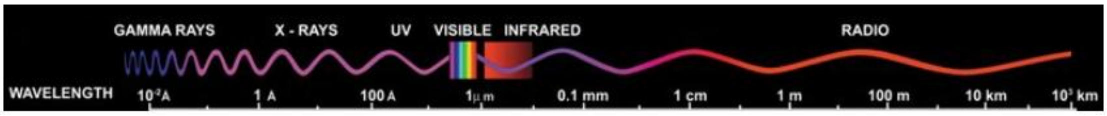


Figure (2.1) Electromagnetic spectrum (Faludi, 2011)

When radio signals radiate away from their source, they rapidly spread out like a wave in water. Radio decay occurs according to the inverse square law; therefore, it needs more power in order to move to longer distances (Faludi, 2011). As such, it is important to keep the inverse square law in mind when designing WSN networks (Faludi, 2011).

$I = P/4\pi r2$ (2.1)

I = Intensity at r

π= Is pi

r = radius of sphere

P = power at source

Surface area of sphere = $4\pi r2$

Wireless communication has become very popular in recent decades because of its flexibility, low-cost management and implementation, in comparison to wired communications.

The increase in the use of wireless communication has caused the radio spectrum to become very expensive. Therefore, many wireless standardised technologies operate in the industrial, scientific and medical (ISM) radio band, which is a group of radio bands internationally reserved for industrial, scientific and medical purposes (Baccour et al., 2013; Coleman and Westcott, 2012). Unlicensed ISM frequency available bands are as follows:

Frequency range		Bandwidth	Centre frequency	Availability
6.765 MHz	6.795 MHz	30 kHz	6.780 MHz	Subject to local acceptance
13.553 MHz	13.567 MHz	14 kHz	13.560 MHz	Worldwide
26.957 MHz	27.283 MHz	326 kHz	27.120 MHz	Worldwide
40.660 MHz	40.700 MHz	40 kHz	40.680 MHz	Worldwide
433.050 MHz	434.790 MHz	1.74 MHz	433.920 MHz	Subject to local acceptance
902.000 MHz	928.000 MHz	26 MHz	915.000 MHz	Subject to local acceptance
2.400 GHz	2.500 GHz	100 MHz	2.450 GHz	Worldwide
5.725 GHz	5.875 GHz	150 MHz	5.800 GHz	Worldwide
24.000 GHz	24.250 GHz	250 MHz	24.125 GHz	Worldwide
61.000 GHz	61.500 GHz	500 MHz	61.250 GHz	Subject to local acceptance
122.000 GHz	123.000 GHz	1 GHz	122.500 GHz	Subject to local acceptance
244.000 GHz	246.000 GHz	2 GHz	245.000 GHz	Subject to local acceptance

Table (1) Unlicensed ISM frequency bands (Radio Regulation, 2012)

The ISM bands rules specify as well that Spread Spectrum has to be used for modulation.

2.2 Spread Spectrum

Spread spectrum (SS) is a technique of generating signals with bandwidths that are deliberately spread in the frequency domain. It is accomplished by combining a code sequence with the digital data before modulation. SS is used to mitigate against noise and jamming (Bullock, 2014).

The basic idea is to mix the narrow band signal with a high frequency pseudo number signal (PN). The process could be reversed using the same code (PN) to recover the original signal (Parker, 2010).

When SS is used, there will be losses due to non-ideal spreading and de-spreading techniques, which leads to reductions in the received signal power. The spread spectrum loss is approximately 1 to 2 dB and it varies from system to system.

$$\text{LSS} = \text{spread spectrum loss (1 to 2 dB)} \qquad (2.2)$$

The main reason for using the SS is to reject other signals and jammers; this ability is called process gain (Gp). The jamming margin (Jm) is the amount of extra power that the jammer transmits to jam the receiver (Bullock, 2014).

$$\text{Jm} = \text{Gp} - \text{LSS} \qquad (2.3)$$

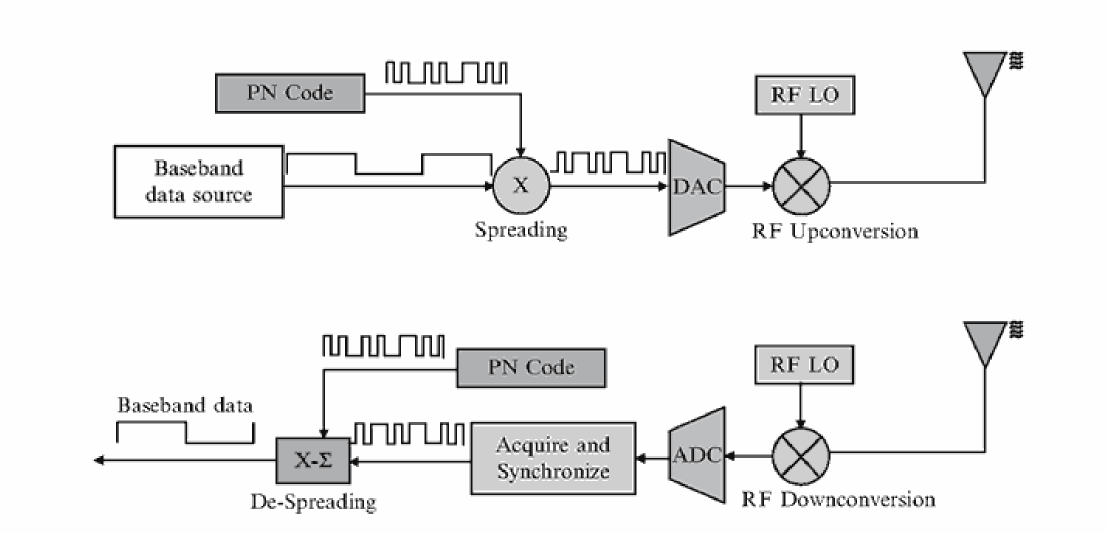


Figure (2.2) Spread spectrum (Parker, 2010).

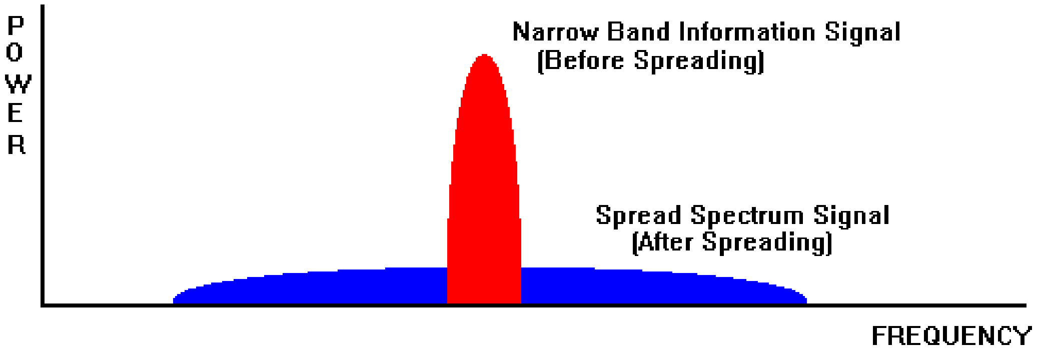


Figure (2.3) Signal power before and after spread spectrum (Prabakaran, 2003)

DSSS is the most common method used in digital telecommunications in which the original signal is modulated by a higher frequency of pseudorandom noise (PN) data. Each bit is a chip. The high rate chip changes will increase the occupied frequency bandwidth of the signal and reduce the concentration of the signal energy around the carrier (Parker, 2010; Finne, 1996).

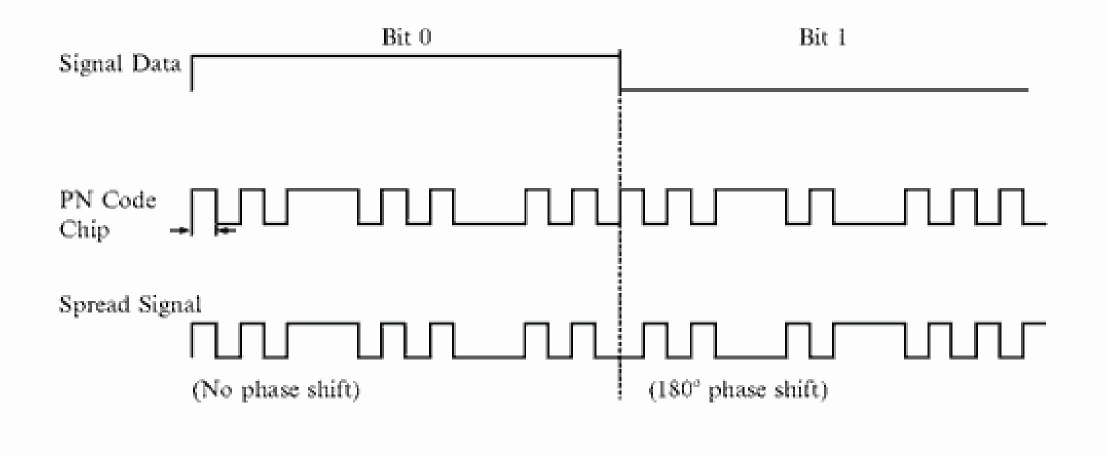


Figure (2.4) Modulation of DSSS (Parker, 2010)

In IEEE 802.15.4 every four bits of actual data are grouped together (symbol) and mapped to a unique 32-bit sequence called pseudorandom noise (PN), while the lookup table contains symbol-to-PN mapping, which includes 16 PN. Each PN consists of a random sequence of zeros and ones. In order to reduce the similarity of PN values in a lookup table a special procedure called a cross-correlation function is used. The DSSS will cause an increase in signal bandwidth; for example, if the original bandwidth is 250 KHz, then after spreading the bandwidth of the signal travelling over air it will be 2 MHz, as shown in figure (2.6).

The despreading on the receiver device will reduce the bandwidth back to its original value, and the spreading/despreading process will not cause increases in noise levels (Farahani, 2008; Muntwyler et al., 2012). The processing gain for 2.4 GHz RF band in IEEE 802.15.4 is equal to 9dB:

Processing gain = 10 * log10 [2Mbps/250Kbps] ≈ 9dB (2.4)

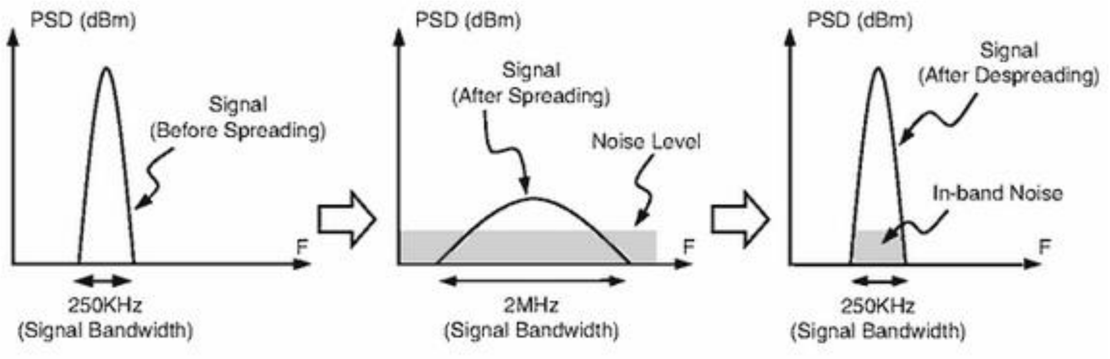


Figure (2.5) Signal PSD before and after DSSS (Farahani, 2008)

Where signal power spectral density (PSD) is the signal power versus frequency (Farahani, 2008), DSSS reduces the interference effect on sent signals because the spread RF signals occupy a larger bandwidth but they use a lower spectral power density (Gascon, 2013).

2.3 IEEE 802.15.4

In the past few years, several short range wireless technologies such as IEEE 802.15.4, have been developed for wireless sensor networks (WSN). These WSN related technologies primarily operate in the unlicensed ISM (industrial, scientific, and medical) band which is shared with other major wireless standards such as IEEE 802.11, Bluetooth, and cordless phone .IEEE 802.15.4 is developed for low-cost, low-power networks. The IEEE 802.15.4 involves the bottom two ISO/OSI layers of medium access control (MAC) and the physical (PHY) layer. It is targeted for low-rate wireless personal area networks (LR-WPAN), as IEEE 802.15.4 is used for short distance communication and has a low cost. There are two options for higher layers, such as the ZigBee protocol stack, specified by the industrial consortia ZigBee Alliance, and IPv6 over a low-power PAN (6LowPAN).

The IEEE 802.15.4 physical layer operates in three different unlicensed bands according to geographical area. The physical layer provides the ability for radio transceiver activation and deactivation, energy detection, link quality, clear channel assessment, channel selection and transmission and reception of packets (Baccour et al., 2013; Buratti et al., 2011).

The RF for 2.4 GHz uses direct sequence spread spectrum (DSSS); the raw bit rate for IEEE 802.15.4 is 2Mbps but because DSSS uses 32-chip for every four bits of data, it will reduce the actual data rate to 250 Kbps. The IEEE 802.15.4 MAC controls the flow of frames that are sent through the radio and transmitted over the air. It is designed to host different network topologies and higher-layer stacks. IEEE 802.15.4 MAC offers security, definite timeslots, beaconing services and node associations for establishing a network.

IEEE 802.15.4 uses standard CSMA/CA protocol with back-off capability. The CSMA/CA is a process for network access when devices are not negotiating timeslots for transmission, as network devices are listening to channels and waiting until the channel is available to start transmitting the data. When the channel is busy, the network device sets a back-off timer and waits for it to expire; when the back-off time expires, the network device will listen again and if the channel is still busy its increment sets the back-off timer to a larger value. The network device may enter sleep mode to save power; during the back-off timer the sleep mode feature is available based on the type of IEEE802.15.4 device (Hunn, 2010; Chiuso et al., 2009).

2.4 Clear Channel Assessment (CCA)

CCA is used by the medium access control (MAC) protocol to decide if the channel is clear enough to transmit WSN packets. CCA detects energy on the RF channel by using a simple energy detection method used by 802.15.4 sender and receiver nodes. The sender uses CCA to identify the availability of the RF channel before it starts sending packets and the receiver uses the same CCA mechanism to detect incoming packets (King, Brown and Roedig, 2014).

The CCA works in three operation modes:

1- Energy detection: the CCA reports a busy channel if the detected energy is above a specified threshold.

2- Carrier sense mode: CCA reports a busy channel if it detects a signal with 802.15.4 characteristics regardless of whether it is lower or higher than the specified threshold.

3- Carrier sense with energy detection: this is a combination of both previous techniques.

MAC utilises CCA in a CSMA/CA mechanism. The CSCA/CA mechanism depends on the network operation behaviour (beacon-enabled or non beacon-enabled) (Tennina et al., 2013).

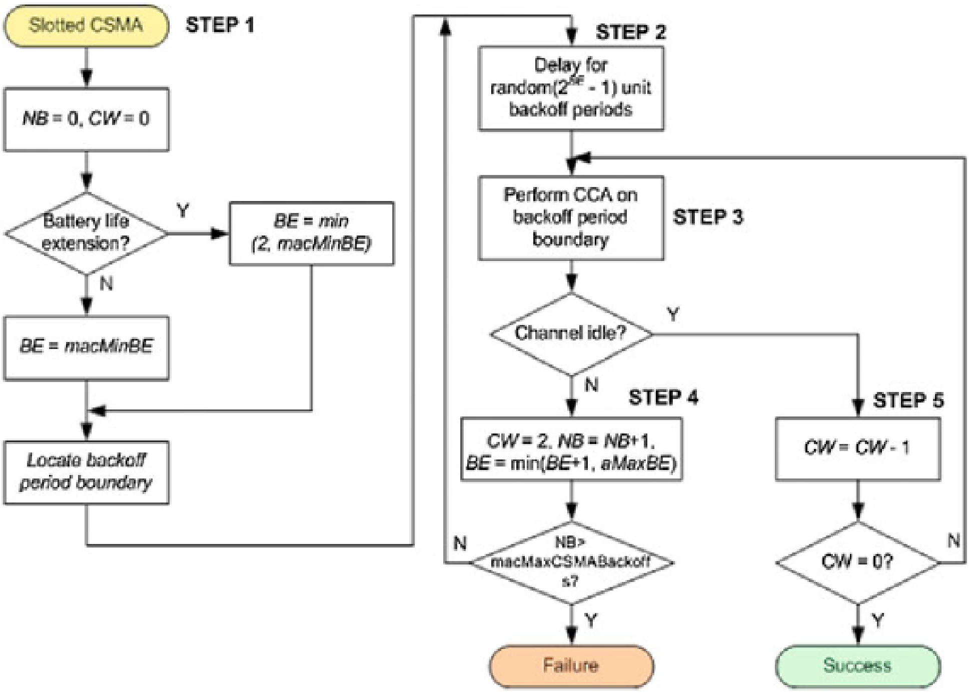


Figure (2.6) CSMA/CA mechanism for beacon-enabled mode (Tennina et al., 2013)

Figure 2.7 shows the CSMA/CA mechanism for the beacon-enabled mode. Three variables are used in the mechanism:

NB: number of backoffs

CW: contention window

BE: back-off exponent

1. Initially, NB and CW equal 0,BE set to a minimum value between 2 and the macMinBE.
2. MAC waits for the random back-off delay before attempting to access the channel.
3. CCA verifies the channel availability.
4. CCA returns a busy channel, NB increases by 1, and the process must start again.
5. CCA returns the idle channel, CW decreases by 1 and when CW reaches 0, the message will be transmitted (Tennina et al., 2013).

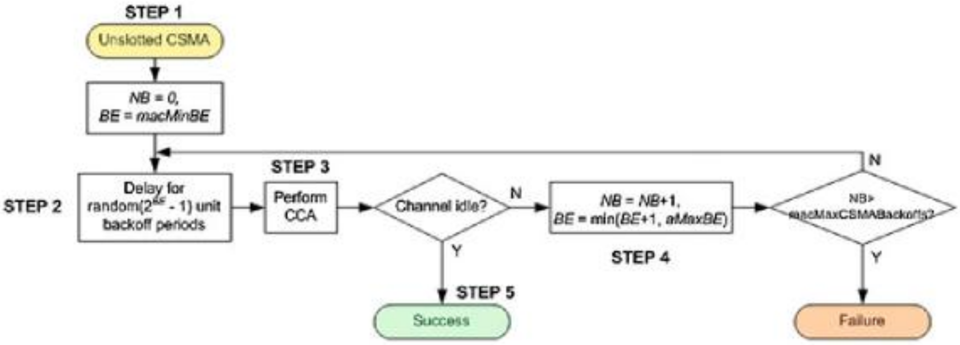


Figure (2.7) CSMA/CA mechanism for non beacon-enabled mode (Tennina et al., 2013).

The CCA threshold value is configurable on the XBee RF module, and the CCA threshold range on XBee is -36 dBm to -80 dBm (XBee RF Modules, 2015; Lee, Kim and Shin, 2012).

XBee calculates CCA on the basis of the channel measurement over 0.128ms (Digi, 2015); the collision happens when XBee starts sending packets concurrently with other devices using a radio frequency channel. The CCA mechanism may not succeed in detecting activity on a channel if transmissions started less than 0.128ms before the CCA sampling (Kiryushin, Sadkov and Mainwaring, 2008).

RSSI readings may include noise components, so in the presence of noise the figure will be inflated (Foster, 2011).

2.5 Interference in 2.4 GHz ISM band

Additional to WSN nodes there are many other wireless communication devices operating on 2.4GHz; for example, microwave ovens, cordless phones, medical diathermy machines, military radar and Wi-Fi. 802.11 devices make 2.4 GHz ISM the most congested ISM band (Baccour et al., 2013).

Bluetooth uses a frequency hopping spread spectrum (FHSS), which hops between 79 channels with 1Mz as the width of each channel. Bluetooth hops 1600 per second because there are only 79 channels available; each channel is used around 20 times each second. The interference produced by IEEE 802.15.1 devices is not problematic for WSN because the interference generated by Bluetooth spreads across the whole 2.4 GHz evenly. Bluetooth version 4 uses adaptive frequency hopping (AFH) to protect against interference; this does not use the hopping sequence, however, because the low power of Bluetooth is not a real threat (Ericsson, 2010).

IEEE 802.11 uses ISM 2.4 GHz bands (2400-2483.5 MHz), which divides the ISM band to 14 channels 22 MHz. IEEE 802.11 devices use very high power (24 dBm) as compared to WSN nodes and uses 22 MHz channels; for that reason it can interfere with many IEEE 802.15.4 channels at the same time. Many studies have been done on the coexistence of IEEE 802.11 and IEEE 802.15.4 and show that WSN suffers from high packet loss in the presence of IEEE 802.11. The packet loss rate of IEEE 802.15.4 depends on IEEE 802.11 device activity and the distance from sensor nodes.

A microwave oven is also a source of interference to WSN that operates on 2.4 GHz. The power of a microwave ovens signal varies; based on the model it could be up to 60 dBm (Baccour et al., 2013; Andrews, 2012).

2.6 Launching and Detecting Jamming Attacks in Wireless Networks

Wireless connectivity threats can be addressed by a suitable design that provides congeniality, authentication and integrity to the wireless network. Wireless, however, is vulnerable to other types of attacks that cannot be protected by cryptography methods.

It is very important to identify the type of attack in order to take suitable action against threats. A jammer is a device that launches attacks against wireless networks and continuously emits RF signals to fill a wireless channel and block genuine traffic. Communications for jammers are not compliant with MAC protocols (Muraleedharan and Osadciw, 2006; Xu et al., 2005). The effectiveness of jammers can be measured based on the following metrics:

Packet Send Ratio (PSR) is the ratio of packets sent out by the legitimate wireless device to the total number of packets that are intended to be sent to a MAC layer. The wireless device sends packets when the channel is idle; therefore, when there is noise on the channel caused by the attacker, this causes a delay in transmitting packets (Sun and Wang, 2010).

PSR = packets sent/packets intended to be sent (2.5)

Packet Delivery Ratio (PDR) is the ratio of packets successfully received by the destination (after passing the CRC check) to the number of packets sent by the sender (Sun and Wang, 2010).

PDR = packets that pass the CRC check/packets received (2.6)

2.7 Jammer Attack Models

A variety of jamming attacks can be performed to interfere with the wireless communication channel. There are four types of jamming attacks:

Constant Jammer

A constant jammer device continuously emits a radio signal without following MAC layer rules, which prevents a legitimate device from being able to use the channel to transfer traffic. A Kmote-S1 Mote platform or a waveform generator can be used for testing (Zhang and Kitsos, 2009).

Deceptive Jammer

A deceptive jammer injects regular packets into a channel without gaps between packets so the legitimate sender will believe that the channel is busy. The jammer could send preamble bits continuously instead of entire packets (Zhang and Kitsos, 2009).

Figure (2.8) shows that constant jammer continually emits radio signal, and can be implemented using either a waveform generator that continuously sends a radio signal or a normal wireless device that continuously sends out random bits to the channel without following any MAC-layer etiquette, aims at keeping the channel busy to cause interference to genuine nodes that have already started data transfer and corrupt their packets. Deceptive jammer instead of sending out random bits, the deceptive jammer constantly injects regular packets in terms of packet format such as preamble ,payload and CRC without leaving any gab between packets to keep the channel busy.

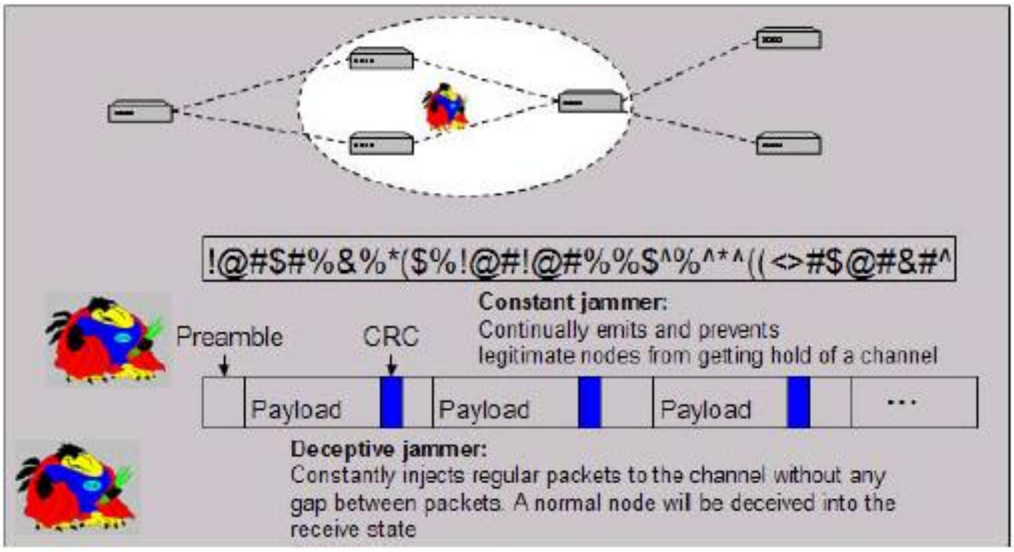

!@#$#%&%*($%!@#!@#%%$^%^*^((<>#$@#&#^
Constant jammer:
Continually emits and prevents legitimate nodes from getting hold of a channel
Preamble
CRC
Payload
Payload
Payload
...
Deceptive jammer:
Constantly injects regular packets to the channel without any gap between packets. A normal node will be deceived into the receive state

Figure (2.8) Constant jammer and deceptive jammer (Mpiziopoulos, 2009)

Random Jammer

A random jammer changes continuously between sleeping and jamming modes. During the jamming mode it could act as a constant or a deceptive jammer. This type of jamming is used when the jammer needs to save power (Zhang and Kitsos, 2009).

Reactive Jammer

A reactive jammer starts transmitting a radio signal as soon as it detects activity on the channel. The jammer will not save power because it is continuously sensing the channel, but it is harder to detect (Zhang and Kitsos, 2009).

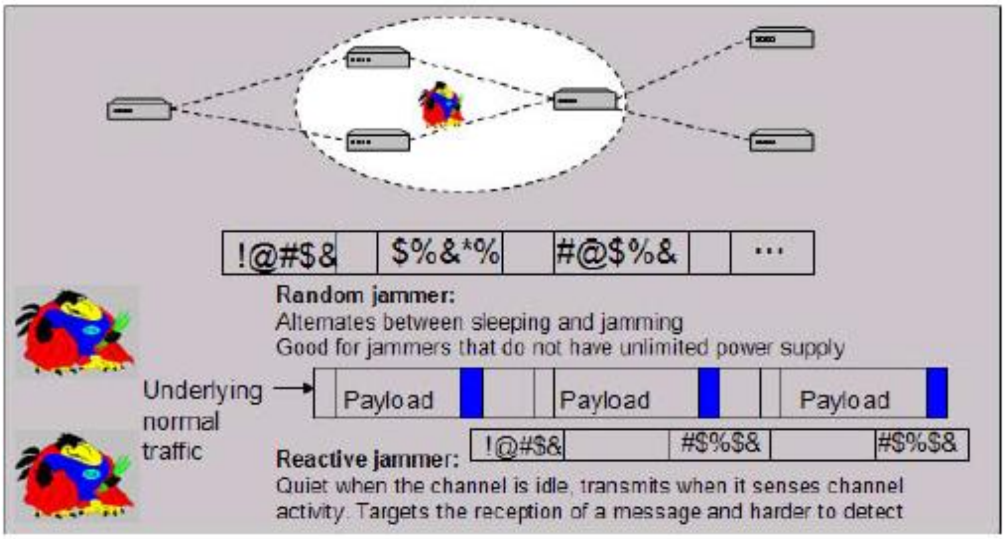

!@#$&
$%&*%
#@$%&
...
Random jammer:
Alternates between sleeping and jamming
Good for jammers that do not have unlimited power supply
Underlying normal traffic
Payload
Payload
Payload
!@#$&
#$%$&
#$%$&
Reactive jammer:
Quiet when the channel is idle, transmits when it senses channel activity. Targets the reception of a message and harder to detect

Figure (2.9) Random jammer and reactive jammer (Mpiziopoulos, 2009)

Figure (2.9) shows that a Instead of continuously sending out a radio signal, a random jammer alternates between sleeping and jamming. after jamming for a while, it turns off its radio and enters a “sleeping” mode. It will resume jamming after sleeping for some time. During its jamming phase, it can behave like either a constant jammer or a deceptive jammer. Quiet when the channel is idle and transmits when it senses channel activity targets the reception of a message and harder to detect .During its jamming phase, it can behave like either a constant jammer or a deceptive jammer.

Constant, deceptive, random and reactive jammers are very effective if they are placed at an appropriate distance from the receiver node. However, constant and deceptive jammers are inefficient because they will consume the power before the victims. Reactive jammers are more energy efficient because they go into sleep mode when the network is idle (Zhang and Kitsos, 2009).

Signal strength is one of the mechanisms that detects jamming therefore Received Signal Strength Indication (RSSI) is utilized for this purpose.

The received signal strength indicator (RSSI) is a feature provided by RF transceivers whose aim is to estimate received power in the selected frequency channel. The power of the signal is received in milliwatts and the unit for RSSI is decibel-milliwatts (dBm) (Sauter, 2011). It is used in many wireless applications and protocols, such as localisation, topology control, link scheduling and link quality estimation. Regardless of the technology, RSSI performance depends on the circuit used to realise the RF transceivers.

RSSI is affected by several factors, such as:

1. **Transmitter variability**: different transmitters behave differently even if they have been configured with the same configuration.
2. **Receiver variability**: different receivers behave differently even if they have been configured with the same configuration.
3. **Antenna orientation**: different antennas have their own radiation patterns.
4. **Multi-path fading and shadowing in the RF channel**: channel behaviour greatly depends on environmental characteristics such as obstacles.

CC2420 provides 8-bit RSSI value. There are two RSSI types sent by radio transmitters; the first measures the strength of the signal for the received packet and the second measures the power of the ambient channel noise (Chen and Terzis, 2010). RSSI can be used to indicate the distance between WSN nodes; for example, if the value of received RSSI is -60 this means that the sender node is close to the receiver, but if the RSSI of the received signal equals -100 dBm this means that the sender is far from the receiver (Sauter, 2011).

The received signal strength can be calculated using the equation below:

$$TRE = TSE.\ GT.\ GR\ [\alpha/4\pi d] \qquad (2.7)$$

TRE: Power received by the receiver

TSE: Transited power by the sender

GT: Transmitted gain

GR: Receiver gain

α: Denoted wavelength

RSSI is the ratio of the received signal strength to the reference power.

$$RSSI = 10\ \log.\ TRE/Re\mathit{f}p \qquad (2.8)$$

Re*f*P: is the reference power equal to 1mW (Manju and Sasi, 2012).

WSN Network devices will need to collect noise levels over a period of time and build a statistics model for the energy level of the network. The statistics values can be compiled either by average signal value or by the total signal energy over a window of N. Another way to detect jamming is by tracking the amount of time that the legitimate network device waits for the channel to become idle and then compare the waiting time with the sensing time during normal traffic. But a long carrier sensing time could be because of congestion (non-jammed scenario), and therefore it is important to use a mechanism to differentiate between normal and abnormal failure in order to access the network channel.

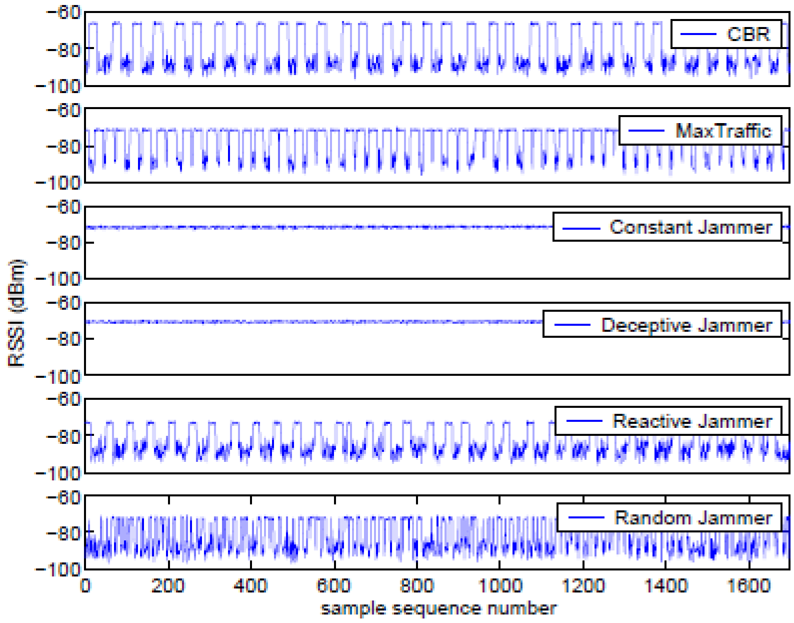


Figure (2.10) Comparing RSSI values for different types of attacks.

Figure (2.10) shows that it is easier to detect a constant and deceptive jamming attack by collecting the RSSI value of the channel as compared to other types of jamming attacks.

According to Xu et al. (2005), the packet delivery rate (PDR) combined with signal strength is one the best means of detecting the jamming attack. When the signal strength is high and the PDR is low, this indicates a jamming attack, while when the signal strength is low and the PDR is low it means a poor link quality. Using PDR alone as a mean of detecting a jamming attack is not efficient because it could be low when WSN is congested with genuine traffic.

2.8 Prior work

There has been a dramatic increase in WSN applications that monitor physical and environmental conditions, for example temperature, sound and pressure; therefore, as in all computing environments it is essential to assure the appropriate functionality of WSN. In order to allow a correct service, WSN should comply with certain security requirements such as integrity and availability. A jamming attack is one of the main security threats that affects integrity and availability and has been intensively studied in resent years.

(Boano et al. ,2011) studied interference on Wireless Sensor Networks using physical wireless sensor nodes and a CC2420 radio chip operating in 2.4GHz ISM band to generate repeatable patterns of interference. They thought that using real nodes rather than simulators would provide a more accurate result of hardware parameters such as RSSI and LQI. They didn't use an 802.11 device to generate interference because WiFi is not suitable to generate tuneable static interference. Also, 802.15.4 devices can use channels that not overlap with 802.11 such as channels 25 and 26. Interference was created using software-defined radio (SDR) through the universal software radio peripheral (USRP). The T-mote sky nodes at a distance of one metre is used to test the level of interference by measuring the SNR.

This experiment showed that SNR drops when there is interference at given instants of time. Homemade antenna made of can (Cantenna) is used to direct the interference and they found that the packet loss increases when the Cantenna points towards nodes. They also found that if interferer sending packets for 125ms per second this will cause 12.5% of packet loss but if interferer sends packets 875ms per seconds this will cause 87.5% pack loss.

Figure (2.11) Homemade antenna made of can (Cantenna).

(Manju and Sasi ,2012) state that a jamming attack can be detected by analysing metrics such as PRD, RSSI and Residual Energy (RE) and the node with high RE acts as a monitor node. Monitoring nodes are responsible for detecting the jammer in a WSN network by collecting RSSI and PDR. They found that jamming damages the data packets and consequently causes a reduction in PDR and this reduces the channel quality by interrupting the radio signal; therefore, PDR and RSSI are considered as metrics that can identify jammers. A weight is a combination of RSSI and PDR. If the weight value is above the threshold then the sender is marked as a jammer and will be isolated from the network. In this study network the simulator NS2 used an IEEE 802.11 MAC layer for communication.

(Morparia, Shah ,2007) found that the strongest packet can be received successfully when there is concurrent transmission by multiple WSN devices when SINR value is above a certain threshold. In their study TinyOS 2.X was used as an operating system and a CC2420 RF module. They disabled CSMA-CA in the CC2420 radio on two sender nodes (SRC1, SRC2); one of the sender nodes (SRC2) was transmitting with fixed power (-8dBm) while the power transmitted from the other node (SRC1) is variable. When the transmit power of SRC1 is between -24dBm and -19dBm the packets from SRC2 are received successfully but when the power of SRC1 between -3dBm and 2dBm the packets from SRC1 are received successfully. When the power transmitted from SRC1 is between -13dBm and -7dBm no packet is received from SRC1 or SRC2.

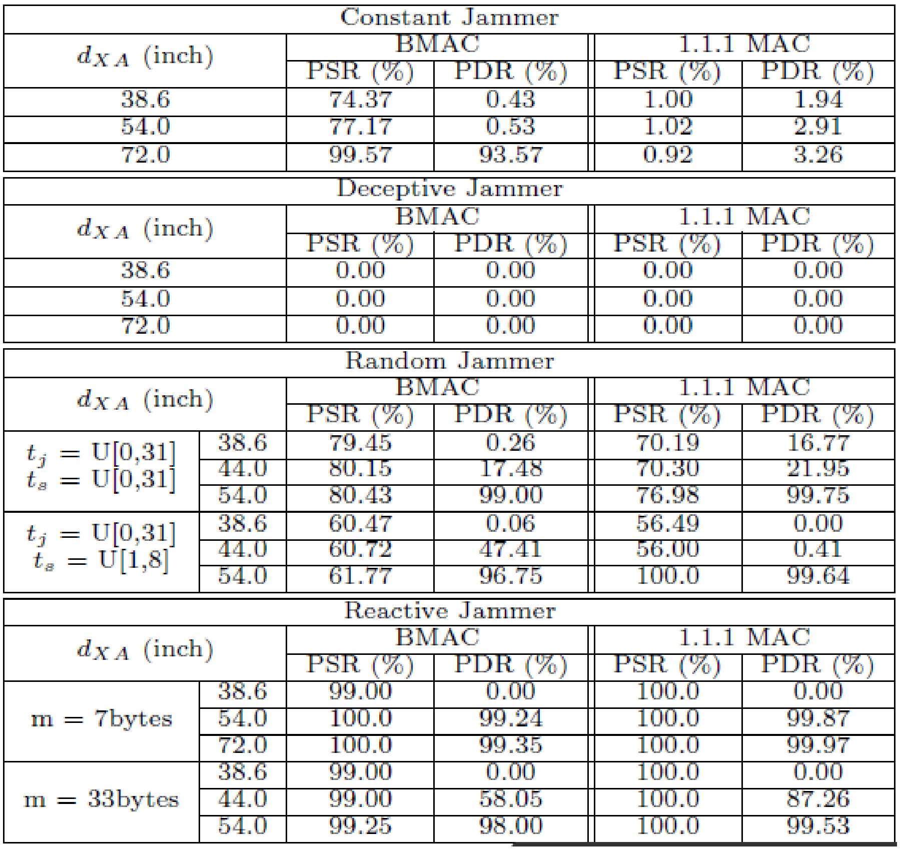
The experiment confirmed that RTS/CTS is not desirable in modern WSN, which supports power control and channel capture.

In this study only two concurrent senders are used when a large number of senders transmit concurrently without RTS/CTS; this will cause packets loss especially when transmitters are at the same distance to a receiver.

(According to Xu et al. ,2005), packet delivery rate (PDR) combined with signal strength is the best means of detecting a jamming attack. When the signal strength is high and PDR is low this indicates a jamming attack, while when the signal strength is low and PDR is low it means poor link quality. Using PDR alone as a means of detecting a jamming attack is not efficient because it could be low when WSN is congested with genuine traffic.

In this study it has been found that the interference level is governed by many factors, such as the jammer distance from the wireless node, the transmission power of the jammer and the MAC protocol used on nodes.

(Xu et al. ,2005) implemented jamming models (constant, deceptive, random and reactive) using Berkeley motes that employed Chipcon CC1000 RF transfer with TinyOS as the operating system with channel sensing and back of operations disabled by passing the Mac protocol. The Mac protocol for TinyOS release 1.1.1 uses a fixed threshold value but the BMAC protocol change threshold value is based on the signal strength by choosing the minimum strength of the most recent readings. The packed send rate and the DSR packed delivery rate (PDS) result were different for nodes using BMAC and nodes using MAC1.1.1 when the same jammers were located over the same distance from the sender and the receiver.



Constant Jammer					
d_{XA} (inch)		BMAC		1.1.1 MAC	
		PSR (%)	PDR (%)	PSR (%)	PDR (%)
38.6		74.37	0.43	1.00	1.94
54.0		77.17	0.53	1.02	2.91
72.0		99.57	93.57	0.92	3.26

Deceptive Jammer					
d_{XA} (inch)		BMAC		1.1.1 MAC	
		PSR (%)	PDR (%)	PSR (%)	PDR (%)
38.6		0.00	0.00	0.00	0.00
54.0		0.00	0.00	0.00	0.00
72.0		0.00	0.00	0.00	0.00

Random Jammer					
d_{XA} (inch)		BMAC		1.1.1 MAC	
		PSR (%)	PDR (%)	PSR (%)	PDR (%)
t_j = U[0,31] t_s = U[0,31]	38.6	79.45	0.26	70.19	16.77
	44.0	80.15	17.48	70.30	21.95
	54.0	80.43	99.00	76.98	99.75
t_j = U[0,31] t_s = U[1,8]	38.6	60.47	0.06	56.49	0.00
	44.0	60.72	47.41	56.00	0.41
	54.0	61.77	96.75	100.0	99.64

Reactive Jammer					
d_{XA} (inch)		BMAC		1.1.1 MAC	
		PSR (%)	PDR (%)	PSR (%)	PDR (%)
m = 7bytes	38.6	99.00	0.00	100.0	0.00
	54.0	100.0	99.24	100.0	99.87
	72.0	100.0	99.35	100.0	99.97
m = 33bytes	38.6	99.00	0.00	100.0	0.00
	44.0	99.00	58.05	100.0	87.26
	54.0	99.25	98.00	100.0	99.53

Table (2) PDR and PSR values for nodes running BMAC and nodes running MAC1.1.1

(Boano et al. ,2011) used motes based on Contiki with CC2420 RF modules in the test beds to generate noise. The RSSI experiment showed that the RSSI noise reading measured in the absence of packed transmission suffers from problems in three scenarios:

1. When transmitting a non-modulated carrier.
2. When a microwave is on.
3. When Bluetooth transmits on the same channel.

RSSI noise measurements were done using an Anritsu MS2711D spectrum analyser. Wrong RSSI readings cause wrong clear channel assessment (CCA). (Boano et al , 2011) experiment showed that activating the peak detectors avoids the wrong RSSI reading during jamming caused by microwave ovens and increases the packet reception rate (PRR) by VP to 12%.

(Bertocco, Gamba and Sona's ,2008) study showed how changing the CCA mode affects the performance of the IEEE802.15.4 network when there is interference. S8 used a CSMA non-beacon mode in the experiment, as there are two modes that CCA can use to decide if the channel is busy. The first CCA mode assumes the channel is busy if it detects that the RSSI is higher. The second CCA mode decides that the channel is busy if any signal is detected in spreading the characteristics of IEEE802.15.4.

Two T-mote sky wireless sensors are connected to a PC used in a non-anechoic room and Agilent E4407B spectrum analyser is used to measure interference level. A high layer protocol is installed on motes to periodical poll information from sensors. The application works in a master and slave mechanism of 1 metre distance between master and slave. The packet error rate (PER) was 55% when CCA modes 1 and 2 were in the presence of ZigBee interference. The performance was improved by disabling CCA since PER = 16.5%.

(Siddhabathula et al. ,2012) developed a program to detect jamming attacks using observation from multiple nodes in order to speed up the detection. In their study they didn’t consider a compromised node scenario. The experiment assumes that attacker disables the carrier sense in enough time to achieve the attack of a constant jammer used in this study. Each node broadcasts beacons to jamming attacks and holds two arrays - current and history. If the node doesn’t receive a beacon it stores the value as zero and one means that the beacon has been received.

If value in history is one and in current is equal to zero for a period of time then an alert will be will be sent to the base station. The base station detects jamming in the network after receiving 10 alerts. 40 Kmote-S1 with TinyOS software was arranged in a grid topology. Jammers were positioned outside the perimeter. It has been found that increased internal time will increase the time to detect jamming. This detection method consumes a lot of power on all nodes in WSN therefore it is not very practical. From the above studies it has been concluded that PDR, RSSI and PER are most practical metrics to detect jamming attacks and that increasing the packet power level will increase the probability of the successful delivery of packets.

(Ramachandran and Roy, 2006) described the methods for Clear Channel Assessment in the 802.11 and 802.15.4 wireless networks. They examined the impact of sensing limitation and the power consumption of the various CCA methods on MAC performance and concluded that simulators that are used for performance evaluations, like ns-2 and OPNET, did not contain detailed models for PHY layer modules like CCA and need to be upgraded.

(Radio Regulation, 2012) studied Real-World Performance of Clear Channel Assessment in 802.15.4 Wireless Sensor Networks. In their experiment they used TmoteSkey motes with a CC2420 RF transceiver operating at 2.4 GHz band. The experiment involved two senders with the same distance to one receiver; the experiments were carried out in a closed room with no movement. All nodes operated on channel 26. They found that smaller CCA threshold results in a significant decrease in packet loss. The distance between sender and receiver and the power of senders were not stated in this study.

In this experiment we studied the effect of CCA value and the power level of genuine packets sent by a WSN node in presence of constant jammers and the effect of jamming generated by WSN nodes on PDR, PSR and RSSI because these are the most used parameters in jamming countermeasures.

The following WSN transceivers have been used in this experiment:

XBee RF Module:

XBee is a module designed by Digi International to meet IEEE 802.15.4 standards for low cost and low power WSN. XBee operates in an ISM 2.4 GHz radio band. The RF data packet structure follows the 802.15.4 specification (XBee RF Modules, 2015)

Figure (2.12) XBee RF Module (XBee RF Modules, 2015)

The XBee RF module connects to an external host device through an asynchronous serial port, which can communicate with a Universal Asynchronous Receiver/Transmitter (UART) compatible interface, as shown in Figure (2.3)

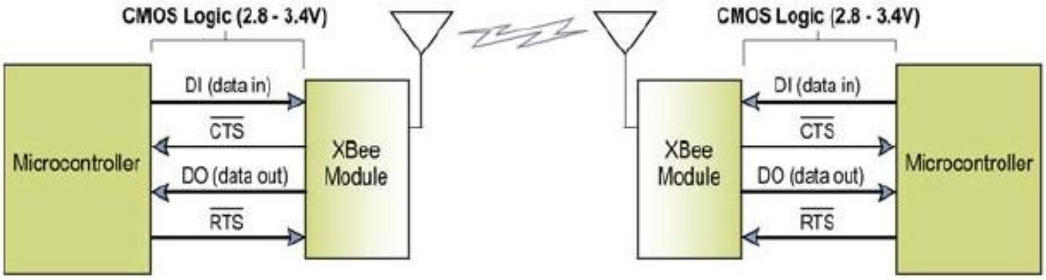


Figure (2.13) Serial communication of XBee (XBee RF Modules, 2015).

Data is received from a host though a DI pin (pin3) as an asynchronous serial. Each byte received starts with a start bit (low) followed by the least significant bits and ends with high the stop bit (high). The microcontroller and the RF module must be configured with similar settings such as baud rate, parity, data bits, start bits and stop bits.

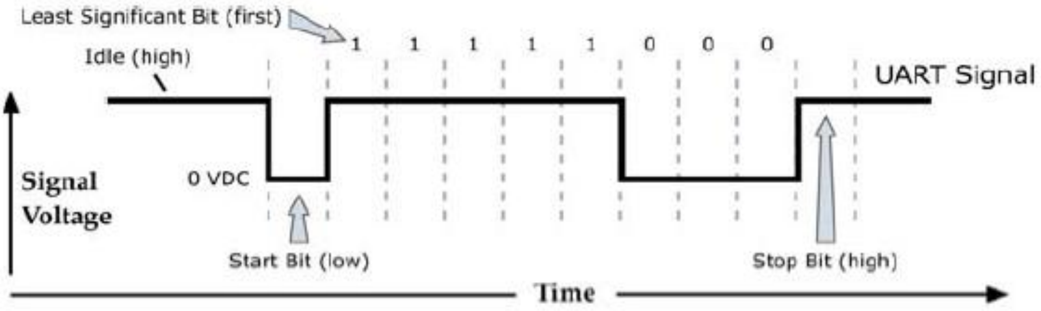


Figure (2.14) (XBee RF Modules, 2015)

By default the XBee module operates in transparent mode, as when the XBee module operates in this mode all data received from the DI pin is queued up for RF transmission and when RF data is received the data is sent out via DO pin. Data is buffered until one of the following incidents happens, then it will be packetised and transmitted:

1. No more data is received from the UART for an amount of time equal or more than the timeout period.
2. The number of characters received is equal to the maximum that can fit into the RF packet (100)
3. The command mode sequence (GT+CC+GT) is received

If the DI buffer becomes full, hardware or software flow control must be implemented in order to prevent overflow (XBee RF Modules, 2015).

In API Operation mode, a host application can interact with the networking capability of the module. XBee can send events within module or defined operations. Transmit

Data Frames (received from the DI pin (pin 3)) include:

- RF Transmit Data Frame
- Command Frame (equivalent to AT commands)

Receive Data Frames (sent out the DO pin (pin 2)) include:

- RF-received data frame
- Command response
- Event notifications such as reset, associate, disassociate.

In API mode a host application can send data frames that contain addresses and payloads. Data frames sent to the host contain status packets, source, RSSI and the payload information from received data packets (XBee RF Modules, 2015).

When API mode is enabled the frame format will be as in figure (2.15), cmdID identifies that the API messages will be in the cmdData frame.

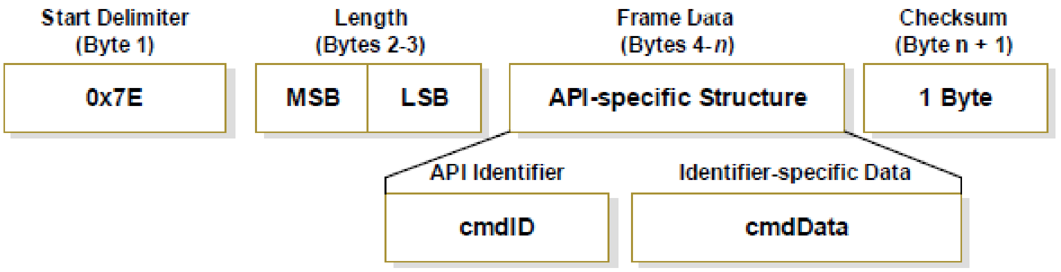


Figure (2.15) API frame format (XBee RF Modules, 2015)

TX (Transmit) Request

The cmdID value of 0x01 will trigger the RF module to transmit the packet.

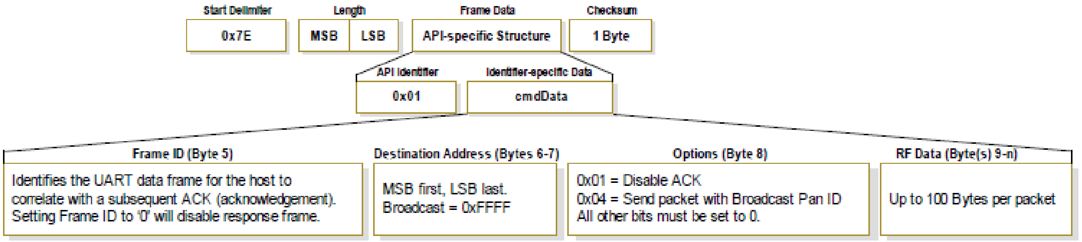

Start Delimiter
0x7E
Length
MSB
LSB
Frame Data
API-specific Structure
Checksum
1 Byte
API Identifier
0x01
Identifier-specific Data
cmdData
Frame ID (Byte 5)
Identifies the UART data frame for the host to correlate with a subsequent ACK (acknowledgement). Setting Frame ID to '0' will disable response frame.
Destination Address (Bytes 6-7)
MSB first, LSB last.
Broadcast = 0xFFFF
Options (Byte 8)
0x01 = Disable ACK
0x04 = Send packet with Broadcast Pan ID
All other bits must be set to 0.
RF Data (Byte(s) 9-n)
Up to 100 Bytes per packet

Figure (2.16) XBee frame cmdID value equal 0x01(XBee RF Modules, 2015)

TX (Transmit) Status:

When the TX request finishes the module sends the API message with cmdID equal to 0x89. It will indicate whether the packet transition was successful or failed

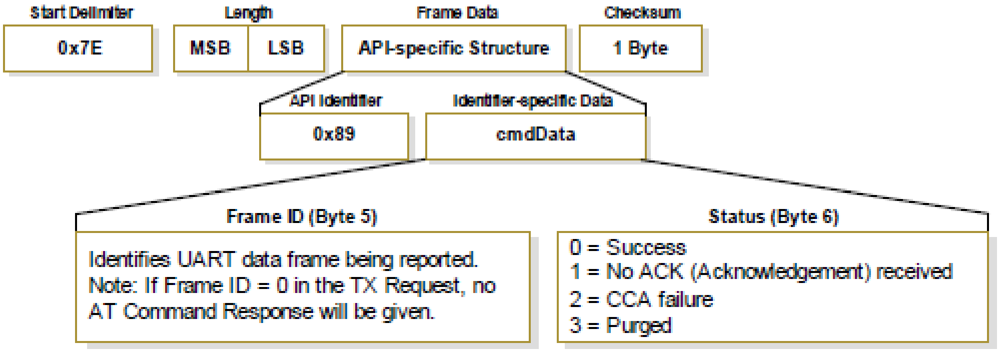


Figure (2.17) XBee frame cmdID value equal 0x89(XBee RF Modules, 2015)

RX Receive Packet

RF module passes on the UART message with cmdID equal to 0x81.

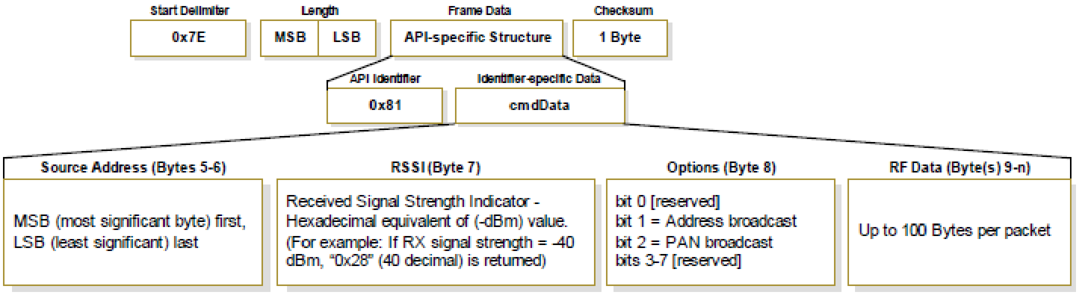

Start Delimiter
0x7E
Length
MSB
LSB
Frame Data
API-specific Structure
Checksum
1 Byte
API Identifier
0x81
Identifier-specific Data
cmdData
Source Address (Bytes 5-6)
MSB (most significant byte) first,
LSB (least significant) last
RSSI (Byte 7)
Received Signal Strength Indicator -
Hexadecimal equivalent of (-dBm) value.
(For example: If RX signal strength = -40
dBm, "0x28" (40 decimal) is returned)
Options (Byte 8)
bit 0 [reserved]
bit 1 = Address broadcast
bit 2 = PAN broadcast
bits 3-7 [reserved]
RF Data (Byte(s) 9-n)
Up to 100 Bytes per packet

Figure (2.18) XBee frame cmdID value equal 0x81 (XBee RF Modules, 2015)

Kmote-S1

Kmote-S1 is a wireless sensor node that comes with a humid/temp/light sensor board. It is supplied with an IEEE 802.15.4 compliant RF transceiver working on 2.4 to 2.4835 GHz, a globally compatible ISM band. Kmote-S1 is capable of transmitting at a 250 kbps data rate and it runs TinyOS 2.1.x (Madabhushi, 2007)

Figure (2.192) Kmote-S1 Mote (Madabhushi, 2007)

The hardware design of Kmote-S1 is identical to Telosb, the microcontroller (MSP430) and radio (CC2420) used in Kmote-S1.

CC2420 is an IEEE 802.15.4 compliant RF transceiver designed for low-power and low-cost WSN implementations. CC2420 contains a digital direct sequence spread spectrum (DSSS) modem, which provides a gain of 9dB and a data rate of 250 kbps. It works in 2.4 GHz ISM RF band and supports packet handling, data transmission, encryption and authentication, clear channel assessment (CCA) and link quality indication. Its features help to reduce the load on the host controller and transmit and receive data using a FIFO concept. CC2420 is used in many wireless sensor nodes such as MICAZ, Telosb and Kmote-S1 (Texas Instrument, 2014).

Kmote-S1 run open source operating system designed for low-power wireless devices called TinyOS, it is used in sensor networks, ubiquitous computing, personal area networks, smart buildings and smart meters. It is a tiny framework designed for systems that require very aggressive resource management due to the highly constrained nature of their resources, such as power and memory.

TinyOS is software that controls communication, routing, sensing and storage subsystems on sensor nodes and consists of the following:

Modules: which provide the implementation of one or more interfaces.

Configurations: which are used to assemble other components together (Suhonen et al., 2012; Levis, 2006).

3. Materials And Methodology

Running a test on a WSN is a challenging task because only a real sensor network testbed can provide the realistic testing to understand resource limitations, communication loss and energy constraints.

Designing and implementing a testbed is the main part of this research that allows us to conduct experiments with this model for the purpose of understanding the behaviour of the system and evaluating the effect of jamming on WSN.

The initial plan was to use Kmote-S1 motes with TinyOS 2.1 as the sender, receiver and jammers nodes. The below steps have been achieved for this purpose:

1. VMWARE workstation 10 was installed to host the Linux-based virtual machine.
2. The Ubuntu 14.04 LTS operating system was installed on a virtual machine to provide the environment to program the Kmote-S1 and Kmote-B sensor notes.
3. NesC is an extension to the C programming language and is designed to represent the structuring concepts and execution model of TinyOS 2.1. Therefore the Eclipse integrated development environment (IDE) and the Eclipse Plug-in (Yeti 2) was used for syntax highlighting, real-time code validation, code completion and providing various search tools.
4. TinyOS 2.1 was installed on Ubuntu virtual machine to upload the settings on Kmote-S1 and Kmote-B.

After starting the work of building the testbed using Kmote-S1 and Kmote-B several challenges were raised due to the complexity of building TinyOS applications and the relative high cost of TinyOS based nodes; therefore, a new testbed setup using XBee was used because it is lower in price and is easier to configure RF module parameters since all parameters can be configured using Graphical User Interface (GUI).

The Kmote-S1 nodes were used as jammers because disabling CSMA/CA is not possible on XBee firmware (10ed).

The new wireless sensor network testbed was built using two XBee series 1 802.15.4 OEM RF modules. Both XBee modules were connected to a computer by USB cables. XCTU is a multi-platform application installed on a managing computer XCTU used to configure and collect data from XBee RF modules. Two Kmote-S1 modules running TinyOS 2.1 were used as constant jammers, while CSMA-CA was disabled on jammers and configured to send packets with power level 0 dBm.

The focus in this study is on the effect of a jamming attack that was generated by one or more wireless sensor network nodes on PDR (Packet Delivery Ratio), PSR (Packet Send Ratio) and RSSI (Received Signal Strength Indication) parameters. The reason of choosing PDR, PSR and RSSI parameters in the study is because they are used in the majority of jamming attack countermeasures. This study assumes that jammers will have similar capability in terms of power and frequency band. The second part of the experiment aims to study the effect of changing the value of CCA on the PDR value in the presence of a jamming attack.

3.1 Experimental Setup

In this experiment two scenarios were carried out; the first scenario aimed to study RSSI, PSR and PDR values with a fixed CCA value and the second scenario studied the effect of CCA on PDR value. In both scenarios the sender and the receiver were placed at a separation of two metres. The experiment was performed in a non-isolated room in order to emulate a real life environment. IEEE 802.11 used a 2.4 GHz ISM radio spectrum except for channels 15, 20, 25 and 26, as in figure (4.2). Therefore, the WSN sender and receiver were configured to use channel 20 to avoid any conflict with IEEE 802.11, as shown in figure (4.2).

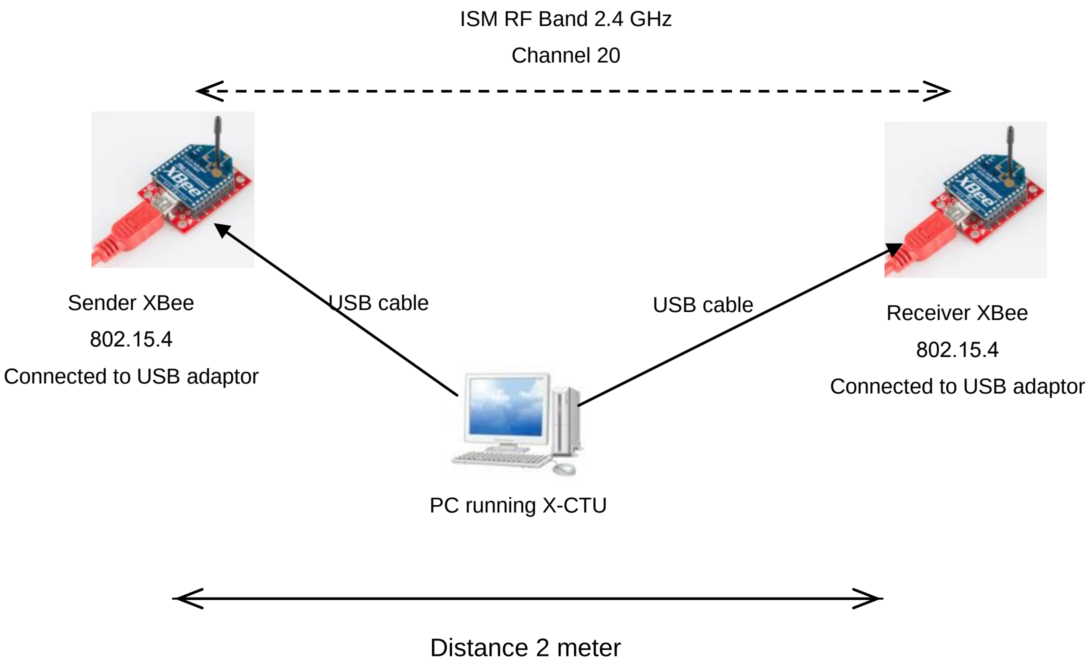


Figure (3.1) Experiment setup.

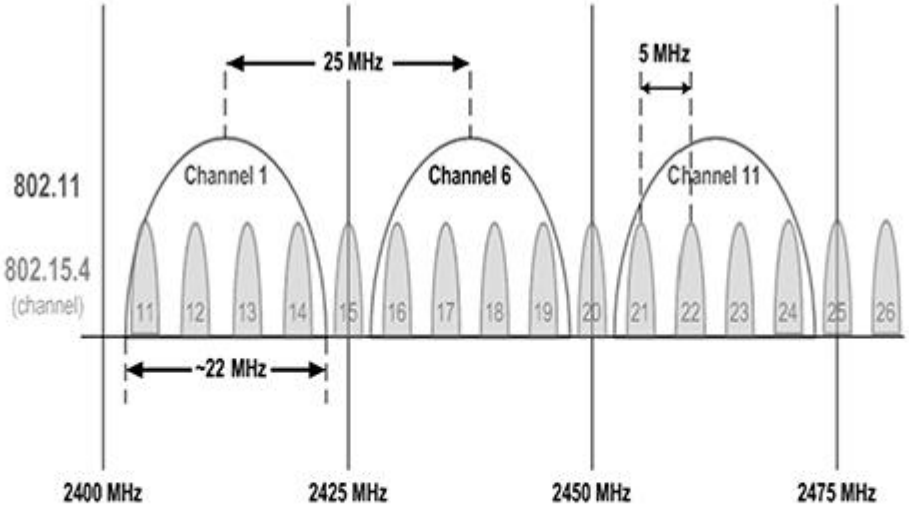
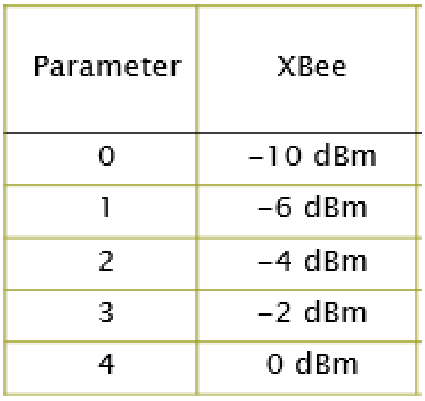


Figure (3.2) 2.4 GHz ISM radio spectrum

100 packet sizes of 10 bytes were sent from the sender to the receiver and a delay of 100ms occurred between packets at each scenario. Packets were collected on a PC using XCTU. Power level on Xbee series 1 with 10ef firmware can be configured with value of (0 dBm,-2 dBm,-4 V,-6 dBm ,-10 dBm), as shown in table (3)



Parameter	XBee
0	-10 dBm
1	-6 dBm
2	-4 dBm
3	-2 dBm
4	0 dBm

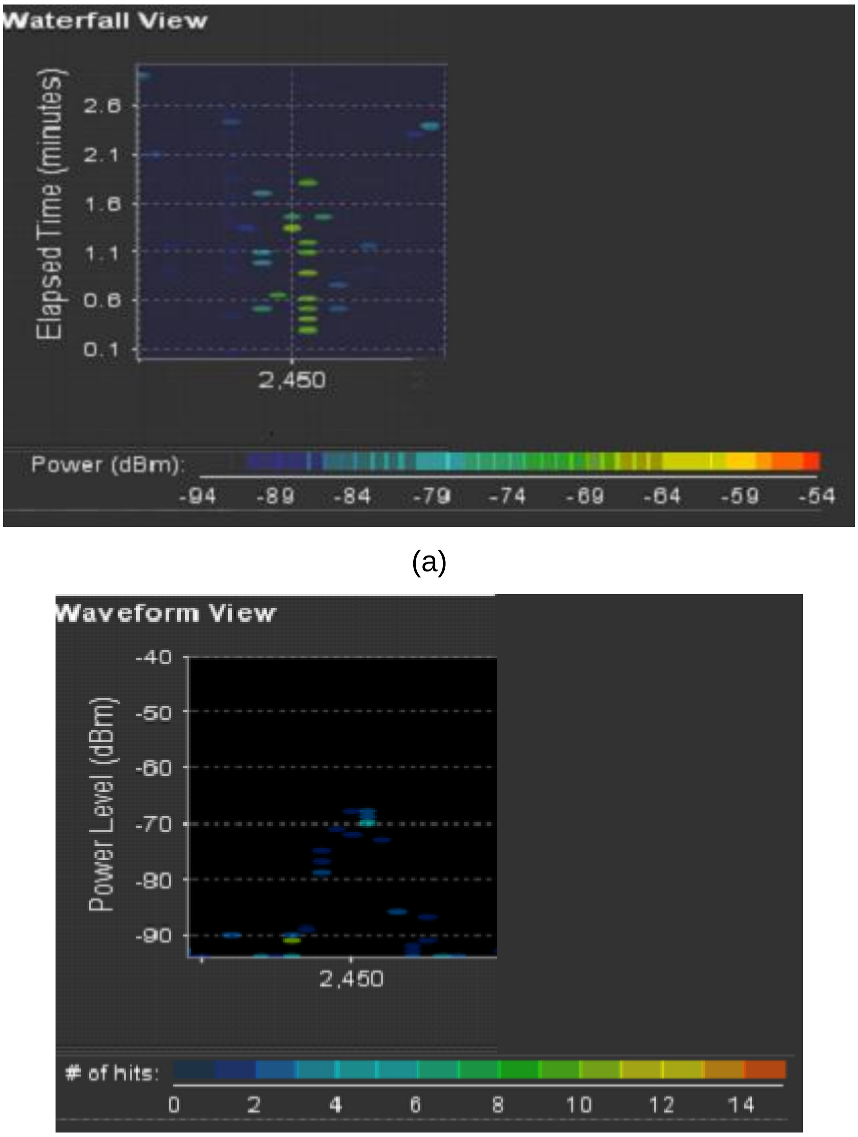
Table (3) Power level of XBee

The clear channel assessment (CCA) threshold value range for Xbee series 1 is 0x24 (-36 dBm) to ox50 (-80 dBm). The highest and lowest values of CCA and power level have been selected in scenarios to illustrate the best and worst performance under the jamming attack.

3.2 Scenario (1) the effect of jamming on RSSI, PSR and PDR

3.2.1 Scenario 1.1

100 Packets with a power level of -10 dBm were sent from sender node, while the Value of Clear Channel Assessment (CCA) was set to -80 dBm. No jammers were present in this scenario. The spectrum analyser (AirView) was placed at 1 metre distance from the sender, and the number of packets sent by the sender increased to 1,000 in order to get clear readings from the spectrum analyser.



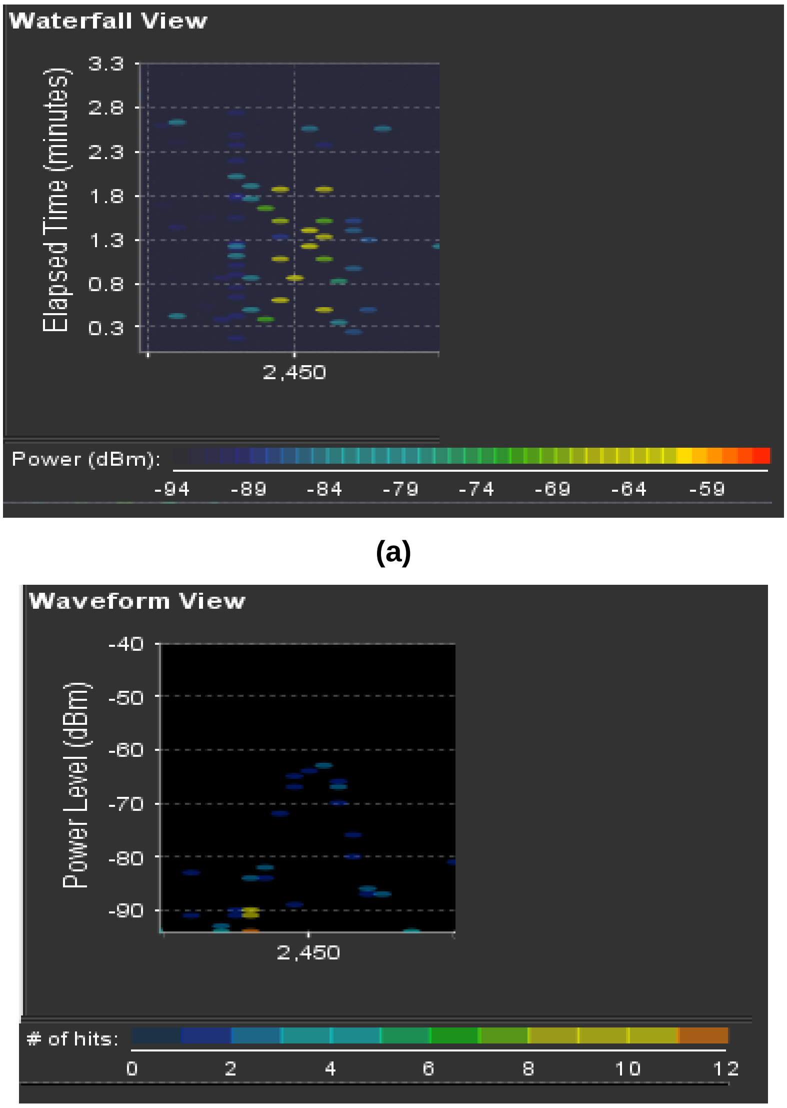
(a)

(b)

Figure (3.3) Readings from spectrum analyser show activities on channel 20 in absence of jamming power level -10dBm.

3.2.2 Scenario 1.2

100 Packets with power level of 0 dBm sent from sender node, Value of Clear Channel Assessment (CCA) on set to -80 dBm. No jammers present in this scenario. spectrum analyzer placed 1 meter distance from sender, In order to get clear reading on spectrum analyzer 1000 packets.



(a)

(b)

Figure (3.4) Readings from the spectrum analyser shows activities on channel 20 in the absence of the jamming power level 0dBm.

3.2.3 Scenario 1.3

100 Packets with power level of -10 dBm sent from sender node, Value of Clear Channel Assessment (CCA) on set to -80 dBm. Two jammers configured to use channel 20 the jammers were sending packets with power level 0 dBm, Jammers placed 1 meter from sender.

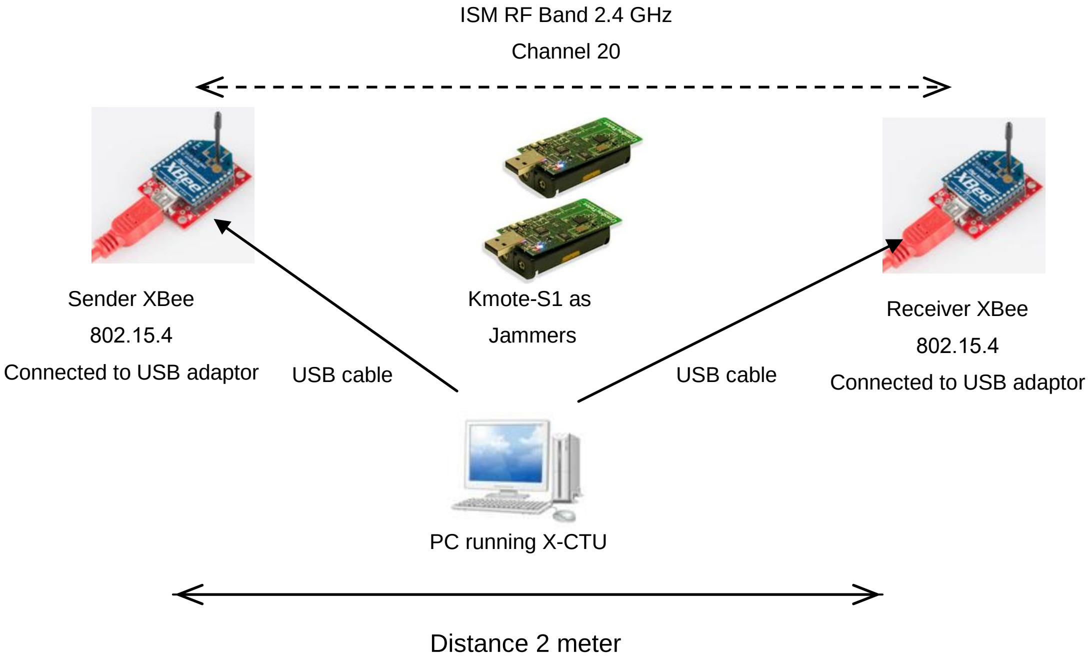
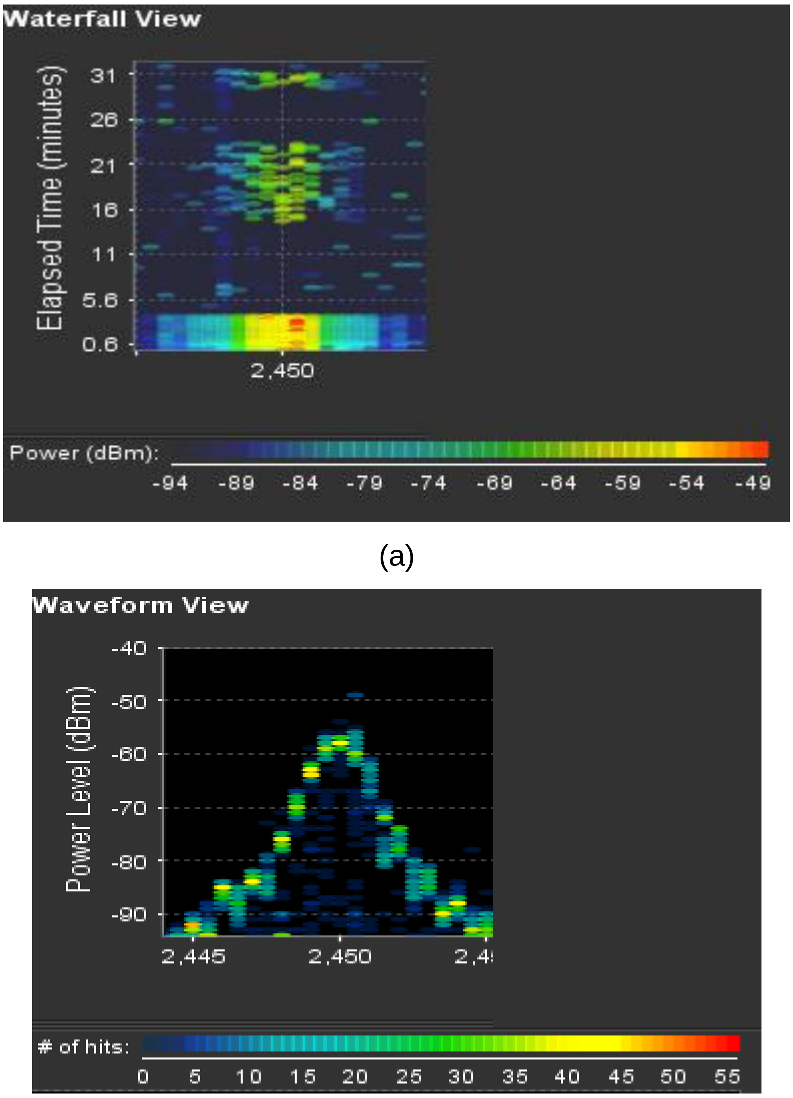


Figure (3.5) Experiment setup jammers were added to the setup



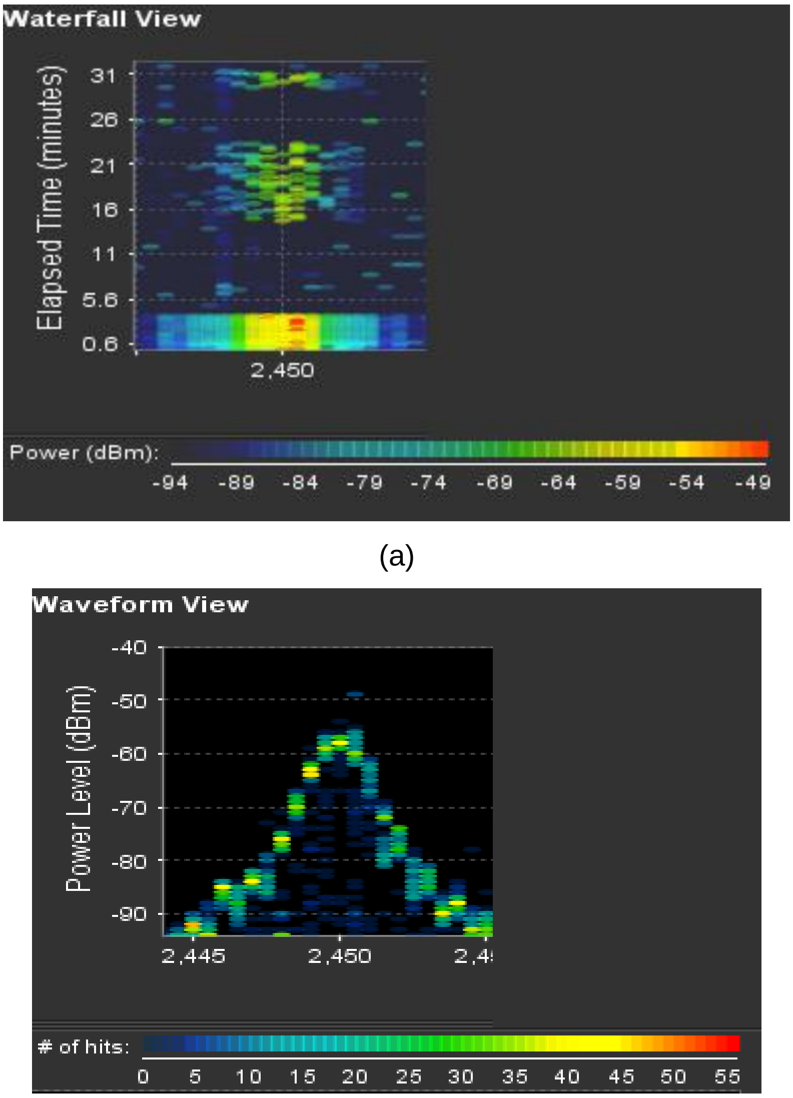
(a)

(b)

Figure (3.6) Readings from the spectrum analyser shows activities on channel 20 in the presence of jamming sending frames with a power level of 0 dBm.

3.2.4 Scenario 1.4

100 packets with a power level of 0 dBm were sent from the sender node, while the Value of Clear Channel Assessment (CCA) was set to -80 dBm. Two jammers were configured to use channel 20 and were sending packets with a power level of 0 dBm. Jammers were placed 1 metre from the sender.



(a)

(b)

Figure (3.7) Readings from spectrum analyser shows the activities on channel 20 in the presence of jamming sending frames with a power level of 0 dBm

3.3 Scenario (2) the Effect of changing CCA values on PDR in presence of jamming

In this scenario five different settings were implemented. In all scenarios 100 packets with power levels of -10 dBm were sent from the sender node but the Value of CCA changed on each scenario (-36, -51, -56, -67, -80) dBm. Two jammers were configured to use channel 20 and were sending packets with a power level of 0 dBm. Jammers were placed 1 metre from the sender.

3.4 Results analysis

3.4.1 Analyzing scenario (1)

3.4.1.1 Analysing RSSI

It has been observed that when sending low power packets (-10 dBm) in the absence of jamming the RSSI value for received packets was -66 dBm but when low power (-10 dBm) packets were sent with the existence of jammers the RSSI value for the received packets was -64 dBm. Similarly, the RSSI value for received high power (0 dBm) packets in the presence of jamming were higher than the RSSI on high power (0 dBm) packets received in the absence of jamming. It demonstrates that RSSI value in presence of noise will be inflated; the findings are compliant with the suggestion by gworle in the XBee-PRO XSC forum (Foster, 2011).

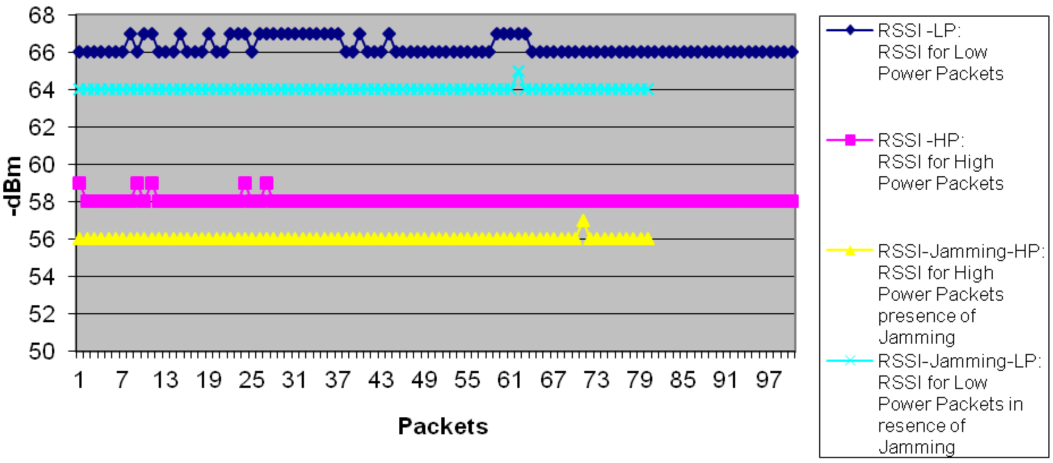


Figure (3.8) RSSI comparison jamming VS non-jamming

Where RSSI-LP: Is the RSSI reading on receiver node when packets are sent with low power. RSSI-HP: Is the RSSI reading on receiver node when packets are sent with high power. RSSI-Jamming-HP: Is the RSSI reading on receiver node when packets are sent with high power in presence of jamming. RSSI-Jamming-LP: Is the RSSI reading on receiver node when packets are sent with low power in the presence of jamming.

3.4.1.2 Analysing PSR and PDR results:

The Packet Send Ratio (PSR) was calculated, which is the number of packets that have been successfully sent out compared to number of packets that were intended to be sent by MAC. The PSR value equals 1 for all scenarios including in the presence of jamming. The hypothesis is that the sender was able to find a time slot to send frames. The reason is firstly because in the testbed Kmote-S1 nodes used as a constant jammer hence they have limited resources such as power level. Secondly, XBee uses Direct Sequence Spread Spectrum (DSSS) to modulate the frames before sending them to the physical layer; therefore, multiple users can randomly access communications and the RF channel with selective addressing (DeBruhl and Tague, 2011) (Pickholtz, Schilling and Milstein, 1982).

With a predetermined distance between sender and receiver and an absence of jamming (scenario 1.1,1.2) the Packet Delivery Ratio (PDR) value equals 1, but in the presence of jamming the PDR was 0.9 when the CCA value was -80 dBm. The PDR value is distressed by jamming because genuine packets had a collision with jammers packets.

The experiment demonstrates that in the presence of constant jamming, when increasing the power of the sent packets without considering the distance, this will not enhance the PDR value because the genuine sender and the jammers sending packets had the same power of 0 dBm but the jammers were closer to the receiver node.

3.4.2 Analysing the effect of changing CCA values on PDR

The XBee sender backs off when noise on the RF channel is higher than the CCA threshold (XBee RF Modules, 2015). The result of scenario (2) demonstrates that changing the CCA threshold value on the XBee RF module influenced the Packet Delivery Rate (PDR) value. Figure (28) shows that PDR is 0.8 when the CCA value equals -36 dBm and PDR increases when CCA decrease to reach 0.95 when the CCA value equals -80, so the findings of this experiment comply with the findings in the study carried by (Kiryushin, Sadkov and Mainwaring, 2008).

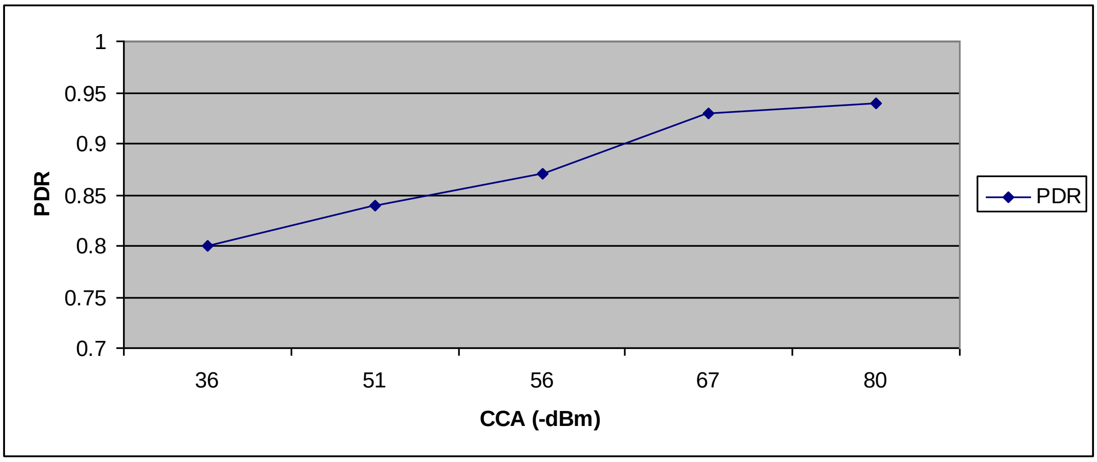


Figure (3.9) The PDR value changes with the changing of CCA.

Because both genuine sender and jammers configured with a similar power level of 0 dBm the jammers are closer to the receiver node as in figure (4.10). Therefore, the jammer packets will be stronger than genuine packets from the receiver's point of view so when a collision occurs the genuine packets will always be lost.

When the CCA threshold value is high in this situation the sender will send packets while the energy (noise) on channel is relatively high, i.e. there are packets generated by jammers in the channel; therefore, the probability of collision becomes high, which will decrease the PDR value.

When the CCA threshold value is low in this situation the sender will send packets while the energy (noise) on the channel is relatively low; therefore, the probability of collision becomes low, which will increase the PDR value.

Finally, it has been observed that there is another reason why the presence of jamming the CCA mechanism on the sender node may not succeed in detecting the activity on a channel if transmissions started less than 0.128ms before CCA sampling as the sender will send the packet simultaneously with jammers packets (Kiryushin, Sadkov and Mainwaring, 2008). Therefore, in the presence of jamming there will always be a packet loss and the PDR for XBee will always be less than 1.

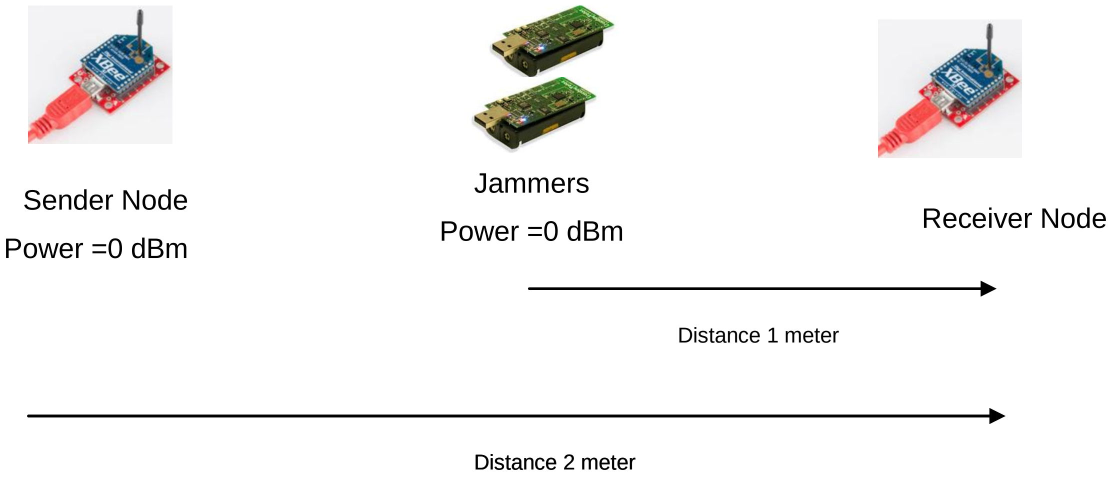


Figure (3.10) Shows jammers are closer to the receiver node

4. Conclusion and future work

The aim of this research is to study the effect of a jamming attack on parameters that are used by the majority of jamming attack countermeasures, such as PDR (Packet Delivery Ratio), PSR (Packet Send Ratio) and RSSI (Received Signal Strength Indication) parameters. Following the study of previous parameters, the effect of changing the value of CCA on the PDR value was studied in the presence of a jamming attack. The experiment was performed in a non-isolated room in order to emulate a real life scenario. WSN nodes were communicating using channel 20 to avoid conflicting with IEEE 802.11 signals.

The wireless sensor network testbed was built using two XBee series 1 802.15.4 OEM RF modules. Two Kmote-S1 modules running TinyOS 2.1 were used as constant jammers. This study presumes that jammers will have similar capability in terms of power and frequency band. CSMA-CA was disabled on jammers and configured to send packets with power level 0 dBm.

The study findings are:

1. The finding of the second scenario should be considered in manufacturing 802.15.4 RF transceivers to be equipped with the capability of configuring CCA value to lower than -80 dBm in order to enhance the PDR value in the presence of jamming or interference that is generated by compromised WSN nodes.
2. The RSSI measured value by XBee is affected by the jamming activity. This fact needs to be considered when utilizing this parameter in jamming attack countermeasures and other implementations such as using XBee in real-time position detection and motion tracking by using RSSI.
3. Overcoming the consequence of collisions that occur between genuine packets and jamming packets is by increasing the power of the genuine signal or by changing the location of the sender node to be closer to the receiver node.
4. When WSN nodes are compromised and used as constant or deceptive jammers they will not be very efficient because they will be consuming the power before the victims.

Areas for future work will include developing a technique to detect and isolate the source of jamming in wireless sensor networks utilizing the parameters (RSSI, PDR, PSR, CCA) that have been studied in this research while considering the findings in this study.

Reference

Acs, G. and Buttyan, L. (2008). *Secure Routing in Wireless Sensor Networks* . In: Lopez, J. and Zhou, J. editors, Wireless Sensors Networks Security. Amsterdam: IOS Press, pp 164-203.

Ajmeri, A. (2013). *Field wireless network ISA-100.11a and other wireless technologies are making inroads into process control and measurement application*. [Online] Available at: https://www.isa.org/standards-publications/isa-publications/intech-magazine/2013/december/field-wireless-networks/ [Accessed 2/3/2015].

Andrews, J. (2012). *A+ Guide to Software Hardcover*. [Online] United State of America: Cengage learning.Available at: https://books.google.com.qa/books?id=fxT7CAAAQBAJ&printsec=frontcover&dq=A%2B+Guide+to+Software+Hardcover&hl=en&sa=X&redir_esc=y#v=onepage&q&f=false [Accessed 2/4/2015],pp353-358.

Augustus, C. et al., (2006). Domotics *Over IEEE 802 . 15 . 4 - A Spread Spectrum Home Automation Application.* , pp.396–400.

Baccour, N., Koubâa, A., Noda, C., Fotouhi, H., Alves, M., Youssef, H., Zúñiga, M.A., Boano, C.A., Römer, K., Puccinelli, D., Voigt, T. and Mottol, L. (2013). *Radio Link Quality Estimation in Low-Power Wireless Networks*. pp 23-24.

Bandyopadhyay, B., Ahmed, S., Das, D. and Chatterjee, A. (2014). *AS 802.15.4: A modified IEEE 802.15.4 standard for more reliable communication and utilization of inactive period using optimized sleep period*. Annual IEEE India conference, pp 1-6.

Bertocco, M., Gamba, G. and Sona, A. (2008). *Is CSMA/CA really efficient against interference in a Wireless Control System? An experiment answer*. ISBN: 1-4244-1506-3, pp 885-892.

Boano, C., Voigt, T., Noda, C., Romer, K. and Zuniga, M. (2011). *JamLab: Augmenting Sensornet Testbeds with Realistic and Controlled Interference Generation*. IPSN 11.

Boyes W. (ed.) (2009). *Instrumentation Reference Book*. United Kingdom: Slsevier, pp 255-261.

Bullock, S.R. (2014). *Transceiver and System Design for Digital Communications*. 4th edn. [Online] New York: UBM Tech. Available at: http://www.eetimes.com/document.asp?doc_id=1271899#msgs [Accessed 15/2/2015].

Buratti, C., Martalo, M., Ferrari, G. and Roberto, V. (2011). *Sensor Networks with IEEE 802.15.4 Systems*. pp7.

Butenko, S., Pasiliao, E. and Shylo, V. (2014). *Examining Robustness and Vulnerability of Networked Systems*. [Online] United State of America: The authors and IOS Press, pp 280-281. Available at: https://books.google.com.qa/books?id=3R7pAwAAQBAJ&pg=PP5&lpg=PP5&dq=Examining+Robustness+and+Vulnerability+of+Networked+Systems&source=bl&ots=jXDAbNLroI&sig=e6-jR4qHn-3rKFrG4kBrUk1W6L4&hl=en&sa=X&ei=twdyVbGBBo-YyAS35YLIAw&redir_esc=y#v=onepage&q=Examining%20Robustness%20and%20Vulnerability%20of%20Networked%20Systems&f=false. [Accessed 2/4/2015]

Chen, Y. and Terzis, A. (2010). *On the Mechanisms and Effects of Calibrating RSSI Measurements for 802.15.4 Radios*, pp 256-271.

Chitode, J. (2009). *Principles Of Communication*. [Online] India: Technical Publications Pune, pp 124,156,157. Available at: https://books.google.com.qa/books?id=6Zunu4Acfg8C&printsec=frontcover&dq=]+Principles+Of+Communication++By+Dr.J.S.Chitode+,2009&hl=en&sa=X&ei=UZd0VeGYNoq8ygOS64G4Ag&redir_esc=y#v=onepage&q=]%20Principles%20Of%20Communication%20%20By%20Dr.J.S.Chitode%20%2C2009&f=false [Accessed 12/3/2015].

Chiuso, A., Fortuna, L., Frasca, M., Rizzo, A., Schenato, L. and Zampier, S.(2009). *Modelling, Estimation and Control of Networked Complex Systems*.[Online] India:

Springer, pp 130-131. Available at: https://books.google.com.qa/books?id=CyhLpzwMFEQC&pg=PR4&lpg=PR4&dq=Modelling,+Estimation+and+Control+of+Networked+Complex+Systems++By+Alessandro+Chiuso,+Luigi+Fortuna,+Mattia+Frasca,+Alessandro+Rizzo,+Luca+Schenato,+Sandro+Zampier&source=bl&ots=uNS9Atf0NR&sig=NcfN3UXuuBbborPxZzza7m91PyU&hl=en&sa=X&ei=YmBWVa6BJIvaU8T8gJAE&redir_esc=y#v=onepage&q=Modelling%2C%20Estimation%20and%20Control%20of%20Networked%20Complex%20Systems%20%20By%20Alessandro%20Chiuso%2C%20Luigi%20Fortuna%2C%20Mattia%20Frasca%2C%20Alessandro%20Rizzo%2C%20Luca%20Schenato%2C%20Sandro%20Zampier&f=false. [Accessed 11/4/2015]

Coleman, D and Westcott, D. (2012). *CWNA: Certified Wireless Network Administrator Official Study Guide*, 3nd edn. Canada: John Wiley&Sons,Ins, pp87-193.

DeBruhl, B. and Tague, P. (2011). *Digital Filter Design for Jamming Mitigation in 802.15.4 Communication*. Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference, pp 1-6.

Digi (2009). *XBee®/XBee-PRO® RF Modules*. [Online] Available at:https://www.sparkfun.com/datasheets/Wireless/Zigbee/XBee- Datasheet.pdf. [Accessed 23/4/2015].

Digi (2015). *Is RSSI the best indication of link quality?*. [Online] Available at: http://www.digi.com/support/kbase/kbaseresultdetl?id=2084. [Accessed 16/4/2015].

Digi (2015). *Sending data through an 802.15.4 network latency timing*. [Online] Available at: http://www.digi.com/support/kbase/kbaseresultdetl?id=3065. [Accessed 12/4/2015]

Ericsson AB, (2010). *BLUETOOTH SPECIFICATION Version 4.0 [Vol 0]*. Pp 1-160.

Faludi, R. (2011). *Building wireless sensor networks*. [Online] United State of America: O'reilly. Available at: http://ab-log.ru/files/File/books/WirelessSensorNetwork.pdf [Accessed 19/3/2015].

Farahani, S. (2008). *ZigBee Wireless Networks and Transceivers*. [Online] United State of America: Elsevier, page 143-145. Available at: http://www.chiaraburatti.org/uploads/teaching/ZigBee-Libro.pdf . [Accessed 12/4/2015]

Finne, M. (1996). *Methods for Direction-Finding of Direct-Sequence Spread-Spectrum Signals.* Sweden: DIANE, pp 3.

Flammini, A., Marioli, D., Mazzoleni, G., Sisinni, E. and Taroni, A. (2006). *Received Signal Strength Characterization for Wireless Sensor Networking*. Instrumentation and Measurement Technology Conference. Proceedings of the IEEE, pp 207-211.

Foster, J. (2011). *XBee Cookbook Issue 1.4 for Series 1 (Freescale) with 802.15.4 Firmware*. [Online] Available at: http://www.jsjf.demon.co.uk/xbee/xbee.pdf. [Accessed 29/2/2015]

Frai, D. and Reichman, A. (2002). *Direct-Sequence Spread-Spectrum Fast Acquisition Architectures in the Presence of Time and Frequency Uncertainty*. Electrical and Electronics Engineers, pp192-196.

Gutierrez, J., Winkel, L., Callaway, E. and Barrett, R. (2011). *Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensors with IEEE 802.15.4*. United State of America: Wiley.

Hanna, S. a. & Sydor, J., (2012*). Distributed sensing of spectrum occupancy and interference in outdoor 2.4 GHz Wi-Fi networks*. GLOBECOM - IEEE Global Telecommunications Conference, (September 2011), pp.1453–1459.

Hanna, S. a. & Sydor, J., (2012). *Distributed sensing of spectrum occupancy and interference in outdoor 2.4 GHz Wi-Fi networks*. GLOBECOM - IEEE Global Telecommunications Conference, (September 2011), pp.1453–1459.

http://www.libelium.com/802-15-4-vs-zigbee , April 28th, 2009 - David Gascón --- November 2013

Hunn, N. (2010). *Essentials of Short-Range Wireless*. United Kingdom: Cambridge University Press.

Khan, S., Pathan, A. and Alrajeh, N. (ed.) (2012).*Wireless Sensor Networks: Current Status and Future Trends*. [Online] United State of America: Taylor & Francis Group, pp 34-36,74-76. Available at: https://books.google.com.qa/books?id=A1DOBQAAQBAJ&printsec=frontcover&dq=Wireless+Sensor+Networks:+Current+Status+and+Future+Trends&hl=en&sa=X&redir_esc=y#v=onepage&q=Wireless%20Sensor%20Networks%3A%20Current%20Status%20and%20Future%20Trends&f=false [Accessed 27/2/2015].

King, A., Brown, J. and Roedig, U. (2014). *DCCA: Differentiating Clear Channel Assessment for Improved 802.11/802.15.4 Coexistence*. ISBN: 978-1-4799-5041-6, pp 45-50.

Kiryushin, A., Sadkov, A. and Mainwaring, A. (2008). *Real-World Performance of Clear Channel Assessment in 802.15.4Wireless Sensor Networks*. pp625 – 630.

Lee, H.,Kim,A. and Shin, Y. (2012).*Retransmission Algorithm for Channel Allocation in IEEE 802.15.4 LR-WPAN*. pp 657- 664.

Levis, P. (2006). *TinyOS Programming*. pp 27.

Madabhushi, N. (2007). *KMote - Design and Implementation of a Low Cost, Low Power Hardware Platform for Wireless Sensor Networks*. Indian, pp 1-28.

Manju, VC. and Sasi, M. (2012). *Detection of Jamming Style DoS attack in Wireless Sensor Network. IEEE International Conference on Parallel, Distributed and Grid Computing*. PP 563-567.

McClaning, K. (2012). *Wireless Receiver Design for Digital Communications*, 2nd edn. [Online]: United State of America: SciTech. Available at: http://www.scitechpub.com/mcclaning/mcclaning_new.pdf. [Accessed 19/2/2015]

Misic, J. and Misic, V. (2008). Wireless *Personal Area Networks: Performance, Interconnection, and Security with IEEE 802.15.4*. [Online] United Kingdom : John

Wiley & Sons, pp 18-38. Available at: https://books.google.com.qa/books?hl=en&lr=&id=BAZf0O_UTgoC&oi=fnd&pg=PR7&dq=Wireless+Personal+Area+Networks:+Performance,+Interconnection,+and+Security+with+IEEE+802.15.4&ots=JHdUz2RyDu&sig=oKwz1vBBs6z0E6FXHlz442kRHvQ&redir_esc=y#v=onepage&q=Wireless%20Personal%20Area%20Networks%3A%20Performance%2C%20Interconnection%2C%20and%20Security%20with%20IEEE%20802.15.4&f=false [Accessed 2/5/2015].

Misra, S., Woungang, I. and Misra, S. (ed.) (2009). *Guide to Wireless Sensor Networks*. [Online] United kingdom: Springer-Verlag London Limited, pp 28-31,205-215. Available at: https://books.google.com.qa/books?id=Iz8gm2BQO1IC&printsec=frontcover&dq=Guide+to+Wireless+Sensor+Networks++By+Sudip+Misra,+Isaac+Woungang,+Subhas+Chandra+Misra,2009&hl=en&sa=X&ved=0CB4Q6AEwAGoVChMIsMCsw-yFxgIV5sByCh3hbgDB#v=onepage&q=Guide%20to%20Wireless%20Sensor%20Networks%20%20By%20Sudip%20Misra%2C%20Isaac%20Woungang%2C%20Subhas%20Chandra%20Misra%2C2009&f=false [Accessed 10/4/2015].

Molisch, A. (2012). *Wireless Communications*. [Online] United Kingdom: John Wiley & Dons Ltd. Available at: https://books.google.com.qa/books?id=877tFGeQo5oC&printsec=frontcover&dq=inauthor:%22Andreas+F.+Molisch%22&hl=en&sa=X&ved=0CCEQ6AEwAWoVChMIjbSsrPGFxgIVJe1yCh1p9wD1#v=onepage&q&f=false [Accessed 11/5/2015].

Morparia, K., Shah, P. and Shah, B. (2007*). Experimental Sutdy of Coneurrent Packet Transmission in Wireless Sensor Networks using Tmote Sky devices*. EE652, pp 1-8.

Mpiziopoulos, A., Gavalas, D., Konstantopoulos, C. and Pantziou, G. (2009) *A Survey on jamming Attacks and Countermeasures in WSN*. IEEE Communications Surveys & Tutorials, pp 42-56.

Muntwyler, B., Lenders, V., legendre, F. and Plattner, B. (2012). *Obfuscating IEEE 802.15.4 Communication Using Secret Spreading Codes*.

Muraleedharan, R. and Osadciw, L.A (2006). *Jamming Attack Detection and Countermeasures In Wireless Sensor Network Using Ant System*. Department of Electrical Engineering and Computer Science Syracuse University. NY 13244-1240.

Ncalculators (2015).*Signal to Noise Ratio Calculator*. [Online] Available at: http://ncalculators.com/statistics/signal-noise-ratio-calculation.htm [Accessed 19/2/2015].

Parker, M. (2010).*Digital Signal Processing 101*. [Online] United State of America: Elsevier, pp 154-156. Available at: http://bayanbox.ir/view/4555413509589846957/Digital-Signal-Processing-101-Everything-you-need-to-know-to-get-started-Elsevier-2010.pdf [Accessed 2/3/2015].

Pickholtz, R., Schilling, D. and Milstein,L. (1982). *Theory of Spread-Spectrum Communications-A Tutorial*. IEEE Transaction on Communications, pp 855-884.

Prabakaran, P. (2003). *Tutorial on Spread Spectrum Technology*. [Online] available at: http://www.eetimes.com/document.asp?doc_id=1271899 [Accessed 23/1/2015].

Radio Regulations, Edition of 2012. ITU-R. Retrieved 2014-11-10.

Ramachandran, I. and Roy, S. (2006). *On the Impact of Clear Channel Assessment on MAC Performance*. National Science Foundation under Grant ANI 0325014 (ITR: Network to Assist Disaster Rescue), pp 1-5.RESCUENET-Embedded In-Building Sensor

Sauter, M. (2011). *From GSM to LTE*. pp 83.

Sauter, M.(2011).*From GSM to LTE: An Introduction to Mobile Networks and Mobile Broadband*. [Online]United KingDom: John Wiley & Sons, Ltd. Available at: https://aliazizjasem.files.wordpress.com/2012/01/mobile_networks2.pdf. [Accessed 26/4/2015]

Siddhabathula, K., Dong, Q., Lui, D. and Wright, M. (2012). Fast *Jamming Detection in Sensor Network*. ISBN: 978-1-4577-2053-6, pp 934-938.

Singal, T. (2010). *Wireless Communications*. [Online] India : Tata McGraw Hill Education Private Limited, pp 451-461. https://books.google.com.qa/books?id=cQJJzA8CCUUC&printsec=frontcover&dq=Wireless+Communications++by++T.+L.+Singa,+2010&hl=en&sa=X&ei=hpx0VdmUGIWysQHciYCQBw&ved=0CC8Q6AEwAw#v=onepage&q&f=false [Accessed 26/2/2015].

Suhonen, J., Kohvakka, M., Hämäläinen, V.K.T.D. and Hännikäinen, M. (2012). *Software And Middleware Services. In: Low-Power Wireless Sensor Networks*. New York: Springer, pp 43-59.

Sun, Y. and Wang, X. (2010). *Jamming Attacks and Countermeasures in Wireless Sensor Networks*. IGI global, pp 334 – 351.

Tang, Y. et al., (2013). *Interference aware adaptive clear channel assessment for improving zigbee packet transmission under Wi-Fi interference*. 2013 IEEE International Conference on Sensing, Communications and Networking, SECON 2013, pp.336–343.

Tennina, S., Koubâa, A. and Daidone, R. (2013). *IEEE 802.15.4 and ZigBee as Enabling Technologies for Low-Power Wireless Systems with Quality-of-Service Constraints. New York: springer*, pp 8,14

Texas Instrument (2014) . *2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver* .[Online] available at : http://www.ti.com/lit/ds/symlink/cc2420.pdf [accessed 23/4/2105]

Wong, C., (2010). An *Additional Clear Channel Assessment for IEEE*. Networks, pp.62–66.

Xiao, Y. and Pan, Y. (ed.) (2009). *Emerging Wireless LANs, Wireless PANs, and Wireless MANs IEEE 802.11, IEEE 802.15, 802.16 Wireless Standard Family*. [Online] United State of America: John Wiley & Sons Inc, pp 648. Available at:

Xu, W., Trappe, W., Zhang, Y. and Wood, T. (2005). *Wireless Information Network Laboratory (WINLAB)*. Rutgers University, NJ 08854.

Zhang, J., Tan, K., Zhao, J., Wu, H. and Zhang, Y. (2008). *A Practical SNR-Guided Rate Adaptation. Conference on Computer Communications IEEE*, pp 2083-2091.

Zhang, Y. and Kitsos, P. (ed.) (2009). *Security in RFID and Sensor Networks (Wireless Networks and Mobile Communications)*. [Online] United State of America: Taylor and Francis Group. Available at: https://books.google.com.qa/books?id=lPEwic6W1RgC&printsec=frontcover&dq=Security+in+RFID+and+Sensor+Networks&hl=en&sa=X&ei=CA1yVfnVAsPnywPTwYKYBA&redir_esc=y#v=onepage&q=Security%20in%20RFID%20and%20Sensor%20Networks&f=false. [Accessed 2/3/2015]

Zheng, G. et al., 2011. A *Link Quality Inference Model for IEEE 802 . 15 . 4. GLOBECOM - IEEE Global Telecommunications Conference*, pp.2–7.

Tennina, S., Koubâa, A. and Daidone, R. (2013). *IEEE 802.15.4 and ZigBee as Enabling Technologies for Low-Power Wireless Systems with Quality-of-Service Constraints. New York: springer*, pp 8,14.