HELSINKI UNIVERSITY OF TECHNOLOGY
Faculty of Electronics, Communications and Automation
Department of Communications and Networking

Umer Javed

Frequency hopping in wireless sensor networks

Thesis submitted in partial fulfilment of the requirement for the degree of Master of Science in Technology in Espoo, Finland, March 2009.

Supervisor: Professor Riku Jäntti
Instructor: M.Sc. Aamir Mahmood

ABSTRACT of the Master's thesis

Author: Umer Javed
Name of the thesis: Frequency hopping in wireless sensor networks
Date: March 2009 **Number of pages:** 58

Faculty: Faculty of Electronics, Communications and Automation
Professorship: S-72 Communications Engineering

Supervisor: Professor Riku Jäntti
Instructor: M.Sc. Aamir Mahmood

Wireless sensor networks (WSNs) are nowadays being used to collectively gather and spread information in different kinds of applications, for military, civilian, environmental as well as commercial purposes. Therefore the proper functioning of WSNs under different kinds of environmental conditions, especially hostile environments, is a must and a lot of research currently ongoing. The problems related to the initialization and deployment of WSNs under harsh and resource limited conditions are investigated in this thesis.

Frequency hopping (FH) is a spread spectrum technique in which multiple channels are used, or hoped, for communications across the network. This mitigates the worst effects of interference with frequency agile communication systems rather than by brute force approaches. FH is a promising technique for achieving the coexistence of sensor networks with other currently existing wireless systems, and it is successful within the somewhat limited computational capabilities of the sensor nodes hardware radios.

In this thesis, a FH scheme for WSNs is implemented for a pair of nodes on an application layer. The merits and demerits of the scheme are studied for different kinds of WSN environments. The implementation has been done using a Sensinode NanoStack, a communication stack for internet protocol (IP) based wireless sensor networks and a Sensinode Devkit, for an IPv6 over low power wireless personal area network (6LoWPAN). The measurements are taken from the developed test bed and channel simulator for different kinds of scenarios. The detailed analysis of the FH scheme is done to determine its usefulness against interference from other wireless systems, especially wireless local area networks (WLANs), and the robustness of the scheme to combat fading or frequency selective fading.

Keywords: Wireless Sensor Networks, Frequency Hopping, Time Synchronization, IEEE 802.15.4, 6LoWPAN.

Acknowledgements

This thesis work has been done in the Department of Communications and Networking (Comnet) of Helsinki University of Technology.

I would like to thank to my thesis supervisor Professor Riku Jäntti for giving me the opportunity to work with him and for the countless patience and dedication he has shown during this thesis work. Also many thanks to my thesis instructor Aamir Mahmood for all of his help and guidance he gave me during these months. English proofreading of this work has been done by William Martin, thanks to him for giving his time.

Special thanks to Viktor, Aftab, Shekar and Tarikul of Comnet for their help in the completion of this thesis.

Finally, an infinite love to my father, mother, brother and sister who have loved, helped and guided me for whole of my life.

I am grateful to the Allah Almighty for his blessings.

Umer Javed.

Espoo, Finland, March 2009.

Table of Contents

ABSTRACT of the Master's thesis....2
Acknowledgements....3
List of abbreviations....6
Introduction....8
1.1 Motivation....8
1.2 Problem formulation and contribution....8
1.3 Thesis outline....9
6LoWPAN/IEEE 802.15.4 Introduction....10
2.1 6LoWPAN....10
2.2 IEEE 802.15.4 PHY specification....11
2.2.1 Frequencies of operation and data rates....12
2.2.2 Channel assignments....14
2.2.3 Channel selection....16
2.2.5 Energy detection....18
2.2.6 Carrier sense....19
2.2.7 Link quality indicator....19
2.2.8 Clear channel assessment....19
2.3 IEEE 802.15.4 MAC specification....20
2.3.1 Beacon mode and nonbeacon mode....20
2.3.2 MAC frame structures....21
2.3.2.1 Beacon frame....22
2.3.2.2 Data frame....22
2.3.2.3 Acknowledgment frame....22
2.3.2.4 MAC command frame....22
Time synchronization in sensor networks....24
3.1 Introduction....25
3.2 Time synchronization challenges....25
3.3 Common time synchronization protocols....26
3.3.1 Reference broadcast synchronization (RBS)....26
3.3.2 Flooding time synchronization protocol (FTSP)....27
3.3.3 Time synchronization protocol sensor networks (TPSN)....28
3.4 TPSN used in this thesis....30
Frequency hopping....31
4.1 Frequency hopping....31
4.2 Adaptive frequency hopping....33
4.2.1 Adaptive frequency hopping limitations....34
4.3 Anti jamming in wireless sensor networks....34
IEEE 802.15.4 coexistence....36
5.1 Coexistence....36
5.2 IEEE 802.15.4 non-collaborative coexistence mechanisms....38
5.2.1 CSMA-CA channel access....38
5.2.2 Frequency hopping....38
5.2.3 Adjacent and alternate channel performance....39
5.2.4 Extremely low duty cycle....39
5.2.5 Dynamic RF output power selection....39
5.2.6 Signal spreading....40

5.2.7 Mesh networking and location aware routing....40
5.2.8 Adaptive packet length selection....40
5.3 Coexistence studies....41
Frequency hopping architecture and performance analysis....46
6.1 Testbed architecture....47
6.1.1 Software components....47
6.1.1.1 NanoStack....47
6.1.1.2 FreeRTOS....48
6.1.2 Testbed....49
6.2 Frequency hopping algorithm....51
6.3 Frequency hopping in IEEE 802.15.4 under IEEE 802.11b....53
6.4 Channel center frequency offset between IEEE 802.15.4 and IEEE 802.11.b....55
Frequency hopping in fading channels....58
7.1 Wireless channel....58
7.1.1 Multipath propagation....58
7.1.2 Time varying channel....59
7.1.3 Fading distributions....60
7.2 Testbed....62
7.3 Channel models....63
7.4 Frequency hopping in frequency selective fading channel....67
7.4.1 Model A....68
7.4.2 Model B....68
7.4.3 Model C....69
7.4.3 Model D....69
Conclusion and future work....70
References....71

List of abbreviations

6LoWPAN IPv6 over low power wireless personal area network
AFH adaptive frequency hopping
API application programming interface
ASK amplitude shift keying
BPSK binary phase shift keying
CCA clear channel assessment
CRC cyclic redundancy check
CS carrier sense
CSMA-CA carrier sense multiple access with collision avoidance
DSSS direct sequence spread spectrum
ED energy detection
FH frequency hopping
FTSP flooding time synchronization protocol
GTS guaranteed time slot
ICMPv6 internet control message protocol version 6
IETF internet engineering task force
IP internet protocol
IPv6 internet Protocol version 6
ISI inter symbol interference
ISM industrial, scientific and medical
LOS line-of-sight
LoWPAN low power wireless personal area network
LQI link quality indicator
MAC medium access control
MGEN multi-generator
MTU maximum transmission unit
MULEPRO multichannel exfiltration protocol
NLOS non-line-of-sight
O-QPSK offset quadrature phase shift keying
OCDM orthogonal code division multiplexing
PAN personal area network
PARSEC parallel simulation environment for complex systems
PER packet error rate
PHY physical layer
PN pseudo-random noise
POSIX portable operating system interface
PSK phase shift keying
PSSS parallel sequence spread spectrum
QoS quality of service
QPSK quadrature phase shift keying
RBS reference broadcast synchronization
RF radio frequency
RSSI received signal strength indicatior
SIR signal-to-interference ratio
TAG technical advisory group

TCP transmission control protocol
TDMA time division multiple access
TG2 task group 2
TPSN time synchronization protocol sensor networks
UDP user datagram protocol
WLAN wireless local area network
WSN wireless sensor network
ZDO ZigBee device object

Chapter 1

Introduction

1.1 Motivation

In the last decade due to the extraordinary rate of developments in communication and networking technologies, monitoring and control systems have become an integral part of daily life [1]. WSNs are being used everyday for this purpose and represent a class of networking technology which is advanced, compact and sophisticated. WSNs are used in many applications such as in industrial control and monitoring, in the home, computing, agriculture, environment and many more. And with this wider use of WSNs in many applications, comes the problem of their optimal design and development for each specific application. The broad topics which are researched in this thesis include system fundamentals, device specifications, network characteristics, network modeling and simulations as well as physical implementation. The research and development in sensor networks is now increasing at a very fast pace, the design of sensor networks now involves the interaction of many scientific disciplines and becomes complex especially in large networks. As shown in the [2] research areas in WSNs can be divided into many levels the most important of which being the *component*, *system*, and, *application* levels. The component level research involves the refinement and improvement of sensing, computation and communication capabilities of a sensor node. The system level research focuses on the networking and communication principles of WSNs, for example, how to efficiently form a communication network starting from scratch and then maintain that network under different kinds of environment especially in the presence of jamming and interference. The application level research concentrates on the data processing and manipulation provided by the sensor. These research levels can be summarized by the following examples: by object localization using the tracking capabilities of multiple sensor nodes, or by determining the spatial profile of a desired signal using multiple sensor nodes measurements, as well as others.

1.2 Problem formulation and contribution

WSNs operate in the license free frequency band, the industrial, scientific and medical (ISM) band [3]. In the ISM band there are many other wireless systems present such as WLANs, Bluetooth, cordless phones, microwave ovens and there can be jammers present operating on the same frequency. So WSNs have to operate under the presence of these wireless systems and survive. There are many methods available which can be used in IEEE 802.15.4 wireless networks that increase the robustness of the network against interference and jamming.

The main objective of this thesis is to use the FH to study the following 2 major problems in WSNs:

1. Use of FH technique to combat the interference in WSNs from WLAN and compare the performance to a single channel network.

2. Use of FH technique to combat the frequency selective fading in one channel or more than one channel and compare the performance to a single channel network.

1.3 Thesis outline

The rest of the thesis is organized in the following way:

Chapter 2. This chapter gives a basic introduction of IEEE 802.15.4, 6LoWPAN and their relationship. The topics included are the most relevant to this work such as the IEEE 802.15.4 physical layer (PHY) and the medium access control (MAC) layer.

Chapter 3. This chapter presents an overview of time synchronization in sensor networks. It discusses the challenges faced by sensor networks in time synchronization, design issues related specifically to time synchronization in sensor networks and the time synchronization algorithm used in the implementation for this thesis.

Chapter 4. This chapter offers an introduction of FH, its advantages and disadvantages. Some advanced forms of FH are also discussed.

Chapter 5. This chapter gives an overview of the coexistence phenomenon, discusses methods used by IEEE 802.15.4 to coexist with other wireless technologies and some studies relating to the coexistence of IEEE 802.15.4 and IEEE 802.11b/g.

Chapter 6. This chapter starts with details of our implementation of FH, its basic components and how these components are used as the building blocks of the FH scheme. The measurement testbed details are discussed including both hardware and software tools used. The usefulness of FH against WLAN interference is analyzed and the results are given on how the FH is a useful tool for maintaining good IEEE 802.15.4 communication in the presence of a WLAN.

Chapter 7. This chapter deals with the properties of frequency selective channels, offering basic definitions to explain the characteristics of the wireless communication channel. The channel models used in our measurements are given and then finally the results of frequency hopping performance over those channels are presented in order to draw important conclusions.

Chapter 8. This final chapter concludes this work and indicates possible future areas of continued research in this field.

Chapter 2

6LoWPAN/IEEE 802.15.4 Introduction

This chapter gives a basic introduction of the IEEE 802.15.4 standard and 6LoWPAN. The topics included are the most relevant to this work such as the IEEE 802.15.4 PHY and the MAC layer.

2.1 6LoWPAN

The details of 6LoWPAN can be found in RFC 4944 [4] proposed by the internet engineering task force (IETF). 6LoWPAN allows for the operations of internet protocol version 6 (IPv6) packets over IEEE 802.15 based networks. The main feature of 6LoWPAN is to achieve considerably less header overhead by employing multiple methods in a severely resource constrained environment. These techniques include the use of shared context, its adaptation to more repetitive processes and the removal of cross layer redundancies over a dynamic multihop network. 6LoWPAN makes use of previous research on stateless IP header compression [5].

The 6LoWPAN specification in [6] shows how IPv6 format packets can be carried inside the 802.15.4 frame and defines the adaptation layer's main parts. 6LoWPAN has 3 main building blocks:

Header compression. The header fields of IPv6 packets are removed when the adaptation layer can infer them from the link layer information of the 802.15.4 frame or by the information of the shared context.

Fragmentation. This involves fragmenting or dividing IPv6 packets into multiple link layer frames to satisfy the minimum maximum transmission unit (MTU) requirement of IPv6.

Layer two forwarding. The adaptation layer makes use of the link layer addresses for the ends of an IP hop to accommodate the link layer forwarding of IPv6 datagrams. The alternative method for link layer forwarding can be that intra personal area network (PAN) routing is done via layer 3 forwarding, making each 802.15.4 radio hop an IP hop.

The stateless compression employed by the 6LoWPAN adaptation layer reduces or removes all of the adaptation, network, and the transport layer header fields to only a few bytes as shown in Figure 1.1. 6LoWPAN achieves this removal or compression of header fields by using the fact that most often they carry common values and when uncommon values appear they can be substituted by a single reserved value. The IP header optimization for 6LoWPAN is achieved in Figure 1.1 by removing all fields in the IPv6 header that can be derived from the 802.15.4 header in the common values, for example, 1) by replacing the source address with one derived form link address; 2) replacing the destination address with the one derived

form link address, the length derived form link frame length; 3) next header value replaced with the user datagram protocol (UDP), the transmission control protocol (TCP), or the internet control message protocol version 6 (ICMPv6). The additional options provided in IPv6 are kept as options in 6LoWPAN also. The stateless compression used in 6LoWPAN has some advantages over traditional stateful techniques in a way that it does not require any per flow state and routes are selected dynamically without compromising the compression ratio. RFC 4944 [6] makes extensive use of stateless compression.

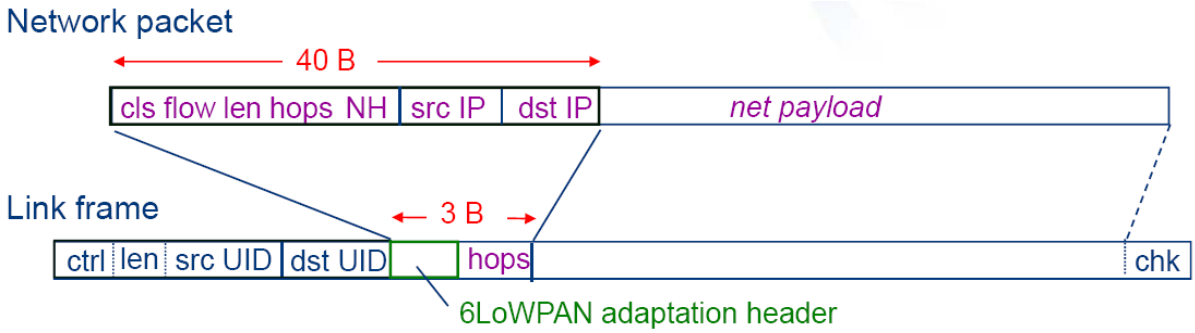


Figure 1.1: 6LoWPAN IP header optimization [6]

If we take the case of 2 802.15.4 nodes communicating with each other, the compressed size of the IP addresses of the source and destination is nearly zero bytes. A single header compression byte sent in the 802.15.4 data packet signals that the IP addresses must be derived from the link addresses (contained in data packet). For communication with other nodes outside of the current cluster, the normal IP address is used. The transmission of small data, smaller than or equal to a data packet size which causes no overhead. In cases when transmitting large data, a fragmentation header is added with the data packet to allow for records the size of fragments. In single hop 802.15.4 communications there is no routing overhead, in a multiple hops case a mesh routing header is added or IP routing can also be used for the whole network.

We can see that the simplest case is most efficient and with the increase in size and complexity of the network, the headers are added as required. This results in a 6LoWPAN being as effective as other link layer protocols in its class, however unlike those protocols it is more suitable for much wider areas of usage.

2.2 IEEE 802.15.4 PHY specification

The PHY is the lowest layer defined in [7], performing the following tasks:

- To transmit and receive data.
- To activate and deactivate the radio transceiver.
- Energy detection (ED) for the operating channel.
- Link quality indicator (LQI) of received packets.

- Clear channel assessment (CCA) in carrier sense multiple access with collision avoidance (CSMA-CA).

- Selection of frequency channel.

2.2.1 Frequencies of operation and data rates

Three frequency bands are defined in [7], which is the second release of the standard. The bands are: 868-868.6 MHz (868 MHz band), 902-928 MHz (915 MHz band), 2400-2483.5 MHz (2.4 GHz band) [3].

The 868 MHz band is applicable in Europe for many applications such as short range wireless networks, which is the considered alternative to Bluetooth. The 915 MHz band and 2.4 GHz band both are part of the ISM band. The 915 MHz band is mostly used in North America and the 2.4 GHz band is used all over the world. The 2.4 GHz band is the most commonly used bands of these 3 bands.

Table 2.1 shows the details of these 3 frequency bands and how they operate together as defined in [7]. The IEEE 802.15.4 standard makes it mandatory for the transceiver to support both the 868 MHz band and 915 MHz band at the same time. These 2 frequency bands are combined together into the 868/915 MHz frequency bands.

Table 2.1: IEEE 802.15.4 Frequency bands and data rates [7]

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS
	902–928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary Orthogonal
	902–928	1000	O-QPSK	250	62.5	16-ary Orthogonal
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

As can be seen from Table 2.1, the 868/915 MHz bands specified by IEEE 802.15.4 have one mandatory requirement and 2 optional requirements. The mandatory requirement is that they are cheap and easy to implement on hardware, therefor having lower data rates of 20 kb/s and 40 kb/s respectively. The optional modes of operation defined in the second release of the 2006 standard allows for the data rates to be increased up to 250 kb/s in the 868/915 MHz bands. Therefore the 868/915 MHz bands and the 2.4 GHz band can be used alternatively for achieving maximum data rates if there is more interference in one band than the other. In the design of a network when the optional modes are used as the primary method of operation, the IEEE 802.15.4 requires that the mandatory low data rate mode must also be implemented

as well, even if it is not used. The transceiver has to have the capability of dynamically selecting between the mandatory and optional modes of operation in the 868/915 MHz bands. A 2.4 GHz band transceiver has the option of supporting the 868/915 MHz bands or not, depending on the system designers and manufacturers. The numbers of channels corresponding to the 868 MHz, 915 MHz and 2.4 GHz bands are 1, 10 and 16 respectively.

The 2.4 GHz ISM band is most widely used worldwide as it gives both the maximum number of channels and data rates at the same time. Therefore, it has been selected by almost all manufacturers as first choice. There are, however, many other wireless technologies that also operate in this band, such as IEEE 802.11.b/g and Bluetooth, so a coexistence issue arises between these standards. The low frequency signals have other noticeable advantages of better penetration through walls and other objects. Therefore, in some situations the designers go for the 868/915 MHz bands as the frequencies of operation.

There are 3 digital modulation types in IEEE 802.15.4: binary phase shift keying (BPSK), amplitude shift keying (ASK), and offset quadrature phase shift keying (O-QPSK).

In BPSK the data is carried by the 2 different phases of the signal. The 2 phases are separated by 180^0, hence the name binary. The exact position of the constellation points on the constellation diagram is not so important. This modulation technique is considered one of the most robust as the receiver can demodulate the signal correctly unless the distortion is too much. The modulation rate is 1 bit/symbol which is very little when it is necessary to transmit at high data rates using limited bandwidth. In O-QPSK the data is carried by the 4 different phases of the signal. As 4 different values of phase are used to transmit 1 quadrature phase shift keying (QPSK) symbol at a time, the phase of the carrier varies by a maximum of 180^0 at a time. At the transmitter during the low pass filtering of the signal, the phase shifts cause large variations in the amplitude of the desired signal. If the timing of odd and even bits are balanced by a 1 bit period or ½ symbol period, the in-phase and quadrature components do not change at the same time instant.

In ASK the transmitted data is represented by the variations in the amplitude of the transmitted signal. The variations in amplitude of the transmitted signal are proportional to the modulating signal while the frequency and phase remain constant. The amplitude variations represent the binary logic of 0 and 1. The resulting carrier signal works as an on or off switch. In the modulated signal the binary 0 represents the absent carrier signal, while the binary 1 represents the present carrier signal. This procedure is the same as on-off keying and is also called on-off modulation.

The spreading method used by the 868/915 MHz bands is binary direct sequence spread spectrum (DSSS) modulation. This and other power efficient signal spreading techniques give low signal-to-noise ratio (SNR) and signal-to-interference ratio (SIR), but the disadvantage comes from the increased transmitted signal bandwidth being much higher than the symbol rate. The major advantage of spread spectrum systems is the lower interference caused to other nodes in a network as well as protection from incoming interference due to their low power spectrum density (PSD).

One of the spreading methods used by the optional 868/915 MHz bands is the parallel sequence spread spectrum (PSSS) also called orthogonal code division multiplexing

(OCDM). In a single data symbol period 20 data bits for 868 MHz are modulated separately onto 20 orthogonal pseudo-random noise (PN) sequences, these PN sequences are summed to a multi level 32 chip symbol equal to 64 half chip symbol. A precoding is applied per symbol to give a multi level 64 half chip sequence. It is then modulated onto the carrier by ASK.

The optional 868/915 MHz bands and 2.4 GHz band use the 16-ary quasi-orthogonal modulation method. In a single data symbol period 4 data bits select one of the available 16 orthogonal PN sequences. The PN sequences to be transmitted are concatenated in series and the resulting chip sequence is modulated onto the carrier by O-QPSK.

2.2.2 Channel assignments

In the 2006 release of the standard the "868/915 MHz band (optional) ASK PHY specifications" and "868/915 MHz band (optional) O-QPSK PHY specifications" were introduced for the first time. However, due to this addition the channel assignments problem occurred as the number of channels defined now were more than 32, which was the maximum channel number defined in the 2003 release of the standard. To solve this problem, channel assignments have been done using a combination of channel numbers and channel pages. The relationship between channel pages and channel numbers can be seen from Table 3.2.

The total channel pages defined are 32. The channel pages 3 to 31 have been for future usage. In each channel page there are 27 channels numbered 0 to 26. The reserved channels are shown in Table 3.2.

In channel page 0 there are 27 channels numbered 0 to 26 for 3 frequency bands. 16 channels in the 2450 MHz band, 10 in the 915 MHz band, and 1 in the 868 MHz band. This channel page is similar to the channel numbers defined in the 2003 release of the standard. The center frequencies of these channels are given by Equation (2.1):

$$\begin{gathered} F_c = 868.3\,MHz,\ for\ k = 0 \\ F_c = 906 + 2(k-1)\,MHz,\ for\ k = 1, 2, \ldots, 10 \\ F_c = 2405 + 5(k-11)\,MHz,\ for\ k = 11, 12, \ldots, 26 \\ where \\ k\ is\ the\ channel\ number. \end{gathered} \tag{2.1}$$

In channel pages 1 and 2 there are 11 channels numbered 0 to 10 for the 2 frequency bands to accommodate the 868/915 MHz ASK and O-QPSK bands, respectively. 10 channels are present in the 915 MHz band and 1 in the 868 MHz band. The center frequencies of these channels are given by Equation (2.2):

$$\begin{gathered} F_c = 868.3\,MHz,\ for\ k = 0 \\ F_c = 906 + 2(k-1)\,MHz,\ for\ k = 1, 2, \ldots, 10 \\ where \\ k\ is\ the\ channel\ number. \end{gathered} \tag{2.2}$$

Table 3.2: Channel page and channel number [7]

Channel page (decimal)	Channel page (binary) (b_{31}, b_{30}, b_{29}, b_{28}, b_{27})	Channel number(s) (decimal)	Channel number description
0	0 0 0 0 0	0	Channel 0 is in 868 MHz band using BPSK
		1–10	Channels 1 to 10 are in 915 MHz band using BPSK
		11–26	Channels 11 to 26 are in 2.4 GHz band using O-QPSK
1	0 0 0 0 1	0	Channel 0 is in 868 MHz band using ASK
		1–10	Channels 1 to 10 are in 915 MHz band using ASK
		11–26	Reserved
2	0 0 0 1 0	0	Channel 0 is in 868 MHz band using O-QPSK
		1–10	Channels 1 to 10 are in 915 MHz band using O-QPSK
		11–26	Reserved
3–31	0 0 0 1 1 - 1 1 1 1	reserved	Reserved

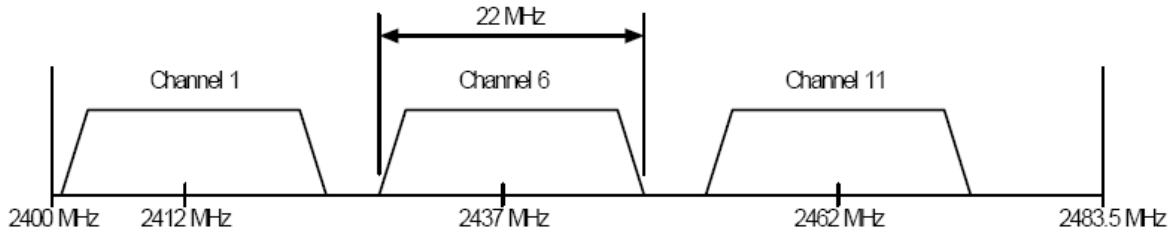
Table 3.3 below shows the details of 16 channels in the 2.4 GHz band, the band which has also been used in this thesis.

Table 3.3: IEEE 802.15.4 2.4 GHz band and frequency channels

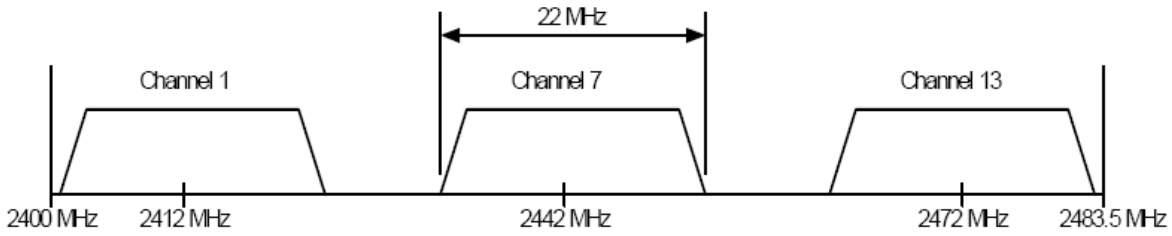
Channel number	Lower frequency	Center frequency	Upper frequency
11	2404	2405	2406
12	2409	2410	2411
13	2414	2415	2416
14	2419	2420	2421
15	2424	2425	2426
16	2429	2430	2431
17	2434	2435	2436
18	2439	2440	2441
19	2444	2445	2446
20	2449	2450	2451
21	2454	2455	2456
22	2459	2460	2461
23	2464	2465	2466
24	2469	2470	2471
25	2474	2475	2476
26	2479	2480	2481

2.2.3 Channel selection

The channel selection of IEEE 802.11b (nonoverlapping sets) and IEEE 802.15.4 2.4 GHz ISM band channels as defined by [7] is shown in Figure 1.2. As can be seen there are 4 channels (15, 20, 25, 26) of IEEE 802.15.4 that lie on the guard bands of the IEEE 802.11b channels. If the IEEE 802.15.4 is operated in these 4 free channels then interference from IEEE 802.11b is minimum compared to the overlapping channels, but not zero because there is still some IEEE 802.11b signal energy present in these guard bands. If possible, as IEEE 802.15.4 network should be operated in these 4 free channels for minimum interference, when IEEE 802.11b is located in close proximity.



a) IEEE 802.11b North American channel selection (nonoverlapping)



b) IEEE 802.11b European channel selection (nonoverlapping)

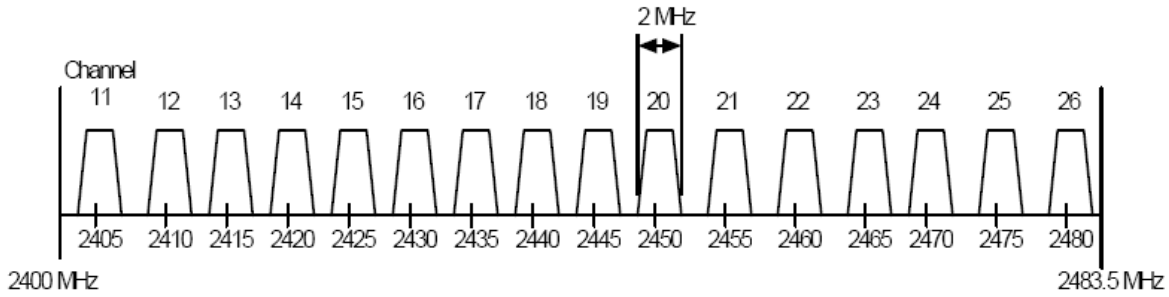


Figure 2.2: IEEE 802.15.4 (2400 MHz PHY) and IEEE 802.11b channel selection

2.2.5 Energy detection

During the process of transmitting a message the node switches back to receive mode and then detects and estimates the signal energy level in the selected channel. This is called

energy detection. The signal energy measurements are taken for consecutive 8 symbol periods and then the average value is calculated. The ED process involves estimating the signal energy level only and no detection of signal type. If the node wants to transmit on a certain channel then it performs ED but this ED will not determine whether the interfering signal is of an IEEE 802.15.4 network or from some other wireless standard. There is a chance that interfering signals of power closer to the receiver sensitivity level will not be detected by ED. The receiver sensitivity level is the minimum signal energy level that the node is able to detect and demodulate while the packet error rate (PER) remains less than 1%. The maximum allowed difference between the receiver sensitivity level and detection level is 10 dB in the IEEE 802.15.4 node. Therefore, an IEEE 802.15.4 node with enabled ED detects and estimates the energy of the present signals at 10 dB above its defined receiver sensitivity level. It can be explained by a general example. If the receiver sensitivity level is defined at -85 dBm, then the ED procedure will detect and estimate the signal energy levels up to a minimum of -75 dBm. The minimum range for ED is 40 dB which for the above example becomes -75 dBm to -35 dBm. The ED request is sent to PHY by the MAC. The PHY then performs ED and the resulting energy level measure from the channel in the form of an 8-bit integer is returned to the MAC. The measured energy accuracy requirement is at least -6 dB or better.

2.2.6 Carrier sense

Carrier sense (CS) is another method like ED for checking the desired channel conditions. In CS, during the process of transmitting a message, the node switches back to receive mode and tries to detect any type of signal present in the selected frequency channel. Unlike ED in CS, after detection, the node demodulates the signal and checks for its modulation and spreading characteristics so as to determine whether they are from an IEEE 802.15.4 node or from a different wireless standard. If the checked signal happens to be of IEEE 802.15.4 PHY type, then it is possible that the node will decide that the selected channel is still busy, ignoring the signal energy level.

2.2.7 Link quality indicator

The LQI represents the strength and quality of a received packet. Possible methods of the LQI include the received signal strength indicatior (RSSI), receiver ED, SNR estimation and a combination of these methods. If the calculated SNR is high then the PER will be low. For this reason, a high SNR signal is usually taken as a high quality signal. Another method for the LQI is a combination of receiver ED and SNR in which 2 methods are used together. The LQI method can be performed for a specific value of consecutive packets, which can be optimized according to the prevailing conditions. There should be at least 8 unique levels that can be assigned to the LQI, higher levels will result in more accuracy at the cost of more computation and storage. The LQI is initiated and returned to the MAC layer and can be used by the network layer and the application layer for further analysis. The LQI measurements of various nodes in a network layer can be utilized for efficient routing of a message. The path for which the reported LQI value is maximum is considered the best path for packet delivery, but the LQI is one of many different factors for determining the optimal path by the routing

protocol. The other important factor is the routing energy efficiency. In case of a low power battery device which is in an optimal position in terms of the LQI as determined by the router node, but when used frequently for routing network packets, its battery will drain out quickly compared to other nodes in a given network. This will result in a overall network performance degradation.

2.2.8 Clear channel assessment

The first part of a CSMA-CA mechanism involves performing clear channel assessment (CCA). The sole purpose of CCA is to make sure the selected channel is not occupied by any other node when the desired node wants to transmit. The CCA is employed by MAC and its command is sent by the MAC to PHY. In PHY the CCA is controlled by its management service. The CCA is performed during an 8 symbols period. The PHY will make sure that the IEEE 802.15.4 node is able to perform CCA by at least 1 of the following 3 modes:

CCA mode 1. Energy above threshold. If the detected signal energy is above the ED threshold level then the tested channel is considered busy.

CCA mode 2. Carrier sense only. The channel is declared busy by the CCA if CS result shows that the detected signal PHY has the same modulation and spreading type as of the node currently performing the CCA. The detected signal threshold is not considered here.

CCA mode 3. Carrier sense with energy above threshold. The CCA result is decided using a logical combination (AND or OR) of CCA mode 1 and CCA mode 2. If the result of this operation is true then the channel is considered busy. The logical combination (AND or OR) is set by the designer according to the network application.

2.3 IEEE 802.15.4 MAC specification

The MAC is responsible for access to the radio channel and performs the following tasks [7]:

- Generation of network beacons by the coordinator node.
- Synchronization of nodes to network beacons.
- Supports PAN association and disassociation services.
- Supports network security.
- Initiating the CSMA-CA mechanism for channel access.
- Implementation of guaranteed time slot (GTS) mechanism.
- Communicating efficiently between 2 networks using same MAC.

The services provided by the MAC are: the MAC data service, and acts as an interface between MAC management service and MAC sublayer management entity service access point. The application level and network level security can also be reinforced strongly by using the hooks of the MAC layer.

2.3.1 Beacon mode and nonbeacon mode

Two methods of channel access have been defined in IEEE 802.15.4: *contention based* and *contention free*. The contention based channel access requires all the nodes in a network using the same channel to first perform the CSMA-CA mechanism and the first node which detects the clear channel starts packet transmission. The contention free channel access consists of a PAN coordinator that allocates time slots to every node. This method is called GTS. Each node transmits only during its own GTS without employing the CSMA-CA mechanism.

The application of GTS by the PAN coordinator requires that all the nodes in a network should be synchronized. A message called a *beacon* is used for this purpose. When a coordinator transmits beacons to its nodes to achieve synchronization, the network operates in a beacon mode. The beacon mode puts an extra overhead on the networking because all the nodes in a network must wake up regularly, listen to the beacons, perform clock synchronization and then sleep again if there is no data to send or receive. Normally, in sensor networks all the nodes do not have data regularly. But in beacon mode they have to wake up regularly for the sake of synchronization only and remain idle for that time. If the beacon transmission itself is not coordinated, then collisions can result also such as direct collisions from neighboring nodes and indirect collisions from non-neighboring nodes belonging to an overlapped network. Therefore, due to these problems the battery of the beacon enabled node drains out too quickly compared to no use of the beacon. Due to these known problems the beacon mode is not supported by commercial devices yet. The nodes used in our implementation also do not support beacon mode and, therefore, *nonbeacon* mode has been used.

A network in which a PAN coordinator does not use beacon operates in nonbeacon mode [6]. There is no GTS and contention free period in a nonbeacon network, so there is no synchronization with the coordinator. In a nonbeacon network, an unslotted CSMA-CA mechanism is used for data transmission. Unlike a slotted CSMA-CA mechanism, the backoff period boundaries are not synchronized. Every node employs single CCA operation and if the considered channel is free it transmits data. The coordinators operate continuously while the ordinary nodes try to sleep most of the time. The nodes start operating when when they want to send measured data to the coordinator and to receive a packet transmitted from the coordinator by following the data request/acknowledgment/data/acknowledgment handshake [6]. The data request is transmitted using the unslotted CSMA-CA mechanism and the corresponding acknowledgement is sent immediately. A similar procedure is followed when the coordinator wants to transmit data to a node. This all means that a node has to remain awake for a specific time after it sends the data request packet. The rate of data requests by a node to a coordinator depends on the application being run. Therefore, there is a large reduction in battery usage of nodes in a nonbeacon network compared to a beaconed network due to less operating time in a nonbeacon network.

2.3.2 MAC frame structures

The design of the frame structures in [7], on one hand, reduces the complexity to a minimum while on the other hand, the frames are optimal to transmit under noisy channel conditions. The layer specific headers and footers are added to the structure as the frame travels through all of the protocol layers. The following frame structures are used: *beacon* frame, *data* frame, an *acknowledgement* frame and a *MAC command* frame.

2.3.2.1 Beacon frame

A *beacon* frame is used by a coordinator in a beacon enabled network. A beacon frame is created in the MAC. Figure 2.3 shows the detailed structure of a beacon frame.

2.3.2.2 Data frame

A *data* frame carries the data to be transfered. A data frame originates from the upper layers of IEEE 802.15.4. Figure 2.4 shows the detailed structure of a data frame.

2.3.2.3 Acknowledgment frame

An *acknowledgment* frame confirms the successful reception of a frame or packet by a receiver. An acknowledgment frame is created in the MAC. Figure 2.5 shows the detailed structure of an acknowledgment frame.

2.3.2.4 MAC command frame

A *MAC command* frame carries commands such as data request, association request and disassociation request with a network. A MAC command frame originates in the MAC. Figure 2.6 shows the detailed structure of a MAC command frame.

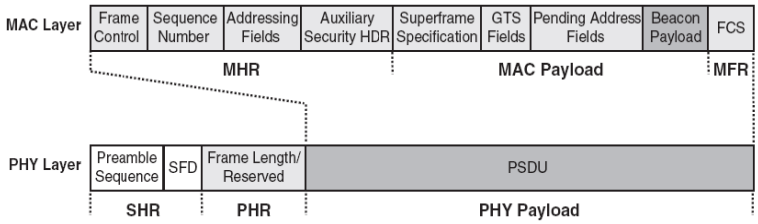


Figure 2.3: Beacon frame [3]

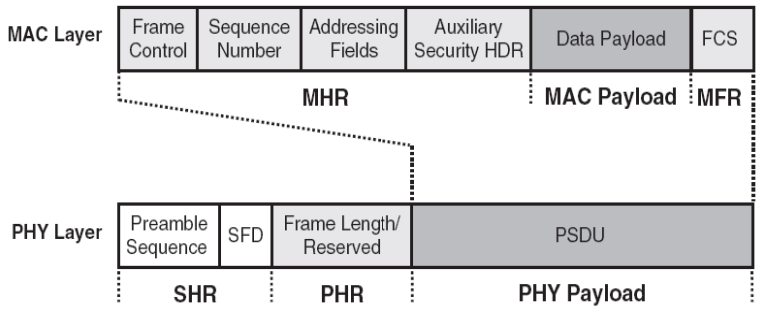


Figure 2.4: Data frame [3]

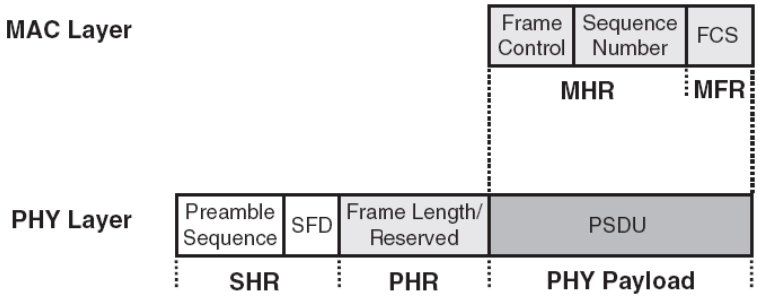


Figure 2.5: Acknowledgment frame [3]

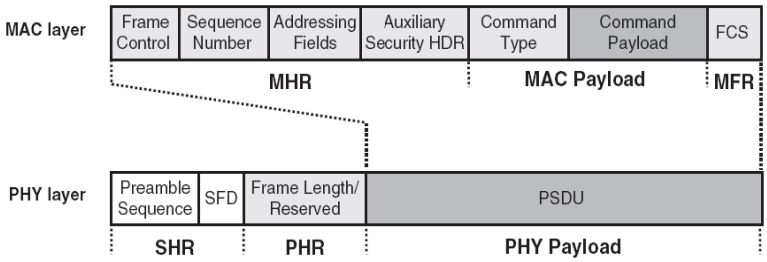


Figure 2.6: MAC command frame [3]

CHAPTER 3

Time synchronization in sensor networks

This chapter gives a basic introduction of time synchronization in sensor networks. It discusses the challenges faced by sensor networks in time synchronization, different time synchronization protocols for sensor networks, their advantages and disadvantages, in addition to the time synchronization protocol used in the implementation for this thesis.

3.1 Introduction

WSNs normally sense or measure one or more physical quantity and then send this information to a central processing unit via a single hop or through other nodes and gateways to a central processing unit where information is processed into useful data. In many cases, the data is combined from several measurements before it arrives at the central or global processing unit. In order for the whole network to perform these tasks the physical time of all the sensor nodes has to be synchronized to either one or many gateways in a network. There are many applications which require time synchronization for them to work correctly such as frequency hopping, localization of sensor nodes, coordination of senor nodes within a network, temporal message ordering, time division multiple access and the energy efficient operation of the network by scheduling the sleep time and wake time of the sensor nodes [9].

3.2 Time synchronization challenges

The synchronization requirements vary from application to application but fundamentally almost all synchronization techniques require some message exchange between nodes, although the amount of messages required for achieving the synchronization depends on the performance of the algorithm being used for synchronization. If the operation of the network itself is nondeterministic in nature during the synchronization, then it leads to an error in synchronization. According to [9], normally the time synchronization schemes for sensor networks have 4 basic packet delay components: *send* time, *access* time, *propagation* time, and *receive* time.

Send time. The amount of time taken by the sender to send the synchronization packet. It includes the time for generation of the packet inside the node and the time required for sending the packet to the network interface.

Access time. This time is the delay in the MAC layer before transmission on the channel due to contention, collisions, and so on. This time varies for different MAC protocols and depends on their complexity. In the case of CSMA, every node is required to sense the medium before transmission and it should not transmit unless the medium is clear. CSMA-CA discussed in Chapter 2 uses both carrier sense and collision avoidance.

Propagation time. This is the time taken by the data to travel from the transmitter to the receiver. The determining factors for propagation time include the location of the transmitter and the receiver so the distance between them is critical. The propagation time for one hop neighbors or a point to point connection is the time spent in traveling through the physical medium. If the sender and receiver are more than one hop, or when switching and queuing times of the system are included, then the propagation time is much higher.

Receive time. The time taken by the receiver for reception of a message, its processing and the acknowledgement process back to the transmitter is called the receiver time. It depends on the receiver in which layer it timestamps the arrived message and whether it includes the overhead time used for transferring the data from the network interface to the host.

Figure 3.1 shows each time of equal and fixed length, which does not happen in real time. Each delay component is different from each other and varies from packet to packet basis. One option is to estimate these times for particular operating conditions.

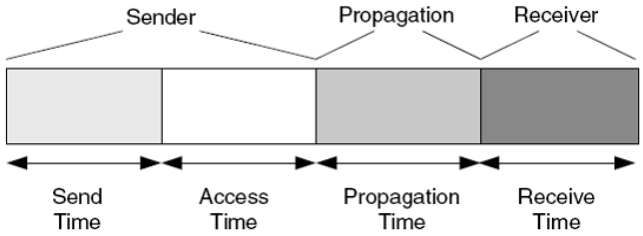


Figure 3.1: Packet delay components [9]

3.3 Common time synchronization protocols

This section gives a brief survey of some of the important time synchronization protocols currently in use, discussing their benefits and pitfalls.

3.3.1 Reference broadcast synchronization (RBS)

The RBS [10] is a timing technique which translates time from the complete network. The time translation is done hop after hop starting from the source to the node which wants to be synchronized with the source. The nodes which can receive the broadcast of the transmitter are easily time synchronized with each other and the transmitter. The number of reference packets which the transmitter broadcasts is fixed. The receivers which are able to hear those packets make a record of the time of arrival of these reference broadcast packets. Then the receiving nodes start communicating with each other to calculate the time offsets between them. The nodes which can receive the reference broadcasts from multiple transmitters are designated as *translation nodes*. The translation nodes translate time or carry time between multiple broadcast regions [3].

The simple illustration of RBS is shown in Figure 3.2. Nodes *A* are transmitters, Nodes *B* are

receivers and Nodes *C* are translation nodes. As mentioned above, the transmitter nodes *A* start by transmitting reference broadcast messages containing timing information. The receiver nodes *B* receive these timing messages. Then the receiver nodes *B* synchronize with each other. The translation nodes *C* are assigned as they are ones which are in broadcast range of both transmitter nodes *A*. A message containing some important information, such as about network topology, is time stamped and then translated by the translation nodes to the other broadcast region and same is done when the response to that message is sent back. This method of time synchronization is flexible and computationally simple but some times for a message route, the translation nodes are not available, and in the worst cases, there may be many such routes. This method cannot be used appropriately in time division multiple access based networks as the there is no centralized time synchronization for all nodes in the network.

The work in [9] lists the multiple types of attack that can happen to RBS. As it is known in RBS that the nodes start to synchronize with each other after the reference broadcast phase, there is a possibility for attack if the receiver nodes have incorrect time or an outsider has gained access to a receiver node and changed its clock. When the faulty node exchanges its timing information with its neighbors, as a result it calculates incorrect time offsets. The multihop case in RBS is also prone to attacks. If a faulty node also happens to be a translation node, then the clock conversion process starts to go wrong and increases with time when the translation node is covering multiple regions. The clock conversion errors propagate deeper into the network.

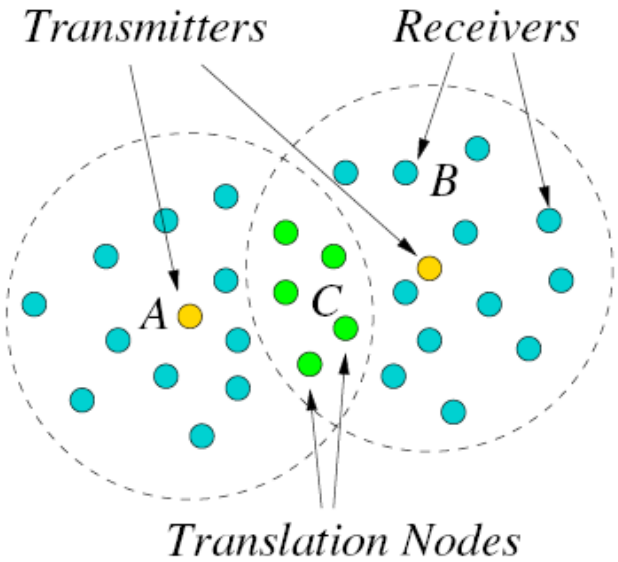


Figure 3.2 : Illustration of the RBS [3]

3.3.2 Flooding time synchronization protocol (FTSP)

The procedure starts with the selection of the root node for the sensor network [9] and [11]. It is the root which acts as a single center for generating and managing the synchronization messages. When any node in a network does not receive a synchronization message within a

predefined amount of time, it should announce itself as a root node. When after declaring itself as a root node if the root node receives a time synchronization message from a node of a lower hop and ID, then it will become an ordinary node from the root node. After receiving a time synchronization message from, the root node, the node adjusts its own time clock to the root node clock and broadcasts its new adjusted time to its neighbors. The broadcast message consists of (in the following order) the preamble bytes, synch bytes, data bytes and cyclic redundancy check bytes.

The advantages and disadvantages of FTSP have been listed in detail in [9]. The FTSP remains operational in case of node failures, as it does not make tree data structures that totally collapse when single or more nodes fail. When a node fails, a whole subtree after that node is cut and if the failing node is a root node, then the complete network fails. The drawback of FTSP is how a root node is elected in a network. As any node has a capability of becoming a root node and the network depends on it to give away its root status voluntarily when it sees a new lower ID root node. A jammer or attacked node disguising itself as a member of a network can become a root node by transmitting the lowest ID of all nodes, and therefore bringing down the original root node. Then it sends incorrect synchronization timestamps to the whole network and ultimately the whole network is jammed.

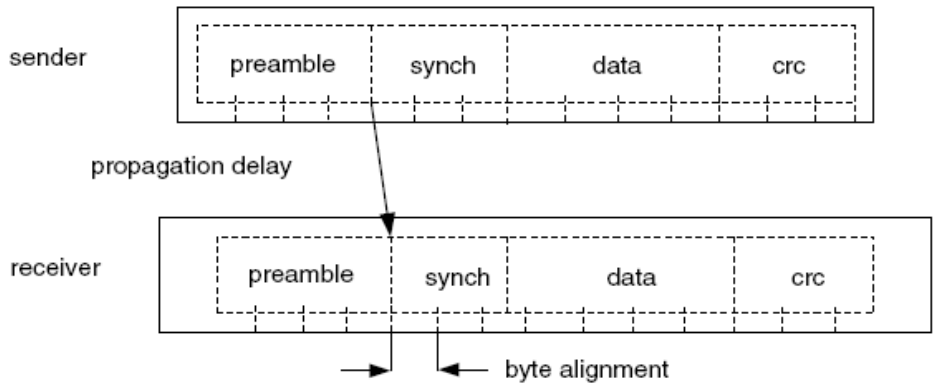


Figure 3.3 : Data packets transmitted in FTSP [9]

3.3.3 Time synchronization protocol sensor networks (TPSN)

The TPSN [12] is a sender-receiver synchronization approach, where the sender initiates the synchronization and synchronizes its clock to the receiver. The TPSN achieves synchronization in 2 phases, the first phase of level discovery and the second phase of clock synchronization.

It is practical to first examine the synchronization procedure between a pair of nodes [9]. The level discovery phase is done by making a spanning tree for the whole network and each node is assigned a level. The root of the tree corresponds to a gateway in a sensor network and has a level 0. The nodes having level *n* are capable of communicating nodes at level *n-1*. Then the synchronization phase starts in which each child node is synchronized to its parent node and this process goes all the way up to a root node. To understand the synchronization phase first see Figure 3.4. As a first step, the child node sends a synchronization request packet at

time *T1* to the root node. This packet is received by the parent node at time *T2* and the parent node sends an acknowledgement packet to the child node at time *T3*. The values of *T2* and *T3* are sent in the acknowledgement packet. The acknowledgement packet is received by the child node at time *T4*. The child node then uses these 4 time values to calculate the clock drift and propagation delay by Equation (3.1) and Equation (3.2) respectively:

$$\Delta = \frac{(T2 - T1) - (T4 - T3)}{2} \tag{3.1}$$

$$d = \frac{(T2 - T1) + (T4 - T3)}{2} \tag{3.2}$$

The network level synchronization [12] starts with the root node broadcasting a time_sync packet. When these packets are received by the nodes on level 1, the nodes waiting after some random time start the above explained 2 way message exchange procedure with the root node. After completing this procedure, the nodes clocks become synchronized to the root node. The nodes in level 2 will also be able to listen to this message exchange, as each node of level 2 is a neighbor of at least one node of level 1. The nodes of level 2 back off for random time when they listen to the message exchange between level 0 and level 1 and then start the 2 way message exchange with the nodes in level 1. The randomization of transmission at any current level *n* ensures that the nodes at the level *n-1* one up from the current level have already been synchronized to the level *n-2* and so on up to level 0. A node responds to the synchronization request only after it is synchronized to a higher level already, so there are no multiple levels of synchronization at the same time in a network. The process continues all the way down to the lowest level until all the nodes in a network are synchronized to a root node. To overcome any packet collisions in a network during synchronization, when a node does not receive an acknowledgement after a random time, it takes a pause and retransmits the synchronization request again.

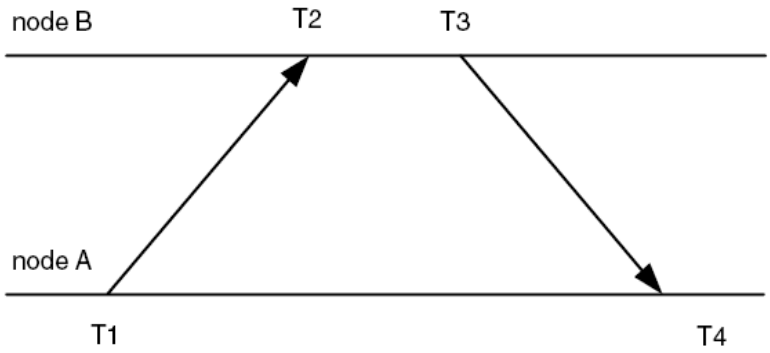


Figure 3.4: Synchronization phase in TPSN [9]

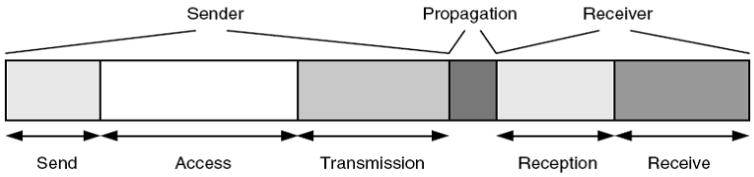


Figure 3.5: Decomposition of packet delay over a wireless link in TPSN [9]

The decomposition of packet delay over a wireless link in TPSN is shown in Figure 3.5. The send, access and transmission times occur at the sender of a message. The propagation time is the time which the message spends on a physical channel and is nearly negligible. The reception and receive times occur at the receiver of a message. The transmission time and reception time both are deterministic in nature, but their values can change due to hardware differences from system to system.

In TPSN, the node which has the communication capabilities to the outside world is normally taken as a root node or gateway. The gateway can use the global positioning system facility to synchronize to other networks or other localization techniques can be used. There is a possibility of changing the root after some specific time by periodically electing a new leader in case of very hostile environments, ensuring that the network integrity remains intact. The ID used by every node should be unique and it should be aware of the nodes to which it can communicate through one hop which are also called neighboring nodes. These prerequisites can be done by link layer protocols before the starting of TPSN otherwise TPSN will not work. The communication link must be bi-directional [12].

3.4 TPSN used in this thesis

TPSN uses a simple and conventional sender-receiver based time synchronization. As proved by the authors, typically for WSNs the conventional technique of sender-receiver based time synchronization is much better suited than receiver-receiver based synchronization [12]. They show this by comparing TPSN with an algorithm based on receiver-receiver synchronization, such as RBS. It is shown that TPSN roughly gives twice the better performance than RBS through analysis and implementation of both methods on motes. TPSN synchronization performance nearly remains the same with increases in size of networks and so it is suitable for multihop sensor networks. The need for resynchronization is minimum compared to other protocols as the synchronization phase takes a negligible amount of time and, therefore, clock drift between the nodes is less. The TPSN also provides small localization capabilities as an added advantage. To, summarize, TPSN is simple, highly efficient and scalable to large networks, easily being one of the simplest synchronization methods to implement on nodes.

CHAPTER 4

Frequency hopping

This chapter gives an introduction of FH, its advantages and disadvantages. Some advanced forms of FH are also discussed.

4.1 Frequency hopping

In FH a radio signal communication is done between 2 or more nodes, by rapidly changing the radio channels following a predetermined pseudorandom channel sequence known to both sender and receiver.

Normally the procedure of FH is as follows:

1. The transmitter sends a request via a predefined frequency channel (control channel).

2. The receiver sends a number sequence, known as a seed. Or in many cases the sender has its own number sequence stored in which case this step in not executed.

3. The transmitter uses the seed as one of the inputs in a random number algorithm, which then calculates the channel sequence, i.e. the sequence of frequencies that is used for communication.

4. The transmitter sends the channel sequence, channel stay time (same for all channels) and the time when it will start transmitting the data.

5. The communication starts at the same point in time, and both the transmitter and the receiver change their frequencies according to the channel sequence.

In [13] the author discusses some basic properties of a FH pattern. In the pattern should appear a truly random number in order for it to ensure the properties of secreteness and unpredictability. Other secondary properties include a large period, a uniform distribution over all frequency channels so that all the channels are used for maximum efficiency and the seed for the hopping pattern should be a multilevel number with a large linear span. If the period is large enough, then it is very difficult for a jammer to intercept and store the pattern. Linear span definition varies from field to field. According to [13], the linear span is defined: the “linear span of a multilevel sequence is the smallest degree of any linear recursion that the sequence satisfies.” If the jammer catches a small portion of the hopping sequence, then it will not be able to reconstruct it completely due to its large linear span property. The random number generator produces a control bits sequence which is equal to a number drawn from a finite field having appropriate properties. Finally a FH pattern is produced by assigning a different frequency to each number.

FH can be divided into 2 types, *fast* and *slow*. In fast FH each symbol is transmitted on more than one hop, or if the rate of change of frequency is much higher than the data rate. In slow FH, one or more data symbols are transmitted during the channel hop time. In WSNs slow FH is considered to be adequate due to the low rate of switching time which results in low energy consumption and a more spectrally efficient transmitted waveform.

FH gives many advantages over a single carrier system. FH is inherently highly effective against narrowband interference and jamming. The interference signal disappears into the background due to its spreading when the spread signal is recollected at the receiver. FH makes intentional interception of information difficult. A narrowband receiver misinterprets the FH signal as an increased background noise. The only chance for an eavesdropper to catch the FH communication is to either intercept the pseudorandom sequence or it should know how to produce the exact pseudorandom sequence itself. A FH system allows for the same frequency band to be shared by other wireless technologies at the same time which may use FH themselves or a single channel. The noise caused by FH signals to narrow frequency communications is minimum and vice versa. This results in more efficient utilization of bandwidth. The 2 most important advantages of FH are its effectiveness against frequency channel interference and frequency selective fading, but it is not effective against white noise and wideband thermal noise. The disjoint frequency channels should be used against narrowband interferers to maximize FH capabilities. The disjoint channels are usually adjacent or have guard bands between them. A procedure called *spectral notching* removes parts of the spectrum that are encountering constant interference or frequency selectivity for some time are removed from the hopset.

The bandwidth used by FH for the same amount of information is much more than that used by a single channel system. But the effective interference bandwidth remains the same as for the single channel because only a small part of whole spectrum is used for communication at any time instant.

In the FH system, the transmitter and receiver should be synchronized before the start of FH because both should change channels at the same instants of time. For these reasons, correct synchronization is absolutely necessary for FH.

One crude approach is given in which requires the transmitter to use all channels for a fixed time period. The receiver picks the random channel and listens for specific data in order to recognize the transmitter. The desired data identification is done by a special sequence before or during data which does not occur normally for this channel and a special data sequence has checksum capabilities and other forms of identification for data integrity. The nodes can also use the fixed tables of channel sequences, like routing tables, so after synchronization, they use those tables for reliable network communication. The transmitter sends its location in the table when present on each channel.

The other reliable and secure option is to first synchronize the transmitter and receiver using some accurate synchronization algorithms and then start the frequency hopping. The synchronization is performed periodically to maintain the accuracy. This approach has been used in this implementation work. For details that concern synchronization problems in sensor networks, as well as the synchronization algorithm mainly used in this work see Chapter 3.

4.2 Adaptive frequency hopping

Adaptive frequency hopping (AFH) is an advanced form of FH used against static frequency interferers considered in [14]. This method was proposed initially for Bluetooth, but it can also be used with least modifications in sensor networks, due to a number of similarities between the 2 wireless technologies. The AFH suggested for Bluetooth in [15] and modified here in terms of sensor networks, can be broken down into 4 main components:

1. *Channel classification*. Each channel in the hopset is scanned for an interference or jamming with some detection technique.

2. *Link management*. The decisions regarding AFH parameters such as the channel list are distributed to all nodes of the sensor network.

3. *Hop sequence modification*. The hopping channels are increased or decreased according to the interference characteristics.

4. *Channel Maintenance*. All the channels are checked periodically to classify them as either good or bad.

Channel classification is a method for detecting an interference on a particular channel. The methods used are such as RSSI measurements, consecutive packet errors for some specific time, packet error averages among othera. In RSSI use, the node can passively measure each channel and multiple channels in the 2.4 GHz ISM band can be checked in a single time slot. The packet delivery methods perform well for the evaluation of a specific point to point link condition, but these methods are sometimes slow, depend on the packet type sent and require at least some packets to be lost before adaptation is done. After channel classification has been done, the quality metrics of every channel are stored individually. The channel will be designated as either good or bad based on these metrics.

The gateway or cluster head, in a sensor network then uses ***link management*** for spreading and receiving the channel classification information to and from the nodes in its area. The channel classification measurements can be taken by all nodes or some specific nodes in a network but only the gateway, or cluster head, performs the job of information distribution. The cluster head (in a nonbeacon mode) accomplishes this by acknowledgment to the data request from the node and then by sending the data to the node to signal the new channel list and when to start operating according to newly these determined channels. This means that for a sensor network to operate using AFH, the gateway or cluster head node must be AFH capable.

After the link management job has been done and the all nodes in the network have received the new channel information, every node must update to the new hop sequence. This process of updating the channel information is called ***hop sequence modification***. There is a requirement for synchronized hop sequence modification, both in time and frequency between any nodes wanting to communicate inside the sensor network.

When a WSN is operating with the maximum allowable set of frequencies or reduced set of

frequencies, the above 3 processes of channel classification, link management and hop sequence modification are performed periodically a process called channel maintenance. The channel maintenance should be done frequently enough so that changing interference conditions are encountered fully. The causes for changing interference conditions include the dynamic interferer constantly changing its jamming properties from low to high intensity and the arrival and departure of mobile interferers in the sensor network. There is a trade off between the regularity of channel maintenance and the resulting power consumption in the nodes and network traffic. The periodicity of channel maintenance should be planned for lowest power consumption for the whole network.

AFH is definitely a robust and efficient tool for achieving coexistence between WSNs and other wireless technologies in the 2.4 GHz ISM band. A lower number of collisions between WSNs and other wireless systems resulting from the implementation of AFH, results in lower latency for both systems. The less number of retransmissions for open and proprietary technologies make the ISM band more safe to operate in.

4.2.1 Adaptive frequency hopping limitations

AFH works when the interference is static in nature, but if the interference is dynamic then the AFH might not work. If multiple frequency hopping networks are operating in a small area, then there is a chance they will interfere with each other and AFH will not be able to prevent that. When the numbers of interferers starts to increase in a small area, then more channels go bad and are removed from the channel sequence. In a network without AFH, the quality of service (QoS) of service will gradually worsen with the increasing number of bad channels. AFH will maintain a good QoS level until the certain minimum channels threshold point is reached. If the WSN operating with these minimum channels encounter ever more interference, then the QoS level will start declining sharply as any further decrease in channels will collapse the whole network.

Due to these shortcomings of AFH, 2 new techniques that dynamically adapt the frequency hopping pattern have been proposed in [16] and [17]. *Adaptive frequency rolling* [16] uses a small hopping pattern which is updated regularly after a changeable predefined time if there are no packet errors. If packet errors become large, the hopping pattern is changed on a truly random principle. This *dynamic adaptive frequency hopping* [17] divides the hopping pattern by using a randomized binary method to make the interfering network and jammer useless.

4.3 Anti jamming in wireless sensor networks

In [18], the authors present a MAC protocol for defeating jamming in WSNs. They mainly focus on a software interrupt jammer having IEEE 802.15.4 class capabilities which is energy efficient, stealthy, and has the capability to completely break down the communication. The 4 methods used by this protocol to counter jamming are frame masking, channel hopping, packet fragmentation and redundant encoding. The other main jamming attacks evaluated are interrupt jamming, activity jamming, scan jamming, and pulse jamming. The best weapon for the power constraint IEEE 802.15.4 class jammer is the pulse jamming. The most severe case

studied was pulse jamming which rendered a complete channel useless, but the packet delivery ratio dropped by only 11% and so the network was completely operational. The main drawbacks of this work are its ineffectiveness against higher power and computationally intensive interferes which are capable of faster scanning and high data rates.

The protocol proposed in [19] is a distributed protocol which uses multiple channels simultaneously to quickly transfer data out of the jammed region. If jamming is sensed and confirmed by the full detection mechanisms, then it switches its operational mode to exfiltration mode. The data is sent out of the jammed region in such a coordinated way that every node participates in exfiltrating the data out and also tries to protect its transmission from the attacker. It is also a scheduling challenge for IEEE 802.15.4 class radios to create the balance between the receiving mode and sending mode when trying to use all communication channels simultaneously to maximize the data rate. The protocol is capable of operating in such a way that there are no 2 hop collisions when one or 2 hop nodes transmit on the same channel at the same time. The approaches used by the protocol to achieve these ambitious goals include vertex coloring and, after it, a distributed scheduling technique based on mutually orthogonal latin squares and no control messages. The authors have shown with simulations that when there are more communication channels available for the whole network then this protocol is 100% effective against multiple dynamic jammers.

The work in [20] proposes both the optimal jamming attacks and then the optimal defense mechanisms against those optimal jamming attacks for sensor networks. The jammer created by them claims to be optimal in many characteristics. The main capabilities include jamming an area in a single channel WSN, control over the jamming probability and variable transmission range, as well as ability to stop the jamming when it has been detected by monitoring nodes of the WSN which intercept the jammer's communication. The jammer tries to calculate the channel access probabilities and the number of monitoring node neighbors. On the other hand in defense mechanisms, the monitoring nodes use an optimal detection algorithm based on the percentage of incurred collisions. The network computes optimal channel access probabilities to reduce the jamming detection time and the time used for sending out the notification of detected jamming. The network calculates the jamming probabilities of the jammer. The cases studied are when both network and jammer has a maximum possible knowledge of each other, when they have no knowledge of each other characteristics, when one of them lacks the strategies employed by the other and when energy constraints apply to both. They propose that future research includes the multichannel jammer and multichannel WSN and seeks to find alternatives for lack of information of each other's strategies.

CHAPTER 5

IEEE 802.15.4 coexistence

These days, many wireless technologies operate side by side in the license free frequency band, 2.4 GHz ISM. As there are so many technologies at work, the cooperation between each of them is nearly impossible and so they affect the performance of each other. This chapter gives an overview of coexistence phenomenon, discusses methods used by IEEE 802.15.4 to coexist with other wireless technologies and presents some studies relating to the coexistence of IEEE 802.15.4 and IEEE 802.11b/g.

5.1 Coexistence

The 2.4 GHz ISM band is used by many other standards besides the IEEE 802.15.4 standard for sensor networks. The other important and most widely used is the wireless standard IEEE 802.11b/g used for wireless internet access everywhere. Bluetooth and cordless phones also operate in the 2.4 GHz ISM frequency band. In many real time situations these systems are operating in close proximity to each other. These wireless standards and others have at least some respect for each other, ensuring that their operation does not affect the other too adversely. In terms of wireless communications, *coexistence* can be defined as the ability to perform communication at a satisfactory level when other systems are operating close by. The system having coexistence capabilities continues to perform according to its own rules regardless of what methods other networks have employed for their safety. To coexist every system employs some mechanisms called coexistence mechanisms [3].

The coexistence of sensor networks should be performed in such a manner that not only it assures maximum efficient operation for sensor networks, but also so that the impact of sensor networks on other wireless networks is minimum. This characteristic of minimum impact of sensor networks on other technologies is inherent in IEEE 802.15.4 right from its origins due to its properties like low RF transmission power, low duty cycle, and the CSMA-CA MAC protocol.

The simplest case of interference is that 2 or more IEEE 802.15.4 nodes operating in the same or adjacent frequency channel transmit at the same time. By default CCA is performed by every node in the contention period and stops transmission if the channel is sensed busy. Exposed and hidden node problems can occur during CSMA-CA. Now consider that an IEEE 802.11b/g network is also operational nearby at the same time, its channel covers the IEEE 802.15.4 channel and nodes also perform CCA before any transmission. But there is a strong possibility that IEEE 802.11b/g nodes will not see the ongoing IEEE 802.15.4 transmission, because the IEEE 802.15.4 channel bandwidth and signal are much lower compared to IEEE 802.11b/g. In beacon mode, GTS allocation can be used by the coordinator to reduce the probability of packet collision within a network, but this does not work in the case when IEEE 802.11b/g or any other networks other than IEEE 802.15.4 are operating as their

working mechanisms, such as active and sleep times, are transparent to the IEEE 802.15.4 network.

For IEEE 802.15.4, the interferer signal which is not present exactly on the same channel as the received IEEE 802.15.4 signal is enough to cause a significant reduction in received packets. If the interferer signals is outside the 2400-2483.5 MHz band, then normally they are filtered out by the receiver before they even reach the first stage of the receiver. The interferer signals inside the 2.4 GHz ISM band, however, are not filtered out at the receiver. So if the interferer signal which is not present exactly on the same channel as the received IEEE 802.15.4 signal, but on a nearby channel, and has considerably higher power than the IEEE 802.15.4 signal, for example, the IEEE 802.11b/g signal on an adjacent channel, it saturates the first stage of the receiver and prevents the complete recovery of the wanted signal. In case of receivers where the first stage output approaches the exact linearity both the desired signal and the interferer signal is transferred to the baseband, which filters out the interferer signal and preserves the desired signal.

The definitions of an in-band blocking signal and an out-band blocking signal will help clarify the concept. If the interfering signal is in the same frequency band as the IEEE 802.15.4 signal, even if the both signals have not the same center frequencies, the interfering signal is called an in-band blocking signal. In the 2.4 GHz ISM band, an in-band blocking signal is present in the frequency range of 2400-2483.5 MHz. In the 2.4 GHz ISM band, the interfering signal present outside the frequency range of 2400-2483.5 MHz is called an out-band blocking signal. If the band select filter is used, then out-band blocking signals are eliminated. The band select filter passes the signals within the 2400-2483.5 MHz frequency range and blocks all the other frequencies outside this range. Normally in many applications where node size is small, or if there is some constraints on price of the devices, then the band select filter is not used as it has no effect on an in-band blocking signal which is a major source of performance degradation in IEEE 802.15.4 networks.

There coexistence mechanisms for IEEE 802.15.4 networks can be divided into 2 major classes: *collaborative* and *non-collaborative*. In the collaborative case, there is some kind of cooperation between the IEEE 802.15.4 network and the other network so that if one is operational the other should remain idle and wait for its turn, as in the case of both networks being synchronized. If both want to operate at the same time, it should be managed so that interference is minimum. There should be at least one dedicated communication link between the IEEE 802.15.4 network and the other network if the collaborative mechanism is used. The non-collaborative methods are most widely used by IEEE 802.15.4 networks to maintain coexistence performance up to the maximum without any prior knowledge of the operations and characteristics of the other network. The heart of the non-collaborative methods is the algorithms used for detection and estimation of any kind of interference and jamming, and how to operate with maximum efficiency under these interference and jamming conditions.

The IEEE 802.19 coexistence technical advisory group (TAG) operates under the IEEE 802 standards committee. It works on developing the coexistence methods for the IEEE 802 wireless systems that operate in the unlicensed spectrum and hence can interfere with each other. Previously, the IEEE 802.15 Task Group 2 (TG2) had worked on the coexistence issues between IEEE 802.11 and Bluetooth as both operate in the 2.4 GHz ISM frequency band. Later this task group became part of the IEEE 802.19 coexistence TAG.

5.2 IEEE 802.15.4 non-collaborative coexistence mechanisms

This section gives an overview of major non-collaborative coexistence mechanisms that can be used by IEEE 802.15.4 networks [3]. Some methods explained in the following sub sections are an essential part of the IEEE 802.15.4 standard, while other optional features vary from applications to device manufacturers and can be used in different ways.

5.2.1 CSMA-CA channel access

CSMA-CA is the basic method used by any IEEE 802.15.4 device before the start of data transmission except when GTS is used in the network. The CCA gives a signal to the device whether the channel on which it wants to transmit is occupied by any other network or not. The different modes of CCA also enable the node to determine whether the interfered signal is from another IEEE 802.15.4 device or from a device of a different wireless standard. If the operation of the interfering network or jammer is dynamic in nature, such that it changes frequency and signal power quickly, then CSMA-CA cannot help much in avoiding interference. In an even worse situation, the IEEE 802.15.4 device starts transmitting while the other network is dynamically operating. This can lead to a total blackout of IEEE 802.15.4 network communication.

5.2.2 Frequency hopping

Detailed information about FH and its advanced variants can be seen in Chapter 4. FH is one of the fastest and computationally efficient method of avoiding interference and jamming in sensor networks. A new method called *frequency agility* has been proposed in ZigBee Pro in which the complete network changes the channel frequencies in the face of interference and jamming. One optimal method can be that if the cluster heads or all nodes in a network have detection and estimation capabilities that allow them to calculate the frequencies and bandwidths of interfering signals, then the IEEE 802.15.4 network could continuously change its channels accordingly. Another technique is called *channel alignment* in which a IEEE 802.15.4 network in the presence of an IEEE 802.11b/g network selects those frequency bands which are not used by the IEEE 802.11b/g network, for example, channels 25 and 26 can be used for this purpose in North American channel selection.

Frequency Agility. This method proposed in ZigBee Pro allows the ZigBee coordinator to make a decision on the frequency channel for the whole network in the presence of interference. A dedicated node called the network channel manager keeps records of interference from all nodes of the network or less nodes as it decides. A router in the network sends reports of data transmission errors if the failure rate starts rising. Based on these collective measurements from nodes and routers in different parts of networks, the network channel manager decides to selects a new channel for the network and all the nodes are informed about the new channel quickly using a dedicated ZigBee device object (ZDO) command. The ZigBee Pro claims that frequency agility significantly improves the ZigBee network performance.

5.2.3 Adjacent and alternate channel performance

The source [7] details the adjacent and alternate channel requirements of IEEE 802.15.4. These requirements are normally taken as a performance measure when an IEEE 802.15.4 signal is present on adjacent and alternate channels, but they are used as overall metrics of receiver performance against other wireless systems. If the IEEE 802.15.4 receiver rejection ratio on the other IEEE 802.15.4 or similar signals is high, then it is possible for it to achieve the same performance against other higher bandwidth and high power signals. The adjacent and alternate channel performance of the receiver cannot be taken as the same as if the interfering signal is the same on the channel as the receiver is operating.

5.2.4 Extremely low duty cycle

This is one of the most fundamentals requirements for WSNs resulting in very long battery life of sensor nodes and hence, the operation of the whole network. A duty cycle of 0.01% is considered extremely low and can be achieved by a node waking up every minute, performing CCA and transmitting or receiving the collected data and then sleeping. The resulting low duty cycle of every node will ensure minimum interference in the whole network. The complete procedure of performing CCA and transmission of data on the channel takes only a few milliseconds to complete. If 2 or more networks are operating in close proximity to each other then they can perform the data communication during those small milliseconds periods when the neighboring network is idle and channel availability is maximum.

5.2.5 Dynamic RF output power selection

The dynamic RF output power selection means adjusting or selecting the transmitted signal power according to the changing channel conditions and distance between the nodes. Normally, the RF output power is chosen at a minimum level that is acceptable for the receiver node so it can receive and decode the information correctly. If the transmitted output power is reduced to a minimum level, then the interference caused to other nearby networks is minimum but then the receiver node cannot function properly if it is also encountering the interference. If a transmitter senses that the other nodes cannot receive its packet despite several retransmissions, it increases the output power for improved SIR. This increase in power will allow for increased packet delivery. At the same time, however, the interference to other neighboring nodes may increase also.

5.2.6 Signal spreading

A signal spreading is a modulation method like the DSSS modulation technique which gives the sensor networks the advantage of processing gain over the same frequency band interferers of higher or equal signal power. This allows for signal spreading to provide a good level of protection against interference and jamming. The signal spreading can also reduce

the interference caused by sensor networks to other low power networks in some cases. The amount of signal energy remains the same after spreading the original signal, but it occupies larger bandwidth than the original signal resulting in the signal energy per Hertz to decrease. When 2 systems are operating nearby and one of them is a WSN, then the mutual interference of both will depend on the frequency band being used by both and not on the total energy of both interfered signals. Therefore, signal spreading reduces jamming energy per Hertz resulting in increased SIR as well as increasing the successful recovery of the intended signal at the receiver.

5.2.7 Mesh networking and location aware routing

It happens many times in WSNs that a part of the network becomes affected by strong interferers. This jamming can partially or fully block the communications in that part of the network. If the communication blocking occurs and the multiple packets sent by the sender are not forwarded by the router node to the next hop then the the network decides to bypass the infected node and route the packet by another route or part which is not affected by the interference. This is called path diversity.

In location aware routing the information regarding the interference affected areas is transferred to the decision making nodes of the network and they use this information in link cost functions for calculating efficient routes. In this case, the information flowing through the interference affected area is avoided at all possible times. Nevertheless, the nodes in the jammed areas remain useless as any information sent by them or sent towards them is lost under the severe interference conditions.

Directional antennas are used nowadays in nodes where cost or size constraints are not strict but coexistence and maximum efficiency is required at all times. When directional antennas and location aware routing are used together in a network, the interference of one node to all others is reduced considerably. The transmitted signal energy is only directed towards the intended receiver as opposed to normal omni directional propagation. When a node having directional antennas is receiving, the interference in non used directions will be negligible due to a very low antenna gain in those non used directions and the intended signal coming in the used directions will be recovered normally due to the high antenna gain for used directions. In this way, directional antennas improve the coexistence of sensor networks.

5.2.8 Adaptive packet length selection

The packet length is changed according to the varying channel conditions. If the network wants to maintain a low PER in the jamming conditions, then normally the packet size is reduced in accordance with the health of channel. Normally, a smaller packet has greater probability of reaching the receiver quickly when the interference occurs in the same frequency channel as used by the network. However there are some studies which argue that reduction in packet size does not always improve the PER, especially in jamming areas. Packet scheduling and data traffic control in WSNs are also non-collaborative coexistence mechanisms.

5.3 Coexistence studies

This section summarizes the most relevant studies dealing with the coexistence of IEEE 802.15.4 with other wireless standards in the 2.4 GHz ISM band [21].

The first experimental study is done in [22]. According to the authors, there is a serious threat to IEEE 802.15.4 networks from other high signal power standards in the 2.4 GHz ISM band. If a IEEE 802.15.4 network is operating in close proximity to a high data rate IEEE 802.11b access point, then it can cause total breakdown of IEEE 802.15.4 communication if the carrier frequencies of both standards are the same. The interference caused by other systems such as Bluetooth and microwave ovens resulted in a PER in IEEE 802.15.4 but most of those levels were below 10%, making these not so critical. Their measurements showed that even in the worst conditions, like minimum separation distance and minimum carrier frequency offset, the PER does not reach 100% and remains at 95%, due to the fact that during the interframe spaces of IEEE 802.11b, the IEEE 802.15.4 packets may reach the destination successfully. It is proposed that under high WLAN interference conditions, the IEEE 802.15.4 network can use those free channels which fall in between the WLAN channels are. These free IEEE 802.15.4 channels are 15, 20, 25 and 26, as they do not fall directly under WLAN channels 1, 6 and 11.

The second study comprising simulations and measurements is done in [23]. The authors of the study discuss the coexistence of IEEE 802.15.4 with IEEE 802.11b/g in the last part of the paper. Figure 5.1 shows the testbed used for measuring the impact of both standards on each other. The distance between the IEEE 802.11b/g nodes and the IEEE 802.15.4 nodes is 3.5m. The measurements are taken when 2 IEEE 802.15.4 nodes are operating and they are interfered by a pair of IEEE 802.11b/g nodes and then vice versa is performed. The measurements are taken for several center frequency offsets between the 2 standards. The authors conclude that there should be at least a 7 MHz offset between the center frequencies of IEEE 802.15.4 and IEEE 802.11b/g in order for IEEE 802.15.4 to operate safely. They show that if both the standards are operating on the same channel, or near channels, then the performance of the IEEE 802.15.4 network is better with a packet size of 20 bytes than the performance with the maximum packet length of 127 bytes. The IEEE 802.15.4 has some effect on the performance of IEEE 802.11b if IEEE 802.15.4 is transmitting 127 bytes packets and IEEE 802.11b packets are more than 600 bytes long and the center frequency offset is 2 MHz or less.

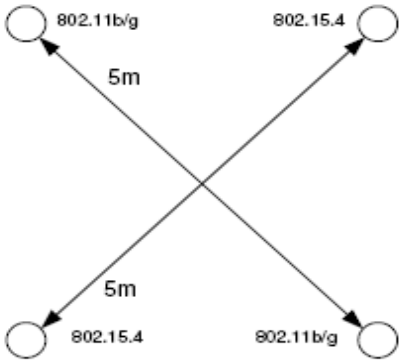


Figure 5.1: Test bed used in [23]

This study has been recently undertaken by [24]. The IEEE 802.11g access point located in the office environment has a peak data rate of 9.8 mb/s. The IEEE 802.11g access point interferer was using channel 6 having a carrier frequency of 2437 MHz. The IEEE 802.15.4 nodes were using channel 17 with a carrier frequency of 2435 MHz. So the central frequency offset was at its minimum value of 2 MHz. In the first case, 2 IEEE 802.15.4 nodes 1 meter apart and an IEEE 802.11g client 10.5 meters far from the 802.11g access point were in the reference cubical as shown in Figure 5.2. In the second case, an IEEE 802.11g client was in the reference cubical, the first IEEE 802.15.4 node was in 1R and second in 1L and the distance between them was 6 meters. In the third case, an IEEE 802.11g client was in the reference cubical, the first IEEE 802.15.4 node was in 2R and second in 2L and the distance between them was 12 meters. The results for all 3 cases are shown in Table 5.1.

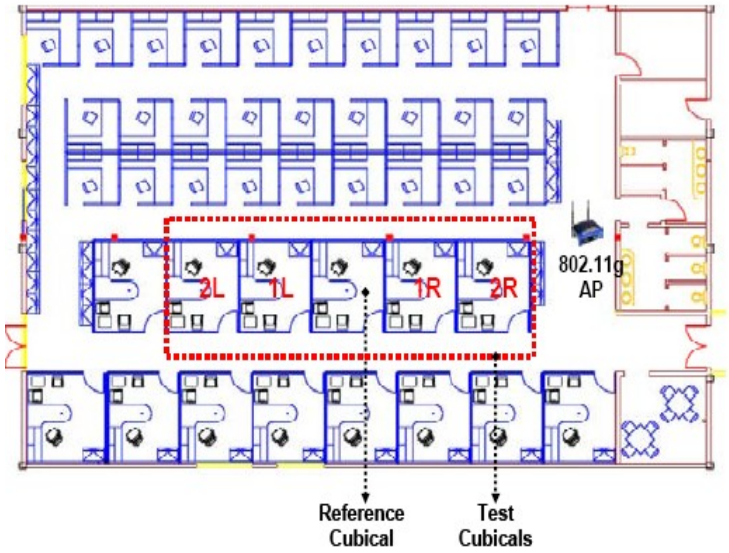


Figure 5.2: Test bed used in [24]

Table 5.1: Results for the 3 test cases [24]

Test Case	Percentage drop in IEEE 802.11g throughput	Percentage drop in Zigbee 802.11g throughput
1	Insignificant	10% (from 100% to 90%)
2	Insignificant	10% (from 100% to 90%)
3	Insignificant	22% (from 83% to 65%)

The study in [25] was done by the ZigBee Alliance on the basis of data collected at HANNOVER MESSE 2008. The purpose of the location was to test in a surrounding environment full of interference from many WLAN, Bluetooth, IEEE 802.15.4 networks as well as many other proprietary wireless standards. They show a packet loss rate of 2% on the network layer and claim that if network layer overheads on measurements are removed, then the packet loss will be 2%. Table 5.2 summarizes their results.

Table 5.2 ZigBee performance [25]

Total Tx packets	Total lost packets	Average latency (ms)	Maximum latency (ms)
25676	555	4.42	874.83

The important theoretical and analytical studies on IEEE 802.15.4 coexistence with WLAN and Bluetooth have been done in [26], [27], [28] and [29]. The [29] is the most important of and most recent of them as it extends on from the previous works. According to [33], the distance and center frequency offset between IEEE 802.15.4 and IEEE 802.11b is very important. The PER of IEEE 802.15.4 is mostly smaller than 10^{-5} if the distance between IEEE 802.15.4 and IEEE 802.11b nodes is more than 8 m. If the offset between the center frequencies of IEEE 802.15.4 and IEEE 802.11b is more than 7 MHz, then the PER of 802.15.4 is smaller than 10^{-4} and there is no effect of IEEE 802.11b interference. The PER as a function of the center frequency offset is shown in Figure 5.3.

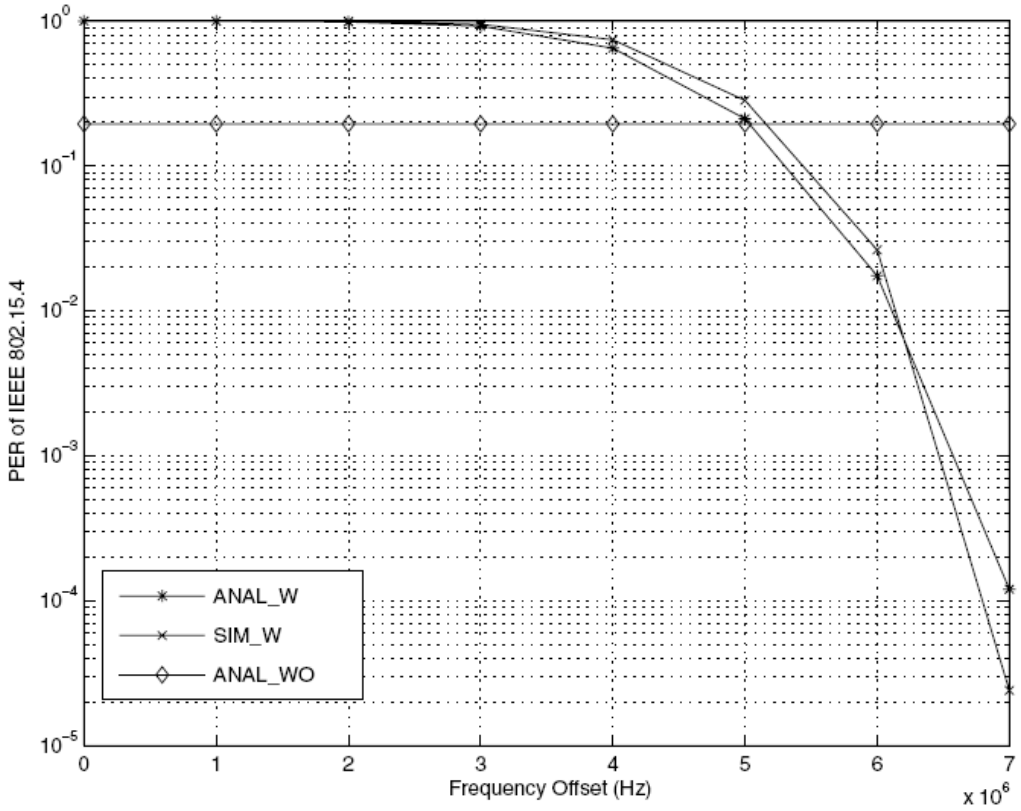


Figure 5.3: PER of the IEEE 802.15.4 with the different frequency offsets to the IEEE 802.11b with distance fixed to 4 m [29].

CHAPTER 6

Frequency hopping architecture and performance analysis

This chapter starts with details of our implementation of FH, its basic components and how these components are used as the building blocks of the FH scheme. The measurement testbed details are discussed including both hardware and software tools used. The usefulness of FH against WLAN interference is analyzed and results are given on how FH is a good tool for maintaining good IEEE 802.15.4 communication in the presence of a WLAN.

6.1 Testbed architecture

The testbed consists of various hardware and software components which are explained in this section. The algorithm and architecture of FH is discussed in the next section.

6.1.1 Software components

This section gives an overview of the software components of our testbed, where the basic and important components are discussed.

6.1.1.1 NanoStack

NanoStack is a protocol stack that implements complete 6LoWPAN architecture and the IEEE 802.15.4 standard. Its basic architecture can be understood by examining Figure 6.1. The protocols which are implemented in NanoStack include IEEE 802.15.4 MAC, 6LoWPAN, ICMP, UDP and Network Manager. These protocols constitute the basic NanoStack architecture. NanoStack is connected to the IEEE 802.15.4 PHY module. On top of the 802.15.4 PHY module and NanoStack resides the user applications such as synchronization and FH applications in our case. All of these modules run in FreeRTOS, a compact real time embedded operating system or kernel written in C programming language. For multihop capabilities NanoStack provides NanoMesh, a multihop forwarding protocol. NanoStack uses a socket interface for enabling simple communications for applications as the socket interface is used in many embedded data communications systems. The NanoStack application programming interface (API) is built using the model of portable operating system interface (POSIX). Furthermore, additional memory management features have been added in the NanoStack API for easy buffer operations. NanoStack can be used both on Windows and Linux based operating systems, although in Windows some additional compilers and graphical interfaces are needed [30].

In FreeRTOS, just as with other operating systems the tasks are scheduled and NanoStack

always runs as a single task inside the FreeRTOS kernel. This results in efficient memory operation and flow control and due to this flow control capability the protocol modules are always executed in a sequential manner as shown in Figure 6.1. The protocol modules are not allowed to call the functions of each other directly which results in greater simplicity. In order to ensure smooth operation of the user application in the protocol stack, all the buffers follow a single queue operation rather than parallel queues at one time.

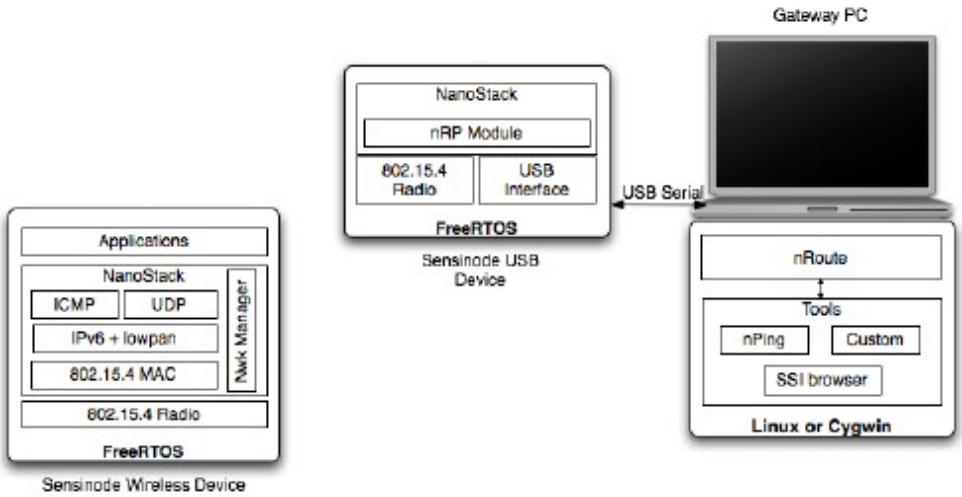


Figure 6.1: The NanoStack architecture [30]

Next is given an example of how a user application is executed in a NanoStack stepwise [31]:

1. Hardware initialization completed by bus_init() and debug_init(speed) functions.

2. NanoStack initialization by stack_init() function.

3. Main application task creation.

4. Execution of FreeRTOS scheduler.

5. Open stack event bus and socket.

The bus_init() function performs principle initialization functions, for instance, when initializing the main system clock. In the case of the debug library, the debug_init(speed) function is used after the bus_init() function. The following C algorithm from [31] explains the above steps:

```
int main( void )
{/* Init System clock & MCU:s port */ bus_init();
/* Init Debug setups */ debug_init(115200);
/* Init stack variables, tasks & modules */ stack_init();
/* Create main task */ xTaskCreate( vMain, "Main",
configMAXIMUM_STACK_SIZE, NULL, ( tskIDLE_PRIORITY + 1 ),
( xTaskHandle * )NULL );
/* Start FreeRTOS Sceduler */ vTaskStartScheduler();
return 0;}
```

6.1.1.2 FreeRTOS

This section describes the fundamentals of FreeRTOS [32] so that reader can understand how FreeRTOS manages the working of NanoStack. FreeRTOS is written in C programming language, being portable to many processor architectures. The kernel is very compact in size making it very suitable for real time embedded applications. The FreeRTOS is a multitasking operating system that allows the complex processes to work together using a simple design approach. In the operating system each each running program is modeled as a task, which is under the control of an operating system. NanoStack uses the multitasking capabilities of FreeRTOS extensively in order to make the protocol operations fast and reliable at the same time. The multitasking inter-task communications are used in embedded operating systems because they allow the partitioning of a complex computational task to be completed in smaller more efficient parallel tasks. This task partitioning allows easier debugging and code reuse. One big advantage of using FreeRTOS with NanoStack is that it shifts the responsibility for complex timing and sequencing operations away from the application code to the operating system kernel.

Scheduling is done by FreeRTOS as it creates the multiple tasks, therefore it has to also schedule and manage them. The scheduler is responsible for which task to start at any particular time and when to stop that task. The scheduler allows for voluntary suspension of the task also if the task decides itself to stop. Normally, the task decides to suspend itself in 3 cases: the task wants to delay, the task wants to wait, or the task waits for a particular event to happen.

FreeRTOS performs context switching of the task suspension and resumption. During the task execution it accesses the processor registers, memory registers and stack. When the task is suspended by the scheduler, the operating system stores the values in the previously stated components and when the task is resumed at a later point in time, these values are available for the task in order to continue its operation. This is called context switching.

The RTOS tick is a useful tool for understanding its timing capabilities. Time is measured in terms of tick count variable in the FreeRTOS real time kernel. The RTOS tick interrupt is used for incrementing the tick count using the maximum time accuracy available on the chip clock.

Other important tools provided by the FreeRTOS include [32]:

Queues. Queues provide intertask communication capabilities.

Binary semaphores. Binary semaphores are responsible for mutual exclusion and synchronization

Counting semaphores. Counting semaphores provide counting event and resource management.

Trace features. They provide tools for keeping record of how a user application is executing, for example, connecting the output to the digital oscilloscope or logic analyzer to determine how the application is running and its timing behaviors.

6.1.2 Testbed

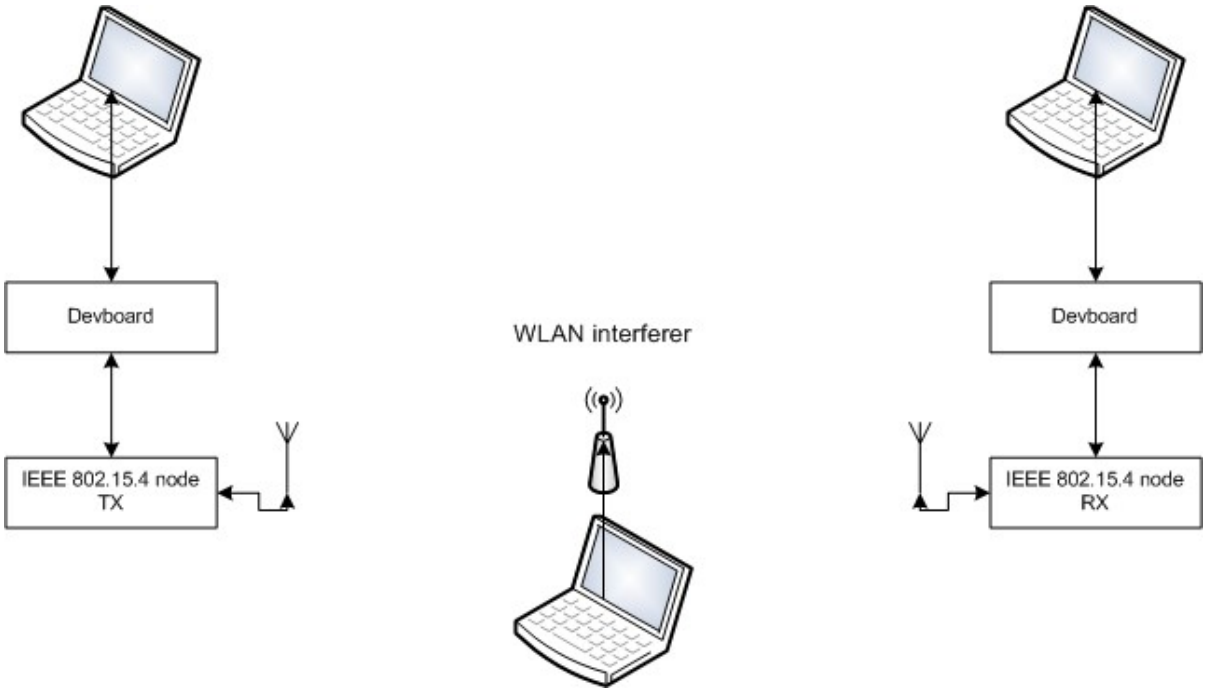


Figure 6.2: Testbed

The first testbed is shown in Figure 6.2. This testbed is used for the performance analysis of FH in the presence of WLAN interference. On the transmitter side, the computer and development board are not necessary if not available, as they are not required for the operation of the node. They should, however, be used if recording the activity of the transmitter node during the measurement test is required. The development board is used for programming the node with C code. The nodes can be powered by 2 batteries or otherwise need no batteries if connected directly to the development board and computer. On the receiver side, the computer and development board should be used in order to record the receiver node activity throughout the measurement test to determine the number of packets received for each channel and also for system debugging purposes.

The interferer setup consists of a laptop computer with an external WLAN card attached to it. The WLAN card's driver allow the user to adjust different operational parameters such as the transmitted power level and the specific channel used for data transmission. Multi-generator (MGEN) has been used as a traffic generator tool for the WLAN interferer. MGEN generates different real time UDP/IP traffic patterns and includes the unicast and multicast modes for WLAN. The following example of an MGEN script used from [33] generates a continuous flow of UDP traffic:

"Transmission Event" script line
0.0 ON 1 UDP SRC 5001 DST 127.0.0.1/5001 POISSON [1 1024]

127.0.0.1 is the loopback interface address and 5001 is port. In [1000 1024] 1000 shows the number of packets sent per second and 1024 in bytes is the payload size or data packet size. POISSON is a traffic pattern.

6.2 Frequency hopping algorithm

This section explains the working of the synchronization and frequency hopping algorithm used in this work. The synchronization algorithm is explained in detail in Section 3.3.3 and in [12]. Figure 6.3 shows the flow chart and working of the used algorithm, which is explained in more detail below:

1. When both nodes are awake, the child node sends a synchronization_pulse packet to the root node at time *T1* after every 5 seconds. The frequency of a synchronization_pulse packet can be increased or decreased from the above value as desired.

2. The root node receives a synchronization_pulse packet at time *T2*. The root node sends back an acknowledgement packet to child node at time *T3*.

3. The child node waits for an acknowledgement packet from the root node for 5 seconds and if not received goes back to step 3.

4. The child node receives an acknowledgement packet at time *T4*.

5. The child node calculates the clock drift and propagation delay between itself and the root node and then adjusts its physical clock according to the above values.

6. Now the child node is synchronized to the root node. This is the end of the synchronization phase.

7. This is the start of the frequency hopping phase. The root node sends to a child node a data packet containing: a random hopping pattern of maximum 16 channels or less, a hop interval time of 1 second and the frequency hopping commence time.

8. The child node receives from a root node a data packet containing: a random hopping pattern of maximum 16 channels or less, a hop interval time of 1 second and the frequency hopping commence time.

9. The child node sends back an acknowledgement packet to the root node.

10. The root node waits for an acknowledgement packet from the child node for a certain time interval and if not received goes back to step 7.

11. The acknowledgement packet from the child node is received by the root node.

12. The root node and child node both start frequency hopping at the hopping commence time determined in step 7.

13. The root node and child node both hop on 16 channels for 16 seconds.

14. After step 13 both nodes go back to step 1 and continue to operate according to the above steps as long as they have data to exchange. When there is no data a child node sleeps.

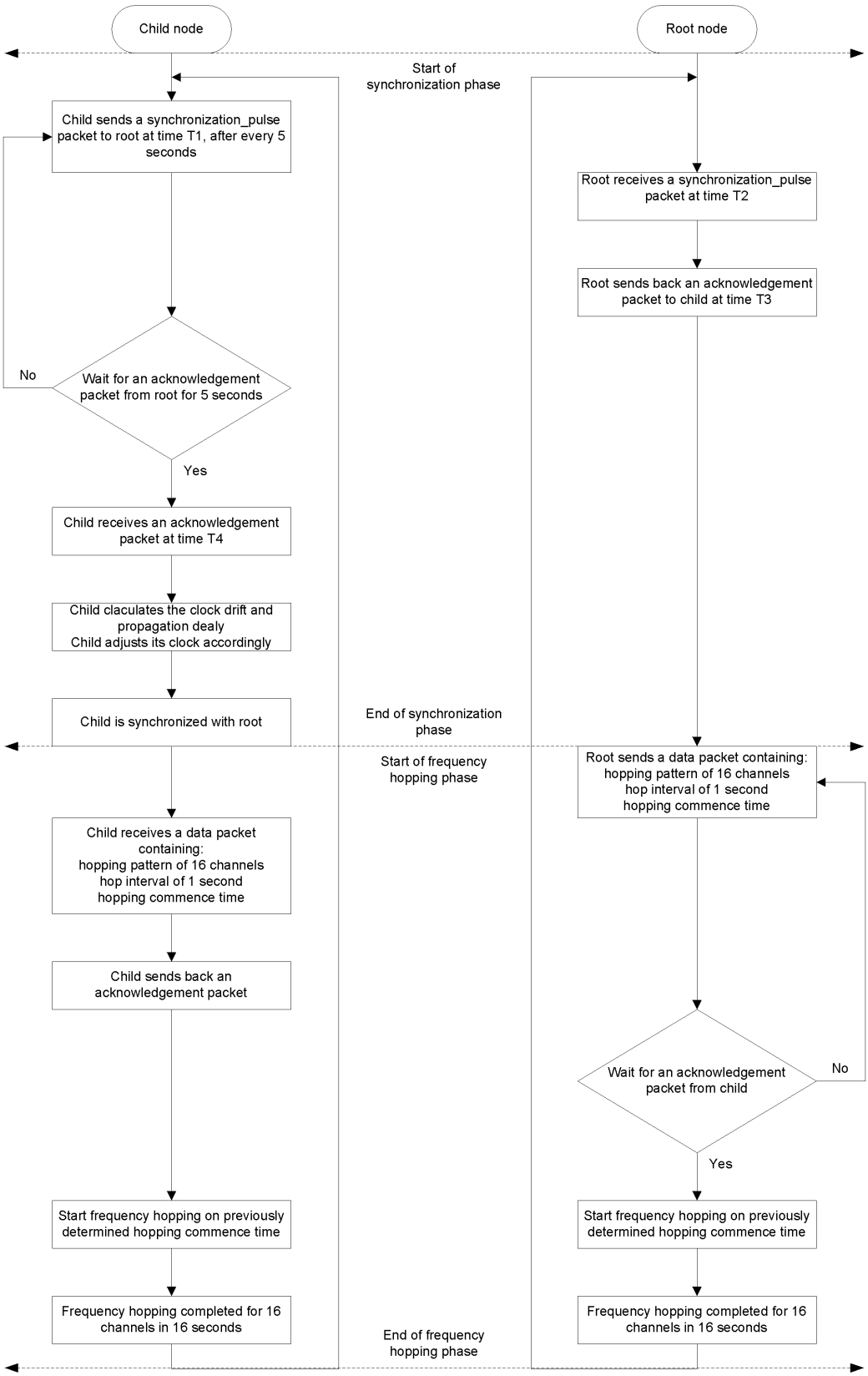


Figure 6.2: Synchronization and frequency hopping algorithm

6.3 Frequency hopping in IEEE 802.15.4 under IEEE 802.11b

This section details the measurements taken from the testbed of Figure 6.2 and the results regarding the performance of the IEEE 802.15.4 sensor nodes operating in an office environment under the strong IEEE 802.11b interferer. The IEEE 802.11b interferer is operated at the maximum allowed transmit power to fully characterize its impacts on the sensor nodes which are using much less power for their operation. It should noted that, the measurements are taken by an interferer using North American channel selection (nonoverlapping). Nearby the office there are other IEEE 802.11b networks using European channel selection (nonoverlapping), having medium signal strength inside our office. The test results should be analyzed keeping in mind these non-deliberate interferer. See Section 2.2.3 for both channel selections. The IEEE 802.11b channel activity of 78% is obtained using the data payload size of 1500 bytes. The important thing to note here is that the measurements are taken in an indoor office environment, so naturally there will be frequency selective fading present which randomly affects the network performance. The IEEE 802.11b interferer does not use FH and therefore keeps on transmitting on the specified channel and is changed in the testbed by using a simple command. Here the packet delivery ratio (PDR) is taken as a performance metric for the WSN. The PDR is described by Equation (6.1):

$$PDR = \frac{Number\ of\ received\ packets}{Number\ of\ transmitted\ packets} \times 100 \tag{6.1}$$

Table 6.1 shows the measurement results for single channel operation in an IEEE 802.15.4 sensor network. The PDR is too low for reliable network operation as was expected in the case of a single channel. The first case considered is when the distance between 2 IEEE 802.15.4 nodes is 1 meter which can compensate somewhat for the IEEE 802.11b interferer operating nearby, also at a distance of 1 meter. However the interference is too large and the resulting PDR is 50% which is considered very poor for sensor networks. It can therefore stated that placing the sensor nodes close together when an IEEE 802.11b interferer is also near to the nodes, especially to the transmitter, will not increase the PDR and reliable network operation. The second case considered is when the distance between 2 IEEE 802.15.4 nodes is 10 meter while the IEEE 802.11b interferer is kept again at a distance of 1 meter. The near zero PDR of 10% in this case is naturally expected because the same amount of interference becomes too large for the receiver when the transmitter is located far away. It can be concluded, therefore, single channel operation in IEEE 802.15.4 is not feasible at all and should be avoided when possible, otherwise sensor network communication will fail.

Table 6.1: IEEE 802.15.4 performance using single channel

IEEE 802.11b channel activity (%) = 78			
Transmitted packets in IEEE 802.15.4 = 544			
Distance between IEEE 802.15.4 receiver and IEEE 802.11b interferer = 1 meter			
IEEE 802.11b channel = 1			
IEEE 802.15.4 channel = 12			
Distance between 2 IEEE 802.15.4 nodes = 1 meter		Distance between 2 IEEE 802.15.4 nodes = 10 meter	
IEEE 802.15.4 PDR (%)	50 ± 1	IEEE 802.15.4 PDR (%)	10 ± 1

Tables 6.2 and 6.3 show the measurements results for FH communication in an IEEE 802.15.4 sensor network. It is clear to see that there is a dramatic improvement in PDR with the FH system compared to the single channel case. For the first case in Table 6.2 when the distance between the 2 IEEE 802.15.4 nodes is 1 meter, the PDR achieved is 88%, 94% and 96% for IEEE 802.11b interferer operating on channels 1, 6 and 11 respectively. It is to be noted that there is not much variation in PDR for these 3 different IEEE 802.11b channels. The improvement achieved with FH over the single channel case is 38%, 44% and 46%. Consider the case when the PDR with FH is 88%, the reason for this value not being above 90% is the frequency selective fading in communication channels, which can greatly reduce PDR over specific selective frequencies. This 88% PDR shows the real time case when the interferes and frequency selective fading are present together. If they are present together then there are 2 possibilities. The first is that fading is present on the same channels which are affected by the interference and not on the interference free channels: in this case, there is already considerable packet drop on the interfered channel and harm caused by fading will not matter. The second possibility is that interference is affecting some channels, while frequency selective fading is present on the clean channels not affected by the interferer. This second possibility reduces the FH effectiveness to some extent, when there are no cognitive or adaptive mechanisms. The 88% PDR case can be understood as a result of the second possibility just explained above. For the second case in Table 6.2 when the distance between 2 the IEEE 802.15.4 nodes is 10 meters, the PDR achieved is 80%, 87% and 87% for an IEEE 802.11b interferer operating on channels 1, 6 and 11 respectively. The improvement achieved with FH over single the channel case is 70%, 77% and 70%. This shows that FH is even more effective when the distance between sensor nodes is large and the interferer is located close to them. These results show that sensor network performance can approach near 100% when fast FH is used as it lessens the effectiveness of interference and jamming.

Table 6.2: IEEE 802.15.4 performance using frequency hopping

Frequency hopping in IEEE 802.15.4					
IEEE 802.11b channel activity (%) = 78					
Transmitted packets in IEEE 802.15.4 nodes = 544					
Distance between IEEE 802.15.4 receiver and IEEE 802.11b interferer = 1 meter					
Distance between 2 IEEE 802.15.4 nodes = 1 meter					
IEEE 802.11b channel = 1		IEEE 802.11b channel = 6		IEEE 802.11b channel = 11	
IEEE 802.15.4 PDR (%)	88 ± 2	IEEE 802.15.4 PDR (%)	94 ± 0.55	IEEE 802.15.4 PDR (%)	96 ± 0.18

Table 6.3: IEEE 802.15.4 performance using frequency hopping

Frequency hopping in IEEE 802.15.4					
IEEE 802.11b channel activity (%) = 78					
Transmitted packets in IEEE 802.15.4 nodes = 544					
Distance between IEEE 802.15.4 receiver and IEEE 802.11b interferer = 1 meter					
Distance between 2 IEEE 802.15.4 nodes = 10 meters					
IEEE 802.11b channel = 1		IEEE 802.11b channel = 6		IEEE 802.11b channel = 11	
IEEE 802.15.4 PDR (%)	80 ± 0.91	IEEE 802.15.4 PDR (%)	87 ± 1	IEEE 802.15.4 PDR (%)	80 ± 0.55

6.4 Channel center frequency offset between IEEE 802.15.4 and IEEE 802.11.b

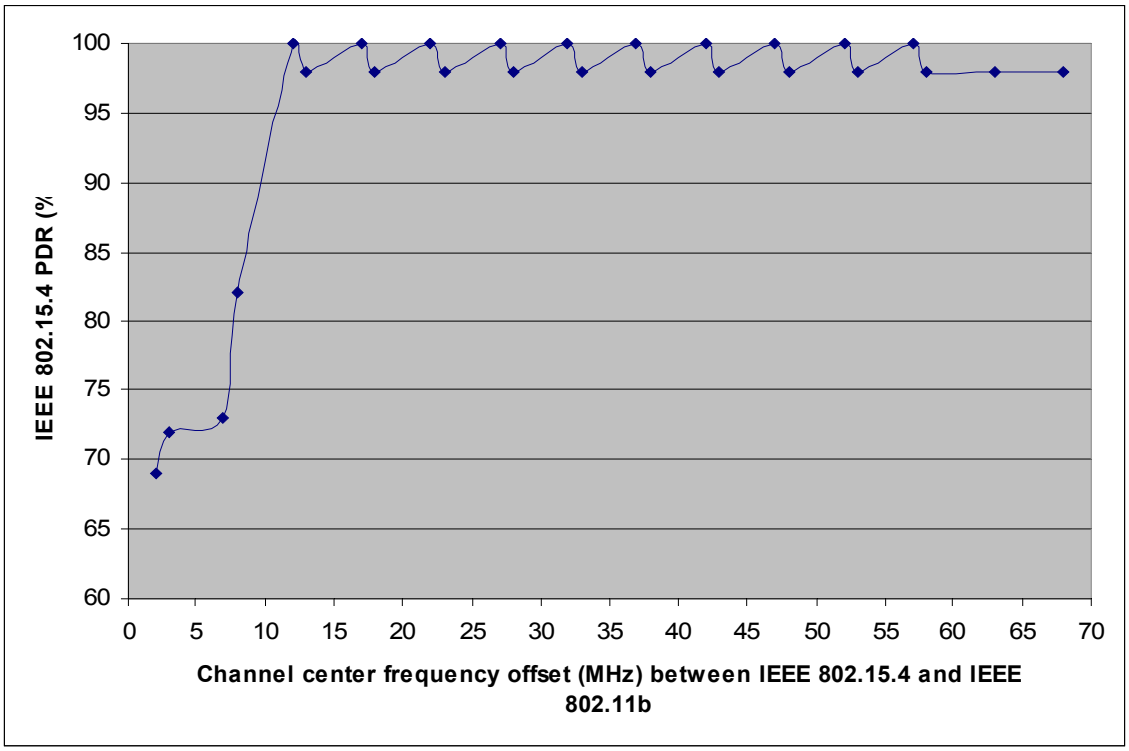


Figure 6.3: Channel center frequency offset, distance between nodes is 1m.

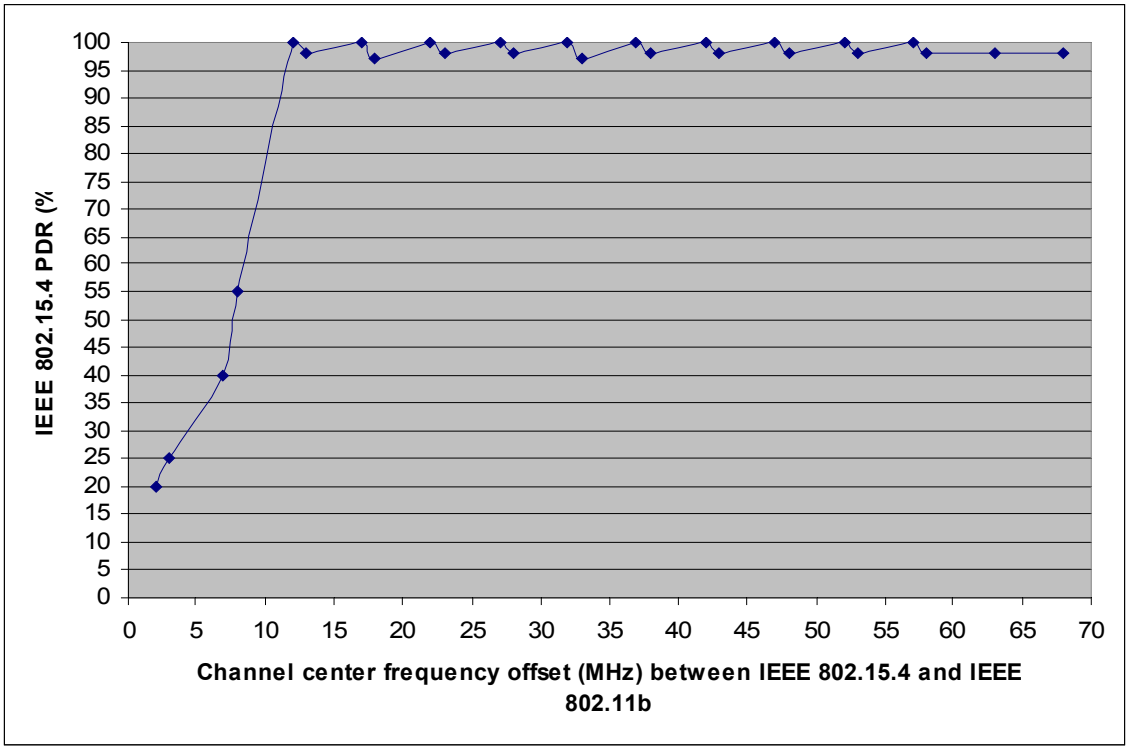


Figure 6.4: Channel center frequency offset, distance between nodes is 10m.

Figures 6.3 and 6.4 explain the dependence of the IEEE 802.15.4 PDR on the channel center frequency offset between an IEEE 802.15.4 network and IEEE 802.11b. It can be observed that when the channel frequency offset between the 2 wireless systems is greater than 7 MHz, the IEEE 802.15.4 communication exceeding 80% giving a reliable sensor network. These results are consistent with the previous works done in [23] and [29]. [23] states that the frequency offset should be at least 7 MHz and [33] recommends that the frequency offset should be larger than 7 MHz. It can also be inferred that in the presence of a nearby IEEE 802.11b link, say at 1 meter or more, the IEEE 802.15.4 network can achieve more than 90 % PDR if the channel frequency offset is greater than 7 MHz. Clearly, FH brings the advantage that less time is spent on the channels having a frequency offset of equal to or less than 7 MHz and the resulting PDR is increased.

CHAPTER 7

Frequency hopping in fading channels

This chapter deals with the properties of frequency selective channels, giving some basic definitions to explain the characteristics of the wireless communication channel. The channel models used in our measurements are given and then finally the results of frequency hopping performance over those channels are included in order to draw important conclusions.

7.1 Wireless channel

This section explains the basic properties of the wireless channel which are desirable for understanding the behavior of multi-path fading channels [34].

7.1.1 Multipath propagation

The received signal at the receiver normally comes from more than one path from the transmitter as shown in Figure 7.1. Each path has its own unique physical properties. These physical parameters include: Path attenuation a_k, path delay τ_k, phase shift ϕ_k and angle of arrival θ_k.

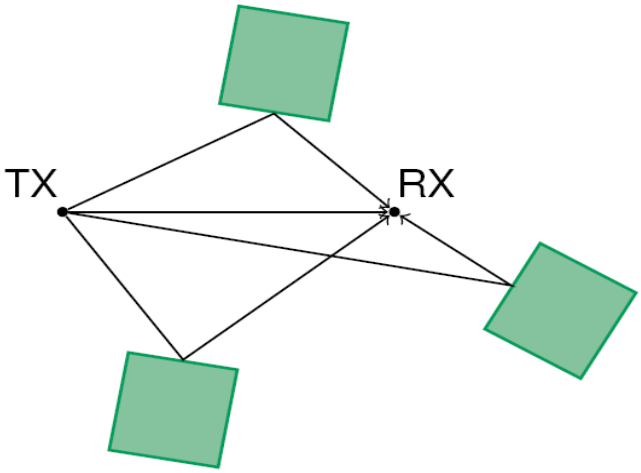


Figure 7.1: Multipath propagation [34]

The impulse response of the baseband channel is described by Equation (7.1):

$$h(t)=\sum_{k=1}^{K} a_k \times e^{j\phi_k} \times e^{-j2\pi f_c \tau_k} \times \delta(t-\tau_k) \qquad (7.1)$$

The phase shifts ϕ_k are caused by delays τ_k.

The received signal is given by the convolution of the transmitted signal $s(t)$ and channel impulse response as described by Equation (7.2):

$$R(t)=s(t)*h(t)=\sum_{k=1}^{K} a_k \times e^{j\phi_k} \times e^{-j2\pi f_c \tau_k} \times s(t-\tau_k) \tag{7.2}$$

The received signal in Equation (7.2) is made up of multiple scaled and delayed copies of the transmitted signal. The variable τ_k is the delay and $a_k \times e^{j\phi_k} \times e^{-j2\pi f_c \tau_k}$ defines the amplitude and phase shift of the kth signal component.

The frequency response of the channel is given by Equation (7.3):

$$H(f)=\sum_{k=1}^{K} a_k \times e^{j\phi_k} \times e^{-j2\pi f_c \tau_k} \times e^{-j2\pi f \tau_k} \tag{7.3}$$

From Equation (7.3), one can see that the frequency response is equal to the complex numbers sum at frequency f. When these complex frequencies are added destructively at the receiver, the frequency response is normally minimum, or zero, on those frequencies. These dips in the channel frequency response are characteristic of wireless communications channels and this phenomenon is called *frequency selective fading* [34]. Multipath propagation in Equation (7.2) can be viewed as undesired filtering of the transmitted signal.

The multipath effect has drastic effects on the communication channel. It can lead to an entire black out of communication between the transmitter and receiver, even when the signals are received they are distorted too much, such as in wideband signals, and it is not simple for the receiver to recognize their original content. The consequences of multipath are studied both in the time and frequency domains and in terms of wide band and narrow band signals as each type of signal has a different response to frequency selective fading.

The frequency selective fading channels are normally studied in the frequency domain as both the transmitted signal bandwidth and channel frequency response can be visualized together, especially in the case of a rapidly changing channel frequency response. The coherence bandwidth is defined as the transmitted signal bandwidth over which the channel frequency response is constant. Flat fading occurs when the channel frequency response is constant over the transmitted signal bandwidth. Frequency selective fading occurs when the channel frequency response changes rapidly over the transmitted signal bandwidth.

There is an interesting duality in the relationship between frequency selective fading and intersymbol interference (ISI). ISI represents the same ideas as frequency selective fading, however, it does so in the time domain. Wide band signals suffer from frequency selective fading and ISI, hence an equalizer is needed at the receiver to recover the signal. The other more efficient alternatives used are FH, orthogonal frequency division multiplexing (OFDM) and Rake receiver. FH have been selected in this work due to its low computational and energy characteristics, which are well suited for low power and size of the WSNs.

7.1.2 Time varying channel

Time variability is another important property of wireless channels which, together with multipath propagation, contributes to fading. The main reason for the time varying channel is the mobility of both the transmitter and receiver or only one of them. As the nodes move, whether slowly or rapidly, the properties corresponding to each path also change. This change of node position affects both the path gain and path delay. The changes in path gain are not large enough to be be effective and can be neglected in some wireless channels. The changes in delay are related to phase changes which play an important factor in any channel frequency, causing the frequency response to change for short time spans resulting in fast fading [34].

Doppler shift

When both of the nodes are moving, or one of them is moving, then on each path due to their speed, there is a corresponding shift in the frequency of a transmitted signal. This frequency shift is the Doppler shift. It is given by Equation (7.4):

$$f_d = \frac{vf}{c} \tag{7.4}$$

where f_d is the Doppler shift in Hertz, f is the transmitted signal frequency in Hertz and c is the speed of light. Take the example of a 2415 MHz carrier frequency in the 2.4 GHz ISM band, which is channel 13 of IEEE 802.15.4, the corresponding Doppler shift is then 6.7083 Hz.

Doppler spectrum

The angles of arrival are different for each each path so each path has a different Doppler shift. These different Doppler shifts form a Doppler spectrum.

Coherence time

The coherence time of a channel is the time during which a channel is considered constant. The coherence time and Doppler spectrum are dual quantities. The Doppler spectrum is used to study the time varying channel in the frequency domain, while coherence time is used to study the time varying channel in time domain. They are related by Equation (7.5):

$$T_c = \frac{1}{f_d} \tag{7.5}$$

where T_c is the coherence time and f_d is the Doppler shift.

The statistical characterization of channels is done by: power delay profile (RMS delay spread), frequency coherence function (coherence bandwidth), time coherence function (coherence time), and Doppler spread function (Doppler spread) [34].

7.1.3 Fading distributions

The fading distributions described here are most commonly used for the modeling of wireless channels. They have also been used by the channel models used in this work [35].

Classical (Rayleigh) distribution

The classical Rayleigh distribution is used in the particular multipath environment where all multipath components suffer the same delay and there is no line of sight signal. The Rayleigh amplitude distribution shows on average the steep and deep fades having a wavelength period. The probability density function of Rayleigh distribution is given by Equation (7.6):

$$p_{Ra}(r) = \frac{r}{\sigma^2} \exp\left(\frac{-r^2}{2\sigma^2}\right) \tag{7.6}$$

Here r is amplitude and $2\sigma^2$ is mean power.

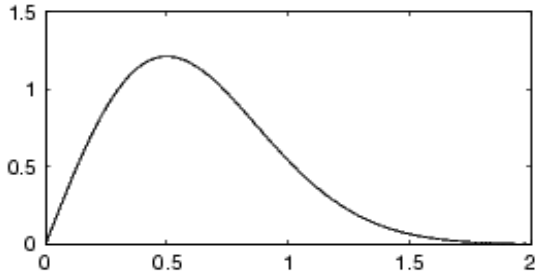


Figure 7.2: Probability density function of Rayleigh distribution [36]

Rice distribution

The Rice model is obtained by combining the classical model and the pure Doppler model. This gives the Rician fading channel one large dominant path along with other multiple scattered paths. If the dominant path is not present or weak, the Rice distribution transforms back to Rayleigh distribution. The Rice distribution of amplitude r is given by Equation (7.7):

$$p_{Ri}(r) = \frac{2\mathrm{rK}}{r_s^2} \exp\left(-K\frac{(r^2+r_s^2)}{r_s^2}\right) I_0\left(\frac{2\mathrm{rK}}{r_s}\right) \tag{7.7}$$

where the Rician factor K is the power ratio between the direct wave and the scattered waves.

$$K = \frac{r_s^2}{2\sigma^2} \tag{7.8}$$

where is the r_s is the amplitude of the classical component and $2\sigma^2$ is the power of the scattered paths.

7.2 Testbed

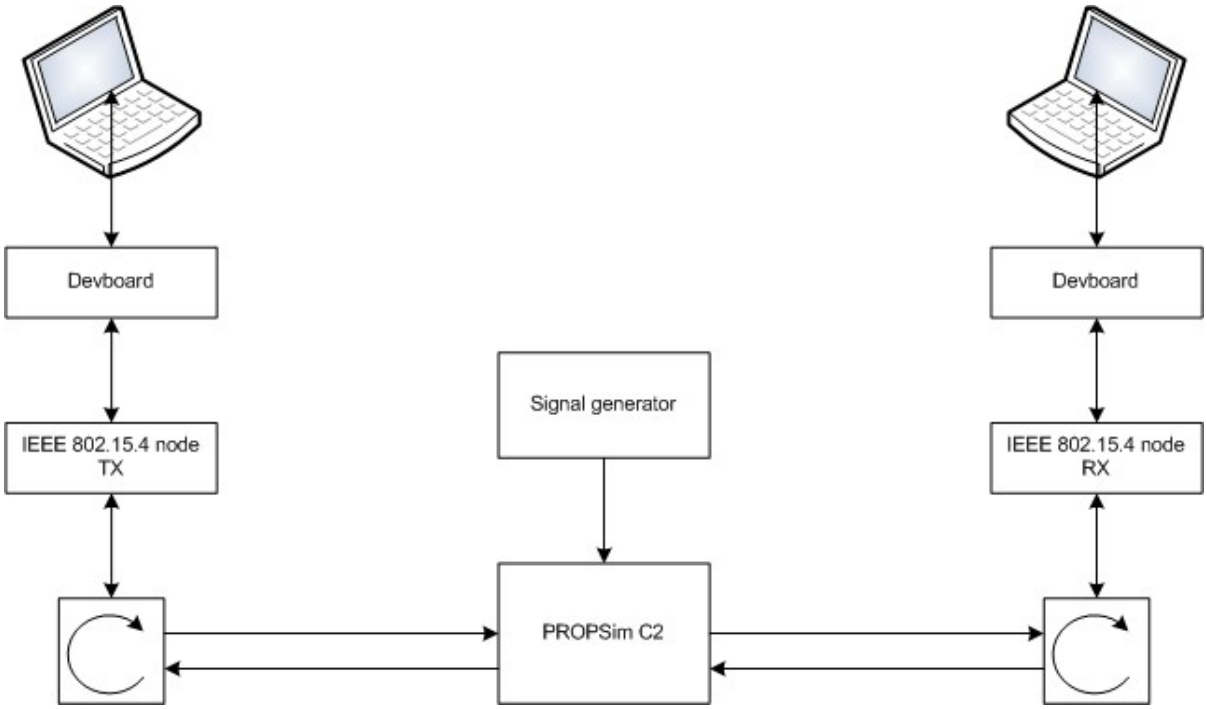


Figure 7.3: Testbed

The testbed shown in Figure 7.3 has been used for testing the FH performance over the frequency selective channel. This test bed is somewhat similar to the first testbed shown in Figure 6.3. This test bed uses a PROPSim C2 channel simulator to simulate the real time wireless channel between the nodes. The other components include the external circulators and the signal generator for providing a clock signal to the channel simulator.

The PROPSim C2 channel simulator [35] is used here to simulate the real time multipath fading channel between the transmitter and receiver. It supports up to 30 MHz of bandwidth, 24 fading paths in one channel and 0.1 ns of delay resolution. The channel simulator has many built in standard wireless channels and the user can input and simulate a completely new channel model by using an easy to use interface. The main simulation parameters are mobile speed, input level, crest factor, output gain, the center frequency of transmitted signal as well as optional noise level. These parameters are entered by the user when building a new channel. The channel path parameters include the delay, delay function, delay properties, amplitude, amplitude distribution, distribution parameters and Doppler spectrum type. These channel path parameters are also entered by the user. The simulation parameters and path parameters together specify a complete wireless channel and their selection requires a basic knowledge of the wireless channel.

The channel simulator requires an external clock signal from a signal generator to simulate the channel properly, otherwise it cannot work. The clock signal frequency entered by the user is equal to the transmitted carrier center frequency plus a fixed 300 MHz factor. The 2 channels provided by channel simulator are one way. External circulators are used to convert these 2 one way channels into one 2 way channel.

7.3 Channel models

The channel models used in this work are from [37] and [38]. The models are applicable for the 2 GHz and 5 GHz frequency bands as the models were developed using experimental data and results from both of these bands. The channel models of [38] are based on WLAN channel models developed by [37]. The models proposed by [37] and [38] are modeled on different environments. The models of [38] are mainly for typically small homes and office environments. The models used are following the:

Model A

Model A is applicable for an office environment, non-line-of-sight (NLOS) conditions having 50 ns rms delay spread.

Model B

Model B is applicable a for large open space and office environments, NLOS conditions having 100 ns rms delay spread.

Model C

Model C is applicable for a large open space (indoor and outdoor), NLOS conditions having 150 ns rms delay spread.

Model D

Model D is the same as Model C, line-of-sight (LOS) conditions having 140 ns rms delay spread. At the first delay, a spike of 10 dB Ricean K-factor is present.

The path loss model used by [38] for the above mentioned channel models consists of the free space loss having a slope of 2 up to a breakpoint distance, changing to a slope of 3 after the breakpoint distance. The breakpoint distance d_{BP} is given by Equation (7.9):

$$\begin{aligned} L(d) &= L_{FS}(d), d \le d_{BP} \\ L(d) &= L_{FS}(d_{BP}) + 35\log_{10}(d / d_{BP}), d > d_{BP} \end{aligned} \tag{7.9}$$

where d is the separation distance in meters between the transmitter and receiver separation. The Doppler spectrum considered in theses models consists of 3 sub components: the main temporal Doppler component, the Doppler component due to a moving vehicle and the Doppler components due to fluorescent lights. The difference in Doppler shifts of all the signal components results in a single fading channel tap, this difference is called the Doppler spread.

The frequency response of Model A, Model B, Model C and Model D is shown in Figure 7.4, Figure 7.5, Figure 7.6 and Figure 7.7 respectively. They are explained in detail in the next section.

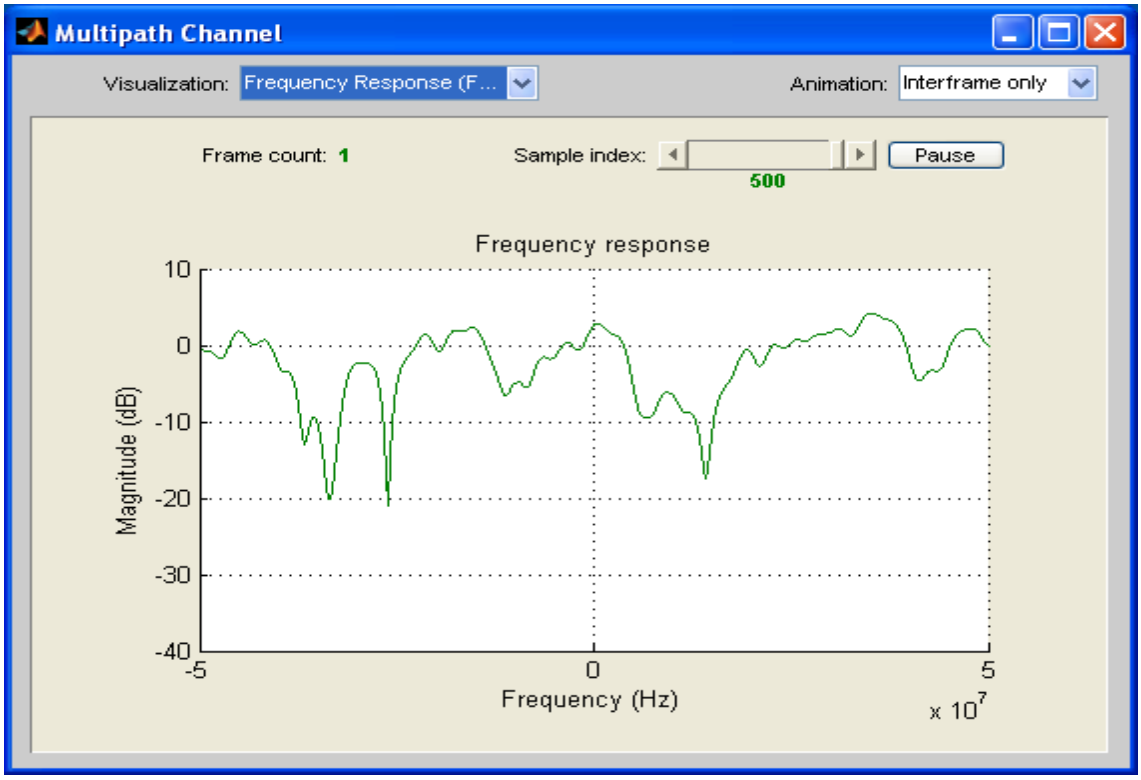


Figure 7.4: Frequency response of Model A

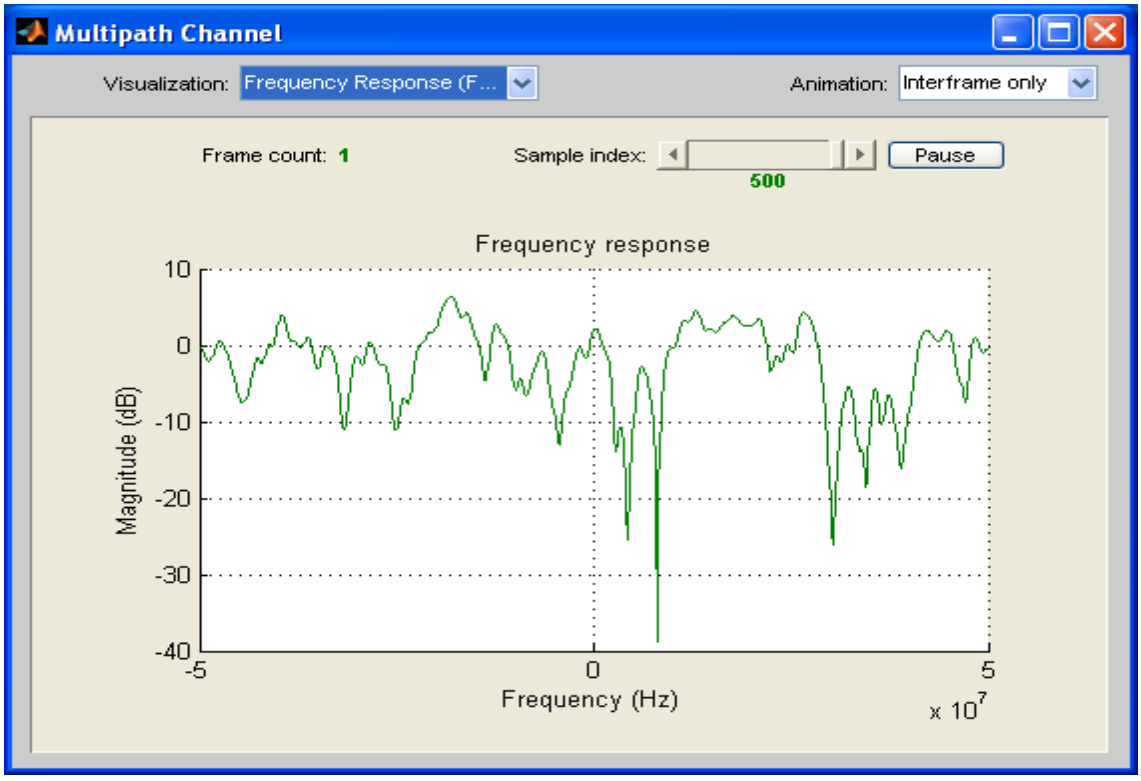


Figure 7.5: Frequency response of Model B

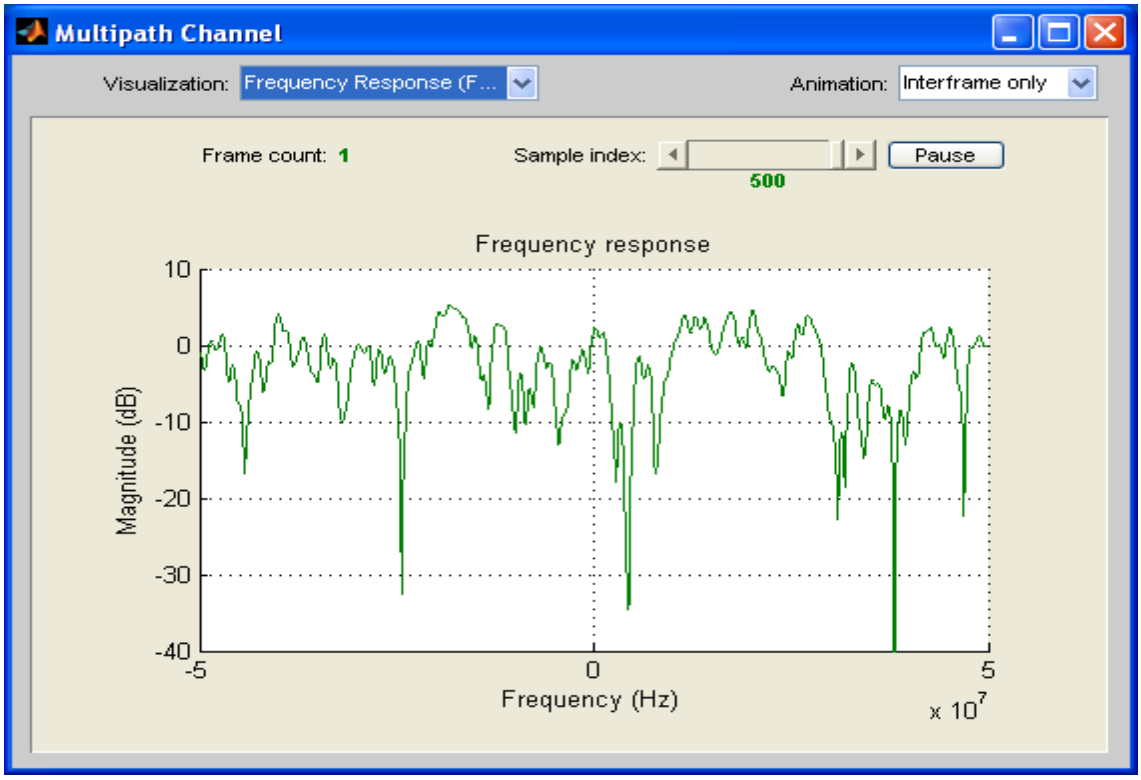


Figure 7.6: Frequency response of Model C

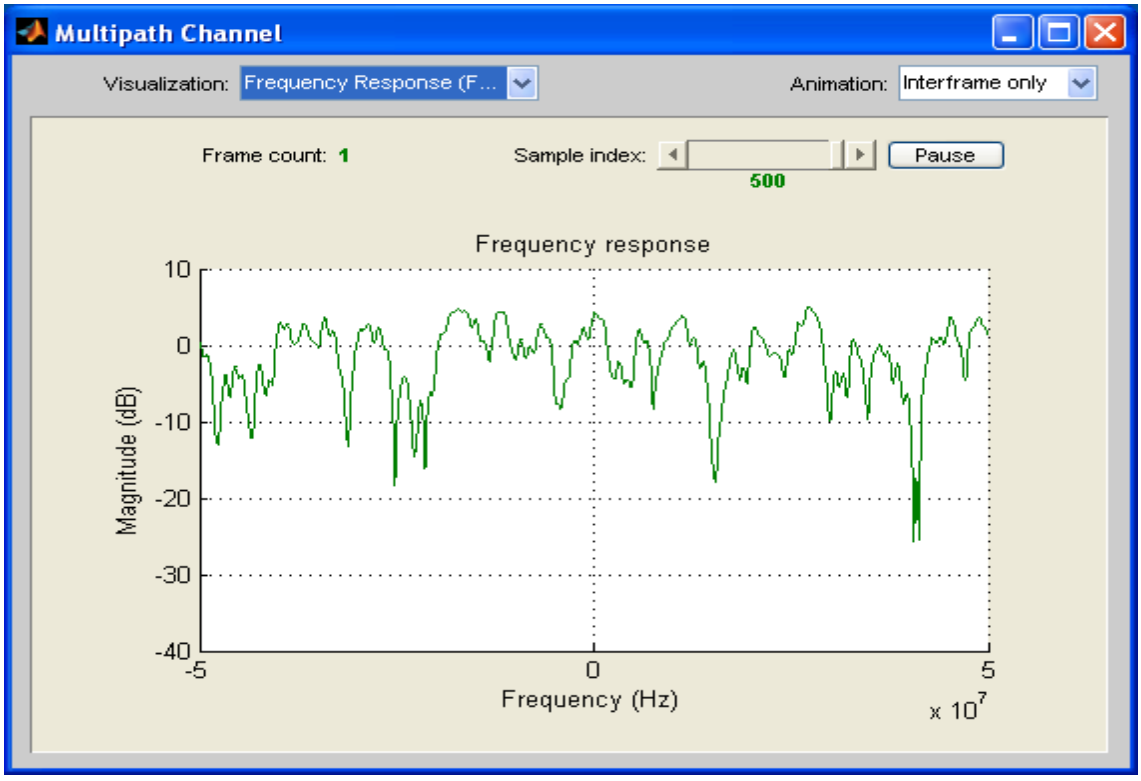


Figure 7.7: Frequency response of Model D

7.4 Frequency hopping in frequency selective fading channel

This section deals with the testbed results and their analysis regarding the performance of frequency hopping in a frequency selective fading channels.

The total bandwidth occupied by 16 channels of IEEE 802.15.4 in the 2.4 GHz ISM band is 83.5 MHz. The channel simulator bandwidth is limited to 30 MHz. Therefore, we reduced channels from 16 having 83.5 MHz bandwidth to only 5 (11, 12, 13, 14, 15) having a 30 MHz bandwidth in the case of FH to compensate for this deficiency in the channel simulator. Consider Figure 7.4, Figure 7.5, Figure 7.6 and Figure 7.7, where the frequency response of the channels is shown over the transmitted signal bandwidth of 100 MHz. Thus the frequency response for both cases can be seen, the one used here of 5 channels having 30 MHz bandwidth, and the original case of 16 channels having a overall 83.5 MHz bandwidth. In the frequency response, the 0 frequency corresponds to the transmitted center frequency of the 5 channels, which is 2415 MHz (center frequency of channel 13). The frequency range of -1.5×10^7 to 1.5×10^7 Hz on the frequency response is same as the frequency range of the 5 used channels from 2400 MHz to 2430 MHz. Similarly, for the 16 channels, the 0 frequency is equal to the center frequency of 2441.75 MHz and the frequency range is -4.175×10^7 to 4.175×10^7 Hz on the frequency response.

Table 7.1 shows the results of an IEEE 802.15.4 single channel operation using the channel models described in Section 7.3. Table 7.2 shows the results of an IEEE 802.15.4 FH operation using the channel models described in Section 7.3. The results are given in terms of the PDR at the receiver. The results for each channel model are subsequently analyzed.

Table 7.1: Testbed results with single channel

Single channel							
Transmitted packets = 510							
Model A		Model B		Model C		Model D	
PDR (%)	85 ± 1	PDR (%)	77 ± 2	PDR (%)	70 ± 2	PDR (%)	80 ± 2

Table 7.2: Testbed results with frequency hopping

Frequency hopping							
Transmitted packets = 510							
Model A		Model B		Model C		Model D	
PDR (%)	95 ± 0.78	PDR (%)	90 ± 2	PDR (%)	85 ± 2	PDR (%)	90 ± 1

7.4.1 Model A

The PDR is 85% with a single channel as shown in Table 7.1 and increases to 95% with FH as shown in Table 7.2. The improvement achieved is 10% with FH compared to single channel. On inspecting Figure 7.4, it is noticeable that the channel is overall good for a 30 MHz bandwidth range of 2400-2430 MHz. There is one deep fade of -16 dB at approximately

2430 MHz and one small fade of -9 dB located on the left side of the deep fade. These 2 fades together serve as the major sources of packet loss. Due to this small number of fades, the transmission in the single channel is able to achieve 85% PDR. These fades that are present are, however, not enough to cause a total blackout of communication and 0% PDR, when the communication channel on these fades. The performance of FH is excellent as expected, because it avoids these fades most of the time giving a 95% PDR. Due to FH, the network spends less time on deep fades and the average network performance is very good. Now it is possible to speculate about the performance for the 83.5 MHz bandwidth case from Figure 7.4 and a 30 MHz bandwidth case. This figure shows, that it includes 2 more fades of a much higher magnitude of -20 dB. Therefore, in single channel case, if the transmitted carrier happens to be on these 2 deep fades, then the PDR is much less than the current 85% PDR, probably around 70%. If FH is used in the 83.5 MHz bandwidth case, then due to the less amount of time spent on all deep fades, the PDR is reduced negligibly and the range for the PDR would be 90%-95%.

7.4.2 Model B

The PDR is 77% with single channel as shown in Table 7.1 and increases to 90% with FH as shown in Table 7.2. This results in a 13% more PDR in FH than single channel usage. From Figure 7.5 can be seen that the channel has approximately 10 small and large fading notches on the 30 MHz bandwidth range of 2400 MHz to 2430 MHz. The 2 largest fades are approximately at 2420 MHz having -25 dB magnitude and 2423 MHz having -39 dB magnitude. These fades can cause total communication blackout when data is transmitted through them. As these channels have frequency selective fading almost throughout the 30 MHz bandwidth, the PDR, therefore, drops to 77% from 85% in Model A for the single channel case. The PDR with FH is 90%, which is very good considering the channel conditions and the improvement over single the channel case. Although the PDR is 5% less than Model A, which is a more flat channel, the same pattern can be seen for the single channel case as the PDR here is 8% less than in Model A. Now it should be possible to predict the 83.5 MHz bandwidth case from Figure 7.5 and the 5 channels case. As can be seen, for the 16 channels there are many more large fades than for the 5 channels case and the fading notches are distributed over half of the channel. When the single channel being used happens to be in one of these large fades, the resulting drop in PDR will be 50% or even zero in many channels. In the case of FH, the fading notches are distributed evenly, and depending upon less channel stay time and a large number of transmitted packets, the PDR range can be from 80% -90%.

7.4.3 Model C

The PDR is 70% with the single channel as shown in Table 7.1 and increases to 85% with FH as shown in Table 7.2. The improvement achieved is 15% with FH compared to the single channel. Figure 7.6 shows that the channel has a lot of attenuation in the 30 MHz bandwidth range of 2400-2430 MHz. The largest fade is of -35 dB at 2420 MHz and the 2 largest notches after it are on either side of this fade, both of approximately -17 dB. There are many small fades also in the result of the frequency band. This channel model has a considerable

amount of frequency selectivity, therefore, the PDR for the single channel case is 70%, the lowest of all channel models. The FH performs well in this channel giving a PDR of 85% despite having the largest frequency selectivity of all channel models. The PDR of 85% with FH is the lowest among all channel models. The assumptions for all 16 channels having 83.5 MHz bandwidth can be made from results from FH over 5 channels and Figure 7.6. For 16 channels having a bandwidth of 83.5 MHz, the channel response is the same as before. In the single channel case, the resulting PDR would be less than 50% and zero in may channels. The network using FH over all 16 channels will achieve the PDR in the range of 75-85% as the channels before the center frequency have the same fading characteristics as of the 2400-2430 MHz range but after the center frequency of 2441.75 MHz, there are large fades which will result in a further packet drop of 5%.

7.4.3 Model D

The PDR is 80% with the single channel as shown in Table 7.1 and increases to 90% with FH as shown in Table 7.2. The improvement achieved is 10% with FH compared to the single channel. Careful inspection of Figure 7.7 shows that the channel is overall consistent for the 30 MHz bandwidth range of 2400-2430 MHz. There is one deep fade of -18 dB at approximately 2430 MHz and 2 small fades of approximately -8 dB each. These 3 fades located at constant frequencies from each other causes a 20% packet drop in the single channel case, making the received PDR to be 80%. As these fades are not of significant magnitude to cause a communication blackout when the channel used lies on these fades, the single channel network can survive on this model as on Model A. The FH performs very well on this channel giving a PDR of 90% as there is one considerable bad channel compared to the other 4 channels, so the total amount of time spent and data sent on the bad channel is small compared to the 4 other channels combined. Now we the performance for the 83.5 MHz bandwidth case is extrapolated from Figure 7.7 and the 30 MHz bandwidth case. It can be seen that it includes at least 7 more fades of higher magnitude higher than -20 dB. So in the single channel case, if the transmitted carrier happens to be on these deep fades, then the PDR drops in the worst case to less than 50%. If FH is used in the 83.5 MHz bandwidth case, then due to the less amount of time spent on all deep fades, the PDR is reduced negligibly and the estimated range for PDR would be 80%-90%.

In summary, the different wireless channel models shown above which represent different frequency selective conditions, clearly demonstrate that FH works in all situations, maintaining a PDR of at least 85%, and normally more than that. However, the same network operation in a single frequency selective channel considerably reduces the amount of data transmission and in some cases there is no data transfer at all when the channel lies directly on the fade. The results of the testing shows that FH should be used as a reliable source of communication method in WSNs as it guarantees successful network operation in nearly all indoor frequency selective environments.

CHAPTER 8

Conclusion and future work

The aim of this thesis was to implement and study the performance of FH in IEEE 802.15.4 based WSNs as a reliable coexistence tool. The results showed clearly that main source of interference for IEEE 802.15.4 networks are IEEE 802.11.b/g networks, which can seriously degrade the performance of WSNs due to their wider and more powerful signals. The performance evaluation of single channel IEEE 802.15.4 nodes and IEEE 802.15.4 using FH was done under the presence of a strong WLAN interference source. It was seen that the performance of a single channel network falls drastically down to less than 50%, while under the same conditions, the performance with FH was more than 90%. With the increase in the distance between nodes, these figures dropped to 10% for the single channel case, but for the FH case, this drop was only to 85% from 90%. The second situation studied was when the communication channel has frequency selective fading. The network performance in the presence of frequency selective fading was first studied with single channel and then with FH. The FH gave a 10% to 20% improvement compared to the single channel in a frequency selective situation. The 10% to 20% results depend on the channel being studied, if the channel is more frequency selective then the performance improvement with FH will be more than these results. Hence, it can be stated with confidence that FH is an excellent tool for reliable IEEE 802.15.4 communications for all situations and it must be used when and wherever possible.

Possible future implementations and research could include the fast frequency hopping scheme, adaptive frequency hopping and efficient interference detection and estimation based scheme. In fast frequency hopping, the channel is changed per data symbol so the effective interference time is very small. In adaptive frequency hopping the hopping pattern is adapted continuously according to the changing channel conditions, and for this performance the built in tools of IEEE 802.15.4 can be used such as RSSI, PER and LQI. The advanced interference detection and estimation based schemes are used in cognitive radio. The main parts of cognitive radio are: spectrum sensing, spectrum sharing, spectrum management and spectrum mobility.

References

[1] Nitaigour P. Mahalik. Sensor networks and configuration: fundamentals, standards, platforms, and applications. Berlin Heidelberg: Springer-Verlag, 2007. VII.

[2] Yingshu Li, My T. Thai and Weili Wu. Wireless sensor networks and applications. New York: Springer Science+Business Media, LLC, 2008.

[3] Shahin Farahani. ZigBee Wireless networks and transceivers. Burlington: Elsevier Ltd, 2008.

[4] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler. Transmission of IPv6 packets over IEEE 802.15.4 networks, RFC 4944, September 2007.

[5] Jonathan W. Hui and David E. Culler. Extending IP to low-power, wireless personal area networks. IEEE Internet Computing July/August 2008: 37-45.

[6] David E. Culler. New IETF 6LoWPAN standard moves wireless sensor networks into the IP mainstream. Arch Rock Corporation 2008.

[7] IEEE Std.802.15.4: IEEE standard for wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LRWPANs), 2006.

[8] Holger Karl and Andreas Willig. Protocols and architectures for wireless sensor networks. West Sussex: John Wiley & Sons, Ltd, 2005. 144-145.

[9] Azzedine Boukerche. Algorithms and protocols for wireless sensor networks. Hoboken: John Wiley & Sons Inc, 2009. 503-519.

[10] J. Elson, L. Girod, and D. Estrin. Fine-grained network time synchronization using reference broadcasts. In Proceedings of the Fifth Symposium on Operating Systems Design and Implementation (OSDI 2002), December 2002, pp. 147–163.

[11] M. Maro´ti, B.Kusy, G. Simon, and A´ . Le´deczi. The flooding time synchronization protocol. In ACM Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSyS 2004), November 2004, pp. 39–49.

[12] S. Ganeriwal, R. Kumar, and M. B. Srivastava, Timing-sync protocol for sensor networks, In ACM Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSyS 2003), November 2003, pp. 138–149.

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

[14] IEEE Std.802.15.2: Coexistence of wireless personal area networks with other wireless devices operating in unlicensed frequency band, 2003.

[15] Eric Meihofer. Enhancing ISM band performance using adaptive frequency hopping. 2001.

[16] P. Popovski, H. Yomo, S. Aprili, and R. Prasad, “Frequecny rolling: a cooperative frequency hopping for mutual inteferring WPANs,” in Proc. ACM Mobihoc Conf., May 2004, pp. 199–209.

[17] P. Popovski, H. Yomo, and R. Prasad, Dynamic Adaptive Frequency Hopping for Mutually Interfering Wireless Personal Area Networks, IEEE Transactions on Mobile Computing, vol.5, no.8, pp. 991-1003, August 2006.

[18] Anthony D. Wood, John A. Stankovic, Gang Zhou, DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks, in The 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), San Diego, CA, June 2007.

[19] G. Alnifie and R. Simon, A multi-channel defense against jamming attacks in wireless sensor networks, in Q2SWinet07: Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks. New York, NY, USA: ACM, 2007, pp. 95-104.

[20] M. Li, I. Koutsopoulos, and R. Poovendran, “Optimal jamming attacks and network defense policies in wireless sensor networks,” in INFOCOM [117], pp. 1307-1315.

[21] Co-existence of IEEE 802.15.4 at 2.4 GHz. Application Note. Jennic 2008.

[22] A Sikora and V. F. Groza, Coexistence of IEEE802. 15.4 with other Systems in the 2.4 GHz-ISM-Band, Proceedings of IEEE Instrumentation and Measurement , May 2005, pages 1776-1791.

[23] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella, Performance Study of IEEE 802.15.4 Using Measurements and Simulations, in Proc. IEEE Wireless Communications and Networking Conference (WCNC), vol. 1, pp. 487-492, April, 2006.

[24] K. Shuaib, M. Boulmalf, F. Sallabi, and A. Lakas, Co-existence of Zigbee and WLAN: A performance study, in Proc. IEEE/IFIP Int. Conf. Wireless & Optical Communications Networks, Bangalore, India, April 2006.

[25] ZigBee and Wireless Radio Frequency Coexistence. ZigBee Alliance. June 2007.

[26] S. Shin, S. Choi, H. S. Park, and W. H. Kwon, Packet error rate analysis of IEEE 802.15.4 under IEEE 802.11b interference, in Proceedings of WWIC 2005, LNCS, Springer, May, pp. 279–288.

[27] Shin S.Y., Park H.S., and Kwon W.H., Packet Error Rate Analysis of IEEE 802.15.4 under Saturated IEEE 802.11b Network Interference, IEICE TRANSACTIONS on Communications Vol.E90-B No.10 pp.2961-2963, 2007.

[28] Shin S.Y., Park H.S., Choi S., and Kwon W.H.,Packet Error Rate Analysis of ZigBee Under WLAN and Bluetooth Interferences, IEEE Transactions on wireless communications, vol. 6, no. 8, pp. 2825-2830, August 2007.

[29] Soo Young Shin, Hong Seong Park, Wook Hyun Kwon, Mutual interference analysis of IEEE 802.15.4 and IEEE 802.11b. Computer Networks: The International Journal of Computer and Telecommunications Networking, Volume 51, Issue 12, pp. 3338-3353, August 2007.

[30] NanoStack Manual. Sensinode Ltd 2008.

[31] NanoStack Reference. Sensinode Ltd 2008.

[32] http://www.freertos.org/, December 2008.

[33] http://pf.itd.nrl.navy.mil/mgen/mgen.html. December 2008.

[34] Dr.B.- P. Paris. From Physical Propagation to Multi-Path Fading Statistical Characterization of Channels. Wireless Communications Course.

[35] PROPSim C2 Wideband Radio Channel Simulator Operation Manual. Copyright Elektrobit Ltd. 2004.

[36] http://www.mathworks.com/access/helpdesk_r13/help/toolbox/stats/prob_d27.html. December 2008.

[37] J. Medbo and P. Schramm, “Channel models for HIPERLAN/2,” ETSI/BRAN document no.3ERI085B.

[38] IEEE P802.11 Wireless LANs TGn Channel Models. May 10, 2004.