WLAN 802.11 b/g interference into ZigBee networks

by

Guang Yang

Yu Yu

Master Thesis in

Information and Communication Technology

Supervisor:

Magne Arild Haglund

Agder University

2008.05

Abstract

ZigBee network as a low rate wireless personal area network (LR-WPANs) developed very fast nowadays. Since both ZigBee network and WLAN (802.11b/g) operate in the 2.4GHz unlicensed industrial scientific medical (ISM) frequency band, signal interference is possible to exist and result in signal degradation when devices are collocated in the same environment.

This thesis analyzes, simulates and measures the interference and evaluates ZigBee network performance under the WLAN interference in terms of Packet Error Rate (PER) and Packet Loss Ratio (PLR). And the investigation emphasis of this thesis is impacts of ZigBee network under diverse interference that with respect to different distances between two networks and different centre frequency offsets. An interference simulation model was suggested in order to obtain analytical PER. AVR RZ200 evaluation kit was used for actual Packet Loss Ratio measurement.

This thesis introduces methods that can be utilized in investigation of interference issue of two coexistent wireless networks. The research results are significant for further research and development in ZigBee field.

Preface

This thesis is submitted in fulfillment of the requirements for the Master of Science degree in Information and Communication Technology at the Faculty of Engineering and Science at Agder University, Grimstad, Norway. This thesis was proposed by Devoteam and carried out under the supervision of Magne Arild Haglund.

First of all we wish to thank our main supervisor Magne Arild Haglund for first-class guidance throughout the project period. His insight and analytical skills have been greatly appreciated in numerous interesting discussions regarding the problem area targeted in this thesis.

We also wish to thank Devoteam assigning this challenge project for us, and especially thank Leif Arne Dalane and Ole-Jonny Gangsøy (Devoteam) giving many technical advices to us and offering us a ZigBee evaluation kit.

Finally we are grateful to Stein Bergsmark, Ole-Christopher Granmo, Sissel Andreassen, Tor Eric Christensen, Pål Grandal and all the teachers. Thank for their teaching and kind help in these two years.

Grimstad, May, 2008
Guang Yang and Yu Yu

Guang Yang

Yu Yu

Table of contents

List of figures

List of tables

Abbreviations and Acronyms

ACK	Acknowledgement
AP	Access Point
APS	Application support sublayer
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
CAP	Contention Access Period
CCA	Clear Channel Assessment
CCK	Complementary Code Keying
CFP	Contention-free period
CRC	Cyclic Redundancy Code
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
CW	Contention Window
DBPSK	Differential Binary Phase Shift Keying
DCF	Distributed Coordination Function
DIFS	DCF Inter Frame Space
DQPSK	Differential Quadrature Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
ED	Energy detection
ERP	Extended Rate PHY
FCC	Federal Communications Commission
FFD	Full-function device
FHSS	Frequency Hopping Spread Spectrum
GPIOs	General Purpose I/O ports
GTSs	Guaranteed time slots
HEC	Header Error Check
IDE	Integrated Development Environment
IEEE	Institute of Electrical and Electronics Engineers
IFS	Inter-Frame Space
IRQ	Interrupt request signal
ISM	Industrial Scientific Medical
ISO	International Organization for Standardization
ISP	In-System Programmer
JTAG	Joint Test Action Group
JTAGICE	Joint test action group in circuit emulator
L2CMP	Logical Link Control and Adaptation Protocol
LED	Light Emitting Diode
LMP	Link Manager Protocol
LSB	Least significant bit
MAC	Media Access Control
MIMO	Multiple-Input Multiple-Output

MISO	Master Input Slave Output
MOSI	Master Output Slave Input
MSB	Most significant bit
MSDU	MAC Service Data Unit
NFC	Near Field Communication
NWK	Network layer
OFDM	Orthogonal Frequency Division Multiplexing
O-QPSK	Offset Quadrature Phase Shift Keying
PAN	Personal Area Network
PCB	Print Circuit Board
PCF	Point Coordinator Function
PER	Packet Error Rate
PHR	PHY header
PHY	Physical layer
PIFS	PCF Inter Frame Space
PLCP	PHY Convergence Procedure
PLME	Physical Layer Management Entity
PLR	Packet Loss Ratio
PN	Pseudo Noise (code sequence)
PPDU	PHY Protocol Data Unit
PSD	Power Spectrum Density
PSDU	PHY Service Data Unit
QPSK	Quadrature Phase Shift Keying
RCB	Radio Controller Board
RFD	Reduced-function device
RFID	Radio Frequency Identification
RISC	Reduced Instruction Set Computing
RSSI	Received Signal Strength Indication
SFD	Start-of-Frame Delimiter
SHR	Synchronization header
SIFS	Short Inter Frame Spacing
SNR	Signal-to-Noise Ratio
SPI	Serial Peripheral Interface
SYNC	Synchronization
WMAN	Wireless Metropolitan Area Network
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
ZDO	ZigBee device object
ZDP	ZigBee device profile

1 Introduction

1.1 Background

In recent years, wireless communication technologies have been developed very fast. Besides our familiar WiFi, Bluetooth, many new technologies such as ZigBee, NFC (Near Field Communication) appeared. But the sequent problem is the unlicensed 2.4GHz (2.4~2.483GHz) ISM (Industrial Scientific Medical) band which is almost global availability becomes crowded. Therefore, the interference issue occurs immediately following a lot of wireless devices sharing the same 2.4GHz frequency band.

So far, 802.11b/g WLAN (Wireless Local Area Network), Bluetooth, ZigBee, cordless telephone and microwave oven utilize the 2.4GHz band, and 802.11n which supposes to release in 2009 is also going to adopt this band, so how these technologies impact each other and their performance in the coexistence environment are important and interesting.

Especially, ZigBee as a really new short distance wireless communication technology which is targeted at low data rate, low power consumption radio frequency applications has potential of developing. Thus, the interference problem between ZigBee and the most prevalent wireless technology WLAN attracts more and more attention.

1.2 Thesis definition

Devoteam is working with ZigBee technology within the Alarm/Security and the Utility segment. Most ZigBee products today are utilizing the 2.4 GHz frequency band (2.4-2.483GHz). WLAN is also operating within the same frequency band.

In this thesis, we focus on analyzing the interference 802.11b/g WLAN brings to ZigBee with respect to the packet error rate (PER) of ZigBee transmission. In order to do this, an interference model will be made, and the relationship between BER (bit error rate) and PER in these environments will be exploited. The model will involve parameters like: ZigBee and WLAN channel choice, the distance between WLAN access point and ZigBee coordinator and WLAN interference into ZigBee nodes. Afterwards, a simple application will be made on ATAVRRZ200 IEEE 802.15.4/ZigBee Demonstration Kit to measure PLR in a ZigBee connection and evaluate the interference model.

1.3 Goal of the project

The goal of this project is to analyse the level of interference between these two wireless technologies with respect to service quality and range when ZigBee networks are overlapping WLAN networks. Sequentially, the most possible channels which can be chosen for the coexistence environment will be concluded.

1.4 Related researches

As an unlicensed frequency band, 2.4GHz band is used by many wireless devices. There already had various studies on the interference issues in this band including researches on the interference problem between WLAN and ZigBee. These researches provide important references for our thesis. In section 3.1, we will give a review about some of these researches.

1.5 Report outline

Chapter 1 is the introduction of this thesis including background, thesis definition, goal of the project and related researches.

Chapter 2 gives the basic description of 802.11b/g WLAN, 802.15.4 WPAN and ZigBee, and takes a look at the general interference issue of 2.4GHz ISM band.

Chapter 3 presents the interference analysis of ZigBee network under WLAN, including BER analysis and PER analysis. The simulated ZigBee PHY layer transmission model and collision time model are defined in this chapter.

Chapter 4 describes the ZigBee demonstration kit which is implemented for test, application layer programming and the actual test processes.

Chapter 5 discusses about comparison of simulation and measurement results, and the other possible parameters could use for evaluating the interference between WLAN and ZigBee network.

Chapter 6 addresses the conclusions drawn from the whole work.

Chapter 7 indicates possible future work.

2 Wireless communication technologies

Due to the fast development in communication field, more and more new technologies are developed and adopted, especially, wireless technology which provides a more convenient way of information transmission that without using cables. In the recent years, there was a vigorous development in wireless communication technology. Such as WiFi for wireless local area network (WLAN), Bluetooth, ZigBee for wireless personal area network (WPAN), WiMAX for wireless metropolitan area network (WirelessMAN) according to IEEE and near field communication (NFC) technology which based on ISO 14443 proximity-card standards, they play very important roles in the communication field. The following Table 2-1 gives basic descriptions of these wireless communication technologies.

Standard	Frequency band	Range	Main feature
WiFi / IEEE 802.11	2.4GHz, 5GHz	~20 - 140 m	ease and low cost, low power radio signal
Bluetooth / IEEE 802.15.1	2.4GHz	1m, 10m, 100m	designed for low power consumption, with a short range based on low-cost transceiver microchips in each device
ZigBee / IEEE 802.15.4	868MHz, 915MHz, 2.4GHz	Many meters	low cost, low power, low data rate and short range
WiMAX / IEEE 802.16	2.3GHz, 2.5GHz, 3.5GHz, 3.7GHz, 5.8GHz	Many kilometers	providing wireless data over long distances in a variety of ways
NFC	13.56MHz	Many centimeters	very short range, secure and compatible with RFID

Table 2-1: Wireless communication technology

Since this thesis primarily concentrates on investigating the interference issue between WLAN and ZigBee, we will go deeply into these two technologies.

2.1 IEEE 802.11 / WiFi

2.1.1 Overview

In the most situations, IEEE 802.11 WLAN would firstly come to our mind when we talk about wireless. IEEE802.11 is a set of standards for wireless local area network (WLAN), which was developed by a working group of Institute of Electrical and Electronics Engineers (IEEE).

a) Evolution of IEEE 802.11

The original version of IEEE 802.11 standard was released in 1997. Table 2-2 lists evolution of IEEE 802.11 standard.

Standard	Release Date	Operation Frequency	Typical Throughput	Max. Data Rate	Modulation Technique	Range (indoor / outdoor)
Legacy	1999	2.4 GHz	0.9 Mbps	2 Mbps	DSSS or FHSS	~20 / 100 Meters
802.11a	1999	5 GHz	23 Mbps	54 Mbps	OFDM	~35 / 120 Meters
802.11b	1999	2.4 GHz	4.3 Mbps	11 Mbps	DSSS	~38 / 140 Meters
802.11g	2003	2.4 GHz	19 Mbps	54 Mbps	OFDM	~38 / 140 Meters
802.11n	06,2009(est.)[1]	2.4 GHz 5 GHz	74 Mbps	248 Mbps		~70 / 250 Meters
802.11y	06,2008(est.)[1]	3.7 GHz	23 Mbps	54 Mbps		~50/ 5000 Meters

Table 2-2: Evolution of IEEE 802.11 standard [2]

- **IEEE 802.11**

The original version of the IEEE 802.11 standard adopts direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) modulation scheme, and specifies two raw data rates that 1 and 2 megabits per second (Mbit/s) to be transmitted in the ISM frequency band at 2.4 GHz. But IEEE 802.11 was rapidly supplemented and popularized by IEEE 802.11b.

- **IEEE 802.11b**

IEEE 802.11b adopts the same modulation scheme DSSS as the original version, but the throughput increases to 4.3Mbps and the maximum data rate is 11Mbps. Since it operates in the unlicensed 2.4GHz ISM frequency band, 802.11b devices will coexist with other products which also utilize the same 2.4GHz ISM band, such as Bluetooth devices, ZigBee devices and so on. And the interference issue is our chief concern in this thesis.

- **IEEE 802.11g**

After four years, in 2003, IEEE 802.11g was ratified. It provides a high data rate 54Mbps and uses the same modulation method OFDM as IEEE 802.11a. IEEE 802.11g also faces the interference problem like 802.11b due to its operation frequency band is still 2.4GHz.

b) Architecture of IEEE 802.11

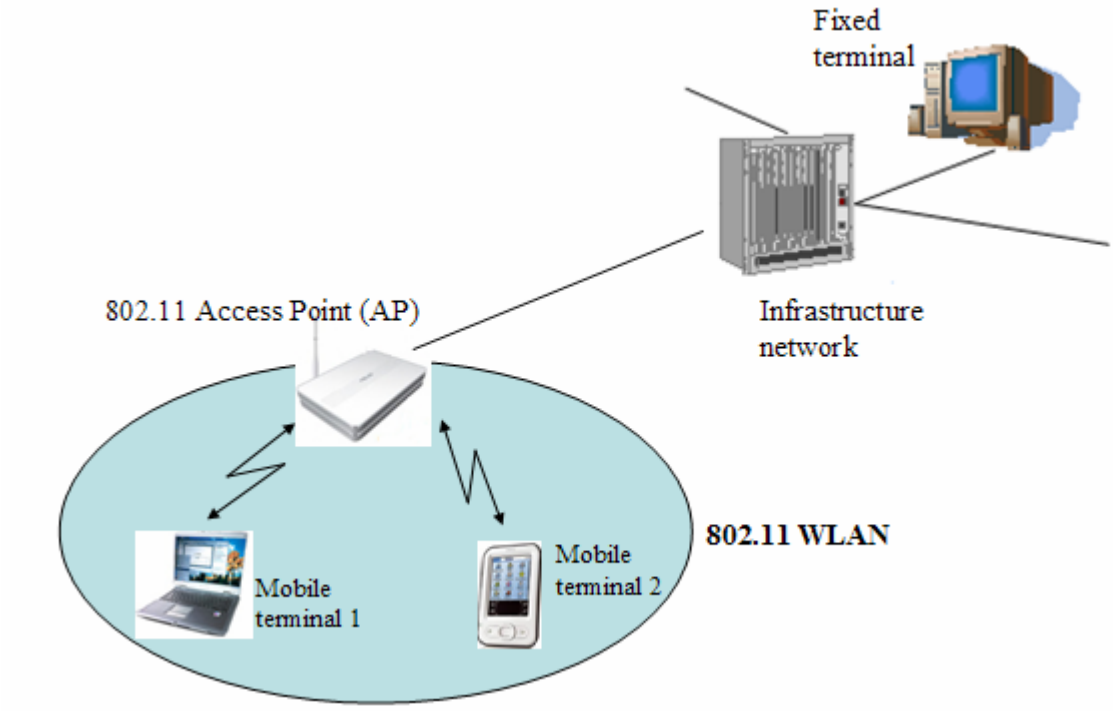

Figure 2-1: 802.11 Architecture of Infrastructure network

2.1.2 IEEE 802.11b

a) Channel selection

IEEE 802.11b standard defines 14 channels in the 2.4GHz ISM band, and there is 5MHz apart from two adjacent channels. Since the bandwidth of WLAN radio signal is 22MHz, not all channels can be used simultaneously. In fact, only three non-overlapping WLAN channels can be used at the same time, there are Channel 1, 6, 11 for North America and Channel 1, 7, 13 for Europe.

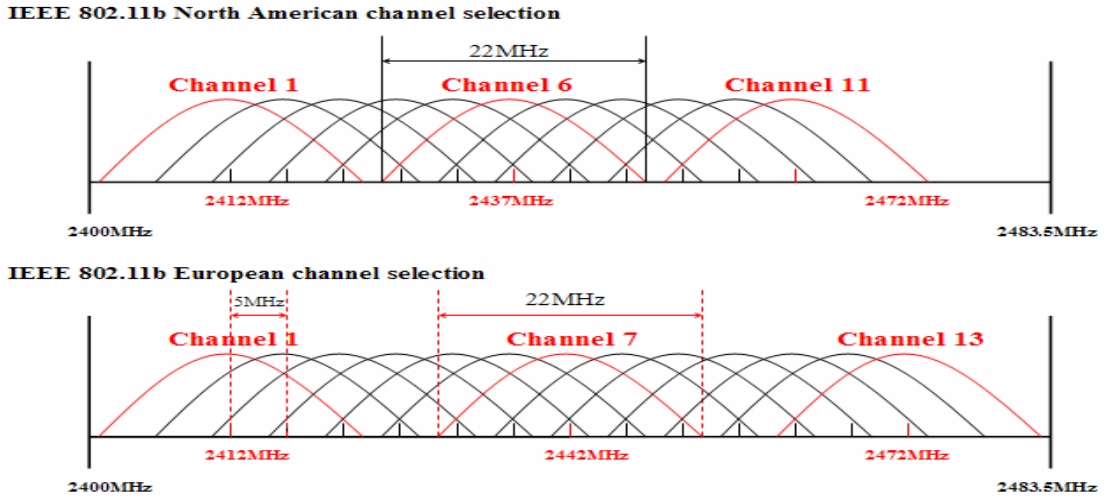

Figure 2-2: WLAN channel selection

b) Modulation technique

802.11b extends the DSSS modulation technique which was defined in the original version of 802.11 standards. This extension of the DSSS system builds on the data rate capabilities, to provide 5.5 Mbit/s and 11 Mbit/s payload data rates in addition to the 1 Mbps which is encoded with differential binary phase shift keying (DBPSK) and 2 Mbps rates which is provided using differential quadrature phase shift keying (DQPSK) at the same chip rate. "In order to provide the higher rates, quadrature shift keying (QPSK) combined with 8-chip complementary code keying (CCK) is employed as the modulation scheme. The chipping rate is 11 MHz, which is the same as the DSSS system described in IEEE 802.11 standard, 1999 Edition, thus the same occupied channel bandwidth is provided." [3]

- **Direct Sequence Spread Spectrum (DSSS)**

DSSS is a modulation technique. It works by modulating a data stream of zeros and ones with a pattern called chipping sequence. In 802.11, Barker code, which is an 11 bits sequence, is used as this chipping sequence. "Baker code has certain mathematical properties to make it ideal for modulating radio waves. The basic data stream is XOR with the Barker code to generate a series of data objects called chips. Each bit is encoded by the 11bits Barker code, and each group of 11 chips encodes one bit of data." [4] Rather than using the Barker code, "IEEE 802.11b uses 64 complementary code keying (CCK) chipping sequences to achieve 11 Mbps data rate." [4] Different from one bit represented by one Barker symbol used in Barker code, up to 6 bits can be represented by any one particular code word, because there are 64 unique code words that can be used to encode the signal.

- **Binary Phase Shift Keying (BPSK)**

"BPSK is the simplest form of PSK. It uses two phases which are separated by 180° and so can also be termed 2-PSK. It does not particularly matter exactly where the constellation points are positioned, and in figure they are shown on the real axis, at 0° and 180°." [5]

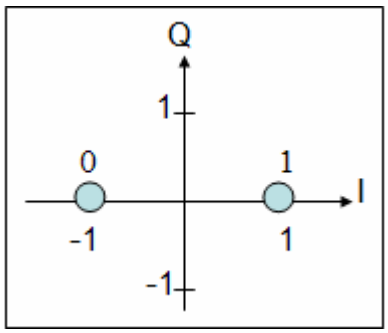

Figure 2-3: Constellation diagram for BPSK [5]

"This modulation is the most robust of all the PSKs since it takes serious distortion to make the demodulator reach an incorrect decision. It is, however, only able to modulate at 1 bit per symbol and so is unsuitable for high data rate applications when bandwidth is limited." [5]

➢ **Quadrature Phase Shift Keying (QPSK)**

"QPSK uses four points on the constellation diagram. With four phases, QPSK can encode two bits per symbol, shown in the figure below with 2 bits gray code to minimize the BER, twice the rate of BPSK." [5] That means each adjacent symbol only differs by one bit.

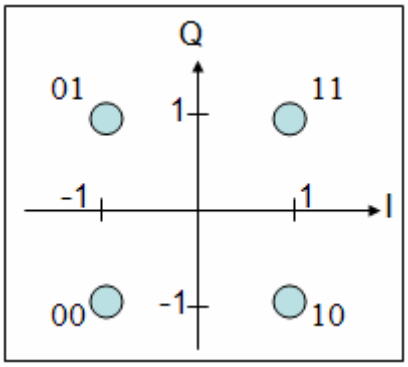

Figure 2-4: Constellation diagram for QPSK [5]

"Analysis shows that QPSK may be used either to maintain the data rate of BPSK but halve the bandwidth needed or double the data rate compared to a BPSK system while maintaining the bandwidth of the signal. Although QPSK can be viewed as a quaternary modulation, it is easier to see it as two independently modulated quadrature carriers. With this interpretation, the even (or odd) bits are used to modulate the in-phase component of the carrier, while the odd (or even) bits are used to modulate the quadrature-phase component of the carrier." [5]

➢ **Complementary Code Keying (CCK)**

"CCK is an M-ary orthogonal keying modulation where one of M unique (nearly orthogonal) signal code words is chosen for transmission. It allows for multi-channel operation in the 2.4 GHz band using the existing 802.11 DSSS channel structure scheme." [4] The same chipping rate and spectrum shape as the Barker's code word spreading functions used in 802.11 are employed in the spreading. It allows three non-overlapping channels in the 2.4 to 2.483 GHz band. "CCK uses one vector from a set of 64 complex (QPSK) vectors for the symbol and thereby modulates 6 bits (one of 64) on each 8 chips spreading code symbol. Two more bits are sent by QPSK modulating the whole code symbol. This results in modulating 8 bits onto each symbol." [4]

c) Physical Layer frame format

Two types of PPDU (PHY protocol data unit) format with different preambles and headers are defined.

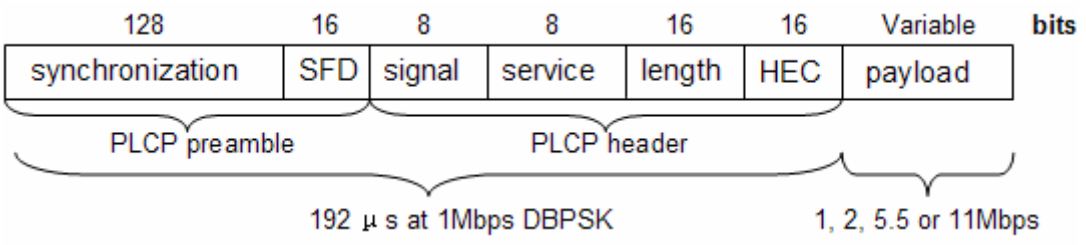

Figure 2-5: 802.11b Long PLCP PPDU format [3]

The format with long preamble is mandatory. Figure 2-5 shows that the long PPDU consists of a long PLCP (PHY convergence procedure) preamble, PLCP header and PSDU (PHY service data unit). The preamble includes a long synchronization field with 16 bytes for receiver performing necessary synchronization operations and 2 bytes SFD (start of frame delimiter) provided to indicate the start of PHY-dependent parameters within the PLCP preamble. The modulation which is used for PSDU transmission and reception is indicated by the signal field. In the one byte service field, 3 bits are defined for high rate extension. 2 bytes length field indicates the number of microseconds required to transmit the PSDU. HEC (header error check) is used for signal, service and length protection. Both preamble and header use 1Mbps Barker code spreading with DBPSK, and PSDU is transmitted at 1, 2, 5.5 or 11Mbps. [3]

The format with short preamble is defined as optional.

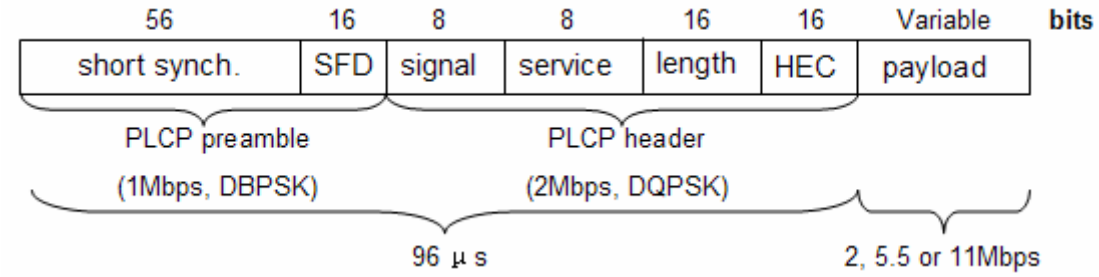

Figure 2-6: 802.11b Short PLCP PPDU format [3]

Figure 2-6 shows that the short PPDU includes a short preamble with 9 bytes, 6 bytes header and variable size of PSDU. The preamble uses 1Mbps Barker code spreading with DBPSK modulation while header uses 2Mbps Barker code spreading with DQPSK, and PSDU is transmitted at 2, 5.5 or 11Mbps. [3]

d) Access Method in Media Access Control (MAC) layer

Carrier sense multiple access with collision avoidance (CAMA/CA) is used in IEEE 802.11 standard.

- Before sending data, station starts sensing the medium, carrier sense based on clear channel assessment (CCA).
- If the media is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type).

- If the medium is busy, the station has to wait for free IFS, and then the station must additionally wait a random backoff time.
- If another station occupies the medium during the backoff time of the station, the backoff time stops (fairness).

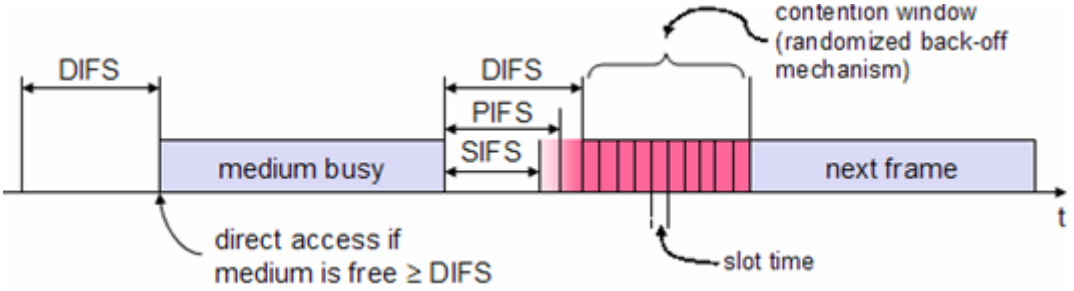

Figure 2-7: CSMA/CA mechanism [3]

- SIFS (Short Inter Frame Spacing): highest priority, for ACK, CTS (clear to send), polling response
- PIFS (PCF, Point Coordinator Function IFS): medium priority, for time-bounded service using PCF
- DIFS (DCF, Distributed Coordination Function IFS): lowest priority, for asynchronous data service

2.1.3 IEEE 802.11g

IEEE 802.11g is an amendment of the IEEE 802.11 specification that extended throughput to up to 54 Mbps using the same 2.4 GHz band as 802.11b. Extended Rate PHY (ERP) is defined in it. The channel selection and MAC layer access method used in 802.11g are the same as 802.11b. (See section 2.1.2)

a) Modulation technique

"The modulation scheme used in 802.11g is orthogonal frequency division multiplexing (OFDM) copied from 802.11a with data rates of 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s, and reverts to CCK (like the 802.11b standard) for 5.5 and 11 Mbit/s and DBPSK/DQPSK with DSSS for 1 and 2 Mbit/s. Even though 802.11g operates in the same frequency band as 802.11b, it can achieve higher data rates because of its heritage to 802.11a." [6]

In order to provide 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s payload data rates while reusing the long and short preambles described in 802.11b, the modulation technique called DSSS-OFDM was used.

b) Physical Layer frame format

Besides long preamble PPDU format (based on 802.11b), short preamble PPDU format (which is optional in 802.11b) and ERP-OFDM preamble PPDU format (based on 802.11a), ERP defined in 802.11g provides two optional PPDU formats to support the optional DSSS-OFDM modulation rates.

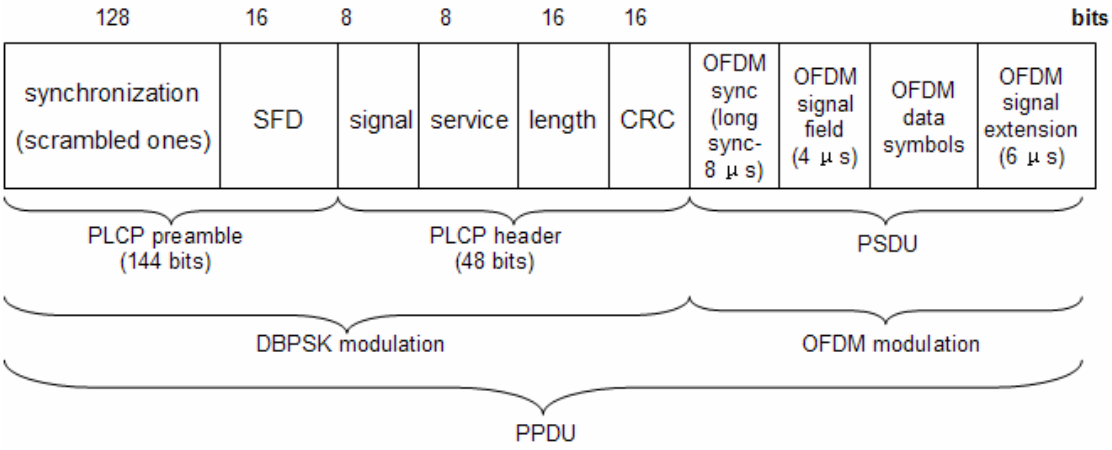

Figure 2-8: Long preamble PPDU format for DSSS-OFDM [7]

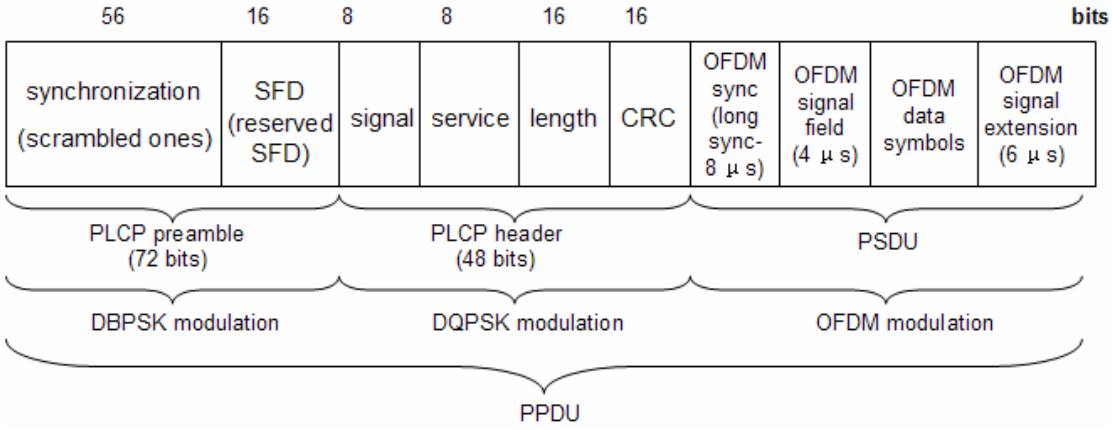

Figure 2-9: Short preamble PPDU format for DSSS-OFDM [7]

Figure 2-8 and Figure 2-9 show that the PPDU format for DSSS-OFDM is relatively unchanged according to 802.11b. The major change is the format of the PSDU. The single carrier PSDU defined in 802.11b is replaced by a PSDU which consists of OFDM synchronization, OFDM signal, OFDM data symbol and OFDM signal extension. [7]

2.2 802.15.4 Low-Rate WPAN

A wireless personal area network (WPAN), which concentrates on personal environment network solution, can be represented as a network for interconnecting personal devices by using wireless connections around an individual workspace. [8]

LR-WPANs which address wireless networking and mobile communication devices have been making effect in various fields. More or less, they have already changed our study and business modality, and will continue. For instance, PCs, PDAs, peripherals, cell phones, Bluetooth earphone, and wireless mouse exist in our daily life. For certain, more WPAN devices will be presented in the future.

WPAN is a really popular technology nowadays. It emphasizes low cost and low power consumption in transmission. While, those attractive advantages usually make a sacrifice of transmission range and rate. That is why it is also called short distance wireless networks. This is just like going an opposite way of the WLAN technologies which emphasize higher rate and longer range at the expense of cost and power.

Some IEEE standards, especially IEEE 802.15 serial standards are referenced in our study through the entire process, including theoretical analysis part, simulation part and test part. IEEE 802.15 serial standards are established by IEEE 802.15 Working Group for Personal Area Network or short distance wireless networks. Here, we introduced them respectively. [8]

- IEEE 802.15.1-2002 Standard primarily defines the lower layer transport layer (L2CAP, LMP, Baseband, and radio) of the Bluetooth wireless technology. It also has reviewed and provided a standard adaptation of the Bluetooth Specification v1.1 Foundation MAC (L2CA, PLMP, and Baseband) and PHY (Radio), and specifies other related aspects. It mainly establishes for Bluetooth device implementations.

- IEEE 802.15.2-2003 is established for coexistence analysis of Wireless Personal Area Network and Wireless Local Area Network (802.11). The IEEE802.15.2 working group developed a coexistence model to quantify the mutual interference of a WLAN and a WPAN. The working group also developed a set of Coexistence Mechanisms to facilitate coexistence of WLAN and WPAN devices. We use the BER analysis model which provided by IEEE 802.15.2, also the algorithms of BER under different transmission types.

- IEEE802.15.4

IEEE802.15.4 specifies wireless medium access control (MAC) sub layer and physical layer (PHY) specifications for low-rate wireless personal area networks. It also explores coexistence of WLAN and WPAN in its Annex.
ZigBee is built on The IEEE 802.15.4. The two lower layers: the physical (PHY) layer and the medium access control (MAC) sub layer of ZigBee stack architecture is specified in IEEE802.15.4. We will go into more details in following sections.

2.2.1 IEEE802.15.4 features [8]

- Data rates of 250 kbps, 40 kbps, and 20 kbps. Symbol rate is 62.5 ksymbol/s±ppm.
- Two addressing modes; 16-bits short (short address) and 64-bit IEEE addressing (long address)
- Optional use Star-topology or Peer to Peer topology, and also supposes Cluster Tree nowadays.
- CSMA-CA channel access
- Automatic network establishment by the coordinator
- Fully handshake protocol for transfer reliability

- Power management to ensure low power consumption
- 16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz and one channel in the 868MHz band.
- Optional to use Acknowledgement packet
- Transmit Power : About 1mW transmit power
- RSSI (Received signal strength indication) measurement

2.2.2 Type of device

IEEE 802.15.4 specifies components based on its transmission mechanism. The most basic components are devices. The LR-WPAN networks consist of devices. There are two types of device: FFD and RFD. FFD is full-function device while RFD is reduced-function device. As their names imply, a FFD has more functionalities than a RFD. Generally, FFD can operate in three modes that are serving as a personal area network (PAN) coordinator, a coordinator, or a device. FFDs take charge of main data source transmission in a network, are able to talk to any other devices. RFDs act as end device that only can associate with one FFD at one time. IEEE 802.15.4 network need at least one FFD in the network to act as a coordinator. All devices should have 64 bits extended address or use 16 bits short address that allocated by coordinator instead. Commonly, RFDs use battery power while FFDs use line power.

2.2.3 Topology

The LR-WPAN may operate in either of two topologies: star topology or peer-to-peer topology.

As Figure 2-10 shows, star topology contains devices and a PAN coordinator which acts as a central controller. The PAN coordinator initiates and terminates the network communication, it also routes communication packets. Generally, the coordinator is a FFD, which could establish a network and identify its network. Other available device, no matter FFD or RFD could join the network. Every star topology network is independently.

In star topology, end device can not communicate with each other without the coordinator. These types of networks are suitable for simple WPAN requirements. This topology, on one hand, can reduce the possibility that any end device causes the connection fail. But, on the other hand, depending on the central coordinator too much may cause the network incurable when the central coordinator collapses down. In star topology, addressing mode uses network and device identifier.

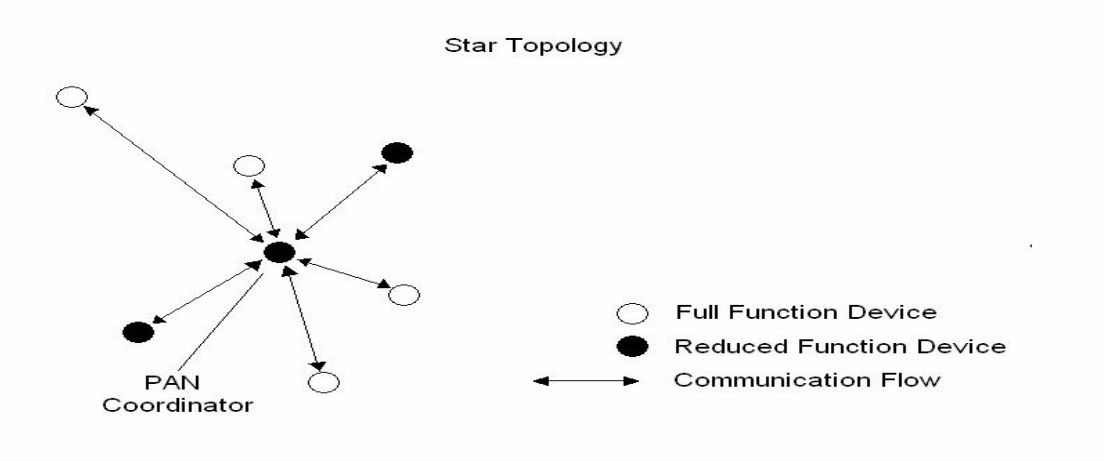

Figure 2-10: Star Topology [9]

The peer-to-peer topology is more complex, it allows end devices to communicate with each other within its radio sphere of influence. It takes use of a PAN coordinator with more network functions comparing with the coordinator in star topology. This topology makes it possible to achieve more complex mission and extend. In peer-to-peer topology, addressing mode uses source/destination identifier.

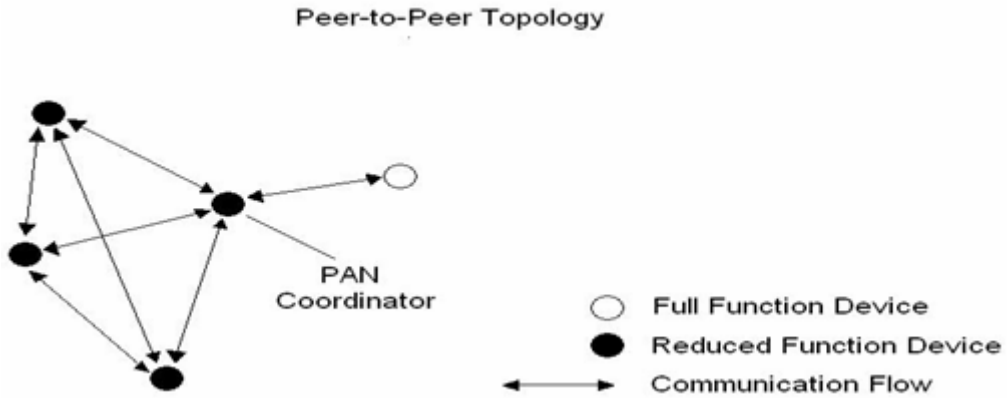

Figure 2-11: Peer-to-peer Topology [9]

2.2.4 PHY layer specification

In IEEE802.15.4, the PHY layer provides PHY data service and PHY management service interfacing to the physical layer management entity (PLME). The PHY data services enable the transmission and reception of PHY protocol data units (PPDUs) across the physical radio channel. IEEE 802.15.4 PHY layer is responsible for:

- Activation and deactivation of the radio transceiver
- Energy Detection within the current channel
- Link quality indication for received packets
- CCA for CSMA/CA
- Channel frequency selection
- Data transmission and reception

The standard specifies three license-free bands, there are: 868-868.9MHz, 902-928MHz and 2400-2483.5MHz. Different frequency bands have their specified transmission rates and modulation modes. 27 channels are available across the frequency bands, from number 0 to 26.

We focus on analysis of transmission quality over the 2450MHz frequency band since it is unlicensed ISM band, which is also utilized by WLAN transmission. 16 Channels distribute over the 2450 MHz frequency band from 2405MHz to 2480MHz, which can be obtain as:

$$Fc=2405+5(k-11) \text{ in megahertz, for } k=11, 12...26 \qquad (2.2.1)$$ [9]

Where k is the channel number

a) Spread and Modulation

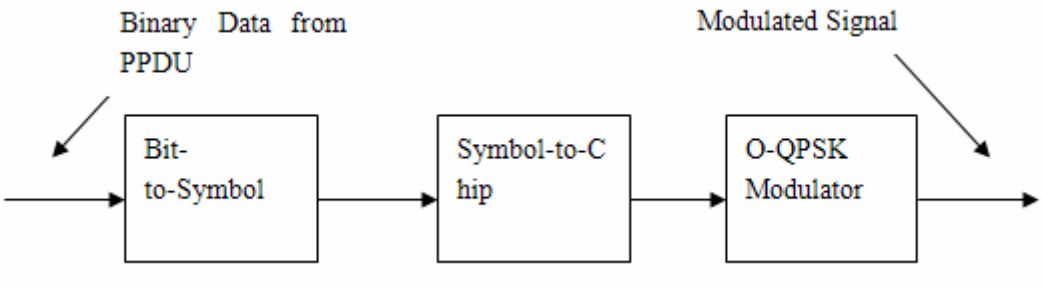

Figure 2-12: Spread and modulation functions [9]

In 2450MHz, PHY uses Direct Sequence Spread Spectrum (DSSS), and modulation type is OQPSK with 32 PN-code lengths. A RF bandwidth occupies 2MHz

➢ **DSSS used in IEEE 802.15.4**

Direct-sequence spread-spectrum is one kind of spread spectrum techniques. In short, spread spectrum technologies make signals taking up wider frequency bandwidth by using of various pseudo-random sequences. Usually speaking, purposes of spread spectrum are enhancing the signals' resistance to noise or interference, also preventing malicious detection. At receiver, same pseudo-random sequence shall be used for de-spread.

In this scenario, the DSSS processes employ PN sequences to represent each symbol. All bytes contained in the PPDU were split into 4 LSBs and 4 MSBs, each of them shall map into one data symbol. There are 4^2 symbols as show in following table:0000,1000,0100,1100,0010,1010,0110,1110,0001,1001,0101,1101,0011,1011,0111,1111. Each data symbol shall be mapped into a 32-chip PN sequence (C_0, C_1 …C_{30}, C_{31}) as specified.

In de-spread process, the 32-chip PN shall map back to 4 LSBs or MSBs. Logically, it is possible that those spreaded signals could not find exactly same chip used to map back since they were transmitted under noise and interference. There are some prescribe of receiver sensitivity, but this paper did not come into that part.

Data symbol (decimal)	Data symbol (binary) (b_0,b_1,b_2,b_3)	Chip values ($c_0c_1...c_{30}c_{31}$)
0	0 0 0 0	1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0 1 1 1 0
1	1 0 0 0	1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 1 0
2	0 1 0 0	0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0
3	1 1 0 0	0 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1
4	0 0 1 0	0 1 0 1 0 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0 0 0 1 1
5	1 0 1 0	0 0 1 1 0 1 0 1 0 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1 1 1 0 0
6	0 1 1 0	1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0 1
7	1 1 1 0	1 0 0 1 1 1 0 0 0 0 1 1 0 1 0 1 0 0 1 0 0 0 0 1 0 1 1 1 0 1 1 0 1
8	0 0 0 1	1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1
9	1 0 0 1	1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1
10	0 1 0 1	0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1
11	1 1 0 1	0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0
12	0 0 1 1	0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1 0 1 1 0
13	1 0 1 1	0 1 1 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0 1 0 0 1
14	0 1 1 1	1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0 1 1 0 0
15	1 1 1 1	1 1 0 0 1 0 0 1 0 1 1 0 0 0 0 0 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 0 0

Table 2-3: Symbol-to-chip mapping in DSSS [9]

- **OQPSK**

OQPSK is offset quadrature phase-shift keying modulation scheme. It divides signal into two portions which are in-phase (I) and quadrature-phase (Q). Q-phase chips shall be shifted by half symbol duration with respect to I-phase chips. There is no phase shifts by 180° compared with QPSK. [10]

The following figure illustrates that the chip sequences representing each data symbol which we describe in DSSS scenario are modulated onto the carrier using OQPSK with half sine pulse shaping. Even-indexed chips are modulated onto the in-phase (I) carrier and odd-indexed chips are modulated onto the quadrature-phase (Q).

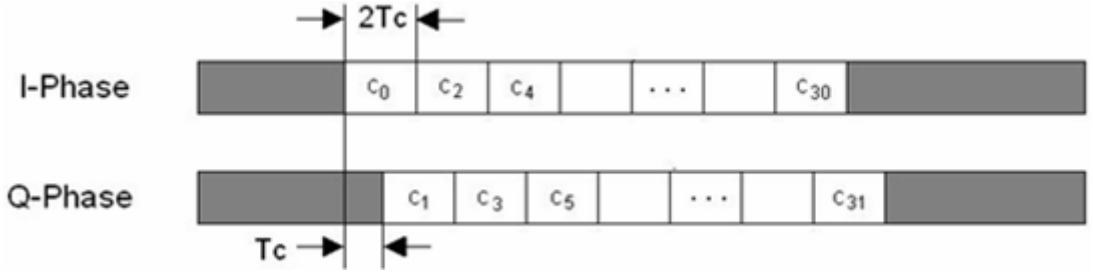

Figure 2-13: OQPSK chip offset [9]

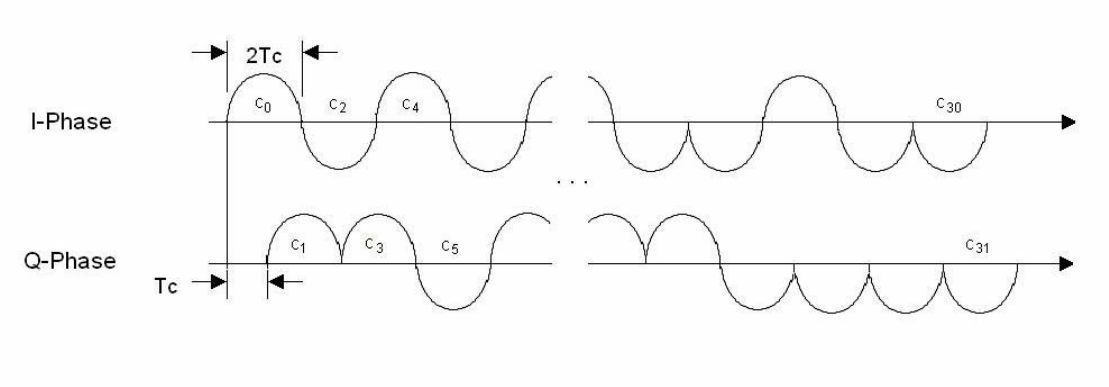

Figure 2-14: Sample baseband chip sequences with shaping [9]

b) PPDU frame format

Usually, PPDU format is used to specify transmission data packets over PHY layer. The PPDU structure can be illustrated as following figure:

Octets:4	**1**	**1**		**variable**
Preamble	SFD	Frame length (7 bites)	Reserved (1 bit)	PSDU
SHR		PHR		PHY payload

Figure 2-15: 802.15.4 PPDU format [9]

Where, the synchronization header (SHR) includes Preamble (32 bits) and Start of Frame Delimiter (8 bits). The PHY header (PHR) has 8bits that first 7bits indicate length of PSDU and reserved 1 bit indicates whether the packet is received. Payload is data field from 0 to 127 bytes.

c) Clear Channel Assessment (CCA) [9]

CCA is an algorithm used to judge whether a channel is busy or idle by detection of the channel energy. IEEE 802.15.4 PHY layer offers three modes of CCA algorithm:

Mode1: define an energy threshold, if energy of the channel is above the threshold, the channel is judged as busy, otherwise it is idle.

Mode2: use carrier sense. The channel is judged as busy when a signal with modulation and spreading characteristics of IEEE802.15.4 are detected.

Mode3: use the carrier sense when detected energy above threshold. Report the channel is busy when a signal with the modulation and spread characteristics of IEEE802.15.4 detected while with the channel energy above the ED threshold.

2.2.5 MAC specification

MAC sublayer handles all access to the physical radio channel and is responsible for:

- Provide a reliable link between two peer MAC entities
- Coordinator generates network beacons
- Support PAN association and disassociation
- Employ CSMA/CA mechanism for channel access
- Handing and maintain guaranteed time slot mechanism

a) Superframe structure

Superframe structure is used for channel bonding, but not limited to. (More information can be found in IEEE 802.22 [11]). It is defined and sent by coordinator in WPAN and can optionally bond its channel.

If a WPAN does not wish to use the superframe structure, coordinator of this network shall not transmit beacons; all transmission shall use an un-slotted CSMA-CA mechanism to access the channel. [12]

A WPAN which is beacons-enabled wishes to use the superframe structure. The superframe is sent bounded by network beacon frame. It is divided into 16 equally sized slots as the following Figure 2-16 shows:

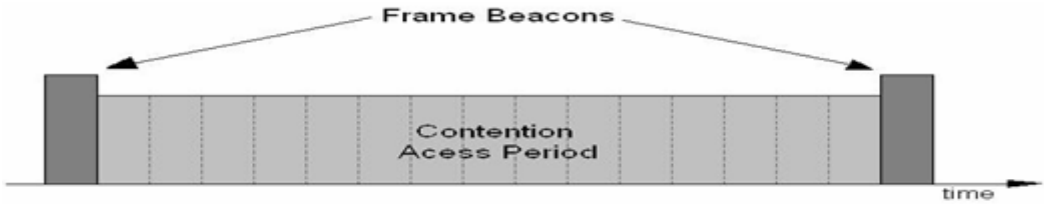

Figure 2-16: Superframe is send bounded by network beacon frame [9]

In IEEE 802.15.4 takes more specification on this point that "For low-latency applications or applications requiring specific data bandwidth, the PAN coordinator may dedicate portions of the active superframe to that application. These portions are called guaranteed time slots (GTSs)." [9] In short, GTSs provide a specific duration of time for the superframe without contention or latency.

Figure 2-17: Superframe with GTSs [9]

GTSs are set in Contention Free Period (CFP), continually following the end slot of Contention Access Period (CAP). A device transmitting in GTSs shall ensure that the transmissions completed before next GTS or end of this CFP. A WPAN coordinator may allocate up to 7 GTSs which means 7 devices as maximum could use GTS in one

network. As coordinator, it must keep record of: starting slot, length of superframe slot, direction and associated device address. As the device associated with GTS must keep record of: starting slot, length of slot, direction. The data frames which use GTS should use short address (16 bits) for transmission.

b) Transmission mechanisms

IEEE802.15.4 specifies three types of data transactions: a device transfer data to a coordinator, a coordinator transfer data to a device, and data transfer between two peer devices. All of these three transmission mechanisms can be used in peer-to-peer topology. Start topology is limited to provide the third one since it does not support communication between two peer devices.

➢ **Data transfer to a coordinator from a device**

In non beacon-enabled network, if a device wishes to send data, it simply send data frame using un-slotted CSMA-CA to coordinator of the network. As shows in Figure 2-18, the coordinator responds with an optional acknowledgment frame.

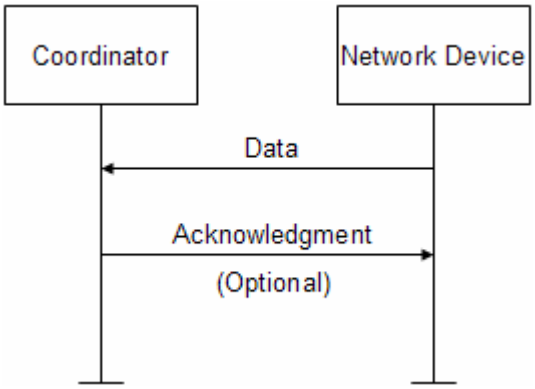

Figure 2-18: Communication to a coordinator in a nonbeacon-enabled network [9]

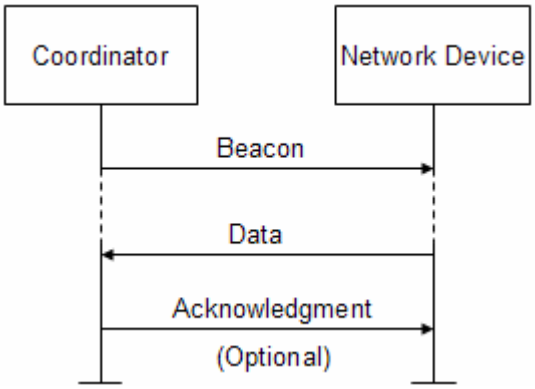

Figure 2-19: Communication to a coordinator in a beacon-enabled network [9]

In a beacon-enable network, when a device wishes to send data to the coordinator, it synchronizes to the superframe structure after it found the network beacon. Then it sends its data to the coordinator by using slotted CSMA-CA. The coordinator responds an optional acknowledgment frame. This sequence is illustrated in Figure 2-19.

➢ **Data transfer from a coordinator**

When a coordinator wishes to send data to a device in a non-enabled network, firstly the device sends *request the data* which stores in the coordinator. Since the coordinator stores the date for different devices, a device may use a MAC command *request the data* by using un-slotted CSMA-CA to the coordinator at an application-defined rate. If the data is pending, the coordinator use un-slotted CSMA-CA to send the date frames. Otherwise, if the data is not pending, the coordinator sends the data with a zero-length payload to denote that. Then the

coordinator responds with an acknowledgment frame and sends data frame sequentially. The coordinator sends out an acknowledgment frame when it finishes the data frame reception. This sequence illustrates as Figure 2-20.

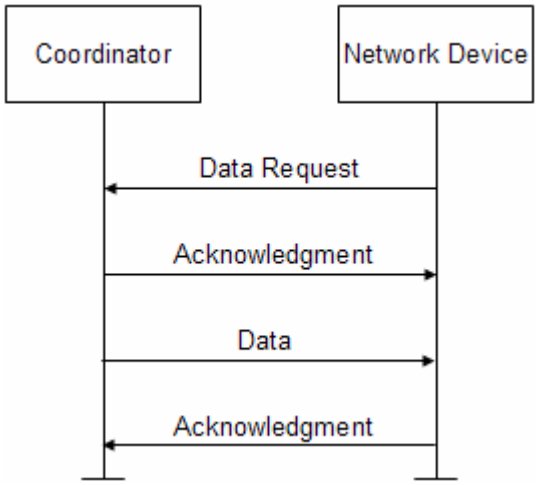

Figure 2-20: Communication from a coordinator in a nonbeacon-enabled network [9]

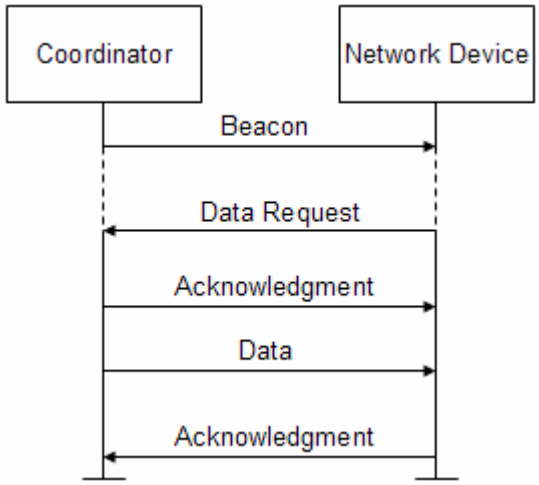

Figure 2-21: Communication from a coordinator in a beacon-enabled network [9]

In a beacon-enabled network, when a coordinator wishes to send date to a device, it first combines network beacon with the pending data message. The device may listen to this beacon and send a MAC command *request the data* using CSMA-CA. After the coordinator gets this request, it sends out an acknowledgment and the data will be sent sequentially by using CSMA-CA. When the data transmission finish, the device sends out an acknowledgment frame. At this time, the message which indicates the pending data is removed from the pending message list. This sequence is summarized in Figure 2-21.

c) MAC layer Frame format [9]

Four MAC frame formats are defined in IEEE 802.15.4. There are beacon, MAC command, data and acknowledgement frame.

Beacon frame has *7 + (4 or 10) + k + m + n* as MAC sublayer frame, and totally has *13+ (4 or 10) + k + m + n* bytes as PPDU in PHY layer. Where, *k* is GTS fields value, *m* is pending address fields and *n* is Beacon payload.

MAC command frame has *6 + (4 or 20) + n* as MAC sublayer frame, and totally has *12 + (4 to 20) + n* bytes as PPDU. *n* is command payload.

Data frame has *5+ (4 to 20) +n* as MAC sublayer frame and totally has *11+ (4 to 20) +n* as PPDU in PHY layer. 4 to 20 are address information. *n* is data payload.

Acknowledgement frame has 5 bytes as MAC sublayer frame and totally has 11 bytes as PPDU in PHY layer.

2.3 ZigBee

2.3.1 Overview

ZigBee networks began in consideration in 1998, people realized that besides those high data rate required network, there are many wireless networks require low latency and low energy consumption but not high data rate, such as control or sensor network. The ZigBee 1.0 specification was released on December 14, 2004, to appease those requirements.

The ZigBee network is actually a standard specified by two organizations that are IEEE 802.15 WPAN task group 4 and ZigBee Alliance. IEEE 802.15.4, which was established in May 2003, scopes on definition of physical layer (PHY) and media access control (MAC). ZigBee Alliance defined application support sub-layer (APS), ZigBee device object (ZDO), ZigBee device profile (ZDP), application framework, network layer (NWK) and ZigBee security services. ZigBee Alliance also publishes application profiles.

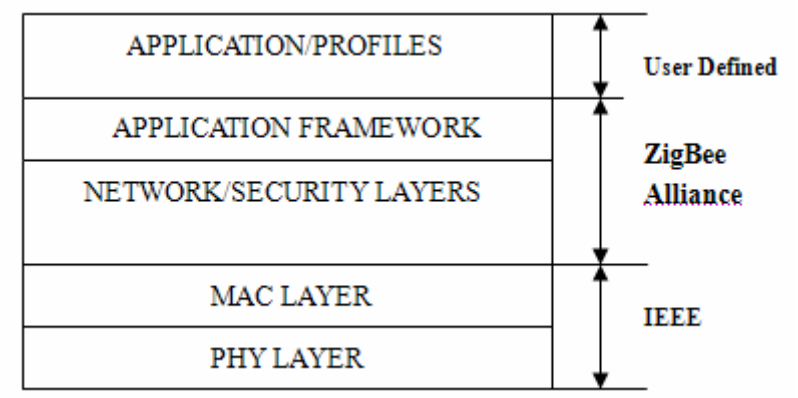

Figure 2-22: ZigBee Layers [13]

The IEEE 802.15.4 PHY and MAC along with ZigBee network and application support layer provide low cost, low power consumption, short range operation, easy to implement and have appropriate level of security communication approach.

ZigBee are typically used for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation, home automation, etc. [14]

2.3.2 Architecture

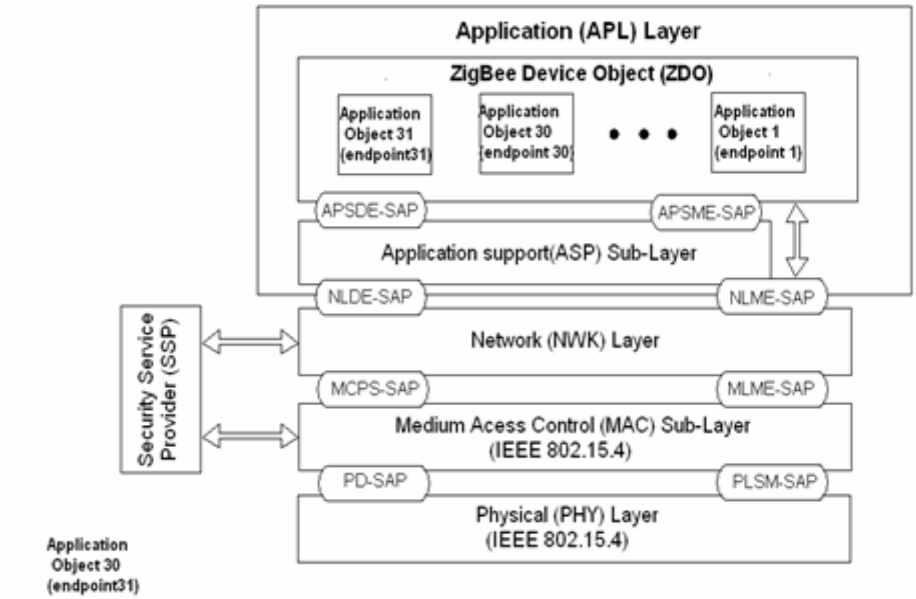

Figure 2-23: ZigBee stack [15]

The ZigBee stack is illustrated as Figure 2-23 shows, the PHY and MAC layer are specified in IEEE 802.15.4 standard as previous section introduced. The ZigBee Alliance builds on this foundation, providing network (NWK) layer and the framework for application layer standards, which includes the application support sub-layer (APS)，the ZigBee device objects (ZDO) and the manufacturer-defined application objects.

a) Network layer

"The network layer builds upon the IEEE 802.15.4 MAC's features to allow extensibility of coverage. Additional cluster can be added; networks can be consolidated or split up." [15]

The ZigBee NWK layer mainly takes charge of:

- Establish a new network
- Joining and leaving a network
- Configure the stack for operation when a new device joins the network
- Assign address to device which is joining the network, this operation is carried by coordinator.
- Routing frame to their destinations
- Enable a device to synchronization with another device either through tracking beacons or by polling
- Applying security operations

b) Application layer

The application layer consists of APS sub-layer and ZDO. It logically includes manufacturer-defined applications, which can be hardware or software.

APS sub-layer provides discovery and binding services. Discovery is used for detecting of devices which are working in range of a device. Binding is used to match two or more devices together and forward messages between bound devices.

Responsibilities of the ZDO are: defining role of devices in the network, initiating and/or responding to binding requests and establishing a secure relationship between network devices.

2.3.3 ZigBee network

ZigBee network support three network topologies, they are star topology, peer-to-peer topology and cluster tree topology. Figure 2-24 shows those three topologies.

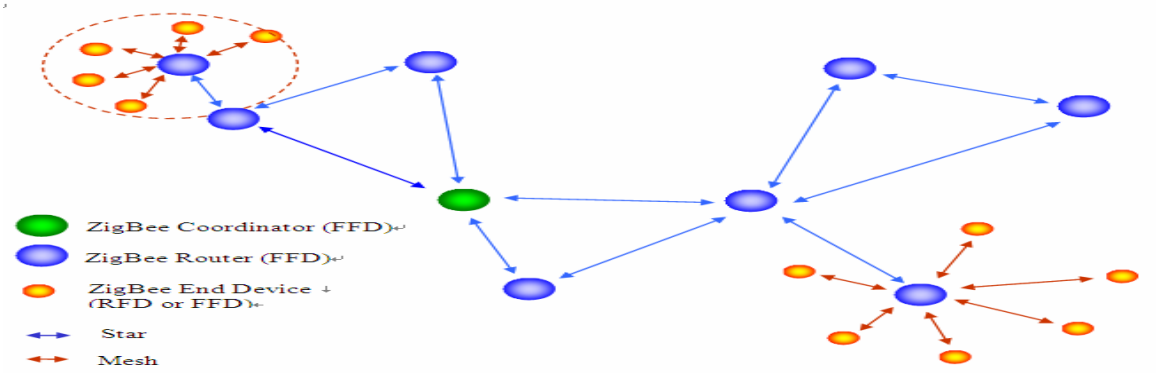

Figure 2-24: ZigBee network Model [15]

As introduced in previous section, star network is suitable for simple requirement with low power consumption. Peer-to-peer network has capability of high level reliability and provides various paths in the network. Cluster tree topology actually just utilizes a hybrid star and peer-to-peer topology, benefits both for high level of reliability and support for battery power nodes. [13]

2.4 2.4GHz ISM band interference issue

ISM bands are originally reserved internationally for the use of RF electromagnetic fields for industrial, scientific and medical purposes other than communications. ISM bands are frequency bands in the radio spectrum that are unlicensed, meaning they can be used for a variety of applications without the requirement for FCC permission. The bands are used traditionally for in-building and system applications such as bar code scanners and wireless LANs. Because there is no licensing requirement, there exists the potential interference. [16]

An RF band with over 80MHz width in the 2.4GHz range was made available for industrial, scientific and medical applications several decades ago. Corresponding to its initial use, this band is usually referred to as an “ISM” band. While originally utilized by device such as commercial microwave ovens and industrial heaters, the band was later opened for license-exempt data communications. By way of nearly global availability, relatively wide range, and the fact that it has the lowest frequency among comparable bands, 2.4GHz has become the logical choice for the deployment of wireless LAN solutions. [17]

The IEEE802.11 series of standards clearly dominates this space and is universally accepted. Also, with new revisions of the standard such as IEEE802.11n, the vast majority of WLAN device can expect to continue to operate in the 2.4GHz band. In comparison with the alternative band in the 5GHz range, the use of the 2.4GHz band provides important advantages in terms of range and coverage indoor environments. [17]

For similar reasons, the 2.4GHz band was also chosen for the solutions for WPANs such as IEEE 802.15, Bluetooth and ZigBee. Coexistence of standards like WLAN, Bluetooth and ZigBee is a critical issue that draws many attentions, and coexistence analysis is essential problem of this thesis.

2.5 Limitation

The aim of the thesis is to analyze the interference WLAN brings to ZigBee. In other words, we want to evaluate the performance of ZigBee under the WLAN interference. There are a lot of parameters can be chosen to achieve our aim, such as packet error rate, throughput, range and so on. But we just put the major concern on the packet error rate due to the limitation of time.

And in the beginning, we suppose to consider about ZigBee performance under IEEE 802.11b and IEEE 802.11g WLAN interference, respectively. In order to evaluate the bit error rate of ZigBee under WLAN interference, the in-band interference WLAN causes to ZigBee should be calculated. Since the in-band interference is determined by the power spectrum density of WLAN with a parameter called in-band interference power ratio, which is related to frequency offset. So how to obtain the in-band interference ratio is the key point. However, we only obtained the in-band interference ratio of IEEE 802.11b from one reference paper, and lack of method to measure the in-band interference ratio of IEEE 802.11g, so in the simulation part of this thesis, we just evaluate the packet error rate of ZigBee under IEEE 802.11b WLAN interference.

In order to simplify the transmission, we ignore WLAN acknowledgement packet and only consider about the ZigBee data, ACK packets and WLAN data packets when building the time collision scenarios.

3 Interference analysis of ZigBee under WLAN

3.1 Literature review

Coexistence in unlicensed frequency bands is not a new problem in radio communication field. Many studies have done various works to explore the coexistence with different motivations.

IEEE standard 802.15.2[18] specifies the coexistence of wireless personal area networks (WPAN) with other wireless devices which operating in unlicensed frequency bands. It introduced coexistence mechanisms that are recommended use to facilitate coexistence of wireless local area network (WLAN) and WPAN.

IEEE 802.15.4[9] Annex E introduces BER of ZigBee network transmission based on its modulation type, spread and de-spread mechanism. And build a propagation model to estimate the PER. This is the most typical way to analyze interference from WLAN to WPAN and vice versa, many afterwards studies are based on this method.

[17] references the introduction in IEEE 802.15.4, and use four IEEE 802.15.4 devices with power amplifiers test these devices performance under WLAN interference. The test selects three IEEE802.15.4 channels for ZigBee transmission with 2MHz, 13MHz and 23MHz offsets from WLAN centre frequency, this means they are in, close to and away from the WLAN channel (North American standard).

[19] is proposed by ZigBee Alliance. In this paper, many real ZigBee products are referenced as examples that explain ZigBee devices can performance well in realistic environment with real data traffic coexist. In the paper, 802.11b/g,Bluetooth,2.4GHz frequency hopping spread spectrum portable phones and numerous proprietary wireless technologies are working in one environment are specified as a realistic environment.

[20] explores mutual interference of IEEE802.15.4 and IEEE 802.11b, evaluates their performance under each others interference. The performance evaluation includes PER, transmission delay, and throughput. This paper constructs network with fixed desired sender and receiver, by change amount of interfering sender and receiver, in order to achieve different volumes of interference strength.

Besides the references we mentioned before, as a well known WPAN device, Bluetooth is also a typical study object under this topic. Researches on the interference problem of Bluetooth also provide us good references.

[21] describes a study on PER analysis of ZigBee under WLAN and Bluetooth interferences. An analytic model for the coexistence among ZigBee, WLAN and Bluetooth is built to evaluate the performance of IEEE 802.15.4 ZigBee respectively under the interference of IEEE 802.11b WLAN, Bluetooth or both.

[22] presents a research about the interference in the 2.4GHz ISM band impact the Bluetooth access control performance. A probability approach is used to obtain the PER for Bluetooth. An interference model is presented first and then validated by a simulation model which is developed with the network simulation tools OPNET.

3.2 Overview

The interference issue of 2.4GHz ISM band is introduced in section 2.5. Analyzing the interference between IEEE802.15.4 and 802.11b/g, and coexistence of them is the main task of this thesis. We primarily focus our work on WLAN as the interference impacts the ZigBee network communication.

WLAN and ZigBee will impact each other because both of them utilize the 2.4GHz ISM band. As in previous chapter mentioned, the IEEE 802.15.4 standard defines 16 channels that are 5MHz apart from each other; bandwidth of each channel is 2MHz, while IEEE 802.11b standard of WLAN defines14 channels within the 2.4GHz band, with 5MHz distance between two adjacent channels. Since the WLAN radio signal has bandwidth of 22MHz, not all channels can be used at the same time. In fact, only three non-overlapping WLAN channels can be used concurrently. For North America, there are channels1, 6 and 11 and for European, there are channels 1, 7 and 13. [17] The following Figure 3-1 illustrates the channel selection for IEEE 802.11b and IEEE 802.15.4, and the overlapping channel between them.

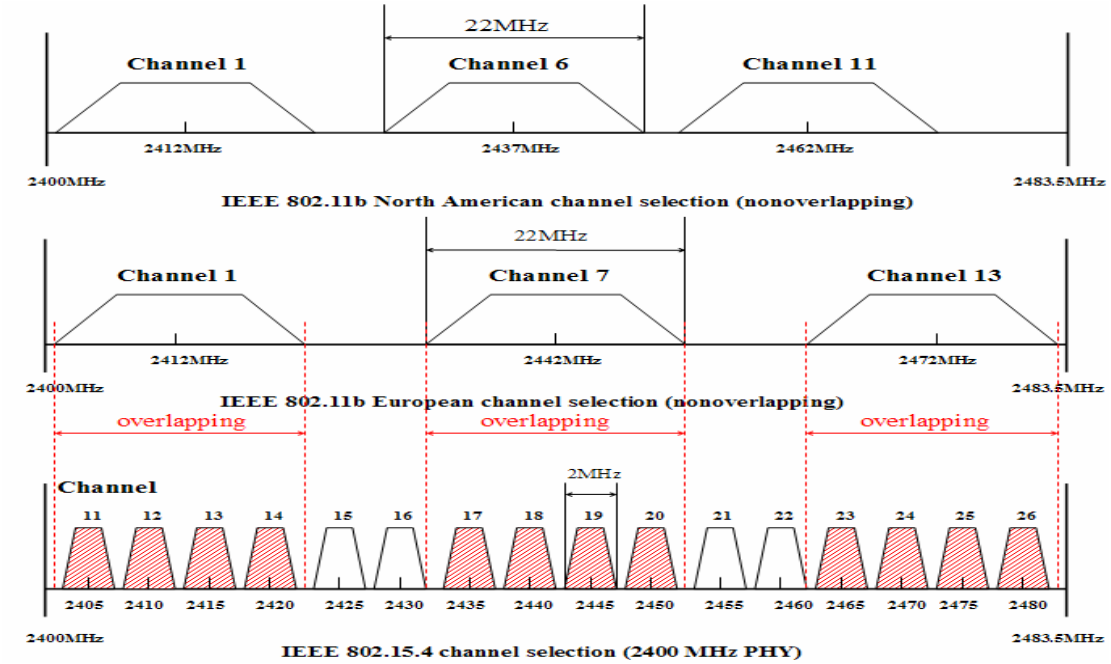

Figure 3-1: Channels of WLAN and ZigBee in 2.4GHz band [9]

There are several ways we could evaluate the impact that WLAN brings to ZigBee network in coexistence environment, such as packet error rate (PER), throughput, transmission range and so on. In this thesis, we analyze the impact according to PER of ZigBee network transmission under WLAN interference.

The PER could be estimated based on bit error rate (BER) and packets collision time. In the following sections, we will introduce BER evaluation and collision time models simulation.

3.3 Bit error rate analysis of ZigBee (802.15.4) under WLAN (802.11b)

Generally speaking, PHY layer transmissions are considered as stationary processes. [18]. By this means, once we define a PHY layer transmission, the transmitter power, modulation type and the position of the device are defined as constants at the same time.

Summarily, there are three primary scenarios need to take in mind when we define a transmission, since they are significant aspects for evaluating PHY layer transmission quality.

1. The generation in which we define modulation, de-modulation type and spread spectrum, de-spread spectrum if any.
2. The propagation of corresponding radio wave through environment in transmission
3. The receiver estimates the transmitted information from the recovered electrical signals.

During the period of stationary, receiver obtains constant signal, noise and interference powers from which BER can be calculated. This also makes it possible to configure those constants corresponding to the requirement for desired network simulation.

3.3.1 BER analysis

PYH layer transmission quality is usually evaluated in terms of BER. There are some important concepts should be indicated before we come to BER.

- **Path loss** [23]

In this thesis, an indoor line-of-sight (LOS) model for signal propagation environment is proposed. Line-of-sight (also named free-apace) model are built in order to simplify transmission path loss between transmitter and receiver.

In the transmission process, propagation condition of radio waves is a significant factor by which we can evaluate performance of transmission signal at receiver. This performance is measured as signal strength; we therefore come to electrical field to explore this issue. For making clear, we start from the concept of isotropic radiation, which is an antenna that transmits equally in all directions, but does not exist in real world. An isotropic source radiates power P watts equally in all directions. Signals are sent spherically from centre source. Every receiver could gain the signal power as:

$$P_r = \frac{P_t}{(4\pi R/\lambda)^2} = \frac{P_t}{L_p} \qquad (3.3.1)$$

Where λ is the wavelength of radiation, R is radius from the signal source to the receiver.

P_r: receiver power
P_t: transmitter power
L_p: line-of-sight path loss between two isotropic antennas.

$$L_p = (\frac{4\pi R}{\lambda})^2 \qquad (3.3.2)$$

In equation (3.3.2), *R* is distance from transmitter to receiver.
The definition discloses that the path loss depends on the wavelength (λ) of transmission.

When non-isotropic antennas are used, the line-of-sight relating received (P_r) and transmitter power (P_t) for general can be obtained as:

$$P_r = \frac{P_t G_t G_r}{L_p} \qquad (3.3.3)$$

G_t: transmit gain
G_r: receive gain
Usually, we use decibel relation to simplify the evaluation:

$$P_r\,(dB) = P_t\,(dB) + G_r\,(dB) + G_t\,(dB) - L_p\,(dB) \qquad (3.3.4)$$

- **Indoor propagation** [23]

In indoor environment, wall attenuation, open-area loss need be taken into consideration for path loss:

$$L_p(dB) = \beta(dB) + 10\log_{10}(\frac{r}{r_0})^n + \sum_{p=1}^{P} WAF(p) + \sum_{q=1}^{Q} FAF(q) \qquad (3.3.5)$$

Where, *r* is distance separating the transmitter from the receiver, r_0 is nominal reference distance，*n* is the path-loss exponent, *WAF(p)* is the wall attenuation factor, *FAF(q)* is the floor attenuation factor, and *P, Q* are number of walls and floors respectively within the transmitter and the receiver.
In this thesis, we simplified the indoor propagation model as below [24]:

$$L_p(d) = \begin{cases} 20\log_{10}(\frac{4\pi d}{\lambda}) & , d \le d_o \\ 20\log_{10}(\frac{4\pi d}{\lambda}) + 10n\log_{10}\frac{d}{d_o} & , d > d_o \end{cases} \qquad (3.3.6)$$

Where, *d* is the distance from transmitter to receiver
$\lambda = c/f$: *c* and *f* stand for light velocity and carrier frequency.
d_0: length of line-of-sight (LOS)
n: path-loss exponent

And the received power: [24]:

$$P_r = P_t \times 10^{-\frac{L_p(d)}{10}} \tag{3.3.7}$$

This is the way to obtain power at receiver when transmitter power is fixed and propagation distance is proposed. We have to point out that signal powers, as the name implies, represents of signal strength which is usually used to compare with noise or interference power when they are in one channel. We will explain more about this afterwards.

As we introduced at the beginning of this chapter, the transmission can be characterized by the generation, path-loss, and the receiver recover ability.
Since the WLAN and ZigBee network are standardized by IEEE, the parameters like the modulation type, the transmitter power are defined or fixed in IEEE standards.

As we know, the modulation method that ZigBee (IEEE 802.15.4) adopts is OQPSK. The following formula is introduced to obtain BER of OQPSK modulation in the Additive White Gaussian Noise (AWGN) channel. [20]

$$b = Q\left(\sqrt{\frac{2\gamma E_b}{N_o}}\right) \tag{3.3.8}$$

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp\left(-\frac{u^2}{2}\right) du \tag{3.3.9}$$

Where, $\gamma = 0.85$ [21]
b: BER in AWGN channel (In other words, *b* stands for BER of ZigBee network without WLAN interference)
E_b: transmitted energy per bit
N_0: one-sided power spectral density of channel noise
Q(x): *Q* function, it is defined as the area under the tail of the Gaussian probability density function with zero mean and unit variance. [18]

- **SNR**

Signal-to-noise ratio is a power ratio between signal and noise within signal bandwidth. Usually, signal power is obtained as receiver power that is decided by transmitter power and propagation condition of the signal. Noise power rests with the signal transmission bandwidth and the noise power spectrum density (PSD) feature.

In this thesis, we firstly assume that all transmissions are happened within an Additive White Gaussian Noise (AWGN) channel. The AWGN noise channel model contains linear addition wideband and white noise with a constant spectral density. AWGN noise channel model simplify complex noise channel to some extent, since it does not involve the fading, interference, nonlinear or dispersion etc. The SNR in the AWGN channel can be expressed as:

$$SNR = \frac{P_{rz}}{N_0 B} \tag{3.3.10}$$

N_0: noise spectral density
P_{rz}: ZigBee signal power at receiver
B：Channel bandwidth
The noise power P with a bandwidth B is:

$$P = (N_0 / 2)(2B) = N_0 B \tag{3.3.11}$$

P is a constant when N_0, B is given.

So the SNR in AWGN channel can be represent as:

$$SNR = \frac{P_{signal}}{P_{noise}} = \frac{P_{rz}}{P} \tag{3.3.12}$$

$$SNR(dB) = 10\log_{10}(\frac{P_{signal}}{P_{noise}}) = 10\log_{10}(\frac{P_{rz}}{P}) \tag{3.3.13}$$

As we introduced in previous section, we assume the ZigBee signal is in an indoor propagation environment. It is feasible to use the path-loss formula (3.3.6) and (3.3.7) to obtain ZigBee signal power P_{rz} at receiver node with the given ZigBee transmitter power P_{tz}. Then the SNR of ZigBee transmission under AWGN can be evaluated.

Sequentially, the BER of ZigBee transmission under AWGN is obtained by replacing the E_b/N_0 (in equation 3.3.8) which is a ratio of energy ratio per information bit to noise indeed with SNR.

$$b = Q(\sqrt{2\gamma\ SNR}) \tag{3.3.14}$$

Where, b stands for BER without WLAN interference.

- **SINR**

When we consider the interference is involved in transmission channel, we use signal-to-interference-plus-noise (SINR) to measure it.

$$SINR = \frac{P_{signal}}{P_{noise} + P_{interference}} = \frac{P_{rz}}{P + P_{ri}} \tag{3.3.15}$$

$$SINR(dB) = 10\log_{10}(\frac{P_{signal}}{P_{noise} + P_{interference}}) = 10\log_{10}(\frac{P_{rz}}{P + P_{ri}}) \tag{3.3.16}$$

Where, P_{rz}, P_{signal} are signal power that receiver gains; P_{ri}, $P_{interference}$ are interference power that receiver gains, and P is noise power.

Actually, since the bandwidth of a WLAN channel is 22MHz, which is much larger than that of a ZigBee channel (2MHz), the interference of WLAN (IEEE 802.11b) could be modeled as AWGN to ZigBee (IEEE 802.15.4) signal after the signal power of 802.11b to 802.15.4 was determined. [20] In this way, the BER of ZigBee network under WLAN interference can be obtained by using SINR instead of SNR in equation (3.3.14).

$$b_i = Q\left(\sqrt{2\gamma\, SINR}\right) \qquad (3.3.17)$$

Where, b_i is BER under WLAN interference.

To make it precise, we explore power spectrum density over their channel frequency, to see how much WLAN interference power the ZigBee receiver gains.

The PSD of WLAN (IEEE 802.11b) is not uniformly distributed across 22MHz. Here, Figure 3-2 illustrates IEEE 802.11b PSD around its centre frequency. [20]

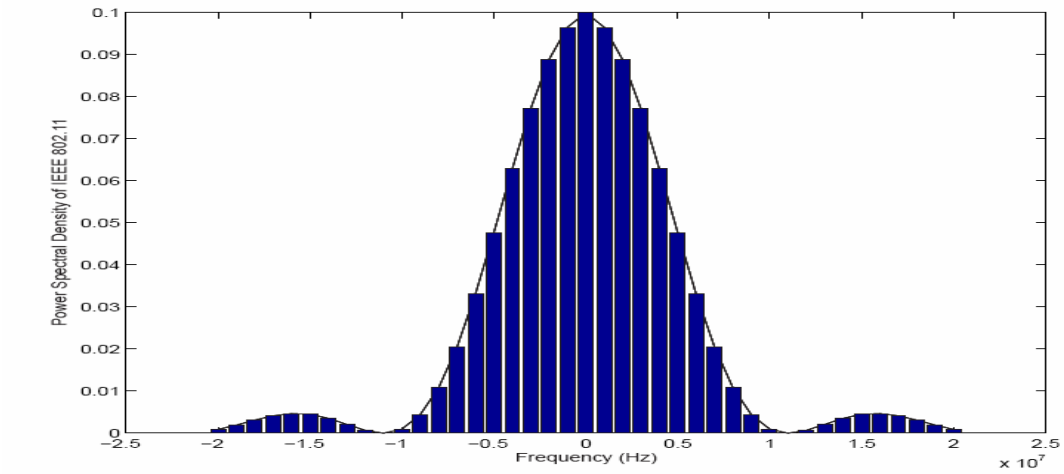

Figure 3-2: Power Spectral Density of the IEEE 802.11b [20]

Table 3-1 shows different in-band power ratio values according to different frequency offsets from the centre frequency.

Frequency offset (MHz)	Ratio
0	0.18995
1	0.18417
2	0.16946
3	0.14761
4	0.12085
5	0.092248
6	0.064803
7	0.040997
8	0.022485
9	0.009931
10	0.003047

Table 3-1: In-Band power ratio [24]

Figure 3-3 illustrates that different offsets from ZigBee (802.15.4) channel centre frequencies to a WLAN (802.11b) channel centre frequency. The 802.15.4 channels: 2405MHz, 2410MHz, 2415MHz, 2420MHz hold 7MHz, 2MHz, 3MHz and 8MHz offsets from the 802.11b first non-overlapping channel 2412MHz. [9]

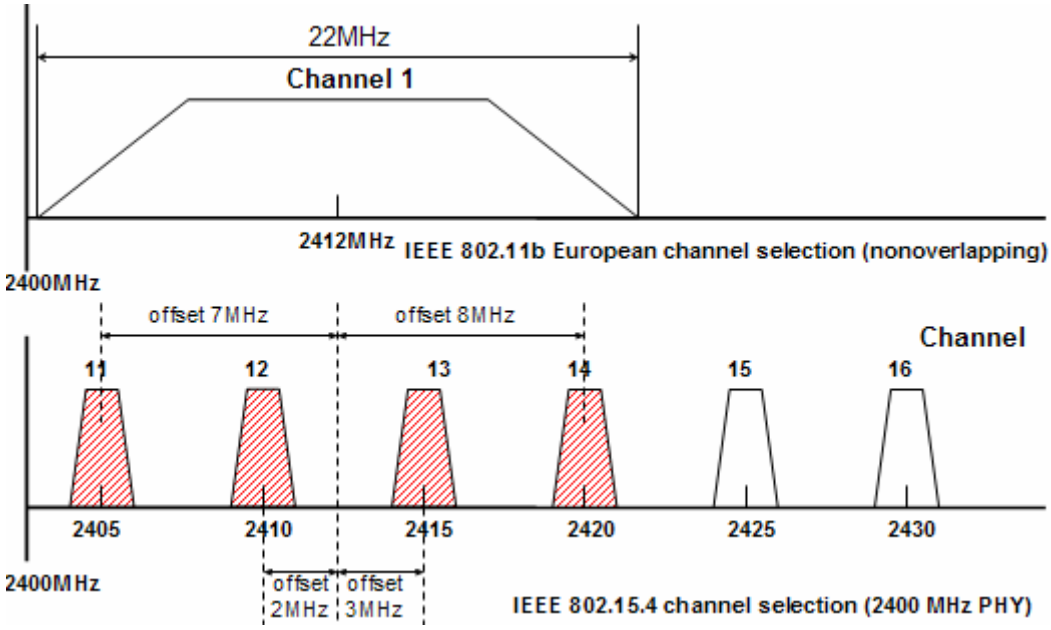

Figure 3-3: Frequency offsets between WLAN and ZigBee channel

As a result, the WLAN interference power at ZigBee receiver P_{ri} can be obtained as:

$$P_{ri} = P_{ti} \times 10^{-\frac{L_p(d)}{10}} \times Ratio \qquad (3.3.18)$$

It is easy to calculate P_{ri} by using the equation (3.3.6) and (3.3.18). Sequentially, the SINR and BER of ZigBee under WLAN interference can be calculated following equations 3.3.16 and 3.3.17.

3.3.2 Simulation

According to our analysis, BER lies on powers of noise and interference within the overlapping channel. We build our simulation work under an assumption that all transmissions are in an indoor environment, where they obey the indoor propagation rules.

Matlab is selected to carry out our simulation work. We use both coding (.M file) and Simulink to simulate the 802.15.4 PHY layer transmission. The simulation mechanism is executed according to following model.

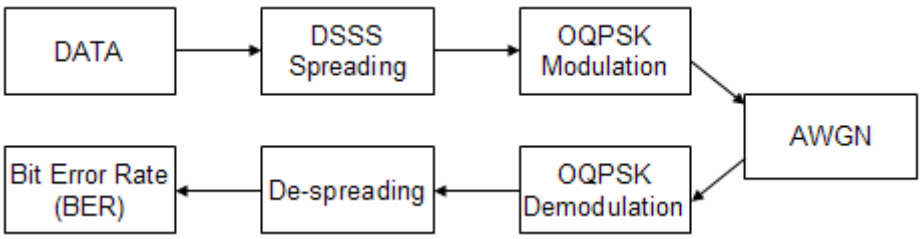

Figure 3-4: Matlab / Simulink model

Figure 3-5 shows the BER calculation of ZigBee transmission model which is build by modules of Simulink.

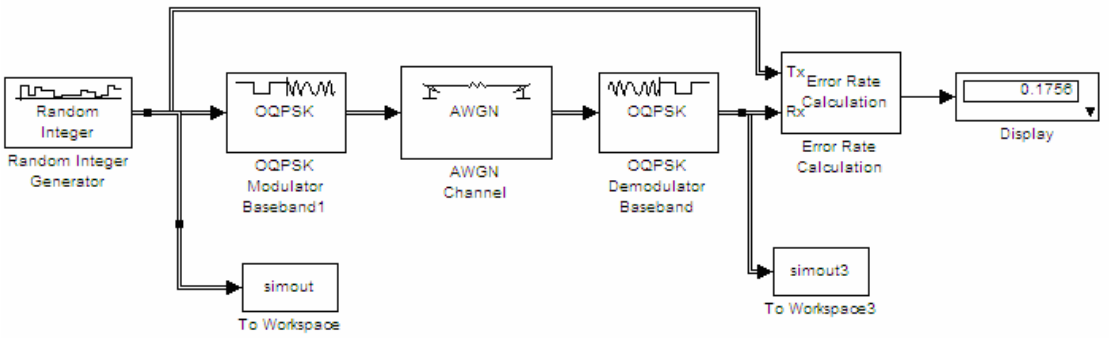

Figure 3-5: Simulink model

Figure 3-6 shows BER of ZigBee transmission in the AWGN channel. The AWGN channel module in MATLAB/Simulink can define SNR parameter. The value of SNR varies from 0 to 8, corresponding error rates are collected. We compare theoretical values with our simulation result in one figure.

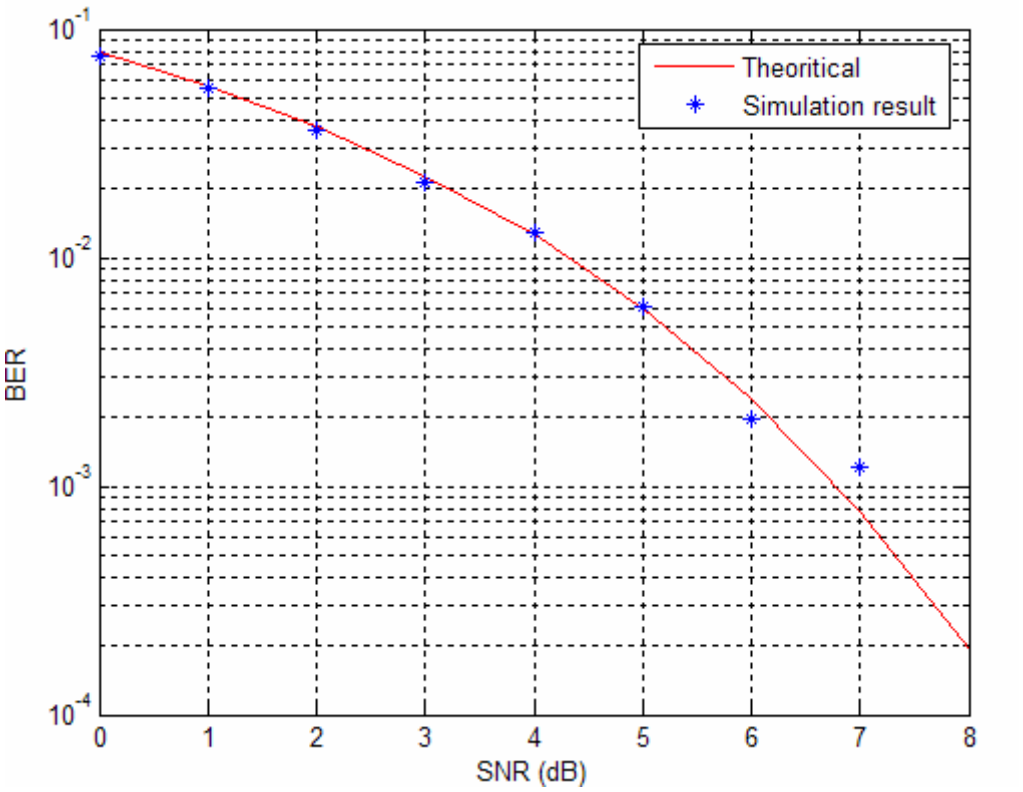

Figure 3-6: BER of ZigBee transmission in AWGN channel

At the same time we calculate the BER of ZigBee (802.15.4) transmission in different channels without WLAN interference. This scenario is intended to see diversity of channels in terms of BER. From the Figure 3-7, we can see that BER of different

channels are not change too much. In this scenario, transmitter power of ZigBee P_{tz} is set as 1mW while noise power P is set as $0.8*10^{-7}$ W, and distance from ZigBee (802.15.4) transmitter to receiver is fixed as 30cm.

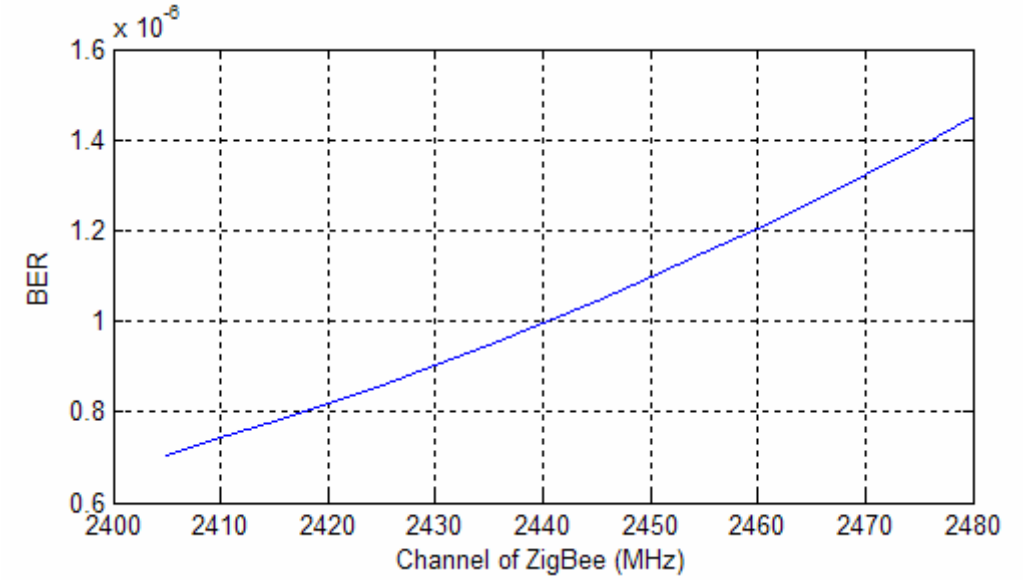

Figure 3-7: BER of ZigBee transmission without interference in different channels

Sequentially, we come to the BER of ZigBee transmission under WLAN interference. As we introduced, we are interested in different distances from the WLAN access point to ZigBee (802.15.4) network coordinator impacting on ZigBee network transmission. The effect is measured in terms of BER. In order to achieve this, we construct a model as the Figure 3-8 shows below.

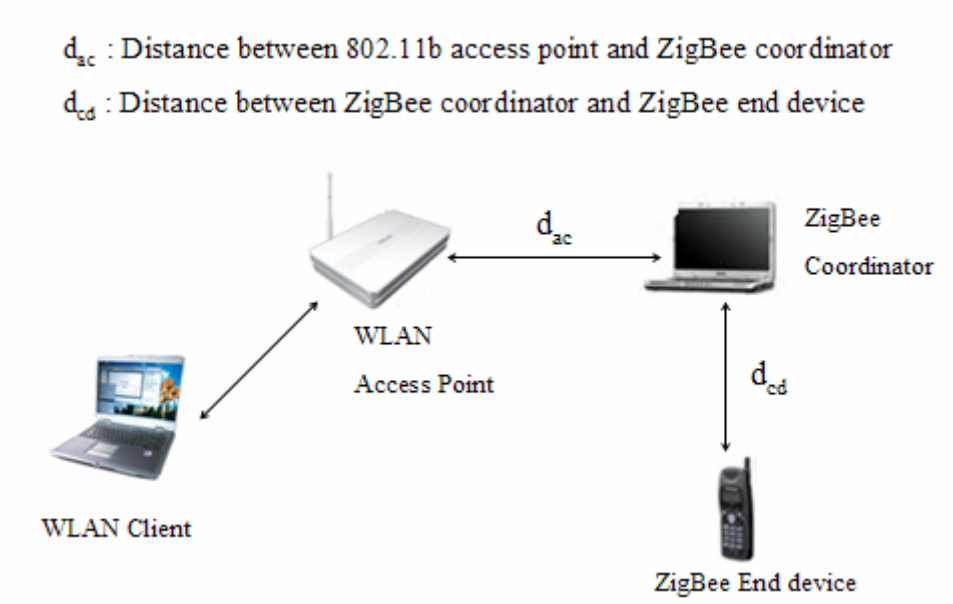

Figure 3-8: Interference model between ZigBee network and WLAN

The overlapping channels of ZigBee and WLAN are chosen to observe interference. Simulation parameters are shown in Table 3-2.

Parameter	Value
Centre frequency of ZigBee channels	2440MHz, 2445MHz, 2435MHz, 2450MHz
Centre frequency of WLAN channel	2442MHz
Transmitter power of ZigBee	1mW
Transmitter power of WLAN	25mW
d_{ac}	From 1m to 10m
d_{cd}	30cm
d_0 (length of light of sight)	8m
n (path loss exponent)	3.3

Table 3-2: Simulation parameter

Figure 3-9 shows the BER of ZigBee transmission under 802.11b WLAN interference with different distance between WLAN access point and ZigBee coordinator when the overlapping channels 2412MHz of WLAN, 2440, 2445, 2435, 2450MHz of ZigBee network are selected, in other words, the centre frequency offsets are 2MHz, 3MHz, 7MHz, 8MHz, respectively.

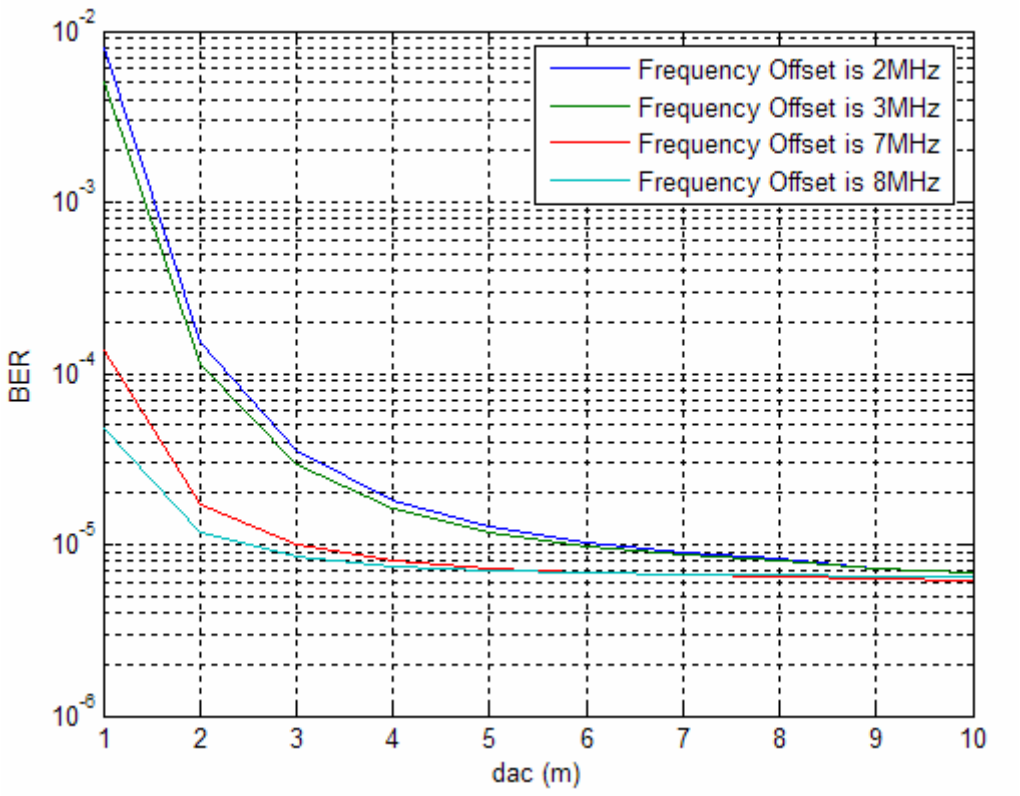

Figure 3-9: BER of ZigBee under 802.11b interference with different frequency offsets

Although we are more concentrated on the different distances between WLAN access point and ZigBee coordinator impacting the BER of ZigBee transmission, it should be known that the different WLAN transmitter powers will also influence the BER of ZigBee transmission.

Figure 3-10 shows the BER of ZigBee transmission under WLAN interference that with different power. d_{ac} equates to 6m while d_{cd} equates to 2m.

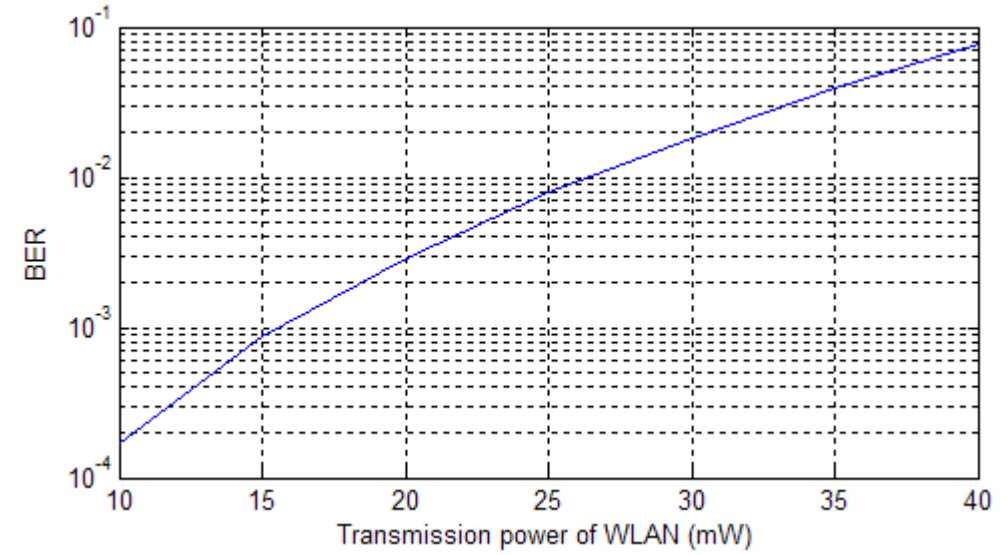

Figure 3-10: BER of ZigBee under 802.11b interference with different WLAN transmitter powers (frequency offset is 2MHz)

3.4 Packet error rate analysis of ZigBee (IEEE802.15.4) under WLAN (IEEE802.11b)

Packet error rate (PER) can be estimated from BER and collision time. In this section, we analyze the collision time when both of networks in transmission processes and then indicate relationship among PER, BER and the collision time.

3.4.1 Collision time model

Both ZigBee transmission (IEEE 802.15.4) and WLAN (IEEE 802.11b) implement slotted carrier sense multiple access with collision avoidance (CSMA/CA) media access method to solve the coexistence problem. In order to directly capture inherent interference, we assume both WLAN and ZigBee network communication are transparence to each other. Under this assumption, status of the channel and retransmission are not taken into consideration.

A collision time model between ZigBee network and WLAN is illustrated as the Figure 3-11.

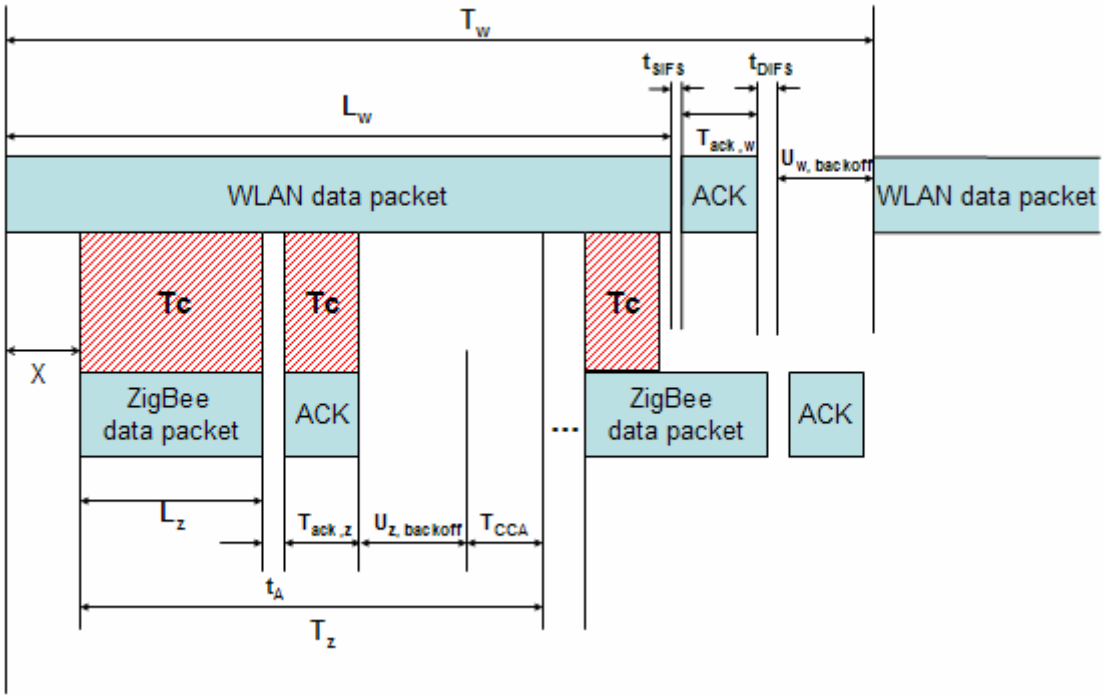

Figure 3-11: Packet collision model between ZigBee network and WLAN

Table 3-3 lists all parameters in the packet collision model:

Parameter	Definition
T_z	Inter-arrival time between two ZigBee data packets
L_z	Duration of ZigBee data packet
t_A	Turn-around time
$T_{ack,z}$	Duration of ZigBee ACK packet
$U_{z,backoff}$	Average *backoff* time of ZigBee
T_{CCA}	Clear channel assessment time
T_w	Inter-arrival time between two WLAN data packets
L_w	Duration of WLAN data packet
t_{SIFS}	Short interframe space of WLAN
t_{DIFS}	Distributed coordination function interframe space of WLAN
$T_{ack,w}$	Duration of WLAN ACK packet
$U_{w,backoff}$	Average *backoff* time of WLAN
X	Time offset
T_c	Collision time

Table 3-3: Parameters in the collision time model

3.4.2 Packet error rate analysis

In order to simplify the collision time model, WLAN acknowledgement (ACK) packet is not considered. The time offset x between WLAN packets and ZigBee packets is assumed to uniformly distributed in $[0, T_w)$ [21]. There are four possible collision scenarios during the transmission.

- First scenario: Part of ZigBee data packet collides with a WLAN data packet.

This scenario will happen with condition:

$$0 < L_w - x - N * T_z < L_z \qquad (3.4.1)$$

N: Number of T_z involved in the transmission collision, $N=0, 1, 2\ldots$

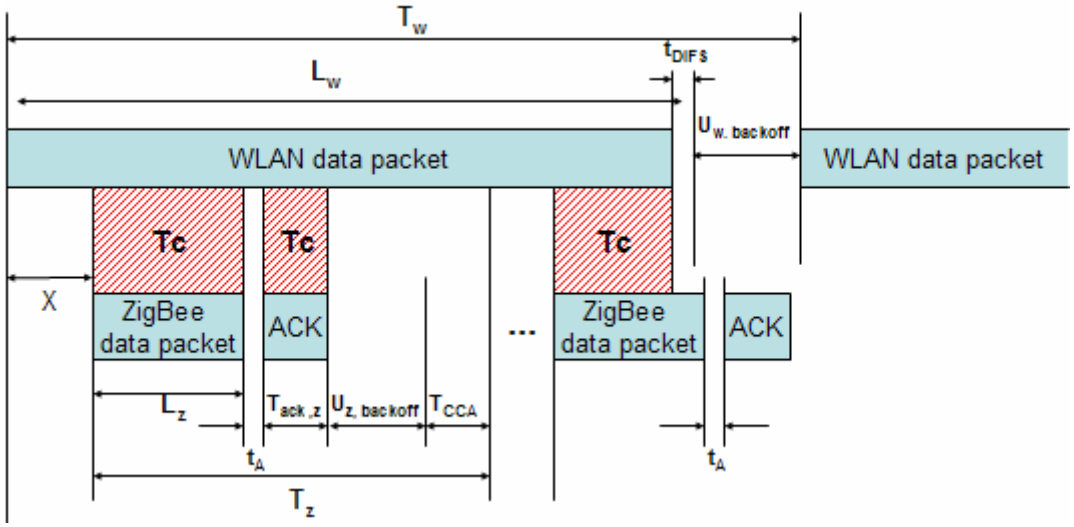

Figure 3-12: Part of a ZigBee data packet collide with a WLAN packet

In this situation, the collision time T_c can be expressed as:

$$T_c = N * (L_z + T_{ack,z}) + (L_w - x - N * T_z) \qquad (3.4.2)$$

N: Number of T_z involved in the transmission collision, $N=0, 1, 2\ldots$

- Second scenario: A whole ZigBee data packet collides with a WLAN packet.

This scenario will happen with condition:

$$L_z \leqq L_w - x - N * T_z \leqq L_z + tA \qquad (3.4.3)$$

N: Number of T_z involved in the transmission collision, $N=0, 1, 2\ldots$

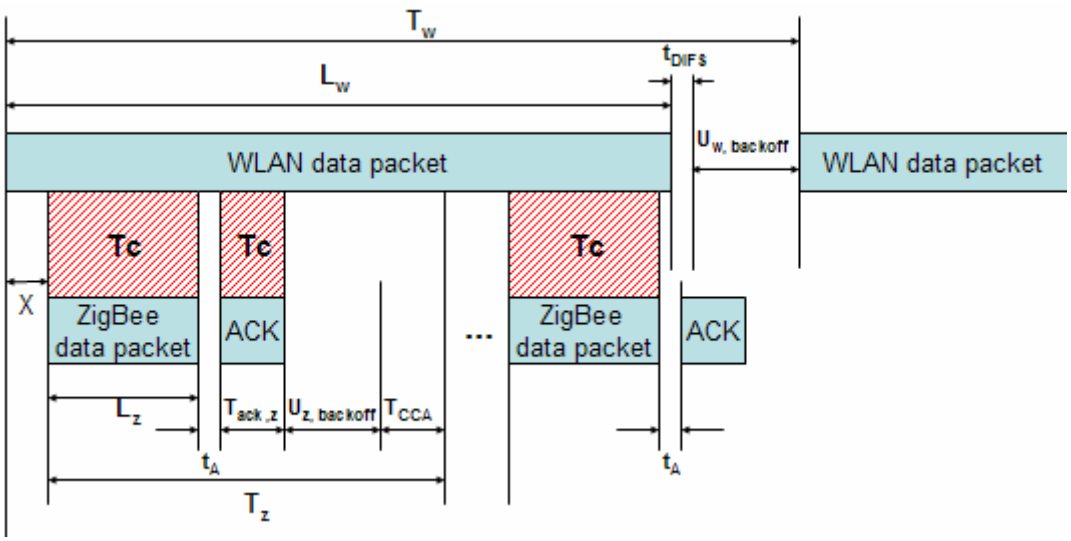

Figure 3-13: A whole ZigBee data packet collides with a WLAN packet

Under this situation, the collision time T_c can be expressed as:

$$T_c = N * (L_z + T_{ack,z}) + L_z \qquad (3.4.4)$$

N: Number of T_z involved in the transmission collision, *N=0, 1, 2…*

➢ Third scenario: A whole ZigBee data packet and part of a ZigBee ACK packet collide with a WLAN packet.

This scenario will happen with condition:

$$L_z + tA < L_w - x - N * T_z < L_z + tA + T_{ack,z} \qquad (3.4.5)$$

N: Number of T_z involved in the transmission collision, *N=0, 1, 2…*

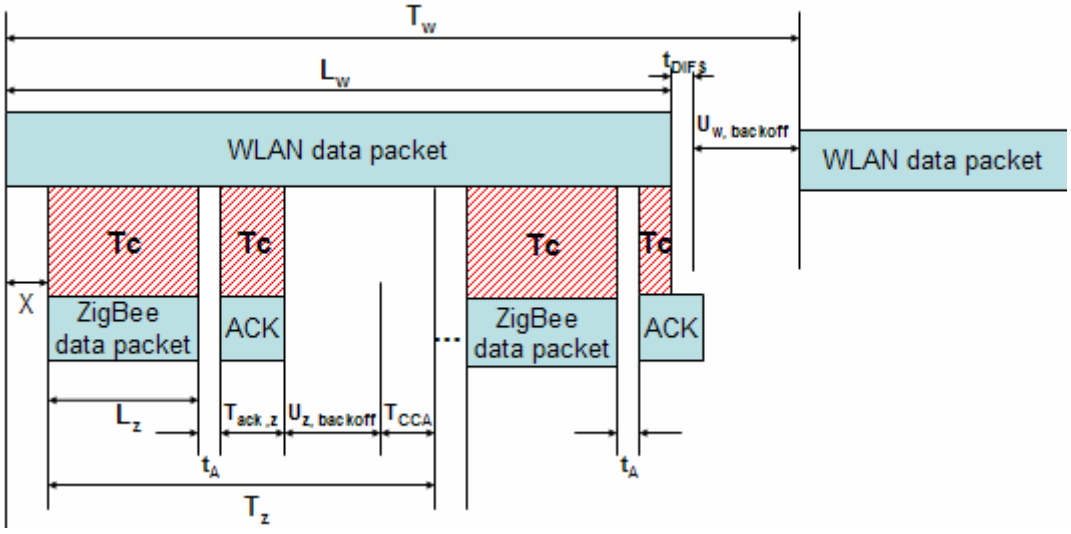

Figure 3-14: A whole ZigBee data packet and part of a ZigBee ACK packet collide with a WLAN packet

In this situation, the collision time T_c can be expressed as:

$$T_c = N * (L_z + T_{ack,z}) + (L_w - x - N * T_z - tA) \qquad (3.4.6)$$

N: Number of T_z involved in the transmission collision, *N=0, 1, 2…*

➢ Fourth scenario: A ZigBee data packet and a ZigBee ACK packet totally collide with a WLAN packet.

This scenario will happen with condition:

$$L_z + tA + T_{ack,z} \leqq L_w - x - N * T_z \leqq L_z + tA + tA + T_z \qquad (3.4.7)$$

N: Number of T_z involved in the transmission collision, *N=0, 1, 2…*

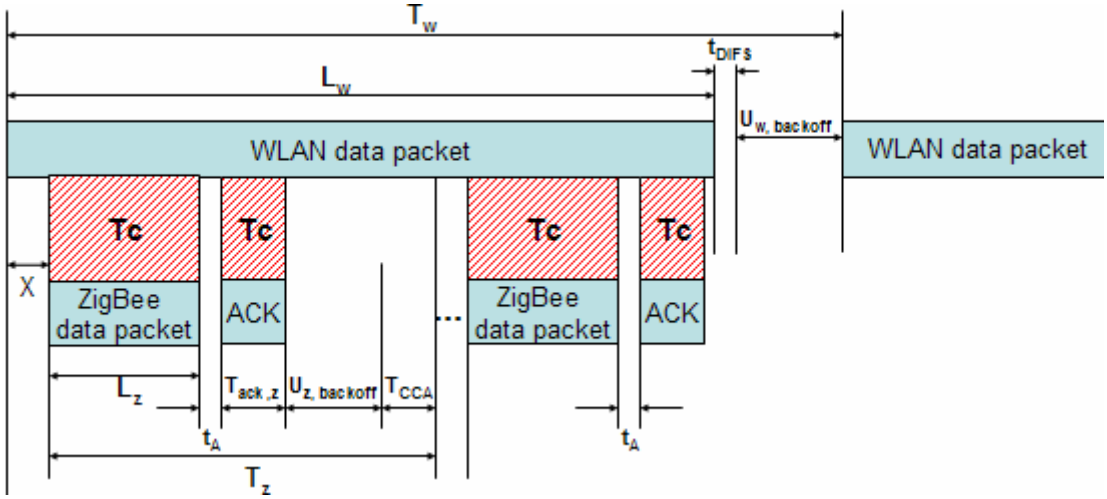

Figure 3-15: A ZigBee data packet and a ZigBee ACK packet totally collide with a WLAN packet

In this situation, the collision time T_c can be expressed as:

$$T_c = (N + 1) * (L_z + T_{ack,z}) \qquad (3.4.8)$$

N: Number of T_z involved in the transmission collision, *N=0, 1, 2…*

In conclusion, the collision time T_c can be obtained as:

$$Tc = \begin{cases} N * (L_z + T_{ack,z}) + (L_w - x - N * T_z) & if \ \ 0 < L_w - x - N * T_z < L_z \\ N * (L_z + T_{ack,z}) + L_z & if \ \ L_z \leqq L_w - x - N * T_z \leqq L_z + tA \\ N * (L_z + T_{ack,z}) + (L_w - x - N * T_z - tA) & if \ \ L_z + tA < L_w - x - N * T_z < L_z + tA + T_{ack,z} \\ (N + 1) * (L_z + T_{ack,z}) & if \ \ L_z + tA + T_{ack,z} \leqq L_w - x - N * T_z \leqq T_z \end{cases} \qquad (3.4.9)$$

N: Number of T_z involved in the transmission collision, *N=0, 1, 2…*

- T_z: inter-arrival time between two ZigBee data packets. It can be easily obtained by the following formula:

$$T_z = L_z + tA + T_{ack,z} + U_{z,\ backoff} + T_{CCA} \qquad (3.4.10)$$

- L_z: duration of ZigBee data packet. It depends on the data rate and length of ZigBee data packet.

$$L_z = Length\ of\ ZigBee\ data\ packet\ /\ Data\ rate\ of\ ZigBee \qquad (3.4.11)$$

- $U_{z,\ backoff}$ / $U_{w,\ backoff}$: average *backoff* time. Both ZigBee (IEEE 802.15.4) network and WLAN (IEEE 802.11b) use CSMA/CA mechanism. In both protocols, nodes must perform a *backoff* process before transmitting a data packet. In the slotted CSMA/CA algorithm, three parameters *NB*, *CW* and *BE* are significant for *backoff* time generation.

NB: number of *backoff*, it is initiated as 0. When a data packet is going to transfer while channel is busy, it generates *backoff* delay time. After this *backoff* delay time, if the channel is still busy, it would generate another *backoff* delay time. While, NB increase by 1. The maximum of *NB* is 4. If the channel is still busy after four times of *backoff* delay time generation, the packet transmission would be cancelled. Consequently, contention window size of IEEE802.11b is not changed.

CW: contention window. It is referenced to define the length of *backoff* delay time. Its initial value is 2, and maximum is 31. *CW* could be divided into units of *backoff periods*, and one b*ackoff* period is the duration of 20 symbols.

BE: *backoff* exponent. $CW=2^{BE}-1$. Its minimum value is 3 and maximum is 5.

The *backoff* time are generated as:

$$Backoff\ time = Random\ (\ ) * aUnitBackoffPeriod$$
$$Random\ (\ ) = [0,\ CW] \qquad (3.4.12)$$
$$CW=2^{BE}-1$$
$$aUnitBackoffPeriod= 20\ symbol\ period$$

In this thesis, since we assume the transmission of ZigBee and WLAN are independent; both of them will transmit packets without consideration of the status of the channel, so the contention window does not need to be changed by the busy channel. In both protocols, the *backoff* time are randomly chosen within the minimum contention window [20]. Therefore, the $U_{z,\ backoff}$ / $U_{w,\ backoff}$ can be obtained as:

$$U_{z,\ backoff} = ST_z * CW_{min,\ z} / 2 \qquad (3.4.13)$$
$$U_{w,\ backoff} = ST_w * CW_{min,\ w} / 2 \qquad (3.4.14)$$

Where ST_z, ST_w stand for unit slot time of ZigBee packet and WLAN packet, $CW_{min,\,z}$, $CW_{min\,,w}$ stand for minimum contention window size of ZigBee packet and WLAN packet respectively.

- tA: turn-around time. It is the time taken by a ZigBee device to switch from the receiver state to the transmitter state. It shall be measured at the air interface from the trailing edge of the last chip (of the last symbol) of a received packet until the transmitter is ready to begin transmission of the resulting acknowledgment. The maximum turn-around time is 12 symbol periods. [9]

- $T_{ack,\,z}$: duration of ZigBee ACK packet.

$$T_{ack,\,z} = Length\ of\ ZigBee\ ACK\ packet\ /\ Data\ rate\ of\ ZigBee \qquad (3.4.15)$$

- T_{CCA}: clear channel assessment time. It will start on a *backoff* period boundary, and the CCA detection time shall be equal to 8 symbol periods. [9]

- T_w: inter-arrival time between two WLAN data packets. It can be obtained by the following formula:

$$T_w = L_w + t_{DIFS} + U_{w,\,backoff} \qquad (3.4.16)$$

- L_w: duration of WLAN data packet. It depends on the data rate and length of WLAN data packet.

$$L_w = Length\ of\ WLAN\ data\ packet\ /\ Data\ rate\ of\ WLAN \qquad (3.4.17)$$

The packet error rate (PER) of ZigBee (IEEE 802.15.4) under WLAN (IEEE 802.11b) interference can be obtained from the BER and collision time. It can be expressed as:

$$Per = 1-(1-b)^{Lz/tz-\lceil Tc/tz\rceil}\,(1-b_i)^{\lceil Tc/tz\rceil} \qquad (3.4.18)$$

Where b, b_i are BER of ZigBee without and with WLAN interference, tz is denoted to be bit duration of ZigBee [20].

3.4.3 Simulation

As we mentioned, in this thesis, we are interested in the interference WLAN brings to ZigBee network, and we focus on how the different distances between WLAN access point and ZigBee coordinator impact the packet error rate (PER) of ZigBee communication, so all the figures are built with distance as the x-axis and PER as the y-axis. Matlab is selected to achieve the simulation. The simulation results of BER are shown in section 3.3.2, the simulation results of PER will be given in the following part, the interference model (Figure 3-8) is also used in this section. Several results are obtained according to different parameters.

Case 1: WLAN (IEEE 802.11b) chooses the channel whose centre frequency is 2442MHz, and ZigBee (IEEE 802.15.4) network uses channel with centre frequency 2440MHz. The packet lengths of WLAN and ZigBee network are fixed. d_{cd} is fixed to 30cm; the value of d_{ac} is changed from 1m to 10m.

ZigBee network(IEEE 802.15.4)		**WLAN (IEEE 802.11b)**	
ZigBee channel	18 (2440MHz)	WLAN channel	7 (2442MHz)
Transmitter power	1mW	Transmitter power	25mW
Payload size (length of data packet)	120 byte	Payload size (length of data packet)	1400 byte
Data rate	250 kbps	Data rate	310 kbps
T_{CCA}	128 μs	t_{DIFS}	50 μs
ST_z (unit slot time of ZigBee)	320 μs	ST_z (unit slot time of WLAN)	20 μs
$CW_{min,\,z}$	7	$CW_{min,\,w}$	31

Table 3-4: Simulation parameters in case 1

Figure 3-16 shows the packet error rate of ZigBee transmission under 802.11b WLAN interference with different distances between WLAN access point and ZigBee coordinator when their channel centre frequency offset is 2MHz.

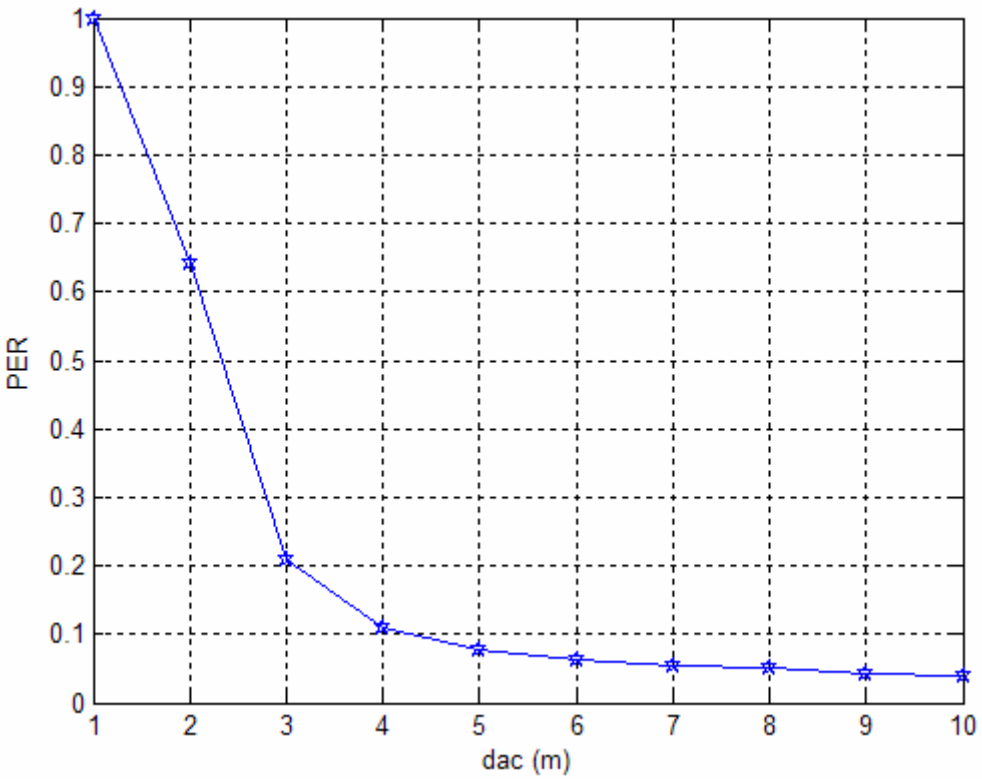

Figure 3-16: PER of ZigBee transmission under 802.11b interference with 2MHz centre frequency offset

Case 2: WLAN uses the channel with centre frequency 2442MHz, and ZigBee network uses channels with centre frequencies 2440MHz, 2445MHz, 2435MHz, and 2450MHz respectively. The packet length of 802.11b and 802.15.4 are fixed. d_{cd} is fixed to 30cm; the value of d_{ac} is from 1m to 10m.

ZigBee (IEEE 802.15.4)		**WLAN (IEEE 802.11b)**	
Centre frequency of ZigBee channel	2440MHz,2445MHz 2435MHz,2450MHz	Centre frequency of WLAN channel	2442MHz
Transmitter power	1mW	Transmitter power	25mW
Payload size (length of data packet)	133 byte	Payload size (length of data packet)	1200 byte
Data rate	250 kbps	Data rate	11 Mbps
T_{CCA}	128 µs	t_{DIFS}	50 µs
ST_z (unit slot time of ZigBee)	320 µs	ST_z (unit slot time of WLAN)	20 µs
$CW_{min,\,z}$	7	$CW_{min,\,w}$	31

Table 3-5: Simulation parameters in case 2

Figure 3-17 shows the packet error rate of ZigBee transmission under 802.11b WLAN interference with different distances between WLAN access point and ZigBee coordinator when the centre frequency offsets are 2MHz, 3MHz, 7MHz, 8MHz, respectively.

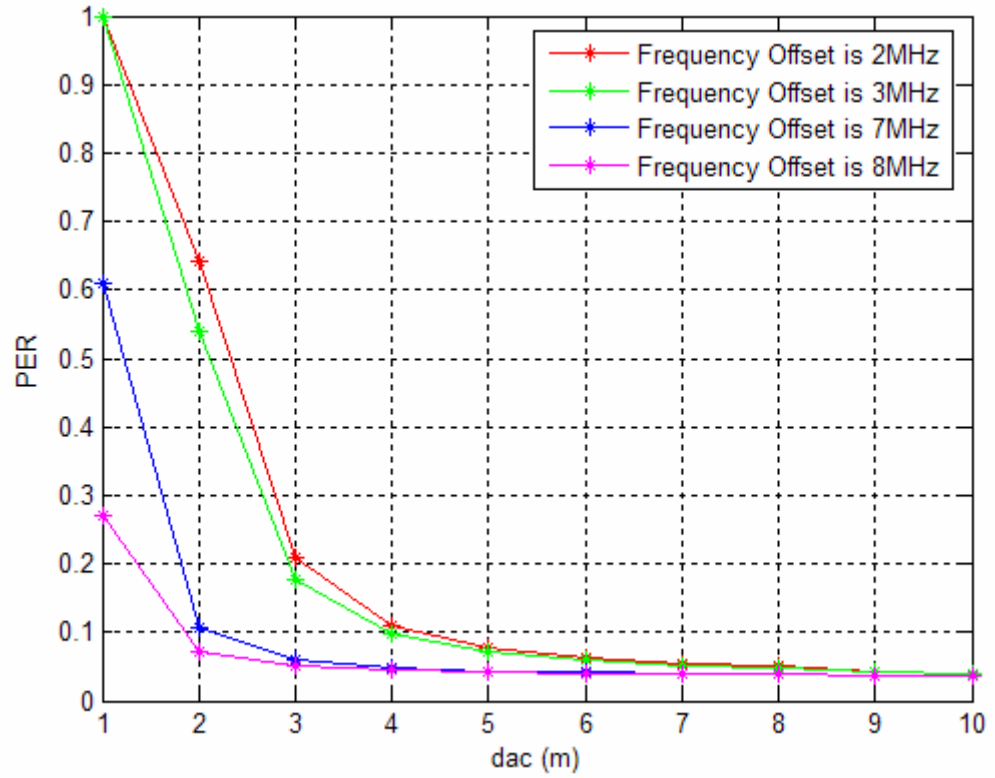

Figure 3-17: PER of ZigBee transmission under 802.11b interference with different centre frequency offsets

Case 3: WLAN uses the channel with centre frequency 2442MHz, and ZigBee network uses 2440MHz. d_{cd} is fixed to 30m; the value of d_{ac} is from 1m to 10m. The packet length of 802.15.4 is fixed. The packet lengths of WLAN are set to 200, 400, 600, 800, 1000, 1200, and 1400 bytes respectively.

ZigBee (IEEE 802.15.4)		**WLAN (IEEE 802.11b)**	
Centre frequency of ZigBee channel	2440MHz	Centre frequency of WLAN channel	2442MHz
Transmitter power	1mW	Transmitter power	25mW
Payload size (length of data packet)	120 byte	Payload size (length of data packet)	200, 400, 600, 800, 1000, 1200, 1400 byte
Data rate	250 kbps	Data rate	310 kbps
T_{CCA}	128 µs	t_{DIFS}	50 µs
ST_z (unit slot time of ZigBee)	320 µs	ST_z (unit slot time of WLAN)	20 µs
$CW_{min,\,z}$	7	$CW_{min,\,w}$	31

Table 3-6: Simulation parameters in case 3

Figure 3-18 shows the packet error rate of ZigBee transmission under 802.11b WLAN interference with different distances between WLAN access point and ZigBee coordinator when the packet lengths of WLAN packet are 200, 400, 600, 800, 1000, 1200, and 1400 bytes respectively with 2MHz centre frequency offset.

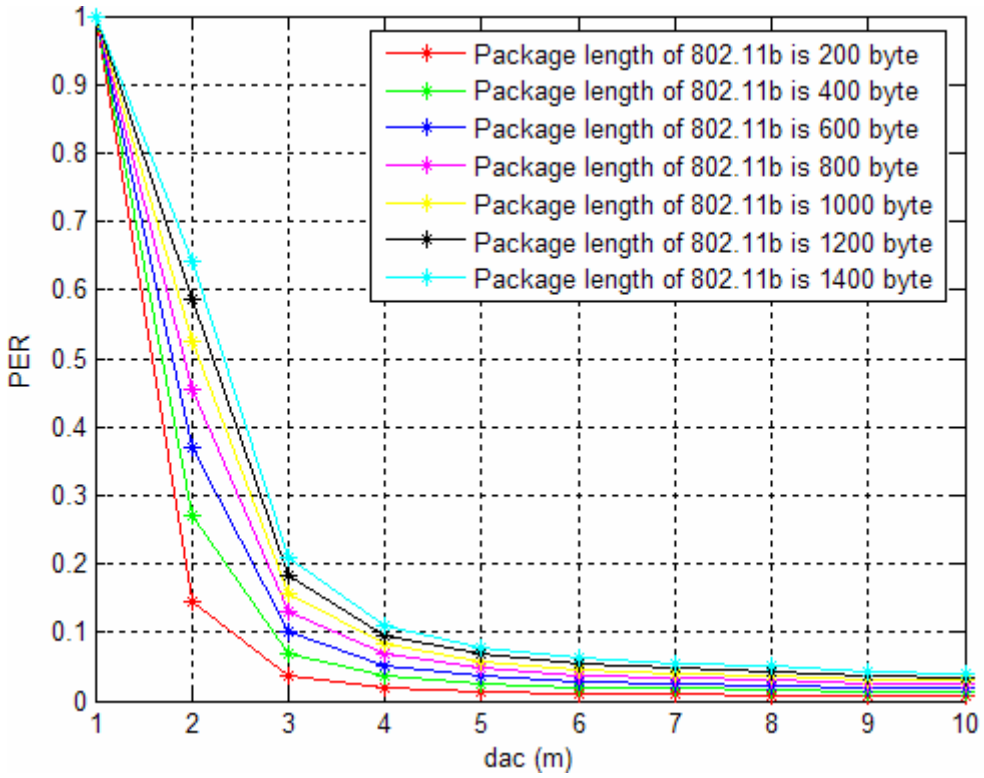

Figure 3-18: PER of ZigBee transmission under 802.11b interference with different WLAN packet lengths (2 MHz frequencies offset)

3.5 Limitation

After the simulation, the measurement will be carried out with the actual devices. The test bed we built, the test environment, processes and results will be mentioned in the next part. There are some limitations during the experiment.

- Test environment: we choose 5IKT Lab to carry out our measurement. Besides the wireless router (WLAN access point) which we used as the interferer in our test bed, some other devices like other WLAN access points fixed in this Lab would also become as interferers. Their existence would impact the test results.

- WLAN packet length: we could not measure the accurate packet length of WLAN. This is another limitation.

- ZigBee transmission data rate: this value is not in control during the measurement.

4 Measurements

4.1 Introduction of ZigBee Demonstration Kit

4.1.1 Atmel

Atmel Corporation is one of the biggest manufacturers of semiconductors in the world. It is founded in 1984, and mainly focuses on system-level solutions built around flash microcontrollers. Its products microcontrollers, Atmel AVR and AVR32 architectures, radio frequency devices, EEPROM, Flash memory devices, also a number of application-specific products. [25]

4.1.2 AVR

AVR is a Modified Harvard architecture 8-bit RISC single chip microcontroller which was developed by Atmel in 1996 [26]. Surprisingly and admirably, the AVR basic architecture was conceived by two students of Norwegian Institute of Technology, they are Alf-Egil Bogen and Vegard Wollan. The AVR microcontrollers support programming and data storing that by using of separate physical memories within different addresses. AVR microcontrollers are multifunction with configurable General Purpose I/O ports, Multiple Internal Oscillators. One attractive point of AVR microcontrollers is that they support In-System Programming by using of ISP (In-System Programmer), JTAG or other methods.

Generally, AVRs are classified as three levels: TinyAVR, MegaAVR, and XMEGA. TinyAVR, MegaAVR, XMEGA are manufactured under differently standardized program memory sizes, pin package lengths or peripheral sets. Additionally, Application specific AVRs are megaAVRs with special features, like LCD controller, USB controller etc.

4.1.3 AVR Z-Link for IEEE 802.15.4 / ZigBee Solution [27]

In order to pursue low-power consumption wireless market, Atmel has developed a complete IEEE 802.15.4 compliant and ZigBee certified solution based on a family of RF transceivers. The solution called AVR Z-Link. A Z-Link application of Atmel was designed based on three components: an AVR microcontroller, an AT86RF230 radio and software MAC that was established by Atmel.

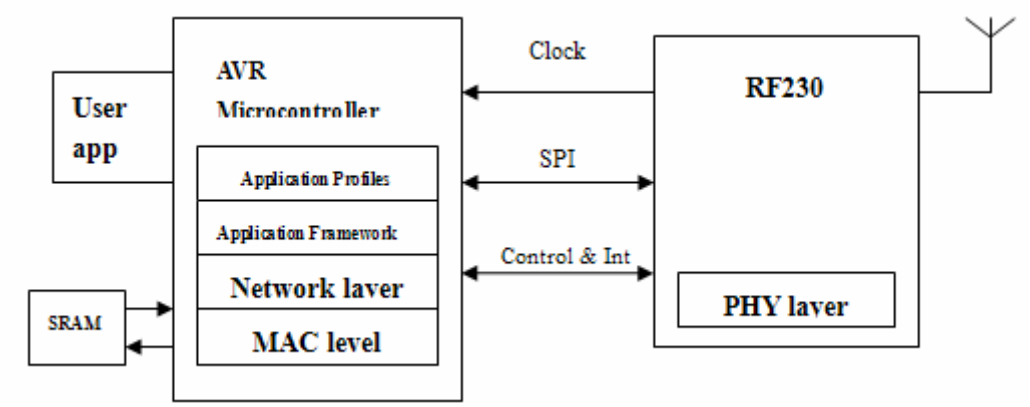

Figure 4-1: AVR Z-Link products' architecture [28]

Figure 4-1 illuminates the AVR Z-Link products' architecture. Z-Link products provide 2.4GHz transceiver with -101 dBm receiver sensitivity and 3dBm transmit power. Atmel has combined a low-power technology which is called picoPower into AVR microcontrollers to achieve low-power consumption in Z-Link products [28]. In order to satisfy different programming requirements, different combinations of AVR microcontrollers and RF230 are available as Z-Link products. Such as: ATmega128RZA chipset is a bundle of ATmega1281 AVR and AT86RF230 radio, ATmega256RZA chipset is a bundle of ATmega2561 AVR and AT86RF230 radio etc .

4.1.4 AT86RF230

AT86RF230 is a low-power 2.4 GHz radio transceiver especially designed for ZigBee /IEEE 802.15.4 applications. It provides a complete radio transceiver interface between antenna and the microcontroller. It uses bidirectional differential antenna pins for transmission and reception. According to IEEE802.15.4 as we introduced in previous chapter, AT86RF230 uses OQPSK with half-sine pulse shaping and 32-length block coding modulation scheme in generation signals for transmission.

Interface of AT86RF230 to Microcontroller is constructed by a slave SPI (serial peripheral interface) and other control signals. Master SPI is on microcontroller side.

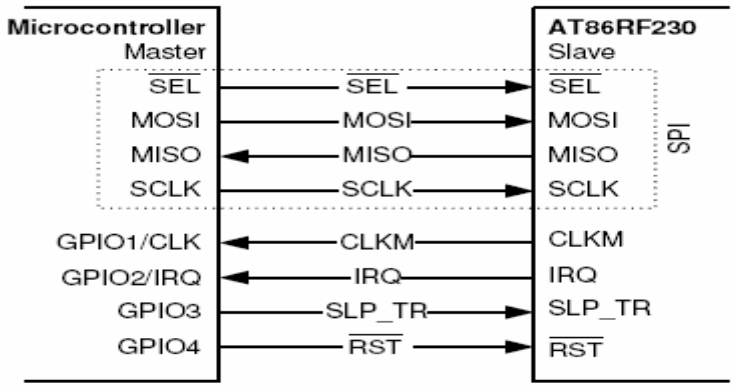

Figure 4-2: Microcontroller to AT86RF230 Interface [29]

This SPI is based on a byte-oriented protocol and used for bidirectional communication between the master and slave. Master initiates by set the SEL=L (low), then transfers one byte that is composed by generated 8 SPI clock cycles via MOSI. At the same time, the slave transfers one byte of data to master via MISO. When SPI transmission is finished, SEL set as H (high). CLKM is AT86RF230 clock output used as microcontroller clock source. IRQ is AT86RF230 interrupt request signal. SLP_TR is multi purpose state control signal and RST is AT86RF230 reset signal.

4.1.5 Atmel designed Medium Access Control (MAC)

As an essential component of Z-Link product, Atmel designed MAC software provides MAC layer services according to IEEE 802.15.4 specified. In the second chapter we introduced that ZigBee as a LR-WPAN standard actually are involved of all layers of ISO created communication s network model. Generally speaking, the application and network layers can be developed to satisfy customer requirement. The development on application and network layer are final software solution that determines usages of a ZigBee product. The MAC level software acts like an interface between PHY layer and the application/network layer. It handles all access the PHY radio channel and provides service to application/network layer.

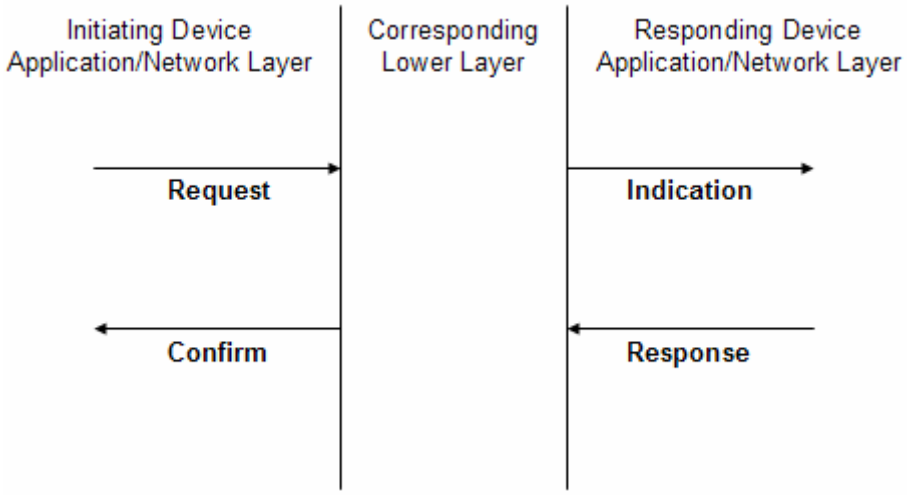

Figure 4-3: MAC software acts as an interface

MAC services provide information interacting with application/network layer. Those information exchanges by using of MAC function call passing between layers. As illustrated in the Figure 4-3, MAC function calls could be classified into 4 types: Request, Indication, Response and Confirm. The *Request* comes from Application/network layer to request MAC to initiate a service. *Indication* is called by application/network layer request or MAC internal event, and passes from MAC. *Response* comes from Application/Network layer to MAC to complete the previous *Indication* procedure. *Confirm* is used to tell Application/Network layer result of previous *Request*. Those functions work in data service of MAC software as following figures show:

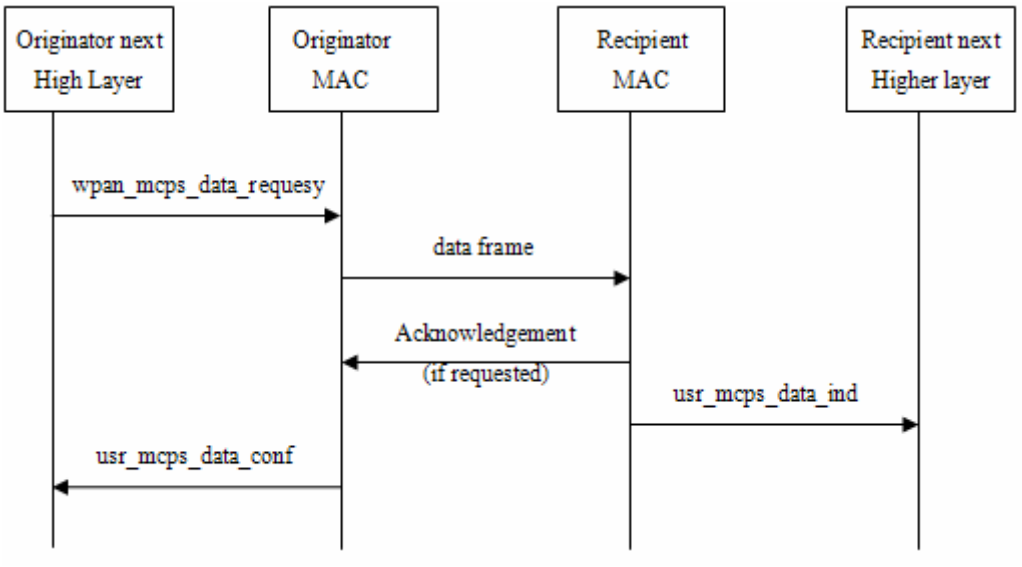

Figure 4-4: Message sequence of data service in MAC software

4.1.6 ATAVRRZ200

We use Atmel AVR Z-Link ATAVRRZ200 Demonstration kit in our test part. RZ200 demonstration kit contains five 802.15.4 compatible 2.4 GHz Radio-Controller Board (RCB), and a display board. Additionally, it contains an AVRISP mkⅡ In-System Programmer (ISP) that can be used for programming firmware.

Figure 4-5: ATAVRRZ200 [30]

Each RCB contains AT86FR230 radio and AVR ATmega1281v microcontroller (v represents that in PCB). The microcontroller contains application firmware which is needed to run customized application/network code.

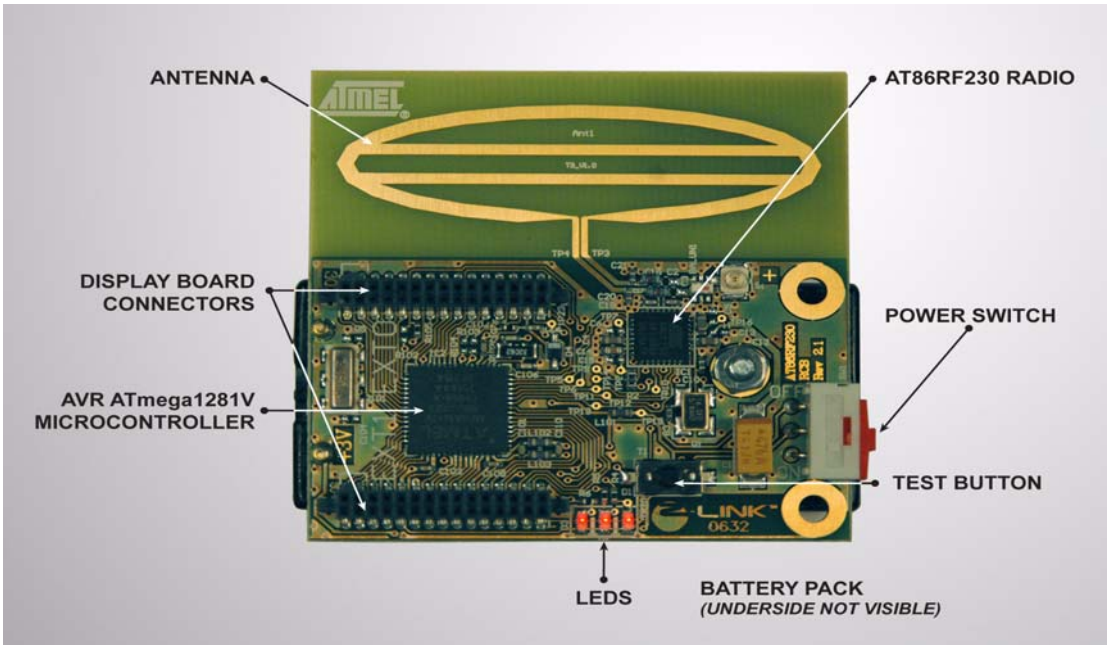

Figure 4-6: RCB [30]

The following figure shows connectors on the display board. It supports the RCB connectors, ISP connectors and JTAG connectors. The ISP, JTAG connectors used for ISP mkⅡ and JTAGICE mkⅡ respectively. Both ISP mkⅡ and JTAGICE mkⅡ are used for in-system programming, JTAGICE is a debugging tool which supports on-chip debugging. ISP mkⅡ is used in our test programming.

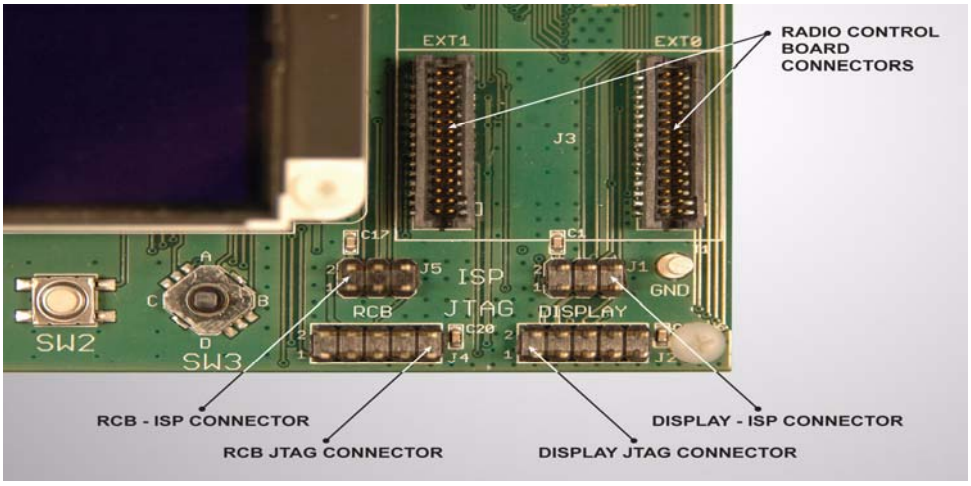

Figure 4-7: Display Board connectors [30]

4.2 Application layer programming

4.2.1 AVR Studio 4

AVR Studio 4 is the most recommended IDE (integrated development environment) for writing and debugging AVR applications in Windows environment. It supports C, Pascal, BASIC and assembly languages and also supports a wide range of emulation and debugging tools.

In this thesis, we use C as programming language to program application layer for test in Windows XP environment. WinAVR compiler combined with AVR studio4 worked as our IDE. We use the AVR ISP mkⅡ (USB version) which was packed together with the ATAVRRZ200 kit.

4.2.2 Basic programming principle

In Application layer programming, we constructed a star topology ZigBee network and arranged data packet to transmit from one end device to coordinator and then relay the data packet to another end device. The RCB which mounted on the display board play the role of network coordinator.

In thesis, we attempt to briefly illustrate the application programming. We modified demo code that is from the ATAVRRZ200 demonstration kit. In main function, it initiates all RCBs, set work modes respectively. We use the above figure to explain how the code works.

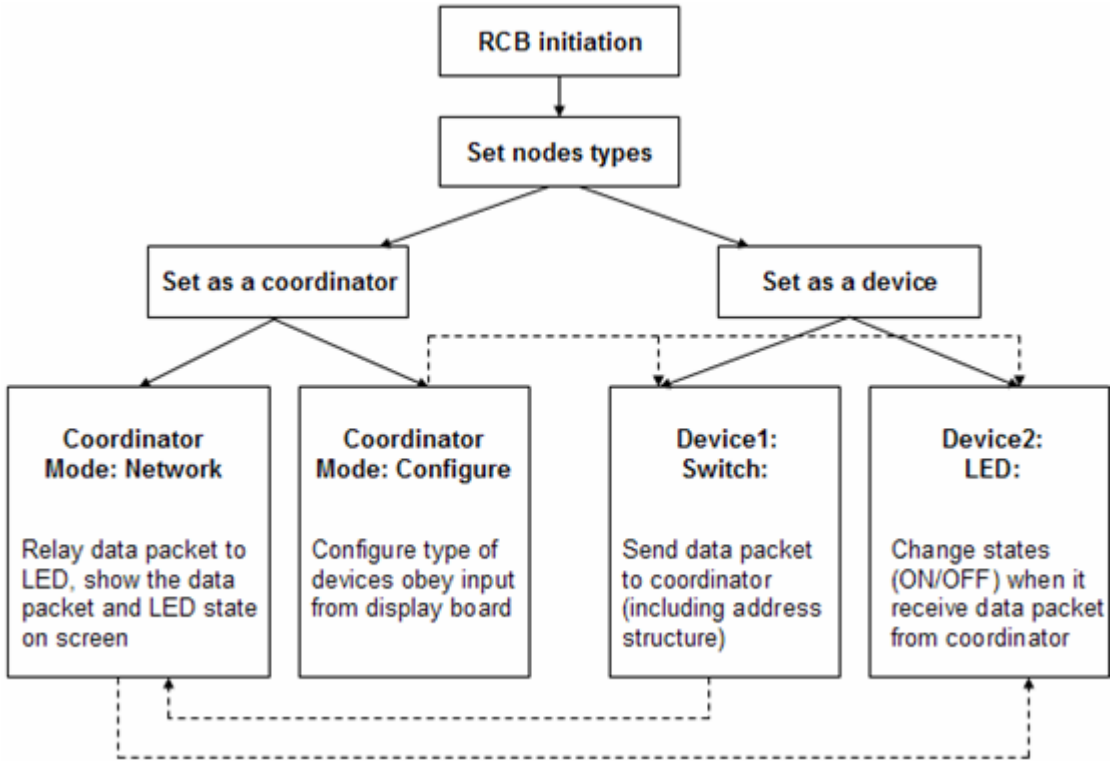

Figure 4-8: ATAVRRZ200 work flow in project

Once the coordinator starts work, it takes responsible for two tasks, end device configuration and network communication. User uses the joystick to set end devices to work as *LED* or *Switch*, and then the coordinator configures end devices to be.

When an end device was set as *Switch*, it sends data packet to the coordinator when its button is pressed. The data packet is composed as IEEE802.15.4 specified PPDU that includes PAN identities, short addresses of the device and coordinator. We use data structure to implement these WPAN information store and calling. According to IEEE802.15.4 specified PPDU length, we set every packet with 126 bytes length in our test which contains 120 bytes data payload.

The end device *Switch* transfers the data packet to coordinator via lower layers. MAC of the coordinator will call coordinator's data *indication* function when it received a data frame. The data *indication* function is firstly to check whether the data is legitimate or not. If data passes the confirmation, the coordinator will call MAC to obtain the RSSI (received signal strength indication) from received frame. In this way, we can obtain the signal power at receiver when the coordinator acts as receptor. Then the coordinator will send the data to the *LED* device with update *LED* information. The press of the *Switch* will trigger screen update *LED* information, display the *LED* current state.

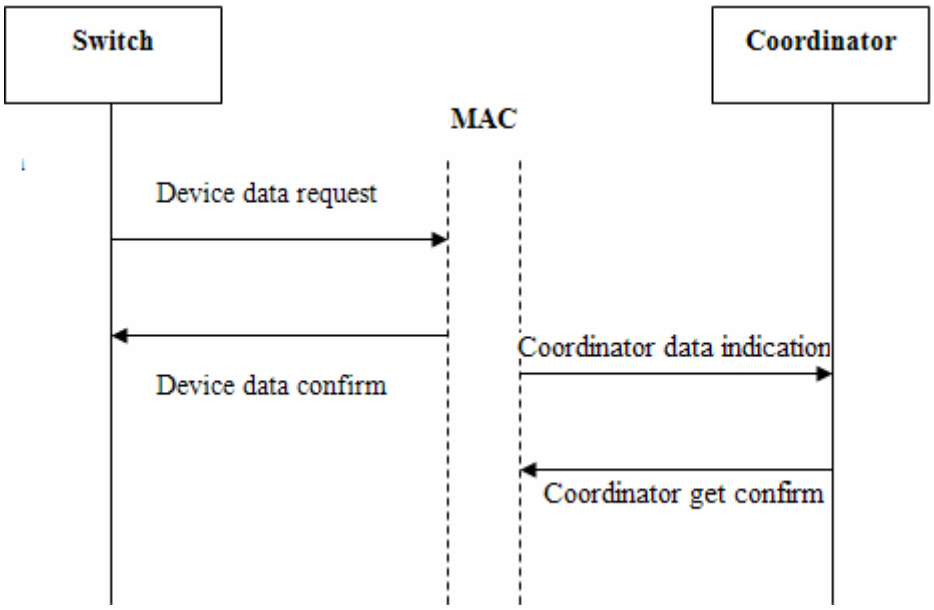

Figure 4-9: Message sequence between Application layer and MAC

Switch implements a *request* function: **device_mcps_data_request_switch_packet** to send data packet which will be read by coordinator. Then switch calls a data *confirm* function: **device_data_confirm_switch**. After *confirmation,* it calls **wpan_mcps_data_request** from MAC library to process the data *request*. This function forms a *mcp* message and puts it in the message queue, returns true or false to indicate whether successfully add the message queue.

Once a device attempts to associate with the coordinator, MAC would call a function to set association permit and a data *indication* callback: **coord_mcps_data_indication**. The MAC of the coordinator would call this *indication* function when it receives a data frame. The function will first make sure that the data frame was sent by an associated device with a legitimate address, and then call the MAC to obtain the RSSI of the received frame, send data to the LED devices with the update *LED* information.

The coordinator sends data to *LED* is not the essential part in our project, we would not explain deeply into it. Since we focus on the network transmission quality, the transmission from one end device to the coordinator is enough.

4.3 Test

In the section4.1 and 4.2, we introduced main devices and corresponded programming which are used to carry out the test. In this section, the test environment, processes and results will be described.

4.3.1 Test Environment

Test place: Agder University 5IKT Lab
Test device: ATAVRRZ200 IEEE 802.15.4/ZigBee Demonstration Kit
Wireless router (TP-LINK)
Laptops (COMPAQ Presario V3000 and Lenovo Tianyi 100A)

Figure 4-10 shows the test bed we built.

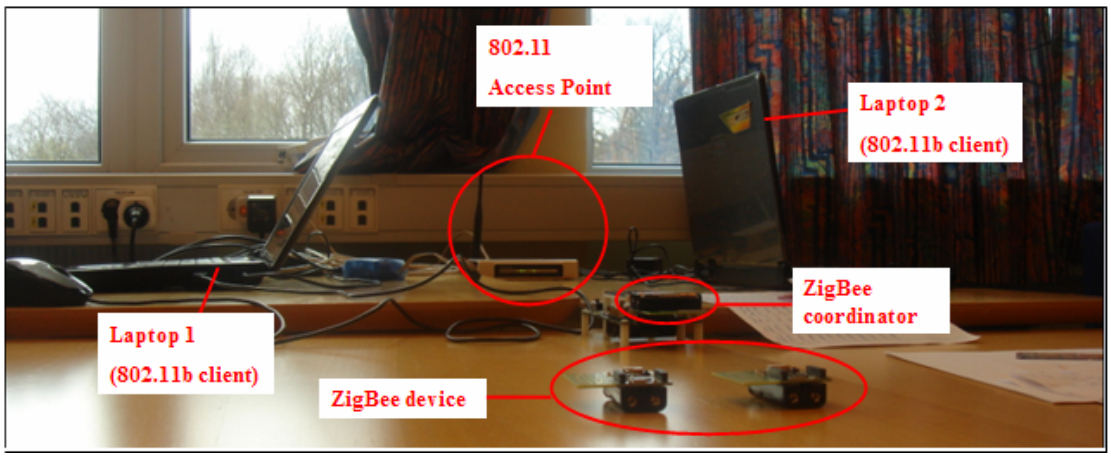

Figure 4-10: Test bed

As shown in Figure 4-10, the test bed consists of two laptops, one wireless router and ZigBee demonstration kit which include one display board and three radio controller boards (RCB). The RCB mounted on the display board plays role of ZigBee coordinator, and the rest two RCBs are worked as ZigBee end devices.

4.3.2 Basic test process

1. Turn on the power of the display board and the ZigBee coordinator (on the display board)

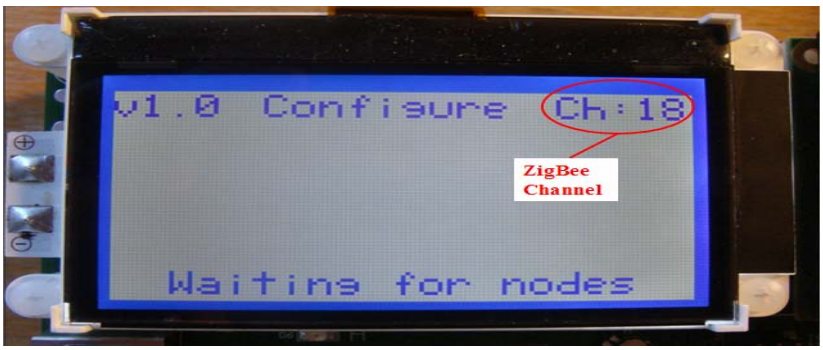

Figure 4-11: Channel information

When the display board and ZigBee coordinator are turned on, the channel which the coordinator currently uses will be shown on the screen, and the whole network including the coordinator is in the state of *waiting for nodes*.

2. Turn on the power of two ZigBee devices

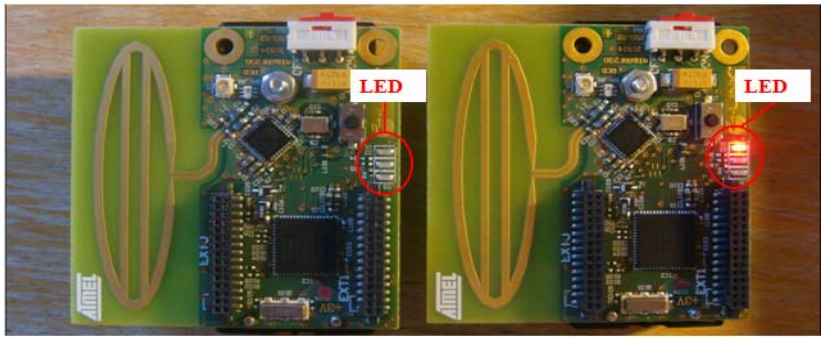

Figure 4-12: ZigBee devices

The LED of the device will blink while they are searching for the ZigBee network.

3. All the nodes have joined in the ZigBee network

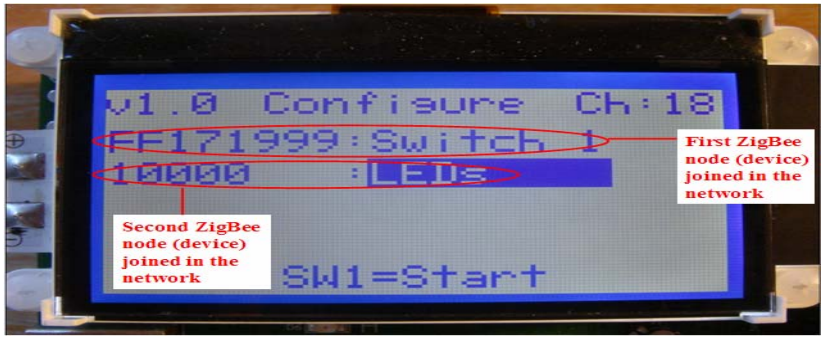

Figure 4-13: Node (device) information

When the two ZigBee devices joined in the network, the LED of the device (Figure 4-12) will turn off, and the nodes information will display on the screen. We configure the first node to work as *Switch* and the second node as *LEDs* by using joystick that on the display board.

4. Waiting for packet transmission

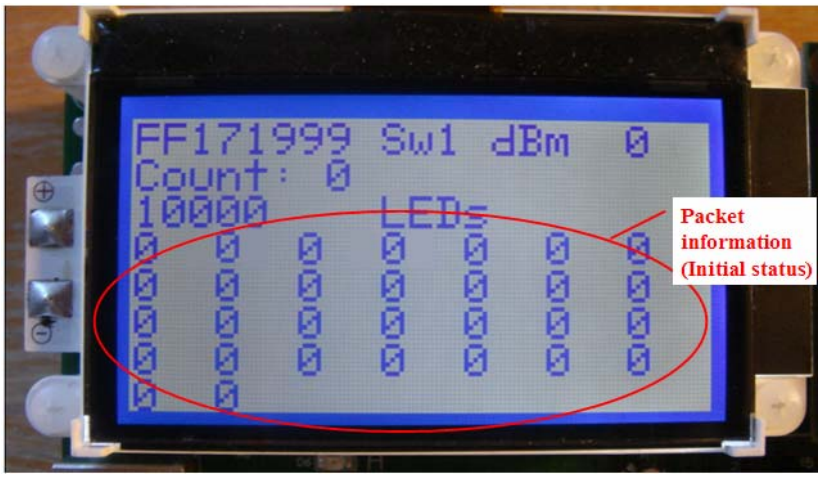

Figure 4-14: Initial packet information

After all the nodes joined in the network, packet transmission is ready to start. The initial data information (all zero) is shown on the screen.

5. Start packets transmission

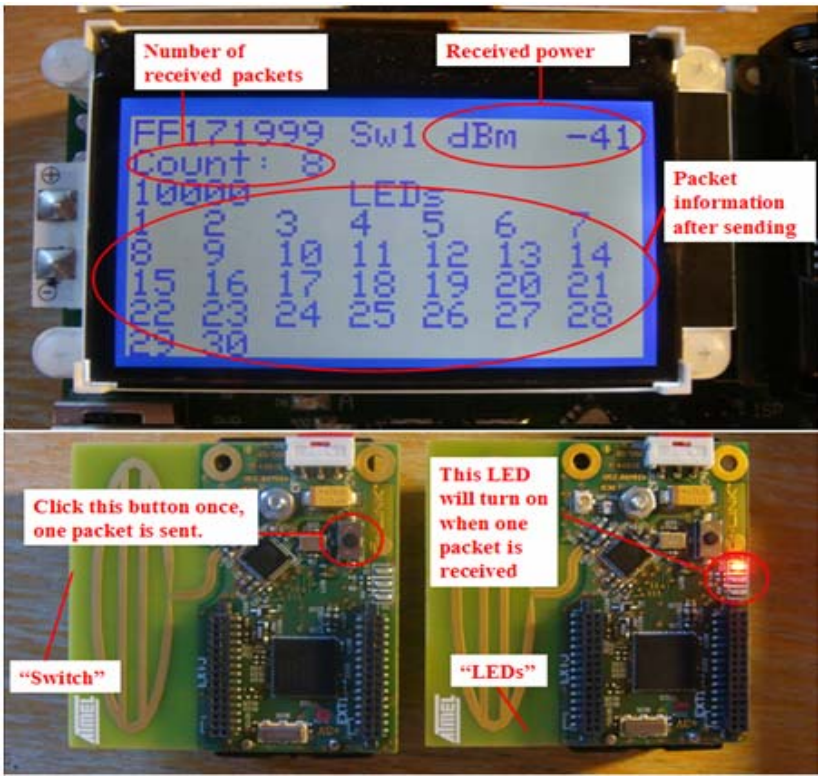

Figure 4-15: Received packet information

Press the button on the device *Switch* once, one packet is sent from the end device to the coordinator, and the data information will display on the screen. Then the coordinator will relay the packet to *LEDs* that will be ON/OFF.

4.3.3 Test

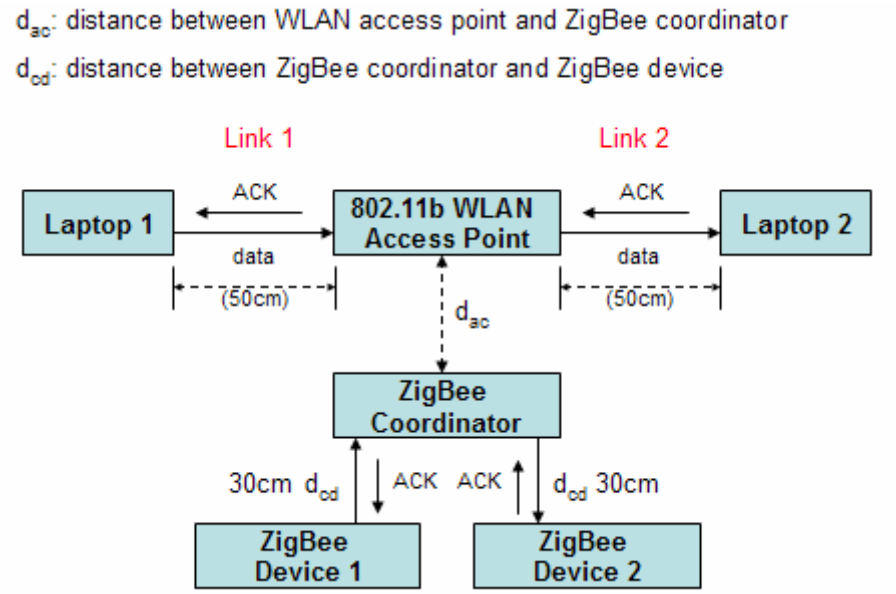

Figure 4-16: Basic test scenario

In test, the WLAN network is constructed by two laptops and one WLAN access point. WLAN data packets are transmitted from Laptop1 to the access point which relays the data packets to the Laptop2. Corresponding ACK are sent back respectively in the channel. As we illustrate in Figure 4-16, Laptop1 is transmitter and WLAN access point is receiver in Link1, while the access point is the transmitter and Laptop2 is receiver in Link2.

Due to the relay via the WLAN access point, the same WLAN packet is sent twice, so the duration of each packet is doubled and every packet occupies the transmission channel both in the Link1 and Link 2 processes (Figure 4-17).

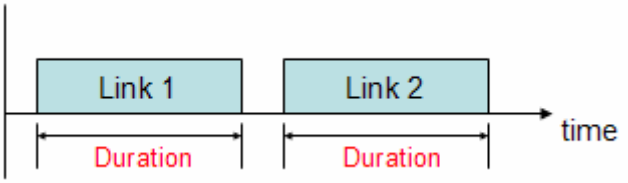

Figure 4-17: WLAN packet duration

Test Ⅰ

WLAN communication based on IEEE 802.11b and WLAN channel fixes to 2442MHz (Channel 7). In this test part, ZigBee network performance is investigated when work on overlapping channels and different locations from WLAN access point.

Scenario one

In test scenario one, distance between WLAN access point and ZigBee coordinator (d_{ac}) is fixed to 3 meters. ZigBee network using the overlapping channel 18,19,17,20 with offsets from WLAN centre frequency 2MHz, 3MHz,7MHz, 8MHz respectively..

Frequency offset (Hz) / Parameters	2M	3M	7M	8M
WLAN channel	Channel 7 (2442M)	Channel 7 (2442M)	Channel 7 (2442M)	Channel 7 (2442M)
ZigBee channel	Channel 18 (2440M)	Channel 19 (2445M)	Channel 17 (2435M)	Channel 20 (2450M)
Transmission type (between two laptops)	.avi file	.avi file	.avi file	.avi file
Data rate (kbps)	260~309	273~322	280~330	267~324
d_{ac} (m)	3m	3m	3m	3m
d_{cd} (m)	30cm	30cm	30cm	30cm

Table 4-1: Parameters for test scenario1

The power spectrum of 802.11b WLAN (Channel 7) is obtained by Handheld Spectrum Analyzer R&S FSH3 with three meters apart from the WLAN access point. And we must point out the values shown on the following figures are peak values, average values are little lower than the peaks'.

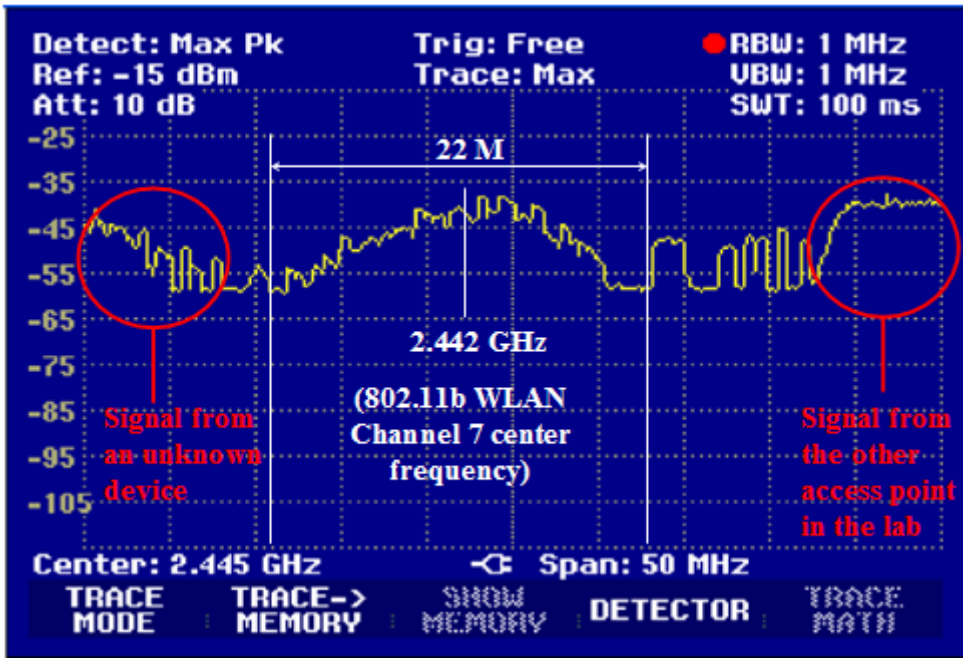

Figure 4-18: Power spectrum of 802.11b WLAN (3 meters to WLAN access point)

The power spectrum of ZigBee (Channel 17, 2435MHz) is obtained by Handheld Spectrum Analyzer R&S FSH3 with one meter apart from ZigBee coordinator.

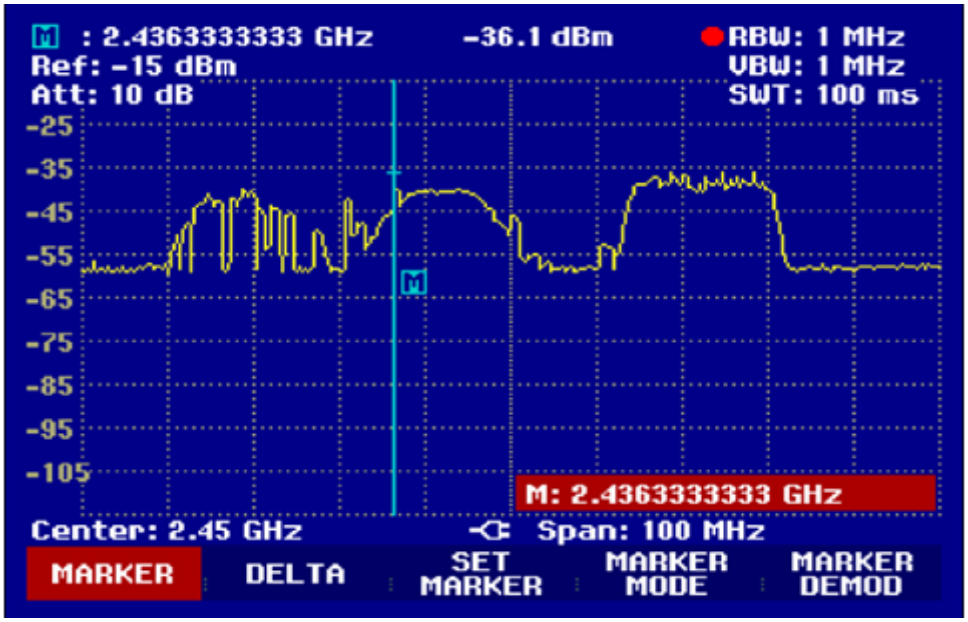

Figure 4-19: Power spectrum of ZigBee (1 meter to ZigBee coordinator)

Test result:

Frequency offset (Hz) / Test result	2M	3M	7M	8M
Time for ZigBee node (device) join in the network (second)	Node 1: 4s Node 2: 12s	Node 1: 4s Node 2: 7s	Node 1: 1s Node 2: 3s	Node 1: 1s Node 2: 2s
Receive power (dBm)	-35 dBm	-29 dBm	-35 dBm	-32 dBm
Number of packets be sent	500	500	500	500
Number of lost packets	228	201	116	104

Table 4-2: Result of test scenario 1

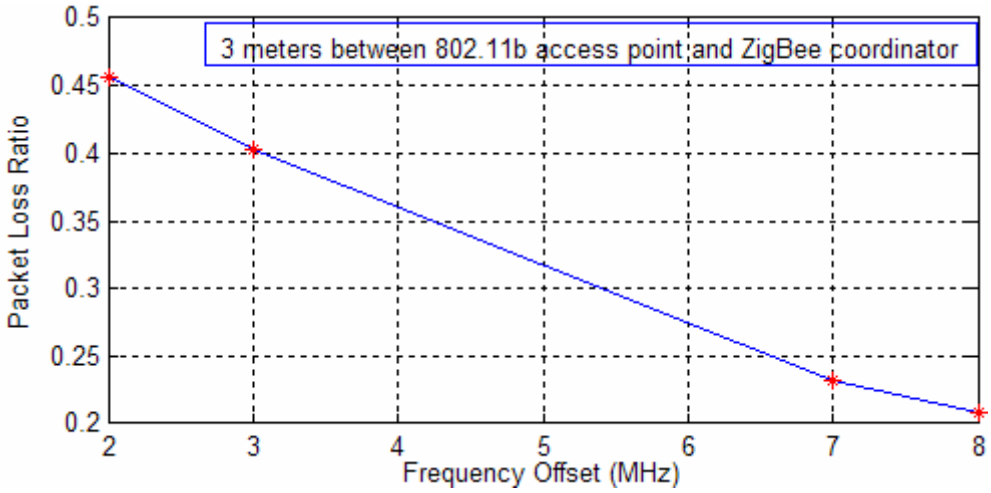

Figure 4-20: Packet loss ratio of test scenario 1

Scenario two:
This test scenario is similar to the test scenario one, only change the distance between WLAN access point and ZigBee coordinator (d_{ac}) from 3 meters to 7 meters.

Frequency offset (Hz) / Parameters	2M	3M	7M	8M
WLAN channel	Channel 7 (2442M)	Channel 7 (2442M)	Channel 7 (2442M)	Channel 7 (2442M)
ZigBee channel	Channel 18 (2440M)	Channel 19 (2445M)	Channel 17 (2435M)	Channel 20 (2450M)
Transmission type (between two laptops)	.avi file	.avi file	.avi file	.avi file
Data rate (kbps)	267~312	280~303	299~306	282~327
d_{ac} (m)	7m	7m	7m	7m
d_{cd} (m)	30cm	30cm	30cm	30cm

Table 4-3: Parameters for test scenario 2

This power spectrum is obtained by Handheld Spectrum Analyzer R&S FSH3 seven meters apart from the WLAN access point.

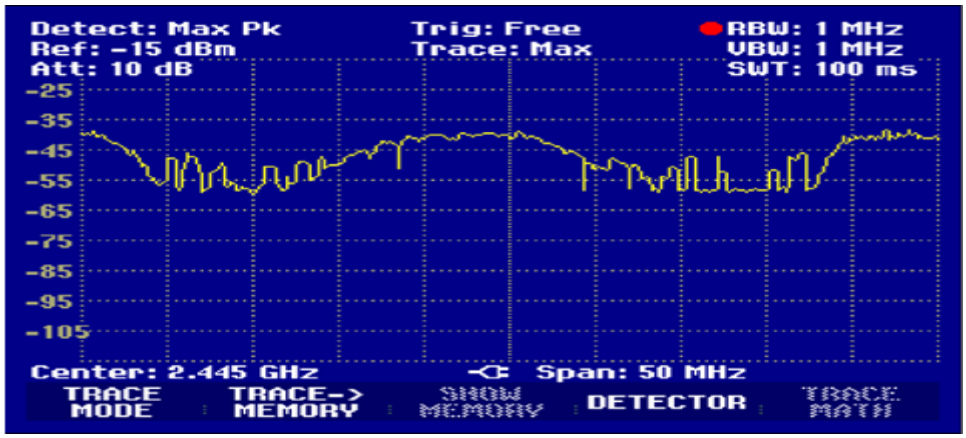

Figure 4-21: Power spectrum of 802.11b WLAN (7 meters to WLAN access point)

Test result:

Frequency offset (Hz) / Test result	2M	3M	7M	8M
Time for ZigBee node (device) join in the network (second)	Node 1: 3s Node 2: 8s	Node 1: 3s Node 2: 6s	Node 1: 1s Node 2: 2s	Node 1: 1s Node 2: 2s
Receive power (dBm)	-35 dBm	-35 dBm	-29 dBm	-32 dBm
Number of packets be sent	500	500	500	500
Number of lost packets	190	126	99	11

Table 4-4: Result of test scenario 2

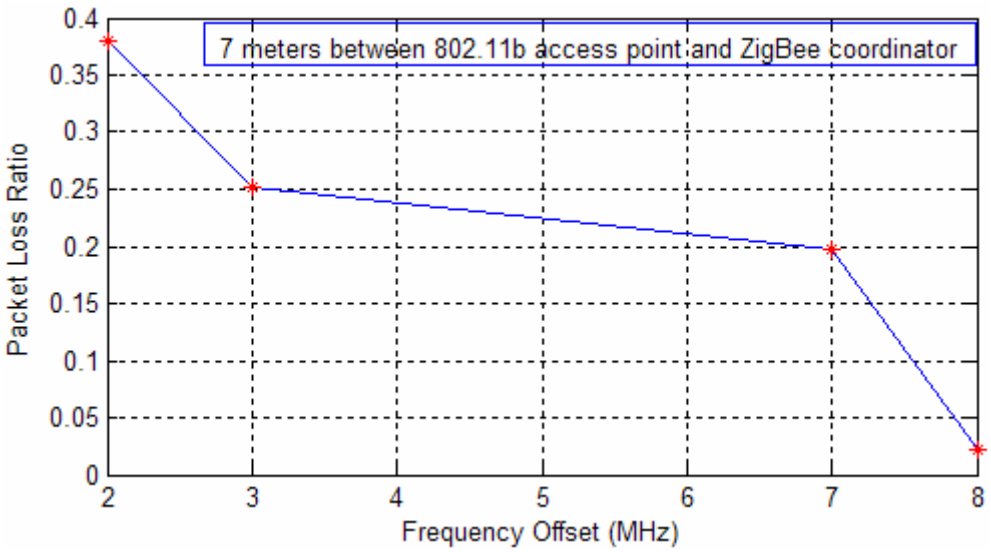

Figure 4-22: Packet loss ratio of test scenario 2

Scenario three:

The same test bed is used. Two overlapping channels, Channel 7 (2442MHz) of WLAN and channel 18 (2440 MHz) of ZigBee have been chosen. The frequency offset fixes to 2MHz, the distance between WLAN access point and ZigBee coordinator (d_{ac}) changes from 1 meter to 8 meters.

d_{ac} (m) / Parameters	1m	2m	3m	4m	5m	6m	7m	8m
Trans. type (between two laptops)	.avi	.avi	.avi	.avi	.avi	.avi	.avi	.avi
Data rate (kbps)	260~306	280~310	265~317	282~320	260~306	280~310	265~317	282~320
d_{cd} (m)	30cm	30cm	30cm	30cm	30cm	30cm	30cm	30cm

Table 4-5: Parameters for test scenario 3

The following figure shows the power spectrum of 802.11b WLAN (Channel 7) which is obtained also by the Handheld Spectrum Analyzer R&S FSH3 with one meter from WLAN access point.

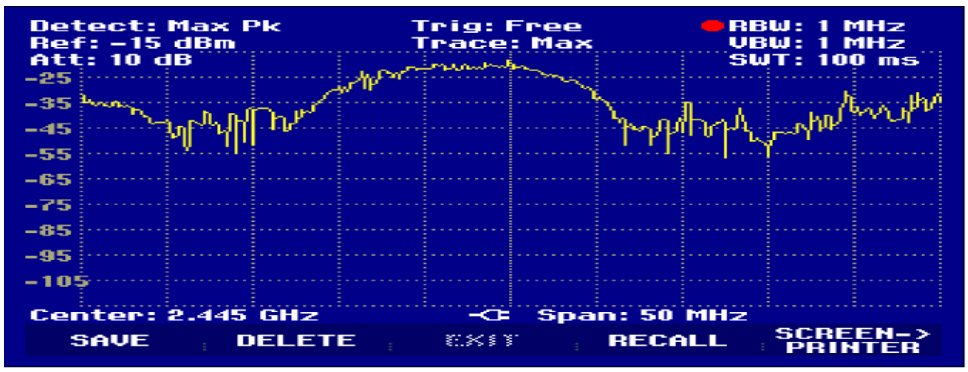

Figure 4-23: Power spectrum of 802.11b WLAN (1 meter to WLAN access point)

Test result:

d_{ac} (m) / Parameters	1m	2m	3m	4m	5m	6m	7m	8m
Time for ZigBee node (device) join in the network (second)	Node1: 2s Node2: 19s	Node1: 9s Node2: 11s	Node1: 6s Node2: 8s	Node1: 5s Node2: 8s	Node1: 5s Node2: 6s	Node1: 4s Node2: 6s	Node1: 2s Node2: 3s	Node1: 1s Node2: 2s
Receive power (dBm)	-29	-35	-35	-32	-32	-35	-35	-29
Number of packets be sent	500	500	500	500	500	500	500	500
Number of lost packets	280	241	228	203	192	185	170	138

Table 4-6: Result of test scenario 3

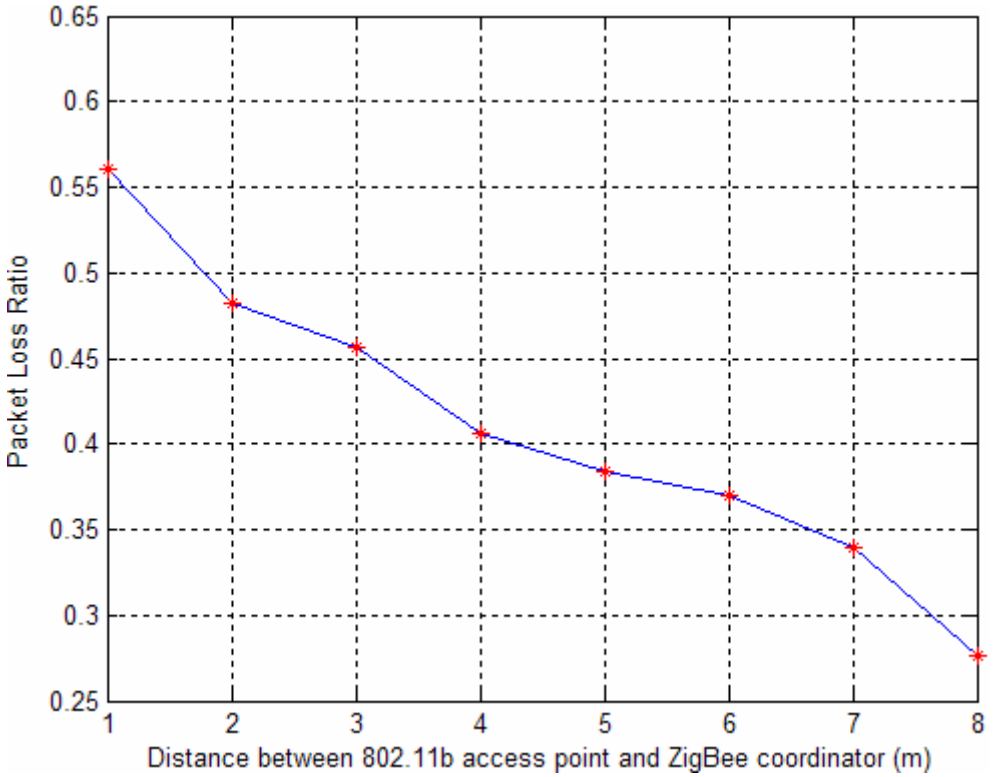

Figure 4-24: Packet loss ratio of test scenario 3 (Frequency offset is 2MHz)

Scenario four:

The test bed is built as same as the third scenario, two non-overlapping channels have been chosen to carry out this test. 802.11b WLAN chose 2442MHz (Channel7) and ZigBee chose 2455MHz (Channel 21) and 2430MHz (Channel 16), respectively. The experimental result shows that there is no packet loss under this situation.

Test Ⅱ

WLAN communication based on 802.11g, and other parameters are kept as Test Ⅰ. WLAN Channel is fixed to the 2442MHz (Channel 7) as in Test Ⅰ, and sends same .avi files as Test Ⅰ. Test scenarios are carried similar to previous test scenarios in order to investigate ZigBee network performance under WLAN 802.11g interference.

Scenario five:

Set distance from WLAN access point to ZigBee network coordinator fixed to 3 meters. ZigBee communications in different channels with different offsets from WLAN channel centre frequency are tested. PER of 2MHz, 3MHz, 7MHz and 8MHz offsets are illustrated in Figure 4-24.

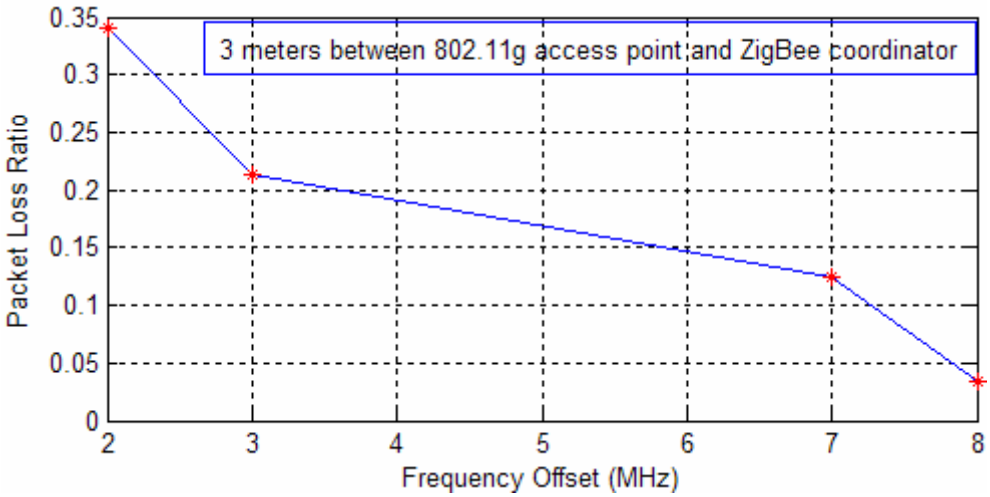

Figure 4-25: Packet loss ratio of test scenario 5

Scenario six:

Set distance from WLAN access point to ZigBee network coordinator fixed to 7 meters while keep other parameters as in scenario six. PER of 2MHz, 3MHz, 7MHz and 8MHz offsets are illustrated in Figure 4-25

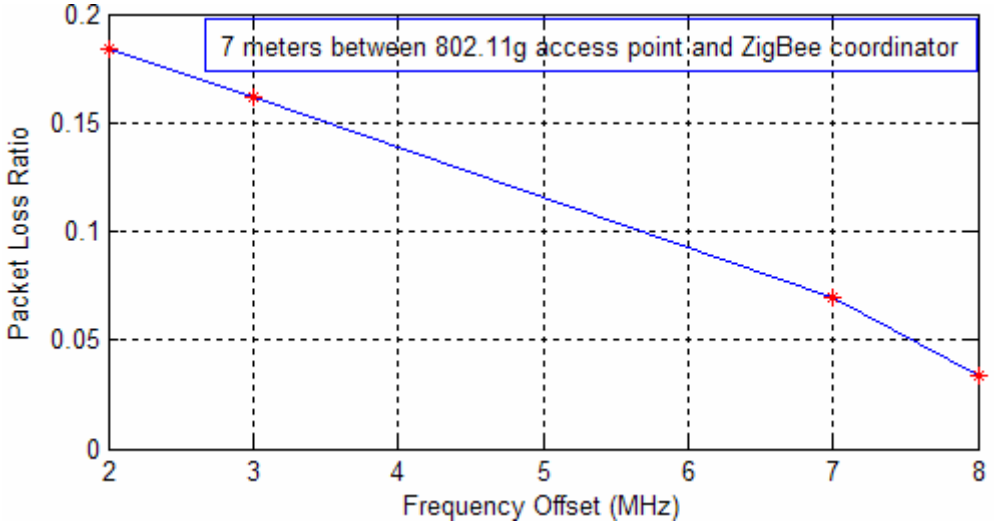

Figure 4-26: Packet loss ratio of test scenario 6

Scenario seven:

ZigBee network uses Channel 18(2440MHz) that is 2MHz offset from the WLAN channel centre frequency. Vary the distances of WLAN access point to ZigBee network coordinator from 1m to 8m to obtain PERs. The PERs are illustrated in Figure 4-26.

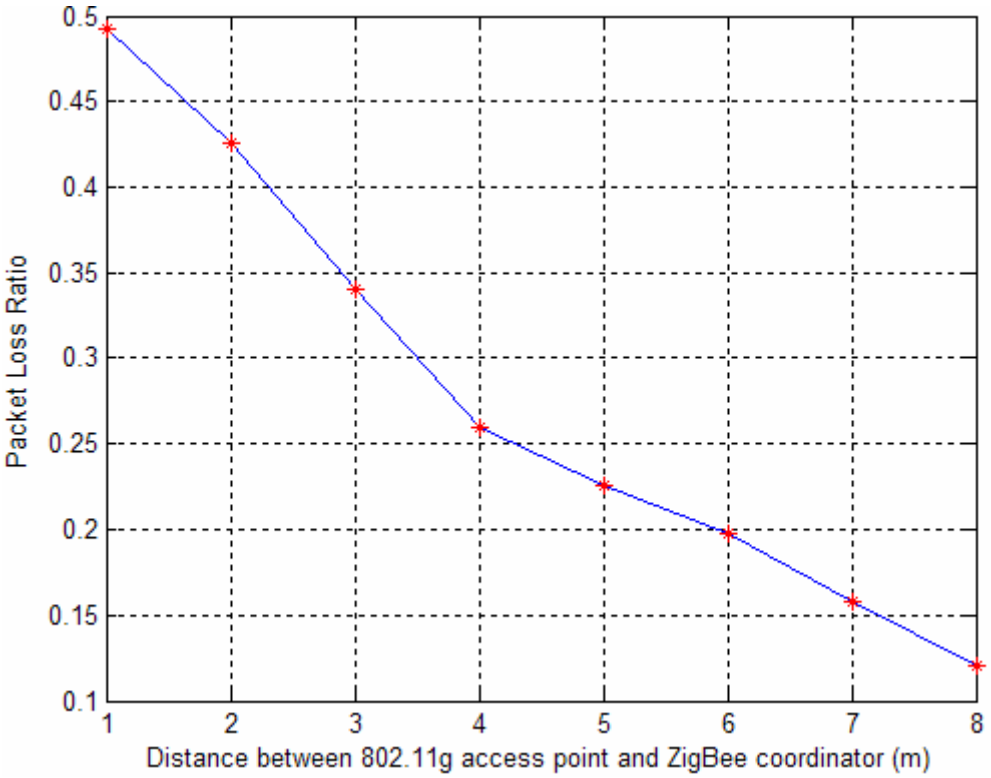

Figure 4-27: Packet loss ratio of test scenario 7 (Frequency offset is 2MHz)

Scenario eight

Investigate ZigBee communication in two Non-overlapping channels with WLAN Channel 7, in this scenario. ZigBee Channel 16 and Channel 21 that have 12MHz and 13 MHz offsets from WLAN Channel 7 centre frequency are used. Distance from WLAN access point to ZigBee coordinator is fixed as 3 meters. (Figure 4-27)

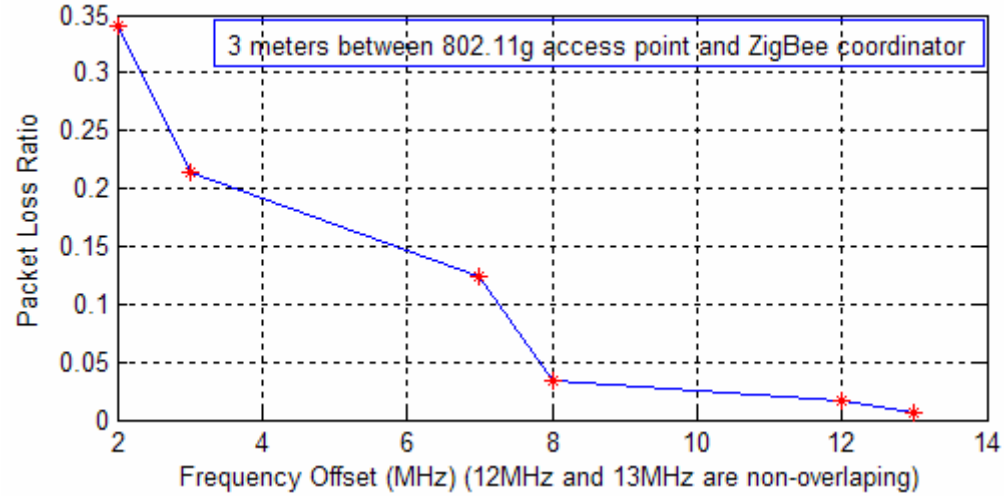

Figure 4-28: Packet loss ratio of test scenario 8

5 Discussions

In this chapter, we discuss ZigBee network performance under WLAN interference from theory analysis to real test observations. Appropriate explanations of our proposed simulation models and the actual measurement results will be given.

First we address the exploratory simulation, explain the results from the quantitative analysis. We discuss our approaches to investigate the interference issues in this thesis, draw the outcomes onto explainable extent.

Secondly, we evaluate ZigBee network performance and analyze the interference issue in terms of frequency offsets and distance. Additionally, the interference that IEEE802.11b brings to ZigBee will be compared with IEEE802.11g.

Finally, other possible parameters which can also be used for the interference issue analysis will be discussed.

5.1 Comparison of simulation and measurement results

Our approaches to investigate the interference issue, in the theoretical analysis we studied probability of ZigBee packet errors under different WLAN interference, while we obtain ZigBee Packet loss in real test since precision of PER could not be achieved and would not be relevant for practical life that ZigBee devices are usually designed for sensor and control networks.

Packet loss could be caused by many factors like network jitter, noise. We specified that the ZigBee packet loss in our real test is caused by collision with WLAN packets. The results from simulation and test can correspond to each other. For instance, when ZigBee network is 3 meters apart from WLAN AP, the simulation and test result shows in Figure 5-1. Packet loss in real test is higher than double PER since our simulation model simplified the transmission.

We considered the ZigBee coordinator was impacted by WLAN interference that result in bit errors happened only in the coordinator received data packets in simulation. This one way transmission model clarifies signal degradation under interference. If we make this to further elaboration, since ZigBee communication usually in short range in real world that WLAN interference powers are gained by both the ZigBee coordinator and ZigBee end devices. The common situation is that the signal degradation happened on both sides. Additionally, WLAN usually utilizes Ad-hoc connection, packets are forwarded within more than one node is not an uncommon situation.

In our constructed test bed, WLAN packets are relayed by the access point, they have been sent twice. This doubly extends the packets transmission, enhances probability of packet error. If we double the duration of each WLAN packet in our simulation model, the simulation results are much closer to the measurement results (Figure 5-2).

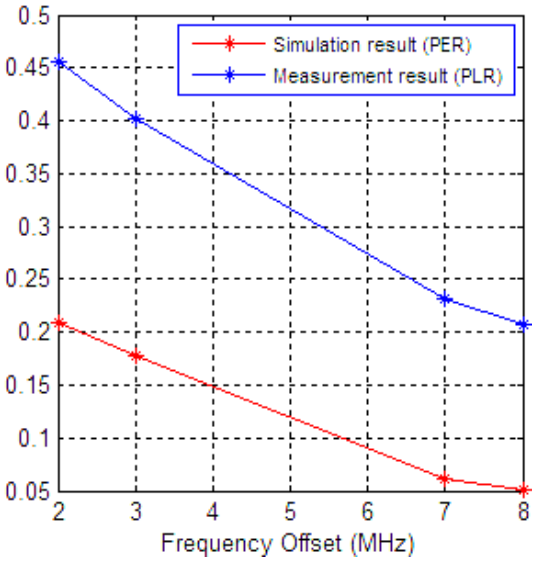

Figure 5-1: Comparison between Simulation and measurement results (3 meters between 802.11b access point and ZigBee coordinator)

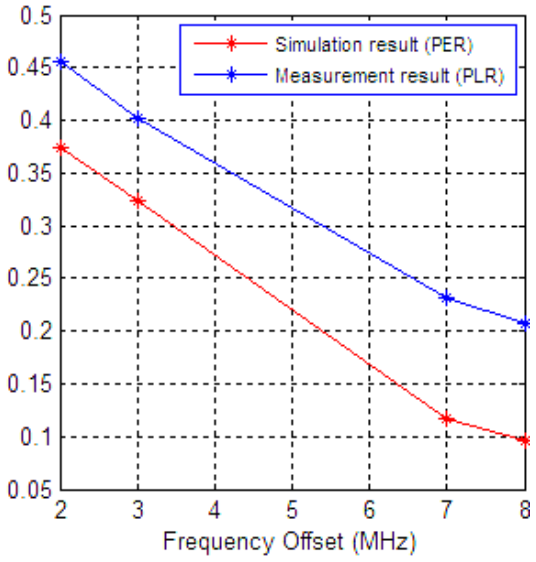

Figure 5-2: Comparison between Simulation (double wlan packet duration) and measurement results (3 meters between 802.11b access point and ZigBee coordinator)

However, after doubling the duration of WLAN packet, the simulation and measurement result still have some difference. The possible reasons are the ACK packets and multiple-fragment of WLAN packets, which we did not take into consideration in the simulation, and they could also make collision increase in real test transmission.

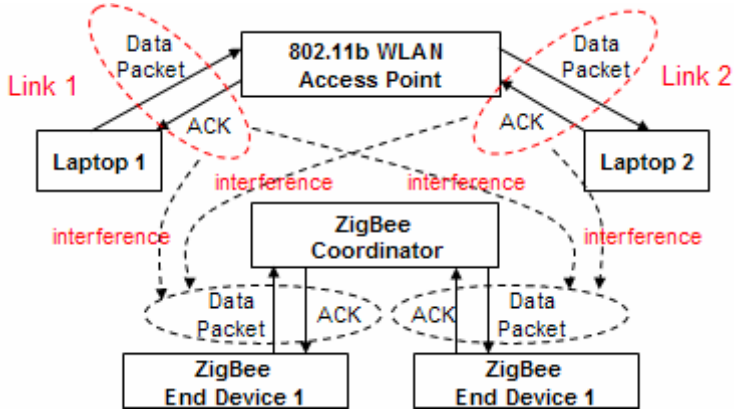

Figure 5-3: General communication processes

We constructed collision time models without taking the WLAN ACK packet into consideration for simplified. In real transmission process in the test, as shown in Figure 5-3, the communication processes within WLAN access point (AP) and its clients is data packets and ACK packets are sent bidirectional in the channel. First Laptop1 send a data packet to the WLAN AP, if the packet is received, a corresponding ACK will be sent back (Link 1). Then the AP forwards the data packet to Laptop2. Laptop2 will response an ACK to the AP if the packet is received successfully (Link 2). So both WLAN data and ACK packets in link1 and 2 are possible to collide with ZigBee data and ACK packets.

Additionally, if we consider about the length of WLAN data packet (i.e. 14000 bytes), fragmentation is possible implemented to increase the reliability during the WLAN transmission. Figure 5-4 shows, the whole WLAN data packet is divided in fragments, and each fragment has a corresponding ACK packet. Consequently, the probability of collision with ZigBee data and ACK packets increase.

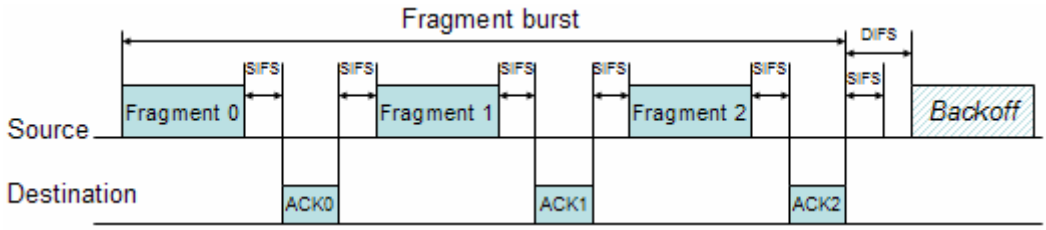

Figure 5-4: Transmission of a multiple-fragment MSDU[31]

Make it more elaboration, the WLAN transmission are also impacted by ZigBee network, the interference between them are mutual. Since the ZigBee network interference, WLAN packets might delay or loss, which cause the durations of those packets increase (Figure 5-5). As aftereffect, the collision time of the two network packets will increase. We would not explain this more deeply since more statistical tests are needed but time is limited.

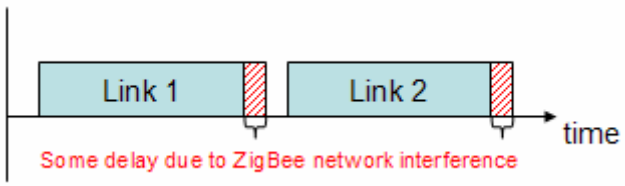

Figure 5-5: WLAN packet duration increase

There was not only packet error but other factors like frequency of packet sending, other unknown noise in the test environment could also make the diversity of the simulation results and test results.

5.2 Relationship between frequency offset and interference power

Put a point of view in frequency domain, signal powers usually concentrate around the centre frequency, and weaken apart from the centre. There are four ZigBee channels overlapping with one WLAN channel as we introduced in chapter 3, they have 2MHz, 3MHz, 7MHz and 8MHz offsets from the WLAN channel frequency respectively. We investigate ZigBee network PER under transmitter power fixed WLAN signals. The ZigBee channel with 2MHz offset is the closest to the WLAN channel centre frequency, that makes it gains most interference. The 8MHz offset channel gains least impact as an overlapping channel can prove that interference power weakens when more part from its centre. The non-overlapping channels gains very seldom interference power, when we set WLAN based on 802.11b, the non-overlapping channel do no have any PER at all, when we set WLAN based on 802.11g, the PER less than 10^{-2}.

The non-overlapping channel seldom gains impact even not at all if we set WLAN transmitter power certain low. In one word, the frequency offset is larger, the interference power is smaller, and the impact is less.

5.3 Relationship between distance and interference power

Distance of ZigBee devices apart from the WLAN access point is another element that impact interference power. We captured the ZigBee coordinator received signal power every time when it receives data packet from an end device. The receiver powers include ZigBee signal power at receiver, WLAN interference power the receiver gains and other noise in the test environment. We measure the power as RSSI (received signal strength indication).

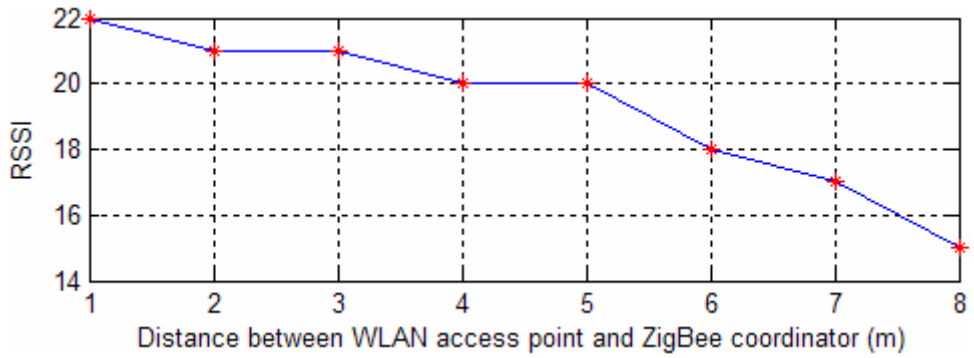

Figure 5-6: Received signal strength indication at ZigBee coordinator

Figure 5-6 indicates that in out test, with the ZigBee coordinator being apart from the WLAN AP from 1 meter to 8 meters, the RSSI decreases from 22dBm to 15dBm. In

other words, longer distance between ZigBee devices and WLAN AP, less interference power are received in the ZigBee devices.

5.4 Comparison of IEEE802.11b and IEEE802.11g as ZigBee network interference

Both IEEE 802.11b and 802.11g operate on 2.4GHz frequency band and it is believed that they are alternatively used in real world transmission. IEEE specified their modulation schemes in PHY layer and defined their data rate, throughput and other parameters. We configured our WLAN to use both of them in test scenarios.

- **Data rate:**

As a straightforward result, WLAN data rate gets obvious increase from value around 310 kbps to 700 kbps in our test when we shift from 802.11b to 802.11g. The change of packet rate correspondingly impact the collision time of two networks' packets.
One packet duration in our test:
ZigBee: *8*126/250000=0.004032s*
WLAN 802.11b: *8*1400/300000=0.037333s*
WLAN 802.11g: *8*1400/800000=0.014s*

Since 802.11g packet duration is less than 802.11b packet duration, ZigBee packet loss ratio would reduce. As our observation illustrates, in the overlapping channels, ZigBee network perform better when WLAN based on 802.11g.

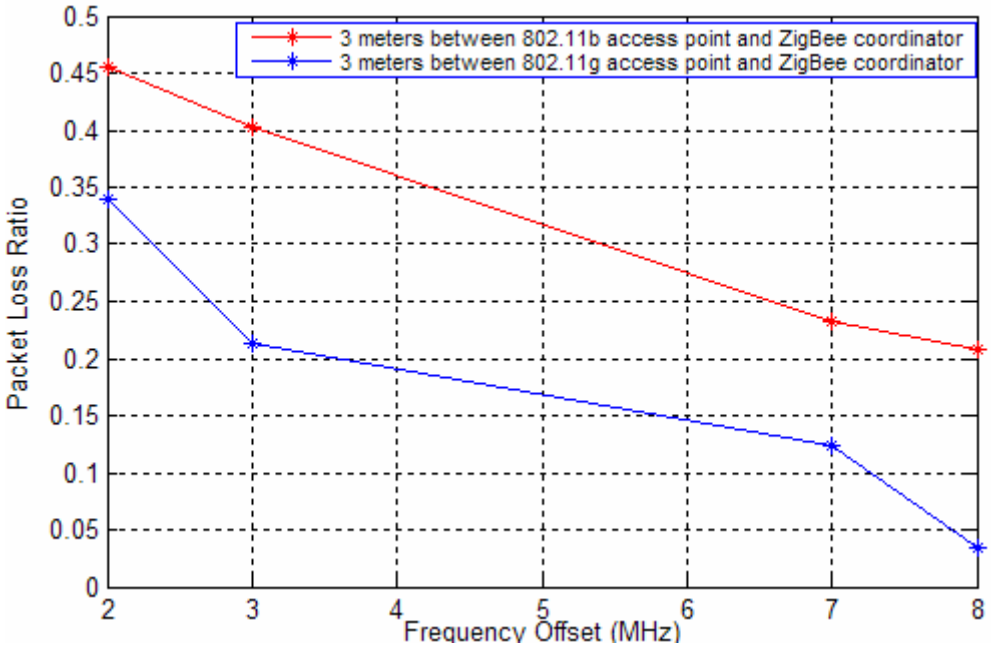

Figure 5-7: Comparison of ZigBee network performance under WLAN 802.11b/g with 3 meters distance

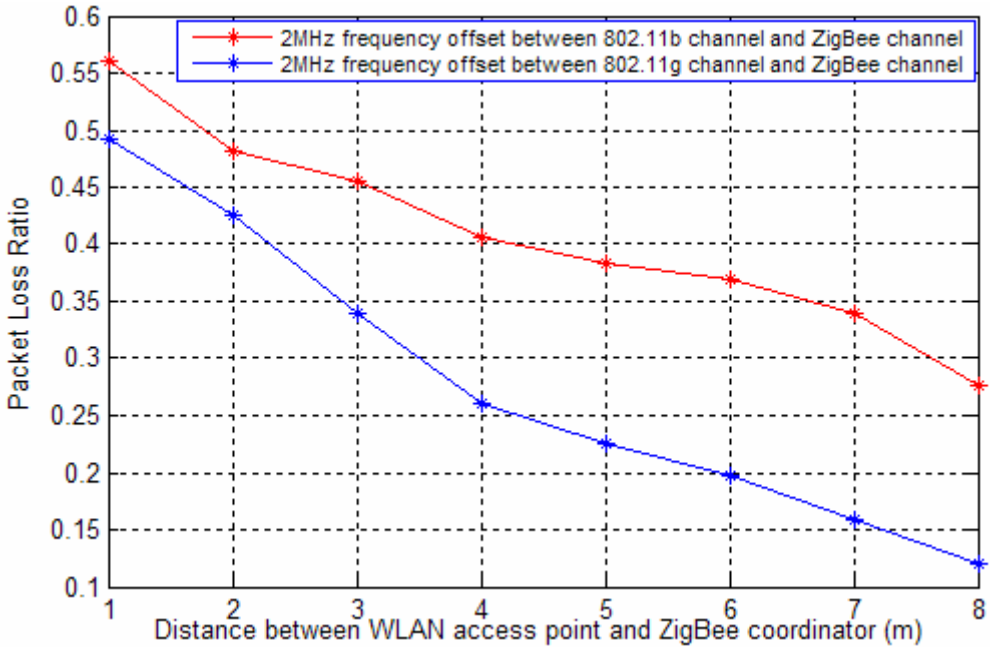

Figure 5-8: Comparison of ZigBee network performance under WLAN 802.11b/g with 2MHz frequency offset

➢ **Power density:**

Another straightforward phenomenon is that IEEE 802.11b and 802.11g have their own power densities since they adopt DSSS and OFDM respectively.

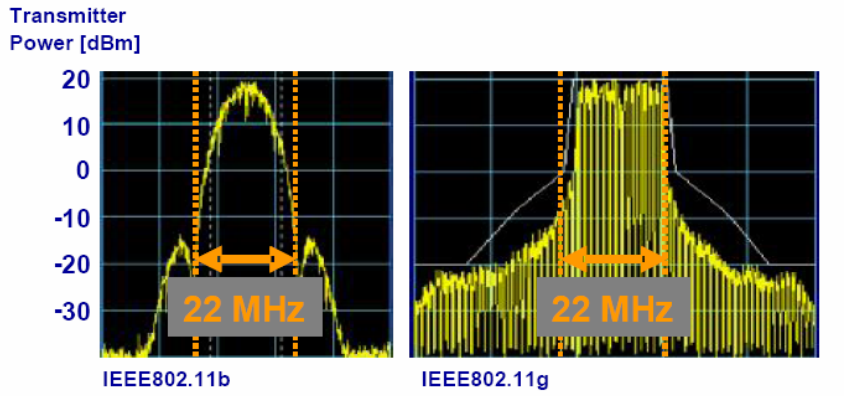

Figure 5-9: Power density of IEEE 802.11b and IEEE 802.11g [16]

802.11g has more slopes outside the 22MHz band, while 802.11b is neater outside of its 22MHz band.

Our test approved that there is no packet loss in non-overlapping channels when ZigBee network under 802.11b interference, but PER exist in non-overlapping channels when ZigBee network under 802.11g interference.

5.5 Other possible parameters used for interference issue analysis

We take PER as a primary approach to investigate the interference since we take the PHY layer transmission, packet length, data rate as variables. There are many other parameters can be used for the evaluation of a network Quality of Services, such as throughput, transmission delay, but there are not considered in this thesis.

5.6 Practical solution

After the research of interference issue between ZigBee network and WLAN, some recommendations in the real coexistence environment are listed below.

- **d_{ac}: distance between WLAN access point (AP) and ZigBee coordinator**

When d_{ac} is shorter than 3 meters, the impact WLAN causes to ZigBee network is serious. The interference is not serious if ZigBee coordinator is at 8 meters or more distance from WLAN AP.

- **frequency offset**

For 802.11b, when the centre frequency offsets are 2, 3, 7, 8MHz, in other words, WLAN and ZigBee channels are overlapping, the interference exists. Especially, ZigBee channel 12, 13, 18, 19, 24 and 25 are not suitable choices in the coexistence environment.

- **ZigBee devices close to AP or WLAN stations**

If ZigBee devices have to be set close to AP or WLAN stations, the best solution to mitigate interference is using the non-overlapping channels.

6 Conclusions

In this thesis, the performance of ZigBee network that operating in the 2.4GHz ISM band are investigated and evaluated based on simulated IEEE 802.15.4 transmissions and real tests of ZigBee devices. Packet error rate (PER) and Packet loss ratio are used as evaluation parameters of the performance.

From simulation and test results, we obtained conclusions below:
The centre frequency offset and the distance between WLAN access point (AP) and ZigBee coordinator (d_{ac} is used to stand for this distance in the following text) are significant for ZigBee network Quality of Services.

In the overlapping channels, take 2MHz frequency offset to illustrate:
The simulation result indicates that when the d_{ac} is less than 2 meters, the PER is quite high and up to 100% when d_{ac} equals to 1 meter. In real test, ZigBee network is hard to manage communication when the coordinator closes to WLAN AP less than 2 meters. When the distance is 3 meters or more than 3 meters, the PER would decrease with the increased d_{ac}.

One WLAN channel overlaps with four ZigBee channels. If ZigBee network operates on one of those four channels, it would be subjected to obvious interference. Different offsets gain different interference, 45.6%, 40.2%, 23.2% and 20.8% packets are lost with 2MHz, 3MHz, 7MHz and 8MHz offsets respectively, when WLAN based on 802.11b and d_{ac} is 3 meters. 34%, 21.4%, 12.4% and 3.4% packets are lost with 2MHz, 3MHz, 7MHz and 8MHz offsets respectively, when WLAN based on 802.11g and distance is 3 meters. In other words, the bigger frequency offset is, the less packet loss will be, and the influence 802.11g brings to ZigBee network is less than 802.11b.

In the non-overlapping channels, if interference comes from WLAN based on 802.11b, it does not impact the ZigBee network, while if WLAN based on 802.11g, the interference impacts the two closest non-overlapping channels, there are 1.6% and 0.6% packets would be lost when ZigBee works on the channels which are 12 MHz and 13MHz centre offsets from the WLAN channel. As a consequence, to minimize the interference of a 802.11b WLAN and ZigBee coexistence environment, ZigBee channel 15 (2425MHz), 16 (2430MHz), 21 (2455MHz) and 23 (2460MHz) can be used.

In this thesis, we approach an exercisable study way to investigate interference issue of two coexisted network. We successfully achieve our tasks that explore ZigBee network performance under WLAN interference. Since our test results can match our simulated results, that the WLAN interference to ZigBee network could get reasonable explanations from this thesis.

7 Future works

In this thesis, ZigBee network was simplified to a one end device communicate with coordinator. ZigBee network could be more complex even cluster tree topology network. It could be taken into consideration that set more ZigBee nodes in one ZigBee network to investigate their performance. Since there only 4 channels are non-overlapping with WLAN 802.11 when the three non-overlapping WLAN channels are using at same time, it has limitation. This part could be taken as further work in future.

On other hand, the results from this thesis and the way to obtain PER could subject for research and development in ZigBee field. Especially, when it is required to consider that ZigBee network operates in WLAN environment, or two of them working on one terminal, this thesis would be usable.

Reference

[1] Official IEEE 802.11 working group project timelines (18/11/07), retrieved on 2007-11-18.
Available: http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm
Reviewed date: 11/12/2007
[2] Wikipedia, IEEE 802.11.
Available: http://en.wikipedia.org/wiki/IEEE_802.11
Date reviewed: 11/12/2007
[3] IEEE Std.802.11b-1999, IEEE standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band
[4] IEEE 802.11b White Paper, VOCAL Technologies, Ltd. 2003-10
[5] Wikipedia, PSK.
Available: http://en.wikipedia.org/wiki/Phase-shift_keying
Reviewed date: 04/01/2008
[6] Wikipedia, IEEE 802.11g.
Available: http://en.wikipedia.org/wiki/IEEE_802.11g
Reviewed date: 11/12/2007
[7] IEEE Std. 802.11g™-2003, IEEE Standard for Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band
[8] IEEE 802.15 Working Group for WPAN homepage.
Available: http://www.ieee802.org/15/
Reviewed date: 09/12/2007
[9] 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 (LR-WPANs), 2003
[10] OQPSK introduction, waveform description
Available: http://www.hoka.com/th/TH_waveformdescription.pdf
Reviewed date: 05/01/2008
[11] IEEE Std.P802.22/D0.1: Draft Standard for Wireless Regional Area Networks Part 22：Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) specifications：Policies and procedures for operation in the TV Bands.
[12] MAC functional-Superframe Structure
Available: http://alkautsarpens.wordpress.com/2008/01/28/superframe-structure-2/
Reviewed date: 16/04/2008
[13] ZigBee: Wireless Control That Simply Works, William C.Craig, Program Manager Wireless Communication, ZMD America, Inc
[14] Wikipedia, ZigBee
Available: http://en.wikipedia.org/wiki/Zigbee

Reviewed date: 11/12/2008
[15] ZigBee Technology: Wireless Control that Simply Works, Patrick Kinney, Kinney Consulting LLC, Chair of IEEE 802.15.4 Task Group, Secretary of ZigBee BoD, Chair of ZigBee Building Automation Profile WG
[16] GPS, Fleet Management and Vehicle Tracking Glossary
Available: http://www.discretewireless.com/products/Glossary/glossary.asp
Reviewed date: 03/04/2008
[17] BGR, "WLAN Interference with IEEE802.15.4", 16-03-2007, z-wave alliance
[18] IEEE Std.802.15.2: IEEE standard for Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands, 2003
[19] ZigBee and wireless radio frequency coexistence, ZigBee Alliance, June 2007
[20] Soo Young Shin, Hong Seong Park and 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, v.51 n.12, p.3338-3353, 2007
[21] Soo Young Shin, Hong Seong Park, Sunghyun Choi, Wook Hyun Kwon, "Packet Error Rate Analysis of ZigBee under WLAN and Bluetooth Interferences", IEEE Transactions on Wireless Communications, VOL.6, NO.8, AUGUST 2007
[22] Nada Golmie, Frederic Mouveaux," Interference in the 2.4 GHz ISM Band: Impact on the Bluetooth Access Control Performance"
[23] Simon Haykin and Michael Moter, "Modern Wireless Communications", International edition
[24] Soo Young Shin, Hong Seong Park, Sunghyun Choi, and Wook Hyun Kwon, "Packet error rate analysis of IEEE 802.15.4 under IEEE 802.11b interference" in Proc.Wired/Wireless Internet Commun., May 2005, pp. 279–288.
[25] Wikipedia Atmel
Available: http://en.wikipedia.org/wiki/Atmel
Reviewed date: 20/03/2008
[26] Wikipedia AVR Atmel
Available: http://en.wikipedia.org/wiki/Atmel_AVR
Reviewed date: 20/03/2008
[27] AVR 8-Bit RISC-IEEE 802.15.4/ZigBee, Atmel homepage
Available: http://www.atmel.com/products/zigbee/
Reviewed date: 20/03/2008
[28] AVR Z-Link for IEEE 802.15.4 and ZigBee Applications
[29] Low Power 2.4 GHz Radio Transceiver for ZigBee TM and IEEE 802.15.4 TM Applications AT86RF230
[30] ATAVRRZ200 Demonstration Kit AT86RF230 (2450 MHz band) Radio Transceiver User Guide
[31] IEEE Std. 802.11™-2007 (Revision of IEEE Std 802.11-1999): IEEE standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications. 12 June 2007
[32] Newbie's guide to AVR development, an introduction intended for people with no prior AVR knowledge. AVRFREAKS.NET July 2002