PERFORMANCE STUDY FOR CO-EXISTING WI-FI AND ZIGBEE SYSTEMS AND DESIGN OF INTEROPERABILITY TECHNIQUES

BY

Yong Tang

Thesis submitted to the

Faculty of Graduate and Postgraduate Studies

In partial fulfillment of the requirements

For Master of Applied Science degree in

Electrical and Computer Engineering

School of Electrical Engineering and Computer Science

Faculty of Engineering

University of Ottawa

Abstract

WIRELESS local area networks (WLANs) and wireless sensor networks (WSNs) technologies have been comprehensively developed and deployed during recent years. Since commercial WLAN and WSN products share the same free of license frequency band, the low power, low rate ZigBee based WSNs are vulnerable to the interference from Wi-Fi WLANs. Therefore, it is important to evaluate the performance of ZigBee WSNs that are subjected to interference generated by collocated Wi-Fi WLANs and to design effective counter-measuring techniques should performance improvement is needed. In this research, a versatile testbed for conducting various experiments is established and the ZigBee system's performance with different clear channel assessment (CCA) modes and energy detection (ED) thresholds are evaluated through extensive experimental measurements in the testbed. It can be concluded from the results that CCA has significant impact on ZigBee's performance. An existing theoretical analysis approach that is based on the collision time model between ZigBee and Wi-Fi packets is suitably modified to provide analytical evaluation means of the cases we examined. In order to mitigate the interference from the collocated Wi-Fi system, a novel and effective interference-aware adaptive CCA (IAACCA) scheme is proposed and implemented as firmware flashed into Crossbow motes. Experiments confirmed the ability of IAACCA to countermeasure effectively interference generated by Wi-Fi and thus improve the performance of ZigBee WSNs. Finally, a thorough statistical analysis is performed to understand the factors impacting the performance of ZigBee system and is used to further verify our experimental methods.

Table of Contents

Abstract i

Table of Contents ii

List of Figures v

List of Tables viii

List of Symbols ix

Acronyms x

Acknowledgement xii

Chapter 1 Introduction 1

1.1 Introduction to Wireless Sensor Networks 3

1.1.1 Wireless Sensor Networks: Overview 3

1.1.2 Characteristics of Wireless Sensor Networks 8

1.1.3 Technical Challenges of WSN 9

1.2 Research Motivations and Objectives 11

1.2.1 Research Motivation 11

1.2.2 Research Objectives 14

1.3 Research Contributions 14

1.4 Thesis Organization 15

Chapter 2 Technical Background 17

2.1 Overview of IEEE 802.15.4 and ZigBee Standards 19

2.1.1 IEEE 802.15.4 Standard 20

2.1.1.1 IEEE 802.15.4 PHY Layer 20

2.1.1.2 IEEE 802.15.4 MAC Sublayer 22

2.1.1.3 IEEE 802.15.4 Topologies 23

2.1.2 ZigBee Standard 25

2.2 Overview of Wi-Fi/IEEE 802.11 Standards.. 27

2.2.1 IEEE 802.11 PHY Layer 28

2.2.2 IEEE 802.11 MAC Sublayer 30

2.2.3 IEEE 802.11/Wi-Fi Authentication 33

2.2.4 IEEE 802.11/Wi-Fi Network Topology.. 35

2.3 IEEE 802.15.4 CSMA/CA and CCA Mechanisms Overview.. 36

2.3.1 IEEE 802.15.4 CSMA/CA Algorithm.. 36

2.3.1.1 IEEE 802.15.4 slotted CSMA/CA Algorithm 38

2.3.1.2 IEEE 802.15.4 Unslotted CSMA/CA Algorithm.. 40

2.3.2 IEEE 802.15.4 CCA Mechanism.. 41

Chapter 3 Related Work on Coexistence Issues and Interoperating Techniques 44

3.1 Study of Coexistence issues between ZigBee/IEEE 802.15.4 WSNs and IEEE 802.11b/g/n WLANs.. 46

3.1.1 Coexistence Issues between WSNs and WLANs 47

3.1.2 Experimental and Simulative Study of Coexistence Issues.. 48

3.1.2.1 Implemented Testbeds 48

3.1.2.2 Performance Evaluation of WSN under WLAN Interference 50

3.1.3 Coexistence Model between ZigBee and Wi-Fi Packets.. 53

3.2 Performance Study on the IEEE 802.15.4 CCA Mechanism.. 56

3.3 Adaptive Mechanisms for Interference Mitigation 59

3.3.1 Frequency Agility Algorithm.. 60

3.3.1.1 Interference Detection Scheme.. 60

3.3.1.2 Interference Avoidance Scheme.. 61

3.3.2 CCA/MAC Parameter Adjustment Mechanisms 64

3.3.3 Collaborative Coexistence Mechanism 67

Chapter 4 Close Examination of CCA and its Corresponding Adaptation Mechanism 70

4.1 Testbed Description 71

4.1.1 Testbed Hardware 72

4.1.2 Testbed Software 73

4.1.3 Testbed Setup 77

4.2Experimental Results and Corresponding Analysis 80

4.2.1 Experimental Study of Different CCA Thresholds and Modes 81

4.2.2 Analysis of Experimental Results 87

4.3 Adaptation Mechanism for Improving Performance 93

Chapter 5 Interference Aware Adaptive CCA Mechanism: Description and Validation 99

5.1 IAACCA Mechanism and its advantages/open issues 101

5.1.1 IAACCA Mechanism Description 101

5.1.2 Advantages Achieved by IAACCA and Remaining Open Issues 107

5.2 Performance Evaluation Results and Discussion 110

5.3 Statistical Analysis of ZigBee Packet Transmission 121

5.3.1 ZigBee Packet Transmission Scenarios 121

5.3.2 Results and Analysis for ZigBee Packet Transmission 128

Chapter 6 Conclusions and Future Work 138

6.1 Conclusions 138

6.2 Future Work 140

Reference 142

List of Figures

Fig.1.1 Structure of a WSN Node[12] 4

Fig.1.2 The Architecture of WSNs[12].. 6

Fig.1.3 RF Spectrum allocation for ZigBee and Wi-Fi... 12

Fig.2.1 ZigBee/IEEE 802.15.4 protocol stack [55] 19

Fig.2.2 IEEE 802.15.4 Operating Frequency Bands [2] 21

Fig.2.3 IEEE 802.15.4 PPDU Structure [57]... 21

Fig.2.4 IEEE 802.15.4 MPDU structure [58]... 22

Fig.2.5 IEEE 802.15.4 Network Topologies [56].. 24

Fig.2.6 IEEE 802.11b/g Operating Frequency Band [74].. 30

Fig.2.7 IEEE 802.11 MAC Frame Format [49].. 30

Fig.2.8 IEEE 802.11 MAC structure [49].. 31

Fig.2.9 IEEE 802.11 basic access method [49] 32

Fig.2.10 Typical Components of a Wi-Fi Network [71] 36

Fig.2.11 IEEE 802.15.4 MAC sublayer superframe structure [57] 38

Fig.2.12 IEEE 802.15.4 CSMA/CA Algorithm [86] 41

Fig.3.1 A Typical Testbed for Coexistence Study of ZigBee and Wi-Fi Communication System [96]... 49

Fig.3.2 A Testbed for Coexistence Study of ZigBee and Wi-Fi Networks [89].......................... 50

Fig.3.3 Packets Transmission of IEEE 802.11b and IEEE 802.15.4[100]................................ 54

Fig.3.4 Time Collision Model between IEEE 802.11b Packet and IEEE 802.15.4 Packet [99] . 56

Fig.3.5 Flowchart of: (a) interference detection and (b) interference avoidance [101]. 63

Fig. 4.1 Testbed' s Architecture 79

Fig. 4.2 ZigBee performance at a rate of 100 packets/second with different ED thresholds under interfering UDP traffic with payload of 1000 bytes/segment and rate of 1000 segments/second 83

Fig. 4.3 ZigBee performance at a rate of 100 packets/second with different ED thresholds under interfering UDP traffic with payload of 5000 bytes/segment and rate of 200 segments/second. 84

Fig. 4.4 ZigBee performance at a rate of 20 packets/second with different ED thresholds under interfering UDP traffic with payload of 1000 bytes/segment and 1000 segments/second.86

Fig. 4.5 ZigBee performance at a rate of 20 packets/second with different ED thresholds under interfering UDP traffic with payload of 5000 bytes/segment and 200 segments/second.... 86

Fig. 4.6 Interference Model between ZigBee and WLAN Frames 88

Fig. 4.7 PLR as a function of ED thresholds under interfering IEEE 802.11g UDP traffic with payload of 1500 bytes/segment and 500 segments/second........ 94

Fig. 4.8 PLR as a function of ED thresholds under interfering 802.11g UDP traffic with payload of 3000 bytes/segment and 250 segments/second........ 95

Fig.4.9 PLR comparison under mixed interfering UDP traffic1 97

Fig. 4.10 PLR comparison under mixed interfering UDP traffic2 97

Fig. 5.1 The new channel assessment process........ 101

Fig. 5.2. ZigBee PLR perfomance with & without IAACCA, in the presence of different Wi-Fi interference with packet sizes of 1000bytes (test 1), 1500 bytes (test 2), 2000bytes (test 3). 113

Fig. 5.3. ZigBee PLR perfomance with & without IAACCA, in the presence of different Wi-Fi interference with packet generationg rates of 300 packets/second (test 4), 400 packets/second (test 5), 600 packets/second (test 6). 113

Fig. 5.4. ZigBee PLR perfomance with & without IAACCA, in the presence of different Wi-Fi interference with random IPT following Uniform distribution (test 7) and Exponential distribution (test 8). 114

Fig. 5.5. ZigBee PLR perfomance with & without IAACCA, in the presence of different Wi-Fi interference with random packet sizes following Uniform distribution (test 9), Exponential distribution (test 10) and Normal distribution (test 11). 115

Fig. 5.6. ZigBee PLR perfomance with & without IAACCA, in the presence of different Wi-Fi interference with random IPT and random packet size both following Uniform distributions. 115

Fig. 5.7. ZigBee PLR perfomance of 10ms IPT with & without IAACCA, in the presence of different Wi-Fi interference with packet sizes of 1000bytes (test 13), 1500 bytes (test 14), 2000bytes (test 15). 116

Fig. 5.8. ZigBee PLR perfomance of 10ms IPT with & without IAACCA, in the presence of different Wi-Fi interference with packet generationg rates of 300 packets/second (test 16), 400 packets/second (test 17), 600 packets/second (test 18).. 117

Fig. 5.9. ZigBee PLR perfomance with & without IAACCA, in the presence of different Wi-Fi interference with random IPT following Uniform distribution (test 19) and Exponential distribution (test 20). 117

Fig. 5.10. ZigBee PLR perfomance of 10ms IPT with & without IAACCA, in the presence of different Wi-Fi interference with random packet sizes following Uniform distribution (test 21), Exponential distribution (test 22) and Normal distribution (test 23). 118

Fig. 5.11. ZigBee PLR perfomance of 10ms IPT with & without IAACCA, in the presence of different Wi-Fi interference with random IPT and random packet size both following Uniform distributions. 118

Fig. 5.12 ZigBee perfomance comparison under interfering Wi-Fi traffic mixed of two different packet rates for IAACCA and default CCA respectively. 120

Fig. 5.13 Scenario of successful first data transmission attempt. 123

Fig. 5.14 Scenario of lost acknowledgement... 123

Fig. 5.15 Scenario of lost acknowledgement and failed retransmission. 124

Fig. 5.16 Scenario of lost first data packet and successful in retransmission.......................... 125

Fig. 5.17 Scenario of lost first packet, successful retransmission and lost acknowledgement.. 125

Fig. 5.18 Scenario of failed in both data transfer attempts.. 126

Fig. 5.19 Scenario of failed in the first data transmission attempt due to CCA detection failure. 126

Fig. 5.20 Scenario of lost acknowledgement and failed data retransmission attempt due to CCA detection failure. 127

Fig. 5.21 Scenario of failed in the first packet transmission attempt and retransmission cancelled due to CCA detection failure. 127

Fig. 5.22 Scenario of packet failed due to TXFIFO overflow. 128

Fig. 5.23 The number of retransmission for default CCA and IAACCA................................ 137

List of Tables

Table 5.1 List of IAACCA Parameters 102

Table 5.2 IAACCA experimental parameters 110

Table 5.3 Testing results for packet transmission using default CCA with ZigBee IPT = 20ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second........ 132

Table 5.4 Number of occurrence for each scenario for default CCA with ZigBee IPT = 20ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second........ 133

Table 5.5 Testing results for packet transmission using IAACCA with ZigBee IPT = 20ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second........ 134

Table 5.6 Number of occurrence for each scenario for IAACCA with ZigBee IPT = 20ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second. 134

Table 5.7 Testing results for packet transmission using default CCA with ZigBee IPT = 50ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second........ 135

Table 5.8 Testing results for packet transmission using IAACCA with ZigBee IPT = 50ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second........ 135

Table 5.9 Number of occurrence for each scenario for default CCA with ZigBee IPT = 50ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second........ 136

Table 5.10 Number of occurrence for each scenario for IAACCA with ZigBee IPT = 50ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second........ 136

List of Symbols

c Empirical coefficient for comparing packet transmission duration

ds the distance between the IEEE 802.15.4 transmitter and receiver

dr the distance between the IEEE 802.11b interferer and the interfered IEEE 802.15.4 receiver

L_{wk} the Wi-Fi packet's transmission time (k = 1, 2)

L_z ZigBee packet's transmission time

L_p UDP segment payload in terms of bytes

N Number of channel assessment periods in one full cycle of channel assessment

N_d Number of RSSI readings in one estimation of channel's idle length period

N_s Number of idle RSSI readings required for starting packet transmission

N_i Number of instruction packets used in the hand-shaking mechanism for channel switching

N_{s_low} Lower bound for N_s

N_{s_high} Upper bound for N_s

N_{max} Maximum number of RSSI readings allowed for the proposed sending mechanism in IAACCA

P_b bit error rate without Wi-Fi interference

P_b^I the bit error rate with Wi-Fi interference

P_{th} ED threshold

T_{wk} the constant Wi-Fi packet inter-departure time

T_c he time duration ZigBee and Wi-Fi packets overlap

T_{MPDU} transmission duration of MPDU of Wi-Fi frame

T_{ACK} transmission duration of Wi-Fi ACK frame

T_{ca} Time interval between two full cycles of channel assessment

t_a the offset time between the initiation of the transmission of a ZigBee packet and the initiation of the transmission of a Wi-Fi packet

t_b the duration of a bit transmission

t_s Time interval between two consecutive RSSI readings

t_{ins} Time interval for sending instruction packet

Acronyms

ACK	acknowledgement
ADAPT	ADaptive Access Parameters Tuning
AODV	Ad hoc On Demand Distance Vector
AP	access point
ASIC	Application Specific Integrated Circuit
BER	bit error rate
BroadWIRLab	Broadband Wireless and Internetworking Research Laboratory
BSS	basic service set
CAP	Contention Access Period
CCA	clear channel assessment
CCAP	clear channel assessment period
CCK	Complementary Code Keying
CFP	Contention Free Period
DIFS	DCF Inter Frame Space
CPR	constant packet rate
CRC	cyclic redundancy check
CS	carrier sense
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CTS	Clear–To–Send
DCF	Distributed Coordination Function
DSN	data sequence number
DSSS	direct sequence spread spectrum
EAP	Extensible Authentication Protocol
ED	energy detection
EDCA	Enhanced Distributed Channel Access
EL	estimation of length
ESS	extended service set
FCS	frame check sequence
FCC	Federal Communication Commission
FFD	Full-Function device
FHSS	Frequency Hopping Spread Spectrum
GTS	guaranteed time slots
HART	Wireless Highway Addressable Remote Transducer
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
IAACCA	Interference Aware Adaptive Clear Channel Assessment
IBSS	independent basic service set

IDT	inter-departure time
IFS	inter–frame space
IPT	inter-packet time
IR	Infrared
ISA	International Society of Automation
ISM	Industrial, Scientific, and Medical
LQI	link quality indication
LTE	long term evolution
MEMS	Micro-Electro-Mechanical Systems
MIMO	Multiple Input Multiple Output
MPDU	MAC protocol data unit
OFDM	orthogonal frequency-division multiplexing
OSI	Open System Interconnection
PCF	Point Coordination Function
PCR	packet collision rate
PDR	packet dropping rate
PIFS	PCF Inter Frame Space
PLR	packet loss rate
PPDU	PHY protocol data unit
PSDU	PHY service data unit
QoS	quality of service
RFD	Reduced-Function device
RTS	Request-To-Sent
RSSI	Receiver Signal Strength Indicator
SCM	spatial channel model
SIFS	Short Inter Frame Space
SS	spectrum sensing
UDP	user datagram protocol
WBAN	wireless body area network
WEP	Wireless Equivalent Privacy
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	wireless local area network
WMSN	wireless multimedia sensor network
WPA	Wireless Protected Access
WPAN	wireless personal area network
WR	wireless router
WSN	wireless sensor network
WSSN	wireless smart sensor network
ZC	ZigBee coordinator
ZED	ZigBee end device
ZR	ZigBee router

Acknowledgement

I am heartily thankful to Dr. Zhipeng Wang who was my direct lead during the entire research. His experience and wisdom enlightened our project and my career life, and also he has provided me numerous suggestions and help both on my work and life.

The same gratitude is given to my supervisor, Prof. Dimitrios Makrakis and Prof. Hussein Mouftah, whose encouragement, guidance and support from the initial to the final level contributed to the successful completion of this research work. Also, the funding provided through the Wisense RE-ORF project is acknowledged which allowed me to focus on my research full-heartedly.

I would like to thank Mr. Tianyu Du for his kind help to complete the many and time consuming experiments and the valuable suggestions he provided during discussions.

I also thank my friends and colleagues in the Broadband Wireless and Internetworking Research Laboratory (BroadWIRLab) for their encouragement and their will to assist whenever I needed assistance.

Last but not least, I owe to express my special gratitude to my parents whose support and love always gave me courage to face any challenges in my life.

Chapter 1

Introduction

The fast expansion and utilization of wireless communication technology can be dated back to the mid-20th century. Particularly since the last quarter of the 20th century, the advancement of wireless technology exploded due to the reality of the great needs for user and application mobility in modern society [1]. Nowadays, wireless technologies have been incorporated into various communication and networking applications embedded in many military, industrial and civilian products. From the perspective of network coverage, the wide area coverage can be provided through various technologies, such as satellite networks, comprehensively deployed 2G/3G wireless cellular networks, WiMAX (Worldwide Interoperability for Microwave Access) targeting metropolitan area coverage and LTE (Long Term Evolution) which is an evolutionary technology test evolving from 3G to 4G technology. Cellular network can establish 1-2km diameter wide cells. Each cell is working cooperatively with its neighboring cells through established call hand-off algorithms to create a seemingly seamless network [1]-[3].

During the mid-1980s, it turned out that an even smaller coverage area cell was needed to accommodate the fast growing traffic. Smaller size cells increase the frequency reuse factor, thus increase the network's capacity per square meter. This gave birth to the micro-cell and pico-cellular networks [4]. However the hunger for higher capacity volume continues, at present the industry is working on the development of femto-cell cellular networks [5]. Starting later but growing faster was the evolution of wireless technology for local area coverage. Its fast market penetration can be attributed to the fast development of a globally accepted standard, known as IEEE 802.11. This generated the era of Wireless Local Area Networks (WLANs), which are gradually removing the IEEE 802.3 (Ethernet) from the dominance of LAN market, a position it held for several decades. In the meanwhile wireless technology is entering new areas of application, generating new technologies, such as Wireless Personal Area Networks (WPANs), Wireless Body Area Networks (WBANs), ad hoc mobile networks, and Wireless Sensor Networks (WSNs).

Different from WLANs which are concerned with features such as Ethernet matching speed, "long" coverage range (e.g. 100m), ability to handle seamless roaming, message forwarding, and relatively high data throughput, WPANs focus on the space around a person or object that typically extends up to 10m in all directions. The aims of WPANs are low-cost, low power, short range and very small size. The IEEE 802.15 working group was formed to create WPAN standards, which has currently defined three classes of WPANs that are differentiated by data rate, battery drain and quality of service (QoS) capabilities [2]: 1) High data rate WPANs (IEEE 802.15.3) that require very high speed and strong QoS support, and are normally used for multimedia applications; 2) Medium data rate WPANs (IEEE 802.15.1/Bluetooth) that handle a number of various tasks such as cell phones and PDA communications (among themselves or with peripherals, e.g. earphones, printers) and provide QoS suitable for voice communications; 3) Low data rate WPANs (IEEE 802.15.4/LR-WPAN) that are intended for a set of industrial, residential and medical applications with requirements of very low power consumption and cost and relaxed needs for data rate and QoS. Wireless Sensor Networks discussed in this thesis belong to the third class of WPANs.

1.1 Introduction to Wireless Sensor Networks

Wireless sensor network is a new generation of large scale networks formed by massively produced sensors that are developed for a number of commercial and military applications, as a result of the advances of new techniques in wireless networking, micro fabrication and system integration, Micro Electro Mechanical Systems (MEMS) and embedded microprocessors [6]-[10].

1.1.1 Wireless Sensor Networks: Overview

WSNs are formed by a large number of sensor nodes that communicate with each other wirelessly. Their software and hardware should support dynamic re-configurability, allowing fast adaption to new environments, requirements and applications [11][12].

1.1.1.1 The Structure of Sensor Nodes

The structure of a typical WSN node is similar to small computers in terms of their interfaces and their components. The node usually consists of a processing unit with limited computational power and memory, sensing unit or data acquisition unit which includes various sensors or MEMS, a communication unit or data transfer unit - usually radio transceivers, and a power source normally in the form of a battery. Other optional components include energy harvesting modules, secondary Application Specific Integrated Circuits (ASICs), and possibly secondary communication devices (e.g. RS-232 or USB) [11]-[14]. Fig.1.1 depicts the typical structure of a WSN node. The cost of sensor nodes varies, ranging from hundreds of dollars to a few cents, depending on the size of the sensor network, the environment it will operate[1], and so on. The set size and cost constraints applied to the sensor nodes define the energy consumption, memory, computational speed and bandwidth limitations of the nodes [2][11][12].

To achieve significant energy consumption efficiency, sensor nodes should have limited one-hop communication range and be able to form multi-hop networks that WSNs commonly rely on [15]. Consequently, nodes have to collaborate in order to accomplish their tasks: sensing, signal processing, computing, routing, localization, security [11][12][16], etc.

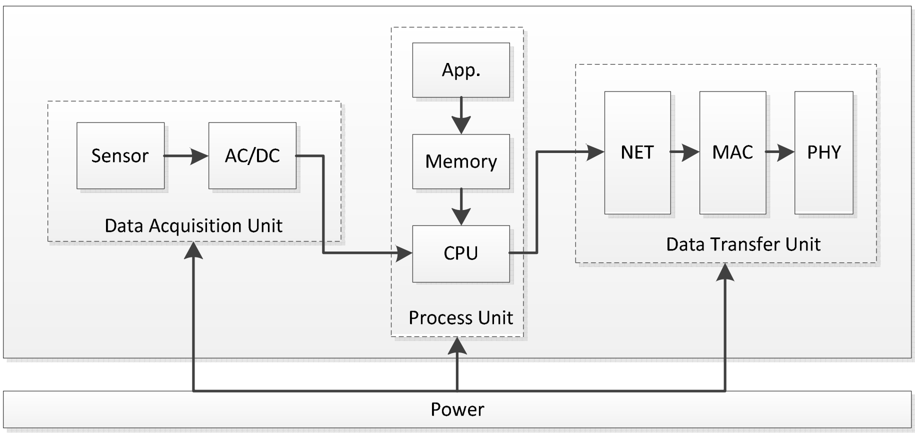

Fig.1.1 Structure of a WSN Node[12]

[1] For example military applications or operation in other harsh environments require very resilient electronics and device, capable to survive under very hot and very cold temperatures, under severe humidity conditions, able to survive falls and rough handling.

1.1.1.2 The Architecture of Wireless Sensor Network

The typical architecture of a WSN is illustrated in Fig.1.2. Generally, a typical WSN system consists of sensor nodes, sink nodes or base stations, manager nodes, and so on. Several sensor nodes are deployed within the area the owner of the WSN has interest to monitor. Sensor nodes collect the required data and transfer them to other nodes which have the ability to apply further processing. Communication between nodes is conducted wirelessly. One or more than one base stations[2] are located within communication access of the sensor deployment area. Its/their purpose is to transfer the collected raw or processed data to a certain destination for further processing and/or use for certain tasks. The base stations or coordinators also act as gateways for forwarding data collected from the WSN to task manager nodes through internet or satellite. Other special components in routing based networks are routers which are designed to compute, calculate and distribute the routing tables and route the network traffic flows [13].

A WSN might include a large number of nodes; for example, Smart Dust [17] is a system of many tiny micro-electromechanical systems such as sensors, robots, or other devices, which form the logic connections [13]. The overall connections among nodes form the network topology, which can be categorized as star connected network and peer to peer network. Topology control is another important issue associated with WSN topology. To maintain the logical connections of WSN, some special WSN-relevant factors such as limited bandwidth, scarce energy, and unstable infrastructure should be considered by the topology control

[2] A more commonly used term in the case of WSN is ***coordinator***.

approaches, along with routing technologies in some circumstances. Moreover, WSNs should have the ability to adapt to the changes of the routing topology such as the node movements or failures of some nodes [13].

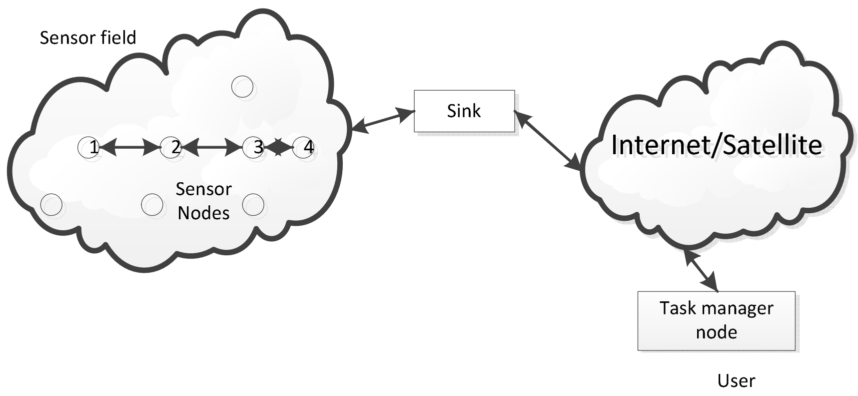

Fig.1.2 The Architecture of WSNs[12]

1.1.1.3 Use of Wireless Sensor Networks

The applications of WSNs are plausible and typically involving some kind of monitoring, tracking, or controlling. In general terms, applications implemented by WSNs can be categorized into five classes: environmental monitoring, e-health, industrial applications, law enforcement/military and security, and home applications [18]-[20].

Environmental Monitoring: The environmental monitoring applications include tracking the movements of birds, animals, and insects; monitoring environmental conditions that affect crops and livestock; chemical/biological detection; biological and seismic monitoring, etc[14][22][23].

E-health: The development in implanted biomedical devices and smart integrated sensors together helps to realize the possible implementation of sensor networks for biomedical applications. Some typical applications include tele-monitoring and tele-medicine [24], emergency response [25],and patient monitoring [26].

Industrial Applications: WSNs provide a promising alternative solution to industrial wired communication networks (e.g. Industrial Ethernet [27], Fieldbus [28]). They have already seen wide deployment in industrial environments due to their ease of deployment, high scalability, and high cost efficiency. Some examples are real-time inventory management [29], process and equipment monitoring [30], and industrial mobile robots [31].

Law Enforcement, Military and Security Applications: These applications are mainly focusing on monitoring the military or battlefield environments such as friendly forces, equipment, and ammunition; battlefield surveillance for reconnaissance of opposing forces and terrain; targeting assistance; battle damage assessment, etc. [18][21][33]. Also in order to prevent terrorist attacks, the homeland security is becoming another hot spot of military application for WSNs, e.g., border patrol and surveillance [33].

Home Applications: The WSN nodes implemented inside domestic devices allow end-users to manage more easily home devices both locally and remotely. Accordingly, WSNs enable the interconnection of various devices at residential places with convenient control of various applications at home, such as home water monitoring systems, lumination monitoring and controlling systems [34].

1.1.2 Characteristics of Wireless Sensor Networks

WSNs are multi-hop self-organizing network systems formed by diversified nodes that communicate with each other wirelessly. This type of network has some distinct characteristics [12][13]:

Application-Related: In order to build efficient and reliable systems, the design work of WSNs is always directly related to the requirements of each specific application to create specific suitable deployment.

High Fault Tolerance: WSNs are often deployed in some harsh industrial environments or large-scale areas with possible high interference. Thus the WSNs should be fault-tolerant and robust to node failures.

Self-Organization: The nodes of WSNs should support fast self-configurable formation and self-management of the network.

Data-Centered: WSN is a task network. In many cases, WSN owners are interested in the values of one or more specific parameters and usually they process the data as aggregate, i.e. the value a single sensor sends isn't very essential.

Dynamic Topology Formation: The topologies of WSNs can change dynamically and frequently due to some new nodes joining or leaving the network (e.g. mobile WSN [35]), node failure, nodes going to sleep in order to save energy, etc. Therefore WSNs should have the ability to reconfigure fast.

Large-Scale Distribution: In several cases, WSNs need to be deployed over a large area. Also, the development of smaller (and possibly weaker) sensor devices (e.g. smart dust) will lead to frequent re-deployment of very dense WSNs.

1.1.3 Technical Challenges of WSN

While a lot of research related to WSNs is available in the open literature, there are several significant technical challenges remaining [13][20][21] that prevent WSNs' wide-spread use. Such challenges are the following.

Energy Efficiency: As energy-efficiency is very essential to WSNs, technologies targeting the development of highly energy efficient communications, computing and memory storage/access technologies, and the miniaturization of high energy capacity batteries remain critical factors. Very useful concepts such as Smart Dust cannot be materialized for massive use unless these technical challenges become overcome.

Integration of WSNs and the Internet: In order to extend the applicability of WSNs, collected data transfer and their efficient access and control through Internet is essential. So far, research has progressed in this area (e.g. [36], [37]), but tight integration and interoperability problems remain [38]. We haven't reached the point of implementing technologies allowing their large scale industrial manufacturing.

Real-Time and Multimedia Communication: Evolution of technology along with the need for more intelligent sensing generate new categories of WSNs, such as wireless smart sensor networks (WSSNs) [39] and wireless multimedia sensor networks (WMSNs) [40][41].

These networks have to support real-time and multimedia communications and satisfy their QoS needs.

Synchronization and Localization: The synchronization and localization protocols developed for WSNs provide a common reference frame for various applications; however there still exist many open issues related to new practical requirements to be addressed.

Protocol Stack: The current MAC solutions are tailored to the unique challenges of the WSN paradigm. Although these solutions address many of the challenges in WSNs, there still exist many open research issues for MAC protocols in WSNs.

Security and Privacy: Since WSN nodes operate on wireless channels and are lack of resources to implement complex security algorithms, they are vulnerable to outside attacks. Therefore, security and privacy issue is becoming a true challenge for future research and applications [42][43].

WSNs in Challenging Environments: With many promising advantages of WSNs that have been summarized before, there emerge several new areas of utilization, such as underwater and underground applications. Thus, more research efforts should be made to cope with the impairments of the propagation medium under such challenging environments.

Coexistence Interference: Due to the extensive deployment and development of wireless technologies, WSN devices are often located in the proximity of other network devices operating in the same frequency band. The coexistence interference from other networks deteriorates the performance of WSN. For example, the low transmission power of a ZigBee based WSN makes it easily vulnerable to interference caused by other wireless systems transmitting powerful signals in the 2.4GHz Industrial, Scientific, and Medical (ISM) band where ZigBee also operates (e.g. IEEE 802.11 WLANs and IEEE 802.15.1 Bluetooth networks)[44].

1.2 Research Motivations and Objectives

In the above WSN overview, the technical characteristics, features, applications and challenges of WSN were introduced and discussed. Among them the coexistence interference is very damaging and remains an open research issue. The significance of this problem motivated us to focus on inventing innovative ways to resolve it. .

1.2.1 Research Motivation

The low-power, low-rate ZigBee/IEEE 802.15.4 WSN is operating at the 2.4GHz ISM band. However, the 2.4 GHz band is heavily used by several other unlicensed products, most prominent of which are IEEE 802.11b/g/n WLANs. Fig. 1.3 shows the overlapping RF spectrums of ZigBee/IEEE 802.15.4 WSN and IEEE 802.11b/g Wi-Fi. There are already confirmed interference problems between collocated devices of different nature [44], and the expectation is that the problem will worsen as the density of such devices per square meter increases. WLAN can cause ZigBee WSN the most severe problem due to the considerably higher level of transmit power it uses and the pervasive deployment of its devices. Therefore, it is important to understand and quantify how the relevant location of interfering devices impacts performance and design effective counter-measuring techniques.

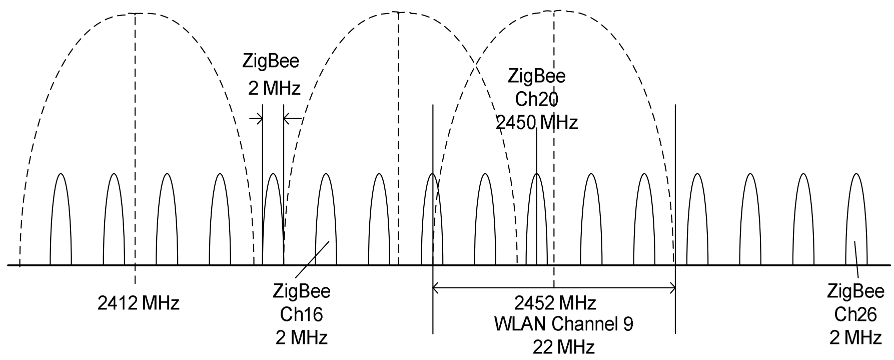

Fig.1.3 RF Spectrum allocation for ZigBee and Wi-Fi

After going through the available literature, we became aware of the significant weaknesses of existing technologies which are designed for alleviating the performance damage on ZigBee system caused by the transmissions of collocated IEEE 802.11 compatible WLAN devices. Such weaknesses can be catastrophic to the proliferation of ZigBee products in critical existing and emerging markets such as smart grid and home automation, monitoring and control, surveillance and tele-health. It is thus of paramount importance to develop cost effective technology that eliminates this threat. We pursued our research using actual, off-the-shelf ZigBee devices (Crossbow MICAzmotes [45]) where we implemented our novel algorithms and developed protocols, and Wi-Fi IEEE 802.11g communicating nodes to generate Wi-Fi interference. We ran extensive experiments which not only enabled us to assess the performance improvements our proposed technology achieves under interference generated by different Wi-Fi traffic scenarios, but to also uncover several specific hardware-protocol interoperability mechanisms which can impact the performance of ZigBee motes under certain operational conditions. This new information led us to the discovery of new, more powerful techniques. In addition, transformation of conventional off-the-shelf ZigBee motes to enhanced performance ones without requiring hardware changes but only modifications made to the mote's software proves beyond doubt that the proposed technology is easily implementable and fast deployable. It generates minimal additional cost and can be viewed as an upgrade to existing ZigBee systems. Last but not least, by following an experimentation approach in performance evaluation rather than use of analysis and/or simulation, ensured that the produced results project the actual performance of the assessed system; it includes all the known and unknown factors impacting performance. Theoretical analysis often makes use of simplified mathematical models and assumptions to reduce complexity and allow analytical tractability. Performance evaluations conducted only through computer simulation have the risk of leaving the impact of hidden factors on the performance unidentifiable. The benefit of this approach can be understood when considering the impact that the mechanisms mentioned above have on the performance. Their impact couldn't be included by following existing analytical performance models or simulation, because those models as well as the simulators would not have them included in their design. This has been confirmed in section 4.2, where performance results generated through an analytical performance evaluation approach [101] are not in agreement with the experimental results. In addition, while for some standards there are well defined channel models (e.g. 3GPP spatial channel model (SCM) [136]), IEEE 802.15.4 standard is not including channel model recommendations. Assuming a certain channel model and use it with analytical and/or simulation approaches could provide us with unreliable results. Our experimentation based approach removes such uncertainty.

1.2.2 Research Objectives

We set following objectives for this work;

1. Evaluate the effect of clear channel assessment (CCA) modes and energy detection (ED) thresholds of ZigBee connection subjected to IEEE 802.11g connection interference using analysis and experimentation, supported by the implementation of a wireless testbed.

2. Design and implement novel interference aware adaptive clear channel assessment (IAACCA) techniques on Crossbow ZigBee devices [45] that improve the ZigBee's performance when subjected to interference from collocated Wi-Fi connection.

3. Evaluate and analyse the effectiveness of the proposed IAACCA techniques through extensive collection and processing of experimental data, using the developed testbed.

1.3 Research Contributions

Our two-year research led to the following research contributions:

1. We established a versatile testbed for conducting a variety of experiments. In addition to the configurations of hardware devices, we developed a series of custom software that offer a wide range of functionalities (e.g. packet generation, transmit

power adjustment, and packet statistics) for the current and future experimental research on ZigBee packet transmission. The proposed performance improvement techniques have been implemented as firmware that can be flashed into Crossbow motes. This proves the applicability and easy inclusion of our techniques in actual commercial products.

2. We evaluated the effect of different CCA modes and ED thresholds on the ZigBee's performance under Wi-Fi interference through extensive experimentation, and also proposed and validated an adaptive mechanism to alleviate such interference.

3. We proposed and implemented an IAACCA scheme that improves the ZigBee's performance under Wi-Fi interference. This IAACCA scheme can determine better timing for transmitting ZigBee packets and adjusts packet size and/or operating channel based on its effective assessment of channel interference conditions and the availability of time and/or spectrum "holes" able to provide communication.

1.4 Thesis Organization

The remaining chapters of the thesis are organized as follows: In chapter 2, related background technology is introduced and in chapter 3, a literature review of the state of the art technology related to our research is presented. Chapter 4 gives a description of our testbed, the preliminary packet collision models between IEEE 802.15.4/ZigBee and IEEE 802.11g/Wi-Fi, and the design of experiments and the followed process. In addition, the effect of different CCA modes and ED threshold values is experimentally evaluated and analyzed. An adaptive mechanism is proposed and validated for improving the performance. In chapter 5, an adaptive CCA mechanism is proposed and evaluated through the use of the established testbed. In addition, an experiment and corresponding analysis are given on statistical scenarios of packet transmission for validating our developed mechanism. Finally, conclusions are drawn and topics for future research are summarized in Chapter 6.

Chapter 2

Technical Background

Considerable effort has been made in recent years to develop and design standards for low rate and low power WSNs. The core outcome of these efforts is the creation of the IEEE 802.15.4 standard [46] that targets low data rate applications requiring wireless interconnection between measurement, analysis, and control devices, which can be classified as Personal Area Networks (PANs). This puts IEEE 802.15.4 in the same general family as the Bluetooth standard (IEEE 802.15.1 [47]), though the low power and low data rate nature of its intended applications differentiates it from the latter. An IEEE 802.15.4 based PAN can be modeled by using a simplified version of the Open System Interconnection (OSI) protocol stack [48] consisting of the following layers (from bottom to top): PHY layer, MAC sublayer, networking (NET) layer, and application (APP) layer. IEEE 802.15.4 specifies only the PHY and MAC layers. The remaining layers are provided by subsequent protocols such as ZigBee [49], WirelessHART [50][51] and ISA100.11a [51][52].

In the above mentioned standards, WirelessHART is specified in the Wireless Highway Addressable Remote Transducer (HART) Field Communications Protocol, a long-established device measurement and control protocol in the area of industrial automation. This technology provides plant operators a reliable and long term solution for industrial intelligent devices with wireless digital communication capabilities [53]. ISA-100.11a is an open wireless networking standard for industrial automation, developed by the International Society of Automation (ISA). Its main role is to provide reliable and secure wireless operation for non-critical monitoring, alerting, supervisory control, and loop control applications [54]. Among these standards, ZigBee is the most prominent and comprehensively implemented WSN standard. It consists of several standardized protocols, forming a protocol stack architecture that is residing directly above the IEEE 802.15.4 PHY and MAC layers.

As indicated in Chapter 1, IEEE 802.15.4/ZigBee is operating at the ISM (2.4 GHz range) band as Wi-Fi networks do, thus the interference problems are inevitable when ZigBee and Wi-Fi devices are located at proximity and operated in overlapping channels. Our research is aiming at investigating the coexistence issue between collocated ZigBee and Wi-Fi connections and the corresponding interoperation techniques that can be implemented on ZigBee compliant devices in order to mitigate the interferences generated by the high power high rate Wi-Fi networks. Thus, in this chapter, background knowledge on related standards and techniques is presented and discussed. Section 2.1 presents the IEEE 802.15.4 and ZigBee standards. An overview of Wi-Fi/IEEE 802.11 standards is provided in Section 2.2. And finally in section 2.3, the Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) mechanism used by the IEEE 802.15.4 MAC layer and the Clear Channel Assessment (CCA) mechanism implemented in the IEEE 802.15.4 PHY layer are described.

2.1 Overview of IEEE 802.15.4 and ZigBee Standards

IEEE 802.15.4 is a protocol designed for LR-WPAN defining the specification of PHY and MAC layers, while ZigBee is a protocol providing NET and APP layer specification and based right on top of the IEEE 802.15.4 specified layers. The complete ZigBee/IEEE 802.15.4 architecture is shown in Fig.2.1.

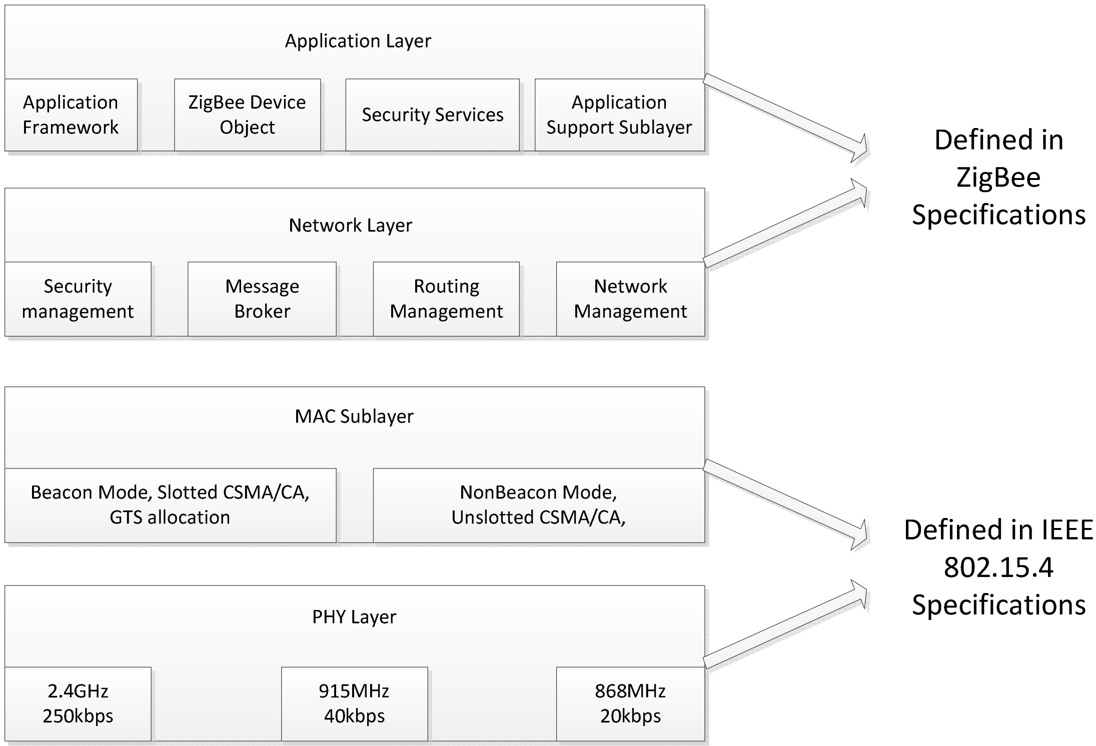

Fig.2.1 ZigBee/IEEE 802.15.4 protocol stack [55]

In the following section, we give a technical overview on both IEEE 802.15.4 and ZigBee standards.

2.1.1 IEEE 802.15.4 Standard

The IEEE 802.15.4 standard provides the specifications for the two fundamental lower network layers (PHY and MAC layers) for WPANs which focus on low-cost, low-speed ubiquitous communications between devices. The emphasis of this standard is on very low cost communications of nearby simple devices with little infrastructure, limited resource and low energy consumption.

2.1.1.1 IEEE 802.15.4 PHY Layer

The PHY layer provides the physical data transmission service and the interfaces to its management entity. Through these interfaces, the PHY layer can access various layer management functions and stores the essential information. Features of the PHY are energy detection, link quality indication (LQI), CCA, channel selection and transmission of PHY packets across predefined physical medium. It operates on one of three possible unlicensed frequency bands [56]:

- 868.0-868.6 MHz: 1 channel in this band and used in Europe.
- 902-928 MHz: 10 channels in this band and mainly used in North America.
- 2400-2483.5 MHz: 16 channels in this band and used worldwide.

Fig. 2.2 illustrates these IEEE 802.15.4 Operating Frequency Bands.

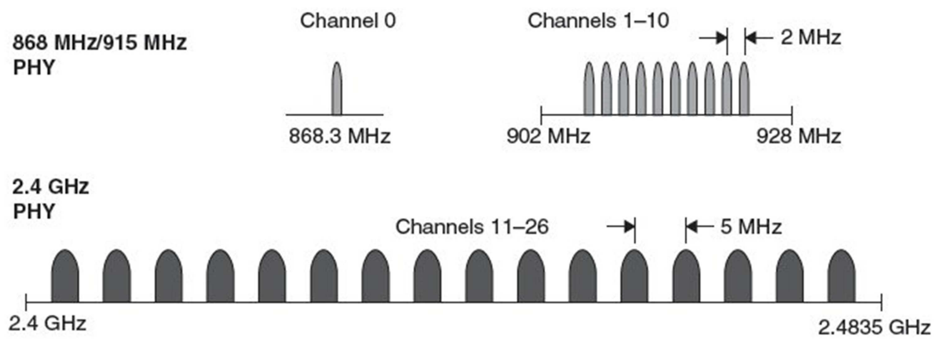

Fig.2.2 IEEE 802.15.4 Operating Frequency Bands [2]

The standard offers two physical options both based on direct sequence spread spectrum (DSSS) techniques: one working in the 868/915 MHz bands with transferring rates of 20 and 40 kbit/s, and the other in the 2.4GHz band with a rate of 250 kbit/s.

Every PHY layer packet, or PHY protocol data unit (PPDU), is constructed with a preamble, a start of packet delimiter, a packet length indicator, and a payload field, or PHY service data unit (PSDU). The functionality of 32-bit preamble is synchronization, and the establishment acquisition of symbol and chip timing. The IEEE802.15.4 payload length can expand from 2 to 127 bytes [57]. This structure is shown in Fig. 2.3.

PHY protocol data unit (PPDU)			
Preamble	Start of Packet delimiter	Length Field	PHY layer payload PHY service data unit (PSDU)
4 bytes	1 byte	1byte	2-127 bytes

Fig.2.3 IEEE 802.15.4 PPDU Structure [57]

2.1.1.2 IEEE 802.15.4 MAC Sublayer

Above the PHY layer in the IEEE 802.15.4 stack, there exists the MAC sublayer, which is responsible for data communication among neighboring devices and the corresponding management services. The MAC data service enables the basic function of data transferring among neighboring devices, mainly the transmission and reception of MAC protocol data units (MPDU) across the PHY data service. Besides the data service, the management service is also offered by the MAC sublayer, which includes management interface to the physical channel, network beaconing, controls frame validation, guaranteed time slot (GTS) mechanism, and handles node associations/disassociations.

Fig.2.4 shows the general structure of an IEEE 802.15.4 MAC frame. The MAC frame normally contains the MAC header which includes frame control field, sequence number, addressing fields, variable MAC payload and a 2-byte frame check sequence (FCS) footer.

Octets:2	1	0/2	0/2/8	0/2	0/2/8	variable	2
Frame control	Sequence number	Destination PAN identifier	Destination address	Source PAN identifier	Source address	Frame payload	Frame check sequence
		Addressing fields					
MAC header						MAC payload	MAC footer

Fig.2.4 IEEE 802.15.4 MPDU structure [58]

The IEEE 802.15.4 standard allows the use of a superframe beacon structure, called beacon-enable mode, for providing dedicated bandwidth to certain applications in order to minimize the latency and to meet the communication requirements. In beacon-enabled mode, a coordinator broadcasts beacons periodically to synchronize the attached devices for communication. Interference occurring among these devices is prevented.

On the contrary, the non-beacon mode uses a simple and traditional channel access mechanism. Under certain circumstances, peer-to-peer network for instance, all the clients remain unknown to each other and can initiate a conversation at will, thus a random and contention based channel access algorithm, i.e. non-beacon mode, is the appropriate choice here. In the non-beacon mode, devices can stay in sleep mode most of the time [59]. They wake up randomly and then confirm their presence in the network. The awaken motes contend for access to the channel in order to transmit their frames. However, this simplicity could cause severe interference among the devices unintentionally. More details will be provided in section 2.3.1.

There are several other important features of MAC sublayer, such as real-time suitability by reservation of GTS in the beacon mode, interference counter-measuring through the use of CSMA/CA mechanism, and support of security. The CSMA/CA mechanism is an essential component implemented in the MAC sublayer and is comprehensively studied in this thesis research. Thus, CSMA/CA and the corresponding CCA mechanism for determining channel status will be discussed in detail later, in a dedicated section of this chapter.

2.1.1.3 IEEE 802.15.4 Topologies

The IEEE 802.15.4 standard defines two types of devices, a Full-Function device (FFD) and a Reduced-Function device (RFD). The FFD is capable of all network functionalities and can operate as a PAN coordinator, a relaying gateway, or simply as a mote. An RFD device is memory and processing limited and can only run low complexity applications, e.g perform sensing of a few environmental parameters [56].

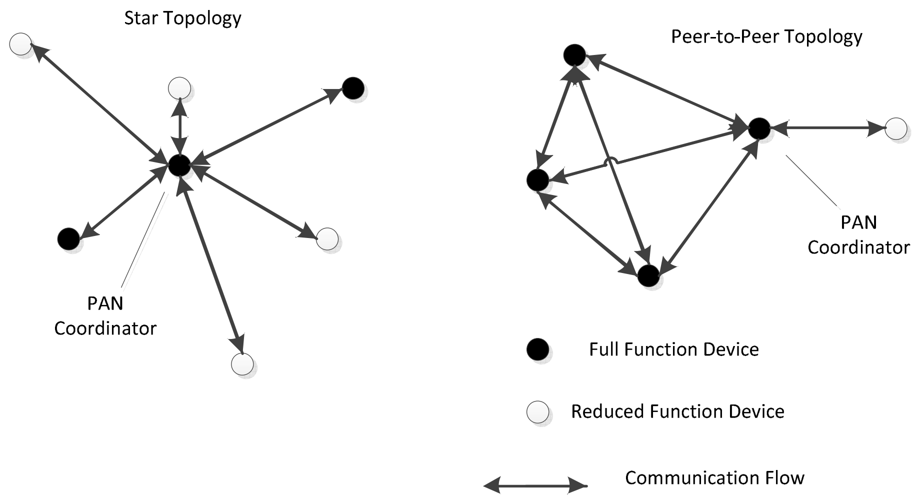

Fig.2.5 IEEE 802.15.4 Network Topologies [56]

Fig. 2.5 depicts two typical topologies for PAN: (1) Star topology: Communication can only take place between the motes and the PAN coordinator. The PAN coordinator, which must be an FFD, acts as the terminating communication station and controlling centre of the network. In most of the time the coordinator maintains its power-on. To establish a network of star topology, an FFD must be activated and act as PAN coordinator. This PAN needs to have a unique PAN identifier that is different from those used by other star networks in range [56]. (2) Peer-to-peer topology: All the FFD devices in PAN can communicate with each other within communication range. However, the RFD devices can only exchange data with the PAN coordinator.

2.1.2 ZigBee Standard

The ZigBee specification offers full wireless mesh networking capability and can support more than 64,000 devices in a single network. It is designed to connect the widest range of devices encountered in any industry, into a single control network [60]. In the following, several essential points of the ZigBee standard specifications are briefly introduced, including the classification of ZigBee devices, routing protocols and the security mechanism. All the industrial developers or manufacturers have to adhere to these specifications as required by ZigBee Alliance. These specifications support interoperability between users' applications.

A. ZigBee Network Technology

ZigBee defines three classes of devices [61]:

- *ZigBee Coordinator (ZC)*: As the most capable device, ZC can control the entire network formation and maintain the security of the network. There is only one ZC in each network and it is the device that initiates the formation and establishment of the network.
- *ZigBee Router (ZR)*: ZR is an optional network element whose major function is to extend the range of the network. It keeps a routing table and controls the addressing/routing issues for the connected end devices.
- *ZigBee End Device (ZED)*: A ZED performs specific sensing or control functions. It also has the capability to communicate with the above two types of devices which

function as its parent nodes. This relationship allows the node to be asleep for a significant amount of time thereby saving the battery energy to a great extent.

While ZEDs are allowed to periodically cycle into a low-power sleep mode in networks, ZRs and ZCs must in general always remain awake. Regarding the network layer, both ZCs and ZRs participate in multi-hop routing activities and ZEDs only process messages to/from their own associated parent device within their radio transmission range [62].

B. ZigBee Routing Protocol

The Cluster-Tree algorithm [63] and Ad hoc On Demand Distance Vector (AODV) algorithm [64] are used in ZigBee networks to reduce cost and power consumption and improve reliability [65][66]: (1)The cluster-tree protocol locates in network layers that transmits link-state packets to setup a single cluster or a multi-cluster tree network. The network is self-organized and also employs network redundancy to achieve fault resistance and self-repair. (2) AODV is a pure on-demand route acquisition algorithm which never relies on active paths. In contrast with the above protocol, routing information is not stored in an AODV network. The network nodes do not need to participate in any periodic routing table exchange activities either. The discovery and maintenance of a route from one node to another is only executed when these two nodes are about to communicate. An exceptional instance is that a node is an intermediate forwarding station which offers connectivity between two other nodes [67].

C. ZigBee Security

The ZigBee security architecture includes security mechanisms built on 128-bit AES at the network and application protocol stack, which are responsible for the secure transport of their respective frames. There are three major considerations when designing ZigBee security architecture, namely, simplicity, directness, and end-to-end security. For simplicity, each layer takes the responsibility for any frames originating from it. For directness, direct key-exchange between the source and destination devices takes place. For end-to-end security, decryption at the destination node is only required, and the intermediate nodes do not perform any decryption or re-encryption activities [68][69].

ZigBee standard is established by the close collaboration of IEEE and ZigBee Alliance, which is aiming at defining the whole specification of the entire protocol stack for WSNs. IEEE 802.15.4 provides specifications for the lower two layers (PHY and MAC) while ZigBee Alliance addresses the standardization of the higher layers and "interoperability between devices of different manufacturers in terms of data networking, security, and a range of wireless home and building control applications". The alliance also brings to the customers other products and technology solutions, such as "interoperability compliance testing, marketing of the standard, and advanced engineering for the evolution of the standard". This will assure consumers to buy products from different manufacturers with confidence in the compatibility [2].

2.2 Overview of Wi-Fi/IEEE 802.11 Standards

The IEEE 802.11 standard provides wireless connectivity to devices that require quick installation, such as computers/tablets, cell phones, or other mobile devices inside a WLAN as an extension or substitute for cabled LAN. It defines PHY and MAC layer specifications as well as the communication protocols handling data transfer at each layer [71].

The IEEE 802.11 family contains a series of over-the-air modulation techniques that use the same basic protocol of which the most popular now are the IEEE802.11g and IEEE802.11n standards. IEEE 802.11n is the latest PHY layer Wi-Fi technology. It is using a multi-streaming modulation technique and makes use of Multiple Input Multiple Output (MIMO) technology. However, due to the existence of a large number of IEEE802.11g devices, the majority of existing Wi-Fi networks operates using IEEE802.11g[3]. Other standards in the family (c-f, h-j) are service amendments or corrections to the previous specifications and some of them have been integrated into real world products [72][49]. Due to their vast deployment and the ease to obtain at the beginning of our experiments, IEEE 802.11g standard compliant devices are used in our research. Thus, the following paragraphs focus on the discussion of IEEE 802.11g standard.

2.2.1 IEEE 802.11 PHY Layer

IEEE 802.11 PHY layer defines the frequency band, data rate, and other details of the actual radio transmission. The initial IEEE 802.11 specification was addressing three different physical technologies: DSSS, Frequency Hopping Spread Spectrum (FHSS) and Infrared (IR). DSSS can effectively increase the data rate by “mapping each data bit into a string of bits

---

[3] Products with IEEE802.11n capability offer backwards compatibility with earlier IEEE802.11 PHY layer standards, thus they can fall backwards and operate as IEEE802.11g or IEEE802.11b if nodes without IEEE802.11n capability are present in the WLAN.

using one string for binary 1 and another for binary 0. DSSS also has better ability to resist interference compared to FHSS” [73].

IEEE 802.11b is an extension to the basic DSSS scheme, providing data rates of 1, 2, 5.5 and 11 Mbps. The IEEE 802.11b standard uses Complementary Code Keying (CCK) [49] as its modulation technique. Its successor, IEEE 802.11g, extends IEEE 802.11b to data rates of 12 to 54 Mbps per channel. IEEE 802.11g uses Orthogonal Frequency Division Multiplexing (OFDM) [49] modulation scheme and can reverse to CCK and become IEEE 802.11b compatible if devices supporting IEEE802.11b are present in the WLAN.

An IEEE 802.11 network is generally a set of IEEE 802.11 compliant devices and access points (APs) communicating through a common RF channel. The IEEE 802.11b/g standard defines a total of 14 frequency channels, each of which is 22 MHz wide. Fig. 2.6 illustrates its frequency band occupation.

There is spectral overlapping between channels and only 3 non-overlapping channel groups can be formed. In the USA, channels 1-11 are allowed to use by the Federal Communication Commission (FCC) while in Europe channels 1-13 are allocated. In Japan, one more choice is allowed, channel 14. In order to reduce the negative impact of interference, that if multiple WLANs are in use within the same area, it is better to select three non-overlapping channels, at least for those being adjacent to each other (e.g. channels 1, 6 and 11, or channels 2, 7. 12).

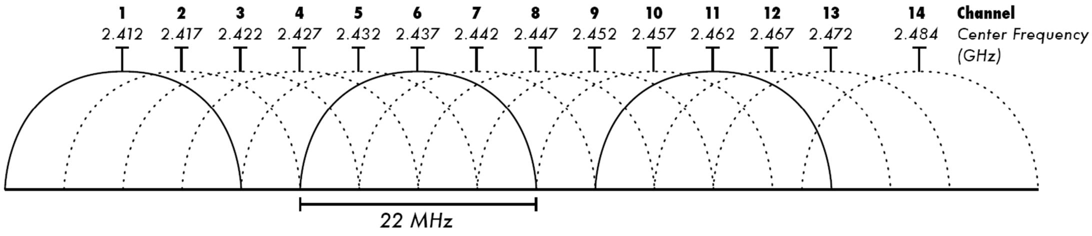

Fig.2.6 IEEE 802.11b/g Operating Frequency Band [74]

2.2.2 IEEE 802.11 MAC Sublayer

The IEEE 802.11 standard specifies that data must be transmitted in blocks, or called frames, as illustrated in Fig.2.7. Each frame includes user data, destination and source address, frame control bits and bits generated by cyclic redundancy check (CRC) applied on the frame [49]. Each IEEE 802.11 device monitors the shared radio medium and receives every readable frame. After decoding the frame, the node checks the frame to see if it contains the node's MAC address in its destination field. If such address is found, the frame is then passed to the higher layer for further processing. Otherwise, the frame is dropped by the node.

2	2	6	6	6	2	6	0 -2312	4
Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

Fig.2.7 IEEE 802.11 MAC Frame Format [49]

The 802.11g MAC layer defines two basic sublayers to access the medium. The lower is the Distributed Coordination Function (DCF) and the higher is the Point Coordination Function (PCF). Fig.2.8 illustrates the IEEE 802.11 MAC structure.

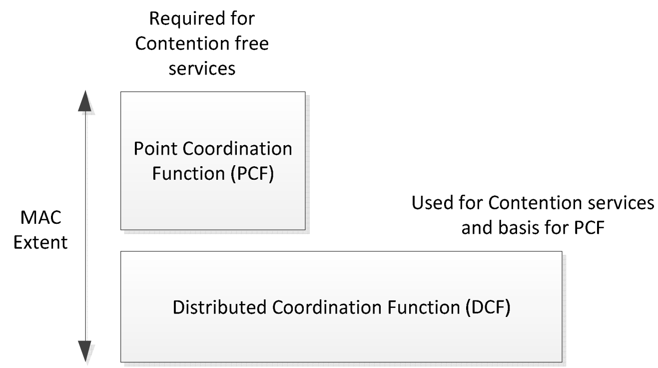

Fig.2.8 IEEE 802.11 MAC structure [49]

DCF defines a contention based access mechanism, which is based on the CSMA/CA scheme [49]. Ordinary asynchronous traffic uses DCF functionality. PCF defines a centralized and polling based access mechanism for accessing the wireless medium that provides contention free time intervals. The IEEE 802.11 standard defines PCF as optional, whereas DCF is mandatory to all IEEE 802.11 compliant devices [58][73].

Implementation of DCF and PCF functionalities makes use of service differentiation principles that are based on transmission timing constraints. As part of the coordination procedure to gain access to the transmission medium, the IEEE 802.11 standard uses three different inter–frame space (IFS) intervals to form a priority scheme: The Short Inter Frame Space (SIFS) is used for the transmission of high priority 802.11 frames, such as Clear–To–Send (CTS) and Acknowledgement (ACK) frames. The PCF Inter Frame Space (PIFS) is a mid-length IFS which is implemented in the coordinator node of a network to transmit the beacon frame, informing the nodes that PCF period starts. The beacon frame includes the time the nodes should refrain from transmitting at free will and do so only if polled by the coordinator. DCF Inter Frame Space (DIFS) is the longest IFS among the three IFS. It is utilized as “a minimum waiting time for asynchronous frames contending for access”. Fig.2.9 illustrates the basic medium access method for IEEE 802.11 standard and the use of the above three types of IFS [49].

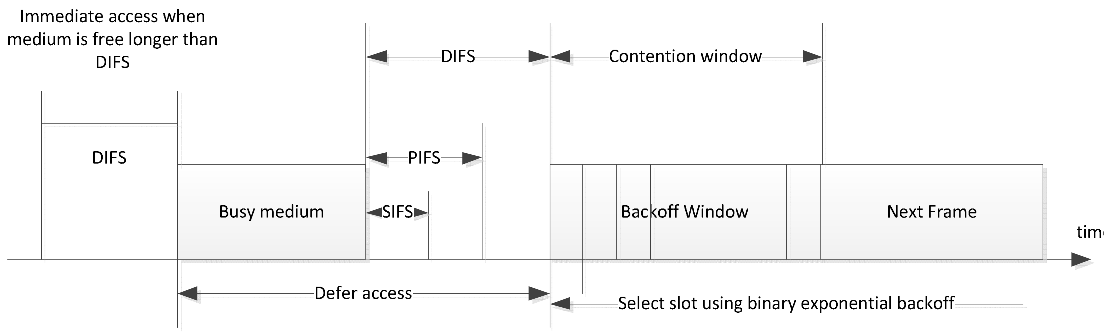

Fig.2.9 IEEE 802.11 basic access method [49]

The legacy IEEE 802.11 MAC sublayer supports limited QoS features. In order to enhance the QoS capability of Wi-Fi WLANs, the IEEE 802.11e [75] was generated as extension of the original IEEE 802.11 standard. Most Wi-Fi products sold today provide IEEE 802.11e functionality. IEEE 802.11e introduces the Hybrid Coordination Function (HCF) for QoS support. HCF defines a new contention-based channel access method called Enhanced Distributed Channel Access (EDCA) and a HCF Controlled Channel Access (HCCA). The EDCA is used in the Contention Access Period (CAP) only while the HCCA is used in both phases (CAP and Contention Free Period (CFP)). Therefore, the HCF combines methods of PCF and DCF [76][77].

The CSMA/CA mechanism requires all stations to sense the medium before attempting transmission. The main goal of CSMA/CA is to reduce the occurrence of frame collisions occurring when the time intervals of frames transmitted from different IEEE 802.11 devices, operating in the same channel, overlap. Also, through use of different size IFS intervals, more important frames have lower probability to experience collision[4] [78].

DCF has two ways to detect the status of the medium, named virtual and physical carrier-sensing. The former applies when the Request-To-Sent (RTS)/Clear-To-Sent (CTS) option of operation is used; in which case, RTS and CTS frames inform other users of the time and duration of the incoming data exchanges. For the physical layer mechanism, a station first senses the medium before sending out a packet. If the medium is detected free for DIFS duration, it starts transmission immediately. Otherwise, the station goes into a backoff procedure [78].

2.2.3 IEEE 802.11/Wi-Fi Authentication

In order to join an IEEE 802.11 network, a mobile device must establish its identity with an AP or wireless router by going through authentication. The IEEE 802.11 standard defines two types of authentication at the link level, namely, the open system and the shared key. In the process of open system authentication, the mobile device sends an authentication request containing the station ID (typically the MAC address) to AP and then the AP will respond with a success or failure message [79]. In shared key authentication, a shared key or passphrase is manually set on both the mobile device and the AP. Then the AP sends the client device a challenge text packet. The client must encrypt the text with the correct key and then return it to the AP. Then the AP decrypts the text with the same key and compares

[4] Assuming the network operates within its range of stability.

the received text with the original one. A success of authentication shall be assumed when the two texts are the same. If the authentication phase fails, the AP will deny access to this device. There are several types of shared key authentication available today for home or small office WLAN environments such as Wireless Equivalent Privacy (WEP) [80][81] and Wireless Protected Access (WPA) [81].

The WEP protocol is first defined in the original IEEE 802.11 standard. An important component of WEP is the use of the stream cipher RC4, which is well known and widely used. Unfortunately, the implementation of RC4 in Wi-Fi is of questionable quality. Many software applications can capture the encrypted form of the response frame (e.g. [81]) and use this information to crack the WEP encryption.

In late 2002, the Wi-Fi Alliance defined WPA, a notable improvement over WEP intended as an intermediate step while the IEEE 802.11i [82] specifications were being worked out. WPA complies with the wireless security standard, and strongly increases the level of data protection and access control (authentication) for a wireless network. WPA enforces the former authentication and key-exchange mechanism and only works with dynamic encryption keys. It is widely implemented in currently commercially available devices. In mid 2004, the 802.11i working group finalized an amendment providing a comprehensive authentication framework based on 802.1X and Extensible Authentication Protocol (EAP) methods, also known as WPA2. It is a security enhancement to WPA [71][79].

2.2.4 IEEE 802.11/Wi-Fi Network Topology

An infrastructure IEEE 802.11 WLAN is based on a cellular architecture in which each cell is called a basic service set (BSS), constructed with various mobile or fixed IEEE 802.11 devices. The simplest network configuration is the independent BSS (IBSS), which forms an ad hoc network topology consisting of at least two IEEE 802.11 devices. Alternatively, the so-called extended service set (ESS) is a set of one or more infrastructure BSSs connected via a distribution system, which is not necessarily a Wi-Fi network but can be a cabled network or some other type of wireless networks. The stations connected to the distribution system are the APs. Services offered by the stations can be categorized in two classes: station services and distribution system services. The station services are provided by any stations within the same BSS, which provide the data interaction among all stations. The distribution system services are offered by the APs, and allow data transfer between stations belonging to different BSSs. The standard also defines the functions of the portal, which is a bridge for interconnecting a Wi-Fi WLAN with a generic IEEE 802.x LAN. Fig. 2.10 illustrates all the typical components of a Wi-Fi network [71].

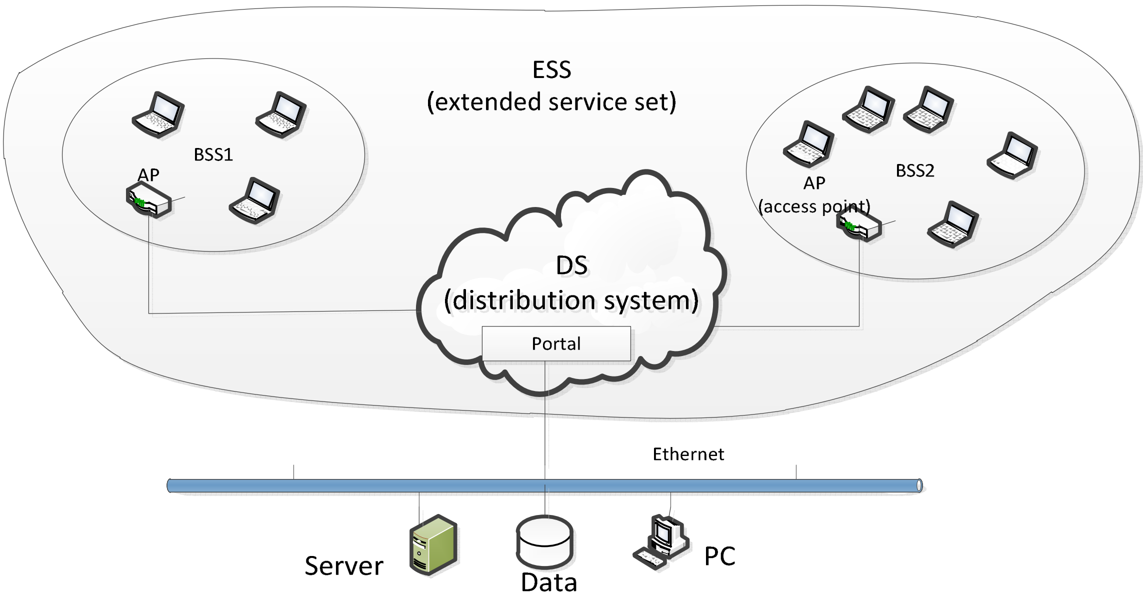

Fig.2.10 Typical Components of a Wi-Fi Network [71]

2.3 IEEE 802.15.4 CSMA/CA and CCA Mechanisms Overview

Similar to the IEEE 802.11 family, IEEE 802.15.4 standard defines the CSMA/CA as its medium access mechanism at MAC sublayer. The CSMA/CA protocol aims at enabling two or more wireless devices to access the same frequency channel resource reducing data collisions and, ultimately, performance loss due to interference. The CCA is a PHY layer function. It is used to sense the power and/or carrier in the operating channel and determines whether a certain channel is active or not. CCA is an essential ingredient of CSMA/CA based MAC protocols.

2.3.1 IEEE 802.15.4 CSMA/CA Algorithm

The CSMA/CA algorithm is implemented for the transmission of packets within the CAP which is defined as a period that any active station can initiate transmission. It is noted that the CSMA/CA algorithm is not used for the transmission of beacon frames in a beacon-enabled PAN, ACK frames, or data frames transmitted in the CFP. Before transmitting a frame, the node first waits for a random period, called initial backoff, and then senses the status of current channel with CCA to determine whether it is free or busy by measuring the power at its antenna output connector. If the channel is detected as free for a certain period specified by standard (details introduced in the following paragraphs), the node sends out the frame, otherwise, the node has to wait and defer its transmission [83]. There are two operational modes defined in IEEE 802.15.4 network standard, beacon-enabled mode and non-beacon-enabled mode [84]:

Beacon-enabled Mode: In the beacon-enabled mode, a superframe structure is used, which is illustrated in Fig.2.11. The superframe format is defined by the network coordinator and normally has an active and an inactive part. The active part is constructed with a CAP and an optional CFP. A device wishing to communicate during the CAP competes with other devices using a slotted CSMA/CA mechanism (detailed description follows). During the CFP, transmission is guaranteed to some devices, for which the time is reserved and all the other devices are instructed to halt transmission of frames and wait for that specific device finishes its transmission. This CFP can be used to serve devices producing packets that require minimal latency and fast response.

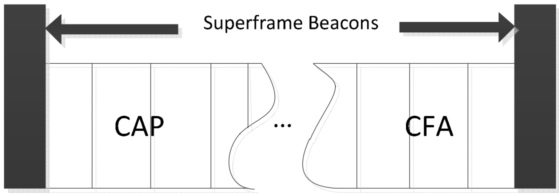

Fig.2.11 IEEE 802.15.4 MAC sublayer superframe structure [57]

Non-beacon-enabled Mode: In the non-beacon-enabled mode, no beacons are transmitted by the coordinator. All the devices that are active to access the channel exploit an unslotted CSMA/CA mechanism. Non-beacon-enabled mode is normally implemented in networks where network coordinators are always power on and ready to receive frames continuously, while transmitters or sensors transmit when an external stimulus is detected. Our research focuses on this type of non-beacon-enabled IEEE 802.15.4 WSNs. Network coordinators are continuously connected to power supply to prevent them from "dying" during experiments.

2.3.1.1 IEEE 802.15.4 slotted CSMA/CA Algorithm

In slotted CSMA/CA, each device in the PAN has its backoff period boundaries aligned with the superframe slot boundaries of the PAN coordinator. For instance, the start of the first backoff period of any device has to be aligned with the start of the beacon transmission [54]. In slotted CSMA/CA, the MAC sublayer requires all the transmissions the PHY activates to be right on the boundary of a backoff period, while in unslotted CSMA/CA, no specific relations are required to be maintained among any devices in the PAN in time [78].

Each device in PAN implements 3 variables for the backoff mechanism of CSMA/CA: *NB*, *CW* and *BE*. "*NB* is the number of times the CSMA/CA algorithm is required to backoff while attempting the current transmission, which is initialized to 0 before every new transmission. *CW* is the contention window length defining the number of backoff periods that need to be clear of activity before the transmission can start, which means that after *CW* times of channel idle sensing the transmission can be activated or the channel is assumed to be busy. Its initial value is set to 2 before each transmission attempt and also each time when the channel is assessed to be busy. *CW* is only used for slotted CSMA/CA. *BE* is the backoff exponent which defines how many backoff periods a device must wait before attempting to sense the channel" [46].

As illustrated in Fig. 2.12, for the first step in slotted CSMA/CA, *NB*, *CW* and *BE* are initialized and the boundary of the next backoff period is located. The MAC sublayer delays CCA for a number of complete backoff periods which is randomly chosen in the range 0 to $2^{BE} - 1$ (step 2) with equal probability, and then requests PHY to perform CCA (step 3). If the channel is assessed to be busy (step 4), the MAC sublayer increments both *NB* and *BE* by one. It should be noted that *BE* cannot exceed *macMaxBE*. In slotted CSMA/CA, and under this circumstance, *CW* should also be reset to 2. If the value of *NB* is less than or equal to *macMaxCSMABackoffs*, the CSMA/CA mechanism returns to step 2, else it reports a Channel Access Failure status and aborts this transmission. If the channel is assessed to be idle (step 5), the MAC sublayer waits until the contention window expires before starting transmission. For this, the MAC sublayer first decrements *CW* by one. If *CW* is not equal to 0, the mechanism turns back to step 3, or else starts transmission on the boundary of the next backoff period. Otherwise, the MAC sublayer proceeds with the frame's transmission, and any acknowledgement can be completed before the end of the CAP [46][85].

2.3.1.2 IEEE 802.15.4 Unslotted CSMA/CA Algorithm

The unslotted CSMA/CA procedure implements backoff and packet transmission procedures without any need to start transmiting at a slot boundary as is the case of slotted CSMA/CA. This feature gives the nodes more flexibility; however it increases the probability of experiencing collision. The unslotted CSMA/CA works as follows:

Every time a device starts to transmit a frame, it first waits for a random number of backoff slots ranging from 0 to $2^{BE}-1$, called initial backoff. *BE* is initialized to *macMinBE* with a default value of 3. In IEEE 802.15.4, regardless of the channel status the backoff counter is decremented to zero when the device activates to perform CCA only once. If the channel is idle during the period CCA is performed, the device transmits its data packet immediately. Otherwise, *BE* is increased by 1 and the random backoff procedure is repeated as described earlier for slotted CSMA/CA [46]. Unslotted CSMA/CA algorithm is adopted in our research and new schemes to enhance its immunity to interferences generated by collocated Wi-Fi devices are developed.

Fig. 2.12 describes in flow-chart form the entire procedure of the IEEE 802.15.4 MAC sublayer CSMA/CA algorithm, including slotted and unslotted processes.

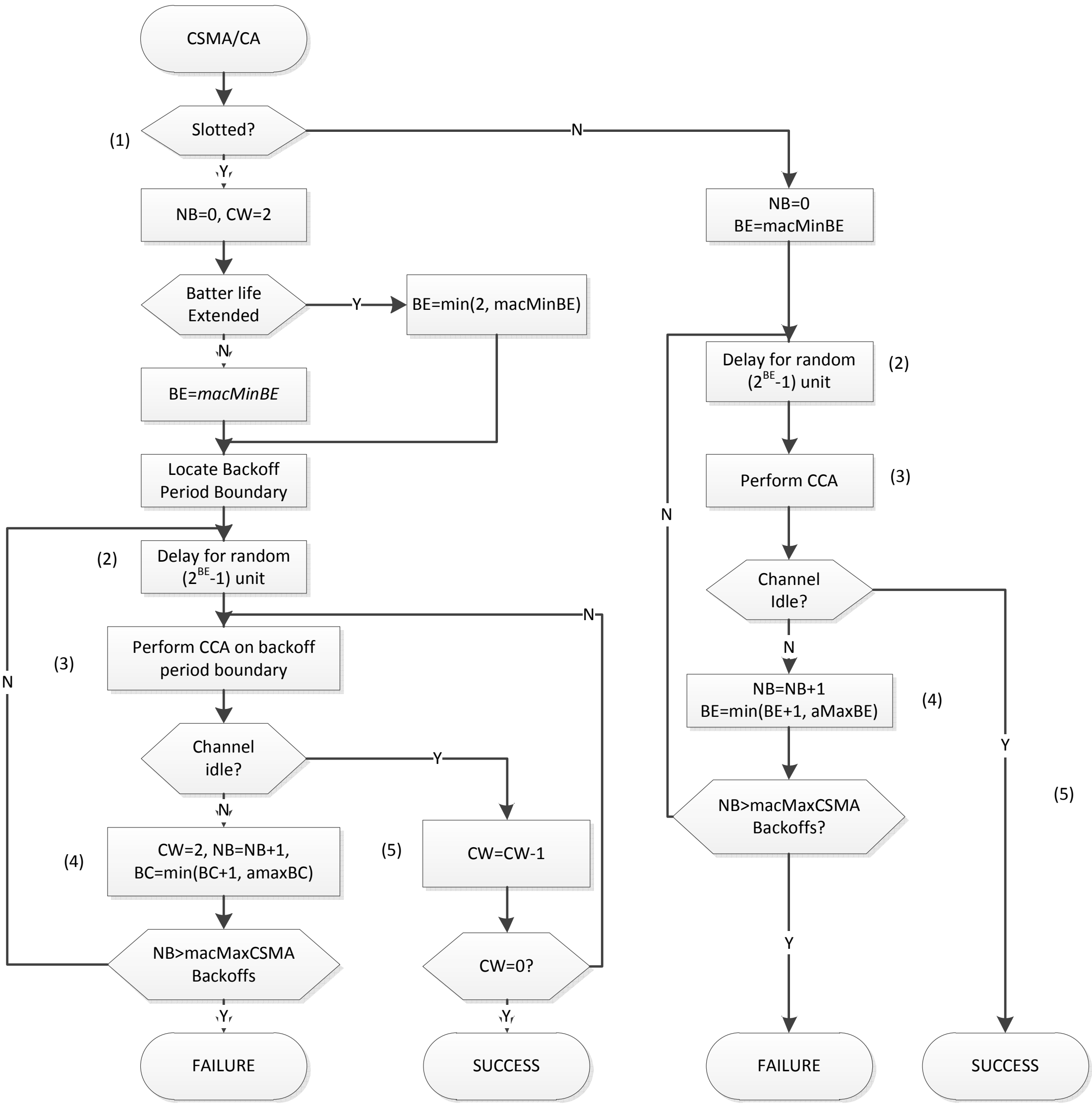

Fig.2.12 IEEE 802.15.4 CSMA/CA Algorithm [86]

2.3.2 IEEE 802.15.4 CCA Mechanism

For CSMA/CA to work, the WSN nodes need to perform CCA to determine the channel's availability or otherwise. The IEEE 802.15.4 standard specifies that the CCA duration should be 8 symbol periods, which comes to 128 µs and can be done either by means of energy detection (ED) or carrier sensing (CS). In CS mode, the medium is considered busy if any signal having the same modulation characteristics as the current wireless network is detected in the channel. In ED mode, the medium is considered busy if the assessed in-channel power is greater than a predefined threshold (ED threshold). IEEE 802.15.4 compliant devices commonly implement ED mode through the use of an embedded specialized circuit called Receiver Signal Strength Indicator (RSSI) [46][83][84].

The receiver ED measurement implemented at the PHY of IEEE 802.15.4 is intended for assisting an IEEE 802.15.4 to select channel. It is used to estimate the received signal power within the bandwidth of an IEEE 802.15.4 channel without any attempts to identify or decode signals present in the channel. The main advantage of ED is its simplicity. Another important feature is that ED has no need to be kept running constantly and can be activated once the MAC sublayer requests the PHY to perform CCA. This allows the radio part of an IEEE 802.15.4 device to be at the sleeping mode for most of its working time, thus saving energy to a great extent. The weakness of ED is that since it does not take advantage of the spread spectrum processing gain inherent in IEEE 802.15.4 signals, the SNR it senses may be relatively low, which could result in failures to identify the signal. IEEE 802.15.4 based ZigBee networks have three different CCA options to select from [84]:

- CCA Mode 1 (ED): Energy detection only. CCA reports a busy medium when the in-channel power is detected to be greater than a preset threshold.
- CCA Mode 2 (CS): Carrier sense only. CCA reports a busy medium only when a signal with the IEEE 802.15.4 modulation and spreading characteristics is detected in the operation channel.

- CCA Mode 3 (ED-CS): Carrier sense with energy detection. CCA reports a busy medium using the combination of the above two methods, which either ED or CS detections assesses the channel as busy.

The CCA mechanism is effective for detecting the channel's status and relatively easy to be embedded using simple electronic circuits. When addressing the interference from non-IEEE 802.15.4 devices, the CCA mechanism, especially its energy detection function, is of great importance. CCA is an essential component of IEEE 802.15.4/ZigBee CSMA/CA mechanism, which can enhance the coexistence of IEEE 802.15.4/ZigBee devices with other wireless devices operating at the same frequency band. Implementing a CCA mechanism that can accurately sense the external interference and enable a transmitting mote to adapt to the characteristics of such interference can be a solution technique in our proposal. By self-adjusting the transmission times of its frames in such manner, this adaptation mechanism improves the chance of successful transmission. We focus most of this research on CCA techniques.

Chapter 3

Related Work on Coexistence Issues and Interoperating Techniques

Wireless communication networks are growing in popularity and become more widespread with the passing of time. They eliminate expensive cable infrastructure wired networks need, improve network scalability and re-configurability, and service efficiently portable and mobile terminals. Over the past two years, the IEEE 802.15.4 gained considerable popularity, becoming the technology of choice for low-power wireless sensors and embedded networking applications. IEEE 802.15.4 has been integrated with the ZigBee standard, which ensures almost ubiquitous deployment of WSNs in homes and business areas. In this dissertation, the terms ZigBee and IEEE 802.15.4 are used interchangeably because our research focuses only on the study of MAC and PHY layers.

ZigBee/IEEE 802.15.4 devices operate in the ISM band (2.40 GHz to 2.50 GHz) but so do IEEE 802.11b/g and Bluetooth [87] devices. Such devices are including PCs, laptops, printers, cellular phones and smart phones, earphones and the list goes on of which size is increasing fast with the passing of time. ISM is without doubt one of the most used spectrum ranges. The recently completed IEEE 802.11n [88] standard that is defining wireless PHY layer technology capable of reaching 600 Mbps transmission rate and doubles the channel bandwidth of IEEE 802.11b/g has opened the opportunity of transporting considerably higher traffic within ISM, thus driving its already high utilization even higher. With many collocated devices operating simultaneously and using the ISM band, as well as the high traffic volumes present in this band, it becomes very sever that several interoperability problems are generated by mutual interference. Therefore, performance degradation due to the presence of interference should always be expected, unless one would take into account specific coexistence issues and adopt proper interference avoidance or mitigation solutions [89][90]. The IEEE working group IEEE 802.15.2 [91] was formed to address this issue and they have come with some recommendations described in [91], [92]. In this dissertation, the terms Wi-Fi and IEEE 802.11 also can be interchangeable. With respect to certain implementation, specific standard, i.e. IEEE 802.11g, will be used.

In this chapter we provide a comprehensive literature survey on the state of the art research on the coexistence issues, CCA effects on WSN performance under interferences and some related adaptive interference mitigation techniques. We summarize and analyze these previous research works and discuss their strengths and weaknesses. Section 3.1 provides a survey of research works on coexistence issues between ZigBee WSNs and WLANs. Related literature on the CCA mechanism implemented in ZigBee/IEEE 802.15.4 PHY layer and its impacts on the performance of ZigBee WSNs are presented and analyzed in section 3.2. Finally, several previous proposed adaptation techniques aiming at mitigating the interference effects on ZigBee WSNs are reviewed and discussed.

3.1 Study of Coexistence issues between ZigBee/IEEE 802.15.4 WSNs and IEEE 802.11b/g/n WLANs

Considerable amount of research work has been performed in recent years to investigate coexistence issues between different types of networks which operate in the same frequency band, such as IEEE 802.11b/g/n WLAN and Bluetooth WPAN.

The IEEE 802.15.2 standard is one of the earlier noteworthy efforts for addressing the coexistence issues of WPANs and WLAN. Specifically, it addresses the coexistence of WPANs with other wireless devices operating in unlicensed frequency bands, especially IEEE 802.11 WLANs. In 2003, an IEEE standard, IEEE 802.15.2-2003 was published [91]. In this standard, a computer model of the mutual interference of an IEEE 802.11b WLAN and an IEEE 802.15.1 WPAN was proposed to estimate the interference between these two networks. Based on the established model, the standard also defined several coexistence mechanisms to facilitate coexistence of the two networks, which could be divided into two categories: collaborative and non-collaborative. These mechanisms can be directions in for the development of technologies supporting the coexistence of WPANs and WLANs. However, due to the limitation of the availability of technologies at that time, IEEE 802.15.4 and IEEE 802.11g were not considered in this standard.

In the following sections, the coexistence issues between IEEE 802.15.4 WSN and IEEE 802.11b/g/n WLAN are discussed, followed by a comprehensive review of recent research work in this area.

3.1.1 Coexistence Issues between WSNs and WLANs

A key issue of wireless sensor networks is their inherent vulnerability to radio interference. WSNs typically have low transmission power and they are commonly deployed in areas that are already crowded with other wireless devices and electrical/electronic appliances. The radio interference on the same or adjacent frequency bands generated by such collocated devices/appliances may result in disruptive effects in the transmission of data packets among WSN devices, including loss of data packets, transmission delay, false commands, false alarms, jitter, and loss of synchronization [93]. This phenomenon is well known as coexistence issue.

As discussed in the previous chapter, IEEE 802.15.4 uses one of the 16 (2 MHz-wide each) channels located in the ISM band (see Fig. 2.6) and has top transmission rate 250 kb/s. The IEEE 802.11b/g standards define a total of 14 frequency channels in the same ISM frequency band, each of which is 22 MHz wide, while the IEEE 802.11n standard defines a wider 40 MHz channel bandwidth [88][94].

The IEEE 802.11n standard expands the operating channel's bandwidth to 40 MHz, making it almost double the IEEE 802.11b/g operating channel's bandwidth. As mentioned earlier, in this work we focus on the coexistence of IEEE 802.15.4 and IEEE 802.11b/g systems. From the RF spectrum characteristics depicted in Fig. 2.2 and Fig. 2.6, every IEEE 802.15.4 channel overlaps with at least one IEEE 802.11b/g channel, which means the quality of IEEE 802.15.4 communications system/network will be suffering from RF interference generated by the collocated IEEE 802.11b/g Wi-Fi networks operating in the overlapping or adjacent channels. The use of broader channels by IEEE 802.11n based systems and the higher traffic, along with the inclusion of new broadband applications (e.g. High Definition Television) in its service and the higher traffic volumes associated with them is expected to worsen the coexistence problem that IEEE 802.15.4 networks face [94].

Compared to the typical IEEE 802.15.4 transmission power of 1mW, the typical transmission power of a Wi-Fi router stands at around 100mW, thus far exceeding the power transmitted by a ZigBee node. If the level of Wi-Fi transmission power reaching an IEEE802.15.4 receiver exceeds a certain threshold, the IEEE802.15.4 frames will be damaged by the high Wi-Fi power; the receiver will not be able to extract useful data [95].

3.1.2 Experimental and Simulative Study of Coexistence Issues

The performance detriment on coexisting networks has been observed and analyzed by researchers in order to help perfecting current network standards and providing design hints and modifications to future protocols or standards. As a low rate and low power network, ZigBee may experience more serious interfering phenomena than other high power peers, and in some extreme cases the transmitted packets may completely be destroyed by the interferer.

3.1.2.1 Implemented Testbeds

Testbeds are required in order to experimentally study the performance of IEEE 802.15.4/ZigBee networks/connections when experiencing interference from IEEE 802.11 WLANs/connections. Quite a few publications exist in the open literature, reporting work involving use of testbed facilities. A basic experimental testbed is normally composed of an IEEE 802.15.4/ZigBee transmitter, an IEEE 802.15.4/ZigBee receiver/coordinator, and a collocated IEEE 802.11b/g/n interferer that can be a laptop or a router generating Wi-Fi traffic. All these components can be arranged with different topologies for distinct objectives. A typical testbed can be found in [96] and is depicted in Fig. 3.1.

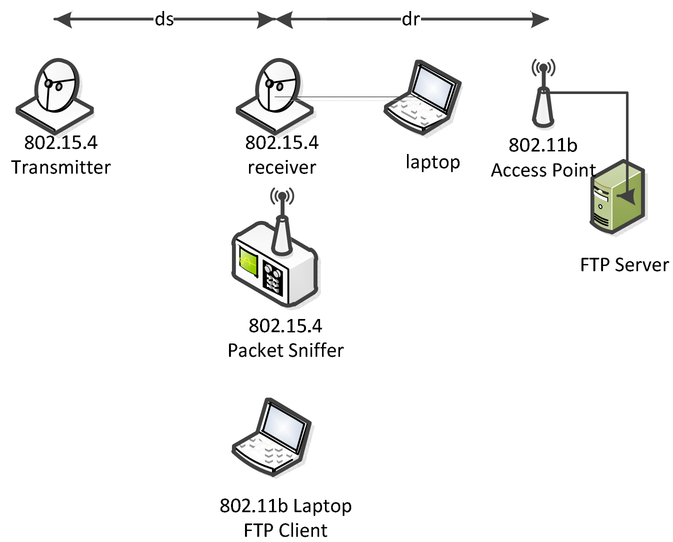

Fig.3.1 A Typical Testbed for Coexistence Study of ZigBee and Wi-Fi Communication System [96].

In Fig. 3.1, *ds* is the distance between the IEEE 802.15.4 transmitter and receiver, and *dr* is the distance between the IEEE 802.11b interferer and the interfered IEEE 802.15.4 receiver. There are two Crossbow MICAz motes acting as the IEEE 802.15.4 transmitter and receiver respectively. One IEEE 802.15.4 compliant packet sniffer is used to collect the received packets. The receiver forwards all the collected data to a laptop for storing and analysis. Another laptop equipped with an Intel PRO wireless 3945ABG (IEEE 802.11a/b/g) card is used as the network FTP client, and a router that is connected to the FTP server acts as an access point (AP) and interfering transmitter in Wi-Fi networks. Testbeds with different topologies can be found in [44][89][94][95][97].

Testbeds consisting of multiple IEEE 802.15.4 transmitters and one IEEE 802.15.4 coordinator are implemented in [90][98][99] for studying the combined interference from of Wi-Fi and competing IEEE 802.15.4 nodes. An example of such type of testbeds is illustrated in Fig.3.3. The testbeds in [96] and [99] include some other types of interferer besides IEEE 802.11b/g/n WLAN, such as IEEE 802.15.1/Bluetooth [99] and microwave oven [96]. Their interference effect on the performance of a collocated IEEE 802.15.4 WSN was evaluated and analyzed. In [89], a testbed with moving IEEE 802.15.4 motes is established to investigate the interference effect imposed on ZigBee network by Wi-Fi network from different distances and angels.

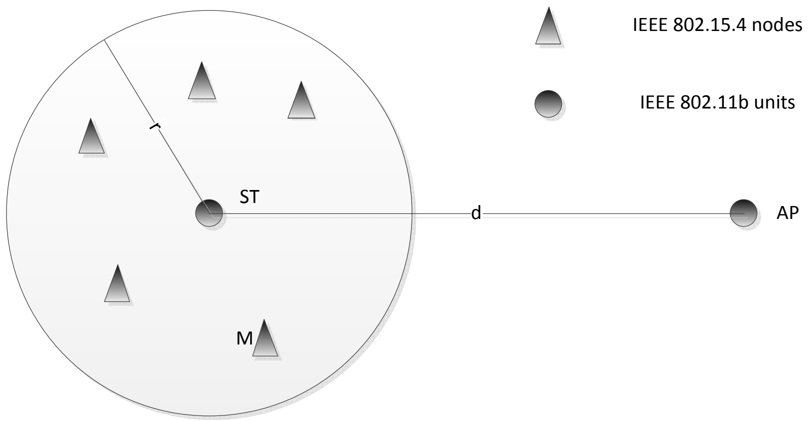

Fig.3.2 A Testbed for Coexistence Study of ZigBee and Wi-Fi Networks [89]

3.1.2.2 Performance Evaluation of WSN under WLAN Interference

There are many papers studying the coexistence issues between IEEE 802.15.4 WSNs and IEEE 802.11 WLANs in the past, e.g. [44], [89]-[100]. Most of these papers investigate the impact of mutual interference in terms of WSN Packet Loss Rate/Packet Error Rate (PLR/PER) or transmission throughput while varying various system parameters such as the packet size, packet rate, centre transmit frequency offset, and distance between WLAN nodes and ZigBee motes. The major findings and results are summarized as follows:

- **Packet Size**: [89] changes the payload sizes of both the IEEE 802.15.4 WSN and the IEEE 802.11n WLAN. From experiment results, some conclusions are drawn that the larger the WSN packet size or the WLAN packet size is, the higher the PLR can be expected when the WSN is suffering from the WLAN interference. The reason is that increasing either the WSN or the WLAN packet size can result in a higher possibility of collision occurrence between the WSN packets and WLAN packets.
- **Traffic Load**: The deterioration of IEEE 802.15.4 performance in terms of PLR worsens significantly with the increase of IEEE 802.11 WLAN traffic load [94]. Similar conclusions can also be found in [89], those being that a IEEE 802.15.4 WSN cannot successfully maintain its service quality when a collocated IEEE 802.11n WLAN is generating a medium or high traffic load. The IEEE 802.15.4 connections experience very high PLR. From the experimental results, [93] claims that interference effects of a WLAN on a WSN can be mitigated by reducing the WLAN duty cycle below a suitable threshold. Therefore, a WSN may coexist with a collocated WLAN but with a degradation of the throughput of the WLAN due to a lower duty cycle.
- **Signal to Interference and Noise Ratio**: The theoretical analysis of [95] gives as conclusion that if the in-band signal to interference and noise ratio (SINR) is larger

than 5-6 dB, an IEEE 802.15.4 packet could be successfully received with probability in the range of 99%. The experimental results in [93] show that the PLR of WSN strictly depends on the SINR. As long as the SINR does not go below a certain threshold, which varies upon different polling window which is the time interval reserved by the coordinator for communicating with one specific mote on a collision free basis, and can be experimentally determined, the PLR of WSN can remain on a very low level.

- **Centre Transmit Frequency Offset**: Several papers (e.g. [44], [89], [96] and [97]) investigated what effect has on the performance the frequency offset between the carriers of IEEE 802.15.4 and IEEE 802.11b/g signals[5]. Measurements were performed for different frequency offsets. From those studies, conclusions can be obtained that centre frequency offset can affect the WSN performance directly, i.e., the smaller the center frequency offset is, the more interference the WSN will suffer. It is also noted that even outside of the operating channel, the out-of-band power emitted by the IEEE 802.11b/g nodes is high enough to interfere with the IEEE 802.15.4 channels if WSN and WLAN transmitters are close enough [93].
- **Distance between WLAN Nodes and WSN Motes**: [95] reports the results of a series of experiments that vary the distance between WLAN nodes and WSN motes. From the measured results, the authors conclude that reliable communications among IEEE 802.15.4 WSN devices can be achieved if such distance exceeds a certain

[5] The carrier frequency of an IEEE 802.15.4 and/or IEEE 802.11 signal is right in the middle of the frequency channel it operates

threshold, otherwise reliable communications cannot be maintained under the interference from IEEE 802.11 WLAN[6]. On the other hand, [99] states that a WLAN appears to be immune to the interference of a ZigBee network when the distance between a WLAN source and a WLAN destination is smaller than 3m. Similar conclusion is drawn in [90]; that the IEEE 802.15.4 networks typically have little impacts on the IEEE 802.11b WLAN performance, which can be expected to hold true for IEEE 802.11g/n WLANs as well.

It is clearly shown from the above literature review that ZigBee communication will experience severe interference from the collocated Wi-Fi operating in overlap or adjacent frequencies and have deteriorated performance. Consequently, interference mitigation techniques are of great importance for addressing this issue.

3.1.3 Coexistence Model between ZigBee and Wi-Fi Packets

To study the interference effects between ZigBee and Wi-Fi communications when they are operating at overlapped or adjacent frequency and in proximity to each other, it is meaningful to develop suitable coexistence models that capture the characteristics of packet transmissions. Many researchers have developed and analyzed coexistence models between IEEE 802.15.4 and IEEE 802.11b/g/n (e.g. [95], [98], [99] and [100]). Most of them are based on forming collision time model between IEEE 802.15.4 packets and IEEE 802.11b/g/n packets or IEEE 802.15.1 (Bluetooth) packets. In the following, two typical time

[6] Our work has not investigated the distance, thus, we are not able to confirm the results of [95].

collision models between ZigBee packets and those of other wireless technologies operating in ISM band are presented and discussed.

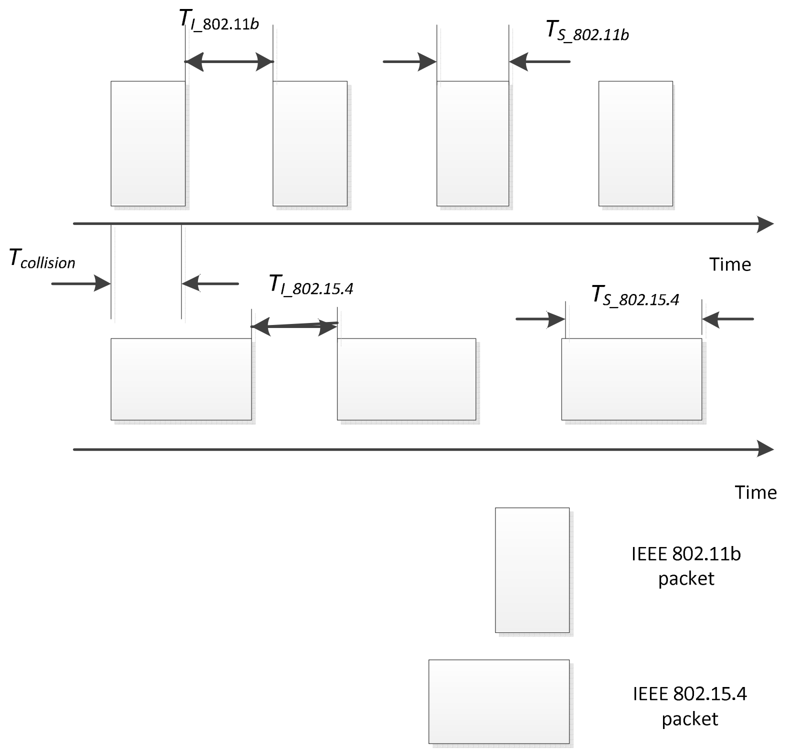

Fig.3.3 Packets Transmission of IEEE 802.11b and IEEE 802.15.4[100]

Fig. 3.3 [100] illustrates the time line comparison of packet transmission between an IEEE 802.11b WLAN and an IEEE 802.15.4 WSN. They denote $T_{I\_802.15.4}$ as the inter-arrival time of consecutive IEEE 802.15.4 packet, $T_{I\_802.11b}$ as the inter-arrival time of consecutive IEEE 802.11b packets, $T_{S\_802.15.4}$ as the transmission time of one IEEE 802.15.4 packet, and $T_{S\_802.11b}$ as the transmission time of one IEEE 802.11b packet. As shown in Fig. 3.3, due to its relatively low data rate, an IEEE 802.15.4 packet has considerably longer transmission time compared to the higher rate IEEE 802.11b network packets.

According to [90] and [99], IEEE 802.11b/g nodes normally cannot sense the IEEE 802.15.4 frames when in transmission, because the transmitting power of IEEE 802.15.4 nodes is considerably lower than that of IEEE 802.11b/g nodes. Thus an IEEE 802.11b/g node simply proceeds to transmit its packets even when there is an ongoing transmission of IEEE 802.15.4 packet in the channel. Contrarily to this, IEEE 802.15.4 nodes can sense the frame transmissions from collocated IEEE 802.11b/g nodes when occurring in their operating channel, and they detect them by using energy detection during their clear channel assessment processes. Thus an IEEE 802.15.4 node activates its transmission only when the operating channel is detected free, i.e., there are no Wi-Fi packets currently in transmission. To determine the channel's availability, the ZigBee mote performs CCA before sending out the packet. If the channel is detected to be busy, the transmission will be deferred in accordance to the exponential backoff algorithm defined in the CSMA/CA. However, since the transmission of IEEE 802.11b/g packets is independent from that of IEEE 802.15.4, it is possible that another IEEE 802.11b/g packet starts to transmit while IEEE 802.15.4 packets are still in transmission. In this case, IEEE 802.15.4 and IEEE 802.11b/g packets will collide with each other. $T_{collision}$ represents the collision time of the two frames. During such collision time, the higher power of IEEE 802.11b/g packets in transmission corrupts badly the low power IEEE 802.15.4 signal, generating a high bit error rate (BER). As a result, the IEEE 802.15.4 frame will be damaged and useful data cannot be extracted by the destination ZigBee mote.

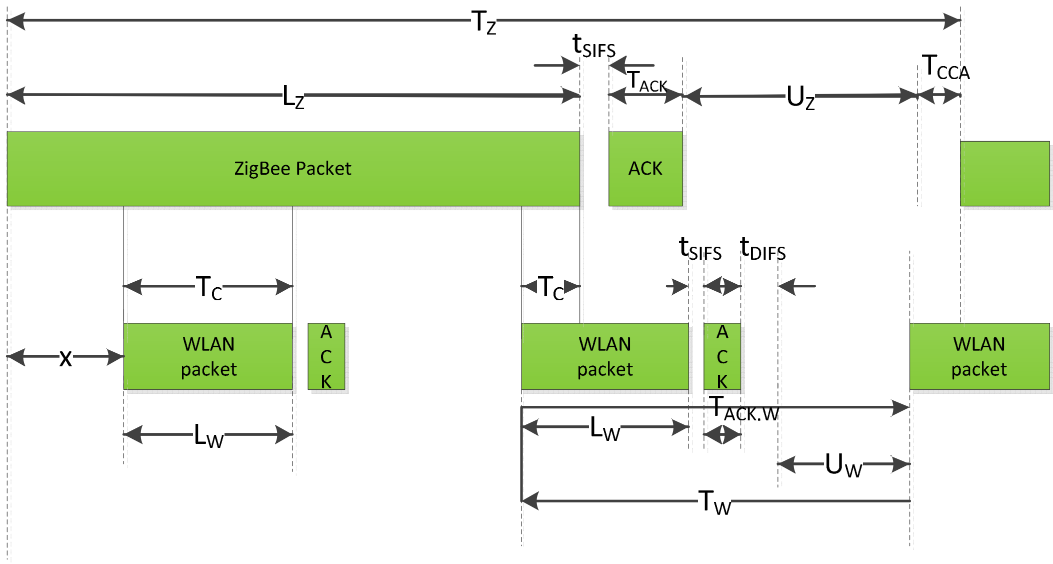

Fig.3.4 Time Collision Model between IEEE 802.11b Packet and IEEE 802.15.4 Packet [99]

An “blind” time collision model is introduced in [99] and has been widely adopted in coexistence issue studies (e.g. [101][102]). The term “blind” means that neither the IEEE 802.15.4 nodes nor the IEEE 802.11b nodes can sense each other. This model is depicted in Fig. 3.4. In this model, both IEEE 802.15.4 and IEEE 802.11b implement acknowledgement mechanism. Due to the characteristics of blind transmission, both the IEEE 802.15.4 and IEEE 802.11b nodes send out their packets without attempting sensing of the channel, which generates higher collision probability between frames of the two different standards.

3.2 Performance Study on the IEEE 802.15.4 CCA Mechanism

CCA is a type of channel sensing technology, which is implemented at the PHY of wireless communication networks and is an essential ingredient of CSMA/CA based MAC protocols. Although CCA itself is implemented at PHY, it has great impact on performance of the MAC sublayer metrics such as throughput, packet loss rate and energy efficiency.

As discussed in section 2.3, in order to sense the status of the operating channel, a CCA procedure is used by all network nodes. When the MAC sublayer receives a packet to transmit, it instructs the PHY to perform a CCA.

IEEE 802.11b/g/n Wi-Fi and ZigBee devices make use of CCA mechanisms. Varying some parameters of these schemes normally can result in different network performance. In this section, related research contributions studying the impact of CCA on ZigBee WSN's performance are reviewed.

Several papers (e.g. [89], [103]-[105]) studied the impact of different ED thresholds on the performance of WSNs. In addition to reporting the performance degradation experienced by the IEEE 802.15.4 based motes operating at ZigBee channels of different frequency offsets from the center frequency of the operation of a collocated 802.11n WLAN, [89] observes that the power transmitted by IEEE 802.11n nodes is high enough to seriously interfere with the IEEE 802.15.4 packets transmitting in ZigBee channels locating even outside of the IEEE 802.11n operating channel due to the highly sensitive ED threshold setting used in the IEEE 802.15.4 devices. Their measurement results show that different ED thresholds can affect the ZigBee performance under interference from IEEE 802.11n Wi-Fi devices operating in overlapped and even in non-overlapped channels. [103] investigates the ramifications of a single misconfigured node, and concludes that varying an ED threshold value implemented in a sensor node affects the network performance in terms of throughput. Through testbed based experiments, they demonstrate that ED threshold values within a given wireless sensor mesh network can affect a ZigBee system's performance, and the degree of impact varies with different network topologies. In [104], a series of experiments were performed during which IEEE 802.15.4 nodes were transmitting concurrently. Purpose of the work was to study the impact of ED threshold's value on the performance of IEEE 802.15.4/ZigBee networks. Their results show that collisions caused by concurrent transmissions in an IEEE 802.15.4 WSN does exist and an ED threshold set close to the operating environment noise floor helps to reduce the amount of such collisions significantly. In [105], CCA mode 1 and 2 operations in the presence of in-channel wide-band additive white Gaussian noise (AWGN) are examined through experimental tests performed by using an IEEE 802.15.4 testbed. Additionally, a series of experiments were carried out studying the impact of different ED thresholds under the same interference. The obtained experimental results show a close relationship between the used value of ED threshold and the immunity level WSN's nodes have in the presence of AWGN.

The above papers investigated the impacts of different ED thresholds or CCA modes on ZigBee WSN's performance. However, the optimized ED threshold or CCA mode is only relevant to specific network topology and interference. They have not studied how the value of ED threshold generating the best performance is affected by some significant network parameters, such as used packet size and/or packet transmission rate. Such knowledge can assist the design of superior CCA adaptation mechanisms.

Cross-layer evaluation of the impact of CCA on MAC performance of IEEE 802.15.4 in the absence of interference is performed in [106]. The study shows that inter-dependency exists between PHY CCA and MAC performance. They also evaluate the MAC performance in terms of packet arrival rate and PHY layer parameters such as SINR, carrier sense threshold and CCA power consumption.

Through these previous researches, the CCA mechanism is confirmed to have a significant impact on IEEE 802.15.4 WSN performance. The CCA modes and ED thresholds both can affect the performance of ZigBee system when it is suffering from the interference of Wi-Fi.

3.3 Adaptive Mechanisms for Interference Mitigation

As discussed in the previous sections, IEEE 802.15.4 WSNs have arising coexistence issues with high power high rate IEEE 802.11 b/g/n WLANs which share the same 2.4 GHz ISM band.

Such coexistence issues introduce severe interference problems that to great extent deteriorate the WSN performance, such as lower transmission throughput, higher packet loss rate, and longer transmitting delay. Therefore, developing techniques that can improve the reliability of WSN packet transmission becomes an important research area in WSN studies. There are many papers proposing adaptive mechanism in order to reduce the interference of IEEE 802.11b/g/n WLANs on the collocated IEEE 802.15.4 WSN devices. In the following, some of the most important interference mitigation mechanisms published in the literature will be summarized and discussed.

3.3.1 Frequency Agility Algorithm

Frequency agility-based interference avoidance algorithms [101][102][107] utilize interference detection (e.g. energy detection or frame error rate) and active avoidance to perform smart channel selection.

3.3.1.1 Interference Detection Scheme

Since ZigBee is a low energy cost networking standard, energy-saving interference detection scheme is essential for its working. From many papers reviewed in section 3.1, it has been concluded that ZigBee experiences significant interference in the in-door environment due to heavy traffic from collocated networks operating at the same ISM frequency band, especially from the high power WLANs. In order to effectively mitigate the interference and extend the battery lifetime, it is essential to design and implement an efficient interference detection scheme before activating any interference mitigation techniques.

Some interference detection schemes have been studied for sensor network in [108]-[111]. [108] presents a radio interference detection protocol to detect run-time radio interference among sensor nodes. However it focuses on the homogeneous network interference rather than heterogeneous networks. An interference detection scheme based on the ED results and RSSI is proposed in [109]. This scheme automatically performs a CCA sensing when a sudden degradation of transmission throughput is detected, which means that the throughput drops below a predefined acceptable value. If the RSSI measured by CCA returns that the energy level on the current channel is above a preset threshold, channel interference is recognized. In [110], a distributed interference detection scheme based on a heterogeneous network equipped with different functional devices is proposed, in which a combined interference detection scheme is established and can indicate the presence of interference. This mixed scheme includes different types of interference detection schemes, such as the ACK/NACK-based, the beacon-based, and the test frame-based schemes, which are implemented into corresponding functional devices. Devices in the same channel group but does not detect the interference directly can receive interference indications from those that have detected interference. [111] proposes an interference detection scheme which utilizes ACK/NACK reporting mechanism to detect interference. In this mechanism, the coordinator sends beacon frame to receivers in a time interval and counts the number of NACKs. If this number exceeds a predefined threshold, interference is assumed to exist. But this mechanism also has obvious downside which is that all ZigBee devices must respond to every beacon request according to the ZigBee standard. Such a scheme will result in significant energy waste throughout the network, which is unacceptable for low power ZigBee networks.

3.3.1.2 Interference Avoidance Scheme

The authors of [112] make an assumption that there are multiple ZigBee PANs coexisting and propose an interference avoidance scheme based on PAN priority. Two rules are set for setup PAN priority: 1) the lower interference a PAN experiences, the higher its priority will be; 2) if the rule 1 cannot be resolved, the lower PAN ID gets higher priority. In the presence of interference, low priority PAN is instructed to change to another free channel determined by the coordinator through means of beacon requests. A pseudorandom-based interference avoidance scheme is proposed in [107]. A pseudorandom sequence is established for channel selection. All devices suffering from interference jump to the next channel based on the sequence. However, other important parameters, such as all the available channel status or the level of interference for devices, are neglected, which obviously increases the delay and energy consumption and reduces the network stability.

[101][102] combine the operations of interference detection and interference avoidance schemes to effectively mitigate the interference from IEEE 802.11 WLAN and save battery energy as well. In their proposed mechanisms, each sender node measures its PER periodically. If the PER exceeds certain threshold, the sender will report to the router to check its link quality indicator (LQI). If LQI is below a certain value, the coordinator which receives the LQI from the router instructs all the routers in the PAN to perform interference detection of the all other channels. Interference detection is achieved by means of ED scans defined in the ZigBee protocol. Based on the feedbacks from all the ED scans, the coordinator selects a channel which has acceptable quality and also not used by other ZigBee PAN. Finally, all the PAN devices migrate to this “safe” channel. The flowcharts of the entire frequency agility mechanism are depicted in Fig. 3.5 including (a) interference detection scheme and (b) interference avoidance scheme.

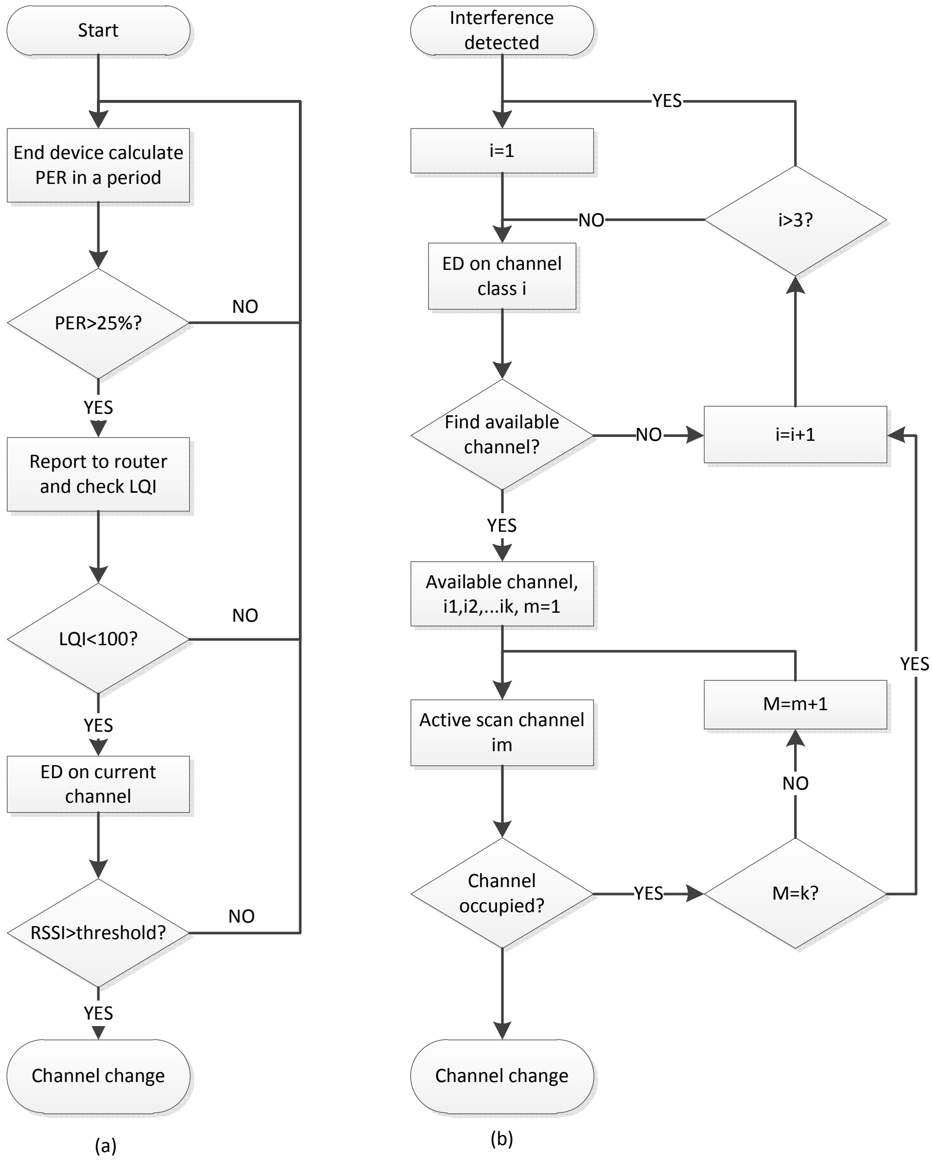

Fig.3.5 Flowchart of: (a) interference detection and (b) interference avoidance [101].

[107] proposes a proactive and network-centric interference mediation scheme in a network environment of WLAN and ZigBee devices. The scheme is composed of a channel status observation part that observes the status of the current operating ZigBee channel, and an interference mediation part that scans the existing WLAN AP channels using its

internal WLAN device and searches for available ZigBee channels not overlapping with the existing WLAN networks.

Although the frequency agility mechanisms such as those proposed in [101][102][107] have their advantages including saving energy on interference detection and realizing the channel selection without inducing complexity, switching the operating channel of the entire WSN in the interference avoidance process introduces considerable extra costs to the network. Particularly, when there are several WLAN APs in the vicinity operating at different channels, channel switching might happen very often and lead to an unstable IEEE 802.15.4/ZigBee WSN operation.

3.3.2 CCA/MAC Parameter Adjustment Mechanisms

In [113], the authors propose a technique to adaptively optimize the ED thresholds of IEEE 802.15.4/ZigBee WSN to mitigate interference from IEEE 802.11b/g WLAN, and reduce effectively the inhibition loss caused by channel access failures. The CCA threshold will be adaptively increased or decreased according to the rate packet transmissions are aborted due to busy channel. However, it is hard to set an appropriate threshold to this rate, especially when the interfering traffic is not heavy. This scheme also needs to interact with the coordinator for the calculation of packet loss rate and the issuing of commands for threshold adjustment. Most significantly, this technique ignores the impact of packet collision. It is observed in our experiments that in many cases only a very small portion of packets are denied access to the channel for CCA failures, while the packet loss rate is very high because of either collision with WLAN packets or the abortion due to high generation rate. When channel is detected to be idle by CCA, the packet is sent out immediately but still has a good chance of colliding with IEEE 802.11 WLAN packet because ZigBee has a much longer transmission time compared to those of Wi-Fi packets.

[114] discusses the slotted CSMA/CA in CAP, which has two CCAs (CCA1 and CCA2) implemented in the protocol before transmitting packets. However, CCA2 may fail in the case that the node performs CCA1 while at least one of the other nodes waits for the acknowledged packet after finishing transmission. However, in such case of CCA2 failure, the data packet can still be transmitted in the slot following the failed CCA2. Therefore, they propose a mechanism that will perform a third CCA (also called CCA3) to detect the channel after the CCA2 failed slot. This scheme can reduce the total number of CCA performed thus save energy and resource. However, it only addresses one special circumstance of CCA2 failure applied to slotted CSMA/CA. Therefore, its performance improvement is limited.

[115] proposes a method of extending the backoff time of an IEEE 802.15.4 compliant device which is used upon success in first CCA and failure in second CCA in the beacon-enabled IEEE 802.15.4 networks. This method is for reducing the possibility of collision occurrence between motes and the number of times of CCA performed in transmitting one frame, so as to improve throughput and reduce energy consumption of an IEEE 802.15.4 device. In [116], performance improvement schemes based on adjusting the MAC parameters are proposed. In this paper, two improved CSMA/CA mechanisms are implemented at MAC sublayer in order to achieve a better performance: a) enhanced

collision resolution mechanism, which adjusts the *BE* based on the combination results of CCA and the packet transmission; and b) enhanced backoff mechanism, which changes the range of backoff counters; this can reduce the frequency of occurrence of follow-up collisions, resulting in additional backoffs.

[117] proposes an ADaptive Access Parameters Tuning (ADAPT) algorithm which is implemented as a module of a cross-layer architecture. It estimates the current packet delivery ratio and automatically tunes MAC parameters according to specific applications with employment of management functions provided by the IEEE 802.15.4 standard. The operations of ADAPT are based on two different elements: a control scheme for estimating the delivery ratio and enforcing the requested reliability level; and a strategy for tuning the MAC parameters accordingly. ADAPT does not impose any modifications in the original IEEE 802.15.4 MAC protocol and thus it is easy to be implemented.

In addition, [93] states that interference effects of a WLAN on a WSN can be mitigated by increasing the WSN polling window and reducing the WLAN duty cycle below a suitable threshold. However, such technique shall lead to a degradation of both the WSN and the WLAN performance that has lower throughput for both networks (higher polling window for WSN and lower duty cycle for WLAN), which is not acceptable in quite a few circumstances i.e., multimedia applications. Also, the two suitable thresholds can only be determined through measurements and are strictly dependent on the characteristics of WLAN interference, which introduces more complexity and loses generality.

As discussed in previous paragraphs, [113]-[117] proposed several different adaptation mechanisms which adjust certain CCA or MAC parameters for achieving performance improvement of IEEE 802.15.4 based WSN when encountering interferences from collocated IEEE 802.11b/g/n WLANs. These mechanisms have their own distinct features and advantages and can be implemented effectively in some circumstances. However, they do not have the capability to sense the time or spectrum “holes” that can make the packet transmission more reliable nor the realization of better transmission timing for ZigBee packets to fit in these “holes”. Therefore, these technologies cannot efficiently adapt to the changing levels or characteristics of WLAN interferences, and thus may not function well in the presence of heavy interferences.

3.3.3 Collaborative Coexistence Mechanism

In [118], an adaptive collocated-collaborative coexistence mechanism that utilizes the RSSI and channel utilization information in WLAN beacon frame is proposed. This scheme includes two parts: a) scanning mode, during which the collocated WLAN station scans through 11 overlapping IEEE 802.11b WLAN channels for beacon frames and measures channel status/network condition information through RSSI value detection; b) active mode, during which the number of GTS for each ZigBee sensor node is calculated according to the sensor node’s data rate and PER for each ZigBee node. The collocated WLAN module shall always attempt to reserve channel for ZigBee beacon or GTS for ZigBee data transmissions.

[119] proposes to use a gateway device that has both ZigBee and WLAN interfaces, which will transmit a message containing purposely an error in order to silent the neighboring

WLAN nodes for a predetermined period so that the Zigbee nodes are able to communicate with each other without WLAN interference. [120] proposes a time-based coexistence method where a network control component coordinates the bandwidth usage of the two wireless networks that are competing for the same frequency band. The two networks respectively use the contention free period and contention access period of the superframe of the primary network. [121] proposes a coexistence system for integrating heterogeneous wireless network devices, which use an identical frequency band, into a single board. The IEEE 802.15.4 LR-WPAN generates an interrupt to make a request for active channel reservation, which is forwarded by a synchronization unit to the IEEE 802.11 WLAN. WLAN reserves a radio channel through an RTS(Request To Send)/CTS(Clear To Send) switching scheme according to the channel reservation request interrupt so that the IEEE 802.15.4 LR-WPAN is able to use the radio channel without WLAN interference.

[118] – [121] all require certain device or coordinator to coordinate the medium access. The coordinator collects received packets and statistically analyzes the status of the current channel frequency or the performance of IEEE 802.15.4 networks; and then accordingly sends out commands to distributed motes for adapting the entire network to changing conditions. However, the implementation of these techniques not only has significant impact on the performance of both networks but also requires substantial modification to them, which is not a simple task, especially when there are several WLAN APs and/or ZigBee networks co-existing and operating at different channels. The deployment of the ZigBee or WLAN network becomes inflexible as well. In addition, since the ZigBee packet

requires longer transmission time, silencing the WLAN for ZigBee packet transmission will result in considerable degradation of WLAN performance. Their implementation and inclusion as standard functionality in future Wi-Fi and ZigBee devices will induce considerable additional cost to the nodes of both technologies. Therefore, to develop an adaptive mechanism that can be implemented in the transmitting motes only and does not need the involvement of coordinators is becoming a challenging research area for WSN interference mitigation.

Chapter 4

Close Examination of CCA and its Corresponding Adaptation Mechanism[7]

From earlier discussions, it became apparent that due to their low transmitted power and low transmission rate, the performance of ZigBee networks can be impacted greatly by the interference generated by the collocated Wi-Fi networks. Major source of the problem is the significant disparity in levels of transmitted power nodes of the different standards generate. As indicated in chapter 2, most of the original research contributions available through the open literature focus on the effect different parameters of the ZigBee system such as ZigBee packet's size, central operating frequency offset and so on, have on performance. However, the characteristics of interfering traffic play a critical role in the coexistence issue. In agreement with results presented in earlier publications, our experimental results also show that interfering Wi-Fi traffic with the same throughput but different transmission rate/packet size combinations can generate noticeably different performance results for the ZigBee network.

[7] A version of this work will be submitted in the near future for possible publication in an IEEE journal. Yong Tang, Zhipeng Wang, Tianyu Du, Dimitrios Makrakis, and Hussein T. Mouftah, "Study of Clear Channel Assessment Mechanism for ZigBee Packet Transmission under 802.11g Wi-Fi Interference".

In our research, we investigate how the values assigned to CCA parameters impact the performance of a ZigBee connection subjected to different IEEE 802.11g Wi-Fi interferences with varying inter-departure times (IDTs) or packet sizes at the physical layer. We also propose an adaptation mechanism for improving ZigBee's performance. In terms of content of this chapter, a detailed description of our testbed is provided in section 4.1. Section 4.2 presents the results of our experimental studies of different CCA modes and thresholds, followed by an elaborate result analysis and discussion based on our collision model between IEEE 802.15.4 packets and IEEE 802.11g packets. The analysis also indicates that the current available analytical models for analyzing the coexistence issue of ZigBee and Wi-Fi need to be modified substantially to account for the many factors that impact the ZigBee packet transmission performance. Finally, in section 4.3, an adaptation mechanism which can improve ZigBee' s performance in some specific cases, which will be elaborated later, is proposed and discussed, and then evaluated by comparative experiments with the default CCA scheme. It should be noted that all the experimental results are marked with a 95% confidence interval in the following two chapters.

4.1 Testbed Description

The testbed includes ZigBee motes that can transmit and receive IEEE 802.15.4 packets, ZigBee coordinator acting as a gateway to PC, IEEE 802.11g based Wi-Fi router and PCs with compatible to Wi-Fi router network cards. In addition to some publicly available open-source software and commercial software package provided along with Crossbow products, we designed and developed a series of client software or scripts to realize the traffic generation and reception for both ZigBee and Wi-Fi connections.

4.1.1 Testbed Hardware

The architecture of our testbed is shown in Fig. 4.1. The experimental ZigBee and Wi-Fi communication links are formed by two ZigBee motes and two Wi-Fi nodes respectively. The Wi-Fi connection consists of an IEEE 802.11 b/g/n wireless router (WR) (ASUS RT-N16 [122]), a Dell Inspiron 1545 laptop with a Dell Wireless 1515 (IEEE 802.11 a/g/n) WLAN half mini-Card (Atheros) built in, and a laptop connected to one of the Ethernet ports of the WR. These two laptops are used for generating and receiving Wi-Fi packets. The power transmitted by the WR can be set to different levels, which allows generating different levels of interference to the ZigBee network. For the ZigBee connection, a pair of Crossbow MICAz motes is used to establish an IEEE 802.15.4 communication connection. Every mote is equipped with an IEEE 802.15.4-compliant CC2420 [123] transceiver which enables transmitting and receiving IEEE 802.15.4 traffic. An MIB600 programming board [124] is used in our testbed as a gateway for protocol translation from ZigBee to Ethernet, allowing the PC to collect all required data.

MICAz's processor and radio platform is MPR2400, which is based on the low-power microcontroller Atmel ATmega128L [125] and the CC2420 chip. The whole system runs MoteWorks [126], an end-to-end enabling platform for the creation of wireless sensor networks, stored in its internal flash memory. The customer sensor application and the network/radio communications stack are configured to run simultaneously. The IEEE

802.15.4-compliant CC2420 transceiver chip operating at the ISM band is designed and manufactured by Texas Instruments. It aims at providing professional grade communications to WSN systems having low power and low voltage requirements. CC2420 contains a digital direct sequence spread spectrum baseband modem, which offers a 9 dB spreading gain and 250 kbps data rate. CC2420 provides a large number of hardware support solutions including packet handling, data buffering, burst transmissions, data encryption, data authentication, CCA, LQI and packet timing information.

In addition to the ZigBee and WLAN components, another laptop is used in the testbed as a monitoring workstation (i.e. wireless sniffer) for capturing and analyzing the transmitted Wi-Fi packets, and a spectrum analyzer, Aeroflex 3252 which has a monitoring frequency range from 1 kHz to 8 GHz and a sweeping time of 10ms for our required band [127], is used to monitor those operational Wi-Fi and ZigBee frequency channels that are overlapping[8], and displays their power spectral content.

4.1.2 Testbed Software

For software used on the Wi-Fi part of the testbed is listed below:

- **The Distributed Internet Traffic Generator**: The D-ITG [128] is a software platform intended for generating traffic that simulates different deterministic and stochastic processes (e.g. exponential, uniform, Cauchy and normal) for both IDT and packet size random variables. It is running on the laptop that is connected to the WR and generates traffic that is having the other laptop as destination node. In our testbed, the D-ITG is

[8] We focus on the overlapping channel, in order to address the worst case scenario.

installed in both the transmitting and receiving laptops for establishing a Wi-Fi connection and produces the required interfering traffic. Using this software, we create Wi-Fi interference with different packet sizes and generating rates.

- **DD-WRT Router Firmware**: DD-WRT [129] is an open source firmware based on Linux that can be implemented in Wi-Fi routers and embedded systems. Noted that not all types of routers can support this firmware. The list of those that can support it includes the following Wi-Fi router models: Linksys WRT54G, Asus RT N16, Sitecom WL-105b. DD-WRT provides a great number of functionalities within the framework of the respective hardware platform used, such as altering the transmitting power, providing advanced QoS support, secure wireless communication, etc. This firmware is flashed into the WR. Functionalities added of the software, used in the experiments are alterations of Wi-Fi communication parameters, such as transmitting power, operating frequency channel and transmission data rate settings.

- **Wireshark network protocol analyzer:** Wireshark [130] is an open-source wireless packet analyzer. Its typical functionalities include network monitoring, analysis, debugging, and development of communications protocol. This software is activated on the monitoring workstation to capture the transmitted Wi-Fi packets for analysis and validation of their packet length, inter-arrival time, etc.

For the ZigBee connection, we developed our own software based on the software platform provided by Crossbow, MoteWorks, and implemented it in the MICAz motes. MoteWorks is a hardware-software system used for the design and development of reliable and flexible wireless sensor networks which includes processing and radio hardware, communication software for mesh networking, gateway functionality and monitoring and management tools. In our research, MoteWorks provides us a set of software development tools, such as MICA sensor board drivers, sensor signal processing handlers and communication message deliverers. In addition, a cross-compiler for the target mote platform and a built-in editor for developing TinyOS applications are also provided by MoteWorks.

TinyOS [131] is an open source, BSD-licensed operating system targeted for wirelessly communicating devices of small energy consumption. It can be used in devices forming wireless sensor networks and/or wireless personal area networks, in ubiquitous computing devices, in monitoring devices placed within smart buildings, etc. To ensure compatibility and reduce the complexity during the software development process, TinyOS provides a series of standardized software APIs or components for different hardware platforms, e.g. Crossbow MICAz platform and TelosB platform.

MoteWorks also provides XServe, a software tool that serves as the main gateway between wireless networks and client applications [132]. XServe is used to provide services to route data between the mesh network and higher level programs. It can process the collected raw data and convert them to a readable form as required by the client programs. In our experiments, Xserve is used on the data collection PC to route all the ZigBee packets for recording and analysis.

Using Moteworks' software and tools, we developed a series of programs enabling highly customizable ZigBee packet generation and reception, which allows controlling and setting the transmitting ZigBee packet size, packet generation rate and stochastic distribution of IDT, adjusting various MAC sublayer parameters, and collecting/recording received packet information for future analysis. In addition to our developed traffic controlling software discussed above, we also have designed the program for the preliminary adaptation mechanism, which can automatically alter CCA parameters to mitigate interference generated from collocated Wi-Fi networks. The adaptation programs will be described in details in later sections.

Some other important software components of MoteWorks we may exploit in the future are [132]:

- **MoteView:** MoteView is a software application that provides an interface between users and the deployed WSN. MoteView's main function is to provide a user-friendly interface for the visualization of the collected data as well as materializing simple, straightforward interaction to end users.
- **XMesh:** XMesh is a mesh networking protocol for wireless sensor networks developed by Crossbow, able to support multi-hop and ad-hoc communications. XMesh network is formed by a number of distributed wireless motes, with each mote communicating with the others. XMesh also directs packets to the base station, from which they are forwarded to a PC running client programs.

4.1.3 Testbed Setup

As discussed before, the testbed mainly contains a Wi-Fi connection part and a ZigBee connection part. The Wi-Fi part consists of a WR, one laptop with wireless card built-in that receives Wi-Fi packets. Another laptop is connected to one of the Ethernet ports of the WR and the generated Ethernet packets are then converted to Wi-Fi packets at the WR. The D-ITG is running on the laptop and generates traffic indicating the receiving laptop as destination node. Thus the WR is acting as the dominant interference source. In our experiments, by observing the power spectrum calculated and displayed by the spectrum analyzer, we confirmed that the signal transmitted by the wireless router can be set and kept at a very stable power level. In addition, experiments were performed to validate the statistical distributions of the IDT of the generated interference traffic. The IDTs of the generated packets were captured by Wireshark. IBM SPSS Statistics software was used to verify the statistical distributions of the IDT (e.g. mean and standard deviation) with the captured data. The statistical analysis results confirmed that D-ITG generates interference traffic with IDT following the required distributions. One Crossbow MICAz mote is used as ZigBee client, transmitting IEEE 802.15.4 traffic with different packet sizes, packet generation rates and IDT distributions in different experiments to the ZigBee coordinator. The coordinator is implemented by another MICAz mote installed on a Crossbow MIB600 programming board. A PC is connected to the MIB600 board, collecting the data received from the ZigBee coordinator. ZigBee client and coordinator software programs are developed and run on the MICAz motes. The PHY layer continuously samples the environment RSSI and the client software reads the RSSI value at a specific time interval so that the external noise level can be monitored in real-time, and allows the user to define the packet size, generation rate and IDT distribution. In addition, the ED threshold and transmit power of the motes can be adjusted as needed. The coordinator collects the received data packets and calculates statistics such as the number of received packets, cancellation packets, and so on. Our study focuses on assessing the impact different CCA modes and ED thresholds have on the quality of communication between two communicating ZigBee motes exposed to the interference generated by a closely located Wi-Fi node that is acting as main traffic source of the Wi-Fi network.

The default CCA mode of MICAz nodes is CS-ED with -77 dBm threshold. The results reported bellow correspond to the existence of one active IEEE 802.11g WLAN connection and one active ZigBee connection. As shown in Fig. 4.1, the MICAz mote acting as the sensor data source is located close to the Wi-Fi WR that is acting as the source for the Wi-Fi connection, whereas the sink mote is located close to the laptop that is acting as the sink of the Wi-Fi connection. The distance between WR and the source mote is 1m. The distance between the source mote and destination mote is 1.5m. The distance between the laptop acting as Wi-Fi traffic's destination and the sensor traffic' destination mote is 2m. In our testbed, the Wi-Fi traffic generating laptop and the experimental data collecting PC are connected by Ethernet cable to the WR and the ZigBee coordinator respectively. Thus their distances can be ignored and have no impact on testing results. The Wi-Fi router is set to use transmit power of 50 mW and generates IEEE 802.11g traffic; the transmitting mote sets the transmit power to be 0 dBm when sending out its IEEE 802.15.4 packets. There are no obstacles between any of the devices in the testbed. Therefore, the transmitting mote and the coordinator have an unobstructed line of sight path, ensuring a strong direct signal reaches the receiver.

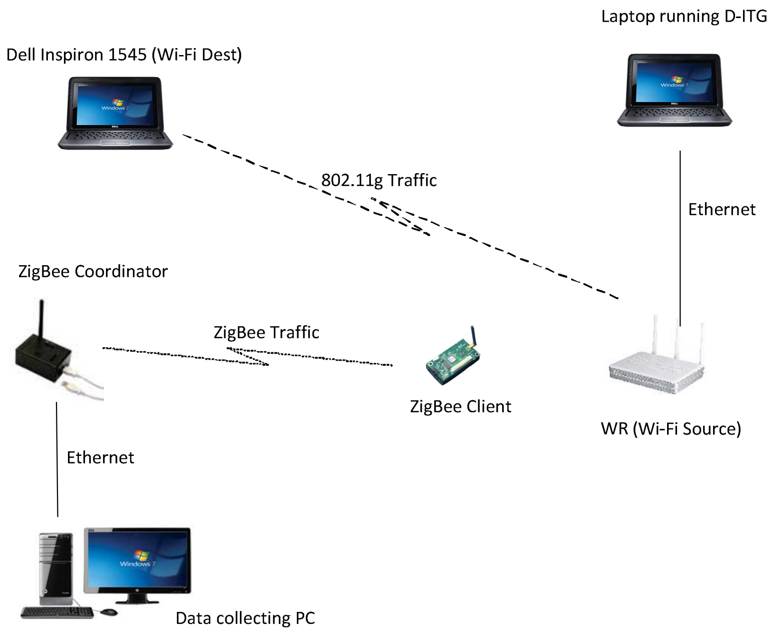

Fig. 4.1 Testbed' s Architecture

It should be noted that since there is only one Wi-Fi and one ZigBee connection, the use of CS is irrelevant, as there is no other carrier signal of the same standard to be identified by the CS module. Therefore only CCA in ED mode with different ED thresholds has been tested. The performance without ED is also evaluated for comparison. Fig. 1.3 shows the bandwidth allocation of WLAN and ZigBee at the ISM band. In our survey, during the time the experiments were performed, WLAN channel 9 was not used by any WR located in the Colonel By building of the University of Ottawa. Thus, we used channel 9 with the 802.11g Wi-Fi router of our testbed. It should be noted that commercial Wi-Fi products tend to generate some power outside the bandwidth of their operational channel, which generates interference to adjacent channels. Considering the significant difference in the levels of transmitted power, such interference can affect the performance of ZigBee.

Before investigating the CCA mechanism in ZigBee devices, the performance of ZigBee transmitting in channels 18 to 22 was evaluated. Channel 20 was found to have the highest packet loss rate; we thus concluded that this channel is experiencing the highest level of interference. This is reasonable, considering this is the ZigBee channel located within the range of Wi-Fi's channel 9 that has its highest level of power spectral density. Based on these results we conclude that in terms of ZigBee performance, the worst case scenario corresponds to the performance of channel 20.

4.2Experimental Results and Corresponding Analysis

This section examines what is the impact of ED threshold's value on the performance of the ZigBee system. The developed application runs on the ZigBee mote acting as the source which generates packets with constant packet IDT and packet length. After the MAC frame formed by one of those packets is transmitted, the source mote waits to receive ACK from the coordinator (acting as sink). If no ACK is received within a certain time frame, the source mote re-transmits the packet once. The D-ITG traffic generator running on the laptop generates UDP packets with different packet payload, packet rate and IDT distributions such as exponential distribution and uniform distribution. The generated traffic is passed to the WR, which transmits it in the format of IEEE 802.11g packets. It is noted that segments with payload size larger than 1500 bytes will be fragmented by Ethernet at MAC layer when the frame is transmitted from the traffic generating laptop to the WR, and then sent out in subsequent frames with an SIFS (Short Interframe Space) interval in between as defined in the standard [72].

4.2.1 Experimental Study of Different CCA Thresholds and Modes

Packet losses caused by one of the following three reasons have been identified from the results generated by our experiments:

1. **Packet cancellations due to CCA detection failures:** According to the IEEE 802.15.4 MAC layer CSMA/CA mechanism described in Chapter 2, the mote senses the availability of the channel using CCA technique before sending out any packets. If the channel is determined to be busy, the transmission of the packet is backed off and waits for the next sensing[9]. After a frame goes through a certain number of backoffs, with default value set to 5 as in the IEEE 802.15.4 standard, without having successful transmission, it is dropped, leading to packet loss. When ZigBee packet transmission is under severe interference, the number of packet loss because of the described reason can be high.
2. **Packet loss due to collisions with interfering WLAN traffic**: ZigBee and Wi-Fi are using the overlapped channels for packet transmission in the experiments. Due to its low transmission speed, the ZigBee packet has a considerably longer channel occupation time compared to that of a Wi-Fi packet. Thus,

[9] For clarification, in the case of ZigBee/IEEE 802.15.4, a frame is backed-off when CCA senses busy channel, which is different from the case in Wi-Fi/IEEE 802.11.

while a ZigBee packet is in transmission, it is possible a Wi-Fi node will start transmitting before the end of ZigBee node's transmission, which generates a damaged packet reception. The larger the size of the ZigBee packet is, the larger the probability that such event will occur.

3. **Packet drops due to CC2420 Transmit First In First Out Byte Register (TXFIFO) overflow**: In our experiments, the transmitting ZigBee mote generates packets at constant intervals as in periodic monitoring applications. The time for completing a packet transmission might include the packet transmission and re-transmission time, ACK waiting, transmission time of ACK, time consumed for CCA detections and time due to backoff. This time duration might well exceed the time interval for generating the next packet. According to the CC2420 data sheet [94], there is only one 128-byte large transmission buffer (TXFIFO) for accommodating the frame being transmitted, i.e., the "TXFIFO can only contain one data frame at a given time". Therefore, a newly generated packet will be dropped if the TXFIFO is being occupied by the preceding frame that is still in the transmission process.

Having identified the causes of packet loss, we proceed to present performance evaluation results generated by experiments focusing on assessing how different ED thresholds and CCA modes affect ZigBee' s packet loss rate under different Wi-Fi interference.

Experiments were performed for two different interfering 802.11g traffic scenarios. One is using 1000-byte UDP segment payload with a generation rate of 1000 segments/second;

the other is using 5000-byte payload and 200 segments/second. The percentage of channel utilization for both cases is around 20%.For both cases, the traffic generator is set to use a constant segment inter-departure time. Figs. 4.2-4.5 illustrate the total packet loss rate (PLR), packet collision rate (PCR) due to collisions with interfering Wi-Fi traffic, the packet drop rate (PDR) due to TXFIFO overflow. The displayed data points are marked with a 95% confidence interval. It should be noted that the collected experimental data shows that the packet cancellations due to channel been detected as busy is negligible. In our experiments, with ED thresholds ranging from -57dBm to -92dBm, the number of cancellation in most experiments are less than 10 out of over 10000 packet transmission attempts. Thus, it is safe to conclude that packet cancellation doesn't have major impact on the packet loss rate of ZigBee systems.

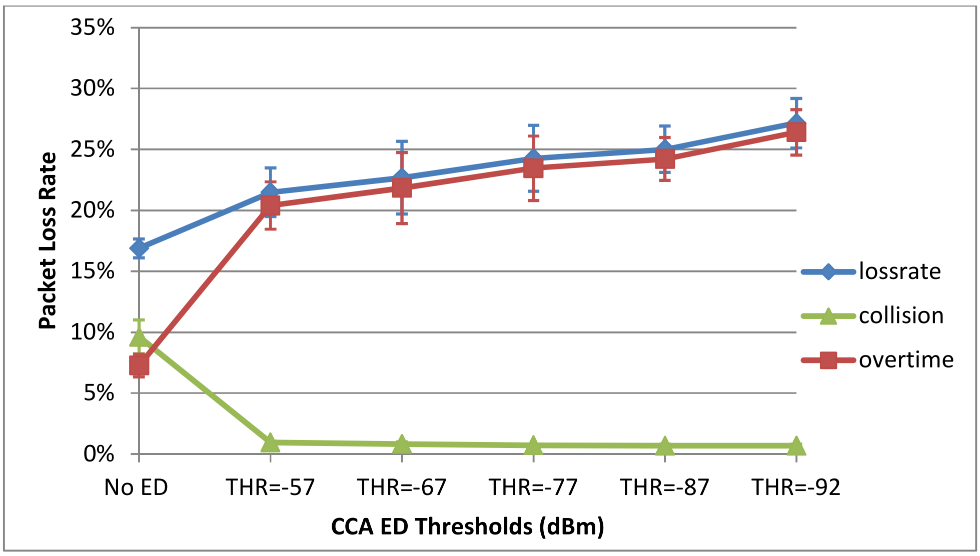

Fig. 4.2 ZigBee performance at a rate of 100 packets/second with different ED thresholds under interfering UDP traffic with payload of 1000 bytes/segment and rate of 1000 segments/second

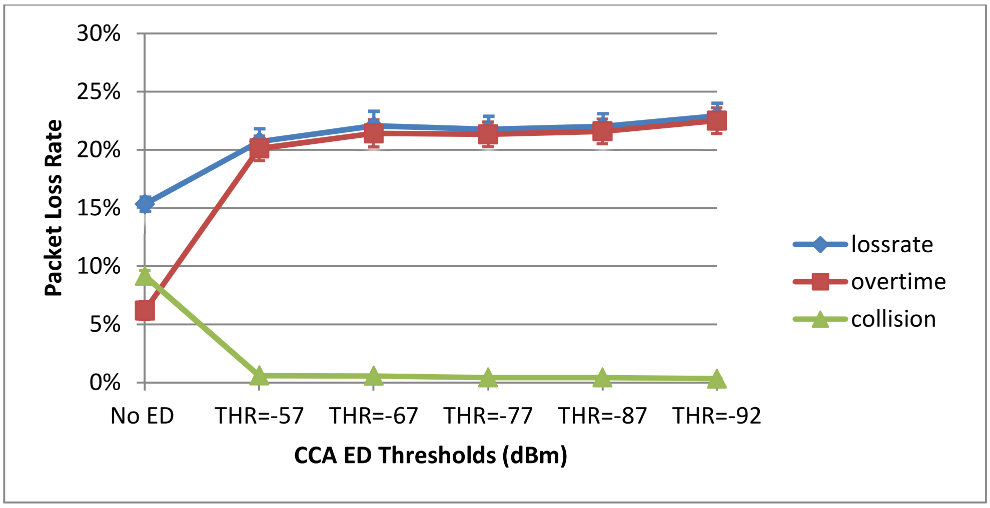

Fig. 4.3 ZigBee performance at a rate of 100 packets/second with different ED thresholds under interfering UDP traffic with payload of 5000 bytes/segment and rate of 200 segments/second.

Figs. 4.2-4.3 illustrate the PLR, PCR and PDR of the ZigBee connection under Wi-Fi interference. The ZigBee source generates traffic at a constant packet rate of 100 packets/second. Interestingly, the curves displayed on Figs. 4.2 and 4.3 indicate that the performance is better with ED disabled when there is a substantial number of packet drops due to TXFIFO overflow. There are several factors contributing to the occurrence of TXFIFO overflow such as ZigBee packet transmission rate, external interference conditions, the configuration settings of MAC layer parameters and retransmission mechanism. It can be seen that in both figures the dominant factor causing packet loss is the TXFIFO overflow. When the ED threshold is set to a lower value, the transmitting mote becomes more sensitive to external interference and enters or stays longer at backoff stages. The lower the threshold is, the more the generated backoffs become, which in turn leads to more packet drops due to buffer filling. ZigBee packets are transmitted at a very low rate compared to Wi-Fi packet transmission (250 kbps maximum for ZigBee versus 54 Mbps maximum speed with 802.11g[10]). In the two cases shown in Fig.4.2 and Fig.4.3, the time gap between two consecutive Wi-Fi packets is 1 ms and 5 ms respectively, corresponding to two Wi-Fi traffic with rate of 1000 segments/second and size of 1000 bytes/segment, and rate of 200 segments/second and size of 5000 bytes/segment respectively. One ZigBee packet needs considerably longer transmission time (3.2ms for a 100-byte packet) compared to the time gap between two consecutive Wi-Fi packets (around 1 ms) in the first case. On the other hand, the interval between two 802.11g packets (around 5ms) in the second case is longer than the transmission time of one ZigBee packet. As long as ED detects the Wi-Fi interference and defers transmission to avoid collisions, ZigBee packets transmitted under interfering traffic with longer packet IDT have better chance to be delivered. Therefore, for each ED threshold, the PLR and PCR values displayed in Fig. 4.2 are higher than those of Fig.4.3. It can also be seen from the curves of Figs. 4.2 and 4.3 that the packet losses due to collisions with IEEE 802.11g packets are approximately the same for all the ED thresholds under investigation. The performance of packet transmission between two ZigBee nodes shows consistency as long as the ED threshold is neither too low (might trigger "false alarms") nor too high (might fail to detect external interference).

[10] The pilot signal use 6 Mbps to transmit, thus the entire data rate is less than 54 Mbps. However we will use the 54 Mbps value since this is generally known and accepted.

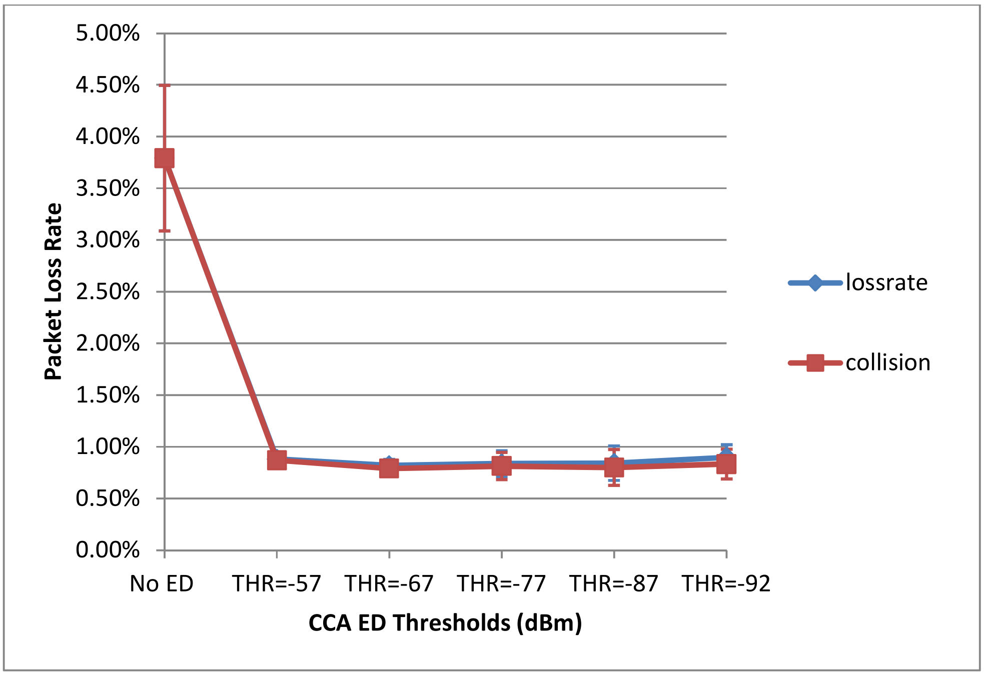

Fig. 4.4 ZigBee performance at a rate of 20 packets/second with different ED thresholds under interfering UDP traffic with payload of 1000 bytes/segment and 1000 segments/second.

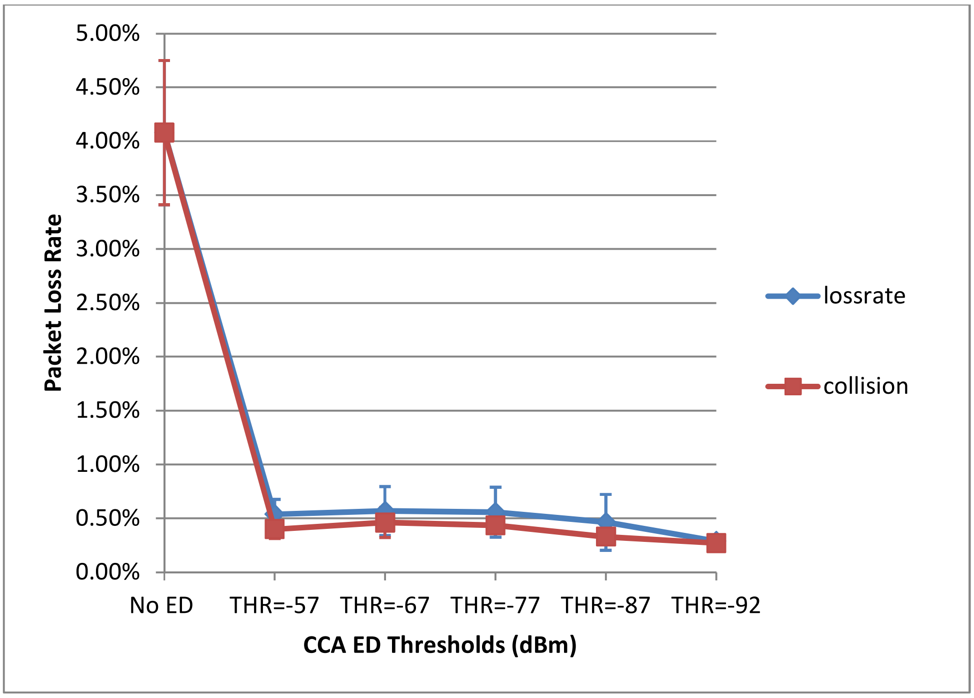

Fig. 4.5 ZigBee performance at a rate of 20 packets/second with different ED thresholds under interfering UDP traffic with payload of 5000 bytes/segment and 200 segments/second.

Figs. 4.4 and 4.5 show the PLR and PCR behavior of a ZigBee connection with a constant packet rate of 20 packets/second subjected to different interference from the IEEE 802.11g Wi-Fi transmission. Since in this case the interval between two subsequent ZigBee packets is considerably longer, the packet drops due to TXFIFO overflow are negligible (less than 10 out of the 10000 transmitted packets) and corresponding curves haven't been included in both figures. Again, the packet losses due to collisions with IEEE 802.11g packets are approximately the same for all tested ED thresholds. Low values of (i.e., more sensitive) ED threshold work better when the interval between two IEEE 802.11g packets is longer.

Another interesting observation is that when the ED of CCA is disabled, ZigBee transmissions under both Wi-Fi interference conditions have very similar PLR. While it is difficult to provide precise close-form expressions for analyzing the PLR, we use collision time model similar to that proposed in [99] for the explanation of these experimental results.

4.2.2 Analysis of Experimental Results

While the analytical model described in [99] is popular and widely adopted by many researchers (e.g. [101], [102]), as stated in our review in Chapter 3, the "blind" assumption is unrealistic and cannot be applied for explaining our experimental results. We extend the model to include the consideration of ED, i.e., the ZigBee transmitting mote can detect Wi-Fi interference if ED is enabled in CCA, and derive expressions for Wi-Fi interfering traffic with different packet sizes and rates according to our experiment setup. The analysis partially explains the observed experimental results and also shows that the existing time collision model needs substantial modification to account for several hidden factors (e.g. corrupted preamble and collisions due to transmitter-receiver turnaround time) in addition to ED that could have impact on ZigBee' s packet transmission performance. In the following, the detailed analysis and discussion are presented.

Since the interval between the Wi-Fi/IEEE 802.11g data packet and its corresponding ACK packet, the SIFS, is 10μs, which is much shorter compared to the duration for transmitting a data packet, the data and its ACK packets can be considered as a block of time with uninterrupted transmission. The assumption simplified the analysis without sacrificing its accuracy.

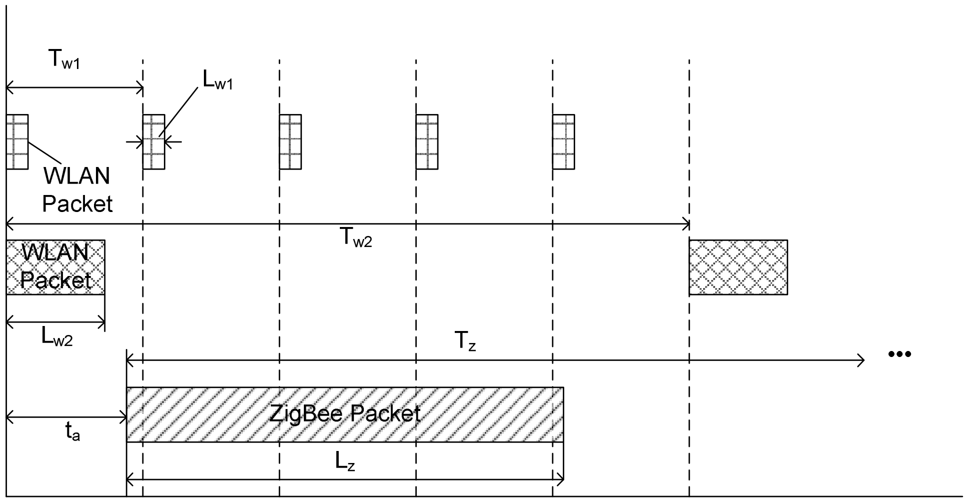

Fig. 4.6 Interference Model between ZigBee and WLAN Frames

Fig. 4.6 illustrates the two interfering Wi-Fi traffic patterns used in the experiment, the ZigBee traffic under evaluation and their relationship in reference to time. We are considering a constant packet transmission rate for both Wi-Fi and ZigBee connections, thus the packet inter-departure times are constant. T_{wk} denotes the constant Wi-Fi packet inter-departure time and L_{wk} denotes the Wi-Fi packet's transmission time (k = 1, 2). Also let L_z be ZigBee packet's transmission time and T_c be the time duration ZigBee and Wi-Fi packets overlap. We will be calling T_c as *collision time*. When there is no CCA ED employed, the time of initiating the transmission of a ZigBee packet is unaffected by the state of the channel; in this case presence or absence of interference. In other words, the ZigBee packet can arrive at any time in the period of [0, T_{wk}]. Thus, the offset time between the initiation of the transmission of a ZigBee packet and the initiation of the transmission of a Wi-Fi packet, represented as t_a can be assumed to be taking values with within the interval [0, T_{wk}] and statistical occurrence described by uniform distribution. Let $n = \lfloor L_Z/T_{wk} \rfloor$, where $\lfloor x \rfloor$ is the largest integer that is smaller than or equal to x. The value of T_c can be derived from Fig.4.6 and depends on the value of t_a. t_a of different value within [0, T_{wk}] is used to derive the corresponding expressions of $T_c(t_a)$. For $L_Z \geq nT_{wk} + L_w$, we have

$$T_C(t_a)=\begin{cases} (n+1)L_{wk}-t_a, & 0\leq t_a \leq L_{wk}, \\ nL_{wk}, & L_{wk}\leq t_a \leq (n+1)T_{wk}-L_z, \\ nL_{wk}+L_z+t_a-(n+1)T_{wk}, & (n+1)T_{wk}-L_z\leq t_a\leq (n+1)T_{wk}+L_{wk}-L_z, \\ (n+1)L_{wk}, & (n+1)T_{wk}+L_{wk}-L_z\leq t_a\leq T_{wk}. \end{cases} \tag{4.1}$$

And for $L_Z < nT_{wk} + L_w$, , we have

$$T_C(t_a)=\begin{cases} nL_{wk}+L_z-nT_{wk}, & 0\leq t_a\leq nT_{wk}+L_{wk}-L_z, \\ (n+1)L_{wk}-t_a, & nT_{wk}+L_{wk}-L_z\leq t_a\leq L_w, \\ nL_{wk}, & L_w\leq t_a\leq (n+1)T_{wk}-L_z, \\ t_a+L_z-(n+1)T_{wk}, & (n+1)T_{wk}-L_z\leq t_a\leq T_{wk}. \end{cases} \tag{4.2}$$

As an example for explaining the above equations, we consider the case of Wi-Fi interfering traffic generated by 1000 segments/second and payload of 1000 bytes/segment. In this case, we have $n = 3$, T_{W1} = 1 ms, and L_{W1} = 0.226 ms (how to get this value will be explained later). Since $L_Z = 3.2 < 3*1 + 0.226$, Eq. (4.2) is used. When t_a has a value between [0, 3*T_{W1} + L_{W1} - L_Z], it is straightforward to derive from Fig. 4.6 that the collision time is 3*L_{W1} + L_Z – 3*T_{W1}. The rest of the $T_C(t_a)$ in Eq. (4.2) can be derived following the same method.

Then the average collision time experienced by a ZigBee packet can be calculated as

$$T_C = \frac{1}{T_{wk}} \int_0^{T_w} T_C(t_a) dt_a \tag{4.3}$$

As in [72], we denote P_b as the bit error rate (BER) without Wi-Fi interference, P_b^I as the BER with Wi-Fi interference, and t_b as the duration of a bit transmission. The packet error rate can be derived as:

$$PLR = 1 - [(1-P_b)^{L_z/t_b - \lceil T_c/t_b \rceil} \times (1-P_b^I)^{\lceil T_c/t_b \rceil}] \tag{4.4}$$

where $\lceil x \rceil$ is the smallest integer greater than or equal to x. Therefore, the difference of PLR observed in the Figs. 4.2-4.5 can be explained by comparing the T_c of each test scenario.

The header sizes of IEEE 802.11g Link/Network Access, IP and UDP layers are 34, 20 and 8 bytes respectively [133].There is also a 4-byte FCS footer at the MAC layer. These headers, footer and UDP data segment combined together construct the 802.11g MPDU, which is transmitted at 54Mbps. At 54Mbps, each symbol encodes 216 bits [134], and takes 4µs to be transmitted [135]. Thus, given a UDP segment payload of L_p bytes, the total time we need to transmit the MPDU is $T_{MPDU} = \lceil 8 * (L_p + 66) / 216 \rceil * 4\mu s$. Each frame has a 20μs header to synchronize with the receiver and a 6μs signal extension duration [133]. After a *SIFS*, an IEEE 802.11g ACK will be transmitted to acknowledge the reception of the data packet. This ACK packet is 14 bytes long and needs one symbol to transmit. Thus, the ACK has a transmission duration of T_{ACK}= (20 + 1 * 4 + 6)μs = 30μs. Therefore, the entire packet transmission duration is L_W = (26 + T_{MPDU} + 10 + 30)μs. Taking a UDP segment with 1000-byte payload as an example, the transmission duration is 226μs, within which there is a 10μs vacancy. In case fragmentation occurs, each fragment is sent out after the preceding one with a *SIFS* interval of 10μs. Similarly, the 5000-byte payload will be fragmented into 4 fragments, each of which has an ACK to acknowledge its reception and a SIFS time interval in between. Thus, the calculated transmission time of a UDP data segment with 5000-byte payload is 1074μs, within which 70μs is vacant.

For UDP traffic with payload of 1000 bytes/segment and 1000 segments/second (scenario 1) we have T_{w1} = 1 ms and $L_{w1} \approx$ 0.226ms and UDP traffic with payload of 5000 bytes/segment and 200 segments/second (scenario 2) T_{w2} = 5 ms and $L_{w2} \approx$ 1.074 ms for the UDP traffic with payload of 5000 bytes/segment and 200 segments/second. For the ZigBee traffic under evaluation, with 100 bytes/packet, we have L_z= 3.2 ms. Substituting these values to Eqs. (4.1) - (4.3), the average collision time T_c when interfering is calculated to be around 0.59ms for scenario 1 and 0.69ms for scenario 2, which explains why the experiments give similar PLR results for both traffic scenarios when ED is not used.

When the ED mechanism is adopted in CCA, the transmission of ZigBee packet will start only when there is no Wi-Fi packet transmission in the channel. In this case, the ZigBee mote performs ED before sending out the packet. If the channel is detected to be busy, the transmission will be deferred following the exponential backoff algorithm. For a simplified estimation, we assume the arrival time of a ZigBee packet still follows the uniform distribution in the silent period when there is no Wi-Fi packet transmission. Following similar analysis discussed earlier, for $L_Z \geq nT_{wk} + L_w$, we have

$$T_C(t_a) = \begin{cases} nL_{wk}, & L_{wk} \leq t_a \leq (n+1)T_{wk} - L_z, \\ nL_{wk} + L_z + t_a - (n+1)T_{wk}, & (n+1)T_{wk} - L_z \leq t_a \leq (n+1)T_{wk} + L_{wk} - L_z, \\ (n+1)L_{wk}, & (n+1)T_{wk} + L_{wk} - L_z \leq t_a \leq T_{wk}, \end{cases} \tag{4.5}$$

and for $L_Z < nT_{wk} + L_w$, we have

$$T_C(t_a) = \begin{cases} nL_{wk}, & L_{wk} \leq t_a \leq (n+1)T_{wk} - L_z, \\ nL_{wk} + L_z + t_a - (n+1)T_{wk}, & (n+1)T_{wk} - L_z \leq t_a \leq T_{wk}, \end{cases} \tag{4.6}$$

Using Eqs. (4.5) and (4.6), the average collision time for two Wi-Fi traffic scenarios when ED is used is calculated to be around 0.54ms and 0.57ms. Although the experimental results verified the performance improvement when using CCA ED, the small difference of the analytical results between no ED and ED (0.59ms vs. 0.54ms and 0.69ms vs. 0.57ms) cannot explain the significant difference of PCR performance between no ED and with ED (using various threshold values) shown in Figs. 4.2-4.5. In our opinion, this discrepancy happens because the collisions with interfering Wi-Fi packets have different effect on data and preamble of the ZigBee packet. Preamble collisions might have more devastating effect on packet transmission because the transmitted packet won't be recognized by receiver if the preamble is corrupted. CCA with ED can avoid a large portion of such preamble collisions, thus achieve better performance in terms of PCR. In addition, after performing CCA, ZigBee transmitter needs to wait for a turnaround time (around 200 μs) [46][123] before sending out the packet. For higher Wi-Fi packet transmission rate, there is a greater chance that a Wi-Fi packet will occupy the channel during the turnaround time and cause preamble error of ZigBee packets, which in consequence results in more packet loss when the packet arrival rate of interfering Wi-Fi traffic is higher. This analysis indicates that the collision time model proposed in previous research contributions (e.g. [101], [102]) should be modified substantially to take into account several additional performance impacting factors such as preamble collision effect and TXFIFO overflow dropping, for accurately analyzing the performance of ZigBee packet transmission with ED in effect

4.3 Adaptation Mechanism for Improving Performance

All these experimental results have shown that CCA mechanisms and the value of ED threshold have impact on the performance of a ZigBee system operating under Wi-Fi interference, especially for traffic intensive applications (e.g. multimedia sensor network applications and surveillance applications that require real time and large amount of data transmission). It is also noticed that CCA has different impact on the performance of ZigBee packet transmission when the interfering Wi-Fi traffic has different characteristics, namely packet size and packet inter-arrival time. Low ED threshold can achieve better performance in terms of PCR but results in many packet losses due to TXFIFO overflow. Different interfering Wi-Fi traffic characteristics have different impact on these two aspects. As indicated earlier, the relatively low transmission rate of ZigBee results in a much longer channel occupation time for ZigBee packet transmission. As a result, when Wi-Fi packets arrive very frequently, i.e. with very short channel silent intervals, ZigBee packets might encounter quite a few collisions even when ED is adopted. The reduction in collisions might not outnumber the TXFIFO overflow packet drops, thus offering no improvement or even generating overall worse performance. On the other hand, when Wi-Fi packets arrive with long inter-arrival time, ED is very effective in locating the period suitable for ZigBee packet transmission, which subsequently increases the number of successful packet transmissions. When there are more reduced collisions than overtime packet drops, performance can improve. Figs. 4.7–4.8 illustrate such cases when the ZigBee mote is transmitting at 50 packets/second.

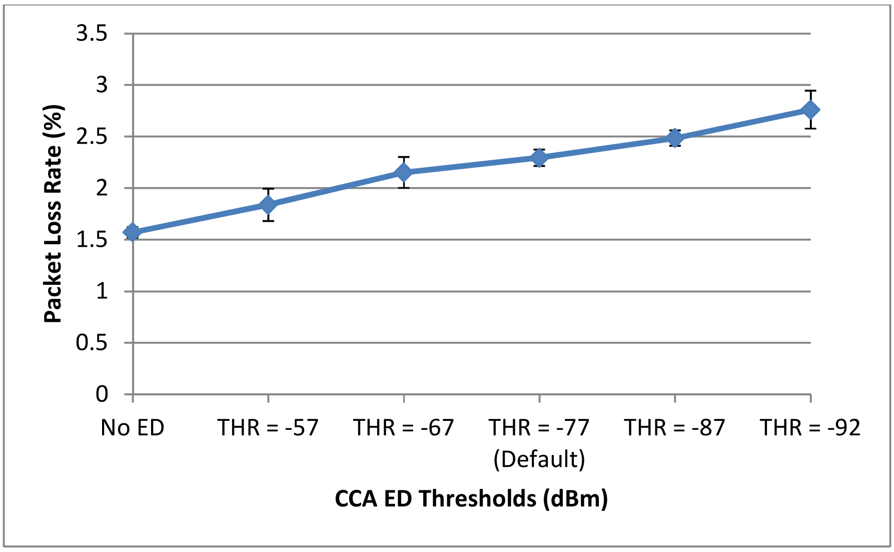

Fig. 4.7 PLR as a function of ED thresholds under interfering IEEE 802.11g UDP traffic with payload of 1500 bytes/segment and 500 segments/second.

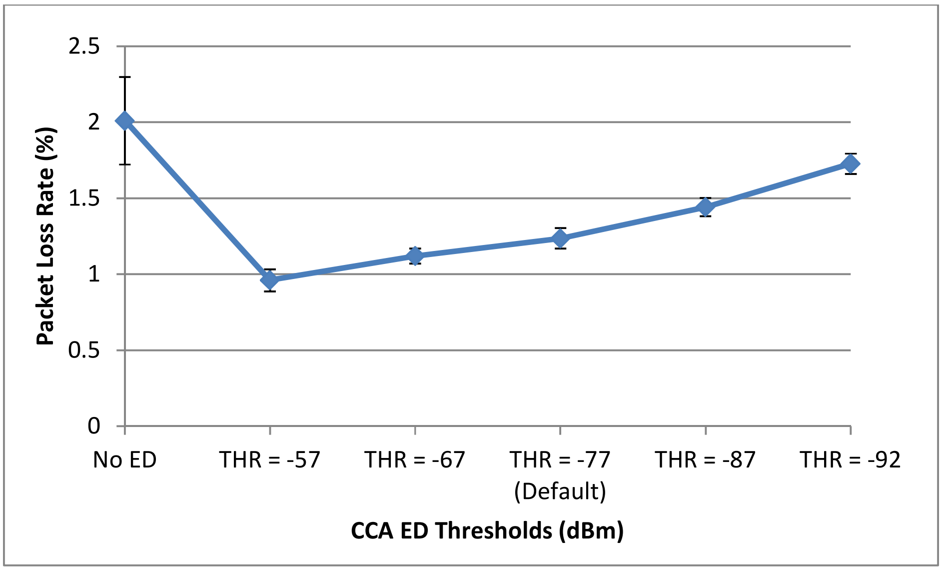

Fig. 4.8 PLR as a function of ED thresholds under interfering 802.11g UDP traffic with payload of 3000 bytes/segment and 250 segments/second.

By decreasing the ED threshold, the transmitting mote can assess the channel status with higher sensitivity and accuracy so as to reduce the number of packet collisions. However in the meanwhile, the decrease of ED threshold might also result in excessive transmission deferrals which could lead to multiple packet losses due to TXFIFO overflow. In Fig. 4.7, the decrease of ED threshold results in a higher PLR, which indicates that the dominant cause of packet loss is TXFIFO overflow. On the other hand, it can be observed in Fig. 4.8 that setting the ED threshold at -57 dBm achieves a better performance compared to other ED threshold values investigated, which is a result of the combined effect of the impact two mechanisms; TXFIFO overflow and packet collisions.

With these observations, it is possible to improve the performance of ZigBee packet delivery rate when there is varying interference from the collocated WLAN by switching the CCA mode according to the statistical results of TXFIFO overflow packet drops and total packet losses[11]. Based on the experimental results, we implement a preliminary adaptive mechanism that changes the CCA mode according to the tradeoff between TXFIFO overflow and collision loss. The transmitting mote and coordinator calculates the TXFIFO overflow and total packet loss during packet transmissions for initial channel performance assessment with or without ED employed. The transmitting mote then chooses the CCA mode that achieves better performance. Any significant changes on TXFIFO overflow or total packet loss would indicate a change of the external interference. The transmitting mote then performs another channel performance assessment for different CCA modes when CCA mode changes if needed. In order to evaluate the performance of our adaptive algorithm with changing interference, in the next set of experiments, the performance of the ZigBee packet transmission under an interfering Wi-Fi traffic applying such adaptive mechanism is evaluated. The interfering traffic starts with 802.11g UDP segments payload of 1500 bytes/segment and generation rate of 500 segments/second. It then changes payload to 3000 bytes/segment and generation rate of 250 segments/second after having gone half-way through the experiment or vice versa. This traffic style corresponds to traffic1 in Fig. 4.9. The experimental results are illustrated in Fig. 4.9. It can be observed from the figure that CCA with default ED threshold setting of -77 dBm has the worst performance while our adaptation mechanism achieved a PLR of 30% less than that of the default one. Compared to CCA with the optimal threshold of -57 dBm, the adaptation mechanism still managed to improve the performance by about 20%. It is noted that this ED

[11] We can record the overall loss packets, TXFIFO overflow packets, CCA failure cancellation packets. Then the collision packets equals to the overall minus overflow minus cancellation

threshold of -57 dBm that achieved best performance in Fig. 4.8 is only valid for this particular testing environment and may vary for other environments.

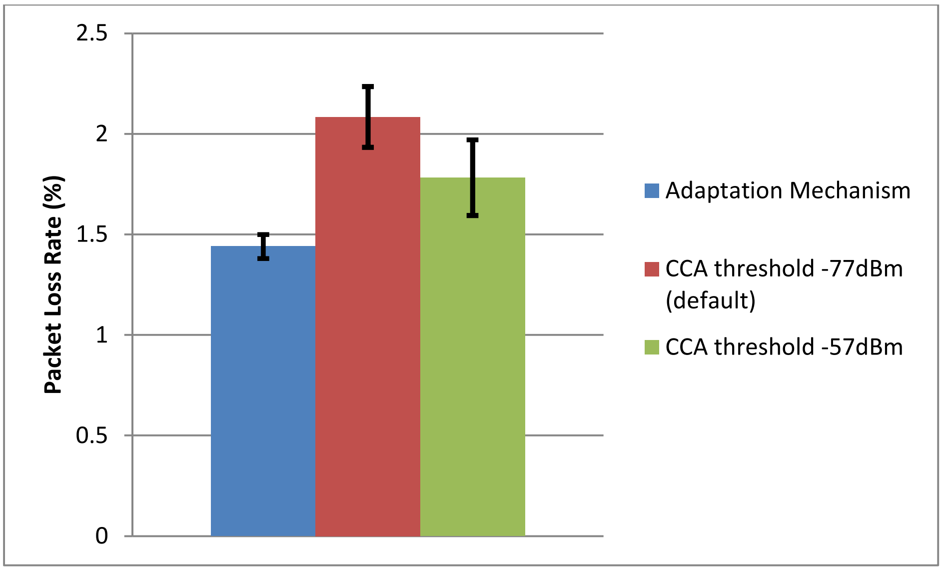

Fig.4.9 PLR comparison under mixed interfering UDP traffic1

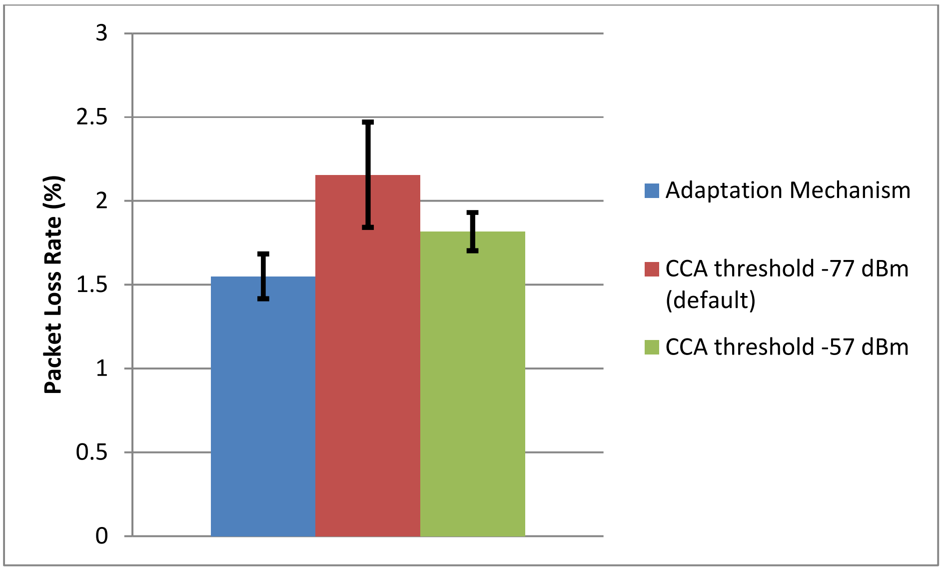

Fig. 4.10 PLR comparison under mixed interfering UDP traffic2

Fig. 4.10 shows the performance evaluation results under a different combination of interfering Wi-Fi traffic. For the first 1/3 of the test, the interfering IEEE 802.11g traffic has a 1500 bytes/segment and 500 segments/second. Then it changes to a payload of 3000 bytes/segment and 250 segments/second for another 1/3 of test time. The preceding described traffic style refers to traffic2 in Fig. 4.10. Finally, it switches back to 1500 bytes/segment and 500 segments/second for the rest of the test. It can be seen from the figure that the adaptive mechanism has achieved a better performance in terms of PLR as expected, similar to the results shown in Fig. 4.9.

Through these performance evaluation experiments, it can be seen that the proposed adaption mechanism can effectively improve the PLR of ZigBee packet transmission as compared to the default CCA scheme. However, this mechanism has some limitations for implementation. It requires some initial testing to determine the best performed CCA mode and ED threshold, and can only be applied in certain scenarios where varying external interference results in performance tradeoff between TXFIFO overflow and collisions.

In next chapter, an improved adaptive mechanism is proposed, implemented in MICAz motes, and evaluated through extensive experiments.

Chapter 5

Interference Aware Adaptive CCA Mechanism: Description and Validation[12]

THROUGH earlier discussions, the Wi-Fi interference can cause substantial performance degradation in ZigBee packet transmissions due to the overlapping of operating frequency channels of ZigBee and Wi-Fi, and the comparatively considerably higher transmit power used by Wi-Fi[13].

In order to mitigate such interference and improve ZigBee's performance, we performed research which analyzes the coexistence issues between ZigBee and Wi-Fi systems. We discussed in Chapter 3 potential mechanisms that can reduce the strength of negative impact Wi-Fi interference has on ZigBee. They can be placed in one or more of the following categories: use of frequency switching; MAC and CCA parameter adjustment; use of collaborative mechanism. Their strengths and weaknesses were discussed as well. From the experimental work and analysis of results presented in Chapter 4 we proposed an

[12] A version of this work will be submitted in the near future for possible publication in an IEEE journal. Yong Tang, Zhipeng Wang, Dimitrios Makrakis, and Hussein T. Mouftah, "Interference Aware Adaptive Clear Channel Assessment for Improving ZigBee Packet Transmission under WLAN Interference".

[13] As indicated earlier 100mW for Wi-Fi versus 1mW for ZigBee. The transmitted Wi-Fi signal is 6 dB stronger than the transmitted ZigBee signal.

adaptation mechanism capable of mitigating the interference by adaptively adjusting the CCA modes.

However, this adaptation mechanism can only be effective in limited circumstances; for example, it requires some initial testing to determine the performance of each ED threshold and no ED mode or when there are too many TXFIFO overflow dropping packets observed at the transmitting mote. Also at this point, we can determine the optimal ED threshold only experimentally. Thus a new mechanism that can be utilized under more generic and diverse conditions, offering greater performance enhancement, is needed.

Motivated by the above, in this chapter, a novel and effective Interference Aware Adaptive Clear Channel Assessment (IAACCA) technique is proposed that achieves the above mentioned target. The proposed technique was implemented in the Crossbow MICAz motes and the testbed we introduced in chapter 4. It is designed to find if the Wi-Fi Inter-Packet Time (IPT) is long enough for the transmission of an entire ZigBee/IEEE 802.15.4 packet. Also, the performance of IAACCA was assessed experimentally and the evaluation results are presented in this chapter as well. The results show that IAACCA can significantly improve the performance of ZigBee connection in terms of PDR when operating in close proximity with a Wi-Fi system.

The remainder of this chapter is structured as follows. Section 5.1 provides a detailed description of the proposed IAACCA mechanism in comparison with the default CCA scheme and gives a heuristic explanation of its advantages. In section 5.2, a series of comprehensive experiments are performed to evaluate the performance of IAACCA and then compare with the default CCA mechanism. Finally section 5.3 analyzes and discusses the experimental performance evaluation results collected under various scenarios of packet transmission.

5.1 IAACCA Mechanism and its advantages/open issues

As mentioned earlier, CCA is performed before the transmission of each ZigBee packet in order to decide whether the medium is busy or not. The proposed IAACCA scheme adopts the default CCA mode of CS-ED used in the Crossbow MICAz motes in our testbed, with the emphasis placed on improving the ED mechanism. With ED, CCA shall report a busy medium upon detecting any energy above the ED threshold (P_{th}). Use of the ED option mitigates coexistence problems by allowing transmission backoff if the channel is occupied by another device, regardless of the communication protocol it may use. The proposed IAACCA scheme makes use of the inter-arrival time occurring between two subsequent ZigBee packet transmissions to perform estimations of the external interference level.

5.1.1 IAACCA Mechanism Description

For the convenience of presentation, the IAACCA channel assessment process is illustrated in Fig. 5.1 with all the parameters listed in table 5.1.

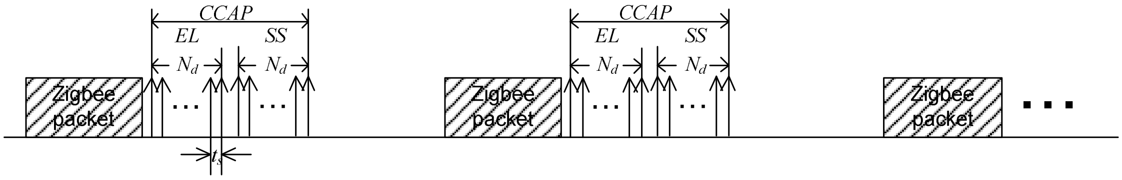

Fig. 5.1 The new channel assessment process

Table 5.1 List of IAACCA Parameters

Parameters	***Meaning***
P_{th}	ED threshold
T_{ca}	Time interval between two full cycles of channel assessment
t_s	Time interval between two consecutive RSSI readings
N	Number of channel assessment periods (CCAPs) in one full cycle of channel assessment
N_d	Number of RSSI readings in one estimation of channel's idle length period (EL)
N_s	Number of idle RSSI readings required for starting packet transmission
N_i	Number of instruction packets used in the hand-shaking mechanism for channel switching
N_{s_low}	Lower bound for N_s
N_{s_high}	Upper bound for N_s
N_{max}	Maximum number of RSSI readings allowed for the proposed sending mechanism in IAACCA
c	Empirical coefficient for comparing packet transmission duration
t_{ins}	Time interval for sending instruction packet

In the proposed IAACCA scheme, a full cycle of channel assessment consists of N clear channel assessment periods (CCAPs). Channel assessment starts right after a ZigBee packet transmission. Two types of channel assessment are performed during each CCAP. One is the estimation of the length of channel's idle period (EL) and the other is spectrum sensing (SS). The purpose of estimating the channel's idle period is to find out if it is long enough to accommodate the transmission of a ZigBee packet. The EL values are used to determine whether there is need to shorten ZigBee packet's payload size and consequently the size of the IEEE 802.15.4 packet. On the other hand, spectrum sensing is used to search for ZigBee channels that are at better condition than the one in use, in order to switch when necessary. It is noted that the channel sensing scheme we developed is different from the approach used in current devices when selecting operational channel [123] as well as those proposed in earlier publications (e.g. [101][102]). Switching to a better quality channel should be activated when the estimated length of currently used channel's idle period becomes too short to accommodate the transmission of ZigBee packets of minimum size, i.e., the size of header plus minimum payload that is required by corresponding applications.

During the EL of each CCAP, the transmitting mote consecutively acquires a certain number N_d of RSSI readings of the current channel at time interval t_s and compares them with a pre-defined threshold P_{th}. The mote calculates the maximum number n_m of successive RSSI measurements (among the N_d readings), where the measured value is lower than P_{th}. It is noted that up to 2 above-threshold RSSI readings which appear amidst a series of consecutive below-threshold RSSI readings will be ignored in order to avoid misjudgment caused by sudden and brief energy fluctuation (e.g. a WLAN client scanning through all channels for AP). This helps isolate the presence of consistent interference. The maximum length of channel idle period in this detection can be calculated as $T_{idle} = n_m \bullet t_s$. We denote the current ZigBee packet transmission duration as t_{cur_pkt} and the transmission time of minimum acceptable ZigBee/IEEE 802.15.4 packet length as t_{min_pkt}. Since the PDR might be still acceptable even when the measured idle period is not long enough for the length of the transmitted ZigBee packets, an empirical constant c $(0 < c < 1)$ is also introduced to assist with the decision to adjust packet size. Obviously, the value of c is mostly influenced by the statistics of Wi-Fi traffic, such as its volume, packet size distribution, and IPT distribution. After N CCAPs, if the average time length of channel idle period $\overline{T_{idle}}$ is larger than $c \bullet t_{cur\_pkt}$, it is decided that the channel is in good condition and no changes of packet size or operational channel are needed. If the average value satisfies { $c \bullet t_{min\_pkt} \leq \overline{T_{idle}} \leq c \bullet t_{cur\_pkt}$}, it is decided that the channel is not in a good condition in terms of accommodating the current packet size, but remains good enough for supporting shorter packet sizes. Therefore the transmitting mote will shorten the packet which has a transmission time duration of t_{min_pkt}. It should be noted that if the motes are powerful enough in terms of computation power, ZigBee packet's size can be adjusted more precisely, setting the frame's transmission time to a value in-between t_{min_pkt} but smaller than $\overline{T_{idle}}$. If an increase in the length of the channel's idle period becomes detected in the following cycles of channel assessment making $\overline{T_{idle}}$ is larger than $c \bullet t_{cur\_pkt}$,, the packet length can be restored to its original size in order to improve the transmission efficiency. If the $\overline{T_{idle}}$ is even less than $c \bullet t_{min\_pkt}$, the transmitting mote concludes that adjustment of packet size cannot help the connection to remain/become reliable and subsequently tries to locate another channel with better transmission conditions to switch, by following a policy elaborated in the following paragraph.

In the SS of each CCAP, the transmitting mote randomly chooses one of the 16 ZigBee channels and performs the same estimation of the length of channel's idle period. It should be noted that the chosen channel can be different for each CCAP. Using the collected SS results, a table of preference for the different ZigBee channels is constructed. The preference value of each channel is stored as one byte. Every time the measured T_{idle} is larger than the transmitting ZigBee packet length, the corresponding preference value of this channel in the table increases by 1, otherwise it remains unchanged. When any of the preference value goes over 255, i.e., the storing byte overflows, the entire preference table will be initialized with every channel's preference value reset to 0. When the transmitting mote needs to switch channel, it checks the preference table and chooses the one with the highest value. Then the transmitting mote initiates a request to change its operating channel by informing the ZigBee coordinator of its preferred channel selection. It is noted that such a full cycle of channel assessment is performed every T_{ca} seconds, depending on the needs of dealing with the changing Wi-Fi interference. For example, in an environment with very stable WLAN traffic profile, T_{ca} can be assigned a large value so as to save the energy in clear channel assessment.

The default CCA mechanism reads the RSSI value once. This is an average value reflecting the signal strength during the previous 128µs. The default CCA compares it to the ED threshold. If the RSSI value is lower than the ED threshold, the channel is assumed to be idle and the ZigBee packet is transmitted right away. In the proposed IAACCA scheme, the transmitting mote increases the CCA detection accuracy by reading the RSSI value consecutively at the short time interval of 16µs that accounts for a small fraction of a symbol's transmission period. This is also the period for updating the RSSI value used by CC2420. The packet transmission starts once N_s consecutive less than P_{th} RSSI readings have been counted. The value of N_s is selected randomly from within the interval {N_{s_low}; N_{s_high} } (e.g. {3 and 6}) according to a uniform distribution. The values of N_{s_low}, N_{s_high} have been selected empirically. The reason to have the mote select random N_s is done to avoid collisions among active motes waiting to transmit, i.e. it acts as a collision avoidance mechanism. If there are not N_s consecutive readings that satisfy the threshold requirement in a maximum readings of N_{max} (e.g. 200) RSSI readings, the new sending mechanism will switch back to the default mode.

In the case of having to switch the channel, the transmitting mote sends a packet containing its preferred channel number to the coordinator and waits for the acknowledgement. The coordinator acknowledges the reception of this channel switch request and sends out the notice to the transmitting mote it communicates with, informing of the planned channel switch and indicating the selected preferred channel. The coordinator then waits to receive the acknowledgement from this mote. After successfully receiving acknowledgement from the transmitting mote, the coordinator starts the channel switching algorithm. It sends out N_i instruction packets which include the parameter of time interval t_{ins} between two consecutive instruction packets and an unique sequence number denoted as i. Each of these instruction packets is broadcasted and contains a request to the receiving mote to switch to the new channel. The mote will switch to the new channel after receiving one of instruction packets and wait for $N_i \times t_{ins}$ to start sending packets in the new channel. This algorithm can make the switching accomplished as long as one of instruction packets is successfully received.

5.1.2 Advantages Achieved by IAACCA and Remaining Open Issues

Through the above descriptions, the newly proposed IAACCA scheme has the following novel functionalities and improvements as compared to the original CCA mechanism:

1. *Estimation of the length of the idle period.* The IAACCA mechanism utilizes the inter-frame vacant time to perform channel condition assessment. Through such procedures, the approximate length of the idle period in current and other channels can be estimated for determining the quality of each channel.

2. *Flexible packet size adjustment according to the estimated length of channel idle period.* The IAACCA scheme can adaptively reduce the packet size to fit in upon the detection of a shorter than the existing packet size channel-idle period. It can also increase the packet size when the idle period becomes longer so as to improve the transmission efficiency and save energy.

3. *Determination of the appropriate timing for ZigBee packet transmission*. In IAACCA, a significant change is that we implement a more precise and appropriate timing method for ZigBee packet transmission. With this mechanism, the start of an idle period can be more precisely determined so that the preamble of a ZigBee packet is able to avoid colliding with interfering Wi-Fi packets to a great extent.

4. *Spectrum sensing*. The IAACCA scheme provides the spectrum sensing functionality which can assess the condition of all the available channels for ZigBee packet transmission.

5. *Preferred spectrum management*. IAACCA statistically evaluates the quality of a channel and stores the priority information of all 16 ZigBee channels in a preferred channel table. The preferred channel table is constructed over a relatively long period of time, thus, its content allows making a better choice for selecting a suitable channel to switch to and prevent channel switching from happening frequently. Such operating channel switching can be realized by our developed notification/hand-shaking procedure, occurring between the transmitting mote and the coordinator.

Although the proposed IAACCA mechanism can effectively improve the performance of ZigBee packet transmission under Wi-Fi interference, as will be shown in the performance evaluation results in the next section, there exist several open issues for future research. The estimation of channel idle period is still not quite accurate and may need to be improved for better detection and calculation. Another issue is the difficulty of adaptively determining optimal value for ED threshold according to the changing external noise and interference level. In addition, it is worth mentioning again that the channel switching algorithm may generate significant drawbacks, such as need to consume more energy, increase end-to-end delays etc. Also the channel switching algorithm does not consider the multiple-mote environment which needs more research to develop an effective new algorithm.

The earlier discussion was based on the following four assumptions. 1) The information transmitting mote can accurately detect the existence of Wi-Fi interference in the common wireless channel, thus it can estimate the “average” length of channel idle period reliably. 2) The standard deviation of the idle channel period is small, which ensures that the probability most of the idle periods will have values close to the estimated average value is high. In the opposite case, the frequency of failed ZigBee packet transmissions will increase, as well as the appearance of unused Wi-Fi interference-free periods, even during times ZigBee devices have data to send. 3) The information transmitting mote and the receiving one receive comparably close amount of interference power when a Wi-Fi device transmits. This is expected to be the case, since the low power ZigBee motes need to be close enough to be able to communicate. 4) The information transmitting and the receiving motes have highly correlated communication channels in reference to receiving the Wi-Fi interfering signal. This ensures that statistically, they will perceive the same channel status most of the time. In the opposite case, the transmitting mote might refrain from sending data during a period the receiving mote does not experience interference from Wi-Fi signals (loss of resource). At other times, the transmitting mote could perceive the channel is free of interference and decides to transmit, while the receiving mote is impacted by interference (data transmission failure). A case this might become major problem is when both motes receive Wi-Fi signal through reflections diffused signal. In this case, the Wi-Fi interfering envelope will display Rayleigh behaviour and motes at distance greater than ¼ of RF signal's wavelength (3.125cm at 2.4 GHz, assuming propagation speed through the wireless medium is that of free space, i.e. 300,000 Km/s), will be operating under statistically uncorrelated channels.

5.2 Performance Evaluation Results and Discussion

In order to validate the performance improvement of the proposed IAACCA mechanism, extensive experiments were performed using the same topology as the one used for the experiments described in section 4.2. The relevant parameters of IAACCA scheme and their values are listed in Table 5.1. Extensive experiments have been carried out to evaluate the performance when using different values for these parameters and the values that have achieved relatively better performance in our experimental setup are empirically chosen as shown in the Table below.

Table 5.2 IAACCA experimental parameters

Parameters	***Values***
P_{th}	-77dBm (CC2420 default value)
T_{ca}	2s
t_s	16µs
N	16
N_d	400
N_s	3 ~ 6

Parameters	*Values*
N_i	10
N_{s_low}	3
N_{s_high}	6
N_{max}	200
c	0.8
t_{ins}	100ms

The ZigBee mote generates traffic with constant packet rate and packet length. After each packet transmission, the source mote waits for Acknowledgement (ACK) from the coordinator. If no ACK is received within a set time frame, the source mote re-transmits the packet once. The D-ITG traffic generator running on the laptop generates UDP traffic with different data segment payload, data segment generation rate and IPT distribution, which are then fed into the WR for generating various interfering 802.11g Wi-Fi traffic. Such different interfering IEEE 802.11g UDP traffic is hereafter described and characterized by the actual PHY layer packet size, packet rate and IDT distribution.

As described in chapter 4, the data segments with payload size larger than 1500 bytes will be fragmented by Ethernet at MAC layer when the frame is transmitted from the traffic generating laptop to the WR, and then sent out in subsequent fragments. For the convenience of notation, we use the sum of the fragmented packets as the packet size for data segments.

In the following, the ZigBee performance comparison between IAACCA and the default CCA mechanisms in terms of PLR are illustrated and discussed. It should be noted that, since switching the operating channel of the ZigBee system generates considerable extra cost to the network and also for the purpose of performing a fair comparison between the proposed IAACCA and the default CCA mechanisms, the channel switching function of IAACCA is disabled for our experiments shown in Figs. 5.2-5.11. The experimental results when employing channel switching function are discussed at the end of this section. For the concise of notation, in all figures hereafter, we denote ZigBee transmission with IAACCA and 50-byte packet as A50 and 100-byte packet as A100; we denote ZigBee transmission with default CCA and 50-byte packet as D50 and 100-byte packet as D100. All sizes refer to packets at PHY layer. The total number of transmitted ZigBee packets is 10000 for each test and we have performed 10 times for each set of tests. All the displayed confidence interval bars correspond to 95% confidence.

Figs. 5.2-5.6 illustrate the performance of ZigBee transmission with a constant packet rate of 50 packets/second in terms of PLR under different WLAN interferences. In Fig. 5.2, the packet rate of Wi-Fi is set to be 500 packets/second and three different Wi-Fi packet sizes are tested. Test 1 uses Wi-Fi traffic with 1000 bytes packet size, test 2 uses 1500-byte packets, and test 3 uses 2000-byte packets[14]. It is observed from the figure that the performance of ZigBee packet transmission deteriorates when the volume of interfering Wi-Fi traffic increases.

[14] We chose the values empirically for generating interference at a level that could produce a ZigBee PLR at around 1% - 4% range, neither too high nor too low.

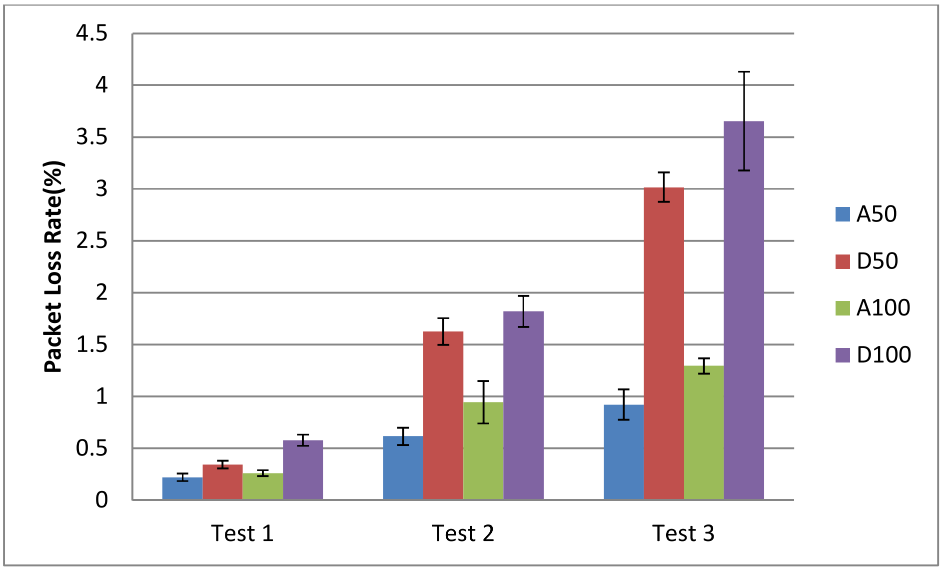

Fig. 5.2. ZigBee PLR perfomance with & without IAACCA, in the presence of different Wi-Fi interference with packet sizes of 1000bytes (test 1), 1500 bytes (test 2), 2000bytes (test 3).

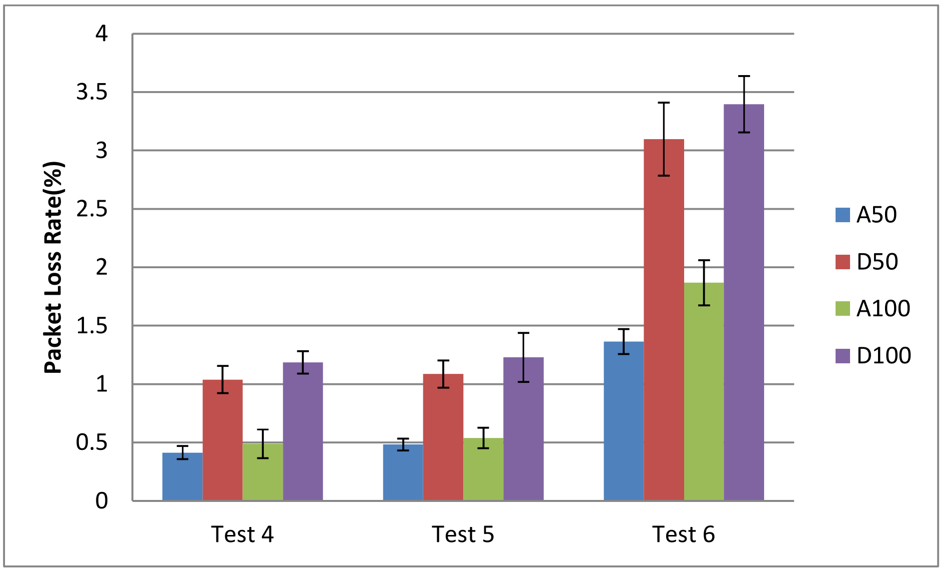

Fig. 5.3. ZigBee PLR perfomance with & without IAACCA, in the presence of different Wi-Fi interference with packet generationg rates of 300 packets/second (test 4), 400 packets/second (test 5), 600 packets/second (test 6).

Fig. 5.3 depicts the ZigBee transmission performance under interfering Wi-Fi traffic with packet size of 1500 bytes and different Wi-Fi packet generates rates and specifically 300 packets/second (test 4), 400packets/second (test 5) and 600 packets/second (test 6). In test 4 and test 5, the PLRs are almost the same although test 4 has a lower volume of interference than test 5. The reason is that in both cases, the channel idle duration is long enough for accommodating a 100-byte ZigBee packet.

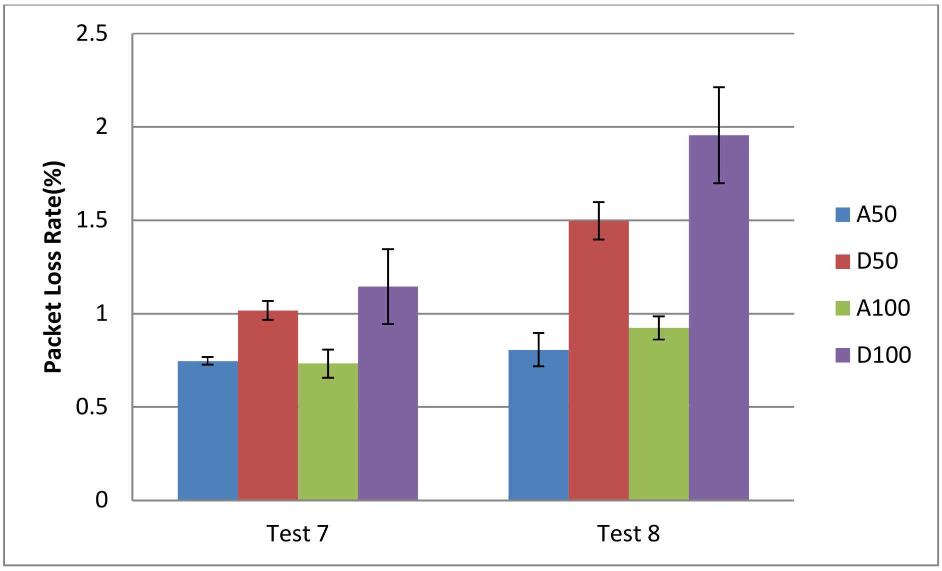

Fig. 5.4. ZigBee PLR perfomance with & without IAACCA, in the presence of different Wi-Fi interference with random IPT following Uniform distribution (test 7) and Exponential distribution (test 8).

In Fig.5.4, the IPT between consecutive Wi-Fi packets are generated following two different random distributions, i.e., Uniform distribution between packet rate of 250 to 750 packets/second (test 7) and Exponential distribution with IPT mean of 2ms (test 8). Similarly, in Fig. 5.5, the generated Wi-Fi packet sizes follow three different random distributions, namely, Uniform distribution between 1000 to 2000 bytes (test 9), Exponential distribution with mean of 1500 bytes (test 10) and Normal distribution with expected value of 1500 bytes and standard deviation of 500 (test 11).

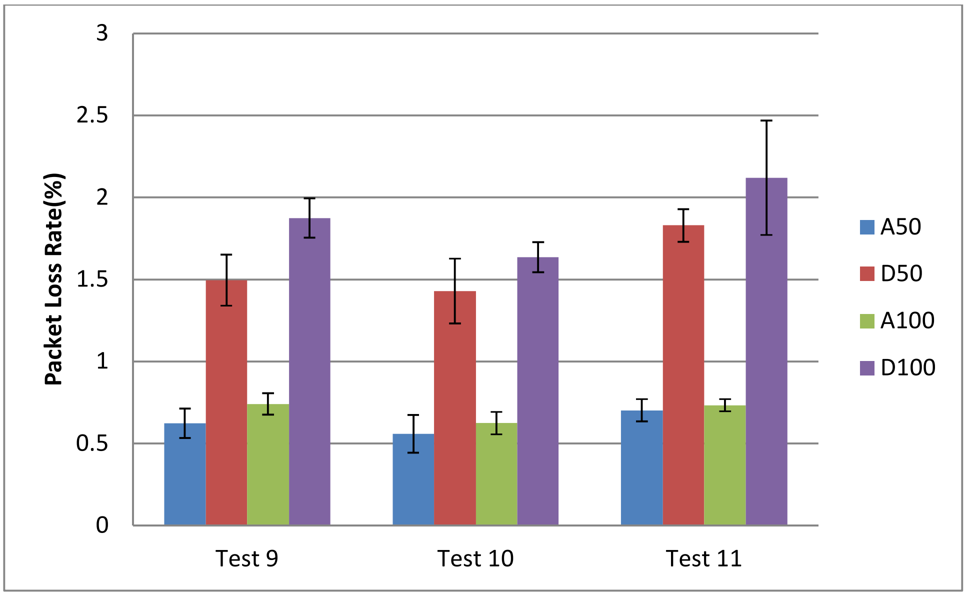

Fig. 5.5. ZigBee PLR perfomance with & without IAACCA, in the presence of different Wi-Fi interference with random packet sizes following Uniform distribution (test 9), Exponential distribution (test 10) and Normal distribution (test 11).

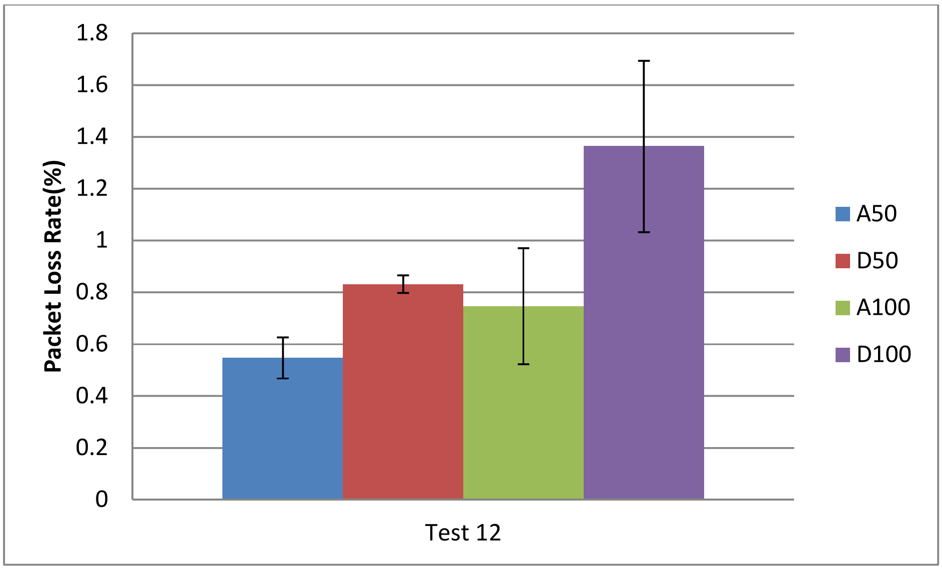

Fig. 5.6. ZigBee PLR perfomance with & without IAACCA, in the presence of different Wi-Fi interference with random IPT and random packet size both following Uniform distributions.

In Fig. 5.6, both the packet size and arrival rate of interfering WLAN traffic are randomly distributed. Test 12 adopts Uniform distributions of packet size between 1000 to 2000 bytes and packet rate of 250 to 750 packet/second.

It can be observed from Figs. 5.2-5.6 that the proposed IAACCA mechanism achieved a much better performance compared to the default CCA. As expected, shorter packet size can reduce packet loss rate compared to the longer one. All experiments are repeated for ZigBee packet transmitted at a higher speed of 100 packets/second. In this set of experiments, due to the shorter ZigBee IPT, the TXFIFO overflow will worsen the performance of ZigBee packet transmission and the proposed IAACCA shall achieve a much better performance than the default scheme. The obtained results are shown in Figs. 5.7-5.11:

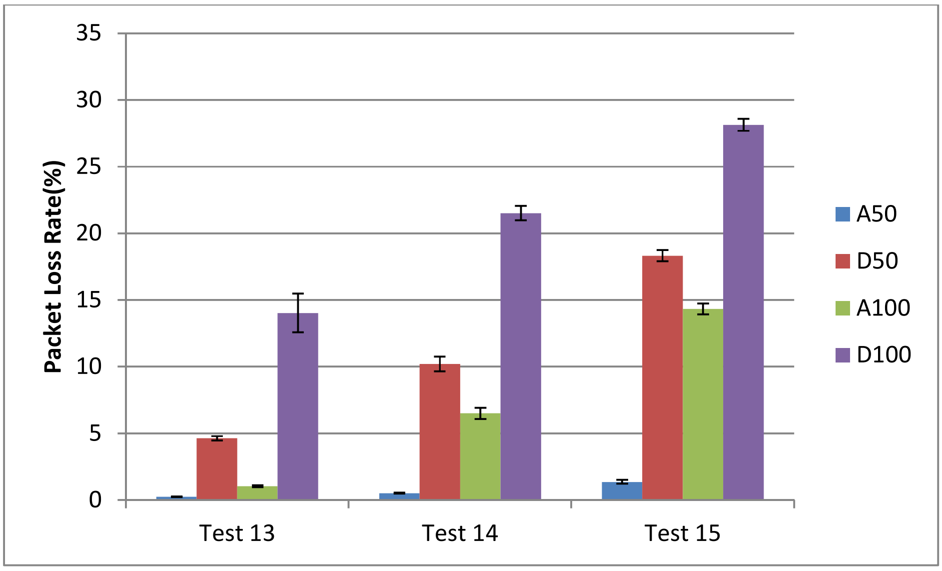

Fig. 5.7. ZigBee PLR perfomance of 10ms IPT with & without IAACCA, in the presence of different Wi-Fi interference with packet sizes of 1000bytes (test 13), 1500 bytes (test 14), 2000bytes (test 15).

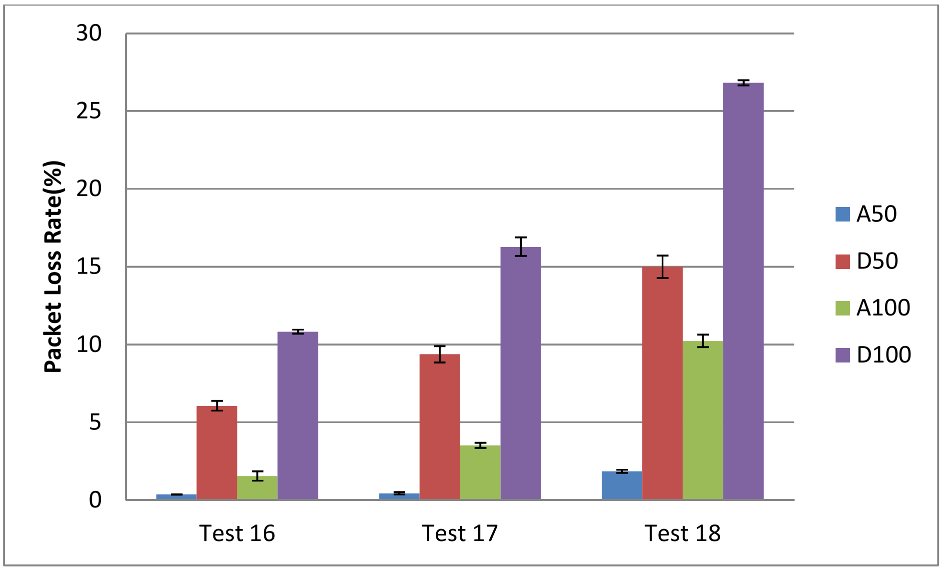

Fig. 5.8. ZigBee PLR perfomance of 10ms IPT with & without IAACCA, in the presence of different Wi-Fi interference with packet generationg rates of 300 packets/second (test 16), 400 packets/second (test 17), 600 packets/second (test 18)

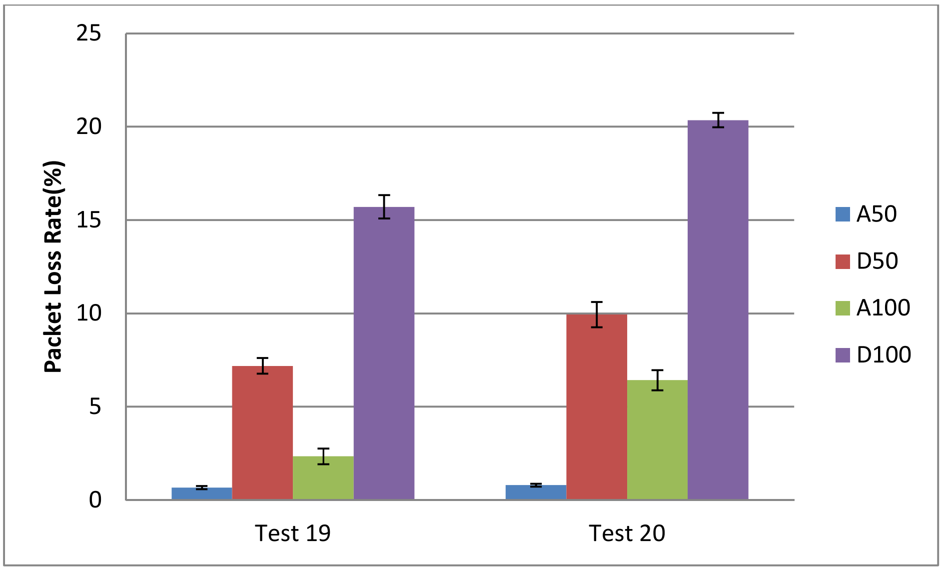

Fig. 5.9. ZigBee PLR perfomance with & without IAACCA, in the presence of different Wi-Fi interference with random IPT following Uniform distribution (test 19) and Exponential distribution (test 20).

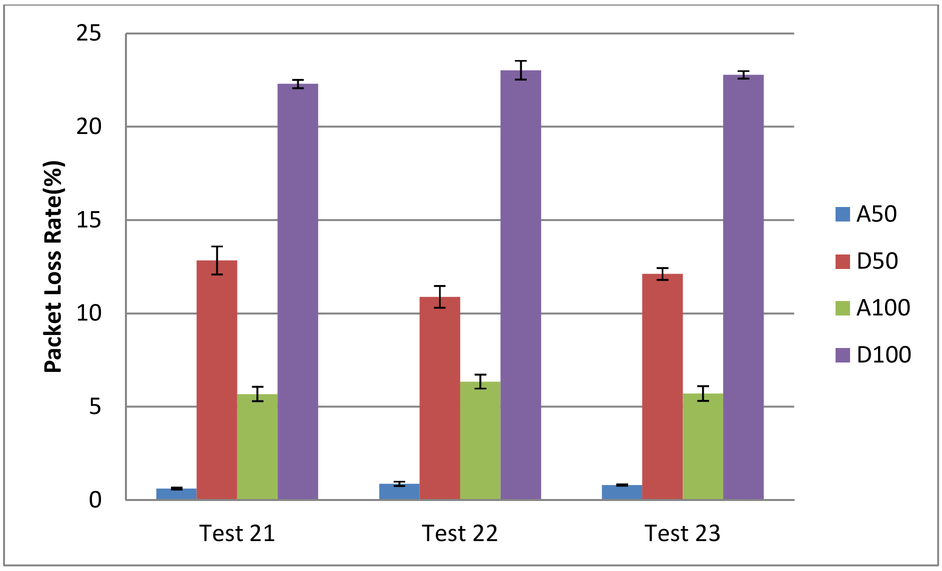

Fig. 5.10. ZigBee PLR perfomance of 10ms IPT with & without IAACCA, in the presence of different Wi-Fi interference with random packet sizes following Uniform distribution (test 21), Exponential distribution (test 22) and Normal distribution (test 23).

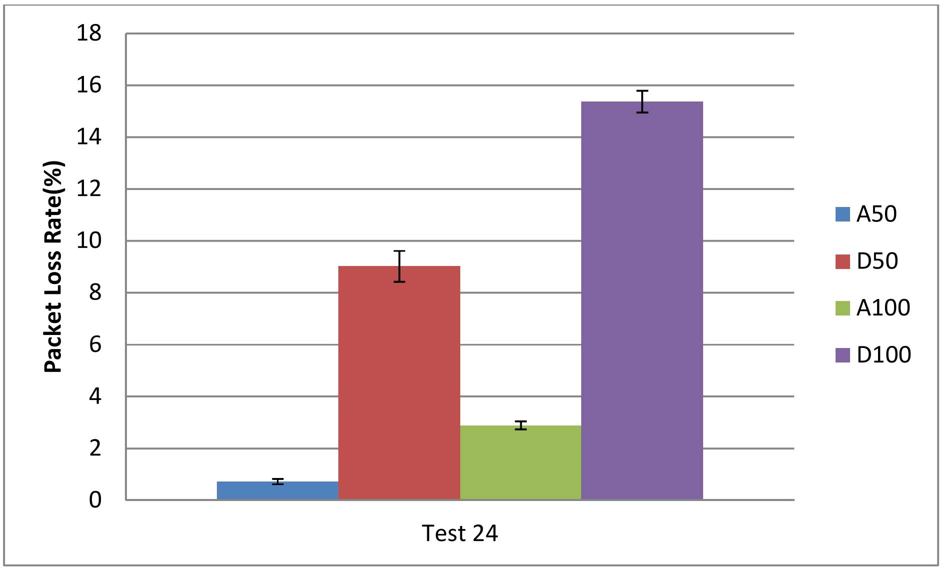

Fig. 5.11. ZigBee PLR perfomance of 10ms IPT with & without IAACCA, in the presence of different Wi-Fi interference with random IPT and random packet size both following Uniform distributions.

It can be seen from Figs. 5.7-5.11 that IAACCA achieves more significant performance improvement when ZigBee mote is transmitting at a higher rate. This is because the proposed IAACCA avoids the deficiencies of the default CCA backoffs and packet retransmission that cause many packet drops due to TXFIFO overflow.

Additional experiments have been performed to evaluate the effectiveness of the proposed packet size adaptation mechanism in IAACCA. In each of these experiments, the ZigBee transmitting node sends out a total of 10000 packets at a constant packet rate (CPR) of 20 packets/second and without retransmission. The interfering Wi-Fi traffic has packet size of 1500 bytes and transmits at the CPR of 600 packets/second. After 250 seconds, the Wi-Fi packet rate drops to 200 packets/second CPR and maintains the same value until the end of the experiment. For convenience, we denote Th_{pkt} as the packet size adaptation threshold which equals to the transmission duration of 100 byte ZigBee packet multiplied by *c*. We consider two ZigBee packet sizes in these experiments, 100 bytes and 50 bytes. It is observed in the experiments that the packet size adaptation mechanism works well and can adapt to the changes of interfering Wi-Fi traffic. The ZigBee transmission starts with a packet size of 100 bytes and then soon drops to 50 bytes because of the very short idle period (below threshold Th_{pkt}) detected. The packet size restores to the original 100 bytes after the interference decreases, i.e., idle period longer than Th_{pkt} has been detected. Fig. 5.12 shows an around 32% improvement in PLR when applying the packet size adaptation mechanism. This is particularly useful for ZigBee motes to transmit essential information with shorter packets in an environment with serious external interference to ensure acceptable PLR.

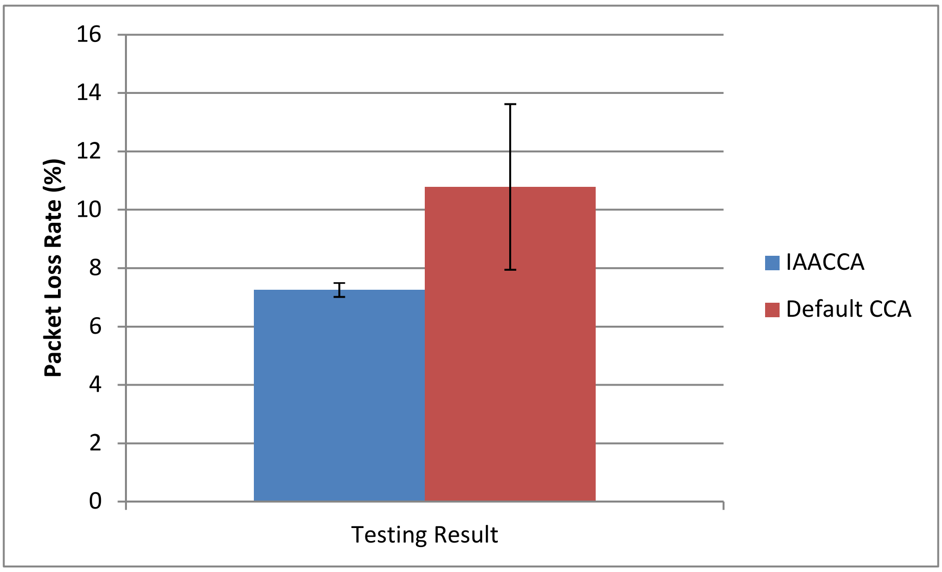

Fig. 5.12 ZigBee perfomance comparison under interfering Wi-Fi traffic mixed of two different packet rates for IAACCA and default CCA respectively.

Channel switching function is also tested in our testbed. It is observed that this function in IAACCA works nicely by successfully constructing a preferred channel table. When the interference is getting worse, the mote and coordinator can switch to a channel that has highest ranking in the table, i.e., has least interference according to the results of the past spectrum sensing. In our tests, since Wi-Fi channels 1, 6 and 11 are being used by other APs in the building, the ZigBee motes always switch to channel 26 and thus experience only trivial packet loss. As mentioned in Section I, when there are several WLAN WRs operating in different channels in the vicinity, channel switching might happen very often and lead to unstable ZigBee operation. In our proposed IAACCA scheme, switching operating channel is the last resort which only happens when the length of channel idle period cannot support the minimum acceptable ZigBee packet size. In addition, the preferred channel table is constructed over a relatively long period of time, thus able to provide a better choice for selecting a channel to switch to and avoid the possible too often channel switching.

5.3 Statistical Analysis of ZigBee Packet Transmission

From the experimental results and discussion in the previous section, it can be seen that the proposed IAACCA mechanism can achieve considerably better performance than the default CCA scheme, especially when the ZigBee packet rate is high. In this section, a thorough statistical analysis is performed to improve our understanding of ZigBee packet transmission process and also further verify our experimental methods. Due to the imperfect channel behavior of the radio medium and the collision prone nature of random access schemes, a transmitted packet does not always reach its intended destination. In the following subsection, all the different data transmission scenarios are listed and discussed.

5.3.1 ZigBee Packet Transmission Scenarios

As discussed in section 4.2, the ZigBee packet losses happen because of 3 circumstances: the packet cancellations due to CCA detection failures, packet loss due to collisions with interfering Wi-Fi packets, and packet drops due to TXFIFO overflow. In the following, results of further and more thorough analysis will be presented. Objective is to understand the workings of specific ZigBee packet transmission scenarios.

The recipient of a data packet should always acknowledge the successful reception by generating and sending an ACK back to transmitting mote, containing the Data Sequence Number (DSN) contained in the data packet it acknowledges.

After sending out the packet, the transmitting mote waits a period of *macAckWaitDuration,* having default length equal to the transmission time of 54 symbols (0.864ms) according to the standard, for the intended ACK to be received. The transmission will be considered successful if an expected ACK as described in the above paragraph is received before the *macAckWaitDuration* expires. Then the transmitting mote can proceed to prepare for the next packet transmission. If an ACK is not received within the *macAckWaitDuration* period or possesses an incorrect DSN, the mote considers this packet transmission as failed and starts the retransmission procedure. The same procedure of acknowledging and waiting for the acknowledgement mentioned above is followed again. It is emphasized that if a packet is aborted due to CCA detection failure, no matter if this packet is a first transmission attempt or a retransmitted one; a transmission failure will be reported to the higher level. Such failure will not trigger a retransmission in our experiment. Thus, packets can go through a single transmit and (if needed) retransmit process. Since in our case success or failure of the 1st retransmission ACK will not affect the result, the mote does not wait for the ACK but enters the process of transferring the following frame and preparing to transmit it.

It should be noted that the transmission of ACK does not implement CCA detection. The acknowledgement is sent out immediately after the data carrying packet has been received, regardless of the status the channel is experiencing. The following 10 figures illustrate the corresponding different data transmission scenarios occurring in our experiments:

1. Successful first data transmission attempt.

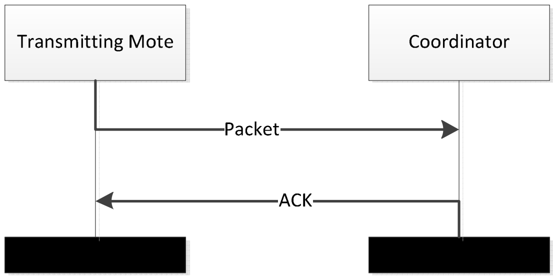

Fig. 5.13 Scenario of successful first data transmission attempt.

The transmitting mote transmits the packet to the coordinator waiting for an ACK with starting the acknowledgement timer. The coordinator receives the packet and then returns an ACK to the transmitter. The transmitter successfully receives the ACK from the recipient before its *macAckWaitDuration* timer expires. The data transfer is now complete, and the transmitter starts to prepare for the next transmission. This is the perfect condition for a transmission. No retransmission is needed here. The entire process of this scenario is illustrated as Fig. 5.13.

2. Lost acknowledgement and successful retransmission.

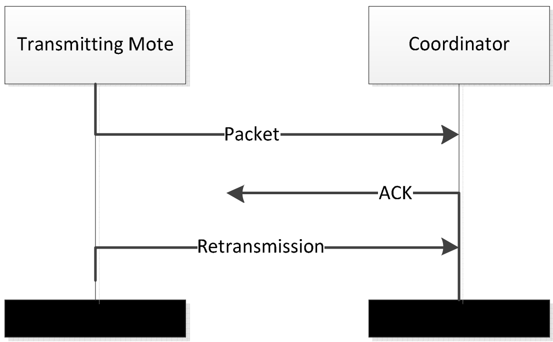

Fig. 5.14 Scenario of lost acknowledgement.

The transmitting mote has succeeded in transmitting the packet to the coordinator. But the ACK sent by the recipient fails to return to the transmitting mote. Since the transmitter does not receive any expected ACKs, the first packet transmission attempt is assumed to have failed. After the expiration of *macAckWaitDuration* timer, the transmitter resends the packet to the coordinator. This retransmitted packet reaches the coordinator but will be dropped by the recipient. This transmission is also considered successful.

3. Lost acknowledgement and failed retransmission.

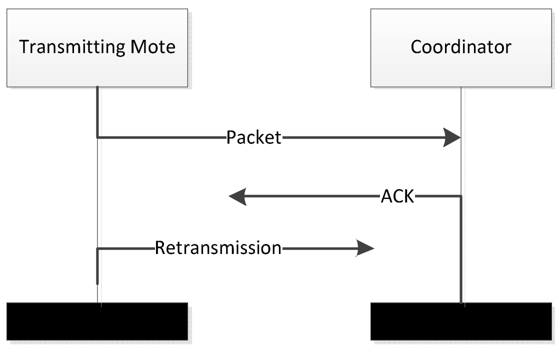

Fig. 5.15 Scenario of lost acknowledgement and failed retransmission.

Similar to scenario 2, the data packet has been successfully transmitted from the transmitting mote to the coordinator. The ACK is also lost in the transmission. After the expiration of acknowledgement waiting timer, the transmitting mote retransmits the data packet. The retransmitted packet is lost and doesn't reach the coordinator. Although the transmitting mote does not know the status of this transmission, it is still a successful one because the recipient obtains the data packet destined to it.

4. Lost data packet in the first transmission attempt but successful in retransmission.

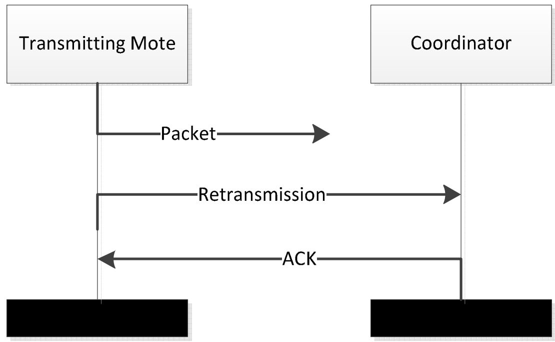

Fig. 5.16 Scenario of lost first data packet and successful in retransmission**.**

The transmitting mote transmits the packet to the coordinator, which is lost in the transmission. The recipient does not receive the packet, and therefore does not respond with an ACK. The timer of the originator expires and the transmitting mote retransmits the packet. In this scenario, the retransmitted packet is successfully received by the coordinator and a sent acknowledgement also succeeds to be received by the transmitting mote.

5. Lost packet in the first transmission attempt, successful retransmission, and lost acknowledgement.

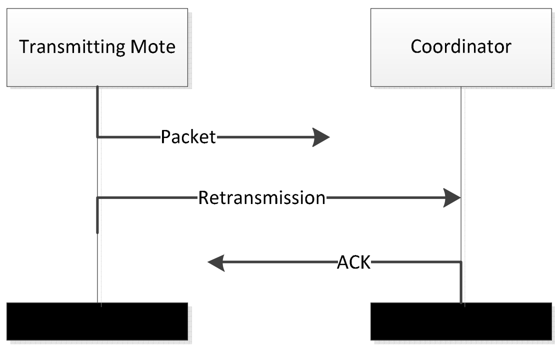

Fig. 5.17 Scenario of lost first packet, successful retransmission and lost acknowledgement.

Similarly to scenario 4, the only difference between scenarios 4 and 5 is that the transmitting mote fails to receive the ACK of the retransmitted packet. Scenario 4 and 5 are both considered successful transmissions.

6. Failed in both data transmission attempts.

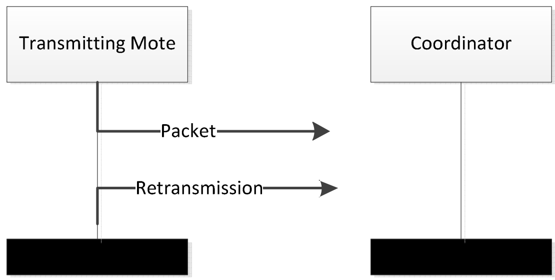

Fig. 5.18 Scenario of failed in both data transfer attempts.

In scenarios 1-5, at least one of the original or retransmitted packets arrives at the coordinator. Therefore, the packet transmission is successful. In this scenario, as depicted in Fig. 5.18, neither the original packet nor the retransmitted one reaches the coordinator, which results in a packet loss, recorded in the process.

7. Failed first data transmission attempt due to CCA detection failure.

Fig. 5.19 Scenario of failed in the first data transmission attempt due to CCA detection failure.

The first packet transmission attempt fails due to CCA detection failure on the transmitting mote's MAC sublayer. As we discussed before, this situation will not incur a retransmission and accordingly there will be a packet loss for this scenario.

8. Lost acknowledgement and failed data retransmission attempt due to CCA detection failure.

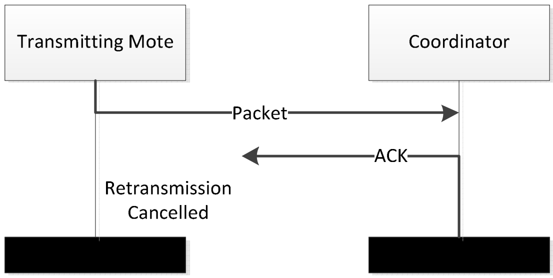

Fig. 5.20 Scenario of lost acknowledgement and failed data retransmission attempt due to CCA detection failure.

In this scenario, the first data frame transmission attempt is successful, but the corresponding ACK is lost. The transmitting mote fails to retransmit the packet due to CCA detection failure. This scenario is still considered a successful transmission.

9. Failed first packet transmission attempt and retransmission cancelled due to CCA detection failure.

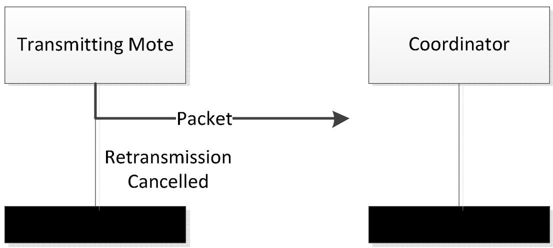

Fig. 5.21 Scenario of failed in the first packet transmission attempt and retransmission cancelled due to CCA detection failure.

As illustrated in Fig. 5.21, the first data packet is lost due to collision and the packet retransmission is cancelled due to CCA detection failure. This scenario also results in packet loss.

10. Packet drops due to TXFIFO overflow.

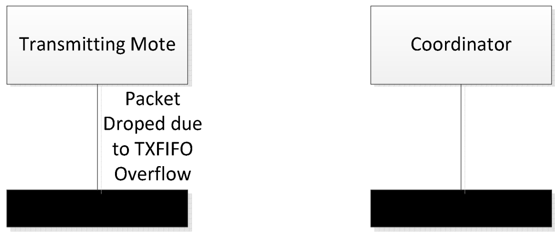

Fig. 5.22 Scenario of packet failed due to TXFIFO overflow.

This scenario can be often spotted when ZigBee motes are transmitting at a relatively high packet rate under interference. The current packet is meant to be sent out while the preceding packet is still in the transmission procedure. In this scenario, the arrival packet is forced to be abandoned by the MAC sublayer because the MICAz mote only has one transmitting register, without any additional memory to buffer more packets arriving from the higher layer. A packet loss is counted for this scenario too.

5.3.2 Results and Analysis for ZigBee Packet Transmission

The previous section elaborated on all scenarios that can occur when transmitting a ZigBee packet in our testbed. To verify our understanding of the ZigBee packet transmission process, a series of experiments have been conducted in order to determine the number of occurrences for each scenario. To achieve our objective, the firmware programs in both transmitting mote and coordinator have been modified to include the capability for recording relevant data that can be used to calculate the number of occurrences for each scenario. However, it is hard to directly determine these numbers for each scenario. Instead, we have defined ten easily measured parameters in the experiments in order to indirectly calculate the number of occurrences for each scenario. They are:

1. *Total*: the total number of packets that are sent out by the transmitting mote. It is always be 10000 in our experiments.
2. *ACKReceived*: the number of ACK packets the transmitting mote received, corresponding to successful first data packet transmissions. This parameter is measured at the transmitting mote.
3. *ReceivedDuplicatePacket*: the number of retransmitted packets the coordinator received after having received the original packets. These retransmitted packets are the duplicate ones the coordinator received, which are identified as duplicates and are dropped immediately upon reception. This parameter is measured at the coordinator.
4. *ACKSent*: the number of ACK packets the coordinator sent out. It is measured at the coordinator.
5. *TransmitterReceivedACK*: The total number of ACK packets the transmitting mote received. This parameter is measured at the transmitting mote.
6. *ReceivedRetransmission*: the number of retransmitted packets the coordinator has received when the original transmitted packet is lost. This parameter is measured at the coordinator.
7. *CCADrop*: the number of aborted original packets due to CCA detection failure. It is measured at the transmitting mote.
8. *AbortedRetransmission*: the number of aborted retransmission due to CCA detection failure. This parameter is measured at the transmitting mote.

9. *Retransmission*: the total number of packets sent out by the transmitting mote, which have to be retransmitted. It is measured at the transmitting mote.
10. *OverflowDrops*: the number of packets dropped because of TXFIFO overflow, discussed in scenario 10. This parameter is measured at the transmitting mote.

All the parameters measured at the transmitting mote are inserted into the payload of the next transmitting ZigBee packet and then transmitted to the coordinator. The coordinator updates the payload with its own measured parameters and transmits all the information to PC for user viewing.

With the parameters introduced above, a set of ten mutually independent equations can be generated and solved for obtaining the number of occurrences of the corresponding ten packet transmission scenarios. For the concise of notation, S*n* is used to represent the number of occurrences for the corresponding scenario *n*. The set of equations are listed below:

$$S1 = ACKReceived \quad (5.1)$$

$$S2 = ReceivedDuplicatePacket \quad (5.2)$$

$$S1 + S2 + S3 + S4 + S5 + S8 = ACKSent \quad (5.3)$$

$$S4 = TransmitterReceivedACK - ACKReceived \quad (5.4)$$

$$S4 + S5 = ReceivedRetransmission \quad (5.5)$$

$$S6 + S10 = Total - ACKSent - CCADrop - AbortedRetransmission \quad (5.6)$$

$$S7 = CCADrop \quad (5.7)$$

$$S8 + S9 = AbortedRetransmission \quad (5.8)$$

S2 + S3 + S4 + S5 + S6 + S8 + S9 = *Retransmission* (5.9)

S10 = *OverflowDrops* (5.10)

From the above equations, the expressions for each S*n* can be concluded:

S1= *ACKReceived* (5.11)

S2= *ReceivedDuplicatePacket* (5.12)

S3= *Retransmission – ReceivedDuplicatePacket – ReceivedRetransmission – Total + ACKSent + CCADrop + OverflowDrops* (5.13)

S4= *TransmitterReceivedACK – ACKReceived* (5.14)

S5= *ReceivedRetransmission – TransmitterReceivedACK + ACKReceived* (5.15)

S6= *Total – ACKSent – CCADrop – AbortedRetransmission - OverflowDrops* (5.16)

S7= *CCADrop* (5.17)

S8= *Total – ACKReceived – Retransmission – CCADrop – OverflowDrops* (5.18)

S9= *AbortedRetransmission – Total + ACKReceived + Retransmission + CCADrop + OverflowDrops* (5.19)

S10= *OverflowDrops* (5.20)

The ZigBee transmitting mote generates constant traffic with packet size of 100 bytes/packet. Two different IPT values, 20ms and 50ms, have been tested. The interfering constant IEEE 802.11g traffic is generated by packet size of 1500 bytes/packet and packet rate of 500 packets/second. In all these experiments, the total number of transmitted ZigBee packets is 10000. It should be noted that the parameter *ACKReceived* is recorded at the transmitting mote and then sent to the coordinator in the next data packet for viewing. Therefore, the information of whether or not the ACK of the last data packet has been received cannot be transmitted to the coordinator because the transmitting mote stops sending packets after the last one. As a result, the *ACKReceived* is most likely to be one less than the actual value, which in turn results in a sum of 9999 for all 10 scenarios.

Table 5.3 Testing results for packet transmission using default CCA with ZigBee IPT = 20ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second

Testing No.	1	2	3
ACKReceived	7414	7155	7233
Retransmission	2479	2745	2668
AbortedRetransmission	1	0	0
CCADrop	1	1	1
TransmitterReceivedACK	8160	7959	8036
ReceivedRetransmission	873	968	949
ACKSent	9791	9774	9800
ReceivedDuplicatePacket	1306	1406	1400
OverflowDrops	105	98	97

Table 5.3 summarizes the experimental results of the ZigBee packet transmission process using the default CCA mechanism with ZigBee IPT as 20ms. The numbers of occurrences for each case are given in Table 5.4:

Table 5.4 Number of occurrence for each scenario for default CCA with ZigBee IPT = 20ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second

Testing No.	1	2	3
S1	7414	7155	7233
S2	1306	1406	1400
S3	197	244	217
S4	746	804	803
S5	127	164	146
S6	102	127	102
S7	1	1	1
S8	1	0	0
S9	0	0	0
S10	105	98	97
SUM	9999	9999	9999

From the above table, we can see that aborted packet transmissions because of failures in CCA detection (S7, S8, S9) are trivial and generally can be ignored. However the number of packets dropped due to TXFIFO overflow (S10) is very high and almost equal to the number of collided packets (S6). The sum of all 10 scenarios, i.e., S1 to S10, is 9999, which validates the correctness of our statistical analysis.

Tables 5.5 and 5.6 summarize the test results for the proposed IAACCA under the same conditions with those used for the default CCA. Comparing the results in Table 5.4 and 5.6, it can be seen that IAACCA improves the ZigBee's performance by reducing the number of dropped packets due to TXFIFO overflow (S10). From these two tables, it can also be observed that IAACCA achieves a smaller number of lost packets (S6 + S7 +S9 + S10), which is improved by around 30% compared to the default CCA mechanism.

Table 5.5 Testing results for packet transmission using IAACCA with ZigBee IPT = 20ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second

Testing No.	1	2	3
ACKReceived	7264	7347	7479
Retransmission	2727	2646	2516
AbortedRetransmittingPacket	0	0	0
CCADrop	2	0	0
TransmitterReceivedACK	7993	8140	8301
ReceivedRetransmission	876	940	942
ACKSent	9860	9858	9862
ReceivedDuplicatePacket	1447	1298	1238
OverflowDrops	6	6	4

Table 5.6 Number of occurrence for each scenario for IAACCA with ZigBee IPT = 20ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second.

Testing No.	1	2	3
S1	7264	7347	7479
S2	1447	1298	1238
S3	272	272	202
S4	729	793	822
S5	147	147	120
S6	132	136	134
S7	2	0	0
S8	0	0	0
S9	0	0	0
S10	6	6	4
SUM	9999	9999	9999

To further investigate the effectiveness of the proposed IAACCA with light traffic load (thus very small possibility for TXFIFO overflow packet dropping, see last row of table 5.7), another series of experiments are performed with ZigBee packet IPT being set to 50ms. The following two tables summarize the test results for the default CCA mechanism and the IAACCA mechanism respectively.

Table 5.7 Testing results for packet transmission using default CCA with ZigBee IPT = 50ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second

Testing No.	1	2	3	4
ACKReceived	4760	4533	5628	5381
Retransmission	5239	5466	4371	4618
AbortedRetransmittingPacket	1	0	0	0
CCADrop	0	0	0	0
TransmitterReceivedACK	5295	4960	6179	5924
ReceivedRetransmission	919	876	836	878
ACKSent	9901	9908	9929	9908
ReceivedDuplicatePacket	3651	3887	3049	3153
OverflowDrops	0	0	0	0

Table 5.8 Testing results for packet transmission using IAACCA with ZigBee IPT = 50ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second

Testing No.	1	2	3	4
ACKReceived	5791	5344	5203	5676
Retransmission	4208	4655	4796	4323
AbortedRetransmittingPacket	0	0	0	0
CCADrop	0	0	0	0
TransmitterReceivedACK	6357	5817	5705	6178
ReceivedRetransmission	866	789	790	768
ACKSent	9912	9905	9926	9916
ReceivedDuplicatePacket	2852	3233	3410	2970
OverflowDrops	0	0	0	0

Similar to Tables 5.3 and 5.5, the number of occurrences for each packet transmission scenario can be calculated from Eqs. (5.11) - (5.20) as shown in Tables 5.9 and 5.10.

Although the average PLR of the two sets of experiments are very close, our IAACCA can reduce the number of packet retransmissions by 9.52% as shown in Fig. 5.23. The transmission of packets consumes most of mote's energy, thus the less the number of packet retransmissions, the more energy the mote saves. Therefore, the proposed IAACCA has achieved a better energy efficiency compared to the default CCA mechanism.

Table 5.9 Number of occurrence for each scenario for default CCA with ZigBee IPT = 50ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second

Testing No.	1	2	3	4
S1	4760	4533	5628	5381
S2	3651	3887	3049	3153
S3	570	611	415	495
S4	535	427	551	543
S5	384	449	285	335
S6	98	92	71	92
S7	0	0	0	0
S8	1	0	0	0
S9	0	0	0	0
S10	0	0	0	0
SUM	9999	9999	9999	9999

Table 5.10 Number of occurrence for each scenario for IAACCA with ZigBee IPT = 50ms and packet size = 100 bytes under Wi-Fi interference using packet size of 1500 bytes and packet rate of 500 packets/second

Testing No.	1	2	3	4
S1	5791	5344	5203	5676
S2	2852	3233	3410	2970
S3	402	538	522	501
S4	566	473	502	502
S5	300	316	288	266
S6	88	95	74	84
S7	0	0	0	0
S8	0	0	0	0
S9	0	0	0	0
S10	0	0	0	0
SUM	9999	9999	9999	9999

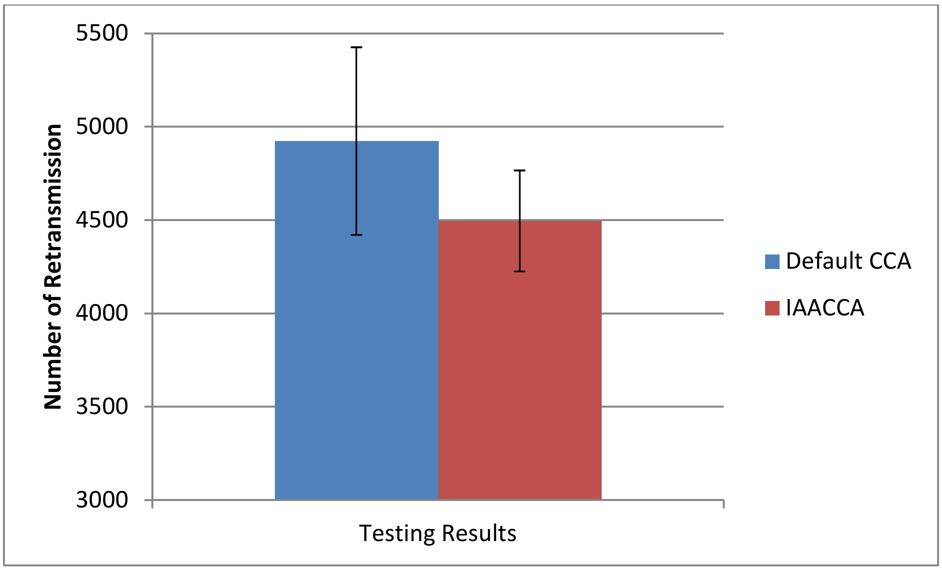

Fig. 5.23 The number of retransmission for default CCA and IAACCA.

Chapter 6

Conclusions and Future Work

IN this thesis, the impact of different CCA modes and ED thresholds on the performance of ZigBee connection, subjected to interference by a collocated IEEE 802.11g system has been studied and novel interference mitigation techniques for improving the ZigBee's performance when subjected to interference by Wi-Fi systems have been proposed. It has been demonstrated from our analysis and experimental results that CCA can impact ZigBee' s performance when there is Wi-Fi interference and our developed adaptive CCA mechanism can effectively mitigate such interference and achieve a lower PLR for the ZigBee connection.

6.1 Conclusions

Throughout this research, we have performed extensive experiments to study the impact of CCA on ZigBee' s performance and developed new interference mitigation techniques. The major contributions of the thesis are

1. The implementation of the testbed is successful and the developed testbed is suitable for carrying out research on the coexistence issue and evaluating various newly proposed and developed performance improvement techniques.

2. Our experimental results clearly show that different CCA modes and ED thresholds have significant impact on ZigBee's performance under interference generated by a collocated Wi-Fi network and have provided us a scope to study more details of the existing CCA mechanism and its impact on ZigBee performance under Wi-Fi interference.

3. An existing theoretical analysis approach proposed in [101][102] that is based on the collision time model between ZigBee and Wi-Fi packets was used and suitably modified to address our scenarios. We did so to assess how close the performance generated using the analytical method is to the experimentally generated performance results. Our study indicates that the analytical results derived from the collision time model can partially explain the observed interference phenomenon and PLR results, but the model still needs revision to account for the capture effect, which may cause the discrepancy between experimental and theoretical analysis results.

4. To alleviate the damaging impact of interference, a primitive adaptive CCA mechanism was designed, implemented and validated. This technique employs an interference detection scheme that can determine different characteristics of interference. It is observed in our experiments that this scheme can improve the performance in some limited circumstances by adaptively adjusting the CCA parameters.

5. To further improve the adaptive CCA mechanism allowing for more general implementations, a novel IAACCA scheme has been proposed and implemented to improve the ZigBee performance under Wi-Fi interference. This IAACCA scheme can

determine better timing for transmitting ZigBee packets and adjusts packet size or operating channel based on its effective assessment of channel interference conditions and the availability of time and/or spectrum “holes” to support reliable packet transmission. It is demonstrated from the experimental results and discussions that IAACCA can significantly improve ZigBee’ s performance in terms of packet loss rate when there is time varying interference from the collocated Wi-Fi networks.

6. An elaborate statistical analysis of ZigBee packet transmission scenarios has been provided. Through such analysis, we have improved the understanding of ZigBee packet transmission under interference and also further verified our experimental methods. This analysis can serve as a stepping stone leading to future research work.

6.2 Future Work

From the contributions and conclusions of this thesis summarized in the previous section, it is clear that development of technology improving the performance of a ZigBee system subjected to severe interference from collocated Wi-Fi systems is a very challenging task. However, the understanding of the interworking between different layers of ZigBee’s protocol stack, provided useful insight on how, why and when performance deterioration occurs. This knowledge can lead to a number of meaningful research directions for the development of impairment counter-measuring technology. Bellow, we suggest several topics for future research.

1. *Study the impact of CCA mechanism in a multi-mote environment.*

In our research, we focused on studying the performance of a single ZigBee communication link and conducted experiments on a testbed consisting of one transmitting mote and one receiving mote. This simplification makes it easier to analyze the packet transmission and helps us to better understand the effects of interference. However, in real world applications, multiple sensor motes are used forming a WSN acting both as source and destination. Such scenario introduces greater complexity to both analytical and experimental work. Therefore, it is meaningful and useful to study the impact of CCA mechanism for a multi-mote environment, forming a WSN.

2. *Propose effective interference mitigation mechanism for multi-mote deployment network architectures.*

   Following the methodology we utilized and described in this thesis, using the detailed knowledge to be acquired through the study of CCA mechanism's functionality/behaviour for the case of having a ZigBee based multi-mote network architecture operating in collocation with interfering Wi-Fi nodes, it is possible to design superior and more efficient interference mitigation techniques.

Reference

[1] F.Zhao, L.Guibas, “Wireless Sensor Networks: An Information Processing Approach”, Morgan Kaufmann Publisher, San Francisco, ISBN: 1558609148, 2004.

[2] S. C. Ergen, “ZigBee / IEEE 802.15.4 Summary”, Technical Report, Advanced Technology Lab of National Semiconductor, August 2004.

[3] E.Callaway, “Wireless Sensor Networks, Architectures and Protocols”, Auerbach Publications, Boca Raton, Fla, ISBN: 0849318238, 2004.

[4] S.Ramanath, E.Altman, V.Kumar, M.Debbah, “Optimizing cell size in Pico-cell networks”, 7^{th} International Symposium on Modeling and Optimization in Mobil, Ad Hoc, and Wireless Networks, pp.1-9, 23-27 June 2009.

[5] V.Chandrasekhar, J.Andrews, A.Gatherer, “Femtocell networks: a survey”, IEEE Communications Magazine, Vol.46, Issue.9, pp.59-67, September 2008.

[6] V.Rajaravivarma, Y.Yang, T.Yang, "An Overview of Wireless Sensor Network and Applications", System Theory, 2003, Proceedings of the 35th Southeastern Symposium on, pp.432-437, March 2003.

[7] J.A.Stankovic, "Wireless Sensor Networks", Computer, Vol.41, Issue 10, pp.92-95, Oct.2008.

[8] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Computer Networks, vol. 52, pp.2292-2330, 2008.

[9] M.Tubaishat, S. Madria, “Sensor Networks: An Overview”, Potentials IEEE, Vol.22, Issue2, pp.20-23, 2003.

[10] A. Bharathidasas and V. Anand, “Sensor networks: An overview”, Technical report, Dept. of Computer Science, University of California at Davis, 2002.

[11] P.Gajbhiye, A.Mahajan, "A Survey of Architecture and Node deployment in Wireless Sensor Network", Applications of Digital Information and Web Technologies, First International Conference on the, pp.426-430, 4-6 August 2008.

[12] Y.Liu, S.Wu, X.Nian, "The Architecture and Characteristics of Wireless Sensor network", 2009 International Conference on Computer Technology and Development, pp.561-565, 13-15 Nov. 2009.

[13] H.Jin, W.Jiang, "Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice", IGI Global, 2010.

[14] M.Aslam, S.Rea, D.Pesch, "A Vision for Wireless Sensor Networks: Hybrid Architecture, Model Framework and Service based Systems", Digital Information Management, 2010 Fifth International Conference on, Thunder Bay, pp.353-359, 5-8 July 2010.

[15] S.Fedor, M.Collier, "On the problem of energy efficiency of multi-hop vs one-hop routing in Wireless Sensor Netoworks", 21st International Conference on Advanced Information Networking and Applications Workshops, 21-23 May 2007.

[16] Karl H, Willing A. "Protocols and Architectures for Wireless Sensor Networks". New York: Wiley, pp.314−340, 2005.

[17] K.Hajdarevic, E.Kurtanovic, "Simulation application for Sleep-Awake Probabilistic Forwarding Protocol for Smart Dust environments", Proceedings of the 34th International Convetion, pp.468-471, 23-27 May 2011.

[18] Th.Arampatzis, J.Lygeros, S.Manesis, "A Survey of Applications of Wireless Sensors and Wireless Sensor Networks", Control and Automation, Proceedings of the 13th Mediterranean Conference on, Limassol, Cyprus, pp.719-725, June 2005.

[19] K.Low, W.Win, M.Er, "Wireless Sensor Networks for Industrial Environments", Proceedings of the 2005 International Conference on Computational Intelligence for Modelling, Control and Automation, and International Conference on Intelligent Agents, Web Technologies and Internet Commerce, pp.271-276, Nov.2005.

[20] Akyildiz, Ian Can Vuran, Mehmet, "Advanced Texts in Communications and Networking: Wireless Sensor Networks", Hoboken, NJ, USA: Wiley, 2010.

[21] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, 38(4):393– 422, March 2002.

[22] R.Mittal, M.Bhatia, "Wireless sensor networks for monitoring the environmental activities", Computational Intelligence and Computing Research, 2010 IEEE International Conference on, pp.1-5, Dec.2010.

[23] K. Lu, Y. Qian, D. Rodriguez, W. Rivera, M. Rodriguez, "Wireless Sensor Networks for Environmental Monitoring Applications: A Design Framework", Global Telecommunications Conference, IEEE, Washington, pp.1108-1113, Nov.2007.

[24] P.A.Morreale, "Wireless Snesor Network Applications in Urban Telehealth", Advanced Information Networking and Applications Workshops, 2007 21st International Conference on, pp.810-814, May 2007.

[25] D. Malan, T. Fulford-Jones, M. Welsh, S. Moulton, "CodeBlue: an Ad Hoc sensor network infrastructure for emergency medical care", Proceedings of Workshop on Applications of Mobile Embedded Systems, Boston, June 2004.

[26] T. Gao, C.Pesto, L.Selavo, Y.Chen, J.Ko, J.Lim, A.Terzis, A.Watt, J.Jeng, B.Chen, K.Lorinez, M. Welsh, “Wireless medical sensor networks in emergency response: implementation and pilot results”, Proceedings of IEEE International Conference on Technologies for Homeland Security, pp.187-192, Waltham, May 2008.

[27] Jean-Dominique Decotignie, "The Many Faces of Industrial Ethernet [Past and Present]," Industrial Electronics Magazine, IEEE , vol.3, no.1, pp.8-19, March 2009.

[28] Gil Shoshani, Stephen Mitschke, Stan Stephan, "Industrial Fieldbus technology and Fieldbus cable overview — Cable standards and electrical qualifications," Petroleum and Chemical Industry Conference (PCIC), 2010 Record of Conference Papers Industry Applications Society 57th Annual, pp.1-10, 20-22 Sept. 2010.

[29] J. King, “BP pioneers large-scale use of wireless sensor networks”, Computer World, Mar 14, 2005.

[30] P. Hochmuth, “GM cuts the cords to cut costs,” Mobility and wireless, Article of Techworld, Jun 2005.

[31] T. K. Moon and T. Y. Kuc, “An integrated intelligent control architecture for mobile robot navigation within sensor network environment” Proc of IEEE/RSJ International Conference on Intelligent Robots and System, pp.565-570, Oct 2004.

[32] T. He, S. Krishnamurthy, J. A. Stankovic, T. Abdelzaher, L. Luo, R. Stoleru, T. Yan, L. Gu, G. Zhou, J. Hui, and B. Krogh. VigilNet, “an integrated sensor network system for energy-efficient surveillance”, ACM Transactions on Sensor Networks, 2(1):1– 38, February 2006.

[33] Viani, F.; Oliveri, G.; Donelli, M.; Lizzi, L.; Rocca, P.; Massa, A.; , "WSN-based solutions for security and surveillance," Microwave Conference (EuMC), 2010 European, pp.1762-1765, 28-30 Sept. 2010.

[34] Chaczko, Z.; Klempous, R.; Nikodem, J.; Szymanski, J.; , "Applications of Cooperative WSN in Homecare Systems," Broadband Communications, Information Technology & Biomedical Applications, 2008 Third International Conference on , pp.215-220, 23-26 Nov. 2008

[35] S.Munir, B.Ren, W.Jiao, B.Wang, D.Xie, M.Ma, “Mobile Wireless Sensor Network: Architecture and Enabling Technologies for Ubiquitous Computing”, 21st International Conference on Advanced Information Networking and Applications Workshops, pp.113-120, 2007.

[36] Hua Zhou, Zhiqiu Huang, Guoan Zhao, "A service-centric solution for wireless sensor networks," Communications and Networking in China (CHINACOM), 2010 5th International ICST Conference on, pp.1-5, 25-27 Aug. 2010.

[37] Colitti, W.; Steenhaut, K.; De Caro, N.; Buta, B.; Dobrota, V.; , "REST Enabled Wireless Sensor Networks for Seamless Integration with Web Applications," Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on, pp.867-872, 17-22 Oct. 2011.

[38] Mainetti, L.; Patrono, L.; Vilei, A.; , "Evolution of wireless sensor networks towards the Internet of Things: A survey," Software, Telecommunications and Computer Networks (SoftCOM), 2011 19th International Conference on, pp.1-6, 15-17 Sept. 2011.

[39] L.F.Herrera-Quintero,F.Macia-Petrez,H.Ramos-Morillo,C.Lago-Gonzalez, "Wireless Smart Sensors Networks, systems, trends and its impact in environmental monitoring", Communications,2009, IEEE Latin-American Conference on, Medellin, pp.1-7, Sept.2009.

[40] A.Sharif, V.Potdar, E.Chang, "Wireless Multimedia Sensor Network Technology: A Survey", Industrial Informatics, 2009, 7th IEEE International Conference on, Cardiff, Wales, pp.606-612, June 2009.

[41] I.F.Akyildiz,T.Melodia,K.R.Chowdury, "Wireless Multimedia Sensor Networks: A Survey", Wireless Communications, IEEE, Vol.14, Issue 6, pp.32-40, December 2007.

[42] A.Habib, "Sensor Network Security Issues at Network Layer", 2nd International Conference on Advances in Space Technologies, pp.58-64, Nov.2008.

[43] M.de los Angeles Cosio Leon,J.Hipolito,J.Garcia, "A Security and Privacy Survey for WSN in e-Health Applications", Electronics,Robotics and Automotive Mechaniscs Conference, 2009, pp.125-131, Sept.2009.

[44] K.Shuaib, M.Boulmalf, F.Sallabi, A.Lakas, "Co-existence of Zigbee and WLAN, A Performance Study", Wireless Telecommunications Symposium, 2006, pp.1-6, Pomana, CA, April 2006.

[45] CrossBow MICAz mote, http://www.openautomation.net/uploadsproductos/micaz_datasheet.pdf, retrieved on June 13, 2012.

[46] IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), IEEE Standard, 2006.

[47] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements. - Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), IEEE Std 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002), p.0_1-580, 2005.

[48] William Stallings, "Data and Computer Communications", Upper Saddle River, NJ:Pearson/Prentice Hall, 9th ed., ISBN:0131302050, 9780131392052, 2011.

[49] Edgar H. Callaway, Jr., "Wireless Sensor Networks: architectures and protocols", Boca Raton, Fla:Auerbach Publiscations, ISBN:0849318238 (alk. paper), 2004.

[50] Muller, I.; Netto, J.C.; Pereira, C.E.; , "WirelessHART field devices," Instrumentation & Measurement Magazine, IEEE , vol.14, no.6, pp.20-25, December 2011.

[51] Petersen, S.; Carlsen, S.; , "WirelessHART Versus ISA100.11a: The Format War Hits the Factory Floor," Industrial Electronics Magazine, IEEE , vol.5, no.4, pp.23-34, Dec. 2011.

[52] R.Wagner, "Standards-Based Wireless Sensor Networking Protocols for Spaceflight Applications", 2010 IEEE Aerospace Conference, pp.1-7, Big Sky, MT, March 2010.

[53] http://www.hartcomm.org/protocol/wihart/wireless_overview.html, last visited on July 20, 2011.

[54] ISA-100.11a-2009, "Wireless systems for industrial automation: Process control and related applications", ISA Standards, 2009.

[55] Li Pengfei; Li Jiakun; Nie Luhua; Wang Bo; , "Research and Application of ZigBee Protocol Stack," Measuring Technology and Mechatronics Automation (ICMTMA), 2010 International Conference on , vol.2, pp.1031-1034, 13-14 March 2010.

[56] N.Salman, I.Rasool, A.Kemp, "Overview of the IEEE 802.15.4 standards family for low Rate Wireless Personal Area Networks", 7th International Symposium on Wireless Communication Systems, pp701-705, 2010.

[57] J.Gutierrez, "On the use of IEEE 802.15.4 to enable wireless sensor networks in building automation", 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, pp.1865-1869, vol.3, 2004.

[58] VILLASENOR-GONZALEZ, L.; PORTILLO-JIMENEZ, C.; SANCHEZ-GARCIA, J.; "A Performance Study of the IEEE 802.11g PHY and MAC Layers over Heterogeneous and Homogeneous WLANs". Ing. invest. y tecnol., Mexico, vol. 8, No. 1, March 2007.

[59] M.A.Shahimi, Z.A.Halim, W.Ismail, "Development of active RFID system using zigbee standard with non beacon mode", IEEE Asia Pacific Conference on Circuits and Systems, Kuala Lumpur, pp.176-179, 6-9 Dec.2010.

[60] http://www.zigbee.org/Specifications/ZigBee/Overview.aspx, last visited on April 23rd, 2012.

[61] http://www.zigbee.org/Specifications/ZigBee/NetworkTopology.aspx, last visited on July 20, 2011.

[62] C.Li, Y.Wang, X.Guo, “The Application Research of Wireless Sensor Network Based on ZigBee”, 2010 Second International Conference on Multimedia and Information Technology, pp.89-92, 2010.

[63] Zusheng Zhang; Fengqi Yu; , "Performance Analysis of Cluster-Based and Tree-Based Routing Protocols for Wireless Sensor Networks," Communications and Mobile Computing (CMC), 2010 International Conference on , vol.1, no., pp.418-422, 12-14 April 2010.

[64] Hu, B.; Gharavi, H.; , "Directional routing protocols for ad-hoc networks," Communications, IET , vol.2, no.5, pp.650-657, May 2008.

[65] Z.Bidai, H.Haffaf, M.Maimour, “Node disjoint multi-path routing for ZigBee cluster tree wireless sensor networks”, 2011 International Conference on Multimedia Computing and Systems, pp.1-6, 2011.

[66] V.Kumar, S.Tiwari, “Performance of Routing Protocols for Beacon-Enabled IEEE 802.15.4 WSNs with Different Duty Cycle”, 2011 International Conference on Devices and Communications, pp.1-5, 2011.

[67] Payal N. Raj, Prashant B. Swadas, "DPRAODV: A DYANAMIC LEARNING SYSTEM AGAINST BLACKHOLE ATTACK IN AODV BASED MANET", International Journal of Computer Science Issues, Vol.2, pp.54-59, 2009.

[68] H.Li, Z.Jia, X.Xue, “Application and Analysis of ZigBee Security Services Specification”, 2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing, pp.494-497, 2010.

[69] G.Dini, M.Tiloca, “Considerations on Security in ZigBee Networks”, IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, pp.58-65, 2010.

[70] J. Song, S. Han, A.M. Mok, D. Chen, M. Lucas, M.Nixon, W. Pratt. "WirelessHART: Applying Wireless Technology in Real-Time Industrial Process Control", Proc. IEEE Real-Time and Embedded Technology and Applications Symposium, pp. 377-386, 2008.

[71] E.Ferro, F.Potorti, “Bluetooth and Wi-Fi Wireless Protocols: a Survey and a Comparison”, IEEE Wireless Communications Magazine, pp.1-24, 2004.

[72] ISO/IEC Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements- Part 11g: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standards, 2006.

[73] William Stallings, "IEEE 802.11:Wireless LANs from a to n," IT Professional, vol. 6, no. 5, pp. 32-37, Sept.-Oct.2004.

[74] http://en.wikipedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_(802.11b,g_WLAN).svg, last visted on April 23rd, 2012.

[75] "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 8: Medium Access Control (MAC) Quality of Service Enhancements," IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003), pp.0_1-189, 2005.

[76] Mangold, S.; Sunghyun Choi; Hiertz, G.R.; Klein, O.; Walke, B.; , "Analysis of IEEE 802.11e for QoS support in wireless LANs," Wireless Communications, IEEE , vol.10, no.6, pp. 40- 50, Dec. 2003.

[77] Xiang Chen; Hongqiang Zhai; Yuguang Fang; , "Enhancing the IEEE 802.11e in QoS support: analysis and mechanisms," Quality of Service in Heterogeneous Wired/Wireless Networks, 2005. Second International Conference on , pp.8 pp.-23, 24-24 Aug. 2005.

[78] M. Zeghdoud, P. Cordier and M. Terre, "Impact of Clear Channel Assessment Mode on the Performance of ZigBee Operating in a WiFi Environment", 1st Workshop on Operator-Assisted (Wireless Mesh) Community Networks, pp. 1-8, Sep. 2006.

[79] http://www.intel.com/support/wireless/wlan/sb/CS-025325.htm, last visited on April 24th 2012.

[80] Kjell J. Hole, Erlend Dyrnes, Per Thorsheim, "Securing Wi-Fi networks," Computer , vol.38, no.7, pp. 28- 34, July 2005.

[81] Lashkari, A.H.; Danesh, M.M.S.; Samadi, B.; , "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)," Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on , pp.48-52, 8-11 Aug. 2009.

[82] "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 6: Medium Access Control (MAC) Security Enhancements," IEEE Std 802.11i-2004, pp.0-175, 2004.

[83] L.Angrisani, M.Bertocco, G.Gamba, A.Sona, "Modeling the Performance of CSMA-CA Based Wireless Networks Versus Interference Level", IEEE Instrumentation and Measurement Technology Conference Proceedings, pp.376-381, 2008.

[84] M.Herrera, A.Bonastre, J.Capella, "Performance Study of Non-Beaconed and Beacon-Enabled Modes in IEEE 802.15.4 under Bluetooth Interference", The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies, pp.144-149, 2008.

[85] H.Lee, K.Lee, S.Ryu, S.Lee, K.Song, Y.Shin, “An efficient slotted CSMA/CA algorithm for the IEEE 802.15.4 LR-WPAN”, 2011 International Conference on Information Networking, pp488-493, 2011.

[86] T.Kim, J.Park, H.Chong, K.Kim, B.Choi, “Performance Analysis of IEEE 802.15.4 Non-Beacon Mode with the Unslotted CSMA/CA”, IEEE Communication Letters, Vol.12, Issue.4, pp.238-240, 2008.

[87] http://www.bluetooth.com/Pages/Bluetooth-Home.aspx, last visited on July 26, 2011.

[88] IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Part 11n: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard, 2009.

[89] M.Petrova, L.Wu, P.Mahonen, J.Riihijarvi, “Interference Measurements on Performance Degradation between Colocated IEEE 802.11g/n and IEEE 802.15.4 Networks”, Sixth International Conference on Networking, pp.93, 2007.

[90] L.Angrisani, M.Bertocco, M.Fortin, D.Sona, “Experimental Study of Coexistence Issues Between IEEE 802.11b and IEEE 802.15.4 Wireless Networks”, IEEE Transactions on Instrumentation and Measurement, Vol.57, Issue.8, pp.1514-1523, Aug.2008.

[91] "IEEE Recommended Practice for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements Part 15.2: Coexistence of Wireless Personal Area Networks With Other Wireless Devices Operating in Unlicensed Frequency Bands," IEEE Std 802.15.2-2003, pp.0_1-115, 2003.

[92] Lansford, J.; Stephens, A.; Nevo, R.; , "Wi-Fi (802.11b) and Bluetooth: enabling coexistence," Network, IEEE , vol.15, no.5, pp.20-27, Sep/Oct 2001.

[93] L.Angrisani, M.Bertocco, G.Gamba, A.Sona, “Modeling the Performance of CSMA-CA Based Wireless Networks Versus Interference Level”, IEEE Instrumentation and Measurement Technology Conference Proceedings, pp.376-381, 2008.

[94] B.Plepalli, W.Xie, D.Thngaraja, M.Goyal, H.Hosseini, Y.Bashir, “Impact of IEEE 802.11n Operation on IEEE 802.15.4 Operation”, International Conference on Advanced Information Networking and Applications Workshops, pp.328-333, 2009.

[95] W.Yuan, X.Wang, J.Linnartz, “A Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g”, 14^{th} IEEE Symposium on Communications and Vehicular Technology, pp.1-5, 15 Nov. 2007.

[96] H.Huo, Y.Xu, C.Bilen, H.Zhang, “Coexistence Issues of 2.4GHz Sensor Networks with Other RF Devices at Home”, Third International Conference on Sensor Technologies and Applications, pp.200-205, 2009.

[97] D.Yang, Y.Xu, M.Gidlund, “Coexistence of IEEE 802.15.4 based networks: A survey”, 36th Annual Conference on IEEE Industrial Electronics Society, pp.2107-2113, 2010.

[98] S. Y. Shin, H. S. Park and W. H. Kwon, “Mutual interference analysis of IEEE 802.15.4 and IEEE 802.11b”, Computer Networks, vol. 51, no. 12, pp. 3338-3353, Aug. 2007.

[99] S.Shin, H.Park, “Packet Error Rate Analysis of ZigBee Under WLAN and Bluetooth Interferences”, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 6, NO. 8, pp.2825-2830, Aug. 2007.

[100] F.Yao, S.Yang, W.Zheng, “Mitigating interference caused by IEEE 802.11b in the IEEE 802.15.4 WSN within the environment of smart house”, pp.2800-2807, Oct.2010.

[101] P.Yi, A.Iwayemi, and C.Zhou, “Developing ZigBee Deployment Guideline Under WiFi Interference for Smart Grid Applications”, IEEE Trans. Smart Grid, IEEE Early Access, 2010.

[102] P.Yi, A.Iwayemi, and C.Zhou, “Frequency agility in a ZigBee network for smart grid application”, IEEE Innovative Smart Grid Technologies (ISGT), pp. 1-6, 2010.

[103] I.Ramachandran and S.Roy, “Clear channel assessment in energy-constrained wideband wireless networks”, Tech.Rep., University of Washington, 2006

[104] Kiryushin, A.Sadkov and A.Mainwaring, “Real-World Performance of Clear Channel Assessment in 802.15.4 Wireless Sensor Networks”, Second International Conference on Sensor Technologies and Applications, pp.625-630, Aug.2008.

[105] M.Zeghdoud, P.Cordier and M.Terre, “Impact of Clear Channel Assessment Mode on the Performance of ZigBee Operating in a WiFi Environment”, 1st Workshop on Operator Assisted Community Networks, pp.1-8, Sep.2006.

[106] I.Ramachandran and S.Roy, “On the Impact of Clear Channel Assessment on MAC Performance”, IEEE GLOBECOM '06. pp. 1-5, Nov. 2006.

[107] B.H.Jung, J.W. Chong, C.Y.Jung, S.M.Kim, and D.K.Sung, “Interference mediation for coexistence of WLAN and ZigBee networks”, IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC 2008, pp. 1-5, 2008.

[108] G.Zhou, T.He, J.Stankovic, and T.Abdelzaber, “RID: Radio interference detection in wireless sensor networks,” in Proc. IEEE 24th Annu. Joint Conf. IEEE Comput. Commun. Soc., 2005, pp. 891–901.

[109] C.Won, J.H.Youn, H.Ali, H.Sharif, J.Deogun, “Adaptive Radio Channel Allocation for Supporting Coexistence of 802.15.4 and 802.11b,” Vehicular Technology Conference, vol 4, pp. 2522-2526, Sep. 2005.

[110] M.Kang, J.Chong, H.Hyun, S.Kim, B.Jung, and D.Sung, “Adaptive interference-aware multi-channel clustering algorithm in a ZigBee network in the presence of WLAN interference,” in Proc. 2007 2nd Int. Symp. Wireless Pervasive Comput., pp. 200–205.

[111] S. M. Kim, J. W. Chong, C. Y. Jung, T. H. Jeon, J. H. Park, Y. J. Kang,S. H. Jeong, M. J. Kim, and D. K. Sung, “Experiments on Interference and Coexistence between Zigbee and WLAN Devices Operating in the 2.4 GHz ISM Band,” in Proc. NGPC, pp. 15 - 19, Nov 2005.

[112] R. C. Shah and L. Nachman, “Interference detection and mitigation in IEEE 802.15.4 networks,” in 2008 Int. Conf. Inf. Process. Sensor Netw. (IPSN 2008), pp. 553–554, 2008.

[113] W. Yuan, J. P. M. G. Linnartz, and I. G. M. M. Niemegeers, “Adaptive CCA for IEEE 802.15.4 Wireless Sensor Networks to Mitigate Interference”, IEEE Wireless Communications and Networking Conference (WCNC) 2010, pp. 1 -5, 2010.

[114] C. Wong and W. Hsu, “An additional clear channel assessment for IEEE 802.15.4 slotted CSMA/CA networks”, 2010 IEEE International Conference on Communication Systems (ICCS), pp. 62-66, 2010.

[115] S. J. Bae, M. Y. Chung, H. J. Ki, T. J. Lee, S. Bae, H. Gi, M. Jeong, and T. Lee, “Method for recognizing available channel in IEEE 802.15.4 protocol CSMA/CA mechanism”, Patent Number(s): US2009129353-A1; KR2009050913-A; KR942891-B1, May 2009.

[116] J. Y. Ha, T. H. Kim, H. S. Park, S. Choi, and W. H. Kwon, “An Enhanced CSMA-CA Algorithm for IEEE 802.15.4 LR-WPANs”, IEEE Communications Letters, vol. 11, no. 5, pp. 461-463, 2007.

[117] M. Di Francesco, G. Anastasi, M. Conti, S. K. Das, and V. Neri, “An adaptive algorithm for dynamic tuning of MAC parameters in IEEE 802.15.4/ZigBee sensor networks”, 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp. 400-405, 2010.

[118] M. L. Huang and S. Park, “A WLAN and ZigBee coexistence mechanism for wearable health monitoring system”, 9th International Symposium on Communications and Information Technology, ISCIT 2009, pp. 555-559, 2009

[119] J. Linnartz, P. Van Kooten, and X. Wang, ”A method for communicating in a network, a system and a primary station therefor”, Patent Number(s): WO2010018505-A2; WO2010018505-A3, Feb. 2010.

[120] J. Espina, S. E. Boleko, F. Dalmases, T. Falck, and S. Boleko, “Time-based coexistence method for wireless communication.” Patent Number(s): WO2007015197-A2 ; EP1913737-A2; CN101238687-A; US2008232345-A1 ; IN200801010-P4; JP2009504059-W, Sept. 2008.

[121] Y. H. Kim, Y. H. Shin, W. H. Kwon, S. Y. Shin, J. Y. Choi, J. W. Lee, J. Y. Ha, and N. H. Kim, “Coexistence system for integrating heterogeneous wireless devices use frequency band into

single board enabling a IEEE 802.11 WLAN and IEEE 802.15.4 LR-WPAN which use frequency band, to work through active channel reservation technique", Patent Number(s): KR2007083321-A, Aug. 2007.

[122] ASUS RTN-16 Router, http://www.asus.com/Networks/Wireless_Routers/RTN16/, last retrieved on June 14, 2012.

[123] CC2420 Data Sheet, www- mtl.mit.edu/Courses/6.111/labkit/datasheets/CC2420.pdf, last retrieved on June 14, 2012.

[124] MIB600 Data Sheet, http://www.investigacion.frc.utn.edu.ar/sensores/Equipamiento/Wireless/MIB600CA_Datasheet.pdf, last retrieved on June 14, 2012.

[125] Atmel ATmega128L Data Sheet, http://www.atmel.com/Images/doc2467.pdf, last retrieved on June 14, 2012.

[126] MoteWorks, http://www.willow.co.uk/html/moteworks_software_platform.html, last retrieved on June 14, 2012.

[127] Aeroflex 3252 Spectrum Analyzer, http://www.aeroflex.com/ats/products/product/General_Purpose_Test/Spectrum_Analyzers/3250_Series_Analyzers~684.html, last retrieved on June 14, 2012.

[128] DITG, http://www.grid.unina.it/software/ITG/, last visited on Jan. 1, 2012.

[129] DD-WRT, http://www.dd-wrt.com/site/index, last visited on Jan.1, 2012.

[130] WireShark, http://www.wireshark.org/about.html, last visited on Jan.1, 2012.

[131] TinyOS, http://www.tinyos.net/, last visited on Jan.1, 2012.

[132] MoteWorks User Manual, Crossbow Corporation, 2005.

[133] A. Wijesinha, Y. Song, M. Krishnan, V. Mathur, J. Ahn, V. Shyamasundar, "Throughput Measurement for UDP Traffic in an IEEE 802.11g WLAN", Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, pp.220-225, 2005.

[134] M. Gast, "802.11 Wireless Networks: the Definitive Guide 2nd Edition", O'Reilly, Sebastopol, CA., 2005.

[135] M. Gast, "When is 54 Not Equal to 54? A Look at 802.11a, b, and g Throughput." http://www.oreilly.com/pub/a/wireless/2003/08/08/wireless_throughput.html, last visited on Mar. 16, 2012.

[136] 3GPP, “Spatial channel model for MIMO simulations”, TR 25.996 V6.1.0, Sep. 2003. [Online]. Available: http://www.3gpp.org/