DESIGN AND DEVELOPMENT OF NOVEL PERFORMANCE IMPROVEMENT TECHNIQUES FOR ZIGBEE PACKET TRANSMISSION UNDER WI-FI INTERFERENCE

BY

Tianyu Du

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

ZigBee based Wireless Sensor Networks (WSN) and Wireless Local Area Networks (WLAN) utilize the same un-licensed 2.4GHz frequency band. In our research, it is noticed that ZigBee could suffer serious performance degradation due to the collocated WLAN interference. After going through the available literature and combining with a thorough statistical analysis of our experimental results, several important factors that severely impact the ZigBee packet transmission performance have been identified. Motivated by these findings, novel techniques are designed to improve the performance of ZigBee packet transmission under WLAN interference. ACK with Interference Detection (ACK-ID) technique is developed to improve the delivery rate of ACK packets, and consequently reduce the number of redundant retransmissions. In order to improve the energy efficiency, Adaptive Transmit Power Adjustment (ATPA) is proposed to adaptively adjust the optimal transmit power while maintaining the predefined Packet Loss Rate (PLR) requirement. Time Aware Backoff and Transmission (TABTx) technique controls the time spent on each packet transmission attempt so as to avoid the Transmit First In First Out Byte Register (TXFIFO) overflow. Adaptive Preamble Padding with Retransmission Control (APPRC) is proposed to improve the transmission efficiency while satisfying the PLR requirement by determining the appropriate number of protective preamble padding bytes and whether or not to adopt packet retransmission. All these novel techniques have been implemented in the Crossbow MICAz motes and evaluated through extensive experimental measurements in the testbed.

Table of Contents

List of Figures

List of Tables

List of Symbols

A_i	The current consumption of power level *i*
DSN_{First}	The data sequence numbers for the first received packets during T_{update}
DSN_{Last}	The data sequence numbers for the last received packets during T_{update}
$Index_{Cur}$	The current power level index
$Index_{Max}$	The maximum power level index
$Index_{Min}$	The minimum power level index
L_{high}	Upper index limits in ATPA
L_{low}	Lower index limits in ATPA
L_{PSDU}	The PHY payload size of ZigBee packet
L_Z	ZigBee packet length
N_{Total}	The total number of packets transmitted including retransmitted packets
N_{max}	Maximum number of RSSI readings allowed for the proposed sending mechanism
N_P	The number of packets that needs to be transmitted
N_R	The number of received packets within T_{update}
PLR_{app}	The required PLR of a specific sensing application
PLR_{CRC}	Packet loss rate due to CRC failures
PLR_{High}	Upper PLR threshold in ATPA
PLR_{Low}	Lower PLR threshold in ATPA
PLR_{total}	The ZigBee packet loss rate
P_{th}	ED threshold
R_Z	Transmit bit rate
T_{BO}	The length of backoff calculated by CSMA/CA
T_{CCA_fail}	CCA failure rate

T_{data}	The time for transmitting the data packet
T_{init_BO}	The maximum length of initial CSMA/CA backoff
T_{int}	The inter-arrival time between two subsequent ZigBee packets
$T_{LMT}(n)$	Time limits for completing the n data packet (re)transmission attempts
T_m	Margin time frame
T_{rmng}	Remaining time before the arriving of next packet
t_s	Time interval between two consecutive RSSI readings
T_{update}	Interval for calculating the PLR value in ATPA

Acronyms

ACK	Acknowledgement
ACK-ID	ACK with Interference Detection
AES	Advanced Encryption Standard
AODV	Ad hoc On Demand Distance Vector
AP	Access Point
APPRC	Adaptive Preamble Padding with Retransmission Control
ATPA	Adaptive Transmit Power Adjustment
AWGN	Additive White Gaussian Noise
BEB	Binary Exponential Backoff
BER	Bit Error Rate
CAP	Contention Access Period
CCA	Clear Channel Assessment
CFP	Contention Free Period
CRC	Cyclic Redundancy Check
CS	Carrier Sense
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSS	Chirp Spread Spectrum
CTS	Clear to Send
DCF	Distributed Coordination Function
DIFS	DCF Inter-frame Space
D-ITG	Distributed Internet Traffic Generator
DSN	Data Sequence Number
DSSS	Direct-sequence Spread Spectrum

ED	Energy detection
FCS	Frame Check Sequence
FFD	Full-function Device
GPS	Global Positioning System
GTS	Guaranteed Time Slots
IDT	Inter-departure Time
ISM	Industrial, Scientific and Medical
IT	Information Technology
LQI	Link quality indicator
LR-WPAN	Low Rate – Wireless Personal Area Network
LTE	Long Term Evolution
MAC	Media Access Control
MIMO	Multiple-Input-Multiple-Output
MPDU	MAC Protocol Data Unit
MTU	Maximum Transmission Unit
OFR	TXFIFO overflow rate
PAN	Personal Area Network
PCCA	Persistent CCA
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PDBPP	Protective Dummy-byte Preamble Padding
PHY	Physical Layer
PLCP	PHY Layer Convergence Protocol
PLR	Packet Loss Rate
PPP	Point to Point Protocol
PSDU	PHY Service Data Unit

O-QPSK	Offset-Quadrature Phase Shift Keying
OFDM	Orthogonal Frequency Division Multiplexing
OFR	TXFIFO Overflow Rate
QoS	Quality of Service
RFD	Reduced-function Device
RSSI	Received Signal Strength Indicator
SHR	Synchronization Header
SIFS	Short Inter Frame Space
SINR	Signal-to-interference-plus-noise Ratio
TABO	Time Aware Backoffs
TABTx	Time Aware Backoff and Transmission
TDMA	Time Division Multiple Access
TXFIFO	Transmit First In First Out Byte Register
UWB	Ultra-wideband
WBAN	Wireless Body Area Network
WCDMA	Wideband Code Division Multiple Access
WISA	Wireless Interface for Sensors and Actuators
WLAN	Wireless Local Area Network
WR	Wireless Router
WSN	Wireless Sensor Networks
ZC	ZigBee Coordinator
ZR	ZigBee Router

Acknowledgement

I would like to express my sincere gratitude 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 in all the time of research and writing of this thesis.

The same gratitude is given to my supervisors, 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.

I would like to thank Mr. Yong Tang, who passed on valuable research experience and academic knowledge to me, and provided helpful suggestions 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

IN the past several decades, the development and deployment of wireless communication networks experienced an unprecedented growth fueled by the information explosion and technique innovations [1]. From the coffee shops offering ubiquitous Wi-Fi coverage to the worldwide popularity of cellular mobile services, which have a mass market of billions of subscribers, wireless technologies have significantly impacted our life-style [2].

Nowadays, various wireless techniques supporting different fixed, mobile or portable applications such as Global Positioning System (GPS), garage door opener, and satellite television are commercialized or undergoing active research and standardization [3]. One of the best known examples is Wireless Local Area Network (WLAN), also known as Wi-Fi, aiming to provide wireless Internet access within a local area, such as campus building or airport. It is driven by the IEEE 802.11 standard, and the newest revision, IEEE 802.11ad, can achieve a theoretical maximum throughput of up to 7Gbit/s [4]. Due to its low cost, ease of installation, and almost no maintenance requirement, WLAN has quickly gained an explosive popularity and is available on most laptops and PDAs (Personal digital assistant). Meanwhile, different wireless computer peripherals (e.g. wireless mice, keyboards,

headsets) using Bluetooth or UWB technologies have been developed and are used to generate products that materialize a fully integrated wireless working environment [2].

However, Wi-Fi devices have relatively small transmission range. Modern mobile networks provide a complementary technique for broadband wireless access to Internet, offering integrated data and voice services. Moreover, with cellular and seemingly seamless hand-off techniques, mobile phone networks can support national or global network coverage and support a large number of subscribers [5]. The "3G", referring to the collection of third generation mobile technologies and standards such as WCDMA (Wideband Code Division Multiple Access) or CDMA2000, can offer a data rate from 384kbps up to 2Mbps, while the undergoing transition to LTE (Long Term Evolution, often branded as 4G) will offer much wider bandwidth [6]. One of the future trends is the integration between Wi-Fi and mobile phone network. Nowadays most smart phones can support both network connections.

Different from previous techniques aiming to provide high bandwidth applications, the potential and needs of low data rate and low cost applications targeting the materialization of ubiquitous interaction between the user and his/her environment have captured the enthusiasm of both academics and industry. These applications have provided motivation for the development and deployment of Wireless Sensor Networks (WSN) [7]. WSN related research has been one of the key and most popular themes of many workshops, conferences and special issues of several renowned journals (e.g. IEEE Conference on Mobile Ad Hoc and Sensor Systems, ACM Conference on Embedded Networked Sensor Systems, and ACM Transactions on Sensor Networks). A brief overview of WSN is given in the next section.

1.1 Overview of Wireless Sensor Networks

Wireless sensor networks consist of spatially dispersed autonomous sensor nodes with sensing, computing and wireless communication capabilities that give an administrator the ability to collect data or monitor and react to events and phenomena in a specified environment, which can be the physical world, a biological system, or an Information Technology (IT) framework. The number of sensor nodes in a WSN can be from a few to thousands, and each node consists of sensor(s), a microprocessor, an energy source and a radio transceiver [8]-[11].

1.1.1 Wireless Sensor Network Architecture

The main features of WSN include scalable with respect to the number of nodes in the network, energy efficient, self-organization, self-healing, having a sufficient degree of connectivity among nodes, low complexity, and small size of nodes [12].

Each sensor node in a WSN forwards data, possibly via multiple hops, to a *sink* (sometimes denoted as *coordinator*) that can use the data locally or pass it to other networks (e.g. the Internet) through a *gateway,* then to the final user. A single-sink WSN is shown in the left part of Figure 1.1. The single-sink scenario does not scale well in respect to the number of nodes it can support with the maximum number determined by the maximum throughput of WSN in the region of the sink and the network's performance expectations. A WSN containing multiple sinks is shown in the right part of Figure.1.1. This kind of WSN scales well in terms of the number of nodes it can contain and effectively service [12].

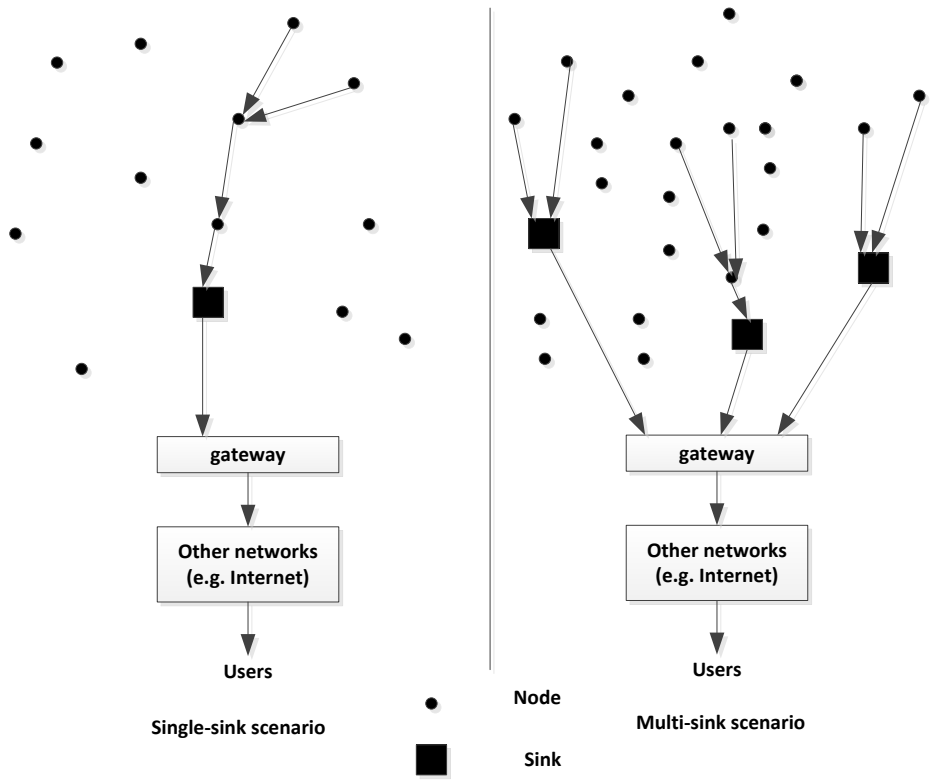

Fig.1.1 Single-sink and Multi-sink WSN [12]

1.1.2 Wireless Sensor Network Applications

The different types of sensors (e.g. visual, infrared, acoustic, seismic, magnetic, thermal, radar) are able to monitor a wide range of ambient conditions such as temperature, noise level, humidity, human and vehicular movement, which fuels the development and deployment of WSN applications. These applications can be classified into the following five categories [10] [13] [14].

A. ***Military Applications****:* WSN can be deployed rapidly and at high density, it is able to self-organize, and is fault tolerant. Those characteristics make WSN very suitable for use in battlefields [15], where WSNs can be used to monitor friendly forces, equipment, and

ammunition, reconnoiter opposing forces and terrain, and detect the presence of harmful nuclear, biological, and chemical agents [10].

B. ***Environmental Applications***: Applications include tracking the movements of animals, use of large-scale Earth monitoring and planetary exploration, sensing of various chemical/biological agents, forest fire detection etc. [10] [16].

C. ***Health Applications*****:** The emergence of tiny, wearable wireless sensors found extensive use in medical care. Some of the existing applications are integrated patient monitoring, safer drug administration in the hospital, tele-monitoring of human physiological signals, replacement of exiting wired telemetry systems, e.g. in the cases of physical rehabilitation or long-term ambulatory monitoring [10] [17].

D. ***Home Applications:*** Various home devices with built-in sensor nodes can interact with each other using the Internet or other external networks (e.g. the cellular network infrastructure). This formed the foundation for the development of new or the improvement of existing applications servicing the home user [18] [19]. Examples are home automation [125], home monitoring for safety/security [126], and cost efficient electric energy consumption (see smart grid [127], [128]). WSN is also a critical technology of the next-generation electric power system, known as *smart grid* [20]. It can be used to enhance the transmission and distribution of electrical power [129] [130] and implement home energy management by providing communication and control capacities at low cost [21], [131], [132].

E. ***Industrial Applications:*** Due to the advantages of easy deployment, high granularity and high accuracy, WSN is also beneficial and frequently used in industrial applications [10],

such as managing inventory, monitoring product quality, building automation, and access control [13].

1.2 Overview of IEEE 802.15.4 and ZigBee Standards

Standardization is very important to the success of WSN market in the commercial due need to the low cost of devices. Several standards are currently either ratified or under development. For example, a Bluetooth variant by ABB Inc. named WISA (Wireless Interface for Sensors and Actuators) [121] targets real-time industrial control applications. Wi-Fi, designed for rather high data rates that are unnecessary in WSNs, still can be useful to be for establishing the wireless connection of selected sink/coordinator nodes. And the IEEE 802.15.6 group, oriented to WSN for WBAN (Wireless Body Area Network), sets the basis for the possible creation of a heterogeneous WSN environment and provides a new technical solution. However, the most important and flexible technology for standardized WSN solutions seems to be the IEEE 802.15.4, which is developed to specify the physical (PHY) layer and Media Access Control (MAC) sub-layer for LR-WPAN (Low Rate – Wireless Personal Area Network), targeting low rate, low energy consumption and low cost wireless applications [22] [23].

On top of IEEE 802.15.4, other network protocols have been designed, such as WirelessHART, ISA100.11a, and ZigBee. WirelessHART [133] and ISA100.11a [134] are designed for meeting the stringent requirements of industrial applications [24], and are addressing strict latency and high reliability, which are required in process automation and

manufacturing. ZigBee is the most widely distributed WSN standard, developed by the ZigBee alliance [26] that has over 400 member companies. The ZigBee standard specifies the network layer and the framework for the application layer of the protocol stack on top of the IEEE 802.15.4 [25] [26]. An introduction of IEEE 802.15.4 and ZigBee is given in the following subsections.

1.2.1 IEEE 802.15.4 Standard

1.2.1.1 IEEE 802.15.4 PHY Layer

IEEE 802.15.4 was launched in 2003, and depending on the geographical area where the system is deployed, three unlicensed frequency bands are defined, namely, a 2.4GHz Industrial, Scientific and Medical (ISM) band (with 16 channels and maximum data rate 250 Kbit/s); a 915MHz band (with 10 channels and maximum data rate 40 Kbit/s); and an 868MHz band (with 1 channel and maximum data rate 20 Kbit/s). Additionally, the subsequent revisions introduced new PHYs including one using Direct Sequence Ultra-wideband (UWB) and another using Chirp Spread Spectrum (CSS), and expanded the available spectrum in Japan and China [22] [27].

The IEEE 802.15.4 PHY is in charge of the following tasks [22] [28]:

- **Activation and deactivation of the radio transceiver**: The radio transceiver may operate in one of the four states: transmitting, receiving, idle or sleeping.
- **Energy Detection (ED) within the current channel:** This measurement is used for channel selection or Clear Channel Assessment (CCA).

- **Link Quality Indicator (LQI) for received packets:** LQI measures the quality of a received signal using receiver ED value, a signal to noise estimation or a combination of both.
- **Clear Channel Assessment (CCA) for Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).**
- **Channel frequency selection:** The physical layer should be able to adjust the operating channel based on the request by a higher layer.
- **Data transmission and reception.** According to IEEE 802.15.4, transmission is organized in frame structures. For different purposes, there are four frame types: beacon frame, data frame, Acknowledgement (ACK) frame, and MAC command frame.

1.2.1.2 IEEE 802.15.4 MAC Sub-layer

The MAC sub-layer provides an interface between the physical layer and the higher layer protocols, and is responsible for the following tasks: supporting PAN association and disassociation, security control, employing the CSMA/CA mechanism for channel access, providing a reliable link between two peer MAC entities, generating or synchronizing the beacons, and maintaining the Guaranteed Time Slots (GTS) mechanism [29].

Two different operational modes corresponding to different channel access mechanisms, namely *beacon-enabled* and *non-beacon-enabled*, are specified in the IEEE 802.15.4 protocol. In the non-beacon-enabled mode, nodes use an unslotted CSMA/CA protocol to access the channel. While in the beacon-enabled mode, the access to the channel is

managed through a superframe (shown in Fig.1.2), starting with a beacon frame and transmitted by the WPAN coordinator. The superframe is composed of an inactive part, allowing nodes to go to sleeping mode, and an active part, which is divided in two parts: the Contention Access Period (CAP) and the Contention Free Period (CFP). In the CAP, nodes access the channel using a slotted CSMA/CA mechanism, while the CFP is formed by Guaranteed Time Slots (GTSs) and is allocated by the coordinator to the specified nodes [22] [30].

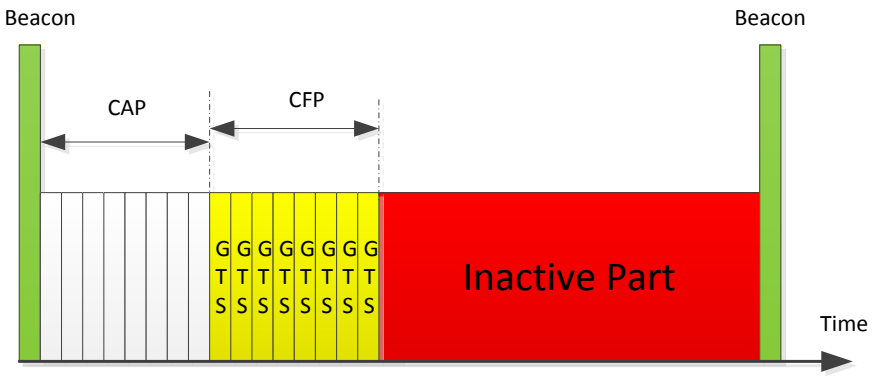

Fig.1.2 IEEE 802.15.4 Superframe structure as defined for the beacon-enabled mode [22]

1.2.1.3 IEEE 802.15.4 Network Topology

IEEE 802.15.4 defines two types of devices: a Full-Function Device (FFD) and a Reduced-Function Device (RFD). A FFD is equipped with the full set of MAC services and can operate as a network coordinator or an end device. A RFD is a device with minimal implementation of the protocol and can only act as an end device [29].

Two basic types of network topologies are considered in IEEE 802.15.4: the star topology and the peer-to-peer topology. Both are shown in Fig.1.3. In the star topology, devices can

only communicate with a single central controller, named PAN (Personal Area Network) coordinator. This topology is better suited when the network coverage is small and a low latency is required. The peer-to-peer topology also has a PAN coordinator, but any FFD is able to communicate with any other FFD as long as they are within the communication range of one another, while a RFD, due to limited resource and memory capacity, can only associate with a single FFD or the PAN coordinator [29] [31].

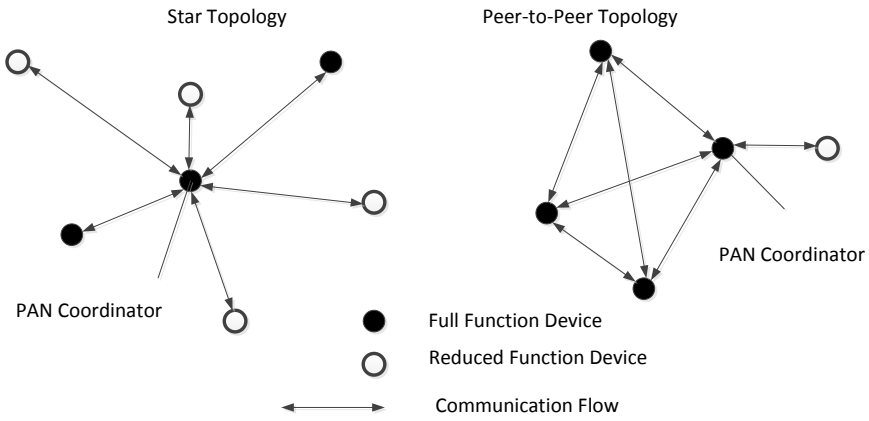

Fig.1.3 Star and peer-to-peer topology examples [29]

1.2.2 ZigBee Standard

As stated before, the ZigBee protocol stack (shown in Fig.1.4) on top of IEEE 802.15.4 is univocally described by ZigBee Alliance to guarantee the interoperability among devices produced by different manufacturers [22].

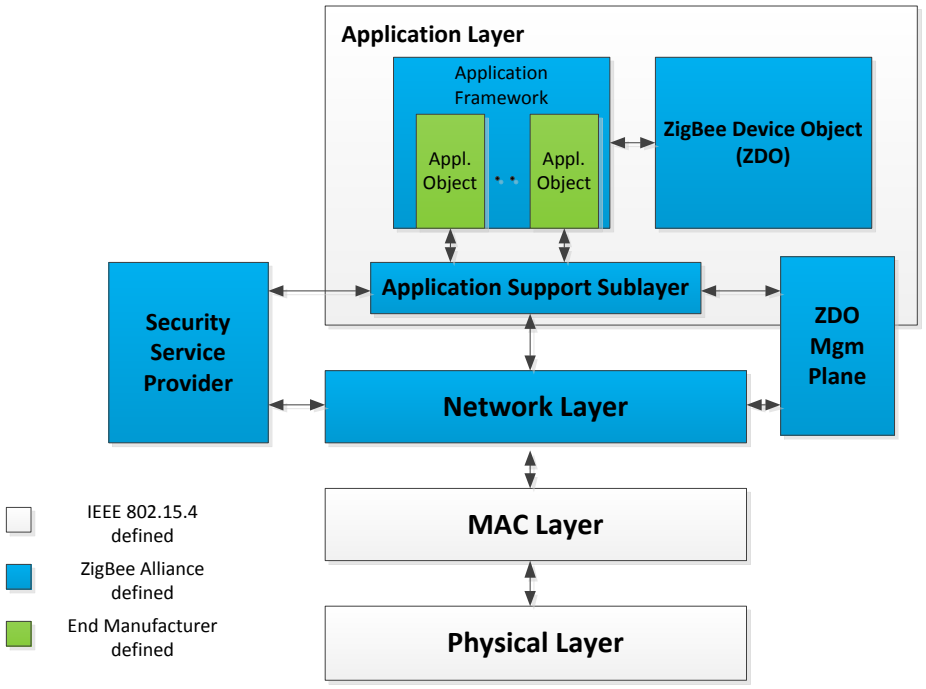

Fig.1.4 Overview of ZigBee protocol stack architecture [22]

1.2.2.1 ZigBee Network Layer

In IEEE 802.15.4 standard, basic device types and topologies are defined, but not completely described. The ZigBee standard expands this work and farther gives the detailed responsibilities of network layer, including mechanisms to establish, join or leave a network, frame security (e.g. 128 bytes AES (Advanced Encryption Standard)), routing (e.g. Ad hoc On Demand Distance Vector (AODV), Routing IP for 802.15.4 [138]), path and neighbors discovery, and neighbor information storage [22] [32] [33].

ZigBee supports three types of devices: ZigBee Router (ZR), acting as intermediate node, relaying data from other devices; ZigBee Coordinator (ZC), a ZR that manages the network; End Device (ED), located at the edge of the network for data collection and unable to relay data of other devices. Besides the star topology defined in IEEE 802.15.4, two more

complicated ones are supported in ZigBee: mesh and cluster tree as shown in Fig.1.5 [34]. Using these two topologies, high level of reliability and scalability are supported with respect to the number of nodes in the network and the area to be covered [22].

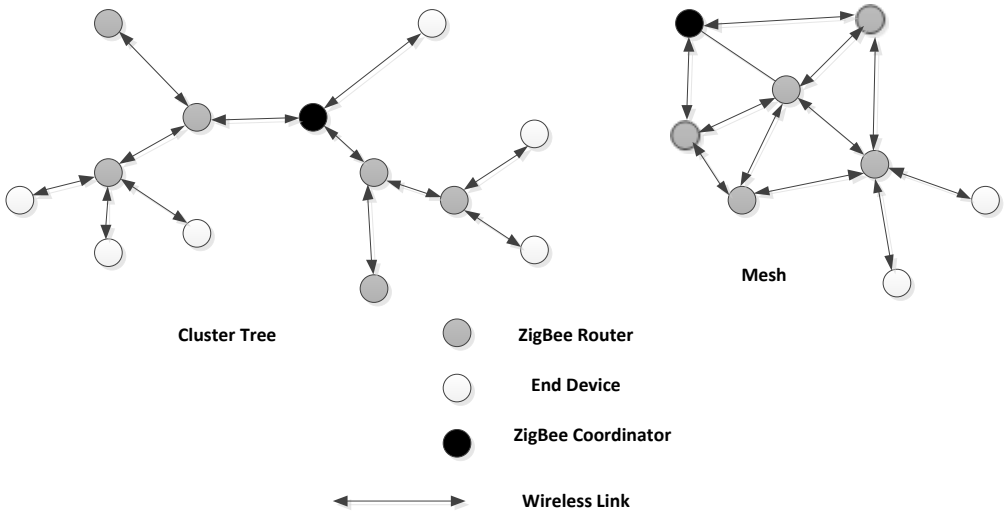

Fig.1.5 Cluster Tree and Mesh topology examples [34]

1.2.2.2 ZigBee Application Layer

As shown in Fig.1.4, the ZigBee application layer is composed of the application support sub-layer, the application framework, the ZigBee device objects and the manufacturer-defined application objects. The application support sub-layer provides an interface between network layer and application layer through a set of services, such as fragmentation and reassembly of packets, message forwarding between bound devices and group address definition and management. The application framework is responsible to provide an execution environment for application objects to transmit and receive data. The overall device management is defined in the ZigBee device objects, including definition of the role of the devices in the network (e.g. ZR or ED), device discovery and determination of

which application is provided, initialing and responding to binding request, and security management [22] [32].

As described in the previous section, ZigBee is a widely deployed and developed WSN standard with hundreds of vendors in ZigBee Alliance. In order to provide device interoperability across different manufacturers, for each application domain or market, an agreement, named as an application profile, is used to describe the devices supporting this specific application and the corresponding message-handling scheme used by those devices to communicate with each other, in effect, defining the type and the features of the network [32] [35]. For example, ZigBee home automation is a ZigBee application profile which defines a series of devices intended for use inside the house. These devices are permitted to exchange well-defined messages to form a wireless home automation application such as sending a light sensor measurement to a lighting controller, turning a lamp on or off, or sending an alert message if a motion sensor detects an unexpected movement [35].

The application profile can be public, managed by the ZigBee Alliance; or private, specified by a ZigBee manufacturer for restricted use. At time of this writing, the following list of public profiles is available [26]:

- ZigBee Building Automation (Efficient commercial space
- ZigBee Remote Control (Advanced remote control)
- ZigBee Smart energy (Home energy savings)
- ZigBee Health Care (Health and fitness monitoring)

- ZigBee Home Automation (Smart Homes)
- ZigBee Input Device (Easy-to-use touch-pads, mice, keyboards, wands)
- ZigBee Light Link (LED lighting control)
- ZigBee Retail Services (Smarter shopping)
- ZigBee Telecom Services (Value-added services)

1.3 Technical Challenges for WSNs

As mentioned earlier, WSNs are receiving significant attention both by academics and industry due to its strong potential in the sector of low power and low cost applications. However, several key technical challenges exist that influence the design of WSNs.

A. ***Scalability*****:** In order to provide redundancy and improve the fault tolerance of a WSN working in a harsh environment, sensor nodes are densely deployed. Therefore, the network protocol should be able to handle a large number of nodes efficiently. Also, the sensor nodes which are prone to frequent failures require careful topology maintenance [10].

B. ***Production costs:*** In a WSN, the number of the nodes can range from a few to thousands. The cost of a single node is very significant factor to the determination of the overall cost of the network. How to reduce the price of a sensor node is challenging. A typical sensor device is composed of a sensing unit, a processing unit, a transceiver unit and a power unit. Depending on the applications, it may also be integrated with a

location finding system, a mobilizer, etc. These are all added to the cost of the device [10].

C. ***Real-time requirement:*** In some WSN cases such as alarm-driven systems or multimedia applications, data must be delivered within time constraints so that real-time operation is a requirement for their associated protocols. In order to guarantee the end-to-end delivery time, delay jitter or other QoS metrics, some real-time routing protocols are proposed. For example, the SPEED [36] protocol uses feedback information to maintain a desired delivery speed for each end-to-end connection across the WSN. However, packet loss, congestion, noise and other problems makes provision of these guarantees difficult [37] [38].

D. ***Security and privacy:*** The resource restraints cause obstacles to implement efficient computer security mechanisms in WSNs. Adopting traditional encryption algorithms such as AES with 128-byte key in IEEE802.15.4/ZigBee based WSNs, will introduce extra cost such as additional computation time or decoding delay. In addition, due to the unreliable communication channels and unattended operation of WSN, WSNs are particularly vulnerable to several attacks, such as privacy violation, physical attacks, and so on [39].

E. ***Energy efficiency:*** Due to the hardware constraints, most sensor nodes are battery-powered and for some applications, replacement of power resource is impossible. Therefore, the lifetime of WSN significantly depends on the energy efficiency. This challenge requires energy awareness at all layers of the WSN protocol stack. At PHY and MAC layers, some researches work on dynamic voltage scaling, low duty cycle, topology

control and so on [135] [136]. At higher layers, different proposals focus on energy efficient techniques such as efficient routing, protocol overhead reduction and reliable relaying of data [40].

F. ***Coexistence with other wireless techniques:*** The IEEE 802.15.4/ZigBee WSN is operating at the unlicensed 2.4GHz ISM band. Due to the operation of other wireless devices operating in the same spectrum, such as IEEE 802.11 b/g/n, Bluetooth, cordless phone, etc., there is concern of potential interference problem. Most worries focus on the Wi-Fi since it uses higher transmit power and is widely deployed in both residential and office environments [41] [42].

1.4 Research Motivations and Objectives

The previous sections introduced the characteristics, applications, standards, and technical challenges of WSNs. Among the challenges, the wireless coexistence interference issue raises growing concerns due to the increasing demand for use of ZigBee based WSN in indoor environment. As described before, most worries come from the collocated 802.11b/g/n Wi-Fi networks, which are also operating at the unlicensed 2.4GHz ISM band. It has been shown that the interference of a ZigBee network to a Wi-Fi network is ignorable even when they are very close due to the much higher transmit power of Wi-Fi devices [43]. However, on the contrary, the low-power and low-rate ZigBee/IEEE 802.15.4 based WSN nodes are vulnerable to the interference generated by the considerably more powerful Wi-Fi devices. The allocation of ZigBee and 802.11b/g WLAN channels over the 2.4GHz ISM band is shown in Fig. 1.6.

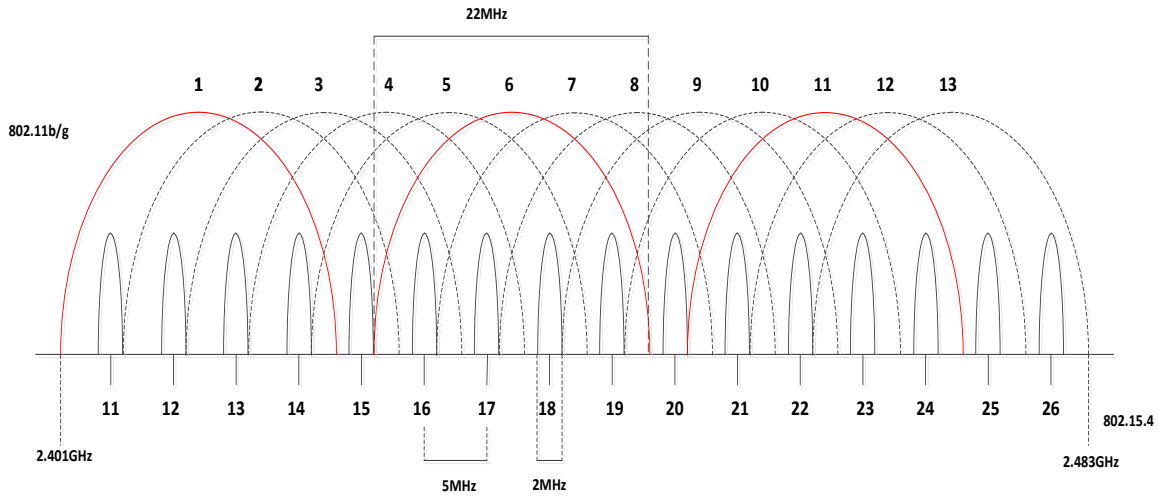

Fig.1.6 Channel Allocation of IEEE 802.15.4 and IEEE 802.11b/g

As shown in Fig.1.6, the most frequently used orthogonal Wi-Fi channels are 1, 6, and 11. In this case, ZigBee channels 15, 20, 25, and 26 are free from Wi-Fi interference. However, operating only in those four channels significantly limits the spectrum usage. And along with the increasing density of Wi-Fi spots, there is no assurance that using these four channels solves the Wi-Fi interference problem. Although frequency agility-based interference avoidance algorithms can be used to perform smart channel selection, switching the operating channel of the entire WSN cluster generates considerable extra financial and performance degradation cost (e.g. higher power consumption, longer delay, possible loss of packets) to the network. Thus, it is necessary to develop cost effective technologies that alleviate the performance degradation of the ZigBee system caused by coexisting Wi-Fi networks operating in the overlapping channels.

There have been several research contributions studying coexistence issues. A comprehensive literature survey is presented in the next chapter. After going through the

available literature and thorough examination and statistical analysis of measurements data we collected during our extensive experimental studies, we became aware of several important factors that severely impact the ZigBee packet transmission, which have not been identified in earlier studies. We also identified some significant weaknesses of existing Wi-Fi induced interference mitigation technologies, designed to improve ZigBee's performance. We summarize the most significant points of such findings below while detailed discussion will be presented in the following chapters.

- Previous proposed techniques focus on improving the performance for the transmission of data packets. However, the transmission of ACK packets might experience the same or similar interference problems with the data packets, which generates excessive number of packet retransmissions. Our experimental results clearly demonstrated such problem, thus techniques for protecting ACK packets are needed.
- It is not energy efficient to set the transmit power of all ZigBee motes in the WSN at one fixed value for operating in the presence of varying interference and for satisfying Packet Loss Rate (PLR) requirements of different sensing applications. Ideally, the motes should be able to adjust their transmit power adaptively and in accordance to the external interference level, the objective is to use the lowest possible power while maintaining the required PLR.
- For periodic sensing/monitoring applications, sensing data need to be sent out at fixed intervals. However, it is was noticed in our experiments that quite a few packets are lost due to overflows occurring at the ZigBee mote's sending buffer. This

becomes particularly problematic when the ZigBee mote is transmitting at high packet rate. Such buffer overflow is due to the possible long delays at sending out packets because of the exponential backoff CSMA/CA algorithm follows when trying to access the shared channel. Suitable modifications to the MAC algorithm are needed to remove or at least reduce the impact of this problem.

- Another important finding derived from our experimental results is that it is very important to protect the ZigBee physical layer's (PHY) header when subjected to external interference. Our experimental data showed clearly that a significant amount of ZigBee packet losses occur due to the corruption the ZigBee packet's PHY header has suffered from Wi-Fi interference, which could happen even when the CSMA/CA algorithms of the Wi-Fi and ZigBee devices are able to detect each other's signal. Techniques that protect the PHY header should be able to reduce packet loss as well as increase data transmission efficiency.

Motivated by the above findings, the research in this thesis aims at studying the factors that cause packet loss, then designing, implementing and testing effective countermeasures. Furthermore, it aims at improving the energy, bandwidth, and data transmission efficiency of ZigBee motes while satisfying the PLR requirements of sensing applications. Thus, we set the following objectives:

- Design and develop techniques to improve the delivery rate of ACK packets when subjected to interference from collocated Wi-Fi connection. The proposed

technique should be simple and effective without introducing significant delay to the packet transmission process.

- Design, implement and evaluate adaptive transmit power control algorithm that can respond promptly to the changing level of external interference so as to save power when interference is low, and boost signal when there is growing interference to meet PLR requirement. The proposed algorithm should be able to respond timely to the interference changes.
- Design, implement and evaluate techniques that address the buffer overflows that are due to the long delays generated by the CSMA/CA protocol's exponential backoff algorithm. The proposed technique should be able to adaptively control the total packet transmission time in accordance to the data generation rate of the serviced sensing applications in order to avoid the buffer overflow.
- Design, implement and test efficient techniques to protect the PHY header corruption of the ZigBee packet when subjected to Wi-Fi interference. The approach should be able to effectively protect the PHY header while introducing little overhead so as to maintain high data transmission efficiency.

Taking into consideration the risk of leaving hidden factors (e.g. inaccurate modeling of channel impairments, and hidden protocol/algorithm interoperability mechanisms) unaccounted through computer simulation or mathematical analysis based performance evaluation approaches, we decided to pursue our research by implementing on our existing wireless testbed the designed technology and evaluate it

through extensive experimentation, so as to assess performance under specific conditions and understand behavior.

1.5 Research Contributions

Our research work led to the following contributions:

- We designed and developed a novel technique named ACK with Interference Detection (ACK-ID) that can effectively reduce the ACK losses, while introducing only small additional delay.
- We proposed and implemented an Adaptive Transmit Power Adjustment (ATPA) technique to improve the energy efficiency of WSN while maintaining the predefined maximum tolerable PLR of the application.
- We designed and developed a Time Aware Backoff and Transmission (TABTx) technique to limit the total transmission time of each packet, and consequently avoid the packet losses caused by packet drops in the transmitter due to transceiver buffer overflow in sending out preceding packets.
- We proposed and evaluated an Adaptive protective dummy-byte Preamble Padding with Retransmission Control technique (APPRC) which significantly improves the performance of ZigBee packet transmission in terms of PLR and transmission efficiency. Furthermore, APPRC enables packet retransmission when the protective dummy-byte preamble padding alone cannot meet the PLR requirement of the sensing application.

1.6 Thesis Organization

The rest of the thesis is organized as follows. Chapter 2 presents a research literature review related to our work. Chapter 3 introduces our testbed and proposes a novel technique named ACK with Interference Detection (ACK-ID). In Chapter 4, an Adaptive Transmit Power Adjustment (ATPA) technique for ZigBee based WSN is proposed and evaluated using our testbed. In Chapter 5, the Time Aware Backoff and Transmission (TABTx) technique is introduced. In Chapter 6, we proposed the Adaptive Protective Dummy-byte Preamble Padding with Retransmission Control (APPRC) technique. Finally, the thesis is concluded and the future work is summarized in Chapter 7.

Chapter 2

Literature Review

Nowdays, ZigBee based WSN can be considered as a core technology for short range wireless communications aiming at low power, low data rate applications. The main operating spectrum for ZigBee based WSN is the unlicensed 2.4GHz ISM band, which is shared with other heterogeneous devices and standards such as Wi-Fi, Bluetooth, Wi-Media, Cordless Phone and microwave ovens [44]. This can result in mutual interference and thus have performance degradation such as increased packet losses, packet transmission delay and delay jitter, which could produce a number of malfunctions, e.g. false commands, false alarms, loss of synchronization. The worst threat comes from the collocated IEEE 802.11b/g/n (Wi-Fi) WLAN due to its wide indoor deployment as well as its higher transmit power and traffic volumes. Therefore, our research focuses on the coexistence impact of IEEE 802.11g on the IEEE 802.15.4. In this dissertation, the terms WLAN and Wi-Fi are used interchangeably. So are the terms ZigBee and IEEE 802.15.4 because our research focused on the MAC sub-layer and PHY layer.

In recent years, there have been several works investigating coexistence issues between IEEE 802.11b/g/n and ZigBee networks. According to [45] [46] [47], due to the low data rate and low transmit power of ZigBee network, Wi-Fi is scarcely affected by the presence of IEEE 802.15.4 network even when they are in the proximity to each other. However, on the

contrary, Wi-Fi impacts significantly ZigBee's performance. Section 2.1 provides a comprehensive literature survey on the coexistence studies of ZigBee networks under Wi-Fi interference. In section 2.1.1, analytical models, simulations or testbed developed to investigate the performance of ZigBee under WLAN interference are presented. Interference mitigation techniques are reviewed and discussed in section 2.1.2.

Most ZigBee nodes are powered by low capacity and in several cases un-rechargeable/un-replaceable batteries, thus energy efficiency is one of the most critical factors to the WSN design. Using the lowest transmit power needed to support the set network performance requirements is one of the most promising ways to preserve a WSN node's energy. The value of lowest transmit power level is dependent on the noise and interference levels within WSN's operational environment. Since interference levels tend to be time- and location-variant, it is necessary to design and implement mechanisms capable of adjusting the transmit power adaptively. In section 2.2, we summarize the current WSN transmit power control mechanisms and discuss their weaknesses.

Due to the coexistence of Wi-Fi transmission in the overlapping channel, the CSMA/CA in ZigBee motes might introduce long delays that can cause the overflow of the transceiver buffer and consequently packet drops. This could be a severe problem when ZigBee mote transmits at high packet rates. A literature review of research works on IEEE 802.15.4 CSMA/CA is given in section 2.3.

2.1 Current knowledge on the behavior of ZigBee under Wi-Fi Interference

Recently, several research contributions dealing with the behavior of a ZigBee network subjected to Wi-Fi interference appeared in the open literature. Theoretical models, experimental results and interference mitigation techniques are available to enhance the ZigBee performance when in coexistence with Wi-Fi networks. These works will be summarized and discussed in the following sections.

2.1.1 Analytical Models and Experimental Performance Assessments

2.1.1.1 Analytical Models

It is meaningful to develop mathematical framework to analyze the performance of ZigBee network under WLAN interference. In [52], a derivation of closed-form expressions for the Packet Error Rate (PER) of heterogeneous packet radio networks is presented. This work applies an energy based interference analysis approach. The packet transmission is considered successful if the total interfering energy (calculated over the duration of the ZigBee packet) is below a predefined tolerable threshold. However, this approach is not accurate as the interference may only exist during a part of the ZigBee packet transmission, yet it can cause several bit errors that result in packet loss.

A more accurate way to estimate the PER could be obtained from the Bit Error Rate (BER) and packets collision time. Several related papers ([53]-[56]) have been published recently using the BER evaluation and collision time model. The interference model between ZigBee and IEEE 802.11b network proposed in [56] is illustrated in Fig. 2.1. This analytical model

assumes that ZigBee devices and WLAN devices are hidden to each other. As shown in Fig. 2.1, T_Z, L_Z, T_W and L_W denote inter-arrival time between two ZigBee packets, length of ZigBee packet, inter-arrival time between two Wi-Fi packets, length of Wi-Fi packet. T_{ACK}, $T_{backoff}$, and T_{CCA} represent duration of ZigBee ACK packet, average backoff time of ZigBee, and ZigBee CCA duration. $T_{collision}$, $T_{ACK,TimeOut}$, and t_{SIFS} are collision time between IEEE 802.15.4 packet and each IEEE 802.11b packet, maximum wait time for Wi-Fi ACK packet, and short inter frame space of 802.11b. For simplicity, ACK packets of both ZigBee and Wi-Fi are not considered in the collision time calculation. By the time-domain analysis of collision process, the collision time can be obtained. The Wi-Fi signal is considered as Additive White Gaussian Noise (AWGN) for ZigBee to calculate BER, while ZigBee signal is treated as partial band jammer noise for Wi-Fi. Then, the PER is obtained from collision time and BER [56].

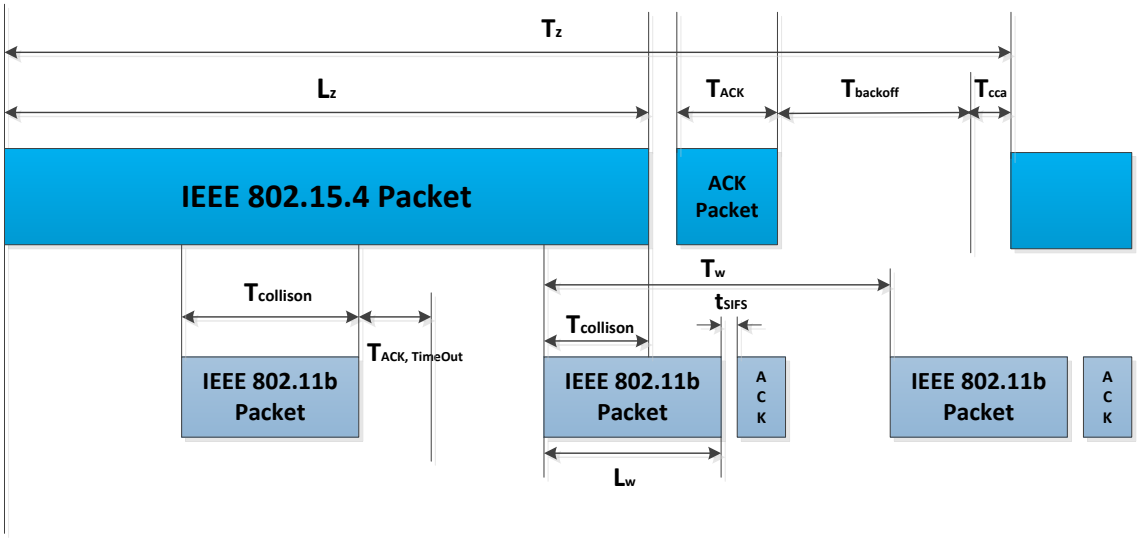

Fig.2.1 Collision time model between IEEE 802.11b and IEEE 802.15.4 [56]

In [53], the impact on IEEE 802.11 network under IEEE 802.15.4 interference is first estimated via performance metrics, i.e. the PER, the distance between IEEE 802.11 network

and IEEE 802.15.4 network and the maximum throughput. In [54], the PER of IEEE 802.15.4 under WLAN interference is analyzed and evaluated via simulations. In [53] and [54], only interference from a single WLAN node is considered. The research is expanded in [55] to analyze the performance of a ZigBee link under a saturated IEEE 802.11b network. As the BER is determined by the Signal-to-interference-plus-noise Ratio (SINR), from the viewpoint of ZigBee, when a collision between Wi-Fi packets happens, the generated signal strength may be increased due to the superposition of signals, which results in stronger interference levels compared to those generated by single Wi-Fi packet transmission. The PER of the IEEE 802.15.4 network under multiple Wi-Fi interference sources is then obtained from collision time model. [56] also considered the impact of interference from Bluetooth nodes on the ZigBee performance. It showed that the impairment generated by the Bluetooth interference on ZigBee is considerably lower than that by WLAN.

The above collision time model assumes blind transmission, i.e. IEEE 802.15.4 nodes are unable to detect on-going activity from IEEE 802.11b nodes and vice versa. However, it is possible that Wi-Fi and ZigBee devices are able to detect each other's signal and apply the CSMA/CA algorithm accordingly. The analysis of coexistence performance presented in [57] and validated in [58] by experiments takes the CCA ED of the two standards into consideration. In [57], the authors consider both transmit power and timing jointly when studying the performance of IEEE 802.15.4 under IEEE 802.11b/g interference. From the power aspect, a concept of coexistence range is introduced and illustrated in Fig. 2.2.

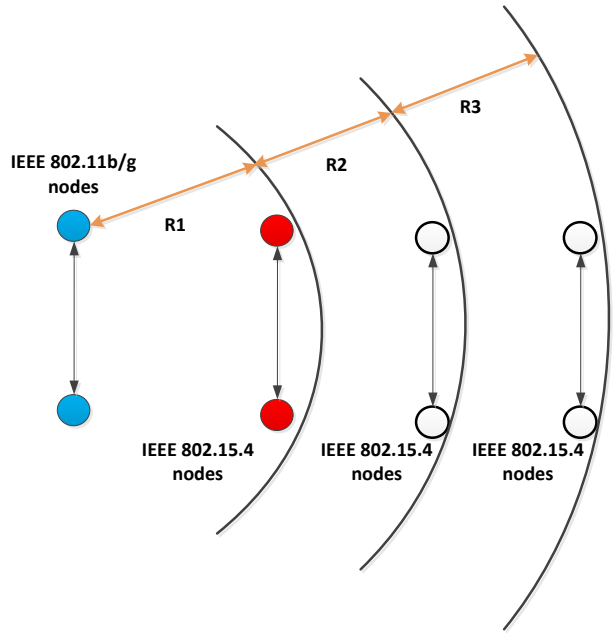

Fig.2.2 Coexistence ranges of IEEE 802.15.4 and IEEE 802.11b/g [57]

The space around a Wi-Fi node is split into 3 regions (R1, R2, and R3) defined by the distance from the Wi-Fi node. Due to different transmit powers and receiver sensitivities of IEEE 802.11b/g and IEEE 802.15.4 devices,

- Within R1, Wi-Fi and ZigBee are able to detect each other's signal.
- Within R2, only ZigBee can sense Wi-Fi packet transmission.
- Within R3, neither ZigBee nor Wi-Fi can sense the other's signal.

From the timing aspect, the research reported in [57] focuses on the coexistence range R1, where that both of their CSMA/CA algorithms work to ensure that no overlapping of transmission happens. For both Wi-Fi and ZigBee, if the channel is assessed to be idle, the device transmits the data packet immediately. Otherwise, the device delays the packet transmission for a random backoff period, and performs a CCA again. As shown in Fig.2.3, Wi-Fi and ZigBee are able to detect each other's signal and go into a backoff procedure

when another transmission is in progress. The maximum throughput of IEEE 802.15.4 under saturated IEEE 802.11b/g interference is then obtained. The analytical and simulation results show that the throughput will decrease to about 6% of the original one (250kbps).

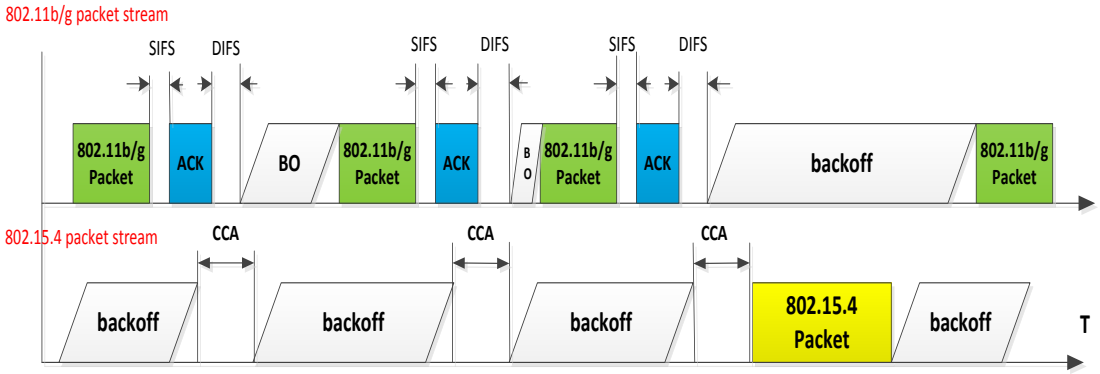

Fig.2.3 Coexistence model in timing aspect within R1 [57]

2.1.1.2 Experimental Assessments

In recent years, several experimental performance assessment studies were carried out, obtaining empirical data corresponding to certain realistic scenarios of IEEE 802.11 WLAN and ZigBee co-located deployment. Basic components of an experimental testbed include a ZigBee coordinator, a ZigBee client, and an IEEE 802.11b/g/n interferer. These nodes can be placed in different environments, with different topologies and network sizes and by running experiments and processing the collected results, the effect of Wi-Fi traffic on ZigBee network can be assessed and understood.

As the IEEE 802.11 family consists of a series of protocols having different coding, modulations and PHY layer data rates, some works ([44] [50] [51]) focused on evaluating the coexistence performance of ZigBee connections under different IEEE 802.11 PHY layer

standards (b/g/n). Table 2.1 shows some system parameters of IEEE 802.15.4 and IEEE 802.11b/g/n [48] [49]. In [50], the experimental results show that: a) Compared with 802.11g, 802.11b takes longer frame transmission time and degrades the performance of 802.15.4 in a wider range of co-channel interference but with less interference strength; b) Different modulation methods used by IEEE 802.11 compatible devices may have different impact on the performance of IEEE 802.15.4. The authors of [51] conclude that subjected to co-located wideband Wi-Fi's interference, ZigBee performs better with IEEE 802.11n than with IEEE 802.11g. One of the best ways to improve coexistence is to reduce the channel occupation time of the interference source. Thus, compared with IEEE 802.11b/g, IEEE 802.11n, which has highest data rate, can coexist better with IEEE 802.15.4 (under same Wi-Fi traffic volume).

Table 2.1 Protocol Parameters of 802.15.4 and 802.11b/g/n

IEEE Protocols	802.15.4[1]	802.11b	802.11g	802.11n
Typical Transmit Power	0dBm	20dBm	20dBm	20dBm
Bandwidth	2MHz	22MHz	22MHz	40MHz
MAX Transmit Rate	250Kbps	11Mbps	54Mbps	600Mbps[2]
Modulation	DSSS	DSSS	OFDM, DSSS	OFDM
Approximate indoor Range	20-30m	35m	38m	70m

[1] The parameters used here are based on the Micaz Mote [110], which is the mote used in our testbed.
[2] This speed is achieved by Multiple-Input-Multiple-Output (MIMO) technique.

Other experimental research works investigate the performance degradation of ZigBee under Wi-Fi interference by varying system parameters such as the central frequency offset, packet size, and distance between ZigBee and Wi-Fi nodes. These findings are very useful to guide the ZigBee deployment in order to mitigate Wi-Fi interference.

- **Packet Size:** The experimental results in [59] show that smaller ZigBee packets suffer less performance degradation than larger ones under IEEE 802.11b/g interference. On the other hand, [44] finds that increasing the WLAN packet size has a negative influence on the performance of ZigBee network. The reason is that increasing either the WSN or the WLAN packet size will generate higher collision probability between packets of the two different standards.
- **Frequency Offset:** In [60], even when ZigBee and Wi-Fi are operating in non-overlapping channels, the IEEE 802.11g device is still able to impact ZigBee's packet transmission due to the highly sensitive Energy Detection (ED) threshold of ZigBee motes. The results reported in [45] also prove that the out of band power emitted by WLAN nodes is high enough to influence the adjacent ZigBee channels deemed to be interference free. In [61], empirical analysis and experimentation are carried out to investigate what the "safe" frequency offset between IEEE 802.15.4 and IEEE 802.11b channels is, that guarantees reliable ZigBee performance.
- **Distance:** [61] claims a "safe distance" of 8m between ZigBee and WLAN. However, this conclusion is based on experiments done with IEEE 802.11b. The corresponding "safe distance" for ZigBee under IEEE 802.11 g/n remains unknown. In addition, this

"safe distance" is directly affected by the transmit power of ZigBee and WLAN nodes, and the nature of the deployment (e.g. indoors versus outdoors, building material).

- **Traffic volume:** The results obtained and reported in [62] underline the importance of *ZigBee polling window* (packet generation interval) and WLAN duty cycle in the optimization of coexistence performance. The reason is that decreasing either the ZigBee polling window or WLAN duty cycle will reduce the ZigBee or WLAN traffic load, which will result in a lower possibility of collision occurrence between the WSN packets and WLAN packets. In order to improve ZigBee's reliability, a longer polling window or a lower WLAN duty cycle is required.

2.1.2 Interference Mitigation Techniques

The research contributions on coexistence issues described in the previous section prove that ZigBee/IEEE 802.15.4 networks experience severe performance degradation when subjected to the interference generated by collocated Wi-Fi networks. Therefore, it is meaningful to design effective interference mitigation techniques, offering performance improvement.

2.1.2.1 Frequency Agility Algorithms

Frequency agility mechanisms, which avoid interference by adaptively changing the carrier frequency to a clear channel, can significantly improve the ZigBee performance in the presence of collocated WLAN. This procedure consists of two parts: **interference detection** and **channel selection**.

Interference detection requires the ZigBee nodes to identify the presence of an interfering Wi-Fi signal with a low false alarm probability. The most widely adopted approach is the Energy Detection (ED) in the Clear Channel Assessment (CCA), which is based on the RSSI (Received Signal Strength Indicator) measurement as per IEEE 802.15.4 PHY. If the value of the RSSI measurement is above a preset energy level threshold, presence of channel interference is decided [63]-[66]. In [67], an *ACK/NACK* based interference detection scheme is presented. If the number of lost ACK frames, denoted as *NACK*, exceeds a preset threshold, the ZigBee transmitter decides that communication suffers from interference. Similar approaches, using beacon frames or test frames instead of ACK frames in interference detection, are proposed in [68].

Once interference is detected by the ZigBee device, a channel selection algorithm to determine which channel is appropriate for all the nodes to change to is initiated. In [68], a new channel is selected based on a predefined pseudorandom sequence. Obviously, this pseudorandom-based interference avoidance scheme doesn't consider the state of the selected new channel and might end up in another busy channel. In [67], an energy detection scan is performed to check the status of all other channels and the channel with the lowest interference is selected. Then, the coordinator commences an active scan that broadcasts a beacon request packet to determine if the proposed mitigation channel is occupied by other ZigBee networks. If the channel is already in use, the coordinator examines the second lowest interference one. Otherwise, the new channel is selected. [64] proposes a channel selection algorithm that selects the channel which gives the maximum Signal to Interference plus Noise Ratio (SINR) to minimize the interference from Wi-Fi as

well as other IEEE 802.15.4 clusters. In order to better estimate the channel state, a capacity based channel selection algorithm is proposed in [63]. It calculates the information-theoretic capacity of each channel using RSSI sampling values. However, a ZigBee based WSN may be deployed in a large area where only some ZigBee nodes in the network are affected by the collocated Wi-Fi interference and need channel migration. For this scenario, a group formation procedure is described in [65]. During group formation, the nodes located within the same interference area form a group and select a new channel. The challenge of this approach is that nodes located at the border of the interference must operate at multiple channels.

It is obvious that switching operating channel could result in large delay, additional power consumption, and packet losses. Particularly when there are several WLAN Access Points (APs) in the vicinity, operating at different Wi-Fi channels and carrying different volumes of traffic, ZigBee WSN could experience unstable network operation because of the possible frequent channel switching.

2.1.2.2 Coexistence Mechanisms in overlapping channels

In the literature, some researchers propose mechanisms for ZigBee and Wi-Fi to coexist in overlapping channels. In [69], the packet losses of ZigBee in the presence of heavy Wi-Fi interference are classified into two types: inhibition loss and collision loss. Inhibition loss is due to channel access failure, i.e. in IEEE 802.15.4 CSMA/CA algorithm, the packet is dropped after a preset number of unsuccessful channel access attempts. [69] also claims that when ZigBee transmitter is located close to a Wi-Fi source and both Wi-Fi and ZigBee

enable CCA ED, inhibition loss is the main reason for packet loss. Then, an adaptive CCA ED threshold algorithm is presented to reduce inhibition loss by adaptively adjusting the ED thresholds. However, the empirical results in [70] show that the ZigBee network still suffers from a significant amount of collision losses due to Wi-Fi interference even when both Wi-Fi and ZigBee enable the CSMA/CA mechanism. [70] also points out that the Wi-Fi traffic contains abundant *white space* (idle channel time between Wi-Fi frame clusters), which can be utilized for more reliable ZigBee packet transmission and alleviate coexistence interference. Subsequently, it proposes a frame control mechanism, named "White Space-aware frame Adaptation (WISE)". Pareto process as one of the most widely adopted power law distribution is chosen to fit the arrival process of Wi-Fi frame clusters. Based on the results of periodical CCA ED detection applied at the ZigBee node and the Pareto model, the length of white space between Wi-Fi frames is estimated, and then the ZigBee frame size is adjusted accordingly to maximize the throughput.

In [71] and [72], certain devices that can communicate with both, the ZigBee WSN and the WLAN, are included to coordinate the medium access for packet transmission. In [71], an interference mediator coordinates the Wi-Fi and ZigBee traffic with a fairness-based TDMA (Time Division Multiple Access) scheme. As shown in Fig. 2.4, the ZigBee and Wi-Fi superframes are combined. The interference mediator estimates the combined superframe structure based on the Wi-Fi and ZigBee traffic, and sends the beacon frames to both ZigBee and Wi-Fi. Based on the combined superframe, when Wi-Fi nodes are in the Point Coordination Function (PCF) duration, placing the Wi-Fi nodes to inactivity for certain period of time, ZigBee nodes transmit, then ZigBee nodes reserve an inactive duration and

Wi-Fi nodes transmit data. In [72], a ZigBee coordinator is combined with a WLAN module. As shown in Fig.2.5, during the ZigBee beacon or Guaranteed Time Slot (GTS) based data transmission, the WLAN module reserves the channel via CTS (Clear to send)-to-itself transmission, placing a hold on the activity of Wi-Fi nodes, for the time duration indicated in CTS's frame. During that period, ZigBee nodes transmit. However, such techniques require substantial modification to the hardware.

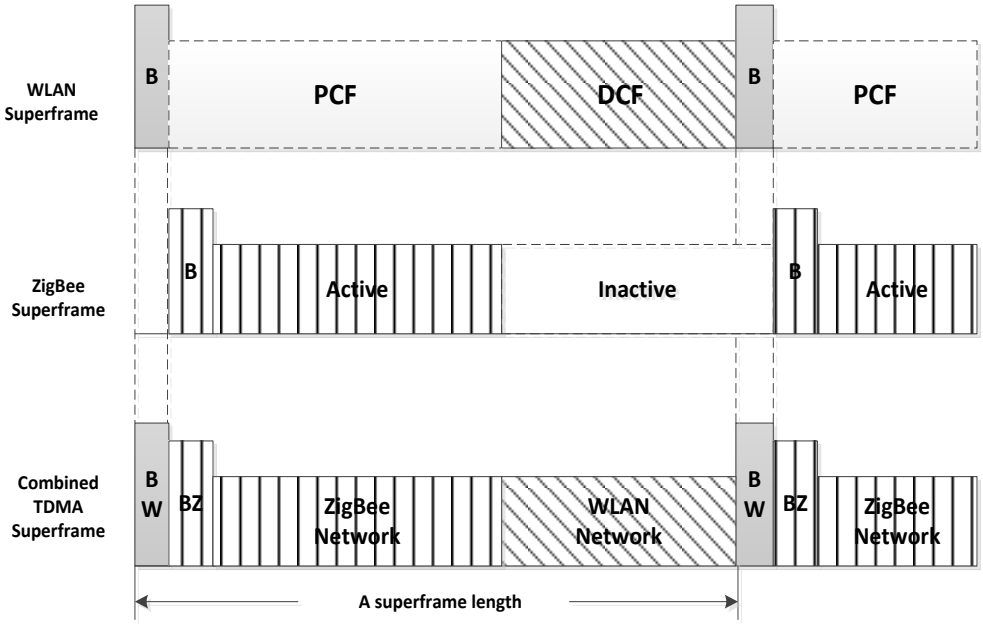

Fig.2.4 TDMA based superframe structure [71]

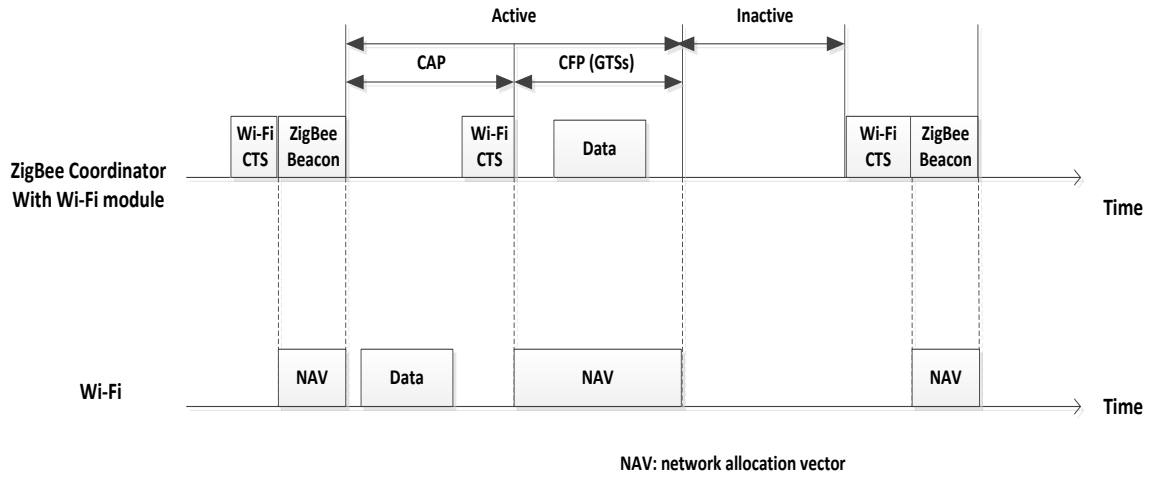

Fig.2.5 ZigBee and Wi-Fi frame exchange sequence [72]

The research of [137] investigates the coexistence issue under persistence and very heavy/saturated Wi-Fi interference. It proposes “BuzzBuzz”, which uses multiple PHY headers to provide header redundancy giving ZigBee receiver multiple opportunities to detect incoming packet. It also applies Forward Error Correction (FEC) code to correct bit errors of PHY payloads when collision happens. However, the extra headers increase the transmission overhead, and more importantly, it requires substantial modifications to the ZigBee packet structure leading to compatibility issues and extra cost for implementation. The FEC code also introduces significant coding and encoding delay to the transmission process. Our proposed APPRC, on the other hand, is more flexible and efficient, which can adjust the number of preamble padding dummy bytes and the number of packet retransmissions according to the PLR requirements and the changing external interference.

2.2 WSN Transmit Power Control Mechanisms

Energy consumption is one of the most fundamental constraints in WSN design, while data transmission is usually the most energy consuming event. Efficient transmit power control algorithm does not only significantly decrease the energy consumption due to communication, but also reduces the effect of interference and thereby maintain the network throughput. According to the adopted transmission link models, which can be divided into two categories (reliable channel model and unreliable channel model), related WSN transmit power control algorithms are discussed and summarized in the following.

2.2.1 Reliable Channel Model

Unlike wired networks that have a fixed topology, each node in a WSN can change the network's topology by adjusting the transmit power. Thus, topology control is required in WSN to decide the transmit power of sensor nodes for maintaining network connectivity and coverage [73].

There are several research contributions making use of reliable channel model to investigate the optimal transmit power for implementing topology control (e.g. [74]-[78]). The reliable channel model means two neighboring nodes are considered to be able to communicate if they are within the transmission range of each other. In [74], each sensor node maintains separate routing tables, one for each power level it could use, and applies the transmit power that minimizes the energy consumption for the entire path before every transmission. [75] presents an algorithm based on "node degree" which is defined as the number of nodes a node can communicate directly. The fundamental idea is that every

node should be monitoring regularly the number of nodes it is in direct contact, and adjusts the transmit power to let its node degree fall between the upper limit and the lower limit. Another topology control algorithm based on direction information about the location of neighboring nodes is proposed in [76]. This technique requires that each node can obtain direction information, i.e. each node is able to estimate the direction from which another node is transmitting. Then each node preserves at least one neighbor in every cone of a typical degree with the minimum power. Similar to [76], [77] presents the algorithm that each node applies minimum transmit power to retain a connection in every preset direction to guarantee global connectivity. In [78], mobile sensor node is taken into consideration. The protocol adaptively adjusts the transmit power in response to the node position changes while preserving network connectivity.

2.2.2 Unreliable Channel Model

A. Fading Channel

The above research contributions assume ideal radio propagation model, which only takes into consideration the distance between two sensor nodes. However, because of multipath fading and/or shadowing, the channel's behavior would be different. General speaking, a higher BER is expected as compared to the case of ideal radio channel, and time variability of BER is also expected to be occurring

In [79] and [80], the optimal transmit power is defined as the minimum power required to maintain the highest tolerable BER. In [79], the study shows that an optimal transmit power exists for a given data rate and a predefined maximum acceptable BER at the end of a multi-hop path. In [80], the determination of the optimal transmit power is investigated

when Maximal Ratio Combining (MRC) space diversity technique is used and the channel is experiencing fading due to shadowing. The paper concludes that the value of optimal transmit power can be significantly affected by the network condition such as the standard deviation of the lognormal shadowing distribution, the number of antennas and the node's spatial diversity.

B. Noise and Interference Channel

Because of background noise and interference power, the quality of radio communication in WSN is time variant. Meanwhile, the transmit power of sensor nodes can directly influence the quality of the received signal and the low transmit power of WSN makes this problem more serious. Thus, the optimal transmit power of WSN should be time and environment independent. In recent years, several papers appeared that are investigating adaptive transmit power control techniques that take the noise and interference power into consideration [81-88].

In [81-85], the calculated optimal transmit power is adjusted based on RSSI readings in order to maintain the required link quality measured as received signal strength at the coordinator. During the packet receiving period, the RSSI value is recorded and used as measurement of the signal strength. In [81], it is proved that the wireless link quality of body-wearable sensor devices varies rapidly because of human activity (e.g. slow walk, normal walk and rest). A dynamic power control mechanism is proposed to adjust the transmit power in order to keep the average RSSI value between the upper and lower threshold. A transmit power control MAC protocol for WSN is proposed in [82]. The basic

idea is that the receiver calculates the optimal transmit power value based on the RSSI value of the received data packet and the minimum required signal power strength, then sends back the optimal transmit power value to the transmitter. The authors of [83] proposed a feedback-based Adaptive Transmission Power Control (ATPC) algorithm for WSN to dynamically retain link's quality over time. The ATPC algorithm is divided into two phases: the initialization phase and the runtime tuning phase. In the initialization phase, each node broadcasts beacons with different transmit power levels. Each of its neighbors measures the beacon RSSI values and sends back to the node. The node then selects an optimal transmit power for each of its neighbors. In the runtime tuning phase, depending on the measured RSSI value of data packet and required link quality, a decision is made to send a notification packet from the receiver to the transmitter. The notification packet contains the difference between the desired link quality and actual measured value, which is then used to calculate the new transmit power. [84] and [85] proposed an On-demand Transmission Power Control (ODTPC) algorithm and its modified version respectively. In ODTPC, without using beacons or notification packets, the receiver inserts the RSSI value of data packet into the ACK message, and then the transmitter obtains the link quality information through data-ACK exchanges. Based on the measured RSSI, the transmitter adjusts the optimal power to satisfy the required RSSI value defined as an upper threshold level and a lower threshold level. However, there might be more than one power levels that can satisfy the required RSSI value. ODTPC stops once a power level that meets the RSSI conditions is found, while the modified ODTPC [85] is developed to further search for the minimal one.

However, the RSSI value is an average of signal strength over a short time period (128us in Micaz motes), while the packet may take a much longer time (e.g. 2ms) to be received. Also, the value of RSSI reading may be based on the superimposed transmitted signal from the ZigBee device, background noise and interference. And if the overlapping of the ZigBee packet with an interfering Wi-Fi frame occurs at the PHY header of the ZigBee packet, the ZigBee receiver may not be able to identify the packet. Thus, the above mentioned algorithms that are based solely on RSSI values of received packets are not able to accurately provide the channel's condition when subjected to interference. In [86-88], other approaches for adaptively adjusting the optimal transmit power are proposed.

In [86], the impact of different transmit powers on link quality is investigated and a transmission Power Control Mechanism with Blacklisting (PCBL) scheme is proposed. In PCBL, each node transmits *N* packets at every transmit power level in the initial phase to calculate the corresponding PER. Compared with the PER threshold, the minimum transmit power is selected as the optimal transmit power. However, it doesn't adaptively adjust the optimal transmit power during the running time, and is consequently not robust to time varying external interference.

[87] describes two power control mechanisms: Multiplicative-Increase Additive-Decrease Power Control (MIAD PC) and Power Control based on the Estimation of the Packet Error Rate (PER PC). MIAD PC is implemented using the actual successful or failed packet delivery events. The transmit power is increased (exponentially) if a packet is delivered successfully and decreased (linearly) if a packet is lost. However, frequent randomly occurring collisions may force the ZigBee mote to frequently adjust the transmit power, which may lead to

unstable operation. In PER PC and in a similar method presented in [88], when there is no ZigBee transmission, the ZigBee mote periodically measures the RSSI value of the link to determine the noise and/or interference intensity. [88] derives the optimal power to guarantee the received signal strength must be higher than the measured noise and/or interference by a certain value. In PER PC, the RSSI sampling values of noise and/or interference are used jointly with the channel model considered to be the one describing more accurately the actual channel's behavior (e.g. AWGN model or Rayleigh model) to determine the SINR and obtain the optimal transmit power. However, as the interference level may be changing over time, the accuracy of the RSSI sampling mechanism in measuring the interference level needs to be further validated. Also, these algorithms are too complicated and hard to implement at the resource limited ZigBee motes.

Thus, it is necessary to develop a simple but efficient adaptive power control mechanism that can make full use of the configurable transmit power provided by the sensor node to dynamically and rapidly select the optimal transmit power based on the intensity of external Wi-Fi interference.

2.3 Study of IEEE 802.15.4 CSMA/CA Mechanism

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is a contention based network multiple access method which has been widely adopted in wireless technologies (e.g. IEEE 802.11, Apple's LocalTalk, and IEEE 802.15.4). A device using CSMA/CA only attempts to transmit data when the channel is sensed to be idle, otherwise a backoff period

is assigned [89]. A typical example is the IEEE 802.11 DCF, which employs a CSMA/CA mechanism with binary exponential backoff algorithm [90].

Compared with DCF in IEEE 802.11, IEEE 802.15.4 CSMA/CA incorporates some energy conserving features such as discontinuous channel sensing at the end of the backoffs and no freezing the countdown of the backoff counter when the channel is busy [91]. Depending on network configuration, two types of CSMA/CA mechanisms are defined in the IEEE 802.15.4 standard[3]. For non-beacon-enabled WSN, an unslotted CSMA/CA channel access mechanism is used, while for beacon-enabled WSN, a slotted CSMA/CA channel access mechanism is employed [29].

In the following subsections, a comprehensive review of recent researches on IEEE 802.15.4 slotted and unslotted CSMA/CA mechanisms will be given.

2.3.1 Performance study of IEEE 802.15.4 CSMA/CA

Recently, with the wide utilization and expansion of IEEE 802.15.4 as a promising WSN technology, a lot of researches were carried out to investigate the performance of IEEE 802.15.4 CSMA/CA mechanism.

A. Slotted CSMA/CA

Most theoretical models analyze the performance characteristics of slotted CSMA/CA for IEEE 802.15.4. In [92], the performance of IEEE 802.15.4 CSMA/CA protocol in terms of throughput and energy consumption is analyzed under different traffic conditions using a deterministic Petri-Net model, which is a mathematical technique that can describe state

[3] The details of IEEE 802.15.4 CSMA/CA mechanism will be introduced in Chapter 5.

changes in a system with transitions. [91], [93]-[96] use Markov chain to analyze the slotted CSMA/CA technique as specified in IEEE 802.15.4. The authors of [91] developed a new analytical model of slotted CSMA/CA using a simple one-dimensional Markov chain to investigate the normalized network throughput in both the saturated and periodic traffic scenarios. In case of acknowledged uplink transmission, a detailed analytical model using a two-dimension Markov chain is derived to study the energy and throughout behavior of IEEE 802.15.4 network in [93]. In order to further reduce the number of Markov states and improve the scalability of the analytical model, [94] presents an analytical model consisting of two two-dimensional Markov chains, which is used to study the impact of the number of contending devices and data frame size on the network throughput and energy efficiency under saturated traffic. The authors of [95] further developed a Markov chain model which considers more characteristics of IEEE 802.15.4 slotted CSMA/CA, such as the superframe structure, acknowledgement and the maximum number of allowed retransmission attempts. In [96], Markov chain and the theory of M/G/1/K queues are combined to evaluate the delay performance of slotted CSMA/CA process. The impact of packet size, packet arrival rate, node's buffer size and the number of nodes are investigated.

B. Unslotted CSMA/CA

Some researchers devoted their attention to the unslotted CSMA/CA mechanism [97-100]. In unslotted CSMA/CA, the start of backoff and packet transmission is not aligned with some slot boundary. Therefore, the authors of [97] proposed a new stochastic model that is using the busy cycle of M/G/1 queuing system to calculate the performance parameters of unslotted CSMA/CA such as packet delay, energy consumption and packet loss probability.

The research work reported in [97] assumes that packet collisions occur occasionally. The authors of [98] point out that packet collision happens frequently when the traffic load of the WSN is high and developed a more accurate model to calculate the packet loss rate and latency. All these research contributions consider asynchronous network traffic, which means all nodes start the CSMA/CA process when the packet is generated. In [99], synchronized traffic is assumed; nodes start the backoff algorithm after receiving the query sent from the coordinator. This work investigates the impact of different network loads (i.e. packet size and the number of nodes) on the probability that a node succeeds in the access to the channel on each time slot. In [100], two independent Markov chains for the node states and the channel states are intergraded to analyze the slotted CSMA/CA process. Compared with previous slotted CSMA/CA models, this one allows any channel activities, including random backoff, CCA and packet transmission start at any time instead of the beginning of time slots, thus it can also be used to analyze the performance of unslotted CSMA/CA process.

However, the above studies only use computer simulations to verify their mathematical models, which may ignore the realities of hardware limitation. Although in [101], analysis, simulation and hardware implementation are used to investigate the maximum throughput of the unslotted ZigBee network, this work still assumes sufficient buffer space and doesn't consider the effect of interference from other networks (e.g. WLAN) on the performance of CSMA/CA algorithm.

2.3.2 IEEE 802.15.4 CSMA/CA Parameter Adjustment Mechanisms

Several research contributions appeared recently, proposing technologies targeting the improvement of IEEE 802.15.4 CSMA/CA's performance. In [102-104], the authors propose new techniques to enhance the slotted CSMA/CA mechanism in order to support different Quality of Service (QoS) requirements. As shown in Fig.2.6, two types of traffics are defined and named as high priority (HP) traffic and low priority (LP) traffic. Instead of having the same CSMA/CA parameters for both traffic types, shorter backoff delay (*macMinBE, aMaxBE*) and lower Contention Window (CW) size are applied to HP traffic to reduce the CSMA/CA delay. In addition, priority queue is used to reduce the queuing delays of HP traffic [102].

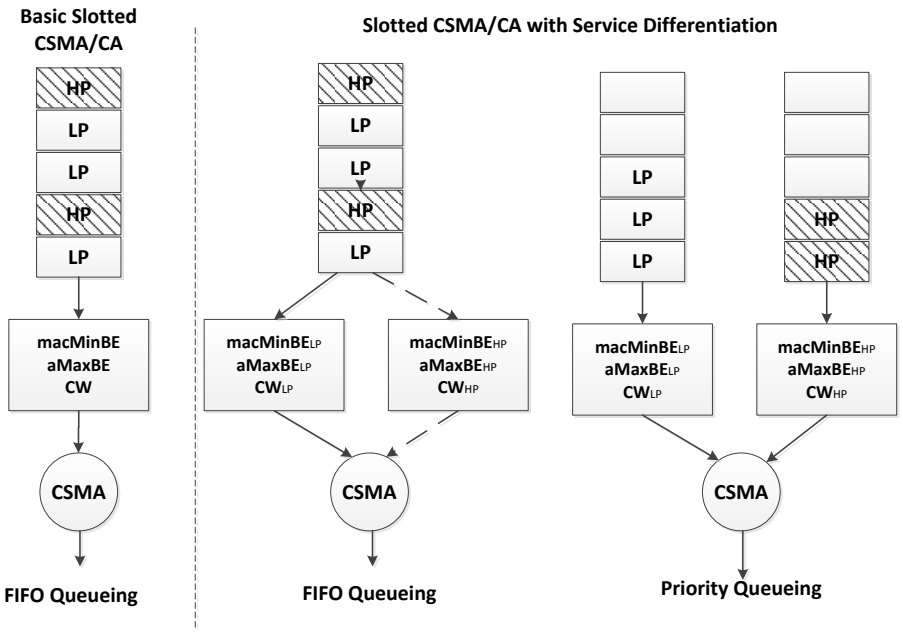

Fig.2.6 Differentiated service strategy [102]

For the same purpose of providing QoS differentiation in terms of data latency and transmission reliability to different traffic classes in wireless sensor networks, two

strategies, the Latency Differentiation Scheme (LDS) and Reliability Differentiation Scheme (RDS), are proposed in [103]. In LDS, smaller backoff windows of CSMA/CA algorithm are assigned to the traffic class with higher priority. In RDS, the maximum number of backoffs in one transmission attempt and the maximum allowed transmission attempts before the packet is dropped are derived according to the traffic classes that have different QoS requirements. The authors of [104] developed a priority-based traffic differentiation scheme as well, which adjusts the contention window size and backoff exponent value according to each service class, and a mathematical model that is based on discrete Markov chain is presented to evaluate the performance of the proposed scheme.

The IEEE 802.15.4 CSMA/CA uses a binary exponential backoff algorithm to determine the backoff time when the CCA detection shows the channel is busy. As discussed in [105], this backoff algorithm may produce a long backoff period, which causes ineffective channel utilization. Thus, a new Delayed Backoff Algorithm (DBA) is proposed in [105] to correct this. In DBA, different initial backoff times are assigned to each sensor node by the coordinator and after the initial backoff the sensor nodes continuously perform CCA detection until the channel is idle. The authors of [106] conclude that the backoff algorithm should take the network size into consideration. The proposed algorithm determines the CSMA/CA parameters based on the average backoff times of all the nodes in the WSN. In the default CSMA/CA algorithm and the previous two modified ones, the backoff time is decided by the coordinator or randomly selected. In [107], the authors take the CCA outcomes into consideration, and propose two techniques to improve the energy efficiency and performance robustness of IEEE 802.15.4 CSMA/CA: a) Enhanced Collision Resolution

Mechanism (ECRM) and b) Enhanced Backoff Mechanism (EBM). ECRM better reflects the overall network contention by adjusting the value of Binary Exponential (BE) based on the results of consecutive CCA detections, i.e. Increase the BE after a preset number of consecutive CCA busy results, and decrease the BE after a successful transmission. EBM shifts the range of backoff counters to avoid additional backoffs and CCAs when there is ongoing transmission. With the average packet length of a network, EBM introduced an expected waiting time for the ongoing transmission and increases the backoff counter by this amount of time after a CCA busy result. The authors in [108] also point out that the default/fixed CSMA/CA parameters defined in the standard suffer from severe inefficiency and unreliability problems due to the time varying network conditions. They proposed an Adaptive Access Parameters Tuning (ADAPT) algorithm for dynamically adjusting the CSMA/CA parameters based on the packet loss rate requirement specified by the application.

The above papers investigate the performance of IEEE 802.15.4 CSMA/CA mechanism and present several performance improvement techniques. However, they all assume a sufficient transceiver buffer size. In reality, the delay introduced by the CSMA/CA may cause the transceiver buffer overflow, especially when the ZigBee mote works at high data rate and coexists with other interfering networks. Thus, it is necessary to design a delay control mechanism to address the buffer overflow issue.

Chapter 3

ACK with Interference Detection Technique

ZigBee is a low-cost, low-power, wireless mesh networking standard, operating at the 2.4 GHz band (2400–2483.5 MHz), known worldwide as Industrial, Scientific and Medical (ISM) unlicensed band. However, the 2.4 GHz band is heavily used by many other wireless products, most prominent of which are IEEE 802.11b/g/n wireless local area networks (WLAN) and Bluetooth Wireless Personal Area Networks (WPAN). Recent studies have shown that the low-power ZigBee based wireless sensor networks are vulnerable to the interference generated by the nodes of Wi-Fi wireless local area networks.

As was discussed in Chapter 2, there are quite a few performance improvement schemes proposed recently in the open literature, which address the interference problem between WLAN and ZigBee/802.15.4. These techniques focus on reducing the loss rate of data packets. However, it is quite likely that a transmitted ACK packet experiences the same or similar interference problems as those damaging regular data packets, causing ACK packet loss. It is noticed from the statistical analysis of the collected experimental data that there

are many ACK packet losses in the ZigBee packet transmission process, resulting in an excessive number of unnecessary packet retransmissions and subsequently a waste of bandwidth and energy.

Motivated by this observation, in this chapter, a novel ACK with Interference Detection (ACK-ID) technique that can effectively reduce the ACK losses and subsequently the packet retransmissions is proposed and implemented in the Crossbow MICAz motes of our testbed. Extensive performance evaluation experiments have been carried out and the results show that the proposed ACK-ID can significantly improve the performance of ZigBee systems in terms of ACK delivery rate, thereby reducing the packet retransmission rate when operating in close proximity with an IEEE 802.11g WLAN.

In section 3.1, a detailed description of our testbed is provided. Section 3.2 elaborates our novel ACK-ID scheme, whose experimental performance evaluation results are presented and discussed in Section 3.3.

3.1 Testbed Description

Our experimental setup is performed in an indoor lab environment, using of-the-shelf computing and communication devices. The proposed protocols and algorithms were implemented in nodes of the testbed and extensive experiments were carried out to help us assess and understand behavior as well as determine performance under specific conditions. As shown in Fig 3.1, the experimental network is formed by ZigBee motes and Wi-Fi nodes.

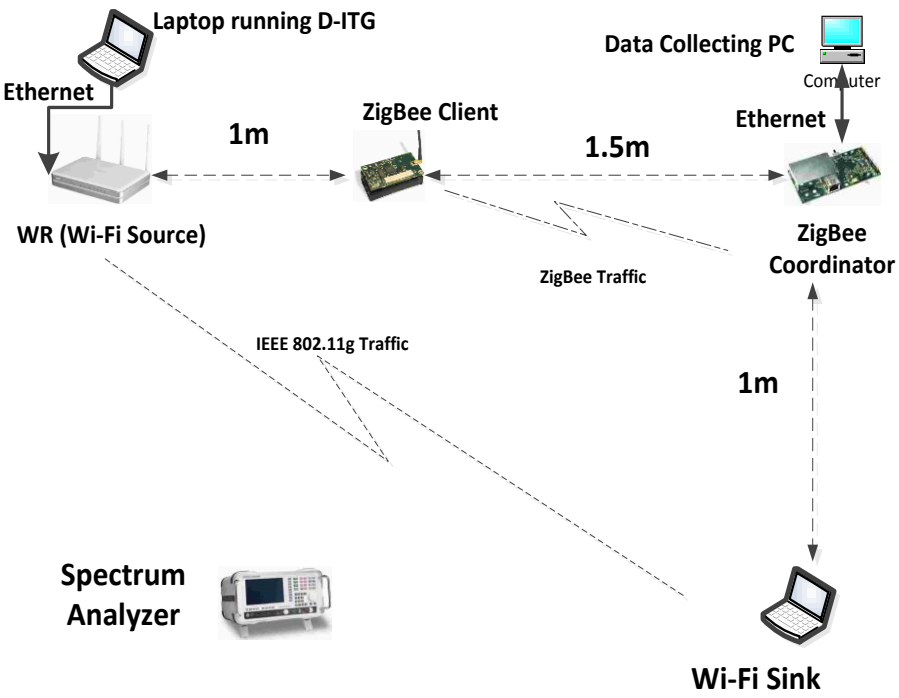

Fig. 3.1 Testbed's Topology

The WLAN consists of an IEEE 802.11 b/g/n Wireless Router (WR) (ASUS RT-N16), a Dell Inspiron 1545 laptop with Dell Wireless 1515 (IEEE 802.11 a/g/n) WLAN half mini-Card (Atheros) installed, and a Toshiba Satellite 2450 laptop connected to one of the Ethernet ports of the WR. In our experiments, it was found that the traffic sent by the wireless router can be set to transmit at a very stable power level. Thus the WR is used in our testbed as Wi-Fi traffic source/transmitter. The Toshiba laptop runs the Distributed Internet Traffic Generator (D-ITG) [109] and generates traffic with different UDP segment payload size, segment rate and inter-departure time (IDT) distribution, which is then "fed" into the WR for generating various interfering 802.11g Wi-Fi traffic that is having the laptop as destination node. It should also be noted that the transmit power of the WR can be set to

different levels, thus enabling control on the interference strength applied to the ZigBee packet transmissions.

One Crossbow MICAz [110] mote equipped with 802.15.4-compliant CC2420 [111] transceiver is used as ZigBee client, transmitting 802.15.4 traffic with different packet sizes, packet generation rates and IDT distributions to the ZigBee coordinator. Another MICAz mote, installed on a Crossbow MIB600 [112] programming board, is functioning as coordinator, receiving data from the client. A PC is connected to the MIB600 board, collecting the received data from the ZigBee coordinator. Custom ZigBee client and coordinator software programs were developed and run on the MICAz motes. The client software allows controlling the packet size, generation rate and IDT distribution. The coordinator software collects the received data packets and performs statistics processing tasks such as calculating the number of received packets, cancellation packets, and so on.

A spectrum analyzer, Aeroflex 3252 with a monitoring frequency range from 1 kHz to 8 GHz and a sweeping time of 10ms, is used to monitor the Wi-Fi and ZigBee channels, and display power spectral density [113]. By scanning all the Wi-Fi channels, we determine that ZigBee channel 20 (2.449-2.451GHz) is not “contaminated” by interference from any other Wi-Fi APs in the building. To minimize the interference from other coexisting WLANs, ZigBee channel 20 is used as our ZigBee operating channel. In addition, since ZigBee channel 20 is located within the range of Wi-Fi’s channel 9 (2.441-2.463GHz) where the power spectral density is the strongest, Wi-Fi channel 9 is used with the WR of our testbed to investigate the ZigBee packet transmission performance in the worst case scenario. Also, the nodes

have been arranged in such manner that both, the ZigBee node-pair's connection and the Wi-Fi node-pair's connection path are unobstructed, thus forming line of sight channels.

In the following sections, the used software and hardware, and the important experimental parameters placed in the ZigBee and Wi-Fi nodes will be discussed.

3.1.1 Wi-Fi Link

The Wi-Fi link of our testbed is composed of a Toshiba laptop running D-ITG, an IEEE802.11 b/g/n WR, and a Dell laptop used as Wi-Fi receiver/sink.

A. Laptop running D-ITG: A Toshiba laptop with Ubuntu operating system is used to run D-ITG to generate UDP traffic and send the traffic flow to the wireless router via Ethernet connection.

D-ITG is a platform able to implement a lot of probability distributions, including constant, Poisson, Uniform, Pareto, Cauchy, Normal, Exponential, and so on, to profile the Inter Departure Time (IDT) between packets and the Packet Size (PS) random variables of generated traffic. It also can emulate various protocols: TCP, UDP, ICMP, DNS, etc. In our testbed, UDP traffic with different probability distributions for both IDT and PS are used. The D-ITG platform consists of three components: ITGSend, ITGRecv and ITGLog. ITGSend is the sender component and able to generate multiple traffic flows. ITGRecv is responsible for managing the communication with the sender. ITGLog is running as a log server to receive and store log information from multiple connections [109]. On the Toshiba laptop, ITGSend is running to generate traffic that has the Wi-Fi receiver as destination node.

B. IEEE802.11 b/g/n WR: The traffic flow generated from the Toshiba laptop running D-ITG is passed to the IEEE802.11 b/g/n WR and then converted to Wi-Fi traffic that is having the Dell laptop as receiver. **DD-WRT** [114], a Linux based open source firmware widely used for wireless routers and embedded systems, is installed in our WR. DD-WRT supports a great number of functionalities, such as radio transmit power control, dynamic DNS, advanced quality of service, virtual private network access, and so on. By accessing the DD-WRT Web-GUI via a Firefox web browser on the Toshiba laptop, the Wi-Fi communication parameters in our testbed are listed in Table 3.1.

Table 3.1 Wi-Fi communication parameters

Standard:	IEEE 802.11g
Channel:	channel 9 (2.441-2.463GHz)
Data Rate:	54Mbps
Modulation:	ERP-OFDM
Transmit Power:	50mW (Adjustable)
CCA sensitivity:	-75dbm

C. Wi-Fi sink: The D-ITG ITGRecv component is running on the Dell laptop for receiving Wi-Fi traffic. **Wireshark** [115] is also used on this laptop to capture Wi-Fi frames in order to analyze and validate their encapsulation. Wireshark [115] is a free, open source and cross-platform packet analyzer that can display the fields and their meanings of different packets specified by different types of network protocols, such as Ethernet,

PPP (Point to Point Protocol) and IEEE 802.11. Defined in the standard [116], the Wi-Fi packet structure is shown in Fig. 3.2.

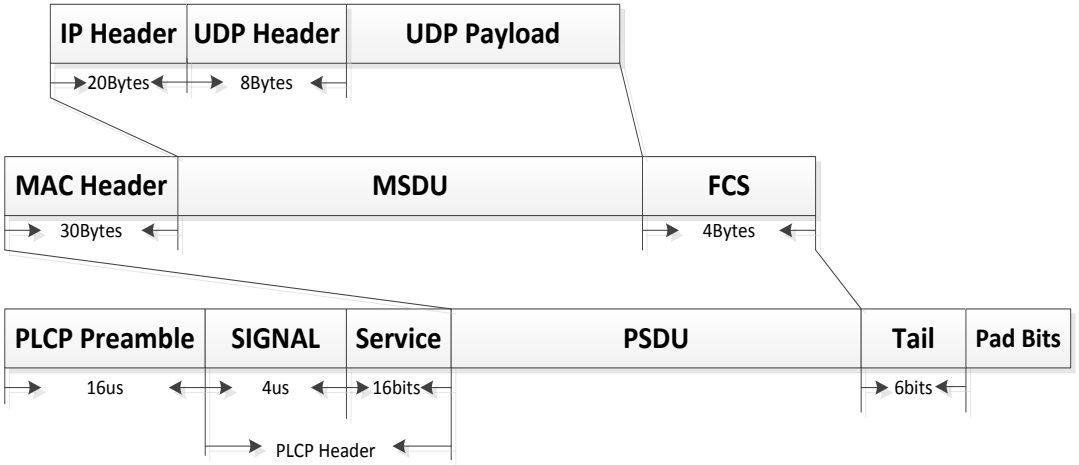

Fig. 3.2 Wi-Fi packet structure [116]

As shown in Fig. 3.2, the UDP segment payload, UDP and IP layer headers, and Frame Check Sequence (FCS) footer combined together construct the 802.11g MAC Protocol Data Unit (MPDU). The MPDU is then passed to PHY and serviced as PHY Service Data Unit (PSDU). In our testbed, ERP-OFDM modulation is applied. Thus, the format for the PHY packet includes the PHY Layer Convergence Protocol (PLCP) preamble, PLCP header, PSDU, tail bits and pad bits[4]. The PLCP preamble takes a fix amount of time; 16μs. The PLCP header is made up of 40bits. The first 24bits are transmitted at 6Mbps and take 4μs. The last 16bits plus PSDU, tail and pad bits are sent at data rate, which is 54Mbps in our testbed [116]. Also, a supplementary time of 6μs, called signal extension is added to the end of each packet transmission. After a *SIFS* (Short Inter Frame Space) interval of

[4] Tail bits are used to unwind the convolution code. Pad bits are used to make data field a multiple of OFDM symbols.

10µs, if the Wi-Fi packet is successfully delivered to the Wi-Fi receiver, a ACK packet containing 14 bytes of PSDU is sent back to the WLAN transmitter [116] [117].

3.1.2 ZigBee Link

The ZigBee connection is composed of a MICAz mote acting as ZigBee client and another MICAz mote functioning as ZigBee coordinator. The ZigBee coordinator is then mounted on a MIB600 programming board that is wired to a PC for collecting and analyzing the received data.

A. MICAZ mote: The major components of the Micaz mote include an **ATmega128L microcontroller** [118] and a **Chipcon CC2420 RF transceiver** [111].

The ATmega128L is a low power microcontroller with 128Kb of program flash memory, 512Kb of serial flash memory, and 4kb of configuration EEPROM. It supports **Moteworks** [119] wireless sensor network platform for reliable ad-hoc mesh networking. Moteworks is based on TinyOS [120], which is a component-based and event driven operating system designed by University of California, Berkeley for low power devices with small memory requirement. Moteworks provides reliable, industry leading mesh network, over the air programming capabilities, server middleware for enterprise network integration, and client monitoring and management tools for analysis and configuration [110]. MoteWorks also offers a series of software development tools for custom mote applications including custom sensor board drivers and sensor signal conditioning and processing handlers. An optimized cross-compiler and an advanced editor for TinyOS application development are also included [119].

The CC2420 is an IEEE 802.15.4 compliant RF transceiver that includes a DSSS baseband modem with a 9dB spreading gain and a 250kbps data rate. It provides extensive hardware support for packet handling, RX/TX data buffering, burst transmissions, data encryption and authentication, CCA, and RSSI/Energy detection. The structures of data packet and ACK packet defined in CC2420 datasheet are illustrated in Fig. 3.3 and Fig 3.4 respectively [111].

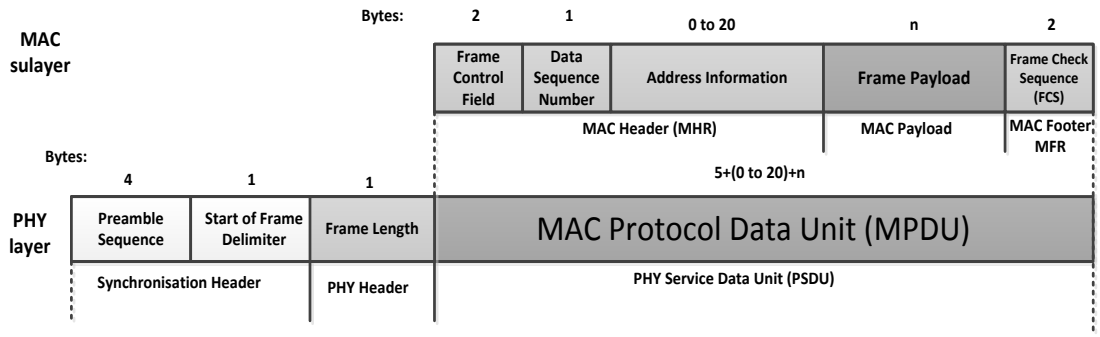

Fig. 3.3 CC2420 data packet format [111]

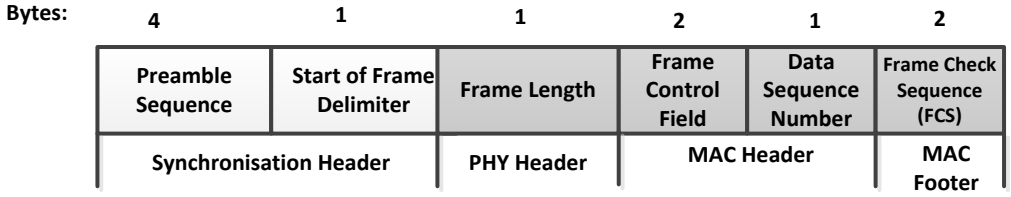

Fig. 3.4 CC2420 ACK packet format [111]

In our testbed, both client and coordinator software run on MICAz motes and read the RSSI value for monitoring the external interference or noise level. In addition, the ED threshold and transmit power of the motes can be adjusted as needed. CCA is performed before the transmission of each packet in order to decide whether the medium is idle or not. The default CCA mode of the CC2420 of MICAz adopts both

carrier sense and energy detection (CS-ED) with set threshold -77 dBm. It should be noted that since there is only one Wi-Fi and one ZigBee connection in our testbed, 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 has been tested.

Some other important ZigBee communication parameters set by CC2420 transceiver are listed in Table 3.2.

Table 3.2 ZigBee communication parameters set by CC2420

Data Rate:	250Kbps
Channel:	channel 20 (2.449-2.451GHz)
Transmit Power:	1mW (Adjustable)
TX/RX FIFO data buffer:	128Bytes
Symbol period:	16μs (using Offset-Quadrature Phase Shift Keying (O-QPSK))
RSSI:	Average over 8 symbol periods

B. MIB600 and PC for data collecting: The MIB600 programming board is used as an Ethernet gateway to relay data from ZigBee network to our desktop computer. It is also used to install custom Moteworks applications into our MICAz motes.

On the PC for data collecting, the Moteworks suite and the Programmer's notepad as a simple IDE for code compilation and debugging are installed. In addition, client tools,

XServe and *MoteView*, are running to display the data from ZigBee network for recording and analysis.

3.2 ACK-ID Technique Description

In this study, the MAC layer of ZigBee implements the functionalities of acknowledgement and retransmission. For convenience of terminology, in the following text, the term “packet” will refer to the PHY layer data unit while the term “frame” to the MAC layer data unit. The MAC layer frame is passed to the PHY layer as the PHY Service Data Unit (PSDU). The PSDU is prefixed with a synchronization header (SHR) and a PHY header (PHR), forming the PHY packet. After each data packet transmission, the source mote waits for receiving ACK packet from the coordinator. A correctly received data frame triggers the generation and transmission of an ACK frame at the receiving mote, in our case the coordinator, containing the same Data Sequence Number (DSN) of the data frame it is acknowledging. The transmitting mote waits a period of time, denoted as *macAckWaitDuration*, for the corresponding ACK to be received. If the ACK with the correct DSN is received within this time period, the transmission is considered successful and no retransmission is needed. If it is not received, the transmitting mote concludes that this transmission attempt has failed. Defining the maximum number of retries allowed for a MAC layer frame as *macMaxFrameRetries*, the mote shall then repeat the process of transmitting the data frame and waiting for the ACK up to *macMaxFrameRetries* times. If none of these attempts succeeds, the transmitter then determines that the transmission of the frame has failed and

drops the frame from the transceiver buffer in order to store a new frame and attempt its transmission.

Due to the poor quality of the wireless radio channel contaminated with noise and interference, a transmitted packet is not always successfully received by its intended destination. Packet loss due to the following three circumstances has been identified and investigated in our experiments:

A. **Packet cancellations due to CCA detection failures**. A ZigBee client mote senses the availability of the channel using CCA 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. After reaching the maximum number of allowed backoffs (*macMaxCSMABackoffs*), the packet is dropped.
B. **Packet losses due to collisions with interfering Wi-Fi traffic**. Due to its low transmission speed (250kbps), a ZigBee packet has considerable longer transmission time compared to that of a Wi-Fi packet sent at high speed (e.g. 54Mbps for IEEE 802.11g) Thus, while a ZigBee packet is in transmission, it is possible a Wi-Fi node would start transmitting before ZigBee packet's transmission is complete. Because of this overlapping, the ZigBee packet transmission attempt may fail.
C. **Packet drops due to CC2420 Transmit First In First Out Byte Register (TXFIFO) overflow**. In CC2420 there is a 128-byte transmission buffer (TXFIFO), capable of storing only the frame that is in transmission process. In our experiments, the ZigBee transmitting mote generates packets at constant intervals as in periodic monitoring applications. However, the time for completing a packet transmission might include the time for packet

transmission and re-transmission, waiting for ACK, CCA detections and a number of backoffs. If this time duration exceeds the packet generation interval, the newly generated frame will be dropped since the transmission of the previous one is still in process and occupying the TXFIFO.

In the following analysis and corresponding experiments, without loss of generality and for simplifying the analysis of packet transmission, *macMaxFrameRetries* is set to 1 in ZigBee client's software program. If no ACK packet is received within a set time frame (*macAckWaitDuration*), the source mote concludes the data packet is lost and re-transmits the data packet once. Firmware programs of both transmitting mote and coordinator are modified to include the capability of recording relevant data. Several parameters are measured in the experiments:

1. *SntACK*: the total number of ACK packets the coordinator sent out for the duration of the experiment.
2. *RecdACK*: the number of ACK packets the transmitting mote received with the first transmission.
3. *RtxPkt:* the total number of retransmitted data packets sent out by the transmitting mote.
4. *DupPkt:* the number of retransmitted data packets the coordinator received even though already having already received them. They are the duplicate ones the coordinator received, and will be discarded immediately upon reception. This happens because the ACK sent from Rx to Tx was lost.
5. *CCAPktDrop:* the number of aborted data packets due to CCA detection failures.

6. *OvfPktDrop*: the number of data packets dropped due to the TXFIFO overflow (preceding packet hasn't been "cleared" or dropped, it is still in TXFIFO buffer).
7. *PktLoss*: the total number of lost packets due to CCA dropping, overflow and collision with Wi-Fi interference.

Periodic monitoring applications, where the ZigBee client mote generates data traffic with constant packet rate and packet length, are considered. In the experiments, the ZigBee transmitting mote generates constant traffic with packet size of 100 bytes/packet and packet rate of 50 packets/second. The total number of ZigBee packets for transmission is set to 10,000 for each experiment. The interfering UDP traffic is generated by the D-ITG running on the PC. In the following text, we use the term "segment" when referring to the UDP data unit. The UDP traffic is generated with constant segment payload size of 1400 bytes, constant IDT and rate of 500 segments/second. The collected experimental results of the parameters introduced above for analyzing ZigBee's packet transmission process are summarized in the table below:

Table 3.3 Experimental Results for ZigBee packet transmission

Experiment Number	1	2	3
total number of packet	10000	10000	10000
SntACK	9780	9781	9760
RecdACK	5962	6088	5736
RtxNum	3904	3785	4133
DupPkt	2645	2502	2718
CCAPktDrop	7	4	4
OvfPktDrop	126	122	126
PktLoss	220	219	240

An important observation is that a substantial portion of data packets were re-transmitted (~39%). Furthermore, the re-transmitted packets may be useless. The useless packet retransmission happens when the original packet was successfully received by the coordinator but their corresponding ACK packet was lost during the transmission to the transmitting mote. If the retransmission succeeds, the receiver gets a duplicate packet. The experimental results reveal that the amount of the duplicate packets is quite significant (~26%), which wastes not only a significant portion of free channel time but also consumes energy unnecessarily. Therefore, it is meaningful to pursue the design of certain technique that reduces the number of lost ACK packets.

The statistical analysis of our experimental results showed that a significant portion of packet retransmissions is due to the loss of ACK packets under Wi-Fi interference. This has negative impact on the performance of ZigBee WSN. The unnecessary retransmissions increase the energy consumption as well as traffic volume in the wireless medium, which increases the delays and the collision rate packets experience.

According to the IEEE 802.15.4 standard [29], the CCA mechanism and CSMA/CA algorithm are not used for the transmission of ACK frames. ACK is sent out immediately regardless of the channel's status at that time. In this contribution we introduce a new technique we named ACK with Interference Detection (ACK-ID) that improves the performance of ZigBee packet transmission when there is varying interference in the wireless medium due to the presence of a collocated active WLAN.

In ACK-ID, a novel interference detection process is performed before the transmission of each ZigBee ACK packet in order to decide whether the channel is experiencing interference or not. After successfully receiving a ZigBee packet, the ZigBee receiving node reads the RSSI value continuously at a very short time interval of t_s (e.g. a symbol duration of 16μs, which is also the RSSI value update frequency used in CC2420 [111]). The ACK packet transmission starts once N (e.g. 2) successive RSSI readings are below the ED threshold P_{th}. However, if after N_{max} (e.g. 20; also $N_{max} > N$) successive RSSI readings, there has not been N successive RSSI readings below P_{th}, the ACK is sent out right after this has been confirmed by the acknowledging mote. The ACK-ID process is illustrated in Fig.3.5. Use of the ED option for interference detection improves the successful ACK delivery. Since the IEEE 802.15.4 ACK packet is very short (11 bytes), it has very good successful delivery rate if its transmission starts when the channel is detected to be idle.

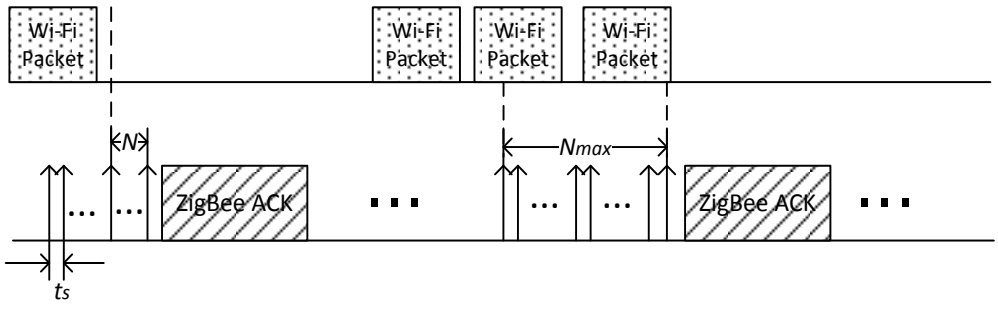

Fig. 3.5 The ACK-ID process

It is evident that the introduced technique allows delaying the transmission of ACK after the data frame has been received correctly in contrast with the standard's recommendation. This needs to be taken into consideration when setting the mote's waiting time for receiving ACKs. Therefore, the maximum duration to wait for an ACK frame to arrive

following a transmitted data frame (*macAckWaitDuration*) should be increased accordingly. Denoting with *maxACK-IDTime* the waiting time spent for the N_{max} RSSI readings, the required extended waiting time *macAckWaitDuration* can be obtained as:

$$\textbf{\textit{macAckWaitDuration}} = aUnitbackoffPeriod + aTurnaroundTime + phyACKDuration + maxACK\text{-}IDTime,$$

where *aUnitbackoffPeriod* is the basic time period (20-symbol duration) used by the CSMA/CA algorithm (*aUnitbackoffPeriod* is used to calculate the *macAckWaitDuration* only when slotted CSMA/CA is applied.); *aTurnaroundTime* has a 12-symbol duration and is the receive-to-transmit (RX-to-TX) or TX-to-RX maximum turnaround time; and *phyACKDuration* has a 22-symbol duration and corresponds to the combined duration of the SHR, PHR and PSDU octets of the ACK packet.

Since the maximum IEEE 802.11g MAC sub-layer protocol data unit (MPDU) size is 2346 bytes, the channel occupation time for the Wi-Fi packet will not exceed 0.4ms. In our experiments, the interfering Wi-Fi traffic has MPDU sizes of no more than 1500 bytes (Ethernet Maximum Transmission Unit (MTU)) which corresponds to channel occupation time of less than 0.3ms when the transmission speed is 54Mbps. Therefore, the proposed ACK-ID adopts ts = 16μs and N_{max} = 20 so that the *maxACK-IDTime* is around 0.32ms, which will enable the coordinator to largely avoid collisions between the ACK packets it sends out and the interfering 802.11g Wi-Fi packets. It is noted that most of the time, ACK could be sent out before reaching N_{max} RSSI readings. Such interference detection process introduces only very small additional delay.

3.3 Performance Evaluation Results and Discussion

In order to validate the performance of the proposed ACK-ID mechanism, we performed an extensive set of experiments using the testbed shown in Fig. 3.1. The ZigBee mote generates traffic with constant packet rate of 50 packets/second and packet length of 100 bytes/packet. After each packet transmission, the source mote waits for ACK from the coordinator. If no ACK is received within macAckWaitDuration, the source mote re-transmits the packet one time. The D-ITG generates UDP traffic with varying segment payload size, segment rate or IDT distribution, which are converted to varying Wi-Fi interference by WR.

In the following, the ZigBee packet transmission performance of ACK with and without use of interference detection mechanism is assessed in terms of ACK delivery rate, packet retransmission rate and duplicate packet received rate. The corresponding results are illustrated and discussed in Figs. 3.6 to 3.9. All the data points are marked with a 95% confidence interval. Fig. 3.6 depicts ZigBee's packet transmission performance when D-ITG generated traffic with constant UDP segment IDT, payload size of 1400 bytes and different segment rates: 300 segments/second (Test 1), 400 segments/second (Test 2), 500 segments/second (Test 3), and 600 segments/second (Test 4).

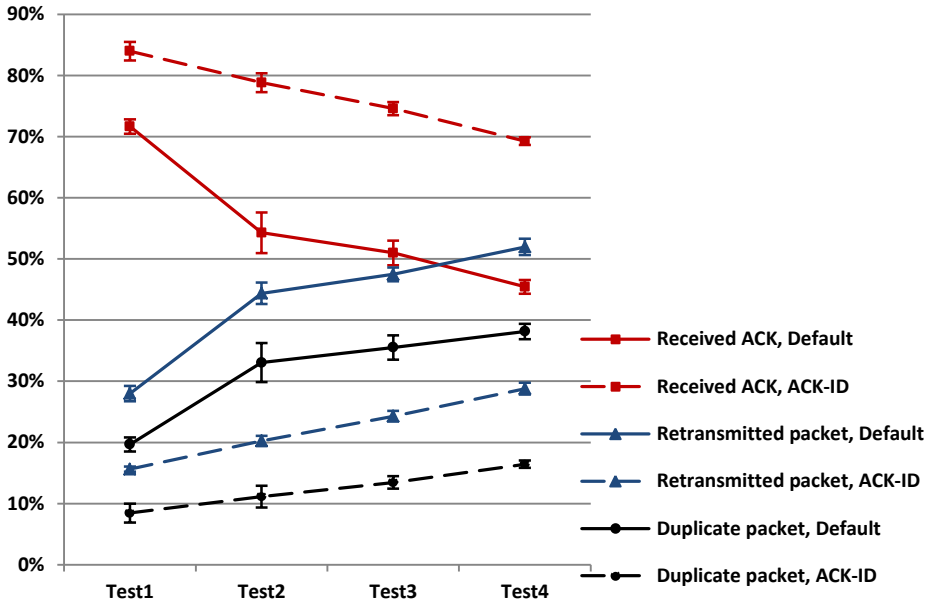

Fig. 3.6 Performance comparison of ZigBee packet transmission under interfering UDP traffic with different segment rates

The results shown in Fig. 3.7 correspond to the case the D-ITG is set to generate UDP segment sequences having constant IDT at the rate of 500 segments/second. Performance was evaluated for four different payload sizes: 500 bytes, indicated in Fig. 6 as test 5; 700 bytes, indicated as test 6; 900 bytes indicated as test 7; and 1100 bytes, indicated as test 8.

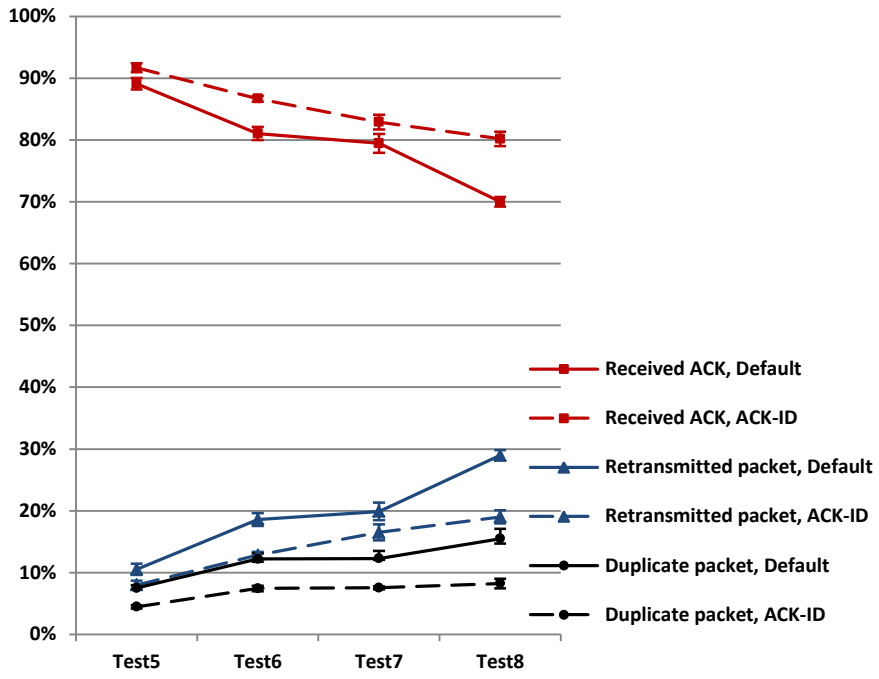

Fig. 3.7Performance comparison of ZigBee packet transmission under interfering UDP traffic with different segment payload sizes.

In Fig. 3.8, the packets generated by D-ITG have the same payload size of 1400 bytes while the IDT is following three different random distributions: Poisson (Test 9), Exponential (Test 10), and Uniform (Test 11), with mean arrival rate of 500 segments/second. More specifically, uniform distributed traffic has a rate between 250 to 750 segments/second.

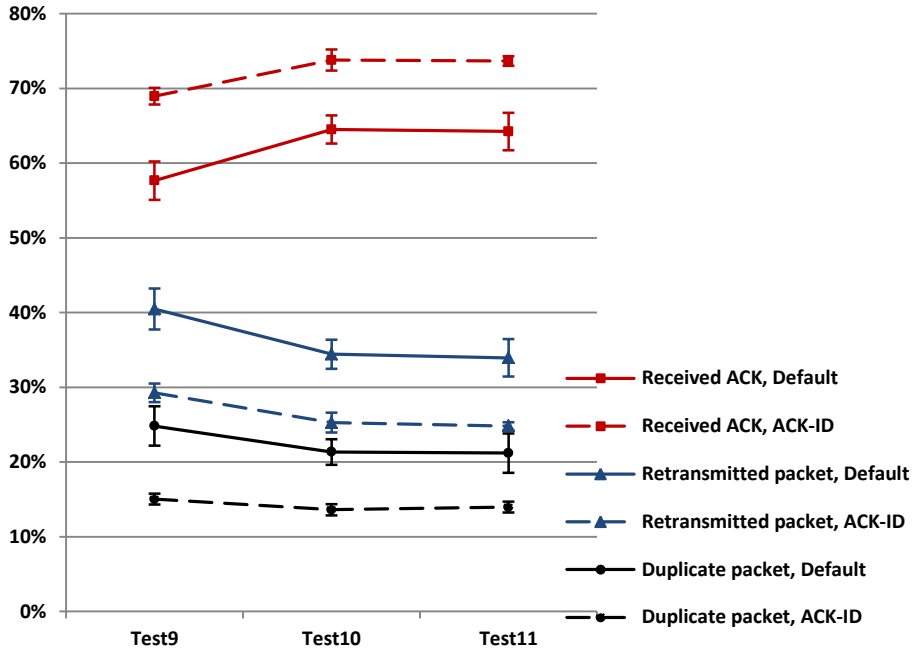

Fig. 3.8 Performance comparison of ZigBee packet transmission under interfering UDP traffic with segment arrival rates following three different random distributions.

For the tests shown in Fig. 3.9, the UDP segment's payload size and IDT are both following four different random distributions, i.e., Poisson (Test 12), Uniform (Test 13), Exponential (Test 14), and Normal (Test 15), with mean payload size 1100 bytes and mean arrival rate 500 segments/second. For the Uniform distribution, the UDP segment generation rate takes values between 250 and 750 segments/second and the payload size between 900 to 1300 bytes. Interfering UDP traffic with Normal distribution has an expected payload size of 1100 bytes and standard deviation of 200 bytes.

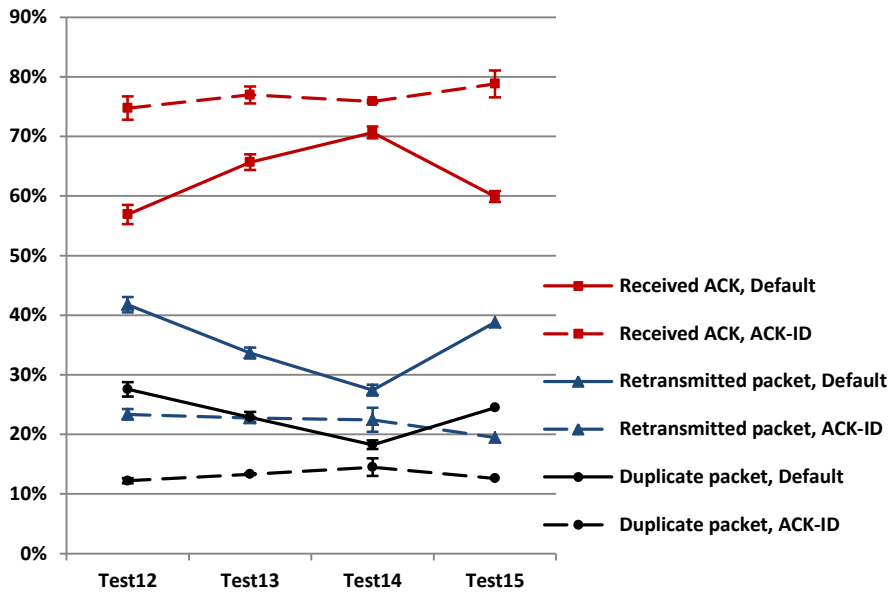

Fig. 3.9 Performance comparison of ZigBee packet transmission under interfering UDP traffic with payload sizes and arrival rates following four different random distributions.

Fig. 3.6 shows that ACK-ID achieves more significant performance improvements in terms of ACK delivery rate when the interfering UDP traffic has higher segment arrival rates (e.g. ~12% increase in the number of received ACKs when the interfering traffic is 300 segments/second and ~24% increase when it becomes 600 segments/second). Observing the curves of Fig. 3.7, we can conclude that when the interfering traffic has smaller segment sizes while without changing the segment generation rate, the performance improvements are less significant (e.g. ~2.5% increase in the number of received ACKs when the payload size of the interfering traffic is 500 bytes compared to ~10.2% increase when the payload size is 1100 bytes). The performance improvement can also be observed in all tests where the segment sizes and/or the IDTs of the interfering traffic follows different random distributions, as illustrated in Figs. 3.8 and 3.9. With the reduced number of lost ACKs, the number of unnecessary packet retransmissions and received duplicate packets are also

significantly reduced, and the same applies to the energy consumption. In addition, by reducing the packet retransmissions, ACK-ID saves a significant amount of channel occupation time spent on packet retransmissions so as to allow more efficient use of the limited bandwidth or support more sensor nodes. Furthermore, the *maxACK-IDTime* ($N_{max} * t_s$, 0.32ms in our experiments) is much shorter than the time needed for packet retransmission (3.2ms for transmitting a 100-byte ZigBee packet plus the time consumed by CCA detections and backoffs). The proposed ACK-ID mechanism has demonstrated significantly better performance compared to the default ACK mechanism while having small impact on the MAC ACK wait duration.

In conclusion, this novel and effective ACK with Interference Detection (ACK-ID) technique improves the performance of ZigBee packet transmission under Wi-Fi interference. The performance improvement has been validated and evaluated through extensive experiments carried out in our testbed. The experimental results confirmed that ACK-ID can significantly improve the performance of ZigBee packet transmission in terms of packet retransmission rate and ACK delivery rate when there is varying interference from the collocated WLAN.

Chapter 4

Adaptive Transmit Power Adjustment Technique

Most sensor nodes in WSNs are powered by batteries, which could be difficult or impossible to replace (e.g. military applications in battlefield environment). Hence, it is very important to use energy in an efficient way so as to extend the lifetime of sensor nodes and the WSN' as a whole. One important strategy for reducing energy consumption is to minimize the transmit power. The selection of transmit power is guided by two considerations. First, different from wired networks that typically have a fixed infrastructure, the choice of transmit power for each node in a mesh based WSN determines its set of neighbors. Second, the selection of transmit power affects the SINR of the received packets, thus the communication link's quality. Based on these two facts, the transmit power adjustment schemes in WSN can be mainly classified into two categories: transmission range based topology control, and link quality control.

The target for transmission range based topology control is to choose the optimal transmit power for each node, so that the global network connectivity can be maintained and energy metrics (e.g. network lifetime) can be optimized. As discussed in Chapter 2, several topology control algorithms [74-78] have been developed that select the optimal power for

each node in WSNs to maintain the network connectivity, i.e. each node is able to communicate to any other node in the WSN via single hop or multi-hop. These solutions derive the static optimal powers at the stage of initial deployment based on the network graph or node density. However, due to the background noise (e.g. thermal noise or environmental noise) and the interference from other wireless networks, the quality of WSN communication link varies with time and environment. The optimal power calculated for fixed channel conditions and a fixed network topology cannot guarantee the communication links' quality.

In recent years, some transmit power control schemes were designed for adapting to the external interference/noise level, adjusting the transmit power to the minimal level that can satisfy the required link quality. In Chapter 2, several dynamic transmit power control mechanisms such as those described in [81-85, 87] were discussed. Some methods [81-85] adjust the power based on the RSSI readings of the received ZigBee packets. However, these RSSI readings may be measuring the superposition of ZigBee signal and interference. In the case of strong interference, the RSSI reading does not reflect reliably the link's quality. In [87], two power control schemes, named as MIAD PC and PER PC, are proposed. In MIAD PC, the transmit power is increased after a packet loss and decreased after a successful packet reception. When frequent packet loss occurs, this method may lead to unstable operation. PER PC determines the background noise level with periodical measurements of RSSI and then derives the SINR based on the applied channel models (AWGN model or Rayleigh model). With the derived SINR, optimal transmit power is obtained. This approach

requires complicated operations and calculation, and is not easy to implement at the resource limited ZigBee motes.

In this chapter, a new but simple and efficient adaptive transmit power adjustment (ATPA) technique, capable to respond promptly to the changing external interference conditions, is described. The scheme estimates the link quality based on the periodically calculated the PLR, and adjusts the transmit power accordingly to try to meet the PLR requirement. The proposed technique was implemented in the Crossbow MICAz motes of our testbed described in chapter 3. It was evaluated experimentally, using the results collected through extensive experimentation. The results show that the ATPA technique improves the energy efficiency of the ZigBee packet transmission while maintaining the predefined maximum tolerable PLR of the application.

The remaining part of this chapter is structured as follows. In section 4.1, a detailed description of the proposed ATPA technique is provided. In section 4.2, a series of comprehensive experiments are described to evaluate the performance of ATAP technique under Wi-Fi interference and the acquired results are presented.

4.1 ATPA Technique Description

The MICAz motes used in our testbed can be programmed to operate at different levels of RF power, which enables the implementation of the ATPA technique for dynamically adjusting the transmit power according to the strength of the time varying external

interference. Table 4.1 shows the different programmable power levels supported by the CC2420 transceiver in MICAz motes and their corresponding current consumption [111].

From the energy efficiency perspective, the MICAz mote should work at the lowest possible power level as long as the reliability of the communication link is satisfying, i.e., the PLR requirement of the sensing application can be met. As shown in Table 4.1, MICAz offers a considerable wide range for adjusting the power settings. Our experimental performance evaluation results, which will be presented in the next section, also show that there is a significant difference between PLRs when the mote operates at the minimum and the maximum power under Wi-Fi interference.

Table 4.1 Output power settings and current consumption [111]

Power Level Index	Output Power [dBm]	Current Consumption [mA]
8	0	17.4
7	-1	16.5
6	-3	15.2
5	-5	13.9
4	-7	12.5
3	-10	11.2
2	-15	9.9
1	-25	8.5

Therefore, when the ZigBee communication link suffers from varying external interference, ideally the motes should be able to adjust their transmit power adaptively according to the interference level and the PLR requirement set by sensing application, i.e., increase the transmit power when PLR exceeds the required threshold value because of the strong interference and reduce the transmit power when the interference decreases as long as the PLR requirement can be satisfied. The proposed ATPA is designed to provide timely power adjustment based on the changing PLR values. The flowchart of the proposed ATPA is illustrated in Fig. 4.1.

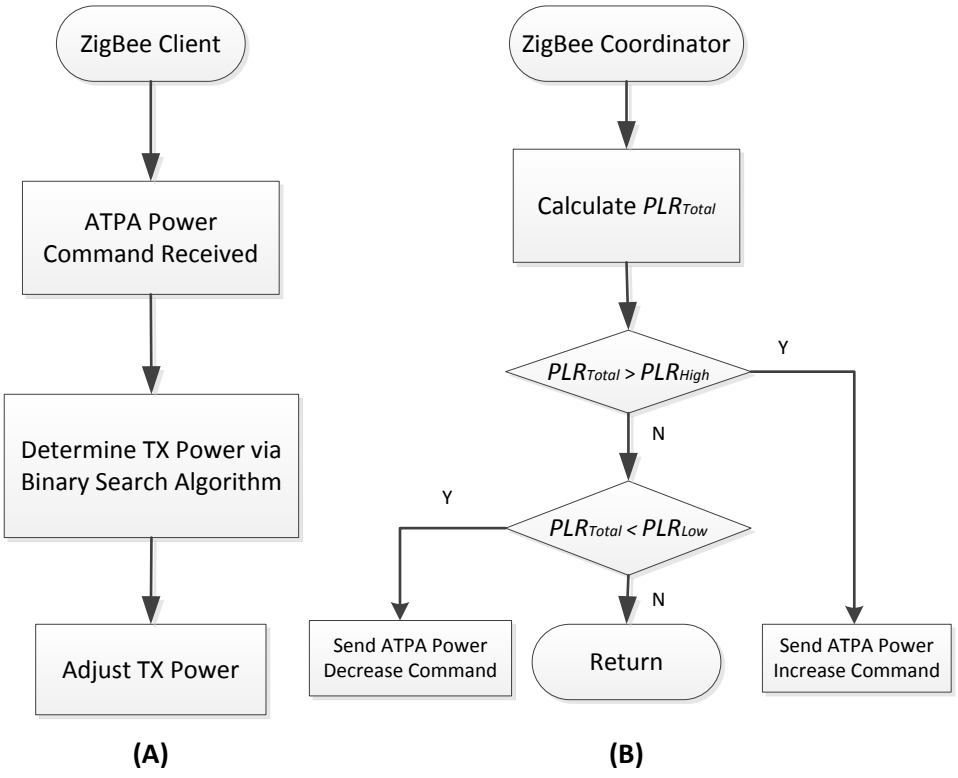

Fig. 4.1 Flowchart of the ATPA mechanism: (A) ZigBee Client (B) ZigBee Coordinator

In the proposed ATPA scheme, the required PLR of a specific sensing application is set at the ZigBee coordinator's firmware. To avoid frequent change of transmit power, two PLR

threshold values are introduced, denoted as PLR_{High} and PLR_{Low}, respectively. PLR_{High} has the value of the required PLR, while PLR_{Low} is set to a lower value. The motes maintain the transmit power when the measured PLR falls between PLR_{High} *and* PLR_{Low}. T_{update} is the time interval for calculating and updating the PLR value. After every T_{update} (e.g. 10 seconds), the coordinator calculates the number of packet losses, denoted as PLR_{Total}:

$$PLR_{Total} = 1 - \frac{N_R}{DSN_{Last} - DSN_{First}}, \tag{4.1}$$

where N_R is the number of received packets within T_{update}, DSN_{First} and DSN_{Last} are the data sequence numbers (DSN) for the first and last received packets during T_{update}, respectively. If PLR_{Total} is higher than PLR_{High}, an ATPA command packet is sent to the ZigBee client to increase its transmit power level. Otherwise, if PLR_{Total} is lower than PLR_{Low}, an ATPA command packet with a message to reduce the transmit power is sent. In addition, the ATPA command packet is sent at the maximum transmit power so as to insure higher delivery rate.

The ZigBee client mote first selects the maximum power level (0 dBm) as the initial transmit power. During the running time, it adjusts its transmit power level based on the received ATPA commands. Considering the power level adjustment happens in every T_{update} seconds, a binary search algorithm is applied to speed up the adjustment mechanism in finding the lowest transmit power that satisfies the PLR requirement.

The pseudo code of ATPA binary search scheme is depicted in Fig. 4.2. As shown in Table 4.1, each output power level is represented as an integer index. We denote L_{High} and L_{Low} as

the two search index limits; $Index_{Max}$, $Index_{Min}$, and $Index_{Cur}$ as the maximum, minimum and current power level index respectively.

Input: L_{High}, L_{Low}, $Index_{Max}$, $Index_{Min}$, and $Index_{Cur}$

Initial phase: $L_{High} = Index_{Max}$; $L_{Low} = Index_{Min}$;

If to increase transmit power:

If ($L_{High} = L_{Low}$) { $L_{High} = Index_{Max}$;}

$L_{Low} = Index_{Cur}$;

$Index_{Cur} = \left\lceil \frac{L_{High} + L_{Low}}{2} \right\rceil$;

If to decrease transmit power:

If ($L_{High} = L_{Low}$) { $L_{Low} = Index_{Min}$;}

$L_{High} = Index_{Cur}$;

$Index_{Cur} = \left\lfloor \frac{L_{High} + L_{Low}}{2} \right\rfloor$;

Fig. 4.2 Binary search algorithm of ATPA

As shown in Fig.4.2, The binary search algorithm is implemented with two index limits, i.e. L_{High} and L_{Low} (initialized with $Index_{Max}$ and $Index_{Min}$ respectively), that progressively narrow the search range. If the received ATPA command is to increase the transmit power, the current operating power level index, $Index_{Cur}$, is selected as L_{Low}. On the other hand, if the received command is to decrease the transmit power, the $Index_{Cur}$ is chosen as L_{High}. The intermediate power level index between the L_{High} and L_{Low} is obtained and the corresponding transmit power is selected at the ZigBee client. Compared to linear search that adjusts the power level by level, whose worst case is *N-1* iterations (*N* is the number of the

power levels supported in the mote.), the binary search is substantially faster as *N* grows large with a worst case of$\lceil log_2(N) \rceil$.

The ZigBee coordinator sends back an ATPA command to trigger the binary search operation until the PLR_{Total} is between the two PLR boundaries, i.e., PLR_{High} *and* PLR_{Low}. Once the external interference changes and the PLR requirement is not satisfied any more, a new ATPA power increase/decrease command will be generated and transmitted to trigger another binary search operation.

4.2 Performance Evaluation Results and Discussion

In order to validate the performance improvement of the proposed ATPA mechanism, we performed an extensive set of experiments using the testbed shown in Fig. 3.1. For comparison, ZigBee's performance was also assessed when the transmit power of the ZigBee client mote was set at the maximum or minimum values. PLR and energy consumption of the CC2420 transceiver in the packet transmission process were evaluated. For transmitting each ZigBee packet, the energy consumed by CC2420 can be expressed as:

$$\mathrm{E} = A_i * V_{cc2420} * \frac{L_Z}{R_Z}, \tag{4.2}$$

With A_i denoting the current consumption of power level *i* (shown in Table 4.1), V_{CC2420} the supply voltage of 1.8V, L_Z the ZigBee packet length, and R_Z the transmit bit rate. Our custom-made ZigBee client firmware calculates the number of ZigBee packets transmitted at each power level so that the total energy consumption in the experiment can be calculated. In

each experiment, the ZigBee client mote is programmed to send out 10000 data packets with 100 bytes/packet at 30ms intervals. Same as previous experiments described in Chapter 3, the D-ITG generates UDP traffic with varying segment payload, segment rate and IDT distribution, which are converted to varying IEEE 802.11g Wi-Fi interference by WR. The corresponding results are illustrated and discussed in Figs. 4.3 to 4.8. All the data points are marked with a 95% confidence interval.

In Fig. 4.3 and Fig. 4.4, ZigBee's performance evaluation results are shown when transmitted packets are not acknowledged, thus there aren't packet retransmissions. The required PLR (PLR_{High}) is set to be 10% and PLR_{Low} is assigned the value of 9%. D-ITG generated UDP traffic with constant segment IDT, payload size of 1400 bytes and different segment generation rates: 300 segments/second (Test 1), 500 segments/second (Test 2), and a combination of 300 segments/second in the first half of the experiment and 500 segments/second for the remaining half (Test 3).

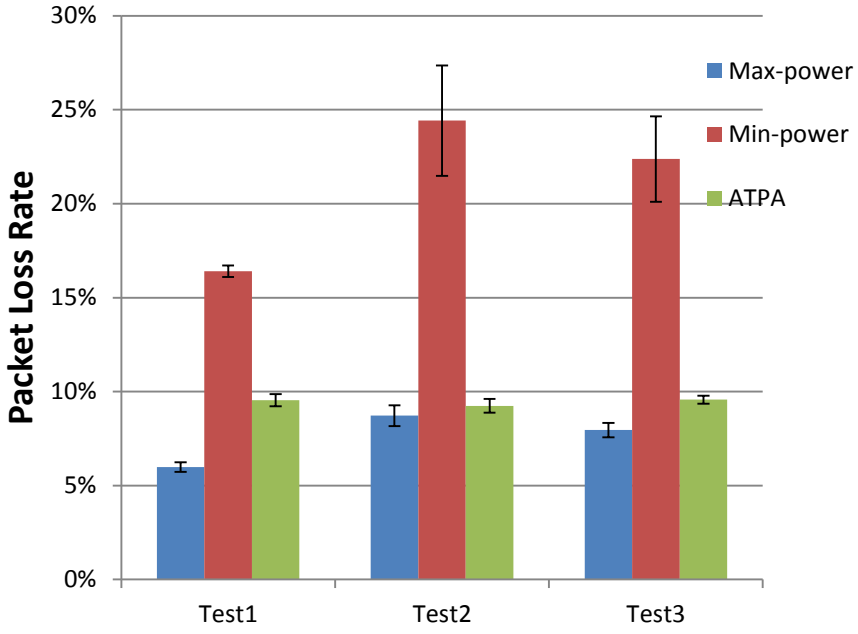

Fig.4.3 Packet loss rate comparison of ZigBee without the use of packet retransmission under interfering UDP traffic with different segment rates.

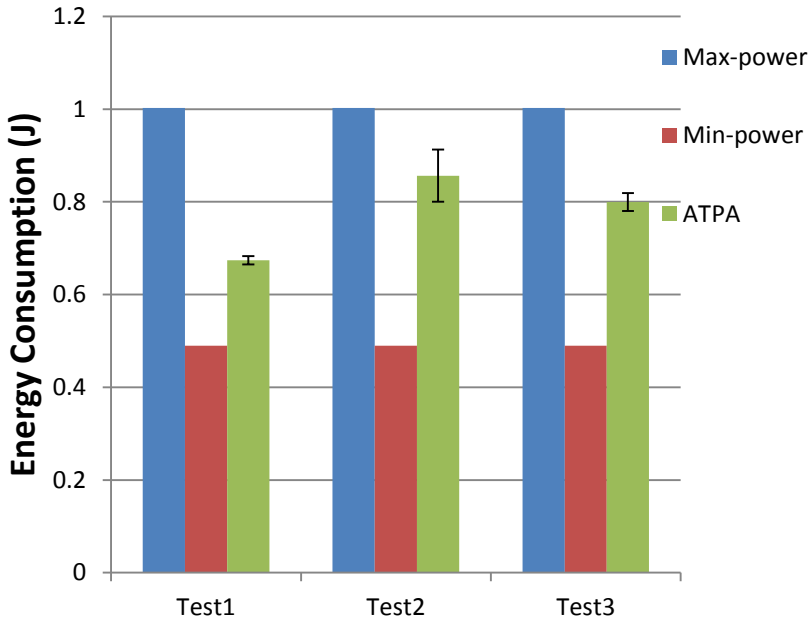

Fig.4.4 Energy consumption comparison of ZigBee without the use of packet retransmission under interfering UDP traffic with different segment rates.

As shown in Figs. 4.3 and 4.4, although using the minimum transmit power consumes the minimum energy for packet transmission, the ZigBee mote suffers from severe packet losses, resulting in PLRs far beyond the required value. While operating at the maximum power achieves the best PLR, the transmitting mote consumes the most energy. Obviously, if the PLR requirement has already been met, there is little or no use for ZigBee mote to sacrifice more energy in exchange of further PLR improvement. The proposed ATPA provides a simple but efficient trade-off algorithm to reduce the energy consumption while maintaining the required PLR. In addition, ATPA handles the changing Wi-Fi interference very well. The Wi-Fi traffic in Test 3 is an equal combination of traffic used in Test 1 and Test 2. Thus, in Fig. 4.3, the PLRs of minimum and maximum transmit power in Test 3 have values larger than those in Test1 but smaller than those in Test2. It can be observed in Fig 4.4 that the energy consumption of ATPA in Test 3 is between the corresponding values in Test 1 and Test 2, which shows the ATPA adjusts the selected transmit power when interference changes. ATPA increases transmit power when interference increases so that PLR is maintained.

In Figs. 4.5 – 4.8, the ZigBee's performance is evaluated when allowing one ZigBee packet retransmission. The results of our earlier proposed ACK with Interference Detection (ACK-ID) scheme, which has been described in Chapter3, are also illustrated for comparison purposes. The PLR_{High} and PLR_{Low} have assigned values of 3% and 2%, respectively. In Fig. 4.5 and Fig. 4.6, D-ITG is set to generate traffic with constant UDP segment IDT, payload size of 1400 bytes and different segment rates: 500 segments/second (Test 4), 700 segments/second (Test 5), and a combined traffic with 500 segments/second in the first

half of the experiment and 700 segments/second in the remaining half (Test 6). For the tests shown in Fig. 4.7 and Fig. 4.8, the UDP segment's payload size and IDT are both following three different random distributions, i.e., Poisson (Test 7), Uniform (Test 8), and Exponential (Test 9), with mean payload size of 1200 bytes and arrival rate of 600 segments/second. More specifically, uniform distributed traffic has a UDP payload size between 1000 to 1400 bytes, and a segment rate between 400 to 800 segments/second.

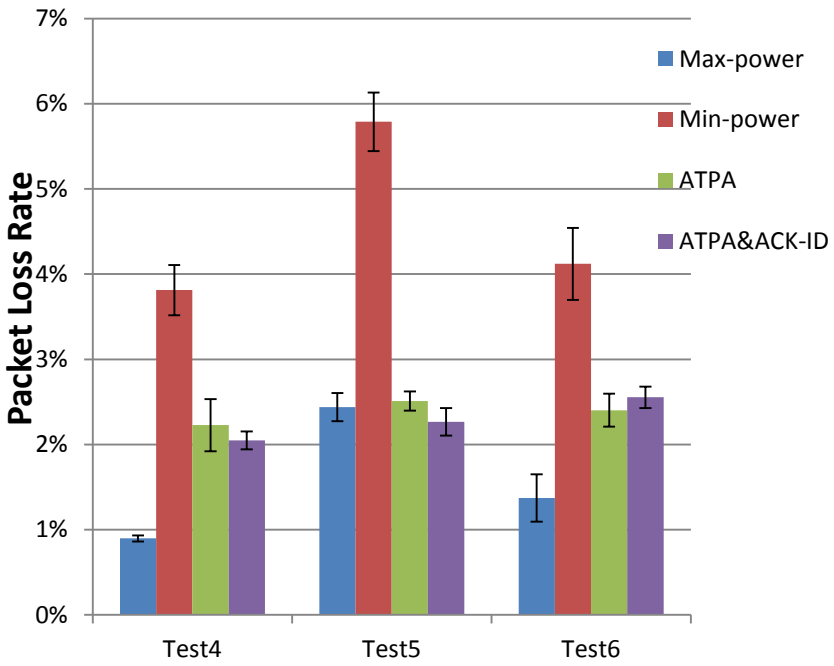

Fig.4.5 Packet loss rate comparison of ZigBee with the use of packet retransmission under interfering UDP traffic with different segment rates.

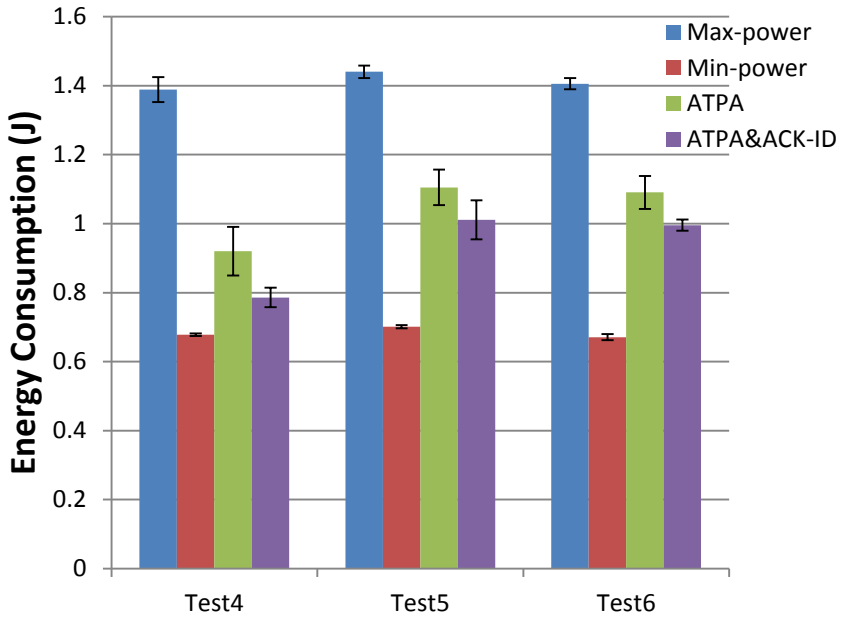

Fig.4.6 Energy consumption comparison of ZigBee with the use of packet retransmission under interfering UDP traffic with different segment rates.

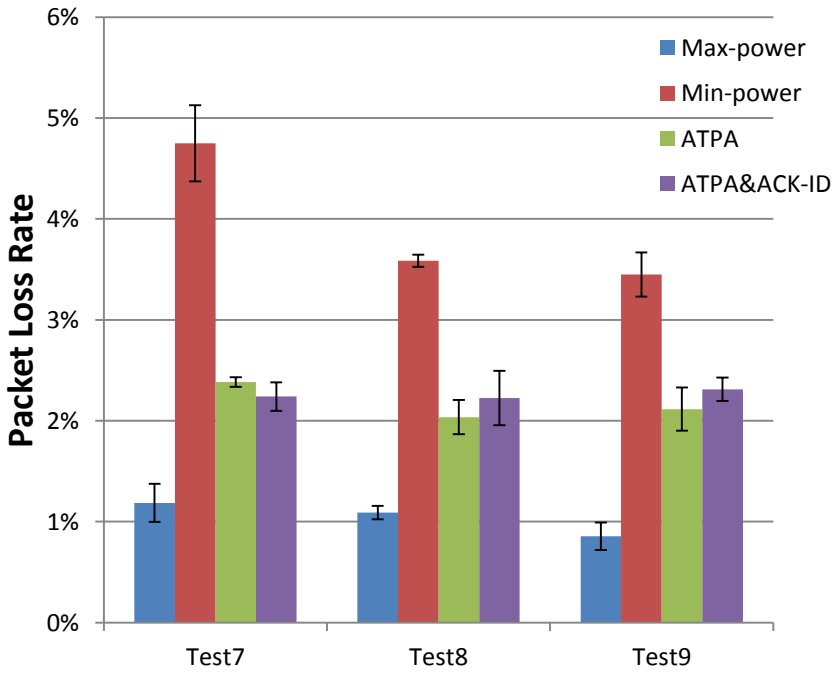

Fig. 4.7 Packet loss rate comparison of ZigBee with the use of packet retransmission under interfering UDP traffic with payload sizes and arrival rates following three different random distributions.

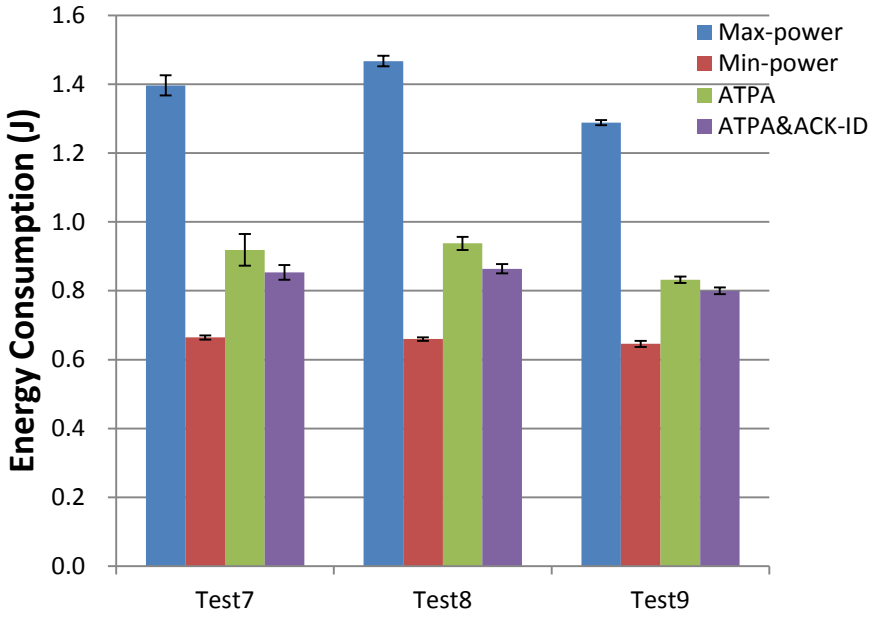

Fig. 4.8 Energy consumption comparison of ZigBee with the use of packet retransmission under interfering UDP traffic with payload sizes and arrival rates following three different random distributions.

From Figs. 4.5-4.8, it can be seen that ATPA reduces the energy consumption for packet transmission while satisfying the predefined PLR requirement when there is varying interference from the collocated WLAN. As discussed in Chapter 3, ACK-ID can significantly improve the performance of ZigBee packet transmission in terms of packet retransmission rate, which consequently saves energy. Based on the experimental results in Chapter 3&4, the ACK-ID and ATPA techniques can be implemented together to achieve better usage of bandwidth and energy when there is varying Wi-Fi interference close by.

Chapter 5

Time Aware Backoff and Transmission Technique

For the very common periodic sensing/monitoring applications, the ZigBee client mote generates packets at equal time intervals, which are transmitted to the data sink mote. In our experimental studies of ZigBee packet loss when subjected to close-by Wi-Fi interference, it is noticed that a substantial amount of packet loss is due to TXFIFO buffer overflow at the transmitting mote. Wi-Fi interference could not cause packet losses due to overlapped transmissions of Wi-Fi and ZigBee frames, but also increase the time needed for completing a packet transmission, leading to packet drops due to TXFIFO buffer overflow. Such prolonged packet transmission process is attributed to the increased number of CCAs, CSMA/CA backoffs, packet retransmissions, and so on. The CSMA/CA mechanism and its corresponding Binary Exponential Backoff (BEB) algorithm defined in the IEEE 802.15.4 standard does not take this time constraint into consideration and could cause a ZigBee packet's loss when the backoff process consumes too much time and the newly generated packet arrives before the proceeding packet is sent out. Therefore, it is meaningful to design and develop new technology for improving the performance of IEEE 802.15.4 CSMA/CA algorithm by imposing time constraints for backoffs.

As introduced in Chapter 2, several earlier research contributions investigated the performance of 802.15.4 CSMA/CA mechanism such as throughput, packet loss rate and latency. Some techniques have been developed to enhance the performance of CSMA/CA by adjusting the CSMA/CA parameters based on traffic class, network size, results of CCAs, etc. However, none of them considered the time constraints for BEBs. Motived by these observations and considerations, we first try to reduce TXFIFO overflow by adjusting the values of CSMA/CA parameters in order to reduce the length of CSMA/CA BEB delay. Although the experimental results show some performance improvements, this approach can only partially alleviate the TXFIFO overflow problem. It is also very challenging to adaptively select the appropriate value for each parameter. We then propose and develop a more effective Time Aware Backoff and Transmission (TABTx) technique that controls the time spent for each packet transmission attempt so as to effectively avoid TXFIFO overflows. In addition, the newly proposed TABTx technique interrupts the default CSMA/CA mechanism only when the calculated backoff period may cause TXFIFO overflow. The TABTx technique was implemented in the Crossbow MICAz motes and an extensive set of experiments were carried out using the testbed we introduced in chapter 3 to evaluate its performance. The results show that the TABTx technique eliminates the TXFIFO overflow completely and as consequence it provides better performance in terms of PLR.

The remaining part of this chapter is structured as follows. Section 5.1 reviews the IEEE unslotted 802.15.4 CSMA/CA with binary exponential backoff algorithm. In section 5.2, we investigate the TXFIFO overflow issue and work on adjusting the CSMA/CA parameters. Then we present the proposed TABTx technique in section 5.3. In section 5.4, the

performance evaluation results compiled from experimental data collected through our comprehensive experiments are presented.

5.1 Introduction to IEEE 802.15.4 unslotted CSMA/CA

The IEEE 802.15.4 standard specifies two types of channel access mechanisms, unslotted CSMA/CA for Nonbeacon-enabled WSNs, and slotted CSMA/CA for beacon-enabled WSNs [30]. As this research focuses on Nonbeacon-enabled WSNs, only the unslotted CSMA/CA mechanism is reviewed in this section. Table 5.1 lists the parameters used in the unslotted CSMA/CA algorithm, and Fig.5.1 depicts in flow chart form the steps followed by the algorithm.

Table 5.1 Parameters in the IEEE 802.15.4 unslotted CSMA/CA [30]

Parameter name	Default value	Definition
BE	Initialized as *macMinBE*	*BE* is the backoff exponent, which is related to how many backoff periods a device should wait before performing CCA.
macMinBE	3	The minimum value of the *BE* in CSMA/CA.
macMaxBE	5	The maximum value of the *BE* in CSMA/CA.
macMaxCSMABackoffs	4	The maximum number of backoffs before declaring a channel access failure.
NB	Initialized as 0	*NB* is the number of times the CSMA/CA algorithm was required to backoff while attempting the current transmission.
aUnitBackoffPeriod	20	The number of symbols that forms the basic time unit used by the CSMA/CA algorithm.

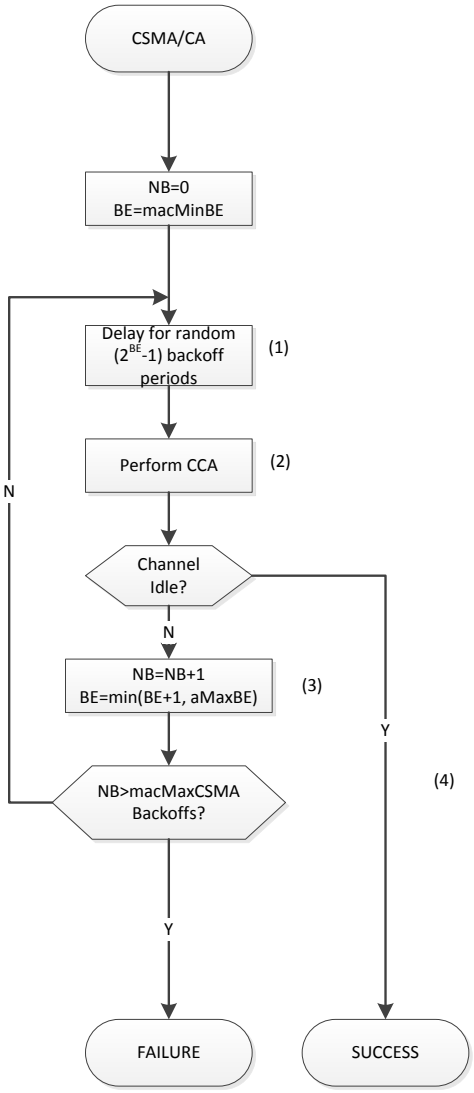

Fig.5.1 IEEE 802.15.4 unslotted CSMA/CA flow chart [30]

As shown in Fig.5.1, the MAC sub-layer shall first initialize *NB* and *BE*, and then delay for a random number of complete backoff periods in the range of 0 to 2^{BE} –1 (Step 1). A backoff period is the basic time unit used by the CSMA/CA algorithm, which is equal to the product of *aUnitBackoffPeriod* and symbol period. When the backoff counter is reduced to zero, the device activates to perform a CCA (Step 2). If the channel is assessed to be idle, the device transmits the data packet immediately (Step 4), otherwise the MAC sub-layer shall increase both *NB* and *BE* by one (Step 3), however ensuring that *BE* will not exceed *macMaxBE*. If the

value of *NB* is less than or equal to *macMaxCSMABackoffs*, the CSMA/CA mechanism returns to Step 1, else it terminates this transmission attempt with a Channel Access Failure status [30].

5.2 Experimental Study of CSMA/CA Parameters Tuning

When there are Wi-Fi packet transmissions in the vicinity, the CCA of ZigBee client mote is likely to report busy medium and trigger backoffs in CSMA/CA. The time consumed by the CSMA/CA binary exponential backoffs can be varied, depending on the values of *macMinBE*, *macMaxBE*, *macMaxCSMABackoffs*, as well as the characteristics of the external interference. In Chapter 3, we discussed the packet drops due to CC2420 Transmit First in First out Byte Register (TXFIFO) overflow. For the very common sensing application of periodic monitoring, when the time for completing the transmission of the preceding packet exceeds the inter-arrival time between two subsequent ZigBee packets, there will be packet drop due to transceiver TXFIFO buffer overflow. While the time for transmitting a ZigBee packet is determined by its packet length and transmission speed, adjusting CSMA/CA BEB parameters could be an effective way to reduce the packet drops due to TXFIFO overflow.

A series of experiments were performed in our testbed, shown in Fig.3.1, to study the impact the adjustment of CSMA/CA parameters has on the performance of PLR and TXFIFO Overflow Rate (OFR). As *macMinBE* and *macMaxBE* are used to decide the maximum time of each backoff, we perform experiments to shorten the CSMA/CA backoff delays by

progressively reducing the value of these two parameters. The following table lists the values of CSMA/CA BEB parameters in the form of (*macMinBE*, *macMaxBE*, and *macMaxCSMABackoffs*) and experiments are performed by adopting the values as shown in different cases.

Table 5.2 Values of BEB parameters and the corresponding length of delay periods

	Case1	Case2	Case3	Case4	Case5	Case6
CSMA/CA parameters	(3,5,4)	(3,4,4)	(3,3,4)	(2,5,4)	(2,4,4)	(2,3,4)
Backoff period range[5] (ms)	[0, 36.8]	[0, 21.44]	[0, 11.2]	[0, 27.84]	[0, 17.6]	[0, 9.92]

The following figure (Fig.5.2) shows the ZigBee system's performance with different CSMA/CA parameters under interfering D-ITG UDP traffic with payload of 1400 bytes/segment, constant segment IDT at the rate of 800 segments/second. The ZigBee client mote is set to transmit 50-byte packet at the rate of 100 packets/s (ZigBee Traffic 2), or 100-byte packet at a rate of 50 packets/s (ZigBee Traffic 1). For either traffic, the maximum number of packet retransmission is set to 1.

[5] The upper limit of backoff periods range denotes the maximum value of total backoff time before claiming a channel access failure.

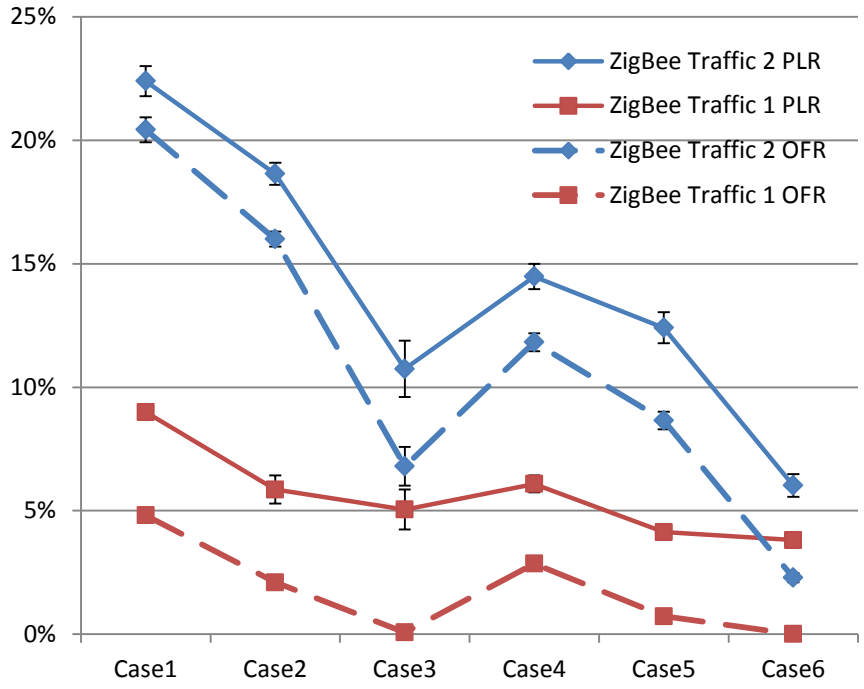

Fig.5.2 ZigBee performances with different BEB parameters under interfering Wi-Fi UDP traffic

It is shown in Fig.5.2 that the TXFIFO overflows become particularly problematic when the ZigBee mote is transmitting at high packet rate. This is due to that under high packet rate, the time interval between ZigBee packets is small that the time spent on packet transmission including the CSMA/CA backoffs can easily exceed this time interval and cause TXFIFO overflow. Fig.5.2 also illustrates that by reducing the values of CSMA/CA parameters, which shortens the delay induced by CSMA/CA BEB, can improve the ZigBee performance when the TXFIFO overflow causes a significant number of packet loss. In these experiments, the values of *macMinBE* and *macMaxBE* are adjusted to investigate their impact on ZigBee performance. While performance improvements can be observed by simply reducing the value of these two parameters, it could be difficult to determine the optimal values for changing external interference and for different sensing applications. In addition, it can be seen from Fig.5.2 that with the reduced values of *macMinBE* and

macMaxBE, packet drops due to TXFIFO overflow can still occur. Since TXFIFO overflow happens when the time spent for sending the current packet in the transceiver TXFIFO buffer exceeds the inter-arrival time of the next packet, we propose a technique, named Time Aware Backoff and Transmission (TABTx), which sets constraint on the transmission time when the packet is in the transceiver TXFIFO buffer. The proposed TABTx will be introduced in the next section.

5.3 Time Aware Backoff and Transmission Technique

The time for completing a ZigBee packet transmission might include the packet transmission/retransmission time, ACK waiting time, CCA detections and a number of CSMA/CA BEBs, and so on. When there is no packet retransmission, the time spent for transmitting a packet primarily includes packet transmission time and CSMA/CA BEBs. When the packet is allowed to retransmit up to *macMaxFrameRetries* times, the packet transmission time might include up to (*macMaxFrameRetries*+1) times of CSMA/CA BEBs, ACK waiting and receiving, and packet transmission/retransmissions, as shown in Fig.5.3. Apparently, Wi-Fi interference could cause ZigBee data and ACK packet losses and increase time spent on CSMA/CA BEBs and packet retransmissions. To avoid TXFIFO overflow, the packet transmission process should be completed before a new packet arrives. For periodic sensing/monitoring applications, the sensing/monitoring interval is known and can be used as a parameter for adjusting the BEB and packet transmission strategies.

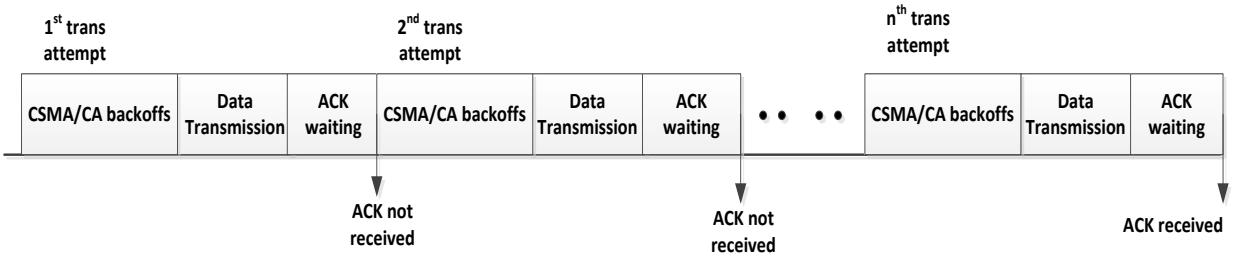

Fig.5.3 the ZigBee packet transmission process

For an application with certain sensing interval, the proposed TABTx calculates a number of time limits, denoted as $T_{LMT}(n)$ (n = 1, 2, …, *macMaxFrameRetries*+1), for completing the n data packet (re)transmission attempts according to the *macMaxFrameRetries* value and the size of ZigBee data packets. As shown in Fig.5.4 in order to allow sufficient time for completing the remaining packet transmission/retransmissions, the time limit for the n^{th} transmission attempt $T_{LMT}(n)$ can be expressed as

$$T_{LMT}(n) = (macMaxFrameRetries + 2 - n) \cdot \left(T_{init\_BO} + macACKWaitDuration + T_{data}\right) - T_{init\_BO},$$

$$n = 1, 2, \dots, macMaxFrameRetries, \quad (5.1)$$

where *macACKWaitDuration* is the maximum number of symbol time periods the senders waits for an acknowledgment, following a transmitted data frame, to arrive (in CC 2420, *macACKWaitDuration* has a value of 40 symbol time periods), T_{data} is the time for transmitting the data packet, and T_{init_BO} is the maximum length of initial CSMA/CA backoff, which can be calculated as:

$$T_{init\_BO} = (2^{macMinBE} - 1) \cdot aUnitBackoffPeriod. \quad (5.2)$$

It should be noted that there are some other factors that contribute to the time consumption, such as instruction processing and hardware RX-TX turnaround time.

Therefore, in order to guarantee the remaining time, it is sufficient for the last retransmission attempt that a margin time frame T_m (1ms) is added to T_{LMT}(*macMaxFrameRetries*+1), i.e.,

$$T_{LMT}(macMaxFrameRetries + 1) = macACKWaitDuration + T_{data} + T_m \,. \qquad (5.3)$$

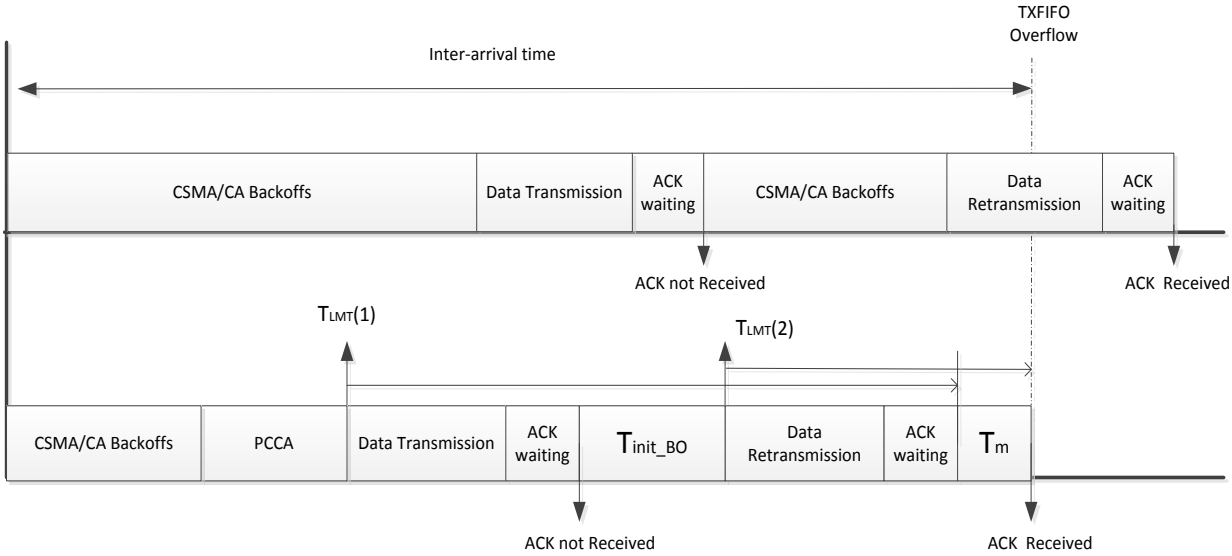

Fig.5.4 TXFIFO overflows and the calculation of time limits

As in IEEE 802.15.4 standard, before each backoff, CSMA/CA calculates the backoff period as

$$T_{BO} = Random\,(2^{BE} - 1) \cdot aUnitBackoffPeriod \;. \qquad (5.4)$$

A timer T_{rmng}, with an initial value of T_{int}, the inter-arrival time between two subsequent ZigBee packets, set at the beginning of a packet transmission process, is used to keep track of the remaining time from the beginning of each backoff to the arrival of the next packet. The upcoming backoff must be completed within a certain time frame so as to allow sufficient time for future (re)transmission attempts. Therefore, if the mote is in the process of its n^{th} transmission attempt, the following relationship needs to be satisfied:

$$T_{rmng} - T_{BO} \geq T_{LMT}(n). \quad (5.5)$$

If the T_{BO}, calculated from (5.4) is too long to satisfy (5.5), the mote adopts a Persistent CCA (PCCA) mechanism. In PCCA, within the time duration of (T_{rmng} - T_{LMT}(n)), the transmitting mote continuously reads the RSSI value at an interval of a symbol time period (16μs defined in standard when operating at 2.4GHz), and the packet transmission starts once *r* (e.g. 2) successive RSSI readings are below the ED threshold P_{th}.

The details of TABTx are given in the following two flow charts. Fig.5.5 shows the process followed by TABTx.

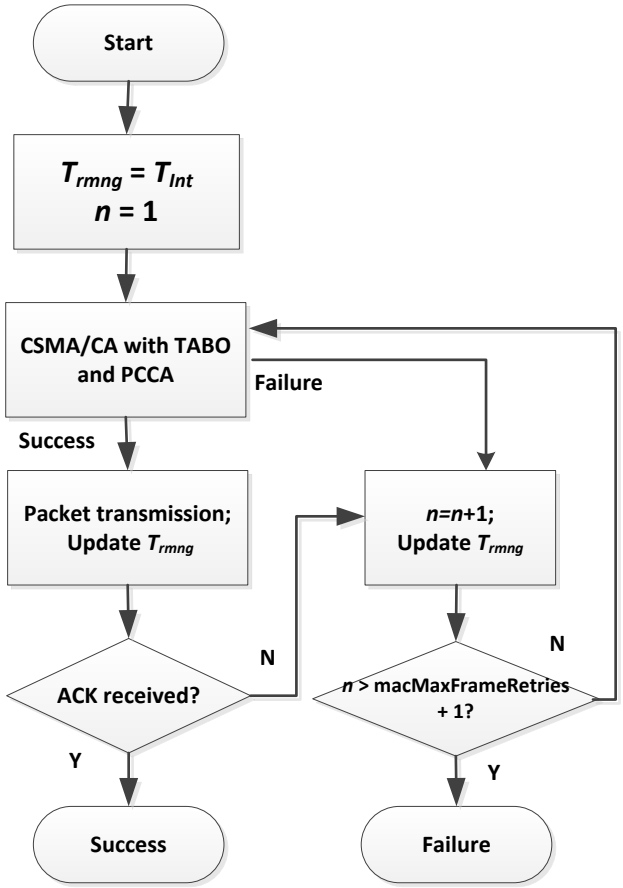

Fig.5.5 the TABTx process

Before the transmission of a packet, T_{rmng} is assigned an initial value of T_{int} and will be updated by subtracting the corresponding time consumption after backoffs and packet

(data/ACK) transmissions. The CSMA/CA in the process is replaced with CSMA/CA with Time Aware Backoffs (TABO) and PCCA mechanism, the details of which are depicted in Fig.5.6, for ensuring that the time consumed by CSMA/CA will not cause TXFIFO overflow.

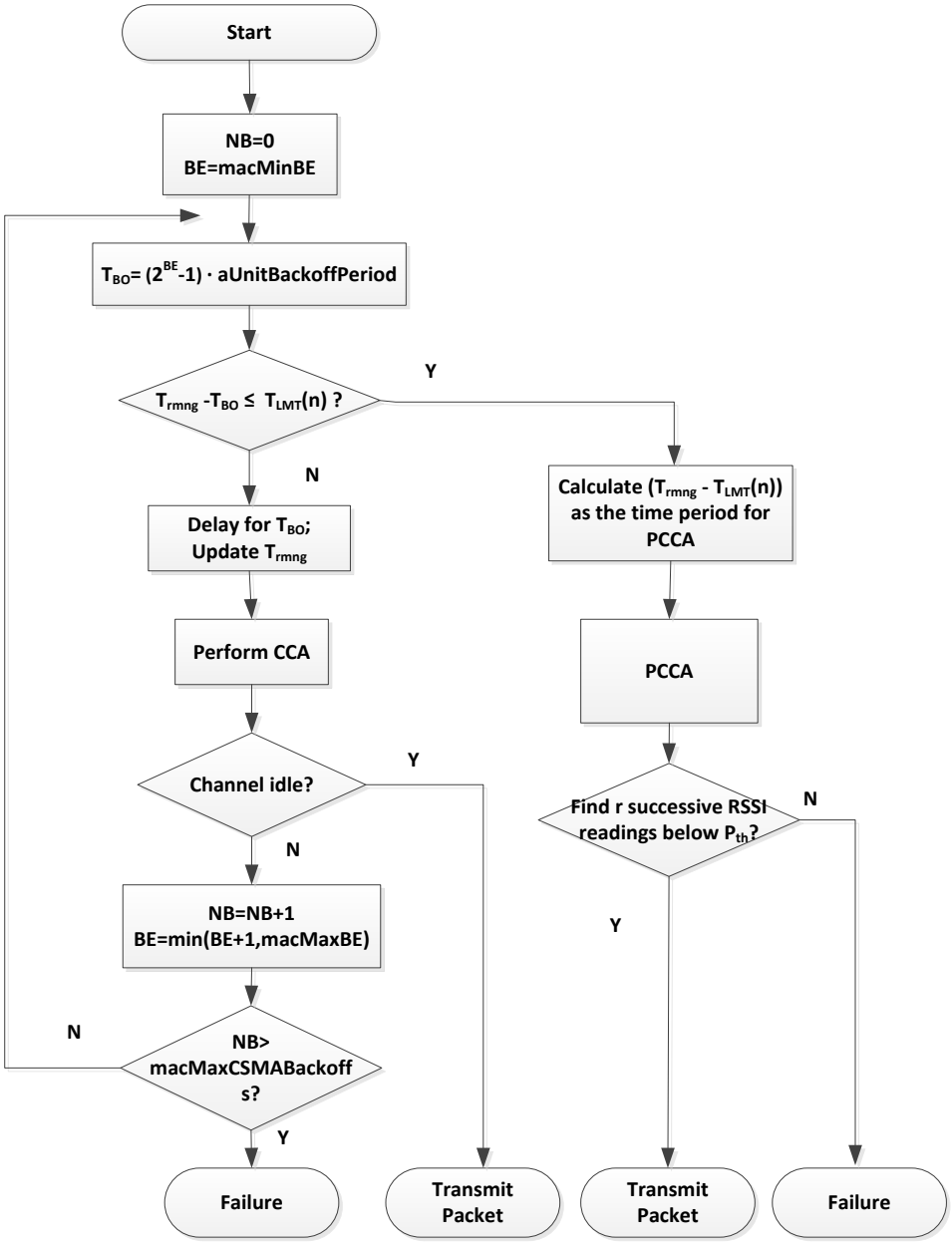

Fig.5.6 CSMA/CA with TABO and PCCA

Fig.5.6 introduces the process of TABO. Before each backoff, the transmitting mote will determine if the remaining time is sufficient for the backoff without causing possible packet

drop due to TXFIFO overflow. If the remaining time is sufficient, the backoff will take place without any intervention. Otherwise, PCCA is used to persistently and frequently check the channel status, seeking opportunity to attempt a packet transmission.

5.4 Performance Evaluation Results and Discussion

TABTx was implemented as firmware and was flashed into the MICAz motes. A series of experiments were performed to evaluate its performance and compare with that of the conventional CSMA/CA. We investigated two sensing application scenarios. The ZigBee client mote is transmitting 100-byte packets at constant packet rate of 50 packets/s in one scenario and 50-byte packets at constant 100 packets/s in the other one. In all experiments, *macMaxFrameRetries* is set to be 1 and we assign 1ms for the T_m. In all figures of this section presenting performance evaluation results, the curves corresponding to PLR results related to the default CSMA/CA are in blue and red colors. Red curves correspond to TXFIFO overflow rate while the blue ones provide the packet loss occurring as result of any possible cause, such as collisions or CCA failures. It is denoted as OLR in the legends of the figures.

Figs. 5.7 – 5.9 show the results for ZigBee packets having size 100 bytes/packet, generated at equal IDT with rate of 50 packets/s. For this specific traffic, we can derive the time limits $T_{LMT}(1)$ and $T_{LMT}(2)$ using equations (5.1) – (5.3) with $T_{data} = 3.2ms$. The calculated values are $T_{LMT}(1)$ = 10ms and $T_{LMT}(2)$ = 5ms. The D-ITG is set to generate UDP segment sequences having constant segment IDT at the rate of 1000 segments/second. Performance was evaluated for three different payload sizes of UDP traffic. The payload sizes are: 900 bytes, indicated in Fig. 5.7 as Test 1; 1100 bytes, indicated as Test 2; and 1400 bytes, indicated as Test 3. Fig. 5.8 depicts the ZigBee transmission performance under interfering Wi-Fi UDP

traffic having UDP segment payload size of 1400 bytes and rates 500 segments/second (Test 4), 800 segments/second (Test 5), and 1000 segments/second (Test 6). UDP segments are generated again with equal IDT. In Fig. 5.9, results are shown when both, the generated UDP segment payload size and segment generation rate follow different random distributions. In Test 7, both segment payload size and segment rate follow Poisson distribution with mean 1100 bytes/segment and 800 segments/s; in Test 8, both use Uniform distributions between 900 and 1300 bytes/segment and 600 and 1000 segments/second; in Test 9, the UDP segment generation rate is fixed at 800 segments/s and the segment payload size follows Normal distribution with expected value of 1100 bytes/segment and standard deviation of 200segments/s.

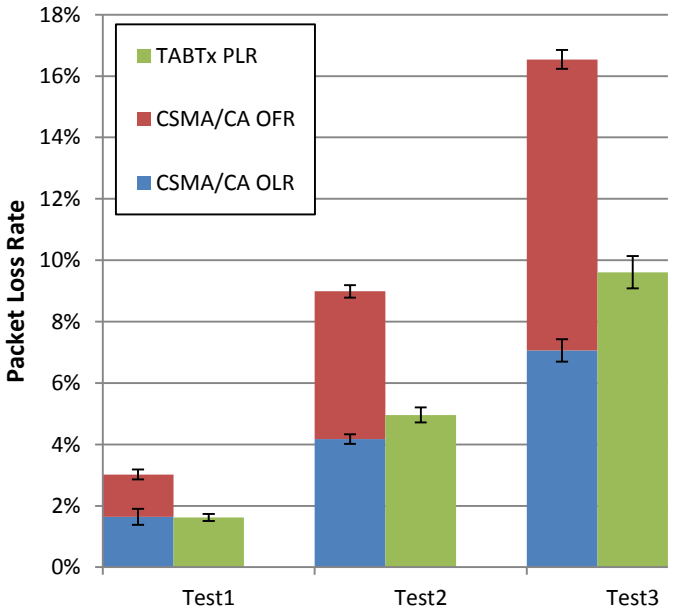

Fig.5.7 ZigBee PLR performances with or without TABTx, in the presence of interfering Wi-Fi transporting UDP traffics generated by D-ITG with different segment payload sizes: 900 bytes (Test 1), 1100 bytes (Test 2), and 1400 bytes (Test 3).

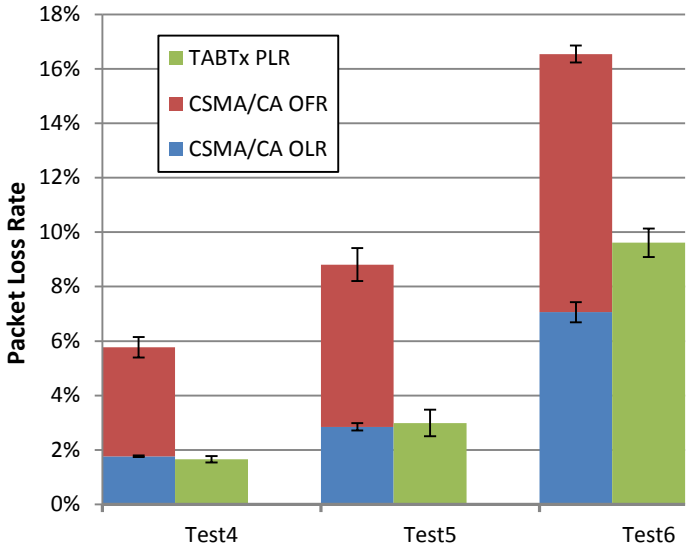

Fig.5.8 ZigBee PLR performance with or without TABTx, in the presence of Wi-Fi transporting UDP traffic generated by D-ITG with 1400 bytes/segment and different generation rates: 500 segments/s (Test 4), 800 segments/s (Test 5), and 1000 segments/s (Test 6)

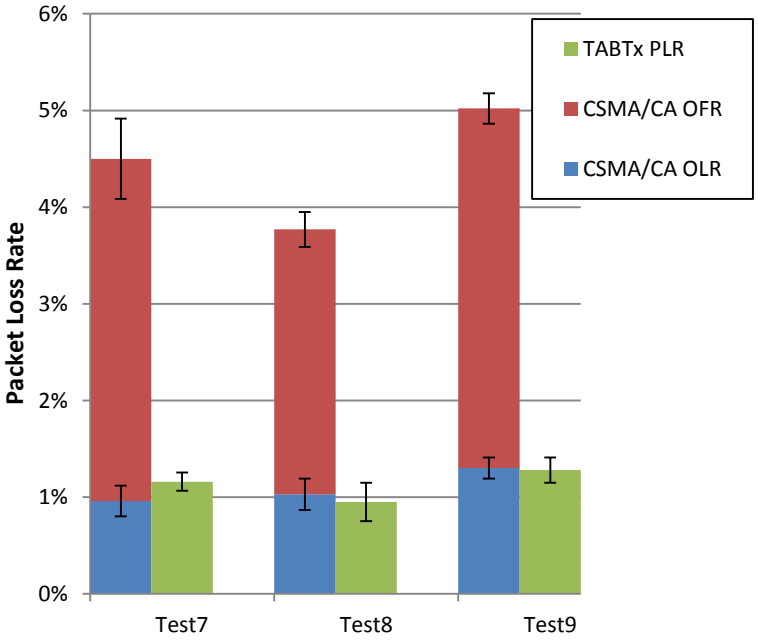

Fig.5.9 ZigBee PLR performances with or without TABTx, in the presence of Wi-Fi transporting UDP traffic generated by D-ITG having segment payload and generation rate following three different random distributions: Poisson (test 7), Uniform (test 8), Gaussian (test 9)

As shown in Figs. 5.7 – 5.9, for the default CSMA/CA, there is a significant portion of packet loss due to TXFIFO overflow (the red portion of the bars). In all tests, the proposed TABTx

mechanism completely avoids the packet drops due to TXFIFO overflow and therefore achieves a better PLR performance. It is also noticed that the PLR of TABTx is slightly higher than the OLR of the default CSMA/CA. This is because without TXFIFO overflow, generally, there will be more packets being sent out, a portion of which could be lost in transmission as result of the Wi-Fi interference.

All experiments in Fig.5.7-5.9 were repeated for another scenario where the ZigBee client mote is sending 50 byte/packets and 100 packets/s. Using equations (5.1) – (5.3) with $T_{data} = 1.6ms$, we get $T_{LMT}(1)$ = 6.7ms and $T_{LMT}(2)$ = 3.2ms. The performance evaluation results compiled by processing the data collect through the experiments are shown in Figs. 5.10 – 5.12.

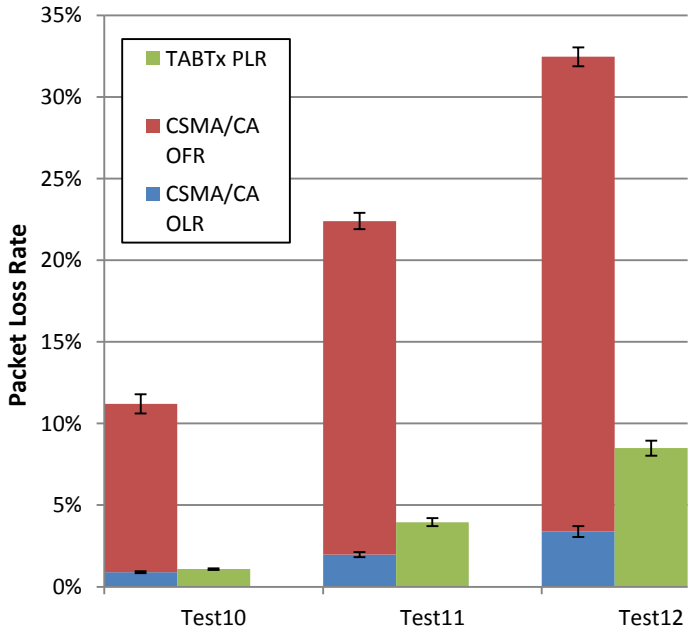

Fig.5.10 ZigBee PLR performances with or without TABTx, in the presence of Wi-Fi transporting UDP traffic generated by D-ITG with different segment payload sizes: 900 bytes (Test 10), 1100 bytes (Test 11), and 1400 bytes (Test 12).

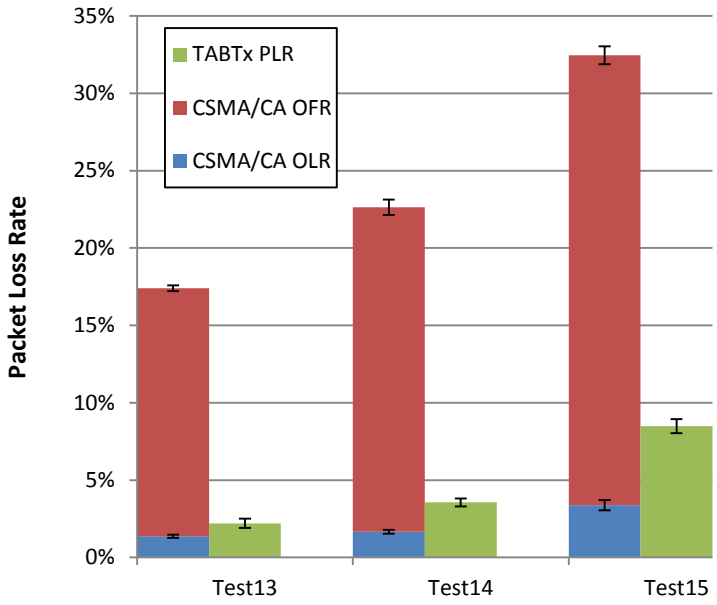

Fig.5.11 ZigBee PLR performance with or without TABTx, in the presence of Wi-Fi transporting UDP traffic generated by D-ITG with different segment generation rates: 500 segments/s (Test 13), 800 segments/s (Test 14), and 1000 segments/s (Test 15)

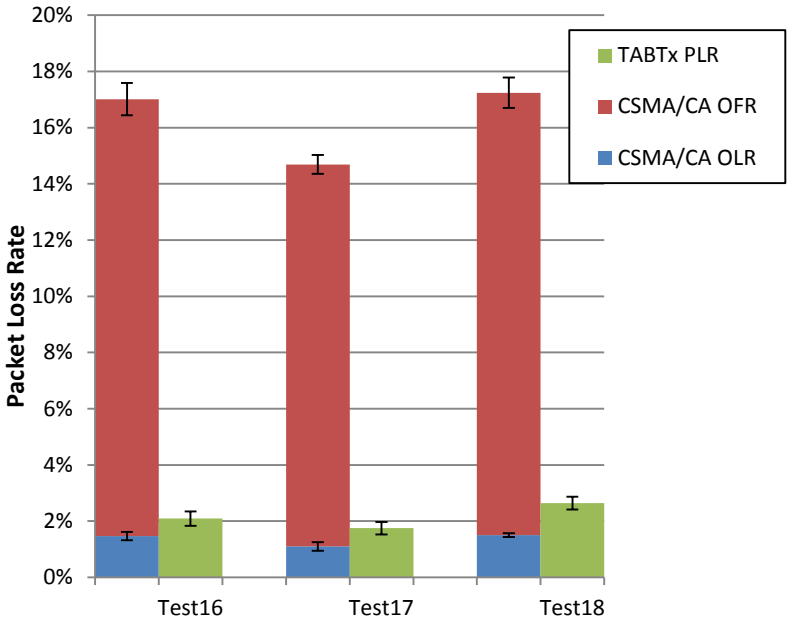

Fig.5.12 ZigBee PLR performances with or without TABTx, in the presence of Wi-Fi transporting UDP traffic generated by D-ITG with different random segment payload sizes and random segment rates

In this set of experiments, due to the shorter ZigBee packet IDT, i.e., 10ms, the default CSMA/CA will have more significant impacts on the packet drops due to TXFIFO overflow. It can be seen from Figs. 5.10 – 5.12, a large portion of packet losses is due to such overflow drops. Since the proposed TABTx is able to avoid TXFIFO overflow, it achieves a much better performance.

The proposed TABTx technique can be applied to applications with different packet sizes and packet rates and is effective when multiple retransmissions are allowed. In addition, this new TABTx technique still uses CSMA/CA and binary exponential backoff algorithm as long as (5.5) can be satisfied, thus ensuring compatibility with existing devices.

Chapter 6

Adaptive Preamble Padding with Retransmission Control Technique

AS mentioned before, earlier studies have shown that the low-power ZigBee based WSNs are vulnerable to the interference generated by closely located nodes of Wi-Fi wireless local area networks (WLAN). Mutual interference can be mitigated at nodes of either technology when ED is enabled in CCA. From our experimental studies on the ZigBee and Wi-Fi coexistence issue we noticed that a significant amount of ZigBee packet losses occur due to Wi-Fi interference induced corruption of the PHY header of ZigBee packets, which could happen even when the ED mechanisms of the Wi-Fi and ZigBee devices are able to detect each other's signal and CSMA/CA algorithms are applied accordingly.

Based on the analysis of our experimental results, it is determined that this phenomenon is due to the hardware's receive to transmit (RX-TX) turnaround time in ZigBee motes. Motivated by this finding, a simple but effective technique named Protective Dummy-byte Preamble Padding (PDBPP) is proposed to improve the performance of ZigBee packet transmission in terms of PLR and transmission efficiency. The experimental performance evaluation results confirmed the effectiveness of PDBPP in terms of improving the PLR and

transmission efficiency of a ZigBee network exposed to interference generated by collocated WLAN nodes.

However, PDBPP cannot adapt to varying Wi-Fi interference. In addition, sometimes PDBPP alone cannot achieve the required reliability for ZigBee packet transmission and therefore needs packet retransmission for the further reduction of PLR. Thus, the Adaptive Preamble Padding with Retransmission Control (APPRC) technique is presented. According to the changing external interference and the required PLR, the proposed APPRC adaptively adds an appropriate number of protective dummy bytes to the ZigBee packet preamble, which reduces packet collisions due to the RX-TX turnaround time in a very efficient manner. Furthermore, APPRC enables packet retransmission when the protective dummy-byte preamble padding alone cannot meet the PLR requirement of the sensing application, or disables it otherwise. The proposed APPRC was implemented on ZigBee devices and its performance was assessed through an extensive set of experiments carried out using our testbed. The experimental results confirmed the superior performance of APPRC technique in terms of transmission efficiency while satisfying the PLR requirements under coexistence conditions.

The remainder of this chapter is structured as follows. In section 6.1, an extension of the testbed setup shown and discussed in Chapter 3, used to study the performance of ZigBee packet transmission when subjected to Wi-Fi interference is introduced, and corresponding experimental results are discussed and analyzed. Section 6.2 elaborates on the PDBPP technique and quantifies its performance improvement via a series of experiments. Section

6.3 presents the APPRC technique and discusses the experimental results for evaluating the ZigBee's performance improvement when applying the APPRC technique.

6.1 Experimental Setup and Results Analysis

Most of the previous studies assumed that ZigBee motes are hidden to Wi-Fi nodes. However, based on the IEEE 802.15.4 and IEEE 802.11 standards, ED can be used by both Wi-Fi and ZigBee to determine the state of the channel. In our testbed, ED is applied by both ZigBee motes and Wi-Fi nodes. Although the low level of ZigBee transmit power (typically 0 dBm or less) has little impact on the performance of communication links between the high power (typically 15dBm - 20dBm) [122] Wi-Fi nodes, it can be detected by the Wi-Fi nodes as long as the strength of the ZigBee signal is above the Wi-Fi CCA ED threshold at the location of the Wi-Fi nodes. When the Wi-Fi node detects energy above its ED threshold, in this case caused by ZigBee packet transmission, it will defer its packet transmission so as to avoid packet collision. However, it was also observed in our experiments that ZigBee transmission could still suffer serious performance degradation even when its signal strength is strong enough to be easily detected by the receiver of a Wi-Fi node. In order to investigate this phenomenon, we extend our testbed setup introduced in Chapter 3.

The study of ZigBee's performance under Wi-Fi interference are carried out for two scenarios, determined by the locations of the interfering Wi-Fi source, i.e., the Wi-Fi router, as illustrated in Figs. 6.1 and 6.2 respectively. For each scenario, the performance of ZigBee

connection was assessed at three different locations of the client mote, corresponding to different distances from the ZigBee coordinator. The relevant locations are indicated as Case 1, Case 2, and Case 3, shown in Figures 6.1 and 6.2. As indicated earlier, the client MICAz mote is acting as the sensor data source and the Wi-Fi router is acting as the source for the Wi-Fi connection, whereas the sink mote is located close to the Dell laptop that is acting as the sink of the Wi-Fi connection. In scenario 1 the Wi-Fi router is located close to Case1, while in scenario 2 it is located close to Case 3.

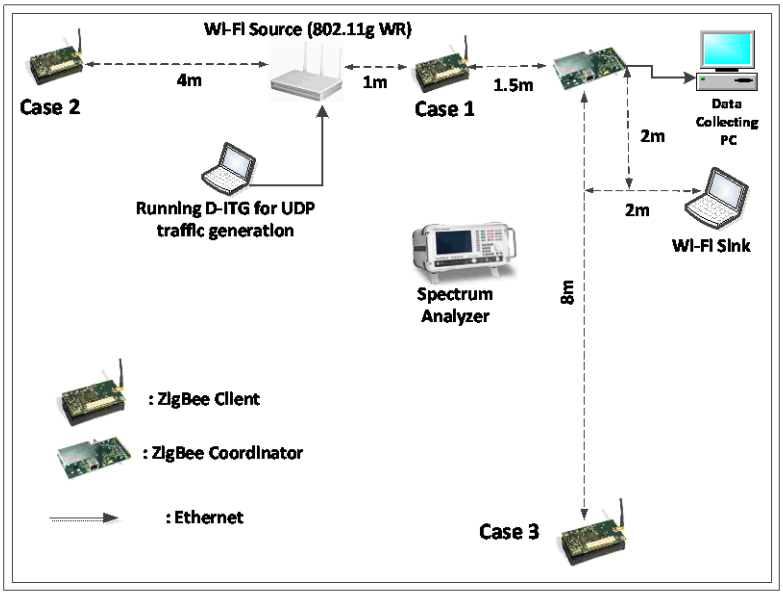

Fig. 6.1 Testbed setup for scenario 1. The Wi-Fi router is located close to the ZigBee mote at the location of Case 1.

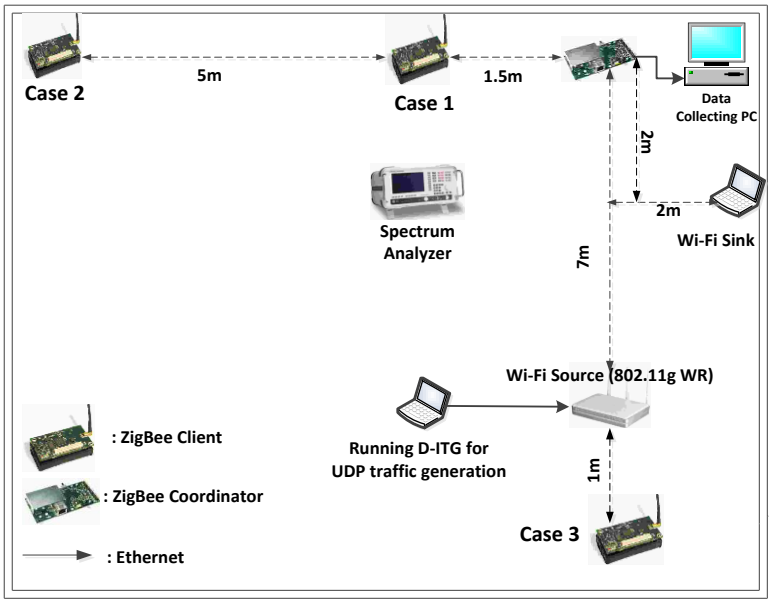

Fig. 6.2 Testbed setup for scenario 2. The Wi-Fi router is located close to the ZigBee mote at the location of Case 3.

Periodic monitoring applications, where the ZigBee client mote generates data traffic with constant packet rate and packet length, are considered. The ZigBee client mote is programmed to send out 100-byte packets at 20ms interval. The D-ITG traffic generator running on the Toshiba laptop generates interfering UDP traffic with segment payload size of 1400 bytes and constant segment IDT at the rate of 500 segments/second, which is then converted to IEEE 802.11g Wi-Fi interference by WR. Our customized ZigBee coordinator firmware calculates the total number of ZigBee packet losses and the number of packet losses due to Cyclic Redundancy Check (CRC) failures. After receiving a data packet, the ZigBee coordinator performs a CRC check to verify that the packet was not corrupted in transmission. The data packet is dropped if the CRC indicates the packet was corrupted. Fig.

6.3 depicts the experimental results. All the data points are marked with a 95% confidence interval.

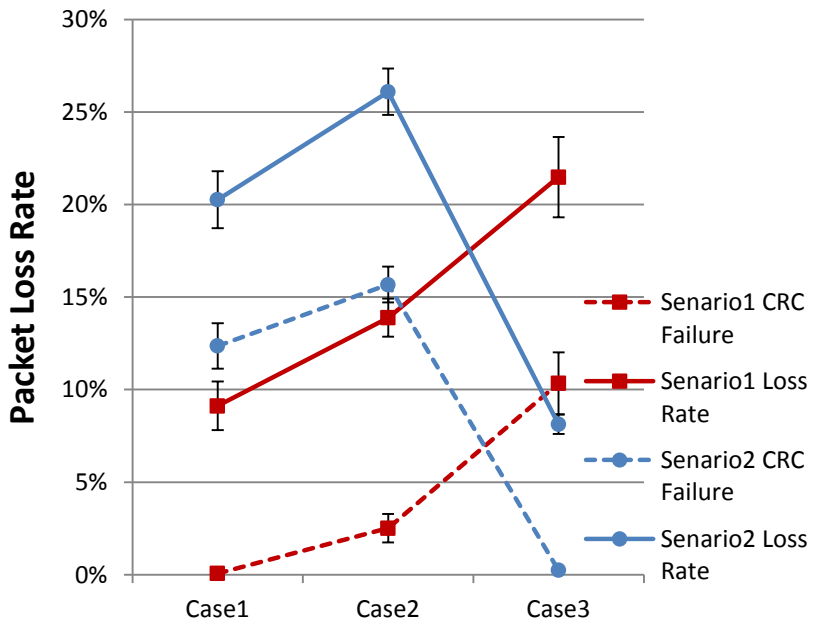

Fig. 6.3 Performance comparison of ZigBee packet transmission under interfering IEEE 802.11g traffic for different test scenarios and cases

The experimental results show that the interfering IEEE 802.11g traffic has substantial impact on ZigBee's packet loss performance. In scenario 1 (Fig.6.1), as the distance between the ZigBee transmitter and the ZigBee sink increases, i.e., from Case 1 to Case 3, the packet loss rate increases. It is evident that the SINR is decreasing when the ZigBee transmitter is moving further away from the sink, which consequently leads to higher packet loss rate.

However, it is observed in scenario 2 that Case 3 achieved the best performance despite the fact that it is located the farthest from the sink. Another interesting observation is that there is significant difference between the number of CRC failures and that of the total packet losses. As introduced in Chapter 3, Packet loss can happen for three different

reasons: 1) Packet cancellations due to CCA detection failures; 2) Packet losses due to collisions with interfering Wi-Fi traffic; and 3) Packet drops due to CC2420 TXFIFO overflow. According to the collected and processed experimental data, the number of packet transmission cancellations due to CCA detection failures is less than 10 out of over 10000 packet transmission attempts (i.e. a packet cancellation rate of less than 10^{-3}). Also there is no TXFIFO overflow packet dropping since packet retransmission is not applied at the transmitting mote in these experiments. Therefore, the packet losses are mostly due to collisions with interfering IEEE 802.11g traffic. Since the 2-byte frame check sequence (FCS) following the last MAC payload byte is calculated over the MAC Protocol Data Unit (MPDU), it can be concluded that the difference between the number of CRC failures and that of total packet losses are due to corrupted SHR or PHR instead of corrupted PSDU.

Based on the above discussion, the better performance of Case3 in scenario2 can be attributed to the sensitivity of the ED (-75dbm) at the WR. Since the ZigBee mote is transmitting packets at a considerably lower power, WR's ED function can better detect the ZigBee transmission when the ZigBee transmitter is closer, and effectively apply CSMA/CA to avoid collision. On the other hand, the WR's ED is not as effective when the WR is located farther away from the ZigBee transmitter and the collisions between interfering Wi-Fi traffic and ZigBee traffic degrade the performance of ZigBee packet transmission.

The experiments are carried out in a laboratory environment. Thus the ITU model [123] for indoor attenuation is adopted for estimating the distance within which Wi-Fi ED can be effective. The ITU indoor path loss model is expressed as:

$$L = 20\log f + N * \log d + P_f(n) - 28 \quad (6.1)$$

where *L* is the total path loss (dB), *f* is the frequency of transmission (MHz), *d* is the distance (m), *N* is the distance power loss coefficient, *n* is the number of floors between the transmitter and receiver, and $P_f(n)$ is the floor loss penetration factor. Based on [123], we adopt the *N* value for office area with operating frequency of 1.8-2 GHz (which is the closest value to the ZigBee operating frequency of 2.4GHz), i.e. *N* = 30. There is no effect of floor penetration, thus $P_f(n)$ = 0. In our testbed, the ZigBee mote is transmitting at 0dBm and the ED threshold for the WR is -75dBm. Therefore, it can be derived from (6.1) that the WR is able to detect the ZigBee packet transmission if the distance between the ZigBee mote and WR is not more than 15m approximately. When WR and ZigBee mote successfully detect packet transmission from each other, they will then apply CSMA/CA for collision avoidance. However, it is noticed that in our experiments, even when the ZigBee transmitter is located very close to the WR, there is still a significant number of packet losses. Although it can be seen from Fig. 6.3 that packet losses due to CRC failures are close to zero when the ZigBee transmitting mote is located very close to the WR (see Case 1 in scenario 1 and Case 3 in scenario 2), there is still a substantial number of packet losses due to corrupted SHR or PHR.

6.2 PDBPP Technique: Description and Evaluation

6.2.1 PDBPP Technique

According to the IEEE 802.15.4 standard, there exists a RX-TX turnaround time between the completion of ED and the start of ZigBee packet transmission, as illustrated in Fig. 6.4. Although this time interval is short (12-symbol duration or around 0.2ms [111]), it can still cause a significant number of misjudgments of the channel state at WR, especially when the Wi-Fi packet rate is high. If the WR performs ED during this turnaround time, it will determine the channel is idle and start to transmit the Wi-Fi packet. This Wi-Fi packet will collide with the ZigBee packet sent out after the turnaround time. We call this type of collision turnaround time collision. Due to the relatively short Wi-Fi packet transmission time (e.g. around 0.25ms for transmitting an IEEE 802.11g packet with 1400-byte UDP payload), this type of collision mostly corrupts the SHR and PHR of the ZigBee packet, resulting in the packet to be lost in the air without being received and processed by the receiving mote. This scenario is depicted in Fig. 6.4.

Based on these observations and analysis, we propose to add protective dummy bytes to the ZigBee packet preamble so as to protect the header which contains the essential information from turnaround time collisions (illustrated in Fig. 6.4). For the convenience of description, we hereafter refer to this technique as Protective Dummy-byte Preamble Padding (PDBPP). PDBPP is implemented as firmware in the MICAz motes and experiments have been performed to evaluate its performance.

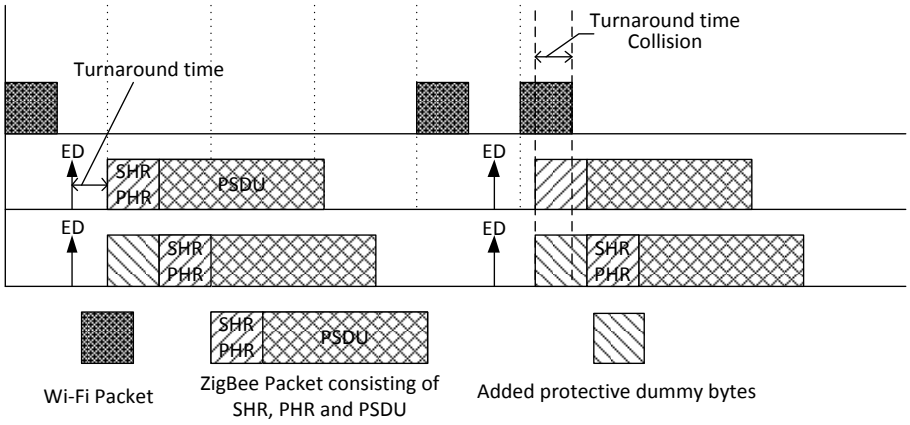

Fig. 6.4 Wi-Fi packet collides with ZigBee packet when starting transmission during RX-TX turnaround time.

6.2.2 Performance Evaluation Results and Discussion

To evaluate the performance of ZigBee packet transmission when adopting the PDBPP technique, a series of experiments were carried out using our testbed setup shown in the Case 1 of scenario 1 (Fig. 6.1). In this case, the WR is closely located to the ZigBee transmitter so that it is able to detect easily the ZigBee packet transmission signal and perform CSMA/CA accordingly for avoiding collisions.

Since protective dummy bytes have been added to the preamble, transmission efficiency, defined as the ratio of effective PHY payload received to the total data transmitted, is also evaluated in the experiments in addition to the packet loss rate. Denoting by L_Z the ZigBee packet length, L_{PSDU} the PHY payload size, P_L the ZigBee packet loss rate, N_P the number of packets that needs to be transmitted, and N_{Total} as the total number of transmitted packets including retransmitted packets, the transmission efficiency can be calculated as:

$$E = \frac{(1-P_L) \bullet N_P \bullet L_{PSDU} / L_Z}{N_{Total}} \tag{6.2}$$

Same as previous experiments, the D-ITG is set to generate interfering UDP segments having constant payload size of 1400 bytes and segment rate of 500 segments/second. Figs. 6.5 and 6.6 show the results for constant ZigBee traffic with 100 bytes/packet and 20 packets/second, and Figs. 6.7 and 6.8 show the results for constant ZigBee traffic with 100 bytes/packet and 50 packets/second. In all figures, performance evaluation results for different number of protective dummy bytes are shown, i.e., 0 (no dummy-byte padding), 4, 8, and 13 bytes. In addition, the performance evaluation results for ZigBee packet transmission with the maximum number of packet retransmission set to 1 and our previous proposed ACK-ID scheme are also illustrated for comparison purpose. Again, all the data points are marked with a 95% confidence interval.

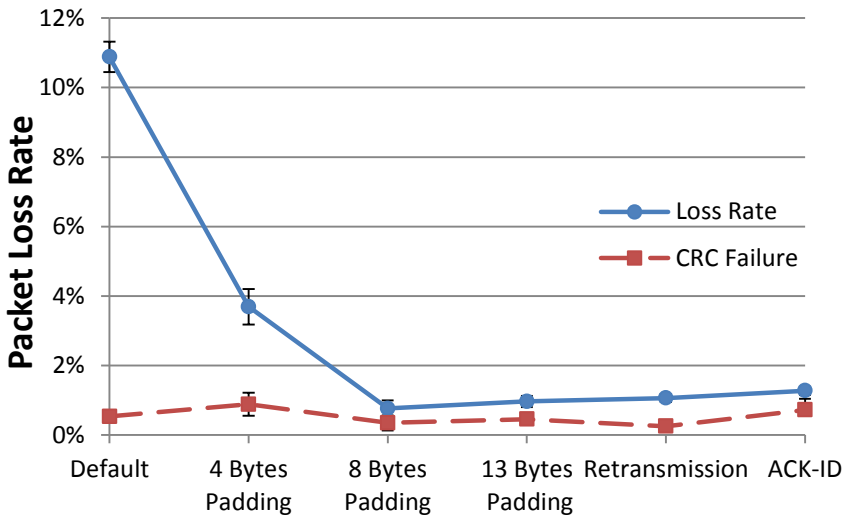

Fig. 6.5 Packet loss rate comparison of ZigBee packet transmission at 20 packets/second with different number of protective dummy bytes under interfering IEEE 802.11g traffic

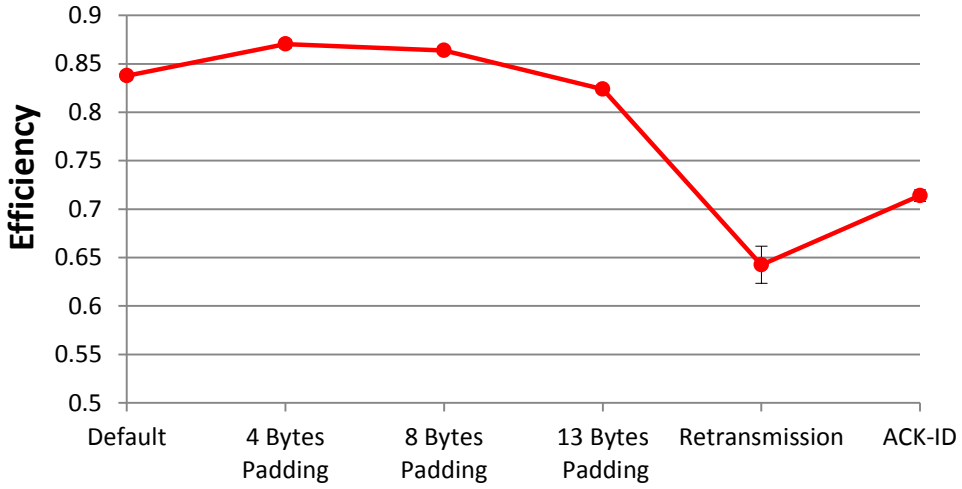

Fig. 6.6 Transmission efficiency of ZigBee packet transmission at 20 packets/second with different number of protective dummy bytes under interfering IEEE 802.11g traffic

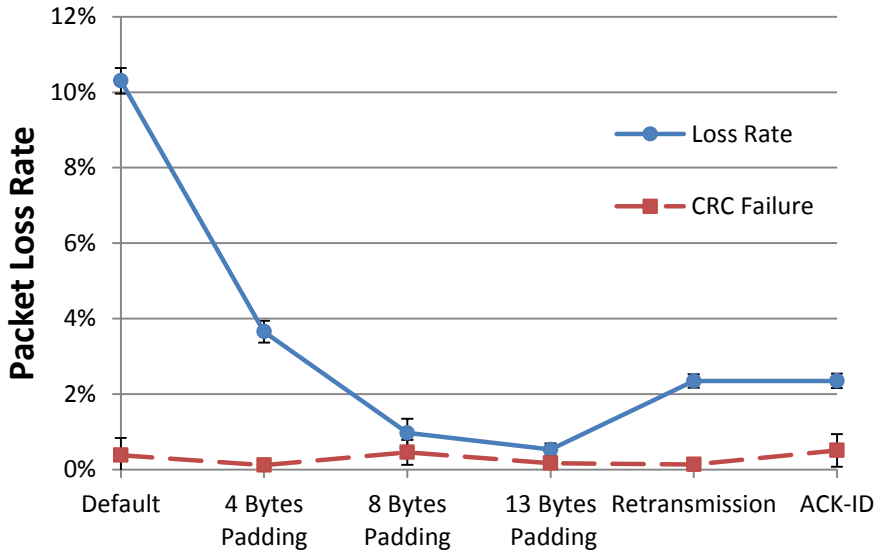

Fig. 6.7 Packet loss rate comparison of ZigBee packet transmission at 50 packets/second with different number of protective dummy bytes under interfering IEEE 802.11g traffic

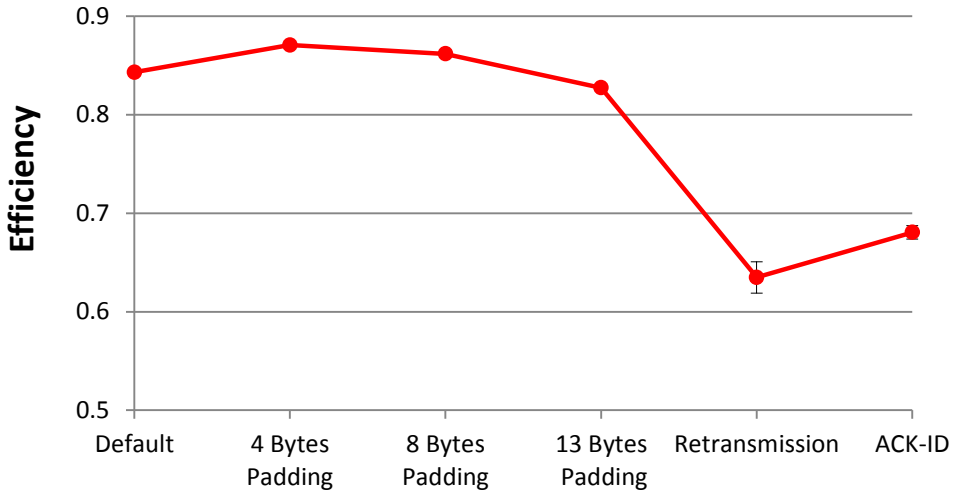

Fig. 6.8 Transmission efficiency of ZigBee packet transmission at 50 packets/second with different number of protective dummy bytes under interfering IEEE 802.11g traffic

Figs. 6.5-6.8, it can be seen that PDBPP provides a simple but very effective way to improve the performance of ZigBee packet transmission when there is Wi-Fi interference close by. It can largely prevent the ZigBee SHR and PHR from being corrupted by the interfering Wi-Fi packets so as to reduce the packet loss. In addition, although adding protective dummy bytes to preamble introduces more overhead to the packet transmission, the reduction in the number of lost packets can largely offset the impact of padding and maintain high transmission efficiency.

Since the maximum IEEE 802.11g MPDU size is 2346 bytes, the channel occupation time for an IEEE 802.11g packet will not exceed 0.4ms. In our testbed, the IEEE 802.11g traffic is generated by the D-ITG running on the laptop that is connected to the Ethernet port of the WR, thus the maximum size of the Wi-Fi packet is even smaller, limited by the Ethernet MTU of 1500 bytes. For the IEEE 802.11g packet with UDP payload size of 1400 bytes used in our experiments, it has duration of around 0.25ms. In the worst case when the Wi-Fi

packet is sent out at the end of the turnaround time, it can at most overlap with around 8 bytes of ZigBee packet transmitted at 250kbps. It can be seen from Figs. 6.5 – 6.8 that it is the most effective to add 8 dummy bytes to the preamble and preamble padding of over 8 bytes is of little use, which is consistent with our analysis.

To further verify the effectiveness of the proposed PDBPP technique, the performance comparison is performed for mechanisms that involve packet retransmission, which can also effectively reduce the PLR. With retransmission, the source mote waits for receiving acknowledgement (ACK) from the coordinator after each packet transmission. If no ACK is received within a set time frame, the source mote concludes the packet is lost and retransmits the packet once. In addition to the default retransmission mechanism, our previously proposed ACK-ID technique, which reduces a significant number of redundant packet retransmissions due to lost ACKs, is also evaluated. Compared to the retransmission mechanisms, PDBPP not only performs better in terms of PLR but also achieves significantly better transmission efficiency when the Wi-Fi interference is closed by. In addition, although PDBPP adds several redundant bytes, it saves the power consumption of receiving the 10-byte ACK. In other words, for packet retransmission mechanisms, the relatively low PLR comes with the penalty of a much higher overhead. Particularly, for the retransmission mechanisms, the time for completing a ZigBee packet transmission might include the time for both packet transmission and retransmission, ACK waiting, CCA detections, and a number of backoffs. This time duration might well exceed the time interval for generating the next ZigBee packet at the transmitting mote. Consequently, the newly generated/arrival packet might be dropped due to the TXFIFO overflow in sending out the preceding packet.

In cases when ZigBee mote is transmitting at high packet rates (e.g. 50 packets/second, for which results are shown in Figs. 6.7 and 6.8), the retransmission mechanisms might incur TXFIFO overflow packet drops, resulting in a higher PLR. The PDBPP technique is proven to be even more efficient in such circumstances.

The extensive experiments carried out in our testbed evaluated and validated the performance improvement of our PDBPP scheme. It is demonstrated from the experimental results and discussion that PDBPP technique can significantly improve the performance of ZigBee packet transmission in terms of packet loss rate and transmission efficiency when there is interference generated by the collocated WLAN. The proposed technique is particularly useful when ZigBee motes are transmitting at high packet rates. Last but not least, the proposed method is very simple for implementation without much computation and memory overhead, which is ideal for low power and low cost wireless sensor nodes.

6.3 APPRC Technique: Description and Evaluation

As described in the above section, we proposed PDBPP technique that adds protective dummy bytes to the ZigBee packet preamble so as to protect the SHR/PHR from the turnaround time collision. However, PDBPP is not able to adjust the size of dummy bytes padding when the external interference varies. Furthermore, once Wi-Fi CCA cannot accurately detect ZigBee packet transmission (e.g. Case 3 in scenario 1), the preamble padding alone may not be able to guarantee the PLR requirement of sensing applications.

Thus, in this section, APPRC technique is presented that significantly enhances the performance of PDBPP.

6.3.1 APPRC Technique

Compared to PDBPP, APPRC flexibly adapts to the varying external interference and the required PLR of different sensing applications by adding an appropriate number of protective dummy bytes to the ZigBee packet preamble so as to more efficiently reduce the turnaround time collisions. When the external interference is too strong or the Wi-Fi CCA cannot accurately detect ZigBee packet transmission and consequently the preamble padding alone cannot meet the PLR requirement of sensing applications, APPRC enables packet retransmission for further improving the PLR performance of ZigBee system. This is achieved at the unavoidable expense of sacrificing transmission efficiency, which is defined as the ratio of effective PHY payloads content received to the total data transmitted.

Our custom-made ZigBee coordinator firmware periodically calculates the number of total packet losses and the number of the packet losses due to CRC failures in the first transmission attempt, and sends the values to the ZigBee client. The ZigBee client mote then calculates the corresponding PLRs denoted as PLR_{total} and PLR_{CRC}, respectively, and starts APPRC algorithm illustrated in the flow chart shown in Fig. 6.9.

The term *macMaxFrameRetrie*s appearing in Fig. 6.9 represents the maximum number of retries allowed after a transmission failure as defined in the standard [30]. When the set value is 0, packet retransmission is disabled. When packet retransmission is used in the ZigBee device, $1 \le macMaxFrameRetries \le MaxRetries$, with *MaxRetries* representing the

largest number of retransmissions the ZigBee system allows. PLR_{app} denotes the required PLR of a specific sensing application of interest.

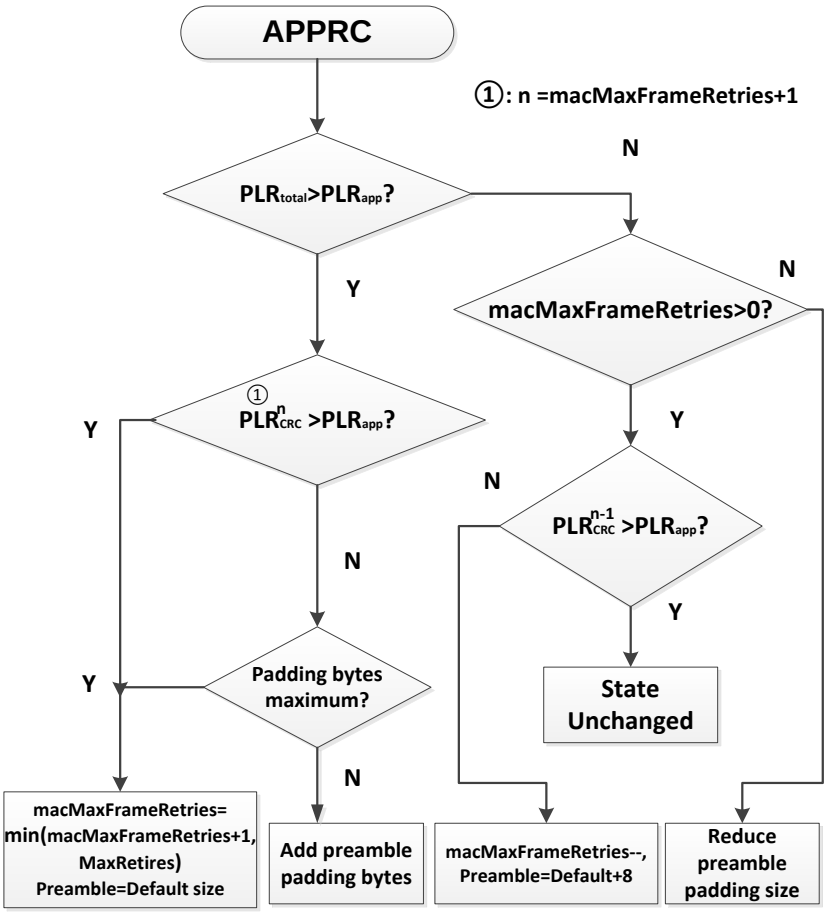

Fig. 6.9 Flow chart of APPRC

The transmitting mote compares the PLR_{total} to the required PLR_{app}. If PLR_{total} is higher than PLR_{app}, APPRC needs to take action to further reduce PLR_{total} in order to meet the application's PLR requirement. Since preamble padding is more efficient than packet retransmission especially under high Wi-Fi interference, APPRC chooses to add protective padding bytes to packet's preamble before increasing the macMaxFrameRetries. However, it is known from section 6.2 that preamble padding cannot reduce PLR_{CRC}. Therefore, APPRC should increase *macMaxFrameRetries* without trying for different size of preamble padding

if PLR_{CRC}^{n}, the RLR due to CRC error after *n* retries, is found to be higher than PLR_{app}. This comparison speeds up the APPRC algorithm in finding the optimal solution for meeting the PLR requirement. Otherwise, APPRC will fine-tune the number of preamble padding bytes, i.e., increase padding bytes from 0 to 4, 4 to 8, and then 8 to 13. The maximum supported preamble size of MICAz mote is 17 bytes, while 4-byte is the default preamble size defined in the IEEE 802.15.4 standard.

On the other hand, if PLR_{total} is lower than PLR_{app}, i.e., meets the PLR requirement, the algorithm will check to see if there is any possibility to improve transmission efficiency by reducing the packet retransmission and the number of preamble padding bytes. Again, APPRC first attempts to reduce *macMaxFrameRetries*, which is only possible when PLR_{CRC}^{n-1} is lower than PLR_{app} as preamble padding cannot reduce PLR_{CRC}. If the packet retransmission has already been disabled, APPRC starts a process that is trying to reduce the number of padding bytes. APPRC records the results of the next *N* (e.g. 200) CCA ED detections. If the CCA failure rate is lower than a set threshold T_{CCA_fail} (e.g. 5%), indicating that the channel quality has improved or the interference has disappeared, APPRC fine-tunes the number of preamble padding bytes in a reversed order, i.e., decrease the number of padding bytes from 13 to 8, 8 to 4, and 4 to 0.

Compared to packet retransmission, preamble padding provides a simpler, more efficient and effective way to improve the performance of ZigBee packet transmission when there is interference generated by close by Wi-Fi nodes. Thus, the proposed APPRC enables the ZigBee transmitter to autonomously select a more efficient way, which allows determining and using the appropriate number of preamble padding dummy bytes or packet

retransmissions, for achieving higher transmission efficiency while satisfying the PLR requirement. APPRC was implemented on ZigBee devices and its performance was assessed through an extensive set of experiments carried out using our testbed. The experimental results confirmed the superior performance of APPRC technique under coexistence conditions, in terms of transmission efficiency, while satisfying the PLR requirements. Those results are presented and discussed in the next section.

6.3.2 Performance Evaluation Results and Discussion

A series of experiments have been carried out in the testbed setup of scenario 1, shown in Fig. 6.1, for evaluating the performance improvement of ZigBee packet transmission when adopting APPRC technique. For comparison, ZigBee's performance was also evaluated when the ZigBee client mote transmits without either preamble padding or packet retransmission (NPPRT), and when macMaxFrameRetries is set to 1 for allowing one retransmission (PRT). The ZigBee client mote was placed in three different locations with respect to the Wi-Fi WR, illustrated in Fig. 6.1 as Case 1, Case 2, and Case 3, respectively, and for each case, a full set of experiments were performed. Periodic monitoring applications, where the ZigBee client mote generates data traffic with constant packet rate and packet length, are considered. The ZigBee client mote is programmed to send out 100-byte packets at 30ms interval. Without loss of generality, the required PLR is set to be 3%. In the experiments, we evaluate both PLR and transmission efficiency (defined in section 6.2.2).

The performance of ZigBee packet transmission is evaluated under different interfering Wi-Fi traffic. The experimental results are shown in Figs. 6.10-6.15 with all the data points

marked with a 95% confidence interval. In Figs. 6.10 and 6.11, the D-ITG traffic generator running on the Toshiba laptop generates interfering UDP traffic with segment payload size of 1400 bytes and constant segment IDT at the rate of 500 segments/s, which is then converted to IEEE 802.11g Wi-Fi interference by WR. It can be seen from Fig. 6.10 that without preamble padding and packet retransmission, NPPRT has the worst PLR which doesn't come close to the required PLR of 3%. In all three cases, APPRC maintains the PLR to be lower than 3%. Although in cases 1 and 2 PRT has better PLR than APPRC, it can be seen from Fig. 6.11 that APPRC achieves considerably higher transmission efficiency than PRT. When compared to NPPRT in Case 1, APPRC not only has better PLR but also exceeds NPPRT in transmission efficiency. This is because although APPRC adds more dummy bytes to the packet preamble, it achieves considerably higher successful packet delivery than NPPRT. In Case 3, PRT with one retransmission can only achieve a PLR of about 4%, while APPRC not only has better PLR but also achieves higher transmission efficiency than PRT. Increasing PRT's macMaxFrameRetries can further reduce its PLR for meeting the PLR requirement of 3%, but in the meantime will worsen the transmission efficiency. On the other hand, APPRC uses preamble padding for satisfying the PLR requirement whenever possible and adopts packet retransmission for further reducing PLR only when preamble padding alone cannot meet the PLR requirement. Obviously, by using both preamble padding and packet retransmission, APPRC can achieve a lower PLR than PRT. And by using preamble padding, APPRC achieved better successful packet delivery rate for both original and retransmitted packets, thus resulting in less retransmissions and higher transmission

efficiency. This clearly demonstrates that APPRC is able to reduce the PLR in a more efficient way.

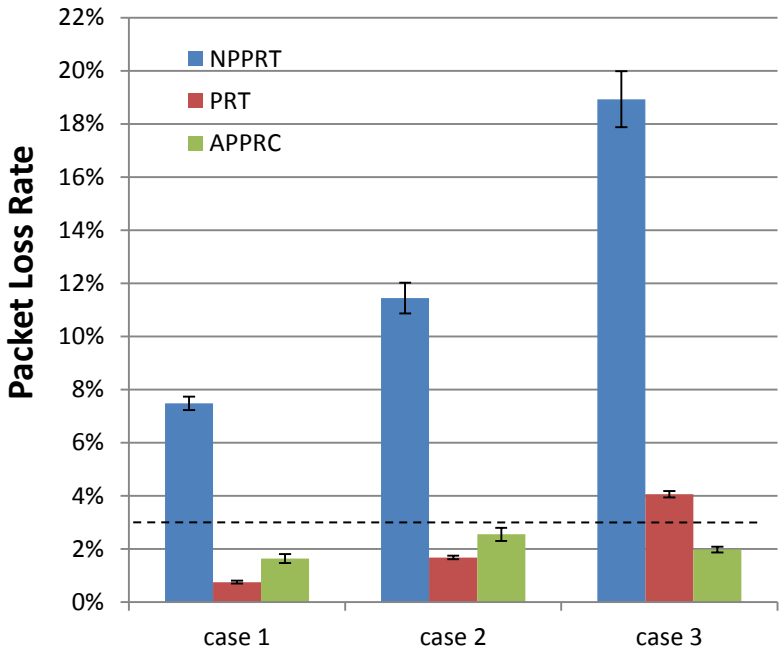

Fig. 6.10 Packet loss rate comparison of ZigBee packet transmission, in the presence of interfering UDP traffic with segment payload size of 1400 bytes/segment and segment rate of 500 segments/s

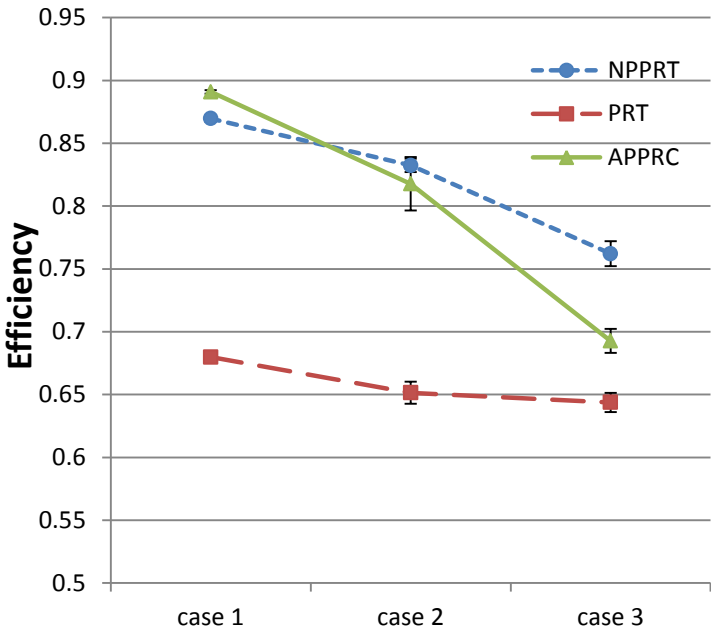

Fig. 6.11 Transmission efficiency comparison of ZigBee packet transmission, in the presence of interfering UDP traffic with payload size of 1400 bytes/segment and segment rate of 500 segments/s

In Figs. 6.12 and 6.13, the D-ITG is set to generate UDP segment sequences having constant segment IDT at the rate of 800 segments/s and payload sizes following the Uniform distribution between 900 to 1400 bytes. This time the interfering Wi-Fi traffic became heavier, thus resulting in more packet losses and reduced transmission efficiency for all three schemes. Similar to the pervious set of experiments, APPRC satisfies the PLR requirement in all cases and achieves much better performance than NPPRT and PRT. Compared to NPPRT, APPRC achieves substantial improvement in PLR at some expense (only in Cases 2 and 3) of transmission efficiency. Compared to PRT, APPRC achieves significantly better transmission efficiency.

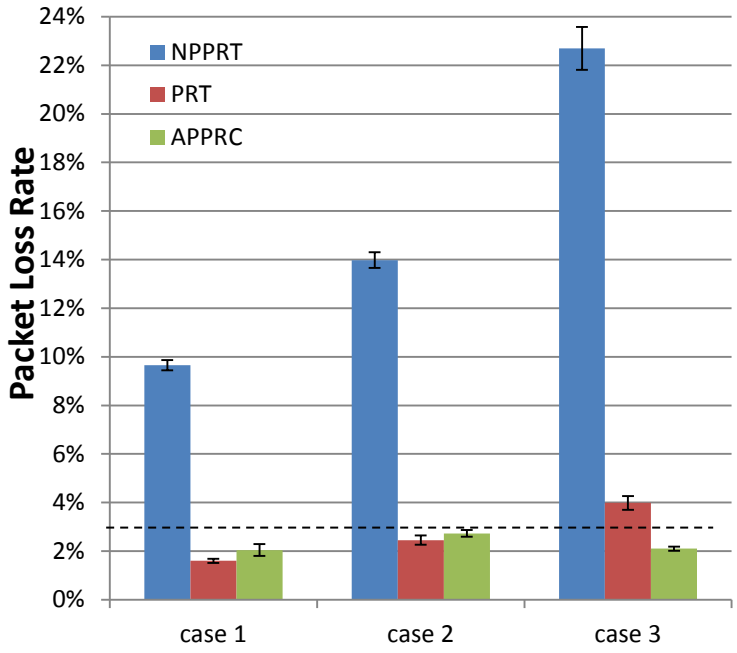

Fig. 6.12 Packet loss rate comparison of ZigBee packet transmission, in the presence of interfering UDP traffic with random segment payload sizes following Uniform distribution and segment rate of 800 segments/s

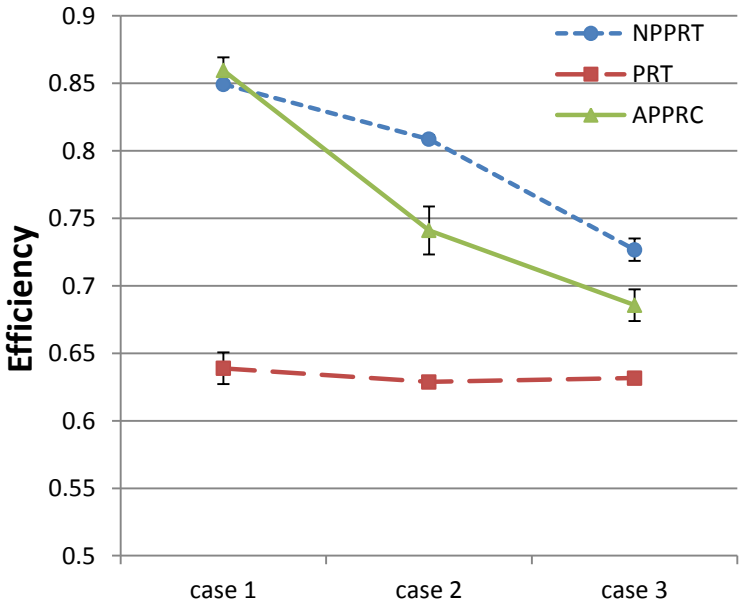

Fig. 6.13 Transmission efficiency comparison of ZigBee packet transmission, in the presence of interfering UDP traffic with random segment payload sizes following Uniform distribution and segment rate of 800 segments/s.

Additional experiments have been performed to address the effectiveness of APPRC under changing Wi-Fi interference. In each of these experiments, D-ITG first generates interfering UDP traffic with segment payload size of 900 bytes/segment at 500 segments/s, then changes to 1400 bytes/segment at 800 segments/s half way through the experiment. That is, the Wi-Fi WR transmits traffic consisting of an equal combination of two traffic patterns, with UDP segment payload size of 900 bytes/segment and segment rate of 500 segments/s in the first half of the experiment, and then changes to 1400 bytes/segment and 800 segments/s for the remaining half. Figs. 6.14 and 6.15 show that APPRC deals with the varying interference quite well and maintains high transmission efficiency while satisfying the required PLR.

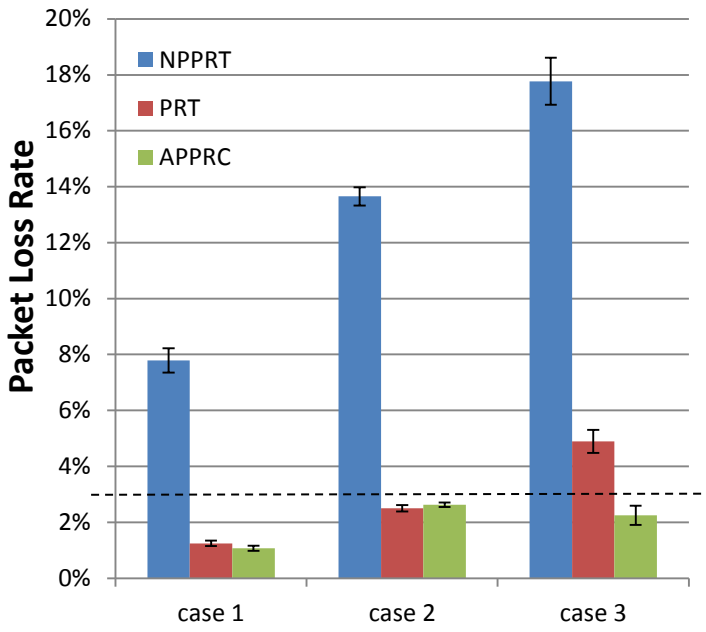

Fig. 6.14 Packet loss rate comparison of ZigBee packet transmission, in the presence of interfering UDP traffic consisting of two different segment payload sizes and segment rates

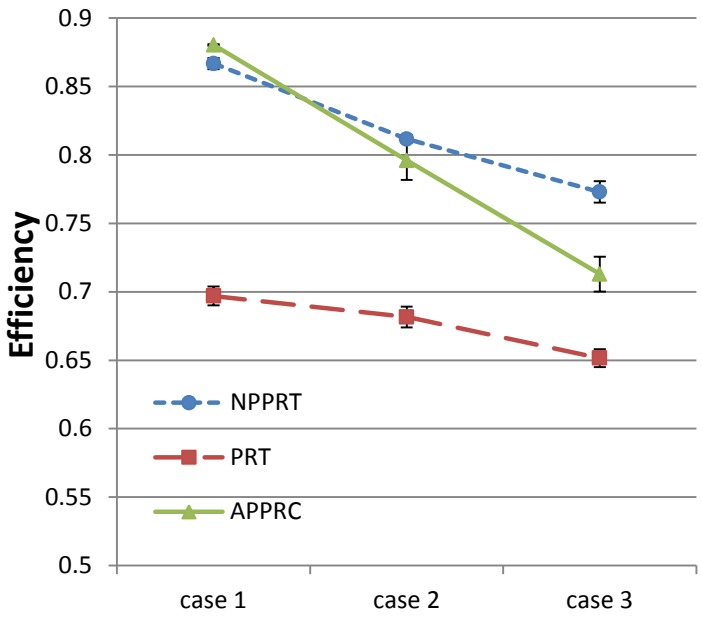

Fig. 6.15 Transmission efficiency comparison of ZigBee packet transmission, in the presence of interfering UDP traffic consisting of two different segment payload sizes and segment rates

From Figs. 6.10-6.15, it can be seen that APPRC is very effective in improving the performance of ZigBee packet transmission when there is Wi-Fi interference close by. Padding ZigBee packet's preamble can largely prevent the ZigBee SHR and PHR from being corrupted by the interfering Wi-Fi packets. Although such padding bytes introduce more overhead to the packet, the reduced number of lost packets can offset such negative impact and maintain high transmission efficiency. Generally, preamble padding is more efficient than packet retransmission in reducing PLR as shown in our previous research work. In case when ZigBee packet transmission is experiencing severe interference and preamble padding alone cannot satisfy the PLR requirement, packet retransmission should be adopted. APPRC efficiently adapts to the changing interference by determining the size of dummy-byte for preamble padding adaptively and whether or not to adopt packet retransmission. Therefore, APPRC significantly improves ZigBee packet transmission

efficiency by using preamble padding whenever possible, and can further reduce PLR by adopting packet retransmission when necessary.

In this section, a novel and efficient Adaptive Preamble Padding with Retransmission Control (APPRC) technique was proposed to improve the performance of ZigBee packet transmission under Wi-Fi interference. In order to meet the packet loss rate requirement of a specific sensing application, APPRC is able to adapt to varying Wi-Fi interference, determining the appropriate number of dummy bytes for preamble padding adaptively and whether or not to adopt packet retransmission. The performance improvement when adopting APPRC has been validated and evaluated through extensive experiments carried out in our testbed. APPRC technique can significantly improve the ZigBee packet transmission efficiency by using preamble padding for satisfying the PLR requirement whenever possible, and can further reduce PLR with packet retransmission when ZigBee mote is experiencing severe interference generated by collocated WLANs and preamble padding alone cannot meet the PLR requirement. In addition, APPRC has been implemented and tested using off-the-shelf ZigBee motes, which proves that the proposed technology is easily implementable and fast deployable, and can be a very valuable upgrade to the current ZigBee devices.

Chapter 7

Conclusions and Future Work

IN this thesis, extensive experiments have been performed to study the performance degradation of ZigBee packet transmission when subjected to interference generated by collocated Wi-Fi network operating in overlapping channels. Several important factors that severely impact the reliability and efficiency of ZigBee packet transmission have been identified in the study. Based on these findings, novel technologies were designed and implemented. They improve the energy, bandwidth, and data transmission efficiency of ZigBee motes. The main contributions of this thesis are:

- Our experimental study shows that a significant number of ACK packets are lost because of Wi-Fi interference, leading to excessive retransmissions and substantial waste of bandwidth and energy. In order to reduce the ACK losses and avoid redundant packet retransmissions, a novel ACK with Interference Detection (ACK-ID) technique has been developed, in which channel assessment is applied before each ACK transmission. It is demonstrated from our performance evaluation results that ACK-ID can significantly improve the performance of ZigBee packet transmission by reducing the packet retransmission rate and increasing the ACK delivery rate when there is varying interference from the collocated WLAN.
- In order to save energy for transmitting ZigBee packets while maintaining satisfactory PLR, we proposed and implemented an Adaptive Transmit Power Adjustment (ATPA)

technique that continuously assesses the channel quality based on the measured PLR and adaptively adjusts the optimal transmit power accordingly for meeting the PLR requirement. The experimental performance evaluation results verified the effectiveness of ATPA in reducing energy consumption while meeting the PLR requirement.

- The delay due to CSMA/CA backoffs could result in TXFIFO buffer overflow, causing packet drop without having made any transmission attempt. In order to eliminate such packet losses, we proposed the Time Aware Backoff and Transmission (TABTx) technique that controls the time spent on each packet transmission including the retransmission attempts. The experimental results show that our TABTx technique completely avoids the TXFIFO overflow and consequently reduced the PLR.
- The RX-TX turnaround time between the completion of ED and the start of ZigBee packet transmission could cause a significant number of misjudgments of the channel state at the Wi-Fi transmitter, which consequently lead to packet collisions that corrupt the PHY header of the ZigBee packet. We proposed to add protective dummy bytes to the ZigBee packet preamble so as to protect the header from such turnaround time collisions. Furthermore, a novel technique named Adaptive Preamble Padding with Retransmission Control (APPRC) has been proposed and implemented in Micaz motes. APPRC determines the appropriate number of protective dummy bytes and whether or not to adopt packet retransmission according to the changing Wi-Fi interference. Consequently, APPRC significantly improves ZigBee packet transmission efficiency while satisfying the PLR requirement.

The contributions in this thesis can lead to a number of meaningful topics for future research.

- **Integrate the proposed interference mitigation techniques.** Different performance improvement techniques proposed in this thesis address different issues under ZigBee-Wi-Fi coexistence, e.g. ACK-ID for ACK loss, ATPA for transmission power adaptation, TABTx for CSMA/CA backoff delay, and APPRC for turnaround time collision. It could be very meaningful to jointly apply these techniques to the ZigBee system for further performance improvements, study the combination effect and apply possible joint optimization. As a starting point, we studied the ATPA in conjunction with ACK-ID, which has been proven to be more energy efficient. It is expected that more significant performance improvement can be achieved by jointly optimizing the techniques.
- **Application of TABTx to multi-hop delay constraint WSN.** Most delay constraint algorithms for multi-hop WSNs are based on hop count measurement [124]. However, with the default CSMA/CA mechanism and unreliable wireless medium subjected to noise and interference, the delay of each hop could fluctuate significantly due to variation in retransmission and CSMA/CA delay caused by varying wireless channel conditions. As discussed in Chapter 5, our proposed TABTx provides strict delay control for each hop. Therefore, by applying the same or similar ideas, it is possible to design more accurate delay constraint algorithms for multi-hop WSN under Wi-Fi interference.
- **End-to-end performance study for different WSN network topologies.** In this thesis research, we focused on MAC/PHY layer techniques for improving ZigBee packet transmission performance between two ZigBee nodes. For WSN with different

topologies such as start, tree, or mesh, new techniques should be developed to improve the end-to-end packet transmission when there is interference on the whole or part of the path. To this aim, our future research should be extended to include network layer techniques such as flow control or advanced routing protocols.

- **Cross-layer optimization techniques for IEEE 802.15.4 based WSNs under Wi-Fi interference.** While techniques at different protocol layer are normally designed to fulfill specific functionalities of that particular layer, cross-layer optimization should be studied to increase efficiency, adapt to changing wireless communications conditions, and ensure the end-to-end performance of WSN. For example, our studies on MAC layer frame transmission, acknowledgement, retransmission and CSMA/CA backoff delay should be studied in conjunction with the network layer packet transmission, acknowledgement, local or end-to-end retransmission, multi-hop and routing delay for getting a more complete picture of packet transmission performance in WSN. It is expected that more significant performance improvements can be achieved by designing novel techniques that consider cross-layer optimization.

Reference

[1] B. Qi, G. L. Zysman, and H. Menkes, "Wireless mobile communications at the start of the 21st century", Communications Magazine, IEEE , vol. 39, no. 1, pp. 110-116, Jan 2001.

[2] P. A. Dharma, and Z. Qing-An, “Introduction to Wireless and Mobile Systems”, Stamford: Cengage Learning, ISBN: 1439062056, pp. 1-27, June 2010.

[3] P. Zheng, L. L. Peterson, B. S. Davie, and A. Farrel, “Wireless Networking Complete”, Burlington, Massachusetts: Morgan Kaufmann, ISBN:0123750776, 2009.

[4] http://en.wikipedia.org/wiki/802.11, last visited on October 12, 2012.

[5] G. L. Stüber, “Principles of Mobile Communication”, Edition 3, New York: Springer, ISBN: 1461403634, 2011.

[6] W. Lehr, and L. W. Mcknight, "Wireless internet access: 3G vs. Wi-Fi?”, in Telecommunications Policy, pp. 351-370, 2003.

[7] E. Gaura, L. Girod, J. Brusey, M. Allen, and G. Challen, “Wireless Sensor Networks: Deployments and Design Frameworks”, NY: Springer, 2010.

[8] C. F. G. Hernández, P. H. I. González, J. G. Hernández, and J. A. P. Díaz, “Wireless Sensor Networks and Applications: a Survey”, IJCSNS International Journal of Computer Science and Network Security, vol. 7, no. 3, pp. 264-273, 2007.

[9] T. Arampatzis, J. Lygeros, and S. Manesis, “A survey of applications of wireless sensors and wireless sensor networks”, Proc. 13th Mediterranean Conference on Control and Automation, pp. 719-724, Limassol, Cyprus, June 27-29, 2005.

[10] I. F. Akyildiz, and M. C. Vuran, “Advanced Texts in Communications and Networking: Wireless Sensor Networks”, Hoboken, NJ, USA: Wiley, ISBN: 0470036013, 2010.

[11] K. Sohraby, D. Minoli and T. Znati, “Wireless Sensor Networks: Technology, Protocols, and Applications”, Hoboken, NJ, USA: Wiley, ISBN: 0471743003, 2007.

[12] C. Buratti, A. Conti, D. Dardari, and R. Verdone, “An overview on wireless sensor networks technology and evolution”, Sensors 2009, vol. 09, pp. 6869-6896, 2009.

[13] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor network: a survey”, Computer networks, vol. 38, no. 4, PP. 393-422, March 2002.

[14] S. H. Gajjar, S. N. Pradhan, K. S. Dasgupta, "Wireless Sensor Network: Application led research perspective," Recent Advances in Intelligent Computational Systems (RAICS), 2011 IEEE, pp.025-030, 22-24 Sept. 2011.

[15] M. P. Durisic, Z. Tafa, G. Dimic, and V. Milutinovic, "A survey of military applications of wireless sensor networks", 2012 Mediterranean Conference on Embedded Computing (MECO), pp.196-199, 19-21 June 2012.

[16] L. Selavo, A. Wood, Q. Cao, T. Sookoor, H. Liu, A. Srinivasan, Y. Wu, W. Kang, J. Stankovic, D. Young, and J. Porter, "LUSTER: Wireless sensor network for environmental research", In Proceedings of the ACM International Conference on Embedded Networked Sensor Systems (SenSys), Nov. 2007.

[17] V. Shnayder, B. Chen, K. Lorincz, T. R. F. Fulford-Jones, and M. Welsch, "Sensor Networks for Medical Care", in Harvard University Technical Report TR-08-05, 2005.

[18] B-K. Kim, S-K. Hong, Y-S. Jeong, and D-S. Eom, "The Study of Applying Sensor Networks to a Smart Home", Fourth International Conference on Networked Computing and Advanced Information Management, Volume 1, pp.676 – 681, Sept. 2008.

[19] J. Cheng and T. Kunz, "A survey on Smart Home Networking", Carleton University, Systems and Computer Engineering, Technical Report SCE-09-10, September 2009.

[20] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid", IEEE Transactions on Industrial Informatics, vol. 57, no. 10, pp. 3557-3564, October 2010.

[21] M. Erol-Kantarci, and H. T. Mouftah, "Wireless Sensor Networks for smart grid applications", Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, pp.1-6, 24-26 April 2011.

[22] C. Buratti, M. Martalò, R. Verdone, and G. Ferrari, "Sensor Networks with IEEE 802.15.4 Systems: Distributed Processing, MAC, and Connectivity", NY: Springer, ISBN: 3642174892, 2011.

[23] G. Fischerauer, R. Stöber, and U. Bayreuth, "WIRELESS SENSOR NETWORKS: STATUS AND TRENDS", SENSOR+TEST Conferences 2009, vol. 2, pp. 11-16, 2009.

[24] G. Wang, "Comparison and Evaluation of Industrial Wireless Sensor Network Standards ISA100.11a and WirelessHART", Master of Science Thesis, Chalmers University of Technology, Gothenburg, Sweden, 2011.

[25] P. Baronti, P. Pillai, V. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless sensor networks: a survey on the state of the art and the 802.15.4 and ZigBee standards", Communication Research Centre, UK, May 2006.

[26] ZigBee Alliance, http://www.ZigBee.org/About/UnderstandingZigBee.aspx, last visited on November 1, 2012.

[27] http://en.wikipedia.org/wiki/802.15.4, last visited on October 20, 2012.

[28] A. Koubâa, M. Alves, and E. Tovar, "IEEE 802.15.4 for Wireless Sensor Networks: A Technical Overview", IPPHURRAY Technical Report, HURRAY-TR-050702, Jul. 2005.

[29] 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.

[30] IEEE Standard for Local and metropolitan area networks— Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs), IEEE Standard, 2011.

[31] L. D. Nardis, and M. G. Di Benedetto, “Overview of the IEEE 802.15.4/4a standards for low data rate Wireless Personal Data Networks”, Workshop on Positioning, Navigation and Communication, Hannover, 2007.

[32] Rabbit-based board and Dynamic C libraries User Manual: An introduction to ZigBee, Digi International Inc., 2008.

[33] S. S. R. Ahamed, “The Role of ZigBee Technology in Future Data Communication System”, Journal of Theoretical and Applied Information Technology, vol. 5, no. 2, pp. 129-135, 2009.

[34] C. M. Ramya, M. shanmugaraj, and R. Prabakaran, “Study on ZigBee technology”, International conference on electronics computer technology (ICECT), vol. 06, pp. 297-301, April 2011.

[35] ZigBee Alliance, “ZigBee Specification”, Technical Report Document 053474r17, 2007.

[36] T. He, J. A. Stankovic, C. Lu and T. F. Abdelzaher, “SPEED: A Stateless Protocol for Real-Time Communication in Sensor Networks”, In IEEE ICDCS 2003, Providence, RI, May 2003.

[37] E. Egea-López, J. Vales-Alonso, A. S. Martínez-Sala, J. García-Haro, P. Pavón-Mariño, and M. V. B. Delgado, “A Wireless Sensor Networks MAC Protocol for Real- Time Applications”, Personal and Ubiquitous Computing, vol. 12, no. 2, pp. 111-122, 2008.

[38] J. A. Stankovic, “Research Challenges for Wireless Sensor Networks”, SIGBED Review: Special Issue on Embedded Sensor Networks and Wireless Computing, vol. 1, no. 2, pp.9-12 , July 2004.

[39] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, “Wireless Sensor Network Security: A Survey", Security in Distributed, Grid, and Pervasive Computing, Editor: Yang Xiao, Auerbach Publications, CRC Press, ISBN: 0849379210, 2006.

[40] G. Anastasi, M. Conti, M. D. Francesco, and A. Passarella, “Energy Conservation in Wireless Sensor Networks: a Survey”, Ad Hoc Networks, vol. 7, no. 3, pp. 537-568, May 2009.

[41] G. Thonet, P. Allard-Jacquin, and P. Colle, “ZigBee - Wi-Fi Coexistence: and Test Report”, Technical report, Schneider Electrics, 2008.

[42] ZigBee Alliance, “ZigBee and Wireless Radio Frequency Coexistence”, ZigBee white paper, June 2007.

[43] S.Shin, and 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.

[44] M. Rihan, M. El-Khamy, and M. El-Sharkawy, "On ZigBee coexistence in the ISM band: Measurements and simulations", 2012 International Conference on Wireless Communications in Unusual and Confined Areas (ICWCUCA), pp.1-6, 28-30 Aug. 2012.

[45] R. G. Garroppo, L. Gazzarrini, S. Giordano, and L. Tavanti, "Experimental assessment of the coexistence of Wi-Fi, ZigBee, and Bluetooth devices", 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp.1-9, 20-24 June 2011.

[46] A. Sikora, “Coexistence of IEEE 802.15.4 (ZigBee) with IEEE 802.11 (WLAN), Bluetooth, and Microwave Ovens in 2.4 GHz ISM-Band”, web document, http://www.ba-loerrach.de/stzedn/.

[47] Jennic Limited, “Co-existence of IEEE 802.15.4 at 2.4 GHz Application Note”, web document, http://www.jennic.com/support/application_notes/, last visited on January 23rd, 2013.

[48] Micaz Datasheet, http://www.openautomation.net/uploadsproductos/micaz_datasheet.pdf, last visited on January 23rd, 2013.

[49] Wikipedia: IEEE 802.11, http://en.wikipedia.org/wiki/802.11, last visited on January23rd, 2013.

[50] Y. Mao, Z. Zhao, and X. Jia, “Understanding the indoor interference between IEEE 802.15.4 and IEEE 802.11b/g via measurements”, 2011 International Conference on Wireless Communications and Signal Processing (WCSP), pp.1-5, 9-11 Nov. 2011.

[51] N. J. LaSorte, S. A. Rajab, and H. H. Refai, “Experimental assessment of wireless coexistence for 802.15.4 in the presence of 802.11g/n”, 2012 IEEE International Symposium on Electromagnetic Compatibility (EMC), pp.473-479, 6-10 Aug. 2012.

[52] A. Stranne, O. Edfors, and B. A. Molin, “Energy-based interference analysis of heterogeneous packet radio networks”, IEEE Transaction on Communications, vol. 54, no. 7, pp. 1299–1309, July 2006.

[53] D. K. Yoon, S. Y. Shin, and W. H. Kwon, “Packet error rate analysis of IEEE 802.11b under IEEE 802.15.4 interference”, IEEE VTC – Spring 2006, pp. 1186–1190, 2006.

[54] S. Y. Shin, H. S. Park, S. Choi, and W. H. Kwon, “Packet Error Rate Analysis of IEEE 802.15.4 under IEEE 802.11b Interference”, in Proceedings of WWIC 2005, LNCS, Springer, pp. 279–288, May 2005.

[55] S. Y. Shin, H. S. Park, and W. H. Kwon, “Packet error rate analysis of IEEE 802.15.4 under saturated IEEE 802.11b network interference”, IEICE Transactions on Communications, vol. 90, no. 10, pp. 2961–2963, 2007.

[56] S. Y. Shin, H. S. Park, and W. H. Kwon, “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.

[57] W. Yuan, X. Wang, and J. M. G. Linnartz, “A Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g”, in Proceedings of the 14th IEEE Symposium on Communications and Vehicular Technology in the Benelux (SCVT '07), November 2007.

[58] W. Yuan, X. Wang, J. P. M. G. Linnartz, and I. G. M. M. Niemegeers, “Experimental Validation of a Coexistence model of IEEE 802.15.4 and IEEE 802.11b/g Networks”, IRA-DSN’09, Hangzhou, China, 2009.

[59] M. Petrova, J. Riihijarvi, P. Mahonen, and S. Labella, “Performance study of IEEE 802.15.4 using measurements and simulations”, Wireless Communications and Networking Conference 2006 (WCNC 2006), vol.1, pp. 487-492, 2006.

[60] M. Petrova, W. Lili, P. Mahonen, and J. Riihijarvi, "Interference Measurements on Performance Degradation between Colocated IEEE 802.11g/n and IEEE 802.15.4 Networks", Sixth International Conference on Networking, 2007 (ICN '07), pp. 93, 22-28 April 2007.

[61] Y. Peizhong, A. Iwayemi, and C. Zhou, “Developing ZigBee deployment guideline under WiFi interference for smart grid applications”, IEEE Trans. Smart Grid, vol. 2, no. 1, pp. 110–120, Mar 2011.

[62] L. Angrisani, M. Bertocco, D. Fortin, and A. Sona, “Experimental study of coexistence issues between IEEE 802.11b and IEEE 802.15.4 wireless networks”, IEEE Trans. Instrum. Meas., vol. 57, no. 8, pp. 1514–1523, Aug. 2008.

[63] F. Penna, C. Pastrone, M. A. Spirito, and R. Garello,"Measurement-Based Analysis of Spectrum Sensing in Adaptive WSNs under Wi-Fi and Bluetooth Interference", Vehicular Technology Conference 2009 (VTC Spring 2009, IEEE 69th), pp.1-5, 26-29 April 2009.

[64] S. Han, Su. Lee, S. Lee, and Y. Kim, “Coexistence Performance Evaluation of IEEE 802.15.4 under IEEE 802.11B Interference in Fading Channels”, IEEE 18th International PIMRC Symposium, 2007.

[65] C. Won, J. H. Youn, H. Ali, H. Sharif, and J. Deogun, "Adaptive radio channel allocation for supporting coexistence of 802.15.4 and 802.11b", IEEE 62nd Vehicular Technology Conference 2005 (VTC-2005-Fall), vol.4, pp. 2522- 2526, 25-28 Sept. 2005.

[66] J. Zheng, and M. J. Lee, “A comprehensive performance study of IEEE 802.15.4”, in Sensor Network Operations, IEEE Press, Wiley Interscience: New York, pp. 218–237, Chapter 4, 2006.

[67] Y. Peizhong, A. Iwayemi, and C. Zhou, "Frequency agility in a ZigBee network for smart grid application", 2010 Innovative Smart Grid Technologies (ISGT), pp. 1-6, 19-21 Jan 2010.

[68] M. S. Kang, J. W. Chong, H. Hyun, S. M. Kim, B. H. Jung, and D. K. Sung, "Adaptive Interference-Aware Multi-Channel Clustering Algorithm in a ZigBee Network in the Presence of WLAN Interference", 2nd International Symposium on Wireless Pervasive Computing, 2007 (ISWPC '07), 5-7 Feb. 2007.

[69] 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", 2010 IEEE Wireless Communications and Networking Conference (WCNC), pp.1-5, 18-21 April 2010.

[70] J. Huang, G. Xing, G. Zhou, and R. Zhou, "Beyond co-existence: Exploiting WiFi white space for ZigBee performance assurance", 2010 18th IEEE International Conference on Network Protocols (ICNP), pp.305-314, 5-8 Oct. 2010.

[71] 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.

[72] M. L. Huang, and S. Park, “A WLAN and ZigBee coexistence mechanism for wearable health monitoring system”, 9th Intl. Symp. Commun. and Inf. Technol., ISCIT 2009, pp. 555-559, 2009.

[73] R. Soua and P. Minet, “A survey on energy efficient techniques in wireless sensor networks”, Wireless and Mobile Networking Conference (WMNC), 2011 4th Joint IFIP, pp. 1-9, Oct. 2011.

[74] K. Vikas and P. R. Kumar, “Power control and clustering in ad hoc networks”, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications (IEEE INFOCOM 2003), vol. 1, pp. 459-469, Mar. 2003.

[75] M. Kubisch, H. Karl, A. Wolisz, L. C. Zhong and J. Rabaey, “Distributed algorithms for transmission power control in wireless sensor networks”, Wireless Communications and Networking Conference (IEEE WCNC), vol. 1, pp. 558-563, Mar. 2003.

[76] L. Li, J. Y. Halpern, P. Bahl, Yi-Min Wang and R. Wattenhofer, “A cone-based distributed topology-control algorithm for wireless multi-hop networks”, IEEE/ACM Transactions on Networking, vol. 13, pp. 147-159, Feb. 2005.

[77] R. Wattenhofer, L. Li, P. Bahl and Y. Wang, “Distributed topology control for power efficient operation in multihop wireless ad hoc networks,” in Proc. INFOCOM 2001, vol. 3, pp. 1388-1397, 2001.

[78] R. Ramanathan and R. Rosales-Hain, “Topology control of multihop wireless networks using transmit power adjustment”, in Proc. INFOCOM 2000, vol. 2, pp. 404-413, 2000.

[79] S. Panichpapiboon, G. Ferrari and O. K. Tonguz, “Optimal Transmit Power in Wireless Sensor Networks”, IEEE Transactions on Mobile Computing, vol. 5, pp. 1432-1447, Oct. 2006.

[80] A. Nandi, D. Bepari and S. Kundu, “Optimal transmit power in wireless sensor networks using MRC space diversity in presence of shadow fading”, 2010 International Conference on Computer and Communication Technology (ICCCT), pp. 28-34, Sept. 2010.

[81] X. Shuo, A. Dhamdhere, V. Sivaraman and A. Burdett, “Transmission Power Control in Body Area Sensor Networks for Healthcare Monitoring”, IEEE Journal on Selected Areas in Communications, vol. 27, pp. 37-48, January 2009.

[82] Z. Zhiwei, Z. Xinming, S. Peng and L. Pengxi, “A transmission power control MAC protocol for wireless sensor networks”, Sixth International Conference on Networking (ICN' 07), pp. 5-5, April 2007.

[83] L. Shan, Z. Jingbin, Z. Gang, G. Lin, J. A. Stankovic, and H. Tian, “ATPC: adaptive transmission power control for wireless sensor networks”, in Proceedings of the 4th international conference on Embedded networked sensor systems (SenSys '06), pp. 223-236, 2006.

[84] K. Junseok, C. Sookhyeon and K. Younggoo, “ODTPC: On-demand transmission power control for wireless sensor networks”, International Conference on Information Networking (ICOIN), pp. 1-5, Jan. 2008.

[85] M. M. Y. Masood, G. Ahmed and N. M. Khan, “Modified on demand transmission power control for wireless sensor networks”, 2011 International Conference on Information and Communication Technologies (ICICT), pp. 1-6, July 2011.

[86] S. Dongjin, B. Krishnamachari and J. Heidemann, “Experimental study of the effects of transmission power control and blacklisting in wireless sensor networks”, 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, pp. 289-298, Oct. 2004.

[87] B. Zurita Ares and P. G. Park and C. Fischione and A. Speranzon and K. H. Johansson, “On power control for wireless sensor networks: System model, middleware component and experimental evaluation”, IFAC European Control Conference (ECC'07), 2007.

[88] L. H. A. Correia and J. M. S. Nogueira, “Transmission power control techniques for MAC protocols in wireless sensor networks”, Network Operations and Management Symposium (NOMS), pp. 1049-1054, April 2008

[89] Wikipedia, http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance, last retrieved on Jan 14, 2013.

[90] Wikipedia, http://en.wikipedia.org/wiki/Distributed_coordination_function, last retrieved on Jan 14, 2013.

[91] F. Shu, and T. Sakurai, “Analysis of an Energy Conserving CSMA-CA”, IEEE Global Telecommunications Conference (GLOBECOM) 2007, pp. 2536-2540, Nov. 2007.

[92] A.H. Shuaib, T. Mahmoodi and A.H. Aghvami, "A timed Petri Net model for the IEEE 802.15.4 CSMA-CA process", 2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 1204-1210, Sept. 2009.

[93] S. Pollin, M. Ergen, S.C. Ergen,B. Bougard, F. Catthoor, A. Bahai and P. Varaiya, "Performance Analysis of Slotted Carrier Sense IEEE 802.15.4 Acknowledged Uplink Transmissions", IEEE Wireless Communications and Networking Conference (WCNC) 2008, pp. 1559-1564, March 2008.

[94] J. He, Z. Tang, H. Chen and Q. Zhang, "An accurate and scalable analytical model for IEEE 802.15.4 slotted CSMA/CA networks", IEEE Transactions on Wireless Communications, vol.8, no.1, pp.440-448, Jan. 2009.

[95] C. Jung, H. Hwang, D. Sung and G. Hwang, "Enhanced Markov Chain Model and Throughput Analysis of the Slotted CSMA/CA for IEEE 802.15.4 Under Unsaturated Traffic Conditions", IEEE Transactions on Vehicular Technology, vol.58, no.1, pp.473-478, Jan. 2009.

[96] J. Zhu, Z. Tao and C. Lv, "Delay Analysis for IEEE 802.15.4 CSMA/CA Scheme with Heterogeneous Buffered Traffic", 2011 Third International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), vol.1, pp.835-845, Jan. 2011.

[97] T.O. Kim, J.S. Park, H.J. Chong, K.J. Kim and B.D. Choi, "Performance analysis of IEEE 802.15.4 non-beacon mode with the unslotted CSMA/CA", IEEE Communications Letters, vol.12, no.4, pp.238-240, April 2008.

[98] M. Goyal, D. Rohm, H. Hosseini, K.S. Trivedi, A. Divjak and Y. Bashir, "A stochastic model for beaconless IEEE 802.15.4 MAC operation", International Symposium on Performance Evaluation of Computer & Telecommunication Systems (SPECTS) 2009, vol.41, pp.199-207, July 2009.

[99] C. Buratti and R. Verdone, "Performance Analysis of IEEE 802.15.4 Non Beacon-Enabled Mode", IEEE Transactions on Vehicular Technology, vol.58, no.7, pp.3480-3493, Sept. 2009.

[100] F. Wang, D. Li and Y. Zhao, "Analysis of CSMA/CA in IEEE 802.15.4," Communications, IET , vol.5, no.15, pp.2187-2195, October.14, 2011.

[101] T.R. Burchfield, S. Venkatesan and D. Weiner, “Maximizing Throughput in ZigBee Wireless Networks through Analysis, Simulations and Implementations”, UTDCS-24-07 and in proceedings of First International Workshop on Localized Algorithms and Protocols for Wireless Sensor Networks (LOCALGOS 2007) located with Distributed Computing in Sensor Systems (DCOSS), 2007.

[102] A. Koubaa, M. Alves, B. Nefzi and Y.-Q. Song, “Improving the IEEE 802.15.4 slotted CSMA/CA MAC for time-critical events in wireless sensor networks”, in Proc.Workshop Real-Time Networks (RTN 2006), Satellite Workshop to ECRTS 2006, Jul. 2006.

[103] F. Shu, "Performance evaluation of the IEEE 802.15.4 CSMA-CA protocol with QoS differentiation", Processing of the International Conference on Intelligent Sensors (ISSNIP) 2008, pp.475-480, Dec. 2008.

[104] M. Kim and C.H. Kang, "Priority-Based Service-Differentiation Scheme for IEEE 802.15.4 Sensor Networks in Nonsaturation Environments", IEEE Transactions on Vehicular Technology, vol.59, no.7, pp.3524-3535, Sept. 2010.

[105] B.H. Lee, and H.K. Wu, "Study on Backoff Algorithm for IEEE 802.15.4 LR-WPAN", 22nd International Conference on Advanced Information Networking and Applications, pp.403-409, 25-28 March 2008.

[106] H. Lee, K. Lee, S. Ryu, S. Lee, K. Song, and Y. Shin, "An efficient slotted CSMA/CA algorithm for the IEEE 802.15.4 LR-WPAN", 2011 International Conference on Information Networking (ICOIN), pp.488-493, 26-28 Jan. 2011.

[107] 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, May 2007.

[108] M.D. 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", 2010 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops), pp.400-405, March. 2010.

[109] D-ITG manual, http://www.grid.unina.it/software/ITG/, last visited on Jan. 1, 2013.

[110] MICAz, http://www.openautomation.net/uploadsproductos/micaz_datasheet.pdf, last visited on Jan. 30, 2013.

[111] CC2420 Data Sheet, http://inst.eecs.berkeley.edu/~cs150/Documents/CC2420.pdf, last retrieved on Jan 14, 2013.

[112] MIB600, http://bullseye.xbow.com:81/Products/productdetails.aspx?sid=179, last retrieved on Jan 14, 2013.

[113] Aeroflex 3252 Spectrum Analyzer, http://www.aeroflex.com/ats/products/product/General_Purpose_Test/Spectrum_Analyzers/3250_Series_Analyzers~684.html, last retrieved on Jan 14, 2013.

[114] DD-WRT, http://www.dd-wrt.com/site/index, last visited on Jan.15, 2013.

[115] WireShark, http://www.wireshark.org/about.html, last visited on Feb.15, 2013.

[116] 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.

[117] 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.

[118] Atmega128L, http://www.atmel.com/Images/doc2467.pdf, last visited on Feb.15, 2013.

[119] MoteWorks Getting Started Guide, Crossbow, http://www.radford.edu/nsrl/creu1011/PowerPoints/MoteWorks.pdf, last retrieved on Mar.4, 2013.

[120] TinyOS, http://en.wikipedia.org/wiki/TinyOS, last visited on Mar.5, 2013.

[121] ABB Inc., "Introduction to WISA - Wireless Interface for Sensors and Actuators", White Paper, July 2006.

[122] Wikipedia, http://en.wikipedia.org/wiki/DBm, last retrieved on Apr. 22, 2013.

[123] "Propagation data and prediction methods for the planning of indoor radio communication systems and the radio local area networks in the frequency range 900 MHz to 100 GHz", ITU-R Recommendations, Geneva, 2001.

[124] G. B. Eslamlu, M. Sabaei, and M. Fereydooni, "The novel delay-constraint topology control algorithm in WSNs", 2012 21st Annual Wireless and Optical Communications Conference (WOCC), pp. 111-115, April 2012.

[125] K. Gill, S-H Yang, F. Yao, and X. Lu, "A ZigBee-based home automation system", IEEE Transactions on Consumer Electronics, vol. 55, no. 2, pp. 422-430, May 2009.

[126] L. L. Yang, S. H. Yang, and F. Yao, "Safety and Security of Remote Monitoring and Control of intelligent Home Environments", IEEE International Conference on Systems, Man and Cybernetics 2006, vol. 2, pp. 1149-1153, 8-11 Oct. 2006.

[127] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and Challenges of Wireless Sensor Networks in Smart Grid", IEEE Transactions on Industrial Electronics, vol. 57, no. 10, pp. 3557-3564, Oct. 2010.

[128] A. A. Sreesha, S. Somal, and I. T. Lu, "Cognitive Radio Based Wireless Sensor Network architecture for smart grid utility", 2011 IEEE Long Island Systems, Applications and Technology Conference (LISAT), pp. 1-7, May 2011.

[129] R. V. P. Yerra, A. K. Bharathi, P. Rajalakshmi, and U. B. Desai, "WSN based power monitoring in smart grids", 2011 Seventh International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), pp. 401-406, 6-9 Dec. 2011.

[130] A. R. Devidas, M. V. Ramesh, "Wireless Smart Grid Design for Monitoring and Optimizing Electric Transmission in India", 2010 Fourth International Conference on Sensor Technologies and Applications (SENSORCOMM), pp.637-640, 18-25 July 2010.

[131] P. Han, J. K. Wang, Y. H. Han, and Q. Zhao, "Novel WSN-based residential energy management scheme in smart grid", 2012 International Conference on Information Science and Technology (ICIST), pp. 393-396, 23-25 March 2012.

[132] O. Asad, M. Erol-Kantarci, and H. Mouftah, "Sensor network web services for Demand-Side Energy Management applications in the smart grid", 2011 IEEE Consumer Communications and Networking Conference (CCNC), pp. 1176-1180, 9-12 Jan. 2011.

[133] Hart Communication Protocol – Wireless HART Technology, HART Communication Foundation, http://www.hartcomm.org/protocol/wihart/wireless_technology.html, last visited on July 16th, 2013.

[134] ISA Standards & Practices Board ratifies ISA-100.11a document, http://www.isa.org/Template.cfm?Section=Press_Releases5&template=/ContentManagement/ContentDisplay.cfm&ContentID=78964, last visited on July 16th, 2013.

[135] N. A. Pantazis, D. D. Vergados, “A Survey on Power Control Issues in Wireless Sensor Networks”, IEEE Communications Surveys & Tutorials, Vol. 9(4), pp. 86-107, 2007.

[136] P. Santi, “Topology Control in Wireless Ad Hoc and Sensor Networks, ACM Computing Survey, Vol. 37, n. 2, pp. 164-194, June 2005.

[137] C-J.M. Liang, N.B. Priyantha, J. Liu, and A. Terzis, “Surviving Wi-Fi Interference in Low Power ZigBee Networks”, In Proceedings of the 8th ACM Conference on Embedded Network Sensor Systems (SenSys 2010), pp. 309–322, November 2010.

[138] A. Sikora, D. Lill, and V. Groza, “Comparison of Internet and Dedicated Communication Protocols for Instrumentation and Measurement Systems Using Short Range Wireless Networks,” IEEE Instrumentation and Measurement Technology Conference IMTC 2006, ISBN: 0-7803-9360-0, pp. 982-986, Sorrento, Italy, April 2006.

[139] Different types of confidence intervals, http://www.csu.edu.au/__data/assets/pdf_file/0005/88610/7-confidence-interval.pdf, last visited on October 15th, 2013.

[140] IBM SPSS, http://www-01.ibm.com/software/analytics/spss/products/statistics/, last visited on October 15th, 2013.

[141] Wikipedia, http://en.wikipedia.org/wiki/Kolmogorov%E2%80%93Smirnov_test, last visited on October 16th, 2013.

Appendix A

Confidence Interval for the Mean

A confidence interval is a type of interval estimate of a parameter determined by using data obtained from a sample and by using the specific confidence level of the estimate. Three common confidence intervals are used: the 90%, the 95%, and the 99% confidence intervals. [139]

When finding the confidence interval for the mean of a population, there are two different situations that may exist. You will be given information that may have the population standard deviation stated or it may be the sample standard deviation that is given. A different formula needs to be used in each case.

Case 1: When the population standard deviation (σ) is known. The confidence interval of the population mean (μ) is calculated using:

$$\bar{x} \pm Z_{\alpha/2} \frac{\sigma}{\sqrt{n}} \qquad \text{(A.1)}$$

Where the level of required confidence level is $(1-\alpha)$ *100%, $\bar{x}$ = sample mean, n = sample size and σ = population standard deviation. Z is the normal distribution's critical value for a probability of α/2 in each tail.

Case 2: When the population standard deviation (σ) is unknown. The confidence interval of the population mean (μ) is found using:

$$\bar{x} \pm t_{\frac{\alpha}{2},n-1} \frac{\sigma}{\sqrt{n}} \quad \text{(A.2)}$$

Where the level of required confidence level is $(1-\alpha)$ *100%, $\bar{x}$ = sample mean, n = sample size and σ = population standard deviation. *t* is the critical value of the *t* distribution with n-1 degree of freedom and an area of α/2 in each tail.

In our research, the formula of case 2 is used to calculate a 95% confidence interval.

Appendix B

ZigBee Performance Evaluation without Custom Defined Wi-Fi Interference

In order to evaluate the influence of background noise and other interference source on the performance of ZigBee transmission in our lab, we performed a set of ZigBee traffic without our custom defined Wi-Fi interference using the testbed shown in Fig.B.1. ZigBee channel 20, the same as the one selected in our ZigBee and Wi-Fi coexistence research, is used. The ZigBee client is located in three locations indicated as Case 1, Case 2, and Case 3 in Fig.B.1.

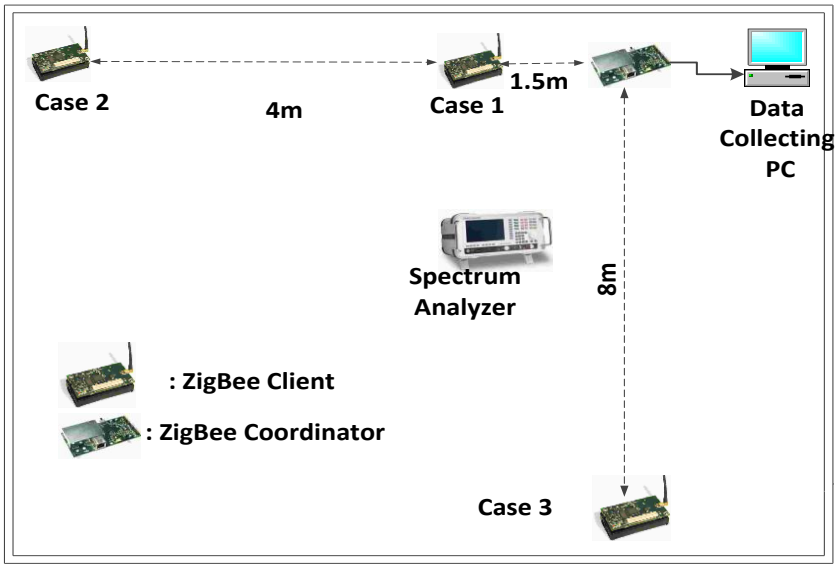

Fig.B.1 ZigBee Performance Evaluation without Custom Defined Wi-Fi Interference

In each test, the ZigBee client mote is programmed to send out 10000 data packets with 100 bytes/packet at 20ms intervals without packet retransmission. The ZigBee performance is evaluated in terms of the number of packet loss.

Table B.1 Experimental Results for ZigBee packet transmission without Custom Defined Wi-Fi Interference

Number of Packet Loss	Case 1	Case 2	Case 3
Test 1	0	0	1
Test 2	0	2	0
Test 3	0	0	2
Test 4	1	2	1
Test 5	0	0	5

Based on the experimental results shown in Table B.1, it can be concluded that ZigBee channel 20 (2.449-2.451GHz) is not “contaminated” by noise or interference from any other Wi-Fi APs in the lab. The performance degradation of ZigBee packet transmission in our ZigBee and Wi-Fi coexistence research is mainly due to our custom defined Wi-Fi interference.

Appendix C

Distributed Internet Traffic Generator (D-ITG) Validation

D-ITG [109] is able to generate traffic that Inter Departure Time (IDT) between packets and Packet Size (PS) follow different probability distributions, including constant, Poisson, Uniform, Pareto, Cauchy, Normal, Exponential, and so on. In our testbed, UDP traffic with different probability distributions for both IDT and PS are used. In order to evaluate the performance of D-ITG traffic generator, we specify the IDT and PS distributions of a UDP traffic flow between a Wi-Fi source and a Wi-Fi sink. **Wireshark** [115] is used on Wi-Fi source to listen to the selected source port of the UDP traffic and capture the UDP packets in order to analyze and validate their distributions. It has been validated that D-ITG can properly generate the UDP traffic flow that PS or IDT follows the selected probability distributions. Some of the analysis results are given in the following part.

UDP traffic flow 1: D-ITG generated UDP traffic with constant segment IDT, payload size of 1400 bytes and segment generation rate of 500 segments/second.

IDT distribution analysis: A sample size of 2000 is used.

The mean of the IDT sample is 2.000014ms.

The standard deviation of the sample is calculated as 0.000383.

UDP traffic flow 2: The packets generated by D-ITG have the same payload size of 1400 bytes while the IDT is following exponential distribution with mean arrival rate of 500 segments/second.

IDT distribution analysis: A sample size of 2000 is used. IBM SPSS Statistics [140] is used to implement one sample Kolmogorov-Smirnov (K-S) test [141] to investigate that if IDT follows the selected distribution. The result of the one sample K-S test is shown in Table C.1.

Table C.1 one sample Kolmogorov-Smirnov (K-S) test

		IDT
N		2000
Exponential Parameter [a,b] Mean		0.0020
Most Extreme Absolute		0.027
Differences	Positive	0.027
	Negative	-0.011
Kolmogorov-Smirnov Z		1.219
Asymptotic Sig. (2-tailed)		0.103

a. Test Distribution is exponential.

b. Calculated from data.

Since Sig. = 0.103 > 0.05 (Significance level), it can be concluded that the IDT of the UDP traffic flow follows the exponential distribution.