Loughborough University

Thesis Access Form

Copy No……...…….**Location**……..……...…

Author……...……Fang Yao……..…….

Title…… Interference Mitigation Strategy Design and Applications for Wireless Sensor Networks……..

Status of access OPEN / RESTRICTED / CONFIDENTIAL

Moratorium Period:……2……years, ending……10……../……2012…….

Conditions of access approved by (CAPITALS):……SHUANGHUA YANG……

Supervisor (Signature)……...……...

Department of……Computer Science……...……

Author's Declaration: *I agree the following conditions:*

Open access work shall be made available (in the University and externally) and reproduced as necessary at the discretion of the University Librarian or Head of Department. It may also be digitised by the British Library and made freely available on the Internet to registered users of the EThOS service subject to the EThOS supply agreements.

*The statement itself shall apply to **ALL** copies including electronic copies:*

This copy has been supplied on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

Restricted/confidential work: All access and any photocopying shall be strictly subject to written permission from the University Head of Department and any external sponsor, if any.

Author's signature…….Date……...……...……...

users declaration: for signature during any Moratorium period (Not Open work): ***I undertake to uphold the above conditions:***			
Date	Name (CAPITALS)	Signature	Address

Interference Mitigation Strategy Design and Applications for Wireless Sensor Networks

by

Fang Yao

A Doctoral Thesis

Submitted in partial fulfilment
of the requirements for the award of

Doctor of Philosophy
Of
Loughborough University

October 2010

Certificate of Originality

This is to certify that I am responsible for the work submitted in this thesis, that the original work is my own except as specified in acknowledgments or in footnotes, and that neither the thesis nor the original work contained therein has been submitted to this or any other institution for a higher degree.

Author's signature ……

Date ……

Acknowledgements

This research would not have been possible without the support of many people, for whom I would like to express thanks.

First and foremost, I owe my deepest gratitude to my supervisor, Professor Shuanghua Yang, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject.

I greatly appreciate and wish to thank all the staff at the Computer Science Department for their great assistance during these years.

I would like to thank Khusvinder Gill and Rodger Knott for their helpful suggestions that increased readability and reduced ambiguity. I would never forget to acknowledge my colleagues in Holywell Park for providing a stimulating and fun environment in which to learn and grow. I am especially grateful to Huangjia Yang, Wei Zheng, Ran Xu, Xin Lu, Yannin Yang, Hesham Abusaimeh, Tareq Alhmieda and Zaid Bin Ahmad. Yunqiu Li was particularly helpful mathematically, patiently teaching me the theory of modelling.

Finally, I am forever indebted to my wife, Yue Xiong, and my family for their understanding, endless patience and encouragement when it was most required.

Abstract

The Institute of Electrical and Electronics Engineers (IEEE) 802.15.4 standard presents a very useful technology for implementing low-cost, low-power, wireless sensor networks. Its main focus, which is to applications requiring simple wireless connectivity with relaxed throughout and latency requirements, makes it suitable for connecting devices that have not been networked, such as industrial and control instrumentation equipments, agricultural equipments, vehicular equipments, and home appliances. Its usage of the license-free 2.4 GHz frequency band makes the technique successful for fast and worldwide market deployments. However, concerns about interference have arisen due to the presence of other wireless technologies using the same spectrum. Although the IEEE 802.15.4 standard has provided some mechanisms, to enhance capability to coexist with other wireless devices operating on the same frequency band, including Carrier Sensor Multiple Access (CSMA), Clear Channel Assessment (CCA), channel alignment, and low duty cycle, it is essential to design and implement adjustable mechanisms for an IEEE 802.15.4 based system integrated into a practical application to deal with interference which changes randomly over time. Among the potential interfering systems (Wi-Fi, Bluetooth, cordless phones, microwave ovens, wireless headsets, etc) which work on the same Industrial, Scientific, and Medical (ISM) frequency band, Wi-Fi systems (IEEE 802.11 technique) have attracted most concerns because of their high transmission power and large deployment in both residential and office environments.

This thesis aims to propose a methodology for IEEE 802.15.4 wireless systems to adopt proper adjustment in order to mitigate the effect of interference caused by IEEE 802.11 systems through energy detection, channel agility and data recovery. The contribution of this thesis consists of five parts. Firstly, a strategy is proposed to enable IEEE 802.15.4 systems to maintain normal communications

using the means of consecutive transmissions, when the system's default mechanism of retransmission is insufficient to ensure successful rate due to the occurrence of Wi-Fi interference. Secondly, a novel strategy is proposed to use a feasible way for IEEE 802.15.4 systems to estimate the interference pattern, and accordingly adjust system parameters for the purpose of achieving optimized communication effectiveness during time of interference without relying on hardware changes and IEEE 802.15.4 protocol modifications. Thirdly, a data recovery mechanism is proposed for transport control to be applied for recovering lost data by associating with the proposed strategies to ensure the data integrity when IEEE 802.15.4 systems are suffering from interference. Fourthly, a practical case is studied to discuss how to design a sustainable system for home automation application constructed on the basis of IEEE 802.15.4 technique. Finally, a comprehensive design is proposed to enable the implementation of an interference mitigation strategy for IEEE 802.15.4 based ad hoc WSNs within a structure of building fire safety monitoring system.

The proposed strategies and system designs are demonstrated mainly through theoretical analysis and experimental tests. The results obtained from the experimental tests have verified that the interference caused by an IEEE 802.11 system on an IEEE 802.15.4 system can be effectively mitigated through adjusting IEEE 802.15.4 system's parameters cooperating with interference pattern estimation. The proposed methods are suitable to be integrated into a system-level solution for an IEEE 802.15.4 system to deal with interference, which is also applicable to those wireless systems facing similar interference issues to enable the development of efficient mitigation strategies.

Keywords: WSN, Wi-Fi, Interference, Mitigation, Energy Detection, Home Automation, Building Monitoring.

Publications

Journal Publications

Yao, F., Xia, B.K., and Yang, S.H., “A ZigBee Based Home Automation System Design and Implementation”, *The Journal of the Institute of Measurement and Control*, Vol. 41, No. 10, pp. 310-314, 2008.

Yao, F., and Yang, S., "Assuring Reliability of Wireless Sensor Networks Through Self-Organising Routing Algorithms", *The Journal of the Institute of Measurement and Control*, Vol. 39, No. 7, pp. 209-213, 2006.

Gill, K., Yang, S., Yao, F., and Lu, X., “A Zigbee-Based Home Automation System”, *The Journal of IEEE transactions on Consumer Electronics*, Vol. 55, No.2, pp.422 -430, 2009

Conference Publications

Yao, F., Zheng, W., and Yang, S., “Mitigating Interference Caused by IEEE 802.11b in the IEEE 802.15.4 WSN within the Environment of Smart House”, to be in Proceedings of *2010 IEEE International Conference on System, Man, and Cybernetics,* Istanbul, Turkey, 2010.

Yao, F., Gill, K., and Yang, S., "A Zibee Based Low Cost Home Automation System", *The 13th International Conference on Automation and Computing*, Staffordshire, UK, pp. 258-263, 2007.

Yao, F., and Yang, S., "A Self-Organising Routing Algorithm for Wireless Sensor Networks", *2006 IEEE Conference on Systems, Man and Cybernetics*, Taipei, Taiwan, pp. 3388-3393, 2006.

Yao, F., and Yang, S., “Dynamic Adjusting Transferring (DAT) Based on Residual Energy in Wireless Sensor Networks”, *Proceedings of the 12th Annual*

Conference of Chinese Automation and Computing Society, Loughborough, UK, pp. 106-110, 2006.

Gill, K., Yao, F., and Yang, S., "Transparent Heterogeneous Networks for the Remote Control of Home Environments", Proceedings of the *2008 IEEE International Conference on Networking, Sensing and Control*, Sanya, China, pp. 1419-1424, 2008.

Gill, K., Yao, F., and Yang, S., "The Design and Implementation of a Flexible Home Gateway Architecture", *The 13th International Conference on Automation and Computing*, Staffordshire, UK, pp. 128-133, 2007.

Yang, H., Yao, F. and Yang, S., "Zigbee Enabled Radio Frequency Identification System", Proceedings of *International Conference on Communication Systems, Networks and Applications*, Beijing, China, pp. 163-168, 2007.

Yang, L., Yang, S. and Yao, F., "Safety and Security of Remote Monitoring and Control of Intelligence Home Environment", Proceedings of *2006 IEEE International Conference on Systems, Man, and Cybernetics (IEEE SMC 2006)*, Taipei, Taiwan, pp 1150-1153, 2006.

Papers under Review

Yao, F., and Yang, S.H., ‘‘Achieving Reliable Multi-Hop Transmission in IEEE 802.15.4 Ad Hoc Network under Interference", submitted to International Conference on Communications ICC 2011, Japan.

Yao, F., and Yang, S.H., ‘‘Application Design for Interference Aware ZigBee Building Monitoring Network”, submitted to International Conference on Communications ICC 2011, Japan.

Yao, F., Zheng, W., and Yang, S.H., ‘‘Mitigating Interference in IEEE 802.15.4 Network with Dynamic Energy Detection", submitted to International Conference on Communications ICC 2011, Japan.

Abbreviations

AD	:	Attached Device
BE	:	Backoff Exponent
BER	:	Bit Error Rate
BI	:	Beacon Interval
BO	:	Beacon Order
BRD	:	Bridge Device
CAP	:	Contention Access Period
CCA	:	Clear Channel Assessment
CCBM	:	Channel Change Broadcast Message
CFP	:	Contention-Free Period
CID	:	Cluster Identifier
CLH	:	Cluster Head
CSMA	:	Carrier Sense Multiple Access
CSMA-CA	:	Carrier Sense Multiple Access with Collision Avoidance
DBPSK	:	Differential Binary Phase Shift Keying
DIFS	:	Distributed Inter-Frame Space
DQPSK	:	Differential Quadrature Phase Shift Keying
DSSS	:	Direct Sequence Spread Spectrum
ED	:	Energy Detection
EDGE	:	Enhanced Data Rate for GSM Evolution
FCC	:	Federal Communication Commission

FDMA	:	Frequency Division Multiple Access
FFD	:	Full Function Device
FTP	:	File Transfer Protocol
GFSK	:	Gaussian Frequency Shift Keying
GPRS	:	General Packet Radio Service
GSM	:	Global System for Mobile Communications
GTS	:	Guaranteed Time Slots
HSDPA	:	High-Speed Downlink Packet Access
IC	:	Integrated Circuit
I2C	:	Inter-Integrated Circuit
IEEE	:	Institute of Electrical and Electronics Engineers
ISM	:	Industrial, Scientific and Medical
KVP	:	Key-Value Pair
LCD	:	Liquid Crystal Display
LQI	:	Link Quality Indication
LR-WPAN	:	Low-Rate Wireless Personal Area Networks
MAC	:	Medium Access Control
MEMS	:	Micro Electro Mechanical System
MSDU	:	MAC Service Data Unit
NB	:	Number of Backoff (periods)
O-QPSK	:	Offset Quadrature Phase-Shift Keying
OSI	:	Open Systems Interconnection
PAN	:	Personal Area Network
PCB	:	Printed Circuit Board
PDA	:	Personal Digital Assistant
PHY	:	Physical Layer

PN	:	Pseudo-random Noise
PRSG	:	Pseudorandom Sequence Generator
PSDU	:	PHY Service Data Unit
RF	:	Radio Frequency
RFD	:	Reduced Function Device
RFID	:	Radio Frequency Identification
SHR	:	Synchronization Header
SNR	:	Signal-to-noise Ratio
SD	:	Superframe Duration
SO	:	Superframe Order
SOC	:	System-On-Chip
TSB	:	Technology Strategy Board
UART	:	Universal Asynchronous Receiver/Transmitter
UDP	:	User Datagram Protocol
UMTS	:	Universal Mobile Telecommunications System
UWB	:	Ultra-Wide Band
WPAN	:	Wireless Personal Area Network
WSN	:	Wireless Sensor Network

List of Symbols

byte/s	:	Byte per second
dB	:	Decibel
dBm	:	Power ratio in decibel of the measured power referenced to one milliwatt
dBm/Hz	:	Ratio of the power in one Hertz of bandwidth
GHz	:	Gigahertz
hop/s	:	Number of channels the Bluetooth transceivers hop per second
kbps	:	Kilo bits per second
Mbit/s	:	Mega bits per second
MHz	:	Megahertz
ms	:	Millisecond
mW	:	Milliwatt
µs	:	Microsecond
F_S	:	Start frequency
F_E	:	End frequency

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

1.1 Background to the Research

Over the last few years, the convenience that the capability of being able to connect devices without the use of wires has led to the increasing take-up of wireless technologies by the consumer goods industry (Willig et al., 2005). Primary wireless technologies which have been widely accepted for serving people in daily life include cellular phone, IEEE 802.11 networks (Wi-Fi), ZigBee (IEEE 802.15.4), Bluetooth (IEEE 802.15.1), Ultra-Wide Band (UWB), and Radio Frequency Identification (RFID) (Webb, 2007). If users need to connect to a network by physical cables, their movement is drastically restricted. Wireless connectivity suffers from no such restriction and provides significantly more freedom of movement for network users. Meanwhile, wireless networks can offer several advantages over wired networks, including ease and speed of deployment, flexibility, and installation cost (Gast, 2002).

The development of wireless networking has increased significantly because of the increasing exchange of data in services such as the Internet, e-mail and data file transfer. The capabilities needed to deliver such services are characterized by an increasing need for data throughput (Gutierrez et al., 2003). However, the emergence of an “intelligent ubiquitous environment” has added a new concept to the development of wireless networking over recent years. The term “ubiquitous” means that the network computation has been extensively expanded and absorbed into the everyday living space, where computers integrate

seamlessly into the background environment to assist and provide services for users (Gill, 2009).

Wireless Sensor Networks (WSNs) provide an emerging research area for studying “ubiquitous computing environments”. Applications for WSNs can be found in industrial automation, agricultural, vehicular, residential, medical sensors, and actuators that have more relaxed data throughput requirements (Howitt and Gutierrez, 2003). WSNs utilize micro wireless sensor nodes to enable information sharing in the same network by monitoring their surrounding environment. Like any sentient organism, ubiquitous computing environments rely first and foremost on sensory data from the real world (Lewis, 2004). Therefore the sensory data in WSNs normally comes from multiple sensors of different modalities in distributed locations, and relies on wireless transfer. Due to the characteristic of wireless communication, the wireless signals, which actually carry the content of sensor information, will be open while they are being transmitted. It is therefore common for WSNs’ communication to be interfered with by unexpected wireless interference. To achieve reliable transmission in WSNs, the design of anti-interference measures must be given special consideration while the development of the relevant system is in progress.

The work outlined in this thesis primarily focuses on interference analysis and the development of mitigation strategies for IEEE 802.15.4 (IEEE Std802.15.4-2003, 2003) based WSNs. The implementation of WSNs does not specify the application of a specific protocol. Therefore, many WSN protocols have been proposed and are available in the literature (Demirkol et al., 2006). To design an efficient medium access control (MAC) protocol, the following attributes should be considered: energy efficiency, scalability, fairness, latency, throughput and bandwidth utilization (Ye et al., 2002). The IEEE 802.15.4 standard is one example of a wireless communication protocol designed to achieve ultra-low complexity, cost, and power consumption for low data rate wireless connectivity between low cost fixed devices (Lu et al., 2004). It has been widely adopted by various industries to develop “ubiquitous” applications since the standard is open and has excellent compatibility ensured by the Institute of Electrical and Electronics Engineers (IEEE) (Zheng and Lee, 2004).

1.2 Wireless Interference in IEEE 802.15.4 Based WSNs

IEEE 802.15.4 devices are designed to operate in the 2.4 GHz license-free frequency band for industrial, scientific and medical (ISM) use, which makes it widely acceptable in most countries. The ideal applications suitable for use with the IEEE 802.15.4 standard include industrial control and monitoring, asset and inventory tracking, intelligent home automation, and security. The IEEE 802.15.4 standards can be configured to allow multiple hops to route messages from any device to any other device on the network, or an IEEE 802.15.4 ad hoc network can be constructed on the basis of a peer-to-peer topology. The standard is applicable for large-scale deployment. Due to the wide popularity of wireless products, it is important for designers of IEEE 802.15.4 applications to consider interference caused by other systems employing different wireless technologies but working in the same frequency band (Won et al., 2005).

Since the 2.4 GHz ISM band has become particularly popular over the last few years, more and more commercial wireless products choose to operate in this band (ZigBee Alliance, 2007). A short list of possible users which might have effect on IEEE 802.15.4 networks includes 802.11b/g/n networks, Bluetooth Pico-Nets, Cordless Phones, Home Monitoring Cameras, Microwave ovens, etc (ZigBee Alliance, 2007). Among these potential interferers, the IEEE 802.11 b/g/n networks are the typical wireless systems that cause interference on IEEE 802.15.4 device operations. Primary research on the interference on IEEE 802.l5.4 systems has been carried out, and the relevant results are stated in the literature (Petrova et al., 2006; Shin et al., 2007; Yuan et al., 2007). The IEEE 802.11b standard is the most frequently mentioned interferer in the interference studies, as it is one of the earliest published industry standards and commercialized techniques working in the 2.4 GHz band (IEEE Std802.11b-1999, 2003). The IEEE 802.11b standard is designed for extending the coverage of the local area network. The deployment of wireless networks conforming to the IEEE 802.11b standard has experienced immense growth in recent years and become the most widespread systems in the 2.4 GHz ISM band (Mishra et al., 2003). IEEE 802.11b

compliant networks are often deployed to provide service for Internet access and multimedia applications. Typically, multiple IEEE 802.11b access pointes are deployed to construct a widely connected network for users roaming around the desired area. In the deployment of IEEE 802.15.4 ad hoc networks for large scale applications, e.g. environment monitoring or building lighting system, the IEEE 802.15.4 network communications relying on multi-hop transmission frequently need to cross part of, or the whole target area (Wheeler, 2007). If both IEEE 802.11b and IEEE 802.15.4 networks are deployed within the same area, interference will not be avoidable when they are in close proximity (Won et al., 2005).

The direct consequences of wireless interference are intermittent network connectivity, packet loss and low network throughput. The root causes can be classified into two broad categories: static and dynamic. The static causes mainly include relative location between the interferer and WSNs, transmission power, frequency, modulation, etc. The dynamic causes relate to factors, which cannot be anticipated at network design time, e.g. interferers temporarily emerge whilst WSNs are in operation (Musˇaloiu-E et al., 2008).

1.3 Research Challenges

The research in this thesis investigates the effects of wireless interference on the operations of WSNs. The IEEE 802.15.4 standard and IEEE 802.11b standard are chosen for research to construct the WSNs and act as wireless interferer respectively. The fact that wireless medium for communication is vulnerable to external interference presents a challenge to wireless system interference study. The level of interference is in general determined by the following factors of interference duration, interference density, and interference pattern which are difficult to predict in advance. In particular, the use of multi-hop transmission for IEEE 802.15.4 ad hoc network has a significant chance of being affected by interference, since the unsuccessful establishment of a communication link between any two hops can result in overall data transmission failure. Additionally, WNSs are resource limited and as such do not have sufficient hardware computation capability to implement complex anti-interference

algorithm, unlike more relatively powerful wireless systems, such as dynamic modulation switching in IEEE 802.11b devices (Heusse et al., 2003).

1.4 Motivation for the Research

As discussed, the use of WSNs extends people's sensing capability by pushing the concept of the "intelligent ubiquitous environment" in the real world. In order to successfully implement the operations of WSNs, the associated interference challenges, which might affect the communication infrastructure of the WSNs, must be addressed. Additionally, in the field of interference study in WSNs, most existing research output has focused on analytical studies, whereas system-level solutions are relatively infrequent. There remains a considerable demand for knowledge transfer in order to fill the gap between academic research and practical applications. The approach adopted in this thesis is to evaluate the effect of interference on IEEE 802.15.4 based WSNs, and then extend the knowledge obtained into practical applications in order to improve any developed system's performance under interference.

1.5 Research Objectives and Contributions

1.5.1 Research Objectives

The research objectives of this study are listed as follows:

- Investigate the existing literature available on IEEE 802.15.4 based WSNs and the associated interference analysis.
- Carry out research of the relevant literature on anti-interference measure for WSNs to obtain a better understanding of how to design effective strategies, and make further improvement.

- Propose and evaluate approaches for enhancing the capability of IEEE 802.15.4 based WSNs to be maintainable and operable when being affected by unexpected interference. In particular:
    - Propose network communication models for IEEE 802.15.4 based WSNs using star topology and peer-to-peer topology, and evaluate the models to obtain the benchmark of the system.
    - Propose interference models according to different interference scenarios to present the interactions between IEEE 802.15.4 network operations and IEEE 802.11b interference activity, mainly in order to address the issues which require consideration when designing IEEE 802.15.4 based WSNs and obtain the benchmark of interference effectiveness.
    - Propose a strategy to enhance IEEE 802.15.4 based WSNs network connectivity while suffering interference.
    - Propose a strategy to enable intelligent interference judgment for IEEE 802.15.4 based WSNs while suffering interference.
    - Propose a feasible mechanism to achieve reliable transmission and support data recovery in IEEE 802.15.4 based WSNs.
    - Evaluate the effectiveness of the proposed strategies by comparing with the benchmark obtained by interference models within the laboratory environment.
    - Evaluate the effectiveness of the proposed strategies by integrating them into typical applications and testing in a practical environment.

1.5.2 Contributions of the Research

This thesis aims to develop a methodology for IEEE 802.15.4 based WSNs to make correct adjustments through energy detection, channel agility and data recovery in order to avoid or mitigate the effect of interference, especially interference from IEEE 802.11 systems. The contribution of this thesis consists of five parts. Firstly, a method is proposed to enable an IEEE 802.15.4 system to maintain normal communications by using the process of consecutive transmissions when the system's default mechanism is insufficient to ensure successful transmission rates during a period of IEEE 802.11 interference. Most of the related work proposes a channel switch when the current IEEE 802.15.4 communication channel is suffering interference. There are some non-overlapping channel settings, which exist for IEEE 802.15.4 system and IEEE 802.11 system, and channel switching to such a channel can obviously reduce the interference effect from an IEEE 802.11 system. However, it is still possible that all the defined communication channels in the IEEE 802.15.4 standard have been affected by multiple IEEE 802.11 networks, which means that such a simple mechanism of channel switching will be ineffective. Therefore, it is crucial to develop a method that can help WSNs maintain acceptable network connectivity under such circumstances without frequent channel switching.

Secondly, a novel strategy is proposed for an IEEE 802.15.4 system to estimate the interference pattern, and accordingly adjust system parameters for the purpose of achieving optimised communication effectiveness during a period of interference. The strategy is feasible to implement, and requires neither hardware changes nor IEEE 802.15.4 protocol modification. In the study of interference, very few researchers emphasise interference pattern research, as typically the interfering signal is unknown to the victim, i.e. IEEE 802.15.4 system. However, by properly setting energy detection periods, the IEEE 802.15.4 device can sense the pattern of interference to a certain degree and further adjustment can be made on the basis of the interference information obtained.

Thirdly, a hardware based reliable multi-hop transmission strategy is proposed. Since the deployment of IEEE 802.15.4 based WSNs may cover a

relatively large area, the adoption of multi-hop transmission within such an ad hoc network is necessary (Krishnamurthy and Sazonov, 2008). Most WSN protocols, which includes IEEE 802.15.4 standard, only define the use of the physical layer (PHY) and medium access control (MAC) layer. The definition for network layer and transport layer are normally not specified due to limited computation resource carried by WSN nodes. Once some wireless communication links which have been established between WSN nodes suffer interference, the final data integrity will be affected due to the lack of higher layer supports. By adding additional control methods, and building up redundancy in the IEEE 802.15.4 based WSNs, the interference effect can be limited, and the lost data can be recovered as much as possible.

The fourth contribution is an application design for integrating an IEEE 802.15.4 based WSN into a home automation system. The use of WSN in home automation is mainly for providing environmental data, e.g. temperature, humidity, light, in order to develop a "smart house". The IEEE 802.15.4 technique is suitable for establishing such a network since it was particularly developed for executing such low cost, and low complexity sensing tasks. However, the WSN operations can possibly be affected by other powerful wireless systems or signals working in the same frequency band, especially the IEEE 802.11b system, since many home users are using this system for their Wi-Fi broadband. The system designed for this home automation application emphasises the use of consecutive retransmission and channel switching to achieve the data provision for a home controller to ensure the desired home management.

The fifth contribution presents a complete analysis and complete system design for an IEEE 802.15.4 based safety-monitoring system in the building environment. The use of WSN in a building environment needs to consider more issues, which includes static WSN deployment, dynamic interference issue, etc. The designed system has been tested and successfully implemented in a relevant research project.

1.6 Organization of the Thesis

The structure of this thesis is as follows: Chapter 2 reviews the IEEE 802.15.4 based WSNs and the types of interference that can affect the operations of the IEEE 802.15.4 networks. Chapter 3 gives a detailed review of the state-of-art of research into the interference analysis in IEEE 802.15.4 based WSNs, and discusses the approaches proposed by other researchers to mitigate interference effects. Chapter 4 describes the proposed interference mitigation strategy for maintaining network connectivity in an IEEE 802.15.4 based WSN with a star configuration. Chapter 5 presents a novel approach for an IEEE 802.15.4 based WSN to intelligently sense the state of interference pattern on the basis of energy detection. Chapter 6 introduces a feasible data recovery strategy aiming at achieving reliable transmission in an IEEE 802.15.4 based ad hoc WSN. Chapter 7 introduces the system design for deploying an IEEE 802.15.4 based WSN in a home automation application. Chapter 8 introduces the system design for deploying an IEEE 802.15.4 based WSN in a large-scale building environment monitoring application. Finally, Chapter 9 summarizes the main contributions of the research and concludes the thesis by identifying areas for future research.

Chapter 2 IEEE 802.15.4 Based WSNs

2.1 Introduction

This chapter provides a comprehensive review of IEEE 802.15.4 based WSNs, and explains the basic concepts of interference in wireless communications. The purpose of this chapter is mainly to conduct a thorough review of the development of WSNs and the IEEE 802.15.4 standard.

2.2 Overview of Wireless Sensor Networks

2.2.1 Wireless Sensor Networks

One of the features of the post-PC era is the movement of computation from desktops and data centres into the physical world to achieve "ubiquitous computation" (Yao and Gehrke, 2002). WSNs form one strand in this development. This post-PC era extends human beings' capability to monitor and control the physical environment.

Recent Integrated Circuit (IC) and Micro Electro Mechanical System (MEMS) have matured to the point where they enable the integration of wireless communications, sensors and signal processing together in one low-cost package (Schurgers and Srivastava, 2001). Such a package (i.e. sensor nodes) is equipped with data processing and communication capabilities. It is now feasible to deploy

ultra-small sensor nodes in many kinds of areas to collect information. The sensing circuitry measures the ambient condition related to the environment around the sensor and transforms them into measurable signals. After necessary processing, the signals are sent to a pre-defined destination via a radio transmitter. All of these operations are powered by batteries for ease of deployment, since a traditional power supply (i.e. mains power) may not be applicable.

WSNs consist of a number of sensor nodes. They are deployed inside or very closely to the phenomenon they are investigating. Under most situations, the topologies of the WSNs do not need to be engineered or pre-determined (Cardei and Wu, 2004). This allows WSNs to be deployed randomly. For example, sensor nodes used to monitor a forest will be deployed by being dropped from a plane and thus it is impossible to locate their landing position accurately. This feature of random deployment also requires WSN protocols to possess capability to self-organize. Another important feature of WSNs, which is different from traditional senor networks, is the integration of microprocessors (Vieira et al., 2003). Traditionally, the sensor nodes in a sensor network are designed to return the raw data when polled by the central controllers. Since a central controller does not physically control the sensor nodes in the WSNs through a cable, the on-board microprocessor must be capable of implementing information processing and relative complex communications wirelessly. The introduction of this computation capability makes WSNs more intelligent in comparison with wired sensor networks. Figure 2.1 shows the structure of a typical wireless sensor network.

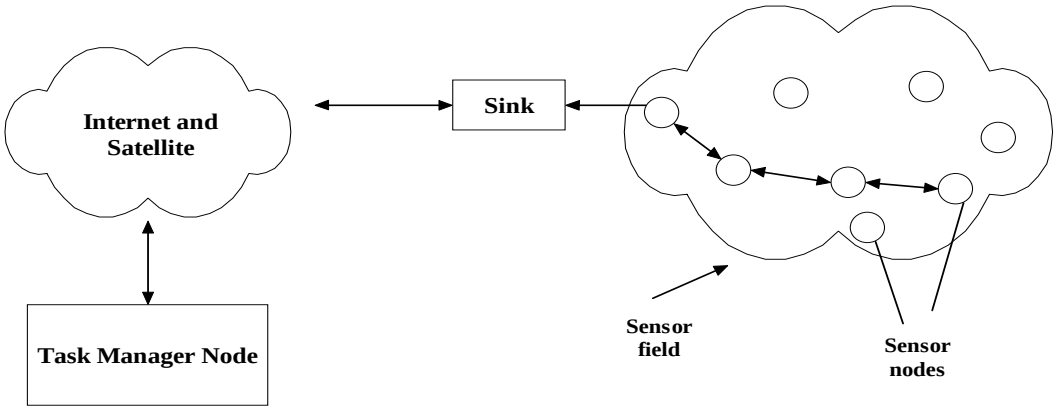

Figure 2.1 Structure of a typical wireless sensor network (Akyildiz et al., 2002)

In Figure 2.1, a typical wireless sensor network is depicted. It includes sensor nodes, sink node, a connection to the Internet or satellite and a task manager node. Sensor nodes do not have a fixed location and most of them are randomly deployed to monitor a sensor field. Sensor nodes usually communicate with each other via an on-board radio system using a multi-hop approach. After primary processing, the data gathered from the sensor field is sent to a base station (sink) which is responsible for transferring data to another network. This function makes a sink similar to a gateway in a traditional network. Finally, the useful data are delivered to the task manager node and become available to the users (Akyildiz et al., 2002).

2.2.2 Wireless Sensor Nodes

Wireless sensor nodes are the basic component of wireless sensor networks. A generic sensor node hardware structure consists of several subsystems (see Figure 2.2): a microprocessor, data storage, sensors, actuators, a data transceiver, and an energy source (Benini et al., 2006).

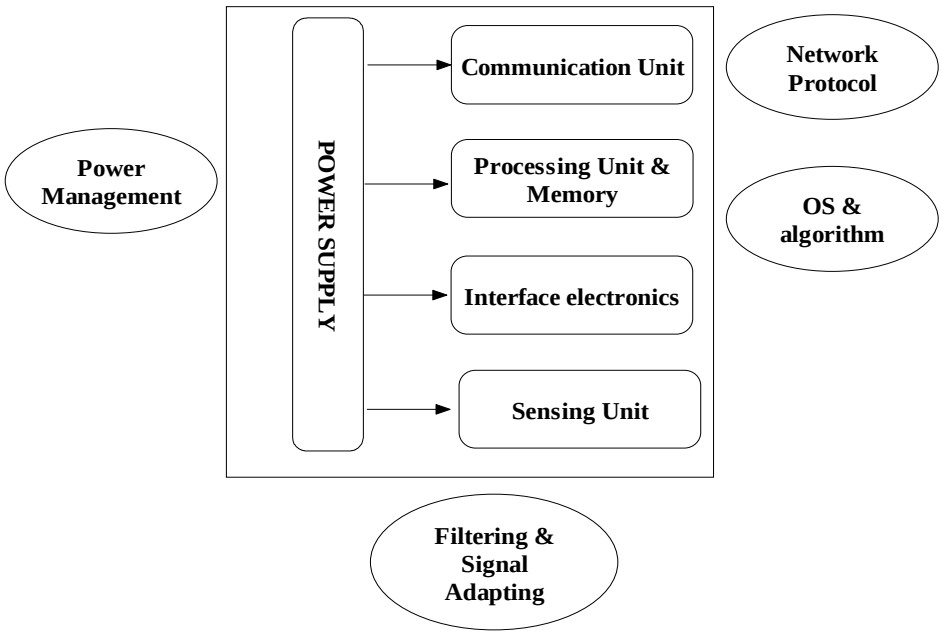

Figure 2.2 Sensor node functional components (Benini et al., 2006)

In Figure 2.2, the “Filtering & Signal Adapting” and “Sensing Unit” components are for implementing the sensing task. Usually sensors are only sensitive to the specified content. “Filtering & Signal Adapting” can remove unwanted elements from the sensing target provided to the “Sensing Unit”. The “Interface electronics” part is mainly used for converting detected sensor information into the digital form. Sensor data can be easily read out by the connected controllers through a standard digital communication interface (e.g. Inter-Integrated Circuit, Serial Perioheral Interface Bus). The “Processing Unit & Memory” and “Communication Unit” parts are responsible for implementing local computation and establishing communication link with external controller that connects to the sensor. The “Power Management”, “OS & algorithm” and “Network protocols” provide the system with necessary software support (Benini et al., 2006).

2.2.3 Design Challenges

The features of WSNs make them suitable in a wide range of application areas. In military applications, WSNs are ideal for the task of battlefield

surveillance, because they provide a low risk level for personnel. For civilian applications, WSNs are often used for building environment monitoring, home automation, industrial control, and assets management in logistics industry, etc. By reviewing the characteristics of WSNs and the corresponding application areas, the challenges for developing WSNs can be concluded as follows:

- Limited power supply. Since the deployment of WSNs is supposed to be random and requires little or no infrastructure involvement, the power supply for driving wireless sensor nodes is mainly provided by a battery (Qi et al., 2002). This is a most important factor which seriously limits the use of WSNs. WSNs are designed to work in unattended areas or, work alone over a considerable long period of time as frequent battery replacement might not easily be achieved.
- Limited effective range of the wireless communication. The transmitter and receiver used by a wireless sensor node are normally powered by a battery. Among the typical components composing the wireless sensor node, the radio transmitter consumes the most energy. Since current technology cannot provide a long-term power supply without replacing the battery, WSNs often limit the transmission power as an effective way to save energy use on wireless sensor node (Cardei and Wu, 2006). Consequently, the effective transmission range of the WSN nodes is restricted.
- Large number of wireless sensor nodes within a WSN. A wireless sensor network often consists of a large number of sensor nodes in order to provide an effective sensor field as required. They can easily cover a relatively wide area. This characteristic makes it impossible for users to maintain the whole network manually. Comprehensive management architecture is required to monitor the WSNs, configure network parameters and implement system updating (Wagenknecht et al., 2008).
- Dynamic changes of the network formation. The topology of WSNs may not be static in the network area. Sensor nodes can easily die and new sensor nodes may be randomly added to the network. All of these require

that the sensor network should have the ability to adjust itself when the topology of the network has changed (Bharathidasan and Ponduru, 2003).

- Management of data flow. In WSNs, each sensor node will generate sensory data and transfer to the specified task manager node for further processing. As a consequence of the characteristics of wide deployment and limited wireless communication range, the implementation of data acquisition and transfer require the involvement of dedicated communication protocols. The use of a strong strategy to manage distributed data flow, query and analysis is important to sensor networks (Elnahrawy, 2003).

2.3 Overview of IEEE 802.15.4 Standard

2.3.1 Wireless Personal Area Network

Prior to WSNs, the primary research and industrial activities in the technology of wireless networking were mainly concerned with high data throughput and increasing communication range in applications, e.g. home entertainment, e-business, Internet browsing. However, the need to construct networks to support "ubiquitous computation" has changed the focus of research. Limited bandwidth, flexible data throughput and low cost are the main features of "ubiquitous computation" network that differ from normal wireless techniques (Weiser, 1993).

Although there are various wireless standards, including IEEE 802.11a/b/g/n, WiMax, GSM, etc, most of these are not suitable to implement "ubiquitous computations" due to their high power consumption (Kim et al., 2008). Wireless Personal Area Network, a new network paradigm based on short-range wireless connectivity has attracted researchers and industrial attention in the last few years (Prasad et al. 2001). The definition of wireless personal area network (WPAN) is that "it is a simple, low-cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements". The main objectives of a WPAN are ease of

installation, reliable data transfer, short-range operation, extremely low cost, and a reasonable battery life while maintaining a simple and flexible protocol (IEEE Std802.15.4-2003, 2003). Figure 2.3 shows a comparison of operating characteristics of various wireless standards.

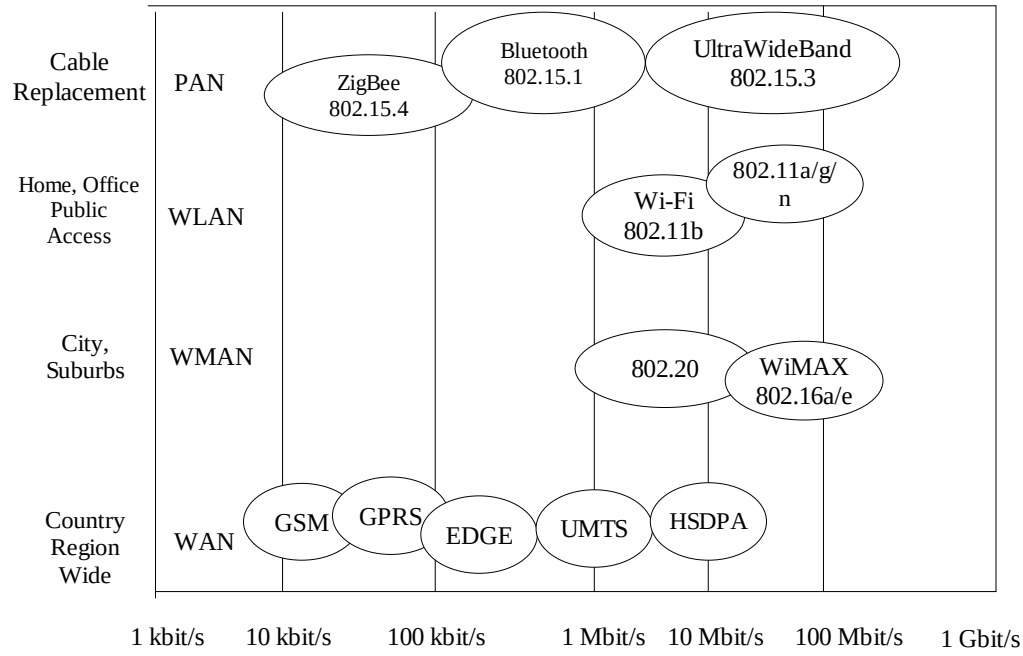

Figure 2.3 Wireless communication standards and their characteristics (Benini et al., 2006)

In Figure 2.3, the wireless standards are categorized according to the supported throughputs, communication range and application areas. The standards such as Wi-Fi, WiMAX, UltraWideBand, and 802.11a/g/n are normally used for high data throughput applications, and generally require main power supply, which make them unsuitable for WSNs. The systems constructed on the basis of Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Enhanced Data Rate for GSM Evolution (EDGE), Universal Mobile Telecommunications System (UMTS) and High-Speed Downlink Packet Access (HSDPA) were for the purpose of achieving full mobility. The design of infrastructure for mobile system is not applicable for WSNs use as most WSNs are static during their lifetime. The Bluetooth standard was mainly developed for computer cable replacement. Its data rate (1 Mbit/s) and defined power

consumption are relatively high. Thus the Bluetooth standard is not a suitable choice for battery driven WSNs.

The IEEE 802.15.4 and ZigBee standards, however, were developed for WSNs. The supported data rate ranges from 20 to 250 kbps, depending on the frequency band used. Regarding the sensor readings whose data length is typically a few bytes, a low data rate can save energy and extend the systems' lifetime, which is very important for WSNs. IEEE 802.15.4 is a public standard developed for low data rate, low power consumption and low cost wireless protocol (IEEE Std802.15.4-2003, 2003). ZigBee technology is a global application protocol targeted towards automation and remote control application (ZigBee Alliance, 2007). The communication protocol defined in the ZigBee standard is built on the basis the of the IEEE 802.15.4 standard.

2.3.2 IEEE 802.15.4 Standard

IEEE 802.15.4 technology is a low data rate, low power consumption, and low cost wireless networking protocol targeted towards automation and remote control applications (Ergen, 2004). The standard defines characteristics of physical and MAC layers for Low-Rate Wireless Personal Area Networks (LR-WPAN). The main advantages of LR-WPAN are ease of installation, reliable data transfer, short-range operation, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol stack (Baronti et al., 2007).

The architecture of the IEEE 802.15.4 standard is defined in terms of a number of layers. Each layer is responsible for a specified task, and provides services to the higher or lower layers. As a 'network-aware' standard, the division of these layers can be described by the Open System Interconnection Reference Model (Freescale, 2007). However, to achieve a low complex wireless communication protocol, only the PHY layer and MAC layer are defined in the standard. A comparison of the IEEE 802.15.4 architecture and open systems interconnection (OSI) Seven Layer Model is shown in Figure 2.4.

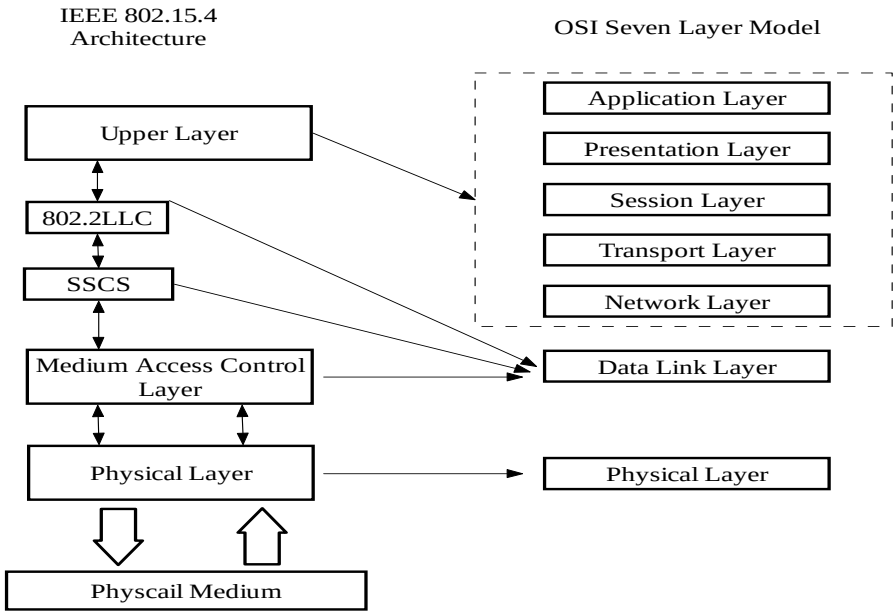

Figure 2.4 Architecture comparison of IEEE 802.15.4 and OSI Seven Layer Model (Freescale, 2007)

In Figure 2.4, the PHY layer of the IEEE 802.15.4 standard is related to the PHY layer in the OSI Seven Layer model. The PHY layer describes the physical properties of the communication network, which can include the electrical properties and signalling properties of the medium, etc. The Medium Access Control Layer, Service Specific Convergence Sublayer (SSCS), and Logical Link Control (LLC) are related to the Data Link Layer in the Seven Layer model. The Medium Access Control generally determines the medium access. The Logical Link Control and Service Specific Convergence Sub -layer provide multiplexing of protocols transmitted over Medium Access Control, optional flow control, and any requested detection and retransmission of dropped packets. The other five additional layers in the OSI Seven Layer model are not supported by the IEEE 802.15.4 standard, as a “simple and flexible protocol” is the primary objective for the IEEE 802.15.4 task group (Freescale, 2007).

- Physical Layer

The IEEE 802.15.4 standard offers two PHY options for the frequency band. The supported data rates are 250 kbps at 2.4GHz, 40 kbps at 915MHz and 20kbps at 868MHz. These frequency bands are all based on Direct Sequence

Spread Spectrum (DSSS). A total of 16 channels are available at 2.4 GHz, numbered 11 to 26. There is a single channel at 868 MHz, and 10 channels at 915MHz. Since the IEEE 802.15.4 standard is intended to comply with established regulations in most countries, the unlicensed 2.4 GHz band is more popular (Kinney, 2003), and mainly considered in this thesis. The IEEE 802.15.4 standard supports a 64-bit long address and a 16-bit short address, theoretically resulting in a single network being able to support a maximum of $2^{16} \approx 65{,}000$ devices.

Devices compliant with the IEEE 802.15.4 standard are required to control power output at around 0 dBm, and typically operate within a 10-meter range. The adopted transmission scheme and modulation technology are DSSS and offset quadrature phase-shift keying (O-QPSK) respectively. Table 2.1 summarizes the properties defined in the IEEE 802.15.4 PHY layer.

Table 2.1 Summary of PHY layer in IEEE802.15.4 standard (IEEE Std802.15.4-2003, 2003)

Property	Range	
Frequency Band	BPSK	868 MHz 1channel 20 kb/s
		915MHz 10 channels 40kb/s
	O-QPSK	2.4GHz 16 channels 250kb/s
Range	10-20 meters	
Addressing	16-bit short address or 64-bit IEEE address	

- MAC Layer

The IEEE 802.15.4 standard defines an efficient low duty-cycle working style for devices designed to implement simple functions with minimal power consumption requirements. There are two types of devices supported in the IEEE 802.15.4 standard: Full Function Device (FFD) and Reduced Function Device (RFD). A FFD can operate in an IEEE 802.15.4 network serving as a personal area network (PAN) coordinator, a coordinator, or a router device. A RFD can

operate as a network device for implementing extreme simple functions. An IEEE 802.15.4 network can be organized into one of two topologies: the star topology and the peer-to-peer topology (see Figure 2.5).

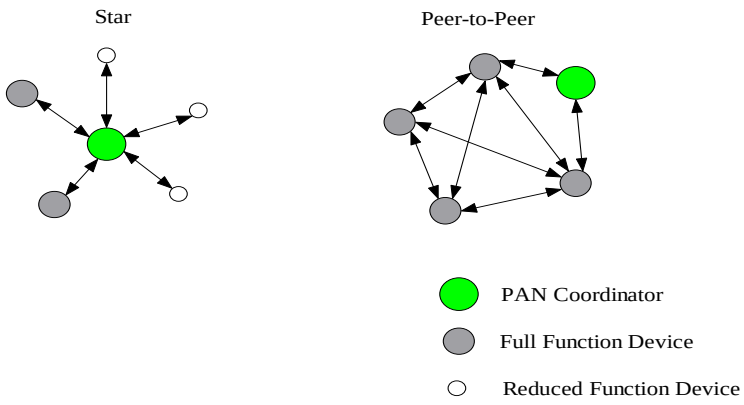

Figure 2.5 Two supported topologies in the IEEE 802.15.4 standard

In the star topology, a FFD serving as a coordinator is specified to be the central device, which is called the PAN coordinator, and starts the whole network. Other coordinators and network devices must join the network by associating themselves with the PAN coordinator. The PAN coordinator controls all network communications.

The peer-to-peer topology also requires a PAN coordinator to initialize the network start-up procedure. However, the communications within a network are based on the peer-to-peer topology and are not limited by the PAN coordinator. Any device can freely talk to any other device so long as they are within an effective communication range.

The IEEE 802.15.4 MAC layer allows the use of the superframe structure. A superframe is defined by the PAN coordinator and bounded by network beacons. The beacons are used to synchronize the devices attaching to the PAN coordinator. Each superframe is equally divided into 16 slots. Figure 2.6 shows the structure of a superframe.

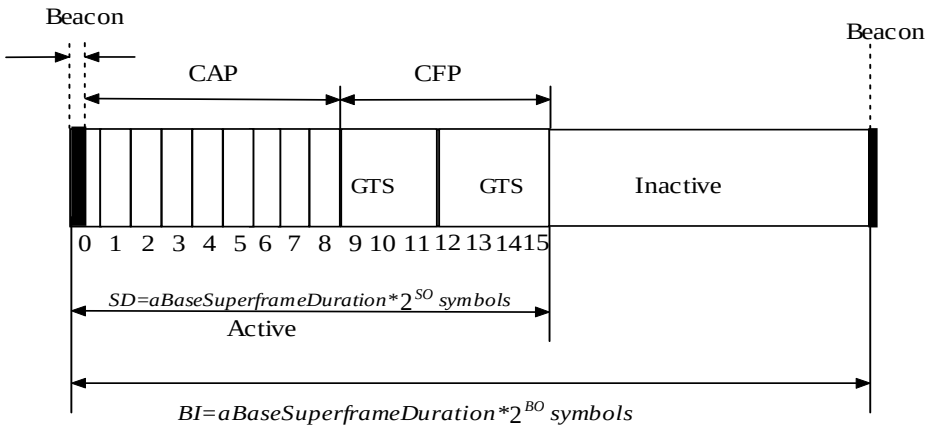

Figure 2.6 Structure of superframe (IEEE Std802.15.4-2003, 2003)

A superframe consists of two main sections: an active period and an inactive period. The active portion is divided into 16 equal time slots (slots 0 to 15 in Figure 2.6) and contains a Contention Access Period (CAP) and Contention-Free Period (CFP). The beacon frame is included in the first slot of the superframe. During CAP, network devices compete for channel access using the mechanism of slotted Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA). In CFP, the PAN coordinator is responsible for administrating and assigning Guaranteed Time Slot (GTS), within which only the selected network devices can commence transmission without contending for channel access. A GTS can occupy more than one slot period. The length of the active period, Superframe Duration (SD), is denoted as follows (IEEE Std802.15.4-2003, 2003):

$$SD = aBaseSuperframeDuration * 2^{SO} symbols \quad (2.1)$$

where *aBaseSuperframeDuration* denotes the number of symbols (a symbol is a fixed time duration at 16 μs) forming a superframe when the *SuperframeOrder* (SO) is equal to 0. According to the IEEE 802.15.4 standard, the value of *aBaseSuperframeDuration* is 960 symbols, which is equal to 15.36 milliseconds. SO describes the length of the active portion of the superframe, which ranges from 0 to 15. The *BeaconInterval* (BI) including active portion and inactive portion of a superframe is denoted as follows:

$$BI = aBaseSuperframeDuration * 2^{BO} symbols \quad (2.2)$$

where *BeaconOrder* (BO) describes the beacon interval ranges from 0 to 15. The values of SO and BO are related as follows: $0 \le SO \le BO \le 14$. If $0 \le SO < BO \le 14$, the difference between the SD and BI is an inactive period, in which all network communications remain idle until the arrival of the next beacon. In order to save energy, the devices' transceivers can move into a sleeping mode during the inactive portion. If $0 \le SO = BO \le 14$, the inactive portion is ignored, as the length of the beacon interval is equal to the active portion. If BO is equal to 15, the value of SO should be ignored and the superframe will not exist, which is used for non-beacon enabled networks. If the nonbeacon-enabled mode is in use, all network devices commence transmission with the mechanism of un-slotted CSMA-CA.

In a beacon-enabled network, the beacon frame is periodically transmitted by the PAN coordinator to allow all the network devices to synchronise with it. All network transactions are only permitted to begin during the active portion. Although the use of a beacon frame can establish a unified network device management, the synchronization in a large-scale deployment is difficult to achieve, as the effective radio sphere of the PAN coordinator is restricted. As a result, the nonbeacon-enabled mode is more popular in existing applications (Koubaa et al., 2007). This thesis thus mainly focuses attention on nonbeacon-enabled IEEE 802.15.4 network.

2.4 Summary

This chapter has provided an overview of IEEE 802.15.4 based WSNs. The basic idea of WSNs is to collect environment information by employing distributed sensor nodes and enable the achievement of "ubiquitous computation". After simple processing, the sensory data are transferred to a specified sink node for further use. Generally, data transfer from the end sensor node to the sink node is implemented by using proper communication protocols. Since WSNs are originally designed to use radio signals to convey information, the wireless communication links established in the WSNs are vulnerable in the radio environment. Issues caused by wireless interference must be analyzed and dealt with.

Chapter 3 Interference Analysis in IEEE 802.15.4

3.1 Interference Overview

Multiple wireless systems working in close proximity might reasonably raise concerns about overcrowding in the unlicensed 2.4-GHz ISM band. Therefore, the performance of IEEE 802.15.4 based WSNs in the presence of interferers such as IEEE 802.11 and Bluetooth should be evaluated, particularly for applications in which resources and bandwidth allocation cannot be guaranteed (Jennic, 2008).

The challenge for analyzing the effect of interference is the uncertainty of possible interference scenarios. There is no fixed interference model as different network sizes, configurations, interference sources and environmental conditions can produce different effects. The interference studies usually give consideration to various aspects, e.g. channel allocation, inter-packet delay, packet payload size and output power (Jennic, 2008). These aspects are usually combined during the process of interference analysis in order to determine the typical characteristics of an interferer and the expected traffic patterns in the network. This chapter will review the techniques used in the IEEE 802.15.4 standard in order to enable an IEEE 802.15.4 device to coexist with other wireless devices, and the relevant interference mitigation strategies proposed by researchers.

3.2 Basic Concept of Interference

3.2.1 Interference Definition

Interference in the context of wireless communication usually refers to one of the following two definitions: (1) multiple (more than two) simultaneous packet transmissions causing packets to collide at the receiver, (2) physical factors in the radio propagation channel (Golmie, 2006). Figure 3.1 illustrates the typical function block diagram of the transmitter and receiver in a wireless system.

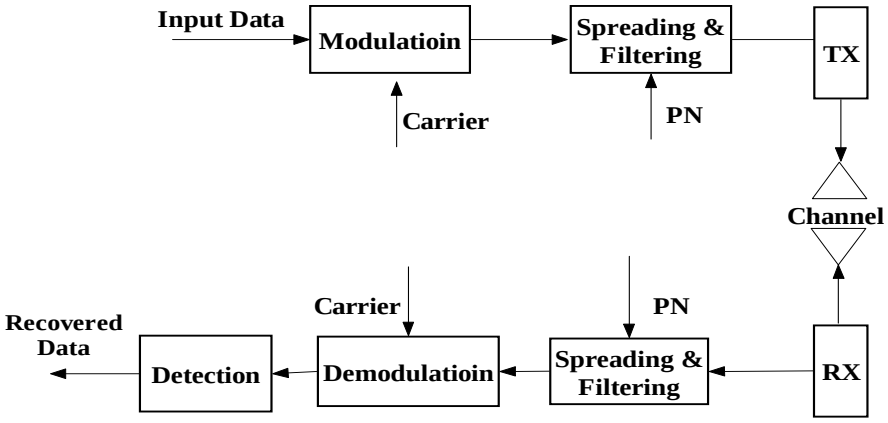

Figure 3.1 Typical components in physical layer (Golmie, 2006)

In Figure 3.1, the input data passed from the upper layer of the system is sent into the “Modulation” function block. The “modulation” function converts the bit stream containing the input data into a waveform (i.e. Carrier in Figure 3.1), which can be sent over an analog channel. The function of “Filtering” is designed to select the desired signal and minimize the effect of noise and interference. “Spreading” is a specialized function designed to deliberately transmit the signal over additional bandwidth with the specified pseudo-random noise (PN) sequence, using less power per frequency, but more frequencies. The “Tx” and “Rx” denote the use of a transmitter and receiver in communication. The “Channel” is a virtual concept that describes the range of radio frequency over which the wireless communication takes place. The implementation of the

functions “Demodulation” and “De-spreading” is the opposite process of “Modulation” and “Spreading”, by which the received wireless signal can be recovered. The “Detection” function is the last processing stage before the receiver obtains the effective binary data. Because the transmitted signal processed by the “Demodulation” function is a combination of N orthogonal waveforms, the receiver must make a comparison between the waveforms and the standard reference signals to determine the exact data that the waveforms contain.

If multiple wireless signals simultaneously arrive at the receiver, the receiver will be unable to abstract any useful information since the desired signal and interfering signal overlap each other.

The physical factor in the radio propagation channel is another challenge to wireless communication systems. Various physical impediments, such as multipath propagation should be taken into consideration for system design. Multipath propagation means that a transmitted signal can reach the receiver via several different paths (e.g. reflections from house, windows, or walls). Figure 3.2 shows an example of multipath propagation.

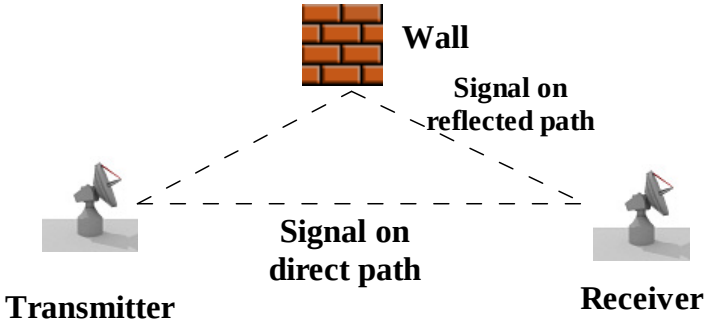

Figure 3.2 Example of multipath propagation

In Figure 3.2, the “signal on direct path” component between the transmitter and receiver is the desired wireless signal path, also called as “Line of Sight connection”. If some obstacle (e.g. like the wall in Figure 3.2) exists in the vicinity of the transmitter, the radio signal could be reflected and reach the receiver via the “reflected path”. Since a simple receiver cannot distinguish multipath signals, it just adds them up. Consequently, the “signal on direct path” and “signal on reflected path” interfere with each other (Molisch, 2005).

In the context of this thesis, the discussion of interference in WSNs is for the purpose of designing a system-level solution. Thus, the form of interference caused by multiple simultaneous packet transmissions is the main focus.

3.2.2 Performance Metric

In IEEE 802.15.4 WSNs, the performance metric used to evaluate the wireless communication can be separated into two parts: PHY layer and MAC layer.

A. PHY layer performance measures

The commonly used metric in the PHY layer of a wireless system is the signal-to-noise ratio (SNR), which denotes the ratio of the average signal power to the average noise power and is measured in decibels (dB). A radio system must transmit a modulated signal around a known frequency and receive it most of the time. If the SNR is less than the defined threshold, the receiver will fail to recover the desired signal (Chandra et al., 2007). Another important metric is the bit error rate (BER), which expresses the number of incorrectly received bits on the receiver side against the total number of transferred bits during a transmission. Because of the use of different modulation schemes, the requirements of SNR and BER for achieving an acceptable performance are different in certain wireless systems. Figure 3.3 illustrates the simulation results of BER at different SNR for various wireless standards.

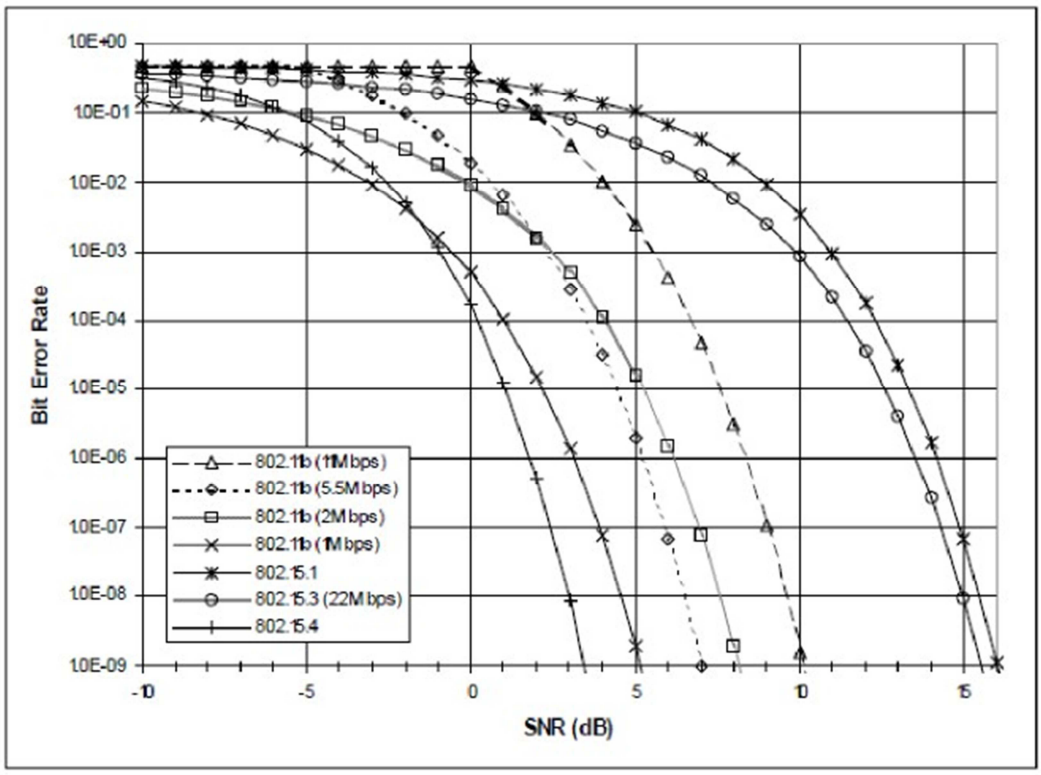

Figure 3.3 BER results for IEEE 802.11, IEEE 802.15.4, IEEE P802.15.3 and IEEE 802.15.4(IEEE Std802.15.4-2003, 2003)

In Figure 3.3, a general tendency is that a low bit error rate can be obtained when SNR increases. For example, if the IEEE 802.15.4 system is required to achieve bit error rate at 1.0E-0.9, the corresponding SNR should be greater than 3 dB.

B. MAC layer performance measures

Although the PHY layer metrics such as SNR and BER are important in describing wireless communication performance, the interference evaluation is concerned with quantifying other data, for example how many packets are successfully transmitted. The MAC layer consists of rules that regulate the mechanism of channel access and sharing. It is also responsible for assembling data packets sent to/from the PHY layer. In order to analyze the effect of interference in WSNs from a system level, the metrics of the packet error rate, transmission delay and throughput should be included (Shin et al., 2007).

- Packet Error Rate: Packet error rate is the percentage of packets lost, as the ratio between the number of packets, which fail to be received by the sink and all packets generated by the source node (Cuomo et al., 2007). One of the consequences caused by interference in WSNs is the increase in the packet error rate. It is the most important metric to validate if the anti-interference design is effective.
- Delay and Throughput: The throughput is the amount of data transferred from one station to another station during a specified period of time (Shin et al., 2007). The occurrence of interference in WSNs will obviously cause an increase in the delay and reduction of throughput, which could be improved by the effective anti-interference design from the level of system.

3.2.3 Factors Affecting Performance

The performance of IEEE 802.15.4 based WSNs in an environment of interference can be affected by many factors, including channel utilization, transmission power, effective data payload, transmission interval, implementation of routing protocol, etc. Under different circumstances (i.e. different application requirements), the same factors will produce different effects according to their own characteristics. The relevant research on the interference effectiveness have been extensively studied and will be discussed in the next chapter.

3.3 IEEE 802.15.4 Physical & MAC Layer Feature

During the design of the IEEE 802.15.4 standard, the 802.15.4 task group cooperated with other Coexistence Task Groups, such as 802.15.2TM to ensure the standard's coexistence capability with other wireless devices (IEEE Std802.15.4-2003, 2003). As a result, the IEEE 802.15.4 standard provides support for coexistence at both the PHY layer and MAC layer. At the PHY layer direct sequence spread spectrum is adopted, and at the MAC layer, Frequency

Divison Multiple Access (FDMA) and Carrier Sense Multiple Access (CSMA) anti-interference measures are adopted.

3.3.1 Direct Sequence Spread Spectrum

The license-free industrial scientific and medical (ISM) bands are crucial to the burgeoning market for wireless embedded technology. A short list of possible users and possible interferers includes: IEEE 802.11b networks, IEEE 802.11g networks, IEEE 802.11n networks, Bluetooth Pico-Nets, IEEE 802.15.4 networks, cordless phones, home monitoring cameras, microwave ovens and WiMax networks (ZigBee, 2007). The IEEE 802.15.4 standard adopts the technology of direct sequence spread spectrum (DSSS) to increase the opportunities for coexistence with multiple users.

The modulation technique “spread spectrum” is designed to promote a radio system’s capability of coexistence and robustness in the presence of interference. The spread spectrum approach originally appeared in military applications. It is used because of a number of attractive properties, e.g. anti-jamming performance, low probability of interception and multiple access communications (Fakatselis, 1996). In normal conditions, even though the centre frequencies of narrow band signals (signals that encode and transmit information use a small band) are not exactly the same, it is still possible to have signal collision and data packet loss. The frequency allocation is restricted and controlled by regulators such as the U.S Federal Communications Commission. However, there is no compulsory requirement in the ISM bands. Thus wireless interference could happen to any wireless system operating with narrowband signal (IEEE Std802.15.4-2003, 2003). Figure 3.4 illustrates collisions between two narrowband signals.

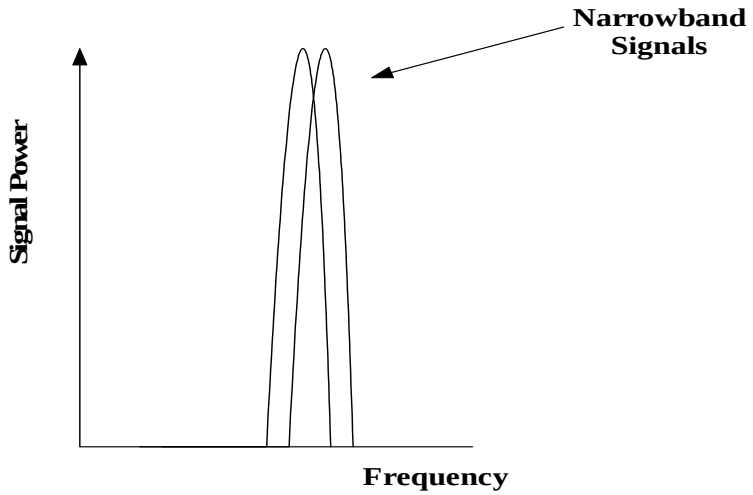

Figure 3.4 Narrowband signals (ZigBee, 2007)

In Figure 3.4, two narrow band signals collide with each other. Since the main bodies of these two signals overlap, the information carried by the overlapping parts could be corrupted due to interference. To avoid uncontrollable interference between narrowband signals, the overlapping parts should be limited. The way of “spread spectrum” was designed to solve the problem. Figure 3.5 illustrates the principle of “spread spectrum”.

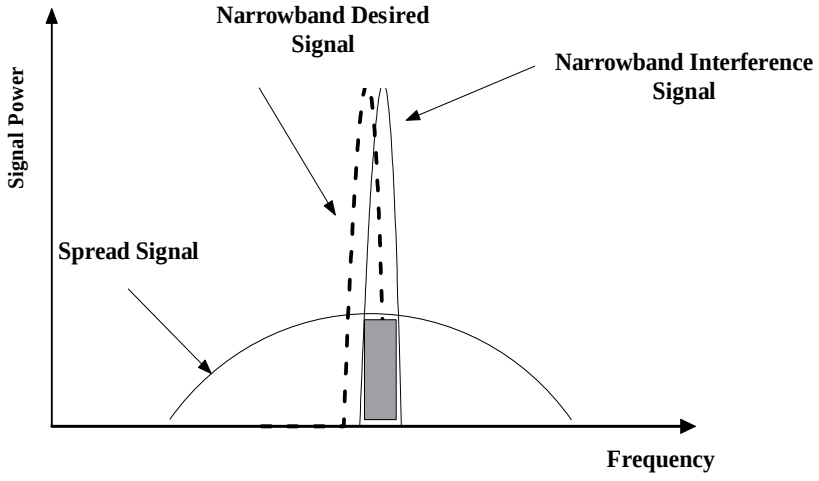

Figure 3.5 Principle of spread spectrum

In Figure 3.5, the two narrowband signals denote narrowband interference signal and narrowband desired signal (indicated by dashed line) respectively. The purpose of the "spread spectrum" approach is to use more bandwidth to convey the bit information originally carried by the narrowband desired signal. After spreading, only a small part of the original narrowband desired signal is affected by the narrowband interference signal (indicated by a fraction of gray cube in Figure 3.5). When the narrow band desired signal reaches the receiver, the system will abstract useful signals by taking action contrary to the "spread spectrum" (Figure 3.6).

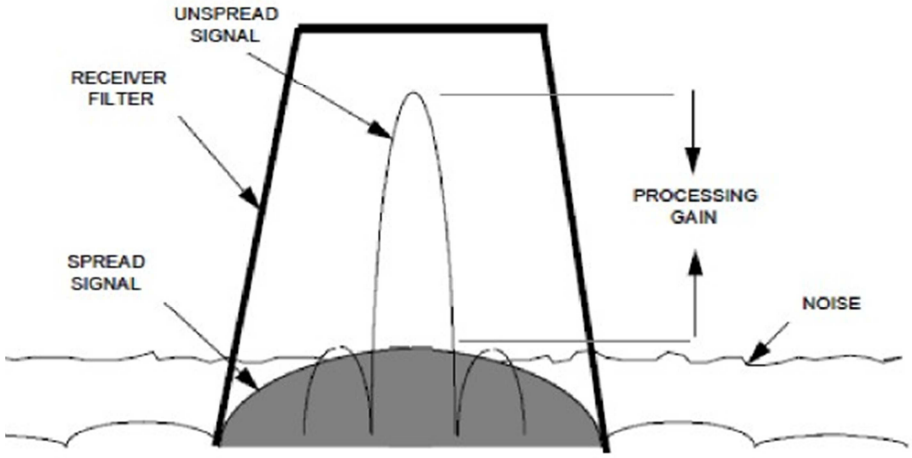

Figure 3.6 Direct spread spectrum at the receiver (Fakatselis, 1998)

In Figure 3.6, the spread spectrum signal is recovered into the form of "unspread" after passing through the receiver filter, whose main function is to make the receiver only be senstive to the signals working on the specifed frequency . Although some parts of the narrowband interference signal would pass through the receiver filter as well, it is highly possible to obtain the desired narrowband signal correctly since only a small portion of the spread signal is affected by the interference. Theoretically, if more bandwidth is used to convey the spread signal, the more interference can be tolerated. A common measure used in spread spectrum is the processing gain G (Golmie, 2006):

$$G = 10 \log(r_c / r_b) \qquad (3.1)$$

where r_b and r_c denote bit rate and chip rate respectively. In a DSSS system, the binary data r_b is multiplied by a pseudorandom noise (PN) binary source with a constant chip (i.e. expression of PN sequence) rate to complete frequency spreading operation (Fakatselis, 1996). The benefit of processing gain is that the PN code spreads the transmitted narrowband desired signal and makes it less susceptible to narrowband interference signal within the employed bandwidth. The processing gain can be thought of as the ratio of signal to interference at the receiver after the dispreading operation (Figure 3.6). For example, a wireless system requires 10 dB E_b / N_o (it is a normalized version of SNR, where E_b denotes the energy per bit, N_O denotes the noise power spectral density) to achieve a satisfactory performance with an acceptable bit error rate. If the process gain is 4 dB, the system can maintain the required performance when the desired signal has 6 dB (10 dB – 4 dB) over the interference. In an IEEE 802.15.4 system working in 2.4 GHz, the chip rate is 2000 kchip/s, and the bit rate is 250 kb/s. Therefore, the processing gain for the IEEE 802.15.4 device is 9 dB.

The use of DSSS in IEEE 802.15.4 systems adds the capability to effectively coexist with a narrowband wireless communication system (e.g. Bluetooth) whose bandwidth is smaller than the bandwidth of IEEE 802.15.4 (IEEE Std802.15.4-2003, 2003).

3.3.2 Frequency Division Multiple Access (FDMA)

The use of FDMA in an IEEE 802.15.4 system divides the 2.4 GHz ISM band into 16 non-overlapping channels as depicted in Figure 3.7.

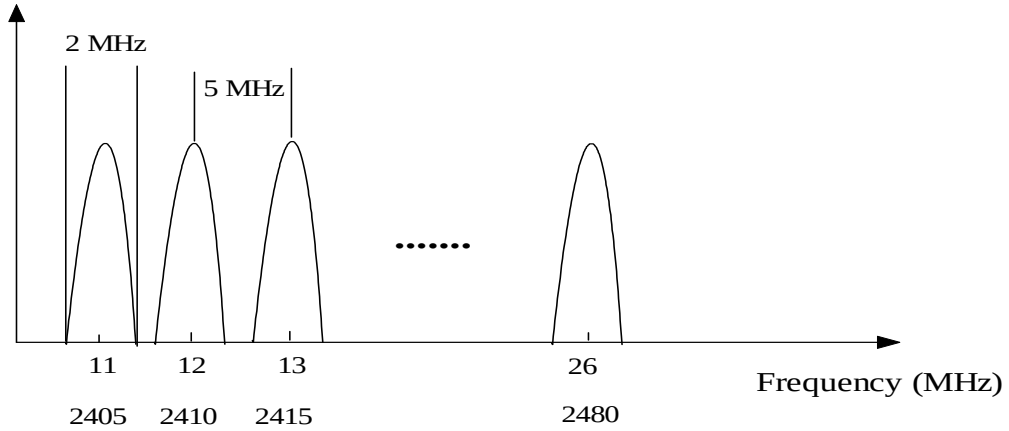

Figure 3.7 Channel allocation of IEEE 802.15.4 in 2.4 GHz band

In Figure 3.7, a total of 16 channels are defined in the 2.4 GHz band starting from 2405 MHz. Each channel is 2 MHz wide and 5 MHz apart. The setting of non-overlapping channels allows multiple users to operate separately on different frequencies without worrying about hearing each other. However, it does not guarantee that other wireless systems employing different channel allocation schemes would not overlap with the IEEE 802.15.4 communication channels in the same 2.4 GHz ISM band. For the convenience of study, two typical wireless standards (IEEE 802.11b and Bluetooth) are selected from the potential interferer list to discuss how interference happens. The IEEE 802.11b technique employs the same DSSS method as the IEEE 802.15.4 technique to achieve wireless communications on 2.4 GHz band. The Bluetooth defines another typical medium access method: frequency hopping.

- Wi-Fi System

Wi-Fi (IEEE 802.11b) technique, which is also well known as the Wi-Fi system, has been rapidly deployed to construct wireless local area networks in recent years. The first version of the IEEE 802.11b standard was published in 1999. The IEEE 802.11b standard defines a total of 14 channels. Each channel is 22 MHz wide, 5 MHz apart in frequency. Due to the wide bandwidth, many IEEE 802.11b communication channels overlap each other. In order to ensure multiple IEEE 802.11b networks simultaneously work in the same area, the frequency spacing between IEEE 802.11b communication channels must be at least 30 MHz

(So, 2004). Therefore, the IEEE 802.11 standard recommends that if multiple IEEE 802.11b networks are required to run in a close vicinity, three non-overlapping channels can be employed. The settings of three non-overlapping channels are not the same in different geographical regions: channels 1, 6, 11 are recommended in China and North American while channels 1, 7, 13 are selected in European (IEEE Std802.11-2007, 2007). Figure 3.8 shows the IEEE 802.11b non-overlapping channel allocations comparing with the IEEE 802.15.4 channel setting.

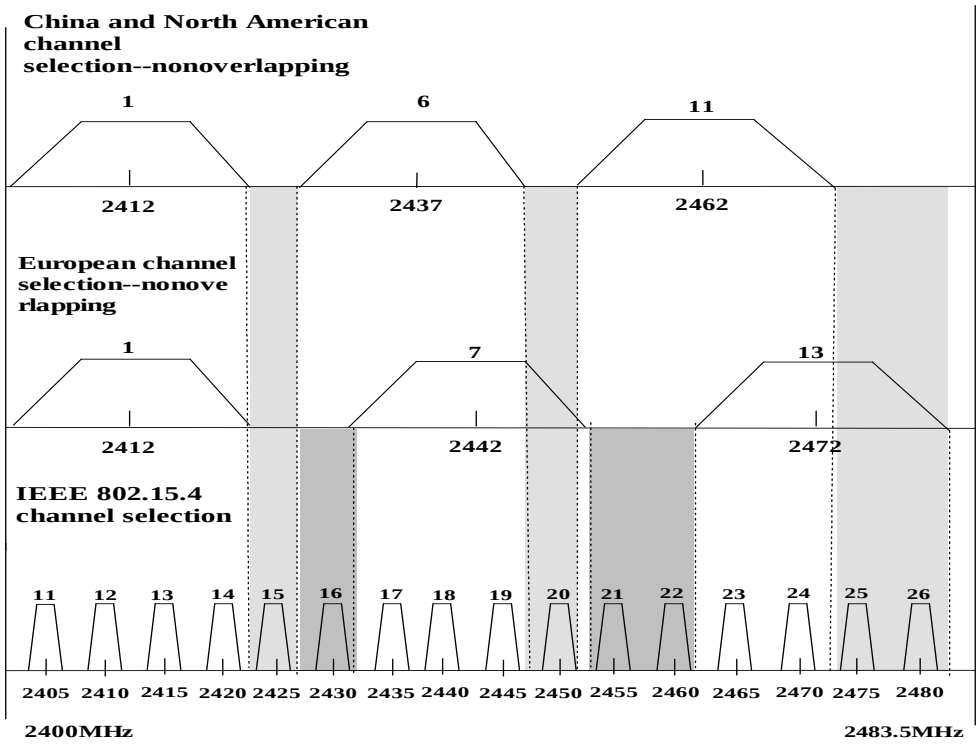

Figure 3.8 Non-overlapping IEEE 802.11b and IEEE 802.15.4 channel allocation

In Figure 3.8, most of the IEEE 802.15.4 communication channels overlap with the Wi-Fi communication channels. Since both IEEE 802.11b and IEEE 802.15.4 employs the technique of DSSS (with different PN sequence), the advantage of “spread spectrum” does not take obvious effect if the centre frequencies of IEEE 802.11b system and IEEE 802.15.4 system are close to each other. Additionally, the maximum transmission power of an IEEE 802.11b device can achieve 20 dBm (equivalent to 100 milliwatt), which is much higher than the

transmission power of IEEE 802.15.4 devices (i.e. 1 milliwatt). Once the IEEE 802.11b signals affect the IEEE 802.15.4 receiver, the relative high output power will contribute to the noise part of SNR. Figure 3.6 illustrates the transmit spectrum mask of the IEEE 802.11b signal.

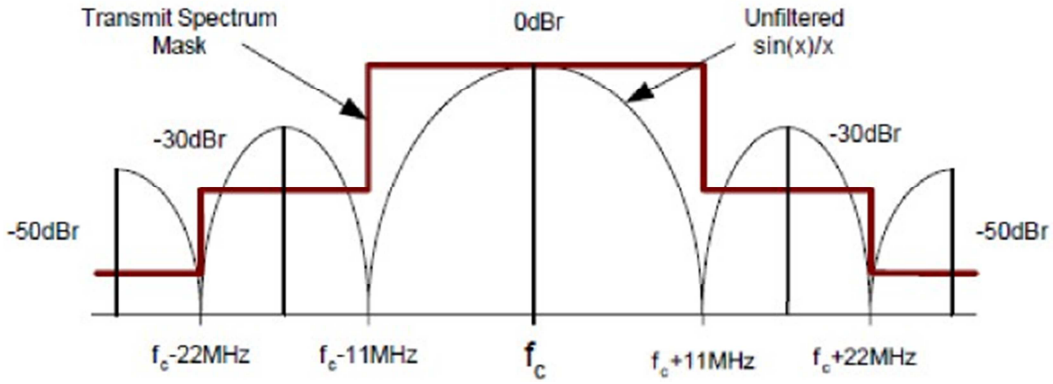

Figure 3.9 Transmit spectrum mask of IEEE 802.11b (IEEE Std802.11-2007)

In Figure 3.9, the power spectrum concentrates on the centre frequency of the selected IEEE 802.11b communication channel. The increment of separation from the centre frequency causes the power contained in the IEEE 802.11b signal to decrease. In (Shin et al., 2007), a simulation was carried out to study the relationship between the interference and frequency offset. The result states that the IEEE 802.15.4 system can achieve an acceptable performance (i.e. PER less than 1%) when the frequency offset between the centre frequencies of these two systems is larger than 7MHz.

- Bluetooth

Bluetooth (IEEE Std 802.15.1, 2005) is a short-range wireless standard for exchanging data over a short range (about 10m) from fixed and mobile devices. A total of 79 channels are defined by the Bluetooth standard in the 2.4 GHz ISM band, each channel has a bandwidth of 1 MHz and a channel separation of 1 MHz. Compared with the IEEE 802.11b, Bluetooth interference acting on an IEEE 802.15.4 system is less significant due to two reasons: frequency hopping and narrow band signal (Jennic Application Note, 2008).

Unlike the technique of “spread spectrum” used in IEEE 802.15.4 and IEEE 802.11b, Bluetooth achieves communications by frequently changing frequencies over time to transmit narrow band signals, which is called frequency hopping. Both Bluetooth communication devices employ the same pre-determined pattern to keep frequency hopping synchronized. The maximum hop rate is 1600 hop/s (IEEE Std 802.15.1, 2005). Due to the constant changes of communication channel, the duration of interference caused by Bluetooth device on IEEE 802.15.4 systems is limited. The effect of interference will disappear very shortly as the Bluetooth transmitter has hopped to a different part of the spectrum (Jennic, 2008).

The IEEE 802.15.1 specification defines three power classes. The maximum output power can be 20dBm (i.e. 100 milliwatt) in class-1. However, many IEEE 802.15.1 devices are enabled by batteries. Therefore the class-2 power setting, whose maximum output power is less than 4 dBm (i.e 2.5 milliwatt), is more commonly used. The maximum output power defined in class-3 is 1 milliwatt. Since the output power of IEEE 802.15.1 devices is close to IEEE 802.15.4 devices’ (class 2 & 3), and the bandwidth of the IEEE 802.15.1 signal is about half of the IEEE 802.15.4 signal, only a small portion of IEEE 802.15.1 signal will fall in the IEEE 802.15.4 receiver bandwidth. Consequently, the interference effect is not critical (Sikora and Groza, 2005).

3.3.3 CSMA-CA

Since IEEE 802.15.4 devices have a high likelihood to coexist with different wireless network devices, including other IEEE 802.15.4 devices belonging to different networks, the IEEE 802.15.4 transmission protocol should take potential collisions into consideration. The IEEE 802.15.4 standard employs an approach known as CSMA-CA. The technique of CSMA-CA has been successfully used in the Ethernet for years. It employs a simple “listen before you talk” strategy. Before wireless transmission, a device listens on the channel and implements channel assessment. If the channel is idle, the transmission will be processed. If the channel is busy, the device will wait for a random interval before checking the channel again. With the increment of channel assessment failure, the

wait interval increases exponentially in order to avoid interference (ZigBee, 2007).

3.4 Analytical and Empirical Study

The research into the interference effect in the IEEE 802.15.4 network can be briefly split into analytical and empirical studies. The analytical studies focus on modelling the PHY layer and MAC layer behaviour. Simulation is the major evaluation measure used by analytical studies. The empirical studies emphasize experimental tests using practical equipment in a real environment.

3.4.1 Analytical Study

The effective wireless communication range is mainly determined by the physical distance between the interferer's transmitter and victim's receiver. There are two parameters usually used to describe the performance of a radio system: output power and receiver sensitivity. The output power indicates the energy level of the output signal sent from the transmitter. The receiver sensitivity denotes the minimum energy level of radio signal which is detectable on the receiver. A receiver can recover the radio signal if the remaining energy level of the output signal is greater than the receiver sensitivity when it reaches the receiver. After propagation, the energy level of the output signal will attenuate with an increase in distance that the signal travels. When the interferer's transmitter and victim's receiver are separated by a certain physical distance, the interfering signal strength reaching the victim's receiver can be reduced. If the remaining energy level of the interfering signal is less than allowed noise level, the victim's receiver should be able to function normally. The signal strength reduction is classified as path loss. Path loss means the ratio of the total radiated power from a transmitter antenna times the numerical gain of the antenna in the direction of the receiver to the power available at the receiver antenna (Chandra et al., 2007). According to different environment conditions, the path loss can be described into different models. The basic model is free space loss applicable to the simplest possible

scenario: a transmitter and a receiver in a free space. The model (Molisch, 2005) is given as

$$L = \frac{P_{TX}}{P_{RX}} = \frac{(4\pi d)^2}{G_{TX} G_{RX} \lambda^2} \tag{3.2}$$

where:

L : Free space path loss

P_{TX} : Output power measured at the transmitter

P_{RX} : Receiving power measured at the receiver

G_{TX} : Gain of the transmitter antenna

G_{RX} : Gain of the receiver antenna

λ : Wavelength of the transmission (m)

d : Distance between the transmitter and the receiver (m)

Equation (3.2) can be expressed in terms of dB (Yilmaz, 2002):

$$L = 20 \log d + 20 \log f + 32.45 \tag{3.3}$$

where:

d : Distance between the transmitter and the receiver in km

f : Frequency of transmission in MHz

In the environment of free space, assuming 1) the output power of interfering signal is 0dBm (i.e. 1 milliwatt), the sensitivity of the victim receiver is -82dBm. 2) The interfering signal and victim receiver work on 2410MHz and 2430MHz respectively. 3) If the interfering power falling on the victim's receiver is less than -82dBm, the interference effect can be ignored. Therefore, the allowed path loss on interfering signal is 0dBm- (-82)dBm = 82dB. According to Equation (3.3), the distance d is obtained as 125 meters, which can be thought as a safe distance for the victim to avoid interference (Rodriguez, 2005). In a practical environment, the calculation of path loss is affected by many factors, e.g. antenna, building structure, street layout.

Shin et al. (2007) analyzed the interference in the IEEE 802.15.4 system caused by an IEEE 802.11b transmitter using a simple indoor path loss model as follows:

$$L_p(d) = \begin{cases} 20 \log_{10}(\frac{4\pi d}{\lambda}) & d \le d_0 \\ 20 \log_{10}(\frac{4\pi d}{\lambda}) + 10\, n \log_{10} \frac{d}{d_0} & d > d_0 \end{cases} \quad (3.4)$$

where d denotes the distance between the transmitter and receiver, d_0 denotes the length of line-of-sight, which is normally 8 meters. The parameter λ is equal to c / f_C, where c is the velocity of light and f_C is the carrier frequency, n denotes path loss exponent which is 3.4 in an indoor environment for distance over 8 meters (Golime et al. 2005). For both IEEE 802.15.4 and IEEE 802.11b systems, if the output power is fixed, the received power on the receiver is obtained as follows (Shin et al. 2007):

$$P_R = P_T \bullet 10^{\frac{-L_P(d)}{10}} \quad (3.5)$$

where :

P_T : Transmission power measured on the transmitter

P_R : Received power measured on the receiver.

$L_P(d)$: The path loss of transmission power after distance d.

The simulation was carried out by Shin et al. (2007) with assumptions that the output power of IEEE 802.11b (interferer) and IEEE 802.15.4 system (victim) are 30 mW and 1mW. The IEEE 802.11b system works at 11 Mbps with a 1500 bytes payload size. The IEEE 802.15.4 works at 250 kbps with a 105 bytes payload size. The offset between centre frequencies of IEEE 802.11b and IEEE 802.15.4 systems is 2 MHz. Consideration was also given to the non-uniform power spectral density distribution of the IEEE 802.11b signal. Simulations were performed using OPNET (OPNET, 2010). The results stated that the packet error rate of the IEEE 802.15.4 was smaller than 10^{-5} when the distance between the IEEE 802.15.4 receiver and the IEEE 802.11b transmitter was greater than 8 meters.

Another simulation study of IEEE 802.15.4 system performance under IEEE 802.11 interference was discussed by Yuan et al. (2007). A coexistence model regarding variant transmission power is illustrated in Figure 3.10.

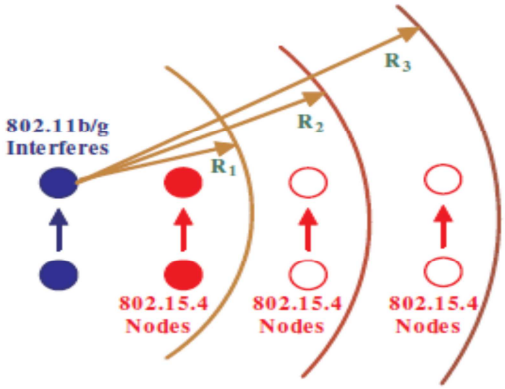

Figure 3.10 Coexistence ranges of IEEE 802.15.4 and IEEE 802.11b/g (Yuan et al., 2007)

In Figure 3.10, the positions of IEEE 802.15.4 nodes are decided by the degradation of IEEE 802.11b/g signals. The interference area is classfied into three ranges: R1, R2 and R3. Within range R1, an IEEE 802.11b/g node and an IEEE 802.15.4 node can sense each other. In range R2, an IEEE 802.15.4 node can sense an IEEE 802.11b/g node, but not vice cersa. Within range R3, neither the IEEE 802.11b/g node nor the IEEE 802.15.4 node can sense each other. However, the IEEE 802.15.4 node still suffers IEEE 802.11b/g interference. The value of R1, R2, and R3 are shown in Table 3.1 for both IEEE 802.11b and IEEE 802.11g nodes acting as an interferer. As the defined receiver senstivity for the receivers of IEEE 802.11b and IEEE 802.11g devices are different, the values for R1, R2, and R3 are different as well.

Table 3.1 Coexistence Ranges of IEEE 802.15.4 and IEEE 802.11b/g (Yuan et al., 2007)

Range	IEEE 802.11b	IEEE 802.11g
R_1	22 m	32 m
R_2	67 m	67 m
R_3	95 m	95 m

Assuming the receiver sensitivity and required SIR (signal to interference ratio) at an IEEE 802.15.4 receiver are -85dBm and 6dB respectively, if the interfering energy falling within the IEEE 802.15.4 receiver bandwidth is greater than (-85dBm)-6dB=-91dBm, the IEEE 802.15.4 signal will not be recognized by the IEEE 802.15.4 receiver. The transmission power of both IEEE 802.11b and

IEEE 802.11g signals is set as 20dBm. The receiver sensitivity of IEEE 802.11b and IEEE 802.11g is -76 dBm and -82 dBm. Through the calculation of path loss accoridng to Equation (3.4), it can be obtained that both IEEE 802.15.4 and IEEE 802.11b/g devices can sense each other within range R1. When the IEEE 802.15.4 nodes are located within range R2, they can sense IEEE 802.11b/g nodes, but not vice versa. Within range R3, neither IEEE 802.15.4 nor IEEE 802.11b/g devices can sense the other.

Simulations were also performed by OPNET. During the test, continuous User Datagram Protocol (UDP) packets were transmitted between two IEEE 802.11b/g nodes. An IEEE 802.15.4 node sended data packet to another IEEE 802.15.4 node where acknowledgement was required. The first simulation was taken in range R1. Compared with the normal condition (i.e. no interference), only 5.56% IEEE 802.15.4 packets were successfully transmitted. When the simulation was taken in range R2, the success rate of IEEE 802.15.4 transmission degraded almost to 0. In the former simulation, both IEEE 802.11b/g and IEEE 802.15.4 devices can sense each other. When the IEEE 802.11b/g nodes recognized the existence of IEEE 802.15.4 packet transmission, they will defer their attempt to access the medium, which leaves a few chances for IEEE 802.15.4 communications. In the latter simulation, the IEEE 802.11b/g nodes cannot detect the existence of IEEE 802.15.4 packet transmission. Consequently, the IEEE 802.15.4 packet transmissions were always affected as the IEEE 802.11b/g node will not defer. Yuan et al. (2007) concluded that the IEEE 802.15.4 packet transmission under IEEE 802.11 interference occured if either of the following conditions is satisfied: 1) when the IEEE 802.15.4 packet overlaps an IEEE 802.11 packet, the in-band interference power from the IEEE 802.11 packet must be significantly lower than the useful signal power from the IEEE 802.15.4 packet at an IEEE 802.15.4 receiver, 2) the transmission time of an IEEE 802.15.4 packet is shorter than the inter-frame idle time between two consecutive IEEE 802.11b/g packets.

3.4.2 Empirical Study

After analytical study, empirical studies are usually employed by researchers to investigate the effect of interference as a more practical approach.

Sikora and Groza (2005) designed three coexistence tests for the IEEE 802.15.4 standard with other devices working in the 2.4 GHz band. They used IEEE 802.15.4 devices based on the CC2420 chip made by ChipCom.

- Test 1: Test 1 is to measure the performance of IEEE 802.15.4 system when interferer (i.e. IEEE 802.11b) works on a different channel. The test 1 deployment is shown in Figure 3.11.

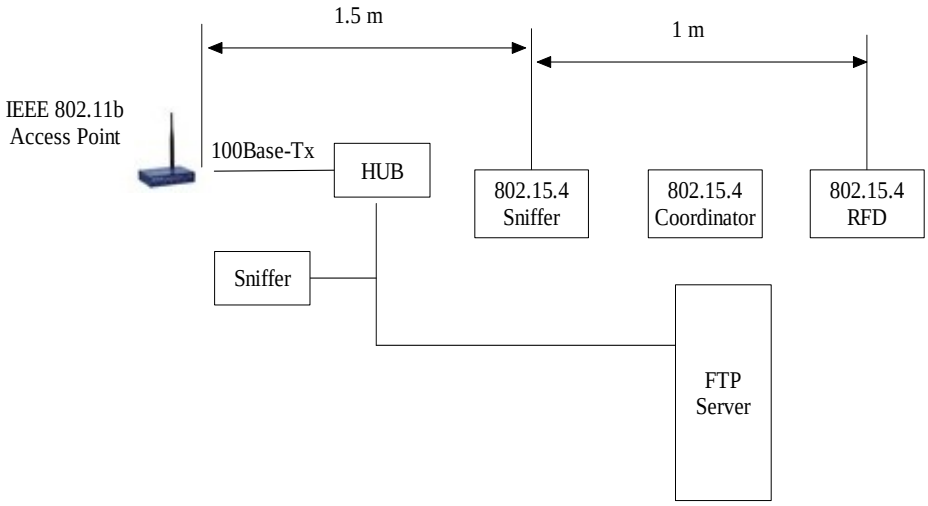

Figure 3.11 Test 1 setup (Sikora and Groza, 2005)

In Figure 3.11: the distance between an IEEE 802.11b transmitter (i.e. IEEE 802.11 Access-Point) and an IEEE 802.15.4 receiver (i.e. 802.15.4 RFD) is set as 1.5+1=2.5 meter. Since the test 1was to evaluate the relationship between the interference and frequency offset, the distance (i.e. 2.5m) between the interferer (i.e. access point) and victim (i.e. 802.15.4 RFD) is not important. The access-point continued to send packets to 802.11b client with packet size of 1446 Bytes. The packet rate was approximate 290 packets /s. In this test, the IEEE 802.15.4 system was operating at channel 16 (2440 MHz). The IEEE 802.11b system worked at various channels. The test result showed that an acceptable performance of IEEE 802.15.4 system (i.e. packet error rate is less than 1%) can

be achieved when the central frequency offset between IEEE 802.11b and IEEE 802.15.4 is over 10 MHz.

- Test 2: Test 2 was to test the impact of Bluetooth operation on the IEEE 802.15.4 system. Two pairs of Bluetooth devices were set to implement a large file transfer. One desktop made a file transfer protocol (FTP) transfer to a personal digital assistant (PDA), another notebook made a FTP transfer to a desktop PC. The observed Bluetooth data rates for these two transfers were 15 kbps and 50 kbps respectively. Due to the working style of frequency hopping employed by Bluetooth, the frequency offset between the Bluetooth channel and IEEE 802.15.4 channel was not considered. The test result indicated that about 10% of the IEEE 802.15.4 packets are lost. The loss of 10% packets in an IEEE 802.15.4 system is acceptable if the application layer retransmission is employed. However, the distance between Bluetooth devices and IEEE 802.15.4 device was not mentioned in the work of Sikora and Groza (2005).
- Test 3: Test 3 was to evaluate the interference on IEEE 802.15.4 systems caused by microwave ovens. The test result showed only 5 and 20 data frames out of 1000 are lost.

These three tests were performed under worst-case scenarios. For test 1, the IEEE 802.11b systems ran with the highest possible rate. In test 2, the FTP transfers for Bluetooth did not consider any speed control. In test 3, the testing devices (i.e IEEE 802.15.4 devices) were put directly onto the top of the oven at a distance of 1 m. The main purpose of introducing strict testing conditions is to provide a baseline for high-level coexistence protocol design in the future.

The work of Petrova et al. (2006) illustrated the design of a similar interference test to evaluate the coexistence issue of an IEEE 802.11 network and an IEEE 802.15.4 network. Figure 3.9 depicts the test bed. The hardware platform is constructed using the CC2420EB from Chipcon.

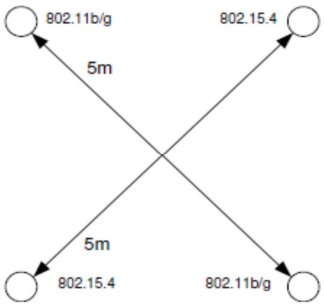

Figure 3.12 Test bed

In Figure 3.12, the distance between two IEEE 802.15.4 devices and two IEEE 802.11b/g devices is equally set as 5 meters. The test was implemented with various frequency offsets between communication channels employed by the two systems, and various lengths of IEEE 802.15.4 packets. The result is shown in Figure 3.13.

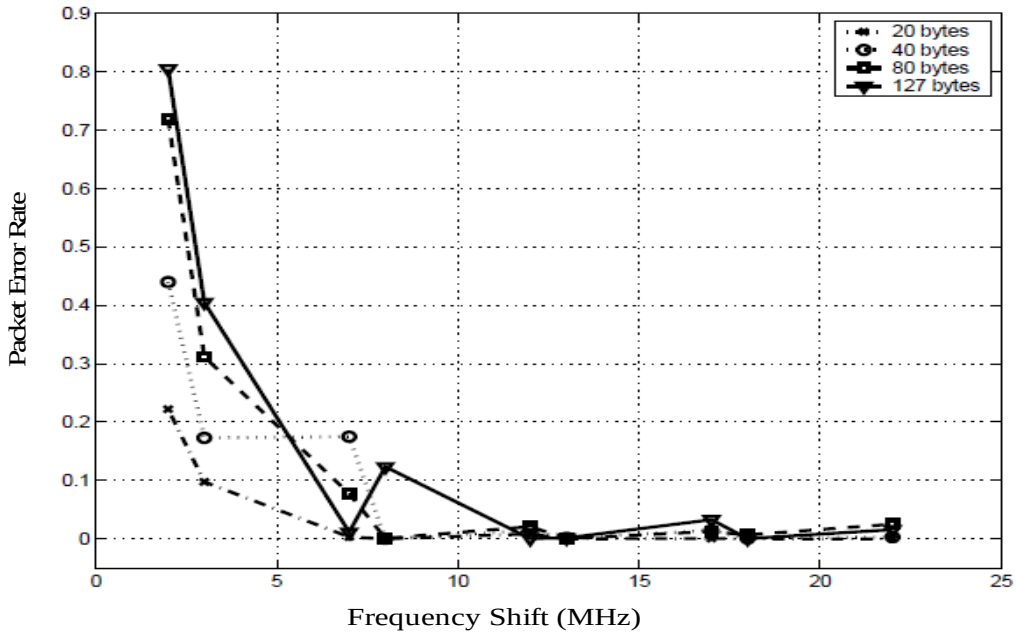

Figure 3.13 IEEE 802.15.4 PER when interfered by an 802.11 transmission (Petrova et al., 2006)

In Figure 3.13, if the frequency offset between IEEE 802.15.4 and IEEE 802.11 channels is over 7MHz, the packet error rate of IEEE 802.15.4 system can be acceptable (i.e. around 1%). A noticeable thing is that packets with larger size are more prone to errors.

Another interference study was conducted by Shuaib et al. (2007) within an office environment. The IEEE 802.15.4 (i.e. ZigBee) devices used in the experiment are Maxstream XBee-PRO (XBee, 2008) USB RF modems. Figure 3.14 depicts the hardware deployment.

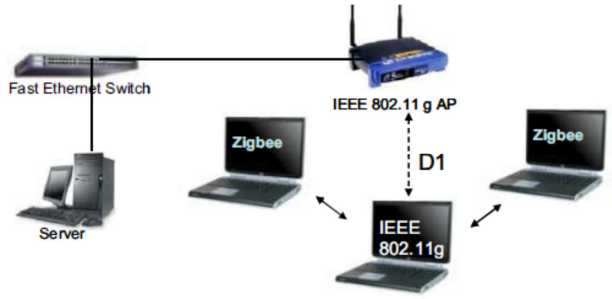

Figure 3.14 Hardware deployment (Shuaib et al., 2007)

In Figure 3.14, the two ZigBee (a technique which utilizes IEEE 802.15.4 technique as communication part) devices are set to transmit data packets at a rate of 115 Kbps with an inter packet delay of 200ms. The IEEE 802.11g device receives data sent from an IEEE802.11g router at a rate of 9.8 Mbps. Two experimental tests were conducted.

Experiment 1: The IEEE 802.11g channel was set as Wi-Fi channel 11 whose central frequency is 2462 MHz. The ZigBee devices were set to work on channel 11 operating at 2405 MHz. The distance between the IEEE 802.11g access point and IEEE 802.11g client is 10.5 meters, which is a reasonable separation in an office environment. The two ZigBee devices, with 1 metre separation, were located in the vicinity of IEEE 802.11g client (see Figure 3.15).

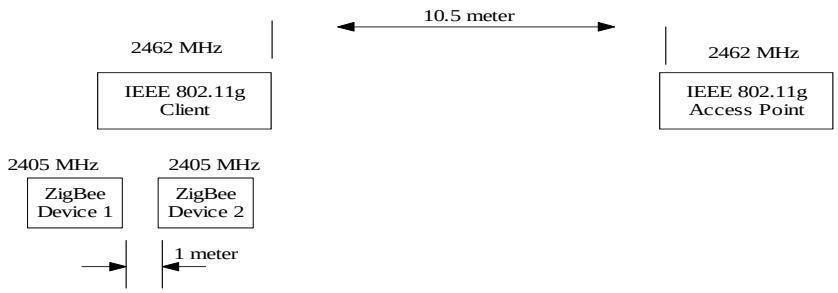

Figure 3.15 Devices deployment in experiment 1

Since the centre frequency offset between ZigBee network and IEEE 802.11g network is 2462 MHz-2405 MHz = 57 MHz, there is no interference effect reported in the test.

Experiment 2: Compared with the experiment 1, the channels of IEEE 802.11g and ZigBee network were changed, and the distance between ZigBee devices were various (see Figure 3.16).

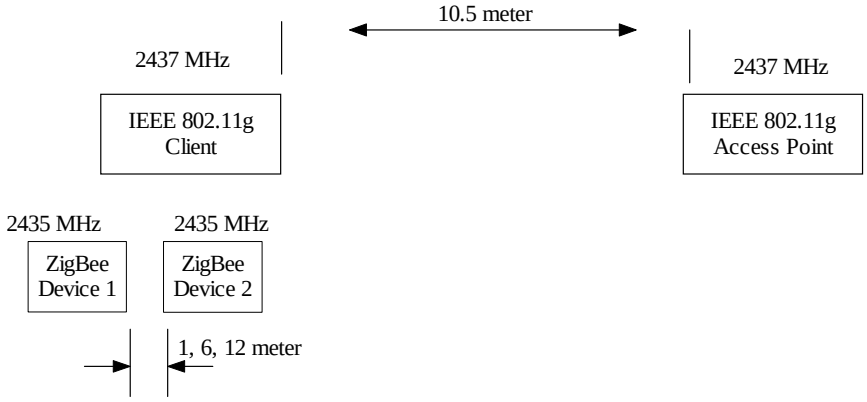

Figure 3.16 Devices deployment in experiment 2

In Figure 3.16, the IEEE 802.11g devices are set to work on Wi-Fi channel 6 (2437 MHz). The ZigBee devices choose to work on ZigBee channel 17 (2435 MHz). The centre frequency offset is 2 MHz, which is the worst case when channel allocation for IEEE 802.11and ZigBee systems is not guaranteed. Experiment 2 was conducted into three cases. In case 1, the two ZigBee devices were located with 1 meter separation, which was the same as in experiment 1. A 10% ZigBee throughput drop is measured. In case 2, the two ZigBee devices were located with approximate 6 metres apart. Also, a 10% ZigBee through drop was measured. In case 3, these two devices were with 12 metres apart. A 22% ZigBee throughput drop was measured.

The conclusions obtained from these two experiments are: 1) The interference effect from IEEE 802.11g signals can be ignored in a ZigBee network when the central frequency offset between these two systems is relatively large (e.g 57 MHz). 2) When a ZigBee device is located 3 meters or 6 metres away from an IEEE 802.11g interferer, the ZigBee throughput decrement between 10%

and 22% can happen when the frequency offset between ZigBee network and IEEE 802.11g network is small (i.e. 2 MHz).

3.5 Interference Mitigation Recommendations and Strategies

Due to the fact that the interference problem in the IEEE 802.15.4 network is significant, especially when interferers have high output power and wide frequency band, a number of suggestions and strategies have been proposed in order to mitigate the effect of interference.

3.5.1 Recommendations from IEEE 802.15.4 Standard

The IEEE 802.15.4 task group has conducted research in order to develop general guidance for IEEE 802.15.4 systems to coexist with other wireless devices operating in an unlicensed frequency band.

The mechanisms provided in the IEEE 802.15.4 standard that enhance the coexistence of IEEE 802.15.4 networks with other wireless systems are clear channel assessment (CCA), dynamic channel selection, modulation, energy detection (ED) and link quality indication (LQI), low duty cycle, low transmit power, and channel alignment (IEEE Std802.15.4-2003, 2003; IEEE Std802.15.2-2003, 2003).

CCA: The CCA is part of the CSMA-CA mechanism. There are three CCA methods available for use: energy detection over a certain threshold, detection of a signal with IEEE 802.15.4 characteristics, or a combination of these two methods. The IEEE 802.15.4 PHY can choose one of the CCA methods to implement channel assessment for detecting whether the channel is occupied by any device.

Dynamic Channel Selection: IEEE 802.15.4 specification does not support direct frequency hopping. However, users can specify a certain mechanism in applications switch to manually to a suitable communication channel when interference is sensed on the current frequency.

Modulation, ED, and LQI: The employed modulation scheme is O-QPSK, which is a power-efficient modulation method that achieves a low signal-to-noise

ratio. The ED and LQI are two measurement functions. The ED is used to detect the energy level within an IEEE 802.15.4 channel. Meanwhile, it can provide useful information for channel selection algorithm executed by a higher layer. The LQI measures the signal strength for each received packet, which is usually used as the indicator of signal quality.

Low duty cycle is a kind of requirement for working style. For a single IEEE 802.15.4 device working within a WSN for environment monitoring, it is reasonable to report sensor readings (e.g. 1-byte temperature reading) every minute or longer. Briefly, assuming an IEEE 802.15.4 packet which contains a 22-byte payload is transmitted with a data rate at 250 kbps every 1 minute, the required transmission time is $22*8/250kbp = 0.704$ milliseconds. Then the duty-cycle of this IEEE 802.15.4 device is $0.704/(1*60*1000) = 1.17\times10^{-3}\%$. The transmitter is in an inactive state for the rest of the working period. By following the suggestion of low duty cycle, the chance for the IEEE 802.15.4 device to compete with interfering signals can significantly decrease.

Low transmit power and channel alignment: Low transmit power is a mechanism mainly for promoting an IEEE 802.15.4 device's capability to coexist with other wireless systems. Although Federal Communication Commission (FCC) rules allow transmit power up to 1 W in the 2400 MHz, IEEE 802.15.4 devices likely operate with much lower transmit power (i.e. typically 1 mW) to minimize interference with other wireless devices. Channel alignment requires a proper separation between the IEEE 802.15.4 communication channel and the potential wireless systems, which can enable multiple wireless systems to work simultaneously without significant mutual interference.

3.5.2 Existing Mitigation Strategies

Swapping the current working channel of IEEE 802.15.4 based WSNs to a relative free frequency when interference occurs is an easy and effective way to combat interference. In this study, we review three typical existing mitigation strategies.

3.4.2.1 Adaptive Interference-Aware Multi-Channel Clustering

Kang et al. (2007) proposed an adaptive interference-aware multi-channel clustering algorithm to avoid IEEE 802.11 interference in a ZigBee network. In the description of this algorithm, a stationary ZigBee network is assumed so that no topology change or mobile node is allowed (See Figure 3.17).

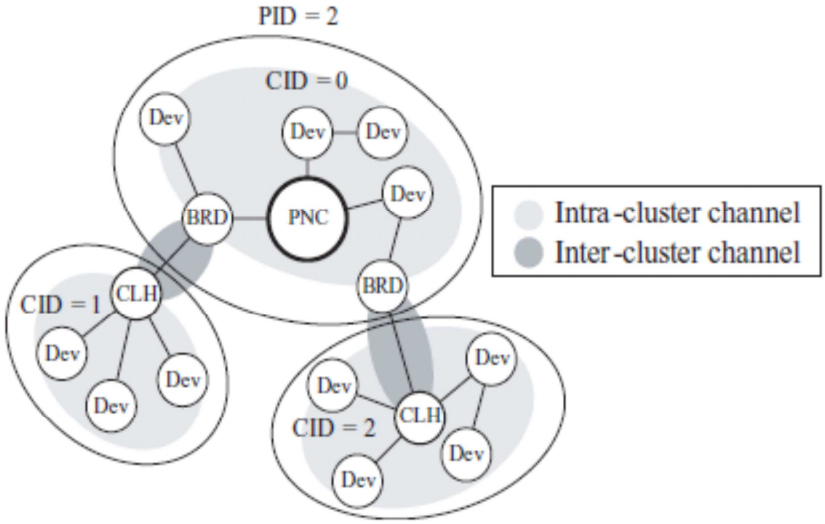

Figure 3.17 ZigBee network with Intra and Inter clusters (Kang et al., 2007)

In Figure 3.17, ZigBee devices are classified into a number of clusters. Except for the PAN Coordinator, each cluster has a cluster head (CLH) responsible for cluster management. A cluster identifier (CID) is used by devices in the same cluster to establish communication. There are two channel settings: An intra-cluster channel for devices in the same cluster and an inter-cluster channel for a cluster header and a bridge device (BRD). A bridge device is a node directly connected to a cluster header of a neighbouring cluster. The use of Inter-cluster is to increase the coverage area of a ZigBee network.

The algorithm consists of two schemes: an interference detection scheme and an interference avoiding scheme.

- Interference Detection Scheme: Once a device in a cluster detects the existence of IEEE 802.11 interference (e.g. loss of beacon synchronization, or loss of acknowledgement), it should broadcast a channel change broadcast message (CCBM) through the cluster, allowing the other devices in the same cluster to detect the interference.

- Interference Avoidance Scheme: On receipt of the CCBM, devices in the same cluster start to change their channel to a new channel. To ensure each device can move to the same channel without introducing additional cost, a combination of PAN identification, cluster ID, current channel and channel switch counter is used as a key to generate the next channel. Devices sharing the same parameters can obtain the same result. These parameters are inputted in a pseudorandom sequence generator (PRSG) (see Figure 3.18).

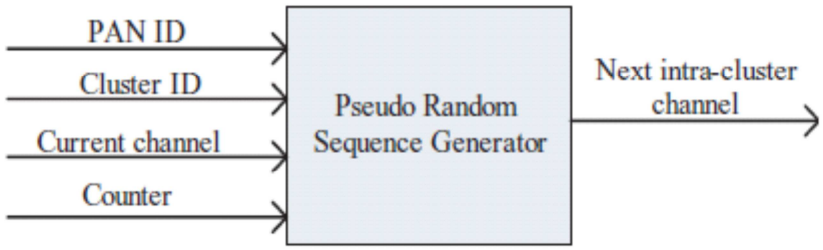

Figure 3.18 Block diagram for pseudorandom sequence generator (Kang et al., 2007)

For the Inter-cluster connection, the cluster head periodically sends a test frame to the bridge node. If a number of acknowledgements are lost, the cluster head assumes that the Inter-cluster channel is experiencing interference. Then it sends out CCBM frame and moves to the next channel. For the bridge node, if a number of test frames are not received as scheduled, it also sends out CCBM to the cluster to which it belongs, and moves to the next channel.

The evaluation test for "interference-aware multi-channel clustering" algorithm was implemented using 30 Chipcon CC2420 chips (CC2420, 2007) working on channel 23(i.e. 2465 MHz). The IEEE 802.11 traffic was configured to work on multiple channels, channel 11, channel 1, and channel 6. The test results were compared according to two situations: with algorithm (situation 1) and without algorithm (situation 2). When an access point worked on channel 11 (2462 MHz), 1/3 of ZigBee devices were unable to communicate in situation 1. However, only 22% frames were lost in situation 2. It was also found that the proposed algorithm cannot resolve the overall problem that ZigBee frame delivery degrades with the increment of IEEE 802.11 access points on different channels.

3.4.2.2 Adaptive Radio Channel Allocation

An adaptive radio channel allocation for supporting coexistence of 802.15.4 and 802.11b was proposed by Won et al. (2005). The algorithm also focuses on IEEE 802.15.4 based WSN for large-scale deployment. The studied IEEE 802.15.4 network with interference presence is illustrated in Figure 3.19.

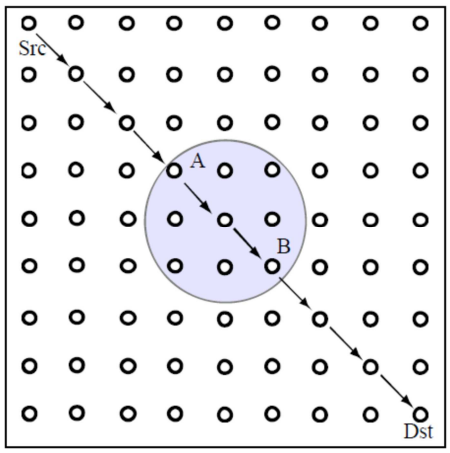

Figure 3.19 Multi-hop IEEE 802.15.4 network with interference (Won et al., 2005)

In Figure 3.19, a deployed IEEE 802.15.4 sensor network using mesh topology is being interfered by IEEE 802.11b signals. The node named "Src" is set to send data packet to the node "Dst". The routing path from the source node to the destination node has been pre-configured by following the solid arrows. The graded area is the part being affected by interference. If the source device can reselect a new route to bypass the affected area, the problem of interference can be solved. However, additional computation cost will be generated. Won et al. (2005) introduced a strategy to save the cost of additional route selection by enabling the nodes within the interfering area to switch communication channel temporarily. The strategy implementation consists of three steps: interference detection, group formation and tear-down.

- Interference Detection

Each IEEE 802.15.4 node in the mesh network keeps monitoring the data throughput and executing interference detection using the standard function of energy detection, or clear channel assessment. Once a sudden degradation of throughput is detected, and the energy detection returns a high level reading, the

node will enter into the procedure of group formation in order to form a temporary group in a clean channel.

- Group Formation

The node, which starts the procedure of group formation should message its immediate neighbours about the information of the channel to which it is going to switch. On receipt of the messages, the neighbour node will change its role to act as a border node, which establishes a bridge between the original mesh network and the nodes within the interference area. The border node will send a reply message on the new channel to the node from which it received the group formation message. The reply message is to confirm that the border node is aware of the situation change. Next, the border node switches back to the previous channel. If new data for the nodes that have joined the temporary group are received by the border node, it quickly switches to the channel used by the temporary group, and sends the data to the desired node. After completion of data sending, the border node returns to the original channel and continues to listen on it.

- Tear-down

The nodes in the temporary group keep checking the previous channel periodically. If the channel is measured to be clear, they will send a tear down message to all immediate neighbours, especially the border nodes. Consequently, the whole group will be torn down when the interference has completely diminished.

In the work of Won et al. (2005), an experimental test was implemented to study the impact of IEEE 802.11b interference on the performance of IEEE 802.15.4 networks. Meanwhile, a simulation test using the NS2 simulator was implemented to evaluate the effectiveness of the proposed strategy.

In the experiment, two IEEE 802.11b network adaptors were configured in ad-hoc mode. One adaptor sent data packets to another adaptor using the maximum data rate of 11 Mbps. Two IEEE 802.15.4 Chipcon wireless modules were located close to IEEE 802.11b adaptors in a peer-to-peer configuration. One module periodically sent packets to another module at an interval of one second. The IEEE 802.11b adaptors worked on channel 6, whose centre frequency is 2437

MHz. The IEEE 802.15.4 network worked on two channels, channel 17 (i.e. 2435 MHz), and channel 21 (i.e. 2455 MHz). If channel 17 is used, the success rate of IEEE 802.15.4 packet delivery was measured at 40% since the centre frequency offset between the IEEE 802.11b network and the IEEE 802.15.4 network is 2 MHz. If channel 21 was used, the IEEE 802.15.4 packet delivery rate was sustained 99% to 100%.

In the NS2 simulation experiment, the IEEE 802.15.4 network was deployed as depicted in Figure 3.19. The effectiveness of the proposed strategy was measured with two metrics: packet delivery success rate and delay. Since the strategy implementation was implemented once interference is detected, and the "adaptive channel allocation" can ensure the success of following packet transmissions, then most of the packets will not be lost. The measured packet delivery success rate sustained between 97% and 86%. During periods of interference, the proposed strategy could still utilize the previous route without issuing a new route selection. However, more time was spent by the "border node" to implement channel switching. In comparison with the situation where no strategy was applied when interference happened, the packet delay measured in simulation tests with the strategy implemented was approximately 40% less.

3.4.2.3 Adaptive Multi-Channel Utilization Scheme

An interesting strategy called "Adaptive Multi-Channel Utilization scheme" was proposed by Hwang et al. (2009) to achieve coexistence of IEEE 802.15.4 with other interfering systems. The strategy assumes the use of IEEE 802.15.4 network is under beacon-enabled mode. If no strategy is specified, all IEEE 802.15.4 devices only work on the selected channel and are associated with the PAN coordinator by tracking the periodic beacons. Each beacon contains a superframe within which all synchronized devices can commence communications. The beacon signal is contained at the first part of the superframe. Once serious interference occurs in the current working channel, IEEE 802.15.4 communications will be interfered until the PAN coordinator restarts a new PAN in a clean channel with small energy level and completes re-association requests from previous devices. To overcome the shortage of the

standard procedure, the proposed strategy utilizes all available channels to maintain multiple superframes on different channels.

When a PAN coordinator is to start an IEEE 802.15.4 network, it first implements energy detection on all 16 IEEE 802.15.4 channels. The channels with energy level less than a certain threshold will be stored on the PAN coordinator. This is different from the normal IEEE 802.15.4 PAN coordinator which sends beacon only on the certain channel after the completion of the energy scan, the PAN coordinator used in "Adaptive Multi-Channel Utilization scheme " sends beacon periodically on multiple channels which are stored as clean channels (see Figure 3.20).

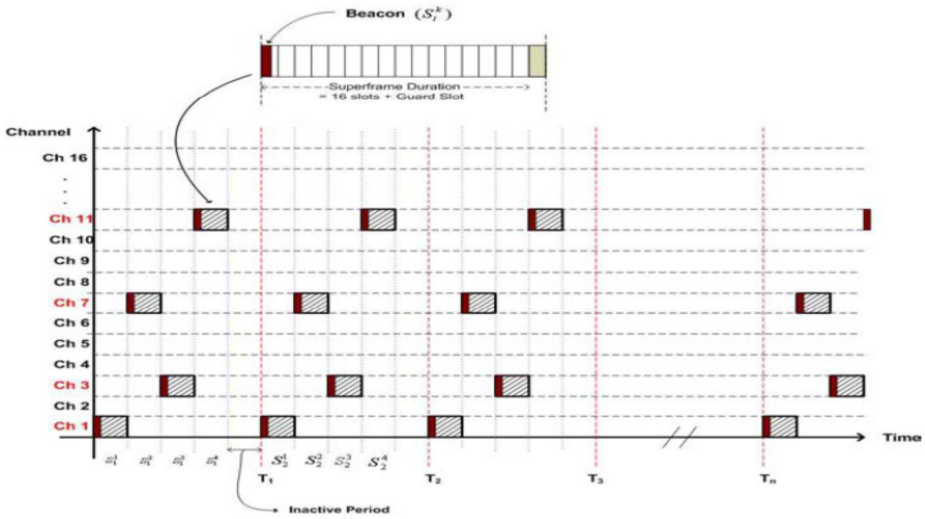

Figure 3.20 Multiple superframe structure by coordinator using multi-channel (Hwang et al., 2009)

In Figure 3.20, the channel 1 7, 3, and 11 are chosen to implement multiple superframes transmission. For each single working period, normal IEEE 802.15.4 devices on these 4 channels will be able to receive a superframe sent from the same PAN coordinator. When a normal IEEE 802.15.4 network device is going to join the network, it firstly implements passive detection on all channels by sequence. Once a superframe is received on a channel, the device will synchronize with the beacon and store the list of the clean channels (i.e. channels with less energy level). When the superframe appears on the same channel in the next loop, the device will send an association request to the PAN coordinator. On receipt of the reply from the PAN coordinator, the association is completed. Then the IEEE device stays on this channel and implements communications.

Once interference occurs on a channel, the IEEE 802.15.4 devices working in this channel will lose synchronization with the PAN coordinator, or the PAN coordinator will receive no acknowledgements. When such phenomena happens, the PAN coordinator and affected devices can simply cancel all transactions on the channel being interfered with, and work on the rest of the clean channels. Since the PAN coordinator and network devices maintain the same channel list, the transfer will be easy to achieve. The experimental test showed that none of the packets are lost until all scheduled channels are interfered.

3.5.3 Comprehensive Suggestions from Industry

In general, the cause of interference in IEEE 802.15.4 based wireless sensor networks can be categorized into two aspects: channel selection and transmission power. On the basis of these two characteristics, Jennic (2008) concludes a number of methods for reducing the effects of interference on an IEEE 802.15.4 network.

Channel Selection: It is recommended to use channels 25 and 26 to avoid most of the IEEE 802.11b/g interference. If the system is deployed within an environment where pre-configuration of wireless systems is controllable, a channel centre-frequency offset of 7 MHz is better to reserve to ensure acceptable coexistence with IEEE 802.11 systems.

Physical Separation: Ensuring a physical separation of at least 8 meters from an IEEE 802.11 access point is useful for coexistence.

Mesh Networking: If applicable, an IEEE 802.15.4 network can be constructed on the basis of mesh topology which provides additional benefits of a self-organizing and self-healing capability.

Network Layer Frequency Agility: By switching to a clean channel when interference occurs, an IEEE 802.15.4 network can effectively avoid performance degradation. The channel hopping is normally charged by high level protocols (e.g. network layer). The decision of dynamic channel selection should be made in terms of results of channel assessments (e.g. energy detection, link quality indicator).

Network Planning: Before deploying an IEEE 802.15.4 network, initial assessment such as a site survey can be performed to evaluate the radio frequency environment. The results provide important guidance for physical installation. During the period of system operation, the radio frequency environment evaluation can be periodically performed to monitor the changes of interference possibility.

3.6 Summary

As discussed before, it is evident that the performance of IEEE 802.15.4 networks can be affected by wireless interference occurring in the same ISM 2.4 GHz band. The level of the interference effect depends on the characteristics of the interferer, e.g. interfering power strength, system duty-cycle, interference frequency. The research on interference mitigation strategies for IEEE 802.15.4 systems are in great demand as more and more wireless products using this technique are coming to the market.

A complete research process regarding wireless interference consists of three steps: analysis for the cause of interference, interference mitigation strategy design, and data recovery strategy design. The idea is that the interference effect can be limited using the corresponding methods if the cause of the interference can be addressed, and the system's performance can be further improved if the lost data can be efficiently recovered. These three steps also compose the methodology employed for the interference study in this thesis.

3.6.1 Analysis for the Cause of Interference

The unexpected interfering energy (e.g. IEEE 802.11 signal) is the essence of interference affecting an IEEE 802.15.4 based wireless sensor network. When interference signals overlap the desired signal, and the corresponding interfering energy reaching the IEEE 802.15.4 receiver is over the allowed noise level, the reception of the desired signal on the IEEE 802.15.4 receiver will fail.

The difficulty for an IEEE 802.15.4 system in detecting the existence of interference at the physical layer, based on the literature review in this chapter, is

that the IEEE 802.15.4 radio system works under half-duplex mode, which means the transmitter cannot monitor the status of signals whilst the transmission is in process. On the other hand, the employed modulation/demodulation technique usually limits the maximum capability of the wireless system's anti-interference capability. Some wireless standards e.g. IEEE 802.11b, allow the system to dynamically switch to a second choice of modulation/demodulation scheme when interference occurs, However, there is no universal modulation/demodulation scheme available for dealing with all situations.

The analysis for the cause of interference on IEEE 802.15.4 based on WSN focuses on the effect of interference at a system level which is higher than the PHY layer (e.g. MAC layer, network layer, application layer), and provides information for the following interference mitigation strategy design.

3.6.2 Interference Mitigation Strategy Design

The IEEE 802.15.4 standard does not support hardware adjustment (i.e. switch modulation/demodulation) to obtain better performance when its system is under interference. However, if the adjustments are made at the MAC layer or above (e.g. reduce overlapping part between desired packet transmission and interference signals, switch communication channels, or implement new route selection), the possibility for the IEEE 802.15.4 network affected by interference to survive could increase.

Many researchers propose their solutions to help IEEE 802.15.4 based networks overcome any interference by intelligently swapping working channel to avoid direct contact with harmful energy (Kang et al. 2007; Won et al. 2005; Hwang et al. 2009). The tests results indicate that the strategies can effectively increase IEEE 802.15.4 network performance when there are "clean" channels available for swapping if the current working channel is experiencing interference. However, the rapid development of personal wireless devices working on the same ISM 2.4 GHz band is forming a situation in which there might not be any clean channel to use within a given environment. For example, it is common for different departments in a company to set up private IEEE 802.11 networks in the same open office environment. If three non-overlapping Wi-Fi

channels are not sufficient for use, some of the overlapping Wi-Fi channels must be used under this circumstance. Consequently, there will be no clean IEEE 802.15.4 channel “isolated” from Wi-Fi networks (see Figure 3.5). The main research interest of this thesis is to discuss and design efficient and feasible strategies from a system level view using the information obtained from interference analysis. The strategies are mainly implemented at the IEEE 802.15.4 MAC layer or above to maintain communications when interference occurs and channel switching is not applicable.

3.6.3 Data Recovery Strategy Design

Since the occurrence of the interference is unpredictable, some data loss is inevitable no matter how interference mitigation strategy is implemented. Consequently, a data recovery strategy is crucial if the lost data is important for the application. By utilizing the convenience provided by the peer-to-peer topology, it is feasible to construct redundancy in the IEEE 802.15.4 network, and enable data recovery when necessary. The data recovery strategy involved in this thesis mainly focuses on the finding of the lost data on the basis of hardware. Details will be given in Chapter 6.

By combing the uses of interference mitigation and data recovery strategies, an IEEE 802.15.4 network can provide upper layers with a complete data service to ensure high system performance under interference.

Chapter 4 Interference Analysis and Mitigation

4.1 Background and Motivation

The basic topologies supported by the IEEE 802.15.4 standard are star topology and peer-to-peer topologies. The star topology is usually used for small area applications, as its coverage area is limited. In a star network, the network controller (i.e. IEEE 802.15.4 PAN coordinator) is in charge of all network operations, which means only one hop range is required for network communications. As the effective communication range of a star IEEE 802.15.4 network is limited, both transmitter and receiver can be affected during periods of interference. In such a case, network communications can be affected when the default mechanism of CSMA-CA fails, or the desired acknowledgment is missed. Although the network communications might return to normal by enabling the PAN coordinator and network devices to switch to a different channel, it is more useful if the communications can be maintained on the current channel when it is not possible to apply channel switching, or other IEEE 802.15.4 channels are also being affected by interference.

4.2 Analysis of Existing Interference Resources

The basic idea of wireless communication is to provide connectivity through the wireless medium. Therefore, wireless systems are required to ensure a certain minimum transmission quality. The metric for measuring the transmission

quality is SNR at the receiver (Zhou et al., 2005). The noise, which is also called interference in this context, can consist of several components, as follows (Molisch, 2005):

1. Thermal Noise: The thermal noise is generated by environmental temperature. Assuming the normal environment temperature is 300 K (around 26 Celsius). The power spectral density of thermal noise affecting the receiver bandwidth is calculated as 174dBm/Hz.
2. Man-made Noise: Man-made noise can be distinguished into two types:
   a) Spurious emissions: It is common for many electric appliances to emit noise over a large bandwidth that includes the range within which the desired wireless communication systems operate. Car ignitions and other impulse sources are typical example sources of man-made noise.
   b) Other intentional emission sources: Several wireless communications systems in close proximity operate in unlicensed bands, particularly ISM 2.4 GHz band. In these bands, all members are allowed to emit electromagnetic radiation without restrictions compared with licensed bands. This interference phenomenon is serious (Chiasserini et al., 2002).
3. Receiver Noise: The amplifier and mixers in the receiver are noisy and compose parts of noise power in the whole system.

Among the listed noise resource, the thermal noise and receiver noise persist all the time and cross the whole available bandwidth. The noise resource of "spurious emission" also crosses the whole available bandwidth. This is an uncontrollable factor which is out of scope of this thesis. The factor of "other intentional emission sources" is caused by wireless systems under control of corresponding protocols. Wireless systems working on the same 2.4 GHz ISM band are all potential interference source.

IEEE 802.15.4 WSNs based on the star topology are suitable for home automation, personal computer peripherals, toys and games, and personal health care (IEEE Std802.15.4-2003, 2003). These application areas are quite common in domestic use. For example, inside the home, several home appliances including

washing machine, radios, televisions, lighting control, automatic curtain etc, can be organized using a universal controller (Callaway et al., 2002). The IEEE 802.15.4 technique can easily enable these devices to be wireless without worrying about the differences of physical characteristics.

IEEE 802.11b based wireless local area networks have become popular in home, enterprise and public access areas due to the features of low cost, simplicity of installation and high data rates (Medepalli et al., 2004). In areas with both IEEE 802.15.4 and IEEE 802.11b systems in operation, problems of coexistence must be considered. For example, an IEEE 802.15.4 enabled light sensor node serving a home automation network is located close to a window. A laptop equipped with an IEEE 802.11b network adaptor is set a few meters away from the window and used for audio application through the IEEE 802.11b network. Then the IEEE 802.11b interference could be harmful to the IEEE 802.15.4 system (Latre et al., 2006).

It has been proved that IEEE 802.11b wireless networks can have different degrees of interference on IEEE 802.15.4 communications (Sikora and Groza, 2005; Petrova et al., 2006; Howitt and Gutierrez, 2003). Under normal circumstance, an IEEE 802.15.4 network can avoid interference from IEEE 802.11b system by enlarging physical separation from an IEEE 802.11b transmitter, or selecting a different communication channel whose centre frequency is away from the frequency employed by the IEEE 802.11b system. However, these measures may not be applicable in practical applications due to two reasons:

1. The capability of automatic channel switching for avoiding interference is not supported by the IEEE 802.15.4 standard. If channel switch is required, it should be carried out by application software with specific interference judgment procedure.
2. IEEE 802.11b system is probably integrated into portable devices (e.g. laptop, personal digital assistant). Therefore, they can work anywhere. However, most IEEE 802.15.4 WSN devices are static after deployment since it is not originally designed for mobile applications.

If the IEEE 802.15.4 system can maintain communications on the current channel whilst IEEE 802.11b interference is occurring, the capability for the IEEE 802.15.4 system to suffer interference can be significantly improved.

4.3 Interference Modeling: Open Loop

Although an IEEE 802.11 system can produce serious interference on an IEEE 802.15.4 receiver, it is still possible for the IEEE 80215.4 to communicate under the presence of interference. IEEE 802.11b wireless communication usually satisfies two characteristics: non-persistence and variable duty cycle.

- Non-Persistence

In wireless communication systems, the state of radio transmission is usually not persistent. Most communication protocols specify the maximum data payload length for each type of supported frame. For instance, an IEEE 802.11b MAC frame can contain a maximum of 2304 bytes as data payload (IEEE Std802.11-2007, 2007). In the case that the amount of desired data is larger than the maximum data payload size, the transmission must be processed packet by packet, which is called datagram fragmentation. After the completion of a packet transmission, the system must consume some necessary time to adjust the transmitter state and process the next frame passed from the upper layers. Therefore, there is always a certain interval existing between each pair of packet transmissions.

- Variable Duty Cycle

Wireless communication systems usually work when required. For an IEEE 802.11 network, the network can be active when users start to access the Internet and initiate certain actions. For example, when the user presses a button on a webpage, the IEEE 802.11 adaptor equipped on the computer will send a request to the website through the wireless router, and display to the user the results when responses are received from the website through the wireless router. The IEEE 802.11 signals travelling between the computer and the wireless router create interference to other wireless communication. Once the process of request

and response is finished, the IEEE 802.11 network will be inactive until the next action is initiated. The duration of a transmitter working period is called the duty cycle. According to the level of utilization, the duty cycle can be various.

When the IEEE 802.11 transmitter is idle or in a listening state, there will be no interference. From the viewpoint of system activity, this situation is called a "low duty-cycle". It is possible that the communications of the IEEE 802.15.4 system will be interfered with by powerful IEEE 802.11 signals, but if the time interval between any two IEEE 802.11 packets is large enough to enable completion of the IEEE 802.15.4 packets transmission, the effect of interference can effectively be reduced. There are two aspects which need to be analyzed: 1) If the time slot existing between two IEEE 802.11 packets is large enough to enable the transmission of IEEE 802.15.4 packets. 2) As the IEEE 802.11 system and IEEE 802.15.4 system are not able to interact with each other, is it possible to ensure that the IEEE 802.15.4 packet transmissions occur when the IEEE 802.11 system is in an idle state.

In this chapter, an IEEE 802.11b transmitter is assumed as the interferer. Figure 4.1 shows the basic access method of the IEEE 802.11b system.

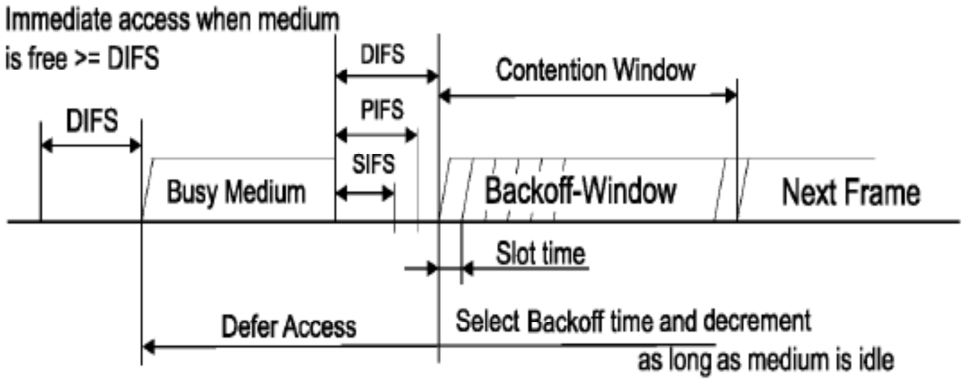

Figure 4.1 Basic access method of IEEE 802.11b (IEEE Std802.11-2007, 2007)

In Figure 4.1, when an IEEE 802.11b device is to transmit a packet, it will monitor the channel until an idle period equal to or greater than a distributed inter-frame space (DIFS) is detected. If the channel is busy, the device will keep deferring. After sensing an idle DIFS, the device selects a random number of "slot

time" (*aSlotTime*) and starts to backoff, which means the device waits for a specified period before starting the transmitting process. The random number is set as the counter. Once the backoff counter reaches zero, the device starts to transmit the packet. If the channel is detected to be busy during the period of backoff, the count temporarily suspends and resumes when a period of idle DIFS is detected.

According to the IEEE 802.11b standard, DIFS and Backoff are defined as follow:

$$DIFS = aSIFSTime + 2 \times aSlotTime \tag{4.1}$$

$$Backoff = Random() \times aSlotTime \tag{4.2}$$

where *aSlotTime* denotes the Slot Time (in microseconds) that the IEEE 802.11 MAC layer will use for defining DIFS periods, *aSIFSTime* denotes the nominal time (in microseconds) that the IEEE 802.11 MAC and PHY layer will require to process the received frame, the function $Random()$ generates an integer drawn from a uniform distribution over the interval [0, CW], where CW denotes contention window whose range is $aCW\min \le CW \le aCW\max$. The parameters of $aCW\min$ and $aCW\max$ are PHY characteristics defined in the IEEE 802.11b standard. Table 4.1 summarizes the related parameters and values.

Table 4.1 IEEE 802.11b parameter

IEEE802.11b Parameter	aSlotTime	aSIFSTime	aCWmin	aCWmax
Value	20μs	10μs	31	1023

In Table 4.1, *aCWmin* and *aCWmax* denote the minimum and maximum size of contention window (in units of *aSlotTime*) respectively. Theoretically, the interval $T_{i\_802.11b}$ between two connective IEEE 802.11b packets is obtained as follows:

$$T_{i\_802.11b} = DIFS + Random() \times aSlotTime \tag{4.3}$$

where $Random() \in [0, CW]$. Therefore, $T_{I\_802.11b} \in [0.67ms, 20.51ms]$.

Similarly, an IEEE 802.15.4 packet transmission also needs to follow certain rules. Figure 4.2 illustrates an IEEE 802.15.4 star network.

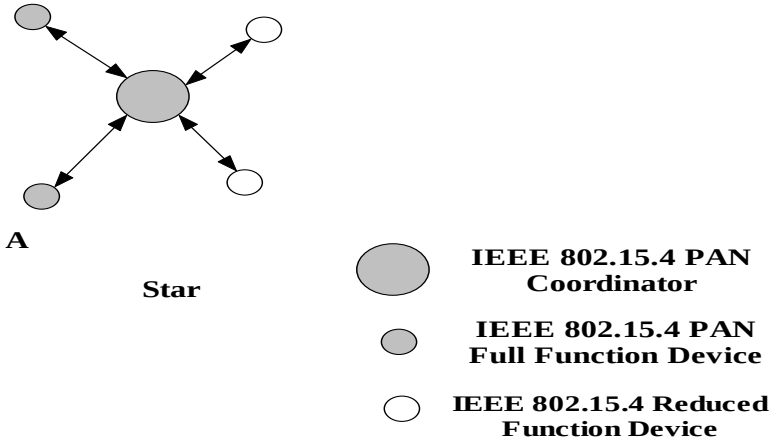

Figure 4.2 IEEE 802.15.4 star network

In Figure 4.2, an IEEE 802.15.4 PAN coordinator acts as the starter of the network. As mentioned in Chapter 2, any IEEE 802.15.4 network must have one and only one PAN coordinator to initiate key network parameters (e.g. network channel, network identification) and maintain network operations during the whole system lifetime. Other devices including IEEE 802.15.4 full function devices and IEEE 802.15.4 reduced function devices can join the established network by associating with the PAN coordinator. The difference between full function device and reduced function device is that a full function device is capable of relaying messages. However, relaying message is not required in a star network. If a network device is to send data to another device, the data must be sent to the PAN coordinator first, and then relayed to the destination device by the PAN coordinator. In other words, communications in a star network always happen between the PAN coordinator and one of the network devices. As mentioned in Chapter 2, the IEEE 802.15.4 star network supports two network modes: beacon-enabled and nonbeacon-enabled. Beacon-enabled network requires beacons generated by the PAN coordinator to synchronize all network devices, whereas nonbeacon-enabled network has no such limitation. For channel access, beacon-enabled and nonbeacon-enabled networks use slotted and unslotted CSMA-CA mechanism respectively. In this chapter, the analysis focuses

on nonbeacon-enabled mode. Figure 4.3 shows the flow chart of unslotted CSMA-CA mechanism.

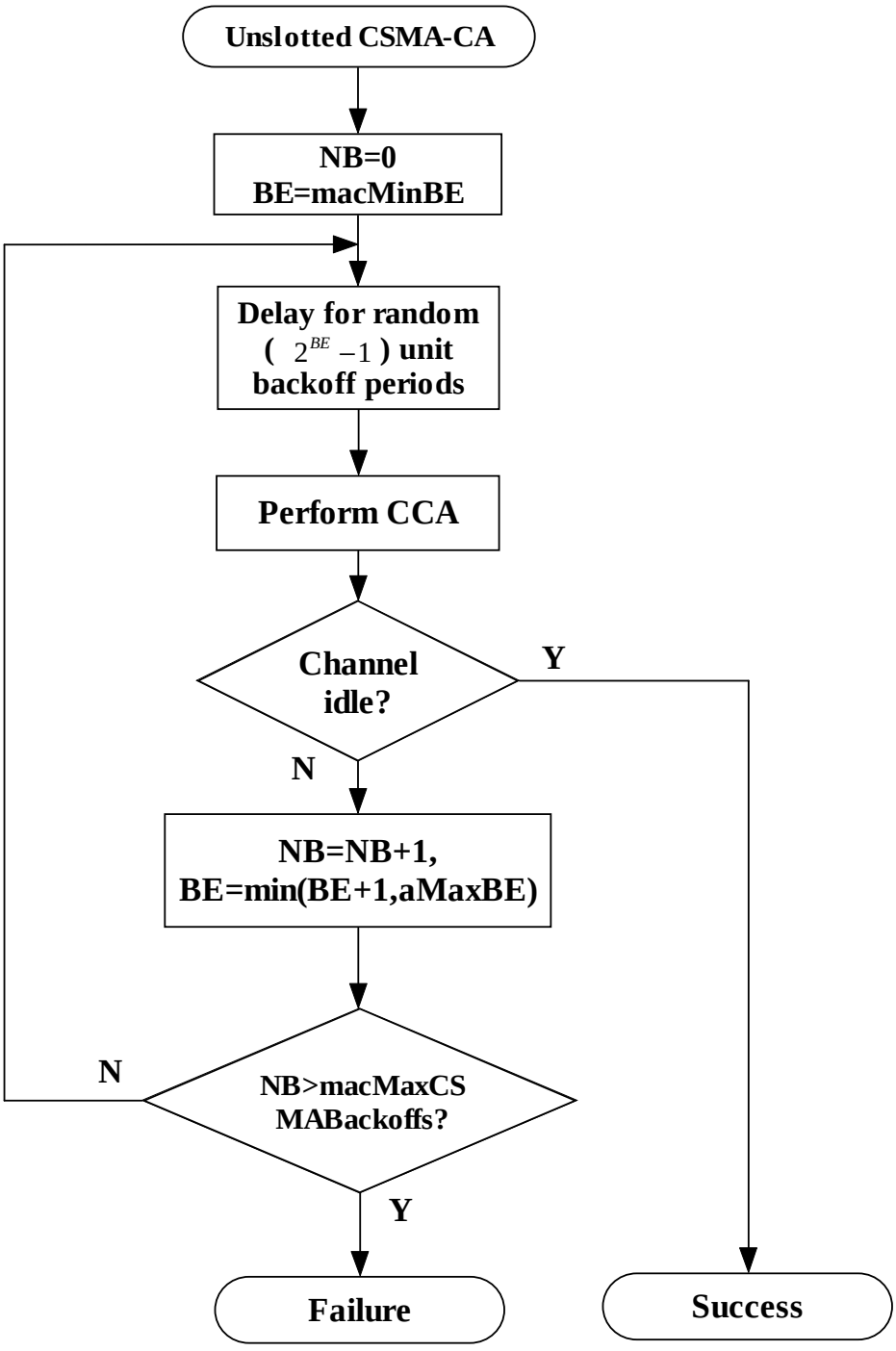

Figure 4.3 Unslotted CSMA-CA (IEEE Std802.15.4-2003, 2003)

The analysis of unslotted CSMA-CA is for the calculation of time period which a standard data transmission requires. In Figure 4.3, when an IEEE

802.15.4 device is going to transmit a packet, it first implements CSMA-CA to determine if the channel is idle. If the channel is reported to be idle, the device can transmit the packet. If the channel is reported to be busy, the mechanism of CSMA-CA will continue to monitor the channel until the allowed number of detections has been tried. The detail procedures are described as follows:

Step 1: Initialize the parameters of NB and BE

NB means the number of times the system will implement the backoff in the current transmission attempt. *BE* is the backoff exponent, which means how many backoff periods should be performed before attempting to assess the channel. *NB* and *BE* are initialized to be 0 and *macMinBE* respectively, where *macMinBE* is the minimum value of the backoff exponent in the CSMA-CA algorithm. The default value of *macMinBE* is 3.

Step 2: Delay and Clear Channel Assessment Implementation

After initialization, the system starts to delay a number of backoff periods. One backoff period is equal to *aUnitBackoffPeriod*, which is 320 μs. The size of the backoff period is randomly selected from 0 to $2^{BE}-1$ (step 1) where the default value for *BE* is 3. When the delay is finished, the MAC layer of the system can perform CCA (step2). Since the random delay is decided within the range of $(2^{BE}-1)$ and complies with uniform distribution, it is reasonable to select variance 4 for calculation. The implementation of CCA requires 128 μs. Then the time $T_{Delay-CCA}$ consumed to implement random delay and CCA is calculated as follows:

$$T_{Delay-CCA} = (2^{BE}-1) * aUnitBackoffPeriod + \text{CCA}$$

$$= 4*320\ \mu s + 128\ \mu s = 1.408\ (ms) \qquad (4.4)$$

Step 3: Judgment of Channel Status

If the channel is assessed to be busy, the system will increase *NB* by 1 and reselect *BE* from the lesser of *BE*+1 and *aMaxBE*, the maximum value of the backoff exponent defined in the CSMA-CA algorithm. If *NB* is greater than *macMaxCSMABackoffs*, which is the maximum number of backoffs that the

CSMA-CA algorithm will attempt to implement before declaring a channel access failure, the current attempt of accessing medium is announced to be failed and the MAC layer should issue a primitive of "CCA Failure" to the upper layer. If *NB* is less than *macMaxCSMABackoffs*, goes to step 1. If the channel is assessed to be idle, the MAC layer can immediately commence data transmission. If no interference is present, the channel should be idle, and the frame transmission can be commenced immediately, which requires $T_{Transmit}$:

$$T_{Transmit} = L_{Packet\_Length} / 250kbps \quad (ms) \tag{4.5}$$

where L_{Packet_Length} denotes the length of the IEEE 802.15.4 packet to be sent out by the PHY layer. The parameter 250kbps is the data rate defined by the IEEE 802.15.4 standard at 2.4 GHz frequency band.

Step 4: Retransmission

After sending out a data packet, the device requires a certain period called *aTurnaroundTime* equal to 0.192ms, to allow the radio system to switch the radio state from transmit to receive.

$$T_{Switch}=0.192 \text{ (ms)} \tag{4.6}$$

If an acknowledgement is required, the system shall wait for at most *macAckWaitDuration*, which is the maximum period of waiting for an acknowledgement to arrive following the transmission of a data packet. The value of *macAckWaitDuration* is equal to 0.864 ms. The length of an acknowledgement frame is fixed at 11 bytes. The minimum duration for acknowledgement frame transmission is 0.352 ms. Then the time T_{ACK} used to wait for an acknowledgement is defined as follows:

$$T_{ACK} \in [0.352ms, 0.864ms] \tag{4.7}$$

If the acknowledgement is received within *macAckWaitDuration* period, the transmission is considered successful. Then the MAC layer initiates a primitive of "MAC_ENMU_SUCCESS" to the upper layer. If the acknowledgement is not received, the system will automatically attempt to retransmit the packet for *aMaxFrameRetries* times, which has a default value of 3.

If the acknowledgement is still not received, the MAC layer should initiate a primitive of "NO_ACK" to the upper layer.

Therefore, if there is no interference existing, the T_{ACK} can select the minimum value. Meanwhile, the automatic retransmission is not needed.

The total transmission time $T_{Total}(L_{Packet\_Length})$ is defined as follows:

$$\begin{aligned} T_{Total}(L_{Packet\_Length}) &= 1.408 + L_{Packet\_Length} \times 8/250 + 0.192 + 0.352 \\ &= 1.952 + L_{Packet\_Length} \times 8/250 \quad (ms) \end{aligned} \tag{4.8}$$

The parameter L_{Packet_Length} denotes the length of the outgoing packet. Its unit is in bytes. Figure 4.4 illustrates the structure of data frame in the IEEE 802.15.4 standard.

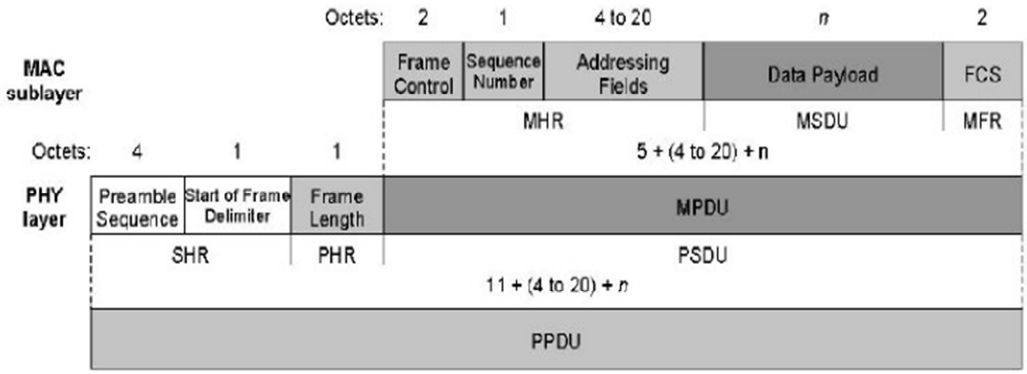

Figure 4.4 IEEE 802.15.4 data frame structure (IEEE Std802.15.4-2003, 2003)

In an IEEE 802.15.4 data frame, the packet length is controlled by the length of data placed in the "Data Payload" field. The "Data Payload" range, which is also called a MAC Service Data Unit (MSDU) is defined as *msduLength*. The definition for *msduLength* is:

$$msduLength \le aMaxMacFrameSize \tag{4.9}$$

$$\begin{aligned} aMaxMacFrameSize &= aMaxPHYPacketSize - aMaxFrameOverhead \\ &= 127 - 25 = 102(byte) \end{aligned} \tag{4.10}$$

where *aMaxPHYPacketSize* and *aMaxFrameOverhead* denote the maximum packet length which can be processed by the IEEE 802.15.4 PHY layer, and the maximum number of byte added by the IEEE 802.15.4 MAC layer to its payload respectively. Then, the maximum length of a data packet sent from the PHY layer of an IEEE 802.15.4 device is:

$$L_{Packet\_Length} = SHR + PHR + PSDU = (4+1)+1+[5+(4 to 20)+n] \quad (4.11)$$

where *SHR*, *PHR* and *PSDU* denote synchronization header, PHY header and PHY service data unit respectively (see Figure 4.4).

If the addressing field uses the minimum allowed value, then L_{Packet_Length} is defined as:

$$L_{Packet\_Length} = 15 + n \quad (byte) \quad n \in [0,102] \quad (4.12)$$

where *n* denotes the data payload .

Applying Equation (4.12) into Equation (4.8), the range of time required to complete an IEEE 802.15.4 packet transmission is obtained as:

$$T_{Total}(L_{Packet\_Length}) = 1.952 + \frac{(15+n)\times 8}{250} \quad (ms) \quad (4.13)$$

since $n \in [0,102]$, the range of T_{Total} is $\in [2.432ms, 5.696ms]$.

It is noticeable that the implementation of CCA has three modes. CCA mode 1 reports a busy medium if the detected energy level is above the energy detection threshold. CCA mode 2 reports a busy medium if a signal with the modulation and spreading characteristics of IEEE 802.15.4 is detected. CCA mode 3 reports a busy medium if a signal with the modulation and spreading characteristics of IEEE 802.15.4 with energy above a defined threshold is detected. When an IEEE 802.15.4 system is affected by IEEE 802.11b interference, CCA mode 1 will always report busy medium since the energy level of IEEE 802.11b signal is relatively high due to its high transmit power. Consequently, IEEE 802.15.4 system continues to defer transmission until transmission attempt failure. Therefore, CCA mode 2 is more suitable to be

applied if external interference is taking place. CCA mode 3 has a similar effect as CCA mode 2.

The interference analysis here emphasizes the effect of interference acting on the IEEE 802.15.4 standard. An open loop analysis is suitable to analyze the interference at the IEEE 802.15.4 receiver while ignoring the interactions between the IEEE 802.15.4 system and interferer system. Figure 4.5 illustrates a comparison of IEEE 802.11b and IEEE 802.15.4 transmission procedures on the basis of the same time line.

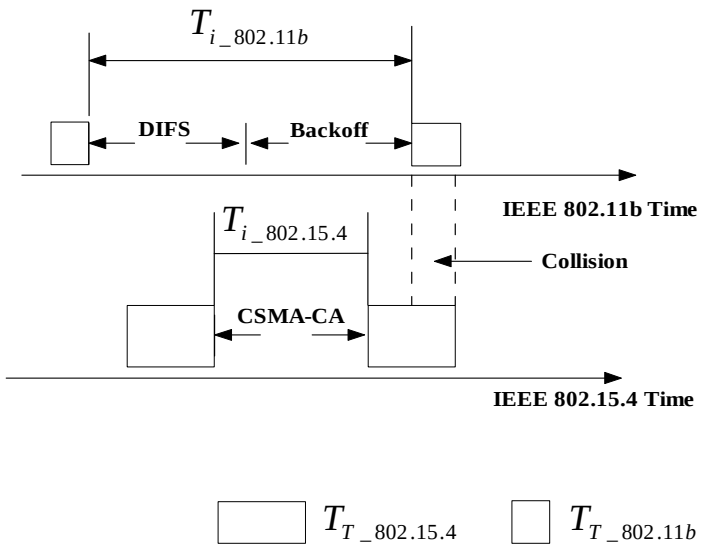

Figure 4.5 Comparison of IEEE 802.11b and IEEE 802.15.4 packet transmission

In Figure 4.5, $T_{i\_802.11b}$ and $T_{T\_802.11b}$ denote the time interval between two consecutive IEEE 802.11b packet transmissions and the time used to transmit an IEEE 802.11b data packet. $T_{i\_802.15.4}$ and $T_{T\_802.15.4}$ denote the time interval between two consecutive IEEE 802.15.4 packet transmissions and the time used to transmit an IEEE 802.15.4 data packet. For example, if the length of an IEEE 802.11b packet is 1024 bytes, then $T_{T\_802.11b}$ is about $1024\times 8/11\times 10^{6} = 0.74$ milliseconds if using 11Mbps data rate (the typical bit rate for IEEE 802.11b system). For IEEE 802.15.4 communication, if IEEE 802.15.4 transmission operates within the period of 0.74 ms which is indicated as collision part in Figure 4.5, the IEEE 802.15.4 receiver will be affected which leads to signal reception failure.

However, if IEEE 802.15.4 data transmission occurs within the period of $T_{i\_802.11b}$, the IEEE 802.15.4 data packet will be successfully transmitted. As described in Equation (4.3), the rang of $T_{i\_802.11b}$ is$\in [0.67ms, 20.51ms]$. According to Equation (4.13), a complete IEEE 802.15.4 data transmission requires time consumption ranging from 2.432ms to 5.696ms. It could be possible for an IEEE 802.15.4 system to communicate when an IEEE 802.1b system is also in operation.

4.4 Baseline Tests

Determining the data transmission capability of an IEEE 802.15.4 system can give a baseline for interference mitigation strategy design. The baseline tests were carried out on a Jennic JN5139R1 platform (JN5139, 2009).

4.4.1 Baseline Test I without Interference

The baseline test I is used to evaluate the maximum transmission capability of the IEEE 802.15.4 system without the presence of interference. The test assumes that an IEEE 802.15.4 star network consists of an IEEE 802.15.4 PAN coordinator, and an IEEE 802.15.4 network device (which is also a full function device) working in nonbeacon-enabled mode. The communication is initiated by the PAN coordinator, which transmits data requests continuously to the 802.15.4 network device. On receipt of the data request, the network device will send back an acknowledgement to the PAN coordinator. The maximum capability indicates how many such standard transactions can be completed by a pair of a PAN coordinator and normal network device within a certain period, e.g. 1 second. In baseline test I, the data transmission employed unslotted CSMA-CA with CCA mode 2.

Theoretically, the amount of IEEE 802.15.4 data packet, N_{Packet}, which can be processed by the system per second (without interference presence) is obtained as:

$$N_{Packet} = 1/T_{Total} \tag{4.14}$$

where T_{Total} is the time required to complete an IEEE 802.15.4 packet transmission and calculated in terms of Equation (4.13).

The baseline test without interference was performed between two IEEE 802.15.4 devices as illustrated in Figure 4.6.

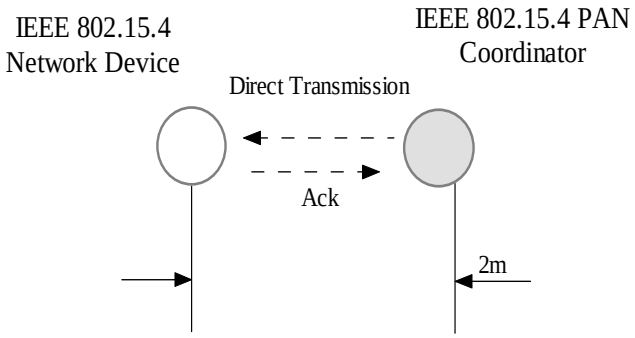

Figure 4.6 Device deployment in baseline test I

In Figure 4.6, the device acting as the IEEE 802.15.4 PAN coordinator is responsible for starting the wireless sensor network. Another IEEE 802.15.4 device acting as a normal network device is an IEEE 802.15.4 full function device. The PAN coordinator is located 2 meters away from the normal network device.

The PAN coordinator was set to continuously transmit data packets to the network device. The packets were generated by a software packet generator running on the PAN coordinator. The packet amount was decided by Equation (4.11) using different length of data payload allowed in the IEEE 802.15.4 standard. The 802.15.4 network device processed the received data packets and sends back acknowledgements to the PAN coordinator to confirm the reception. The test results are summarized in Table 4.2 and illustrated in Figure 4.7.

Table 4.2 Summary of time duration for IEEE 802.15.4 data packet transmission

Data Payload (byte)	Theoretical	Practical	Data Payload (byte)	Theoretical	Practical
2	401	361	62	226	198
12	355	290	72	211	184
22	319	264	82	198	176
32	289	245	92	186	166
42	265	227	102	176	156
52	244	209			

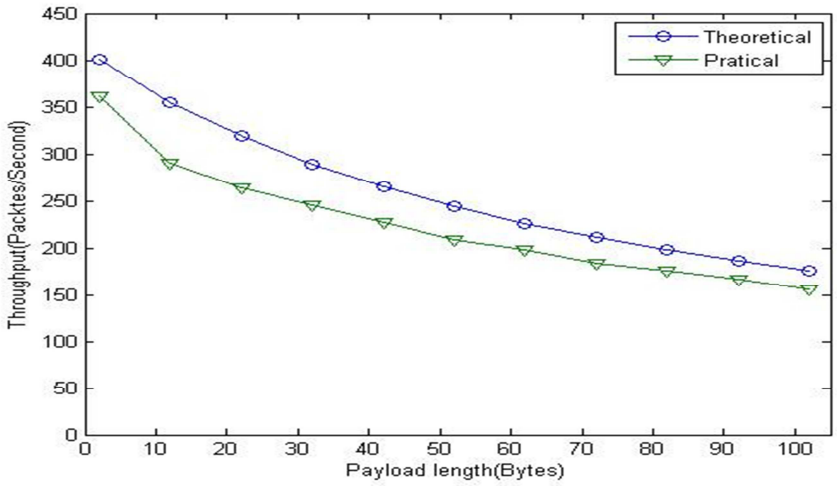

Figure 4.7 Results of baseline test I

In Table 4.2, the column labelled “Theoretical” refers to the analyzed number of data packets, which can be processed by the IEEE 802.15.4 system with different data payload length in terms of Equation (4.14). The column labelled “Practical” means the actual amount of processed data packets obtained from the baseline test I by counting the received acknowledgements on the PAN coordinator. Figure 4.7 is the comparison of the practical and theoretical values. The curve with circle denotes the theoretical packet throughput between the two IEEE 802.15.4 devices without interference. The curve with triangles denotes the practical packets throughput obtained from the baseline test I. The horizontal and vertical axes denote the payload length and IEEE 802.15.4 packet throughput

respectively. In Table 4.2 and Figure 4.7, the practical values are less than the corresponding theoretical values under the same conditions. Since the theoretical calculation does not include the time consumption required by software stack processing, it is reasonable to conclude that the practical results match the theoretical analysis. The following tests will use the result of the baseline test I as reference for the maximum transmission capacity of an IEEE 802.15.4 system.

4.4.2 Baseline Test II with Interference

The baseline test II is to evaluate the IEEE 802.15.4 system performance when interference is present. Figure 4.8 shows the device deployment in the baseline test II.

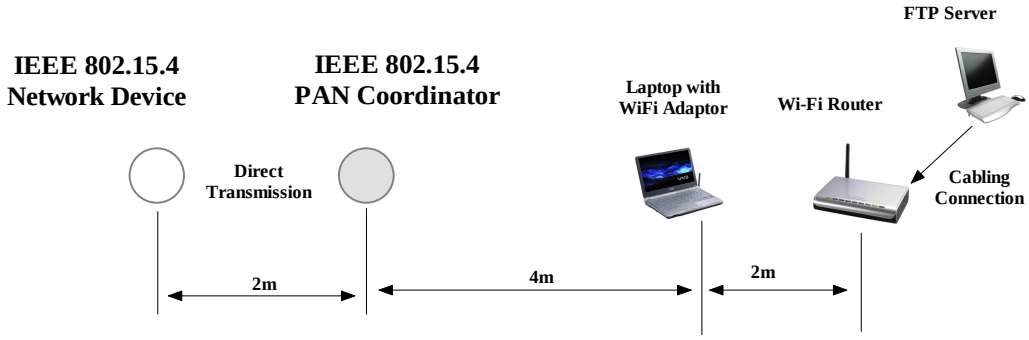

Figure 4.8 Device deployment in baseline test II with interference

In Figure 4.8, a laptop is set to download a large capacity file from a FTP server running on a computer, which uses a cable connection to a Wi-Fi (IEEE 802.11b) router. The test was carried out with four different FTP settings: no speed limit, speed limitation of 250KByte/s, speed limitation of 125KByte/s, and speed limitation of 62.5KByte/s. The PAN coordinator transmitted data packets with different data payload to the 802.15.4 network device. To illustrate the effect of interference, the IEEE 802.11b router and adaptor located with the laptop were set to work on 802.11b channel 6 (2437 MHz). The IEEE 802.15.4 network operated on 802.15.4 channel 18 (2440 MHz). The frequency offset between the IEEE 802.15.4 system and IEEE 802.11b system was 3 MHz. As the direction of IEEE 802.11b communications were mainly from the wireless router to the laptop, the interference was generated by the wireless router. The separations from the

IEEE 802.15.4 PAN coordinator and the network device to the wireless router are 6 m and 8 m respectively, which were within the 802.11b interference area. The data transmission of IEEE 802.15.4 network is the same as in baseline test I. The test results are shown in Figure 4.9.

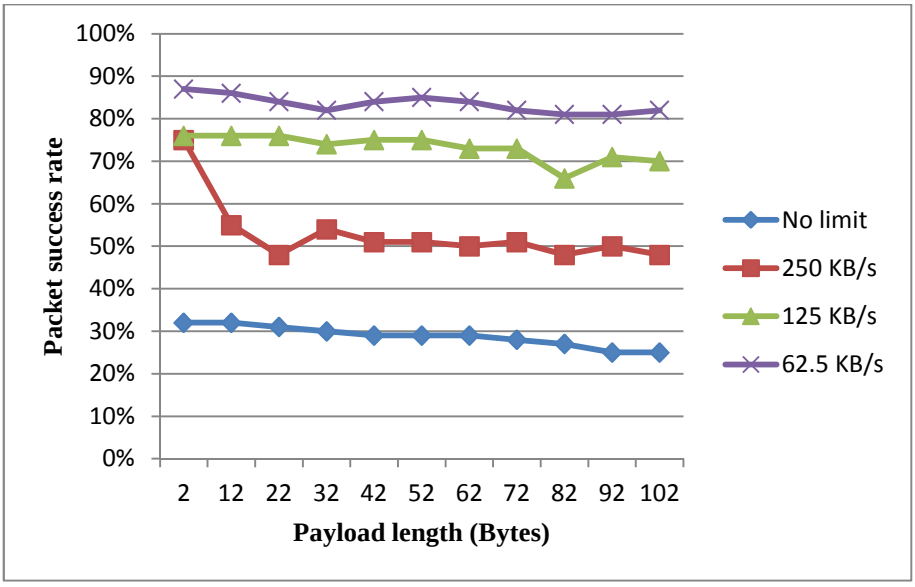

Figure 4.9 Test results of baseline test II with IEEE 802.11b interference

In Figure 4.9, the horizontal axis expresses the different lengths of data payload contained in the IEEE 802.15.4 data packets. The vertical axis expresses the packet transmission rate of the IEEE 802.15.4 communication with various IEEE 802.11b traffics (e.g. 62.5 KB/s, 125 KB/s, 250 KB/s and no limit). It is obvious that the IEEE 802.15.4 system can still possibly achieve communications when the interference is serious (the most IEEE 802.11b traffic is observed at 500-600 KB/s if it is not limited). The packet rate is obtained by comparing the amount of the received packets under the presence of interference with values derived from the column “Practical” in Table 4.2. The minimum successful rate (25%) occurs at the point where the data payload contained in the IEEE 802.15.4 packet is 102 bytes and the speed of the Wi-Fi traffic is unlimited. The maximum successful rate (87%) is observed at the point where the data payload contained in the IEEE 802.15.4 packet is 2 bytes and the speed of Wi-Fi traffic is limited to 62.5 KB/s. Therefore, we conclude that the success rate of IEEE 802.15.4 data transmission under various IEEE 802.11b traffic ranges from 25% to 87%.

4.5 Interference Mitigation Strategy

Since it has been shown that IEEE 802.15.4 communication can maintain an effective data rate under interference, the mitigation strategy can start from the point whether it is possible for an IEEE 802.15.4 system, when it is suffering from interference, to maintain communications by using consecutive data transmission. The implementation of a mitigation strategy is divided into two components: one on the PAN coordinator and another one on the normal network device.

PAN coordinator: The PAN coordinator is required to implement a regular check. Each time it sends out a data packet to the normal 802.15.4 network device, a sub-procedure for checking the result is trigged 1 second afterwards. The purpose is to check if acknowledgement has been received from the network device for the previously sent request. If the corresponding acknowledgement has been received, the task is considered to be successful. Otherwise, the PAN coordinator will assume the communication has failed. Assuming the success rate for the IEEE 802.15.4 devices communication under interference is $R_{Interference}$, and the system is achieving at least one successful communication at a probability of $P_{Success}$ after consecutively sending *n* packets, the following equation should be satisfied:

$$1-(1-R_{Interference})^n \geq P_{Success} \tag{4.15}$$

Then the number of consecutive data packets *n* can be derived by

$$n \geq \frac{\log(1-P_{Success})}{\log(1-R_{Interference})} \tag{4.16}$$

where $R_{Interference} \in [25\%,87\%]$. Given a successful rate $R_{Interference}$, which is obtained from baseline test II, the number of consecutive data packet sending given by Equation (4.16) can guarantee the success of communication. For example, if the selected rate $R_{Interference}$ is 25%, and the demanded probability $P_{Success}$ is 90%, the controller should send out 8 (i.e. packet number *n*) data request packets. If the desired acknowledgement is not able to be received after that, the PAN coordinator assumes the interference is serious. It will then send a number of

data packets consecutively for 1 second. The number of packets is decided by the data payload length. For example, if the requested packet contains a two-byte data payload, the number of packets will be 361 (refer to Table 4.2). If an acknowledgement is received during this period, the consecutive transmission should stop and the regular check is considered to be successful. Otherwise, the PAN coordinator should start energy detection and switch to a clean channel with the least energy activities. Figure 4.10 illustrates the flow chart describing the strategy implementation on the PAN coordinator.

Network device: The 802.15.4 network device implements connection-loss detection using a fixed interval. The process is: send a data packet requiring acknowledgement to the PAN coordinator every second. If the received acknowledgement matches with the outgoing packet's sequence number, the connection is thought to be normal. If a number of acknowledgements are lost, the sensor device should try to search the network on all available channels, and if it can be located, join it again. The flow chart is illustrated in Figure 4.11

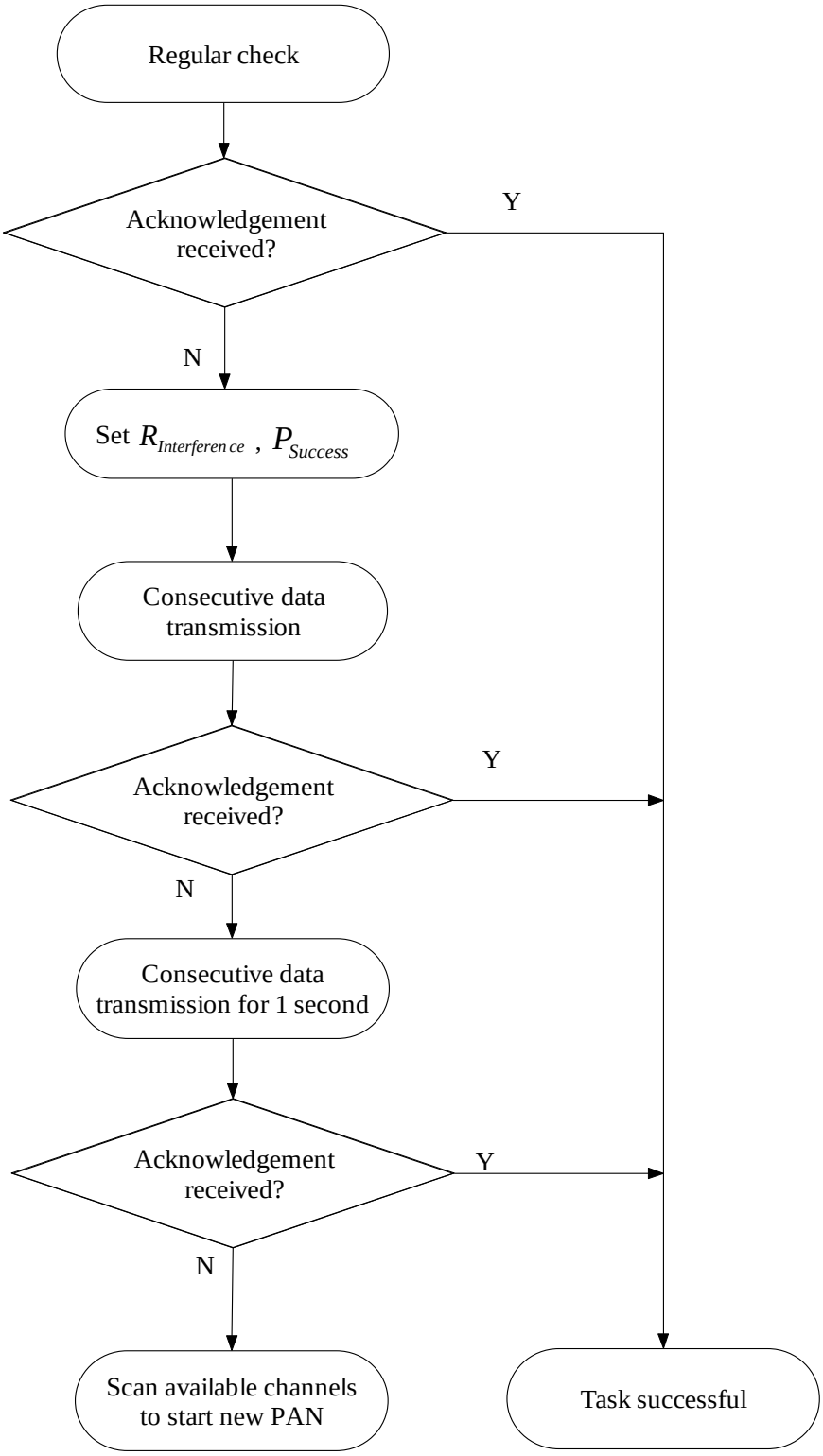

Figure 4.10 Flow chart of consecutive data transmission on PAN coordinator

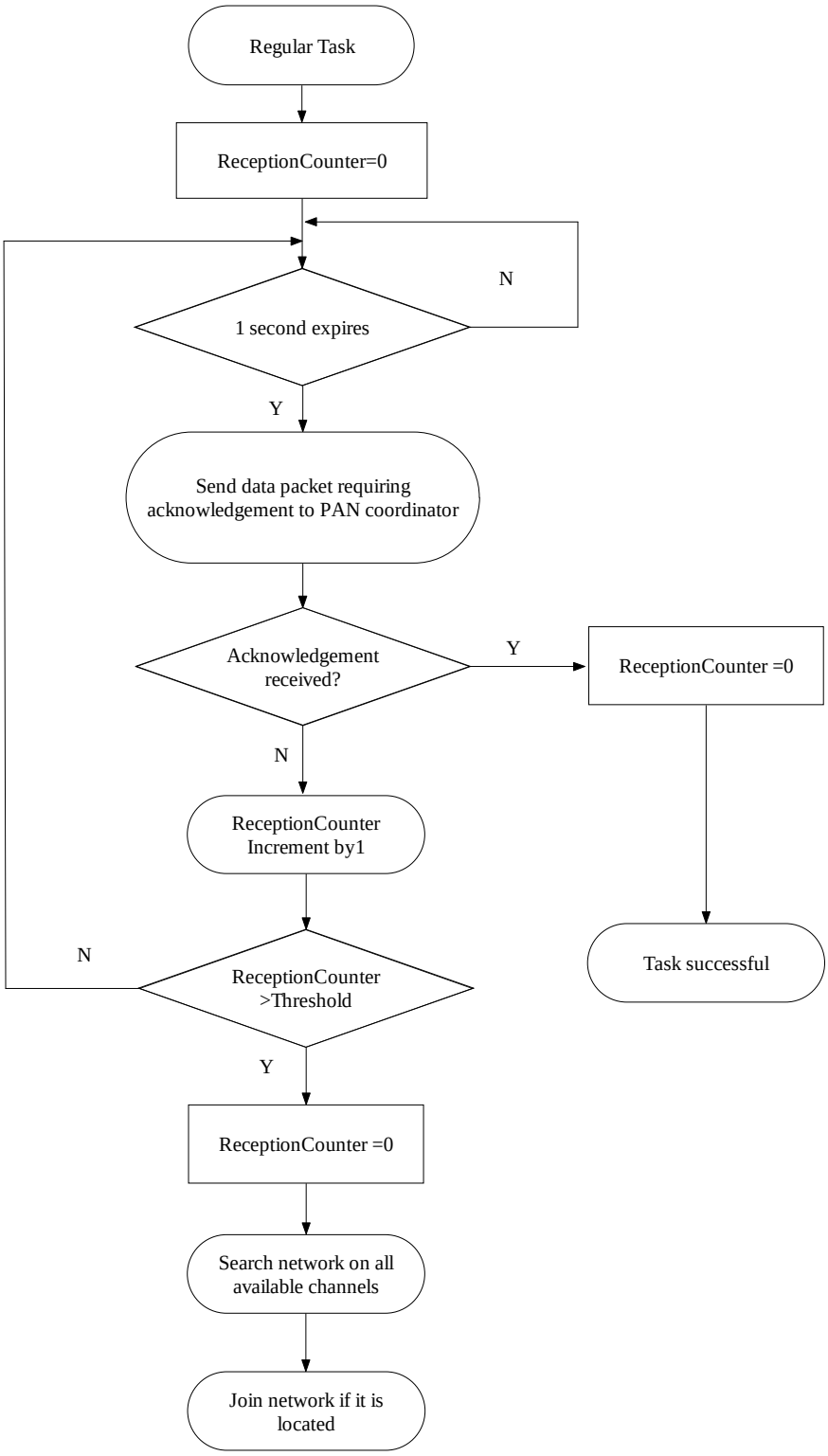

Figure 4.11 Flow chart of strategy implementation on IEEE 802.15.4 device

4.6 Evaluation Test

The evaluation test is designed to evaluate if the strategy is effective for an IEEE 802.15.4 network to achieve effective communications during the period of interference. The hardware deployment for the evaluation test is similar to that used for the base line test II. Two additional laptops are added to the scenario to generate more Wi-Fi traffic. Figure 4.12 shows the deployment.

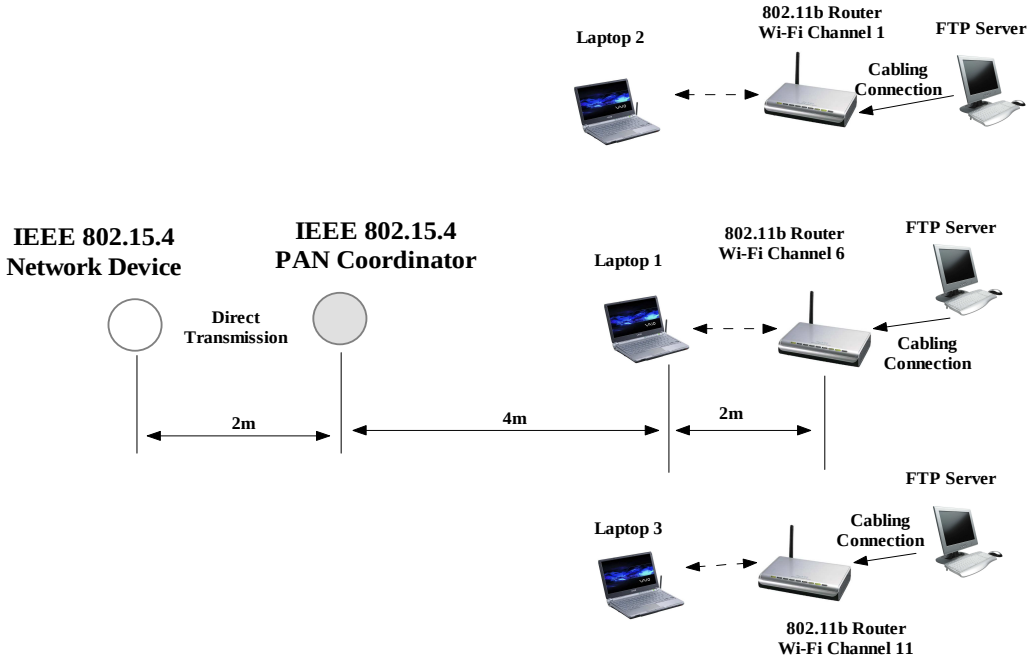

Figure 4.12 Device deployment for evaluation test

In Figure 4.12, the laptops 2 and 3 connect to two IEEE 802.11b routers working on the Wi-Fi channels 1 and 11 respectively. The laptop 1 and the connected Wi-Fi router work on the Wi-Fi channel 6. Then the three suggested non-overlapping Wi-Fi channels are utilized to realize a normal case of IEEE 802.11b networks usage. All three laptops are programmed to download large data files. The setting for the download speed is the same as in baseline test II that starts from no speed limitation and progresses to 62.5 KByte/s, 125 KByte/s, and 250 KByte/s. The working channel of the IEEE 802.15.4 network is initially set at IEEE 802.15.4 channel 18, whose centre frequency is the closest to the Wi-Fi channel 6. During the evaluation test, the PAN coordinator was set to send data

packet and required acknowledgements from the 802.15.4 network device every 5 seconds with three levels of data payload, 2 bytes, 52 bytes and 102 bytes. A total of 13 requests were used in the test. Therefore, the controller should complete the designed tasks in 60 seconds if no interference existed. If the loss of acknowledgement was detected on the PAN coordinator, the proposed mitigation strategy will be implemented. The IEEE 802.15.4 device kept implementing a connection test every second. If ten acknowledgements from the PAN coordinator were lost, the IEEE 802.15.4 network device should start to scan available channels to locate the network. Due to the uncertainty of interference, the selection of threshold did not have certain rules to follow. The smaller the threshold was, the quicker the response will be made by the network device, and vice versa. However, a small threshold possibly made the network device frequently search network, and a large threshold can lead to a long delay in response. In practical application, the selection of threshold should accord with system requirements. To make it convenient for comparison, the test was carried out with and without interference occurring respectively. The test results are shown in Figure 4.13 and Table 4.3.

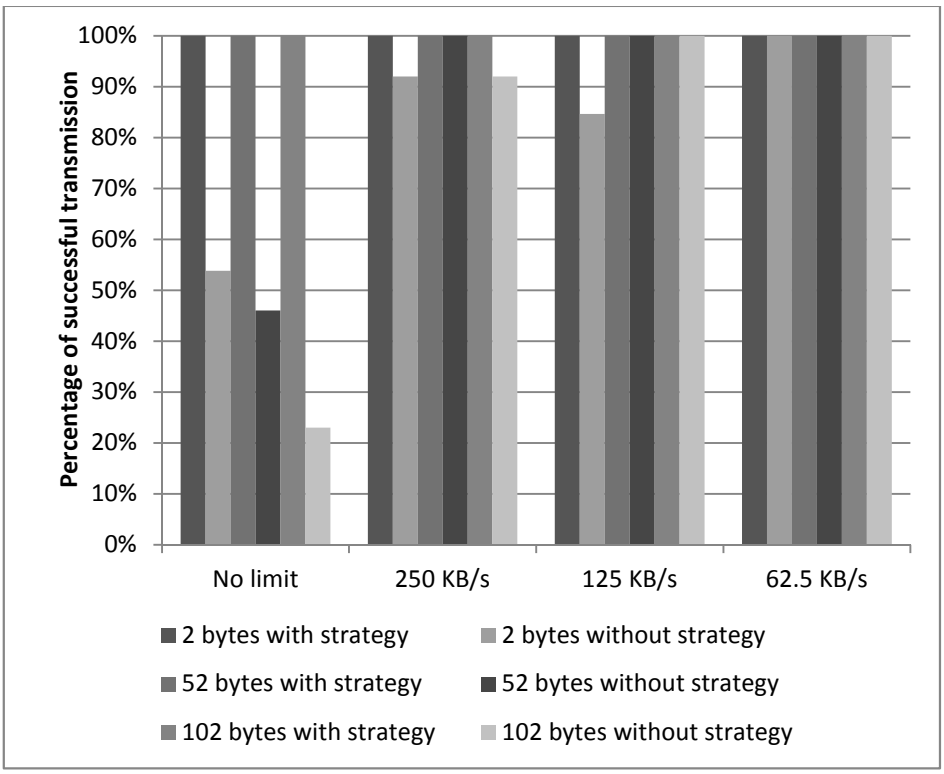

Figure 4.13 Probability of successful transmission in the evaluation test

In Figure 4.13, test results with three kinds of data payloads generated by the PAN coordinator are selected for comparison. The columns indicate the success rates for packets with different payloads under different IEEE 802.11b interference. The primary difference between the results obtained with and without 802.11b interference mainly occurs at the point where no speed limitation is applied to the IEEE 802.11b traffic. For data packets sent by the PAN coordinator, if no strategy is applied, the higher data payload contains the lower successful rate is obtained. For example, when no speed limitation is applied to the IEEE 802.11b traffic, and if data payload is 2 bytes, the success rate is 53.8%. If the data payload is 102 bytes, the success rate is 23%. When IEEE 802.11b traffic is slower, the success rate of data transmission without strategy implementation is slightly less than the success rate with strategy implementation. No data transmission is lost when the strategy was applied as the system utilizes consecutive retransmission to ensure connectivity. For other settings of IEEE 802.11b traffic, the successful rates for both of the two situations were similar.

Table 4.3 Result summary of evaluation test

		With strategy				Without strategy			
Payload (Byte)	Date Rate	Channel Switch	Time (Second)	Retry	Success	Channel Switch	Time (Second)	Retry	Success
2	No limit	1	97	520	13	0	60	0	7
2	250KB/s	0	65	3	13	0	60	0	12
2	125KB/s	0	65	0	13	0	60	0	11
2	62.5KB/s	0	65	0	13	0	60	0	13
52	No limit	1	98	468	13	0	60	0	6
52	250KB/s	0	66	7	13	0	60	0	13
52	125KB/s	0	65	0	13	0	60	0	13
52	62.5KB/s	0	65	0	13	0	60	0	13
102	No limit	1	95	238	13	0	60	0	3
102	250KB/s	0	65	6	13	0	60	0	12
102	125KB/s	0	65	3	13	0	60	0	13
102	62.5KB/s	0	65	3	13	0	60	0	13

Table 4.3 gives a summary of the actual result obtained from the evaluation test. The column labelled as “Payload” denotes the payload length contained in packets sent by the PAN coordinator. The label “Data Rate” indicates the IEEE 802.11b traffic setting. The label “Channel Switch” indicates how many

times the PAN coordinator switched channel when consecutive data transmission strategy was not effective. Column with label “Time” means how long the 13 data transmissions are completed. The label “Retry” means how many consecutive data transmissions were implemented with the given condition. The label “Success” means the number of successful data transmission of 13 designed packets. If no strategy is applied, the PAN coordinator will neither switch channel nor attempt to retransmit. When the IEEE 802.11b traffic is not limited, the data transmission with a 2-byte data payload has a success rate of 53.8% (which means 7 of 13 data transmission are successful), and a request with a 102-byte data payload has a success rate of 23% (which means 3 of 13 data transmission are successful). If the strategy is applied, the PAN coordinator will switch the channel once when the traffic has no limitation. For other IEEE 802.11b traffics (e.g. 250 KB/s, 125 KB/s and 62.5 KB/s), the PAN coordinator implements the consecutive data transmission for a few times, whereas channel switch is not used.

Although the three typical non-overlapping channels specified in the definition of IEEE 802.11b have been occupied by the three Wi-Fi routers used in the evaluation test, the PAN coordinator is still able to switch to the last two IEEE 802.15.4 channels (channel 25 and 26) which are isolated from the effect of the IEEE 802.11b communication channels. This is the reason why only one channel switch was needed during the test. According to the observation during the evaluation test, the maximum IEEE 802.11b data rate stays at around 500-600 KBytes/s, which is thought to be close to saturation in a practical environment (Thonet et al. 2008; Xiao, et al 2002). Therefore, the PAN coordinator has to retransmit several times in order to maintain communications. When the 802.11b traffic is limited, the PAN coordinator might still need to retransmit a few times, but there is no need to switch channel. When the Wi-Fi traffic is reduced to 62.5KByte/s, the IEEE 802.15.4 network is almost unaffected. The reason is that, if the 802.11b traffic is controlled at 250KByte/s or less, and assuming a typical 802.11b packet length is 1024 bytes, the interval between two 802.11b packets is on average 3.4 ms or more. If the IEEE 802.15.4 packet length is 17 bytes (2 bytes for data payload, 15 bytes for packet header), the actual radio transmission time is $17 \times 8 bits / 250 kbps = 0.544 ms$, which is small enough to be completed within an

IEEE 802.11b packet interval. Consequently the successful rate of the IEEE 802.15.4 network communication will be higher if the IEEE 802.11b traffic rate becomes lower.

The implementation time required for the mitigation strategy is longer than the one without strategy. When the PAN coordinator decides to change the working channel, the communication will be suspended until the network device re-associates with the PAN coordinator. The decision for the network device to start the procedure of re-association depends on the definition of connection-loss detection. If the network device selects a large counting value, for example, 100 as the threshold to judge if the PAN coordinator has moved to other channels, it will start re-association only after the counter expires.

The proposed strategy allows an IEEE 802.15.4 based star WSNs to maintain communications without frequently switching working channels when interference is occurring. It is probable that a Wi-Fi network is in stature state (e.g. IEEE 802.11b network with traffic over 600 KB/s) in a home environment, e.g. downloading file, multimedia applications. Therefore, the interference issue caused by a Wi-Fi system is becoming more and more important for IEEE 802.15.4 networks. The increasing popularity of home appliances working on the 2.4 GHz band, e.g. wireless monitoring camera, cordless phone, headset, will also probably result in the situation that there is no “clean” channel for IEEE 802.15.4 networks to switch. Therefore, the proposed strategy can be used to ensure acceptable network connectivity during the periods of interference.

4.7 Summary

The IEEE 802.15.4 based WSNs are suitable for home automation, personal computer peripherals, toys and games, and personal health care applications. When such kinds of wireless sensor networks are deployed in the vicinity of an IEEE 802.11b network, the 802.15.4 network communications could be affected when the IEEE 802.11b traffic is high. However, by utilizing the interval existing between 802.11b packets and consecutive data transmission with proper time control, 802.15.4 communication can still be achieved under

interference. The proposed mitigation strategy can provide the wireless sensor network with the greatest ability to maintain communications when saturated traffic from a Wi-Fi system occurs. Through maintaining the minimum and essential communications, the wireless sensor network can always remain in operation by the means suggested in this chapter, or another e.g. by switching to other channels.

As most research outputs focus on the interference analysis and static deployment to mitigate interference effect, the proposed strategy is a practical solution to enable the system to implement anti-interference to a level. The detailed analysis and implementation of consecutive data transmission strategy for an IEEE 802.15.4 based home automation network will be described in Chapter 7 as a case study.

Chapter 5 Interference Estimation According to Dynamic Energy Detection

5.1 Background and Motivation

In Chapter 4, an interference mitigation strategy was proposed for an IEEE 802.15.4 based WSN to maintain communications under interference. Since the strategy is achieved through consecutively transmitting data packets, it is suitable for applications that have a small number data acquisition at relatively long intervals. Other applications may require data at relatively shorter intervals. As indicated in the IEEE 802.15.4 standard, a wireless sensor network is also suitable for applications such as personal computer peripherals, toys and games. Consecutive data are required in such applications for data sampling and control purposes. For example, if a pair consisting of an IEEE 802.15.4 transmitter and a receiver is adopted for a computer mouse, the transmitter should continuously send sampling data of the position of the sensor to the receiver, in order to display the movements of the mouse on the computer screen. As more and more computers are integrated with IEEE 802.11 network adaptors, the IEEE 802.11 signals can cause interference that affect the use of the IEEE 802.15.4 peripheral devices operating in the same physical location. In this situation, employing consecutive transmissions for individual IEEE 802.15.4 data packets is unrealistic.

Due to the low complexity of the IEEE 802.15.4 protocol stack, the standard does not specify physical layer strategies for mitigating the effect of

interference (i.e. modulation scheme switch or frequency agility). Although this lack of capability for implementing a sophisticated algorithm makes the IEEE 802.15.4 system inefficient in responding to interference, it is possible to apply system level adjustments to maintain an acceptable level of performance. An IEEE 802.15.4 transmitter can adjust the length of the data packets to reduce the chance of collision with interfering signals if a brief estimation of the interference pattern is detectable. In this chapter, a feasible mitigation strategy is proposed for IEEE 802.15.4 WSNs to estimate interference by detecting energy activities on the corresponding radio frequency, and make appropriate software adjustments without changing hardware settings.

5.2 Interfering Signal and Energy Activity

Different wireless systems usually employ different wireless techniques to achieve communications. For example, IEEE 802.11b uses a baseband modulation of differential binary phase shift keying (DBPSK) and differential quadrature phase shift keying (DQPSK) to provide wireless communication capability (IEEE Std802.11, 2007). Bluetooth and IEEE 802.15.4 employ Gaussian Frequency Shift Keying (GFSK) (IEEE Std802.15.1, 2005) and offset quadrature phase-shift keying (O-QPSK) respectively (IEEE Std802.15.4-2003, 2003). Therefore, wireless devices employing different techniques cannot establish direct wireless communication links. If an IEEE 802.15.4 WSN is experiencing interference, it is impossible for the 802.15.4 system to identify the origins of that interference by itself.

This lack of knowledge about the characteristics of the interferer makes the victim (i.e. IEEE 802.15.4 WSN) unable to take the initiative in avoiding interference, e.g. arranging a special channel access mechanism by cooperating with interferers. However, a brief state of interference is possible to be estimated. In general, the progress of radio signal transmission is also the progress of energy radiation in space (Foschini et al., 1998). When interference happens, the IEEE 802.15.4 receiver located within the same region as the source of interference can detect this change of energy level on the specified channel by implementing energy detection. As mentioned in chapter 2, an IEEE 802.15.4 receiver can be

functional if the measured SNR (Signal-Noise Ratio) is greater than a certain threshold, which means the allowed noise on the current communication channel should be less than a certain predefined level. If the detected energy level on the communication channel is higher than the permitted value, it can be concluded that the radio environment is being interfered with.

As indicated by Petrova et al. (2006), the payload length of an IEEE 802.15.4 packet can impact on the system performance when 802.15.4 communications are experiencing interference. Employing a shorter payload on the 802.15.4 transmitter can effectively reduce the chance of a given data packet experiencing interference. Once the energy from the source of interference is detectable on the communications channel, the IEEE 802.15.4 transmitter can improve system performance by making appropriate adjustments on the system such as select a suitable data payload length, or change transmission interval.

5.2.1 Interference Analysis

The IEEE 802.15.4 technique employs DSSS in its physical layer to spread the desired signal over a wide frequency band in order to reduce the chance of being affected by narrow band signals (ZigBee, 2007). In addition to DSSS, the IEEE 802.15.4 standard divides the 2.4 GH ISM band into 16 non-overlapping channels. When IEEE 802.15.4 devices are in communication, the signals' characteristic in the frequency domain is a continuous energy distribution within a range of frequency band (Beyer et al., 2006) (See Figure 5.1).

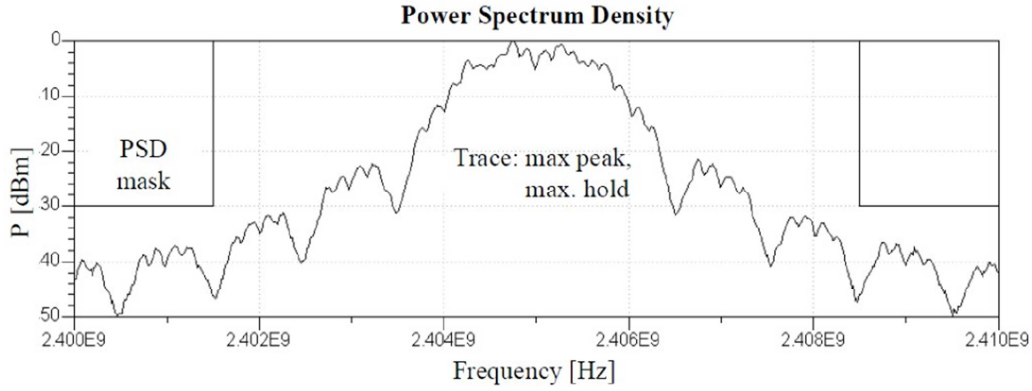

Figure 5.1 Transmission power spectrum density of IEEE 802.15.4 (Beyer et al., 2006)

In Figure 5.1, the power spectrum density measured on the 802.15.4 transmitter describes the energy distribution on 802.15.4 channel 11, whose centre frequency is 2405 MHz. According to the requirement of the IEEE 802.15.4 standard, the maximum output power is 0 dBm, which is equivalent to 1 milliwatt. With the increment of distance that signals travel, the level of energy attenuates. When two IEEE 802.15.4 devices are communicating with each other, the energy radiation persists till the signal transmission finishes.

Among the other network standards operating in the 2.4 GHz ISM band, Bluetooth and IEEE 802.11b are two typical examples utilizing distinct channel access mechanisms. They also have similar characteristic on the transmission power spectrum density. The Bluetooth technique utilizes frequency hopping to establish wireless communication links. Each Bluetooth communication channel has a bandwidth of 1 MHz which is half of the IEEE 802.15.4 channel. A total of 79 channels are defined in the Bluetooth standard. The output power is often less than 4 dBm, which is equivalent to 2.5 milliwatt. A Bluetooth device can achieve a hopping frequency of up to 1600 hop/s, which means it only operates in 1 channel for 625μs. Even if the current Bluetooth channel overlaps with the IEEE 802.15.4 channel, it will hop to another channel very soon. Therefore the Bluetooth standard will not severely affect 802.15.4 communications (Jennic, 2008).

The IEEE 802.11b utilizes DSSS like the IEEE 802.15.4 standard. Each IEEE 802.11b communication channel has a bandwidth of 22 MHz, which is much larger than an IEEE 802.15.4 communication channel with a bandwidth of 2 MHz. In the IEEE 802.15.4 standard, the effect of the IEEE 802.11b interference signal on an IEEE 802.15.4 receiver is assumed to be similar to additive white Gaussian noise in the same bandwidth, which normally compose part of the noise measured on the IEEE 802.15.4 receiver. During periods when the IEEE 802.15.4 devices are in communications, whilst the employed communication channel overlaps with the IEEE 802.11b channel, the IEEE 802.15.4 receiver will continue to suffer interference. The effect of interference is usually measured by two metrics: bit error rate and packet error rate (Petrova et al., 2006). The “bit error rate” is used to measure the probability of bit transmission error when the victim (e.g. IEEE 802.15.4 signal) overlaps with an interferer (e.g. IEEE 802.11b signal).

The value of bit error rate is a variable depending on both the modulation techniques employed by the victim and interferer. The "packet error rate" indicates the probability for a packet received in error. We denote the bit error rate of IEEE 802.15.4 system by $B_{802.15.4\_802.11b}$ when the interferer is IEEE 802.11b signal, and the packet error rate by P_{Error}. For an IEEE 802.15.4 packet to be error on the receiver, this value is defined as follows(Shin et al., 2007):

$$P_{Error} = 1 - (1 - B_{802.15.4\_802.11b})^{T_C / T_{Bit\_Duration}} \quad (5.1)$$

where T_C and $T_{Bit\_Duration}$ denote the duration of collision for IEEE 802.15.4 and IEEE 802.11b transmissions, and the time required to transmit 1 bit of IEEE 802.15.4 data. As specified by the IEEE 802.15.4 standard, the performance of an IEEE 802.15.4 network is acceptable if P_{Error} is less than 1% (IEEE Std802.15.4-2003, 2003). However, the packet error rate calculation shown in Equation (5.1) is not applicable when an IEEE 802.15.4 system is in practical use. One of the greatest difficulties in wireless interference studies arises from the victims' (i.e. IEEE 802.15.4) inability to recognize the type of interfering signal due to the different modulation schemes employed. Hence the value of the bit error rate cannot be determined. T_C is also undetectable since an IEEE 802.15.4 transmitter is unable to sense the existence of interference during the time of transmission. Figure 5.2 compares the packet transmission of IEEE 802.11b and IEEE 802.15.4 systems.

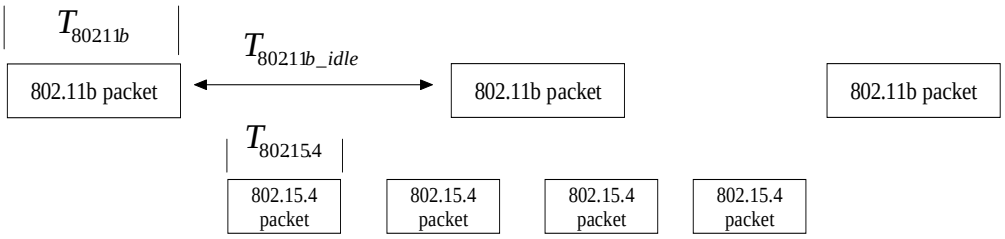

Figure 5.2 Comparisons of IEEE 802.11b and IEEE 802.15.4 packet transmissions

In Figure 5.2, $T_{802.11b\_idle}$ denotes the interval between two IEEE 802.11b packets, $T_{802.11b}$ and $T_{802.15.4}$ denote the time consumed to transmit an IEEE 802.11b

signal and a IEEE 802.15.4 signal respectively. As analyzed in Chapter 4, if the IEEE 802.15.4 packet transmission is completed within $T_{802.11b\_idle}$, the WSN communications can be achieved when the network is under interference. However, an IEEE 802.15.4 system is unable to know when the interferer's transmission starts and how long it will last. A reasonable way to mitigate interference effects under such situations is to adjust the IEEE 802.15.4 packet length in order to increase the possibility for the 802.15.4 packet to be processed within $T_{802.11b\_idle}$.

5.2.2 Energy Detection

Energy detection is usually used to detect the energy activity on the specified frequency band. An energy detection experiment was implemented in this study to verify if the IEEE 802.15.4 receiver could sense the existence of interfering energy and idle periods. During the energy detection test, an IEEE 802.15.4 receiver and an IEEE 802.11b transmitter were set to work in close proximity (e.g. about 2 metres). The IEEE 802.15.4 receiver concentrated on energy detection with the specified parameters. The IEEE 802.11b transmitter continued to send out data packets with a fixed packet length. Figure 5.3 illustrates the hardware used in the energy detection test.

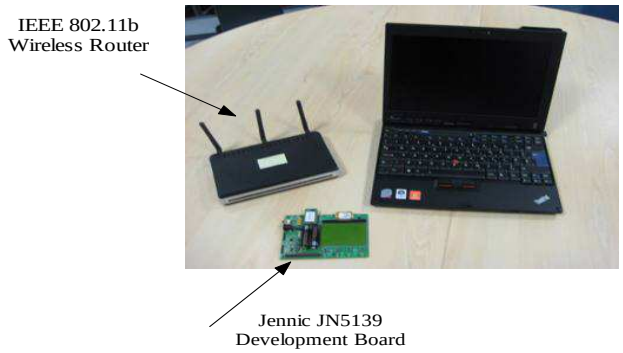

Figure 5.3 Hardware used in energy detection test

In Figure 5.3, the wireless router is set to work under the IEEE 802.11b mode. The Jennic JN5139R1(JN5139, 2009) development board is configured as

an IEEE 802.15.4 receiver to periodically implement the energy detection and display the result on an liquid crystal display (LCD) screen. The IEEE 802.11b traffic is generated by the laptop and broadcast via the wireless router. Table 5.1 and 5.2 summarize the testing parameters for the IEEE 802.11b traffic and IEEE 802.15.4 energy detection. Figure 5.4 depicts the deployment of energy detection experiment.

Table 5.1 IEEE 802.11b traffic setting in energy detection test

Packet Length (Byte)	1024
Transmission Rate (Mbps)	11 Mbps
Traffic Rate (Packet/second)	600, 500, 400, 300, 200, 100, 10
Working Channel	11
Frequency Range (MHz)	2451<->2473
Centre Frequency (MHz)	2462

Table 5.2 IEEE 802.15.4 receiver setting in energy detection

Single Sampling Period (μs)	128, 1024, 2048, 4096
Sampling Resolution (MHz)	1
Energy Detection Range (dBm)	-11 <-> -98
Sampling Frequency range (MHz)	2380<->2505

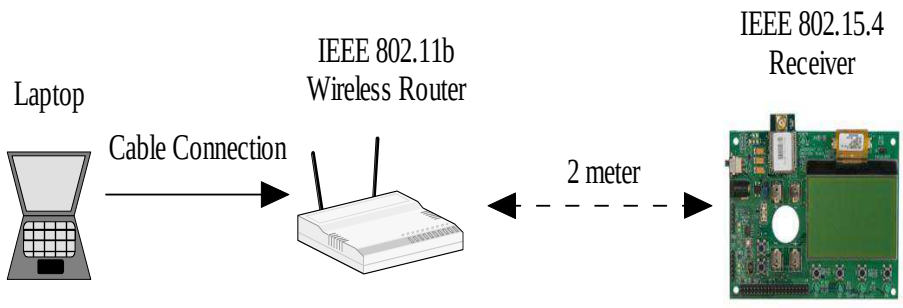

Figure 5.4 Hardware deployments for energy detection test

As depicted in Figure 5.4, the laptop connects to the IEEE 802.11b wireless router using a cable connection. The router works on the IEEE 802.11 channel 11 whose centre frequency is 2462 MHz and the frequency convergence

ranges from 2451 Mhz to 2473 MHz. The length of the IEEE 802.11b packet is fixed at 1024 Bytes. A packet generator running on the laptop enables the wireless router continuously to broadcast IEEE 802.11b signals. The IEEE 802.15.4 receiver listens on sampling frequency (from 2380 MHz to 2505 MHz) in turn and displays the result on the screen using a bar graph. Initially, the sampling period is 128μs, which means the 802.15.4 receiver will listen on a frequency for 128μs and then move to the next frequency. Figure 5.5 illustrates the flow chart of the energy detection experiment.

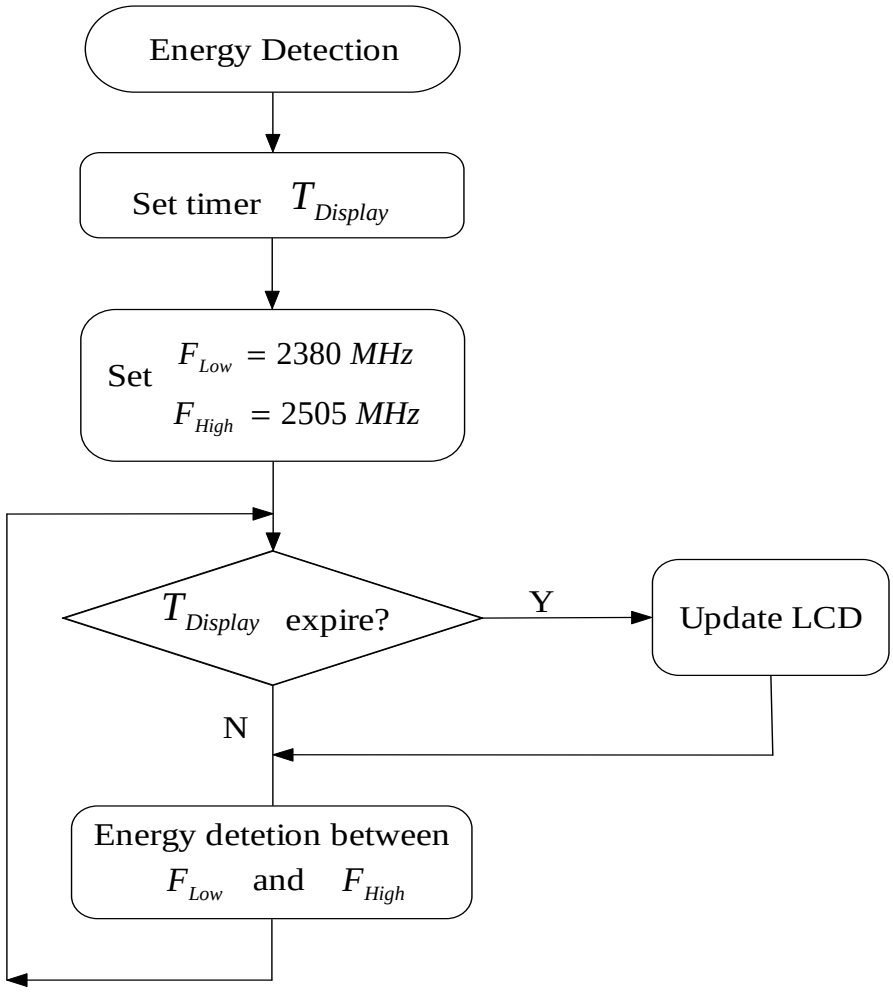

Figure 5.5 Flow chart of the energy detection experiment

In Figure 5.5, the IEEE 802.15.4 receiver firstly sets a timer $T_{Display}$ to regularly update the LCD. The energy detection range on the frequency is set between 2380 MHz and 2505 MHz. If $T_{Display}$ expires, the LCD screen will be

updated with the latest energy detection result. Otherwise, the energy detection function will be continuously implemented. Figures 5.6 to 5.12 illustrate the energy detection result shown on the LCD screen with the corresponding IEEE 802.11b traffic rate.

Figure 5.6 802.11b traffic 600 packet/second

Figure 5.7 802.11b traffic 500 packet/second

Figure 5.8 802.11b traffic 400 packet/second

Figure 5.9 802.11b traffic 300 packet/second

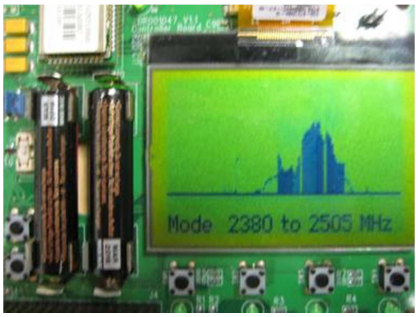

Figure 5.10 802.11b traffic 200 packet/second

Figure 5.11 802.11b traffic 100 packet/second

Figure 5.12 802.11b traffic 10 packet/second

In the above figures, the parameter “mode” means the displayed content on the screen is the result of energy detection, “2380 to 2505 MHz” denotes that the energy detection is implemented on the radio frequency ranges from 2380 MHz to 2505 MHz. From Figure 5.10 to Figure 5.12, the displayed bar chart becomes more and more sparse. This is due to the decrement of the IEEE 802.11b traffic. Take Figure 5.12 as an example, only a small fraction of the IEEE 802.11b energy activities is captured. The 10 packet/second traffic means a period of IEEE 802.11b packet transmission which is equivalent to $1024Byte \times 8/11Mbps = 740\mu s$

should occur every 100 millisecond. Since energy detection is implemented by keeping the receiver listening on the specified frequency, a short sampling period will lead to fast frequency switching. Then, before the next time 802.11b packet transmission takes place, the energy detection function has completed tasks on several frequencies, and updated the graphic interface displaying a low level of energy activities. If the sampling period is relatively enlarged, the receiver will stay on each individual frequency longer, and the chance of experiencing interfering energy will be increased. Figures 5.13 to 5.15 show the energy detection result with different sampling periods.

Figure 5.13 802.11b traffic 10 packet/second, 802.15.4 sampling period 1024μs

Figure 5.14 802.11b traffic 10 packet/second, 802.15.4 sampling period 2048μs

Figure 5.15 802.11b traffic 10packet/second, 802.15.4 sampling period 4096μs

As expected, the energy detection with an enlarged sampling period is shown to have more chance to determine the existence of interference energy on the frequency. By using different sampling periods, the results of energy detection can provide two kinds of information: the energy level of the interference on the specified frequency band and the interference frequency during the sampling period. Although a victim cannot establish direct communications with the source of the interfering signals, the above information revealed by energy detection provides a theoretical possibility that the victim can adjust its packet length to make use of idle periods existing within interfering signals, which aims to achieve an optimized performance under interference. In other words, if the sampling period of energy detection is equal to or greater than the transmission period of the desired packet, the IEEE 802.15.4 device should be able to estimate if the data transmission will be affected at the current time.

5.3 Interference Mitigation Strategy with Energy Detection

On the basis of the energy detection test results, a strategy has been proposed to help IEEE 802.15.4 based systems carry on working under the presence of interference. The idea is that if the IEEE 802.15.4 system can detect the length of the idle period between the interfering signals, and adjust its packet to a suitable length, then the chance for IEEE 802.15.4 packet transmissions to collide with interference packets can be reduced. Consequently, the interference can be mitigated to some extent. The energy detection test shows that when interference occurs, it will cause energy change in the radio frequency field. The change can only be detected when the interfering transmitter is working.

5.3.1 Estimation of Interference Pattern

When an IEEE 802.15.4 transmitter realizes that the data transmission is becoming unstable (e.g. too many acknowledgements are lost), it can start energy detection to scan the frequency currently being used and the adjacent radio frequencies. The energy detection $E(F_S, F_E, N)$ is defined as follows:

$$E(F_S, F_E, N) = \begin{bmatrix} E_{F_S,1} & E_{(Fs+1),1} & \cdots & E_{(F_E-1),1} & E_{F_E,1} \\ E_{F_S,2} & E_{(F_S+1),2} & \cdots & E_{(F_E-1),2} & E_{F_E,2} \\ \cdots & \cdots & \cdots & \cdots & \\ E_{F_S,N} & E_{(F_S+1),N} & \cdots & E_{(F_E-1),N} & E_{F_E,N} \end{bmatrix} \quad (5.2)$$

where F_S and F_E denote the range of the frequency band (the lower band and the upper band) on which the victim will implement energy detection, *N* denotes the times of detection. The result of energy detection is an energy matrix, which reflects the status of energy distribution on the selected frequency range and time domain. Note that the selection of F_S and F_E depends on the estimation of the frequency range within which the victim could be affected. Theoretically, a 2MHz scope can satisfy the use of IEEE 802.15.4 receiver as its receiver bandwidth is 2MHz. However, the scope can be properly increased in order to cover the energy distribution over a wide frequency range. This is potentially useful if channel switching is required. The element of energy matrix $E_{(F_s+i),j}$ expresses the detected energy level on the specified frequency i for the jth energy detection, where $(F_s + i) \in [F_S, F_E]$ and $j \in [1, N]$.

The energy matrix is used to express how powerful interference can be at a range of the possible interfering frequencies. Each element of the energy matrix records the maximum energy value detected on the specified radio frequency within the specified duration. However it does not mean any of these values is harmful to IEEE 802.15.4 transmissions. An IEEE 802.15.4 receiver can tolerate a certain level of interference if the required SNR is satisfied. For example, in the IEEE 802.15.4 standard, a normal IEEE 802.15.4 system requires the packet error rate to be less than 1%. Correspondingly, the required SNR is greater than 5 dB (IEEE Std802.15.4-2003, 2003). If the energy level of the IEEE 802.15.4 signal falling within a receiver bandwidth is -80dBm, the interference energy level which is greater than -85dBm (-80-5) is unacceptable. If the energy detection returns value over -85dBm, the current frequency might be unsuitable for IEEE 802.15.4 communications, and -85 dBm can be set as a threshold $E_{Threshold}$ to determine if the current channel is suitable for the IEEE 802.15.4

communications. The interference means that a receiver is unable to be functional during periods of interference. Therefore the energy detection is useful if it is implemented at the receiver side. However, for short-range applications (e.g. motion sensor on game controller or wireless mouse), it is reasonable to have the transmitter implement energy detection for two reasons:

1) IEEE 802.15.4 is a short-range technique for devices working within 10 meters. The energy level detected on the transmitter could be close to the value measured on the receiver when the transmitter is relative close to the receiver.

2) In such applications, IEEE 802.15.4 receiver usually works in passive mode, which means it is always in the state of receiving. Logically, the receiver would not take the initiative in implementing energy detection unless specified.

Once the threshold is determined, the processed energy matrix can be converted into a new binary matrix, which contains only the binary values 0 and 1. The value 0 means the frequency is clean during that period if the energy level is less than the threshold. The value 1 means the frequency is not suitable for IEEE 802.15.4 communications. A typical binary matrix is shown as follows:

$$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{5.3}$$

5.3.2 Proposed Interference Mitigation Strategy

The difficulty in analysis is that the value “1” only expresses the highest energy level sensed during the sampling period. The result does not record any details of the interfering signal, e.g. the duration of interfering signal transmission, when the interfering signal starts, and when it ends. The high energy level does not mean the remaining part of the sampling period is unsuitable for the victim’s communications. In contrast, in the binary matrix the value “0” shows that no unacceptable energy levels are detected during this sampling period. Such periods can be considered as an “idle slot” existing on the interfering transmitter, and the

detection of “idle slot” is the main objective for the implementation of energy detection.

The length of the sampling period for energy detection depends on the length of the desired packet. For example, if the length of an IEEE 802.15.4 data frame outputted from the PHY layer is 47 bytes, the required sending time is (47*8)/250=1.504 milliseconds. To ensure the detected idle slot is long enough to complete the desired packet transmission, the detection period should be at least twice the required transmitting time. The ratio R of idle slot to interfering period can be obtained as follows:

$$R = idle/(idle+busy) \tag{5.4}$$

where “idle” and “busy” denote the number of idle slots (i.e. “0”s) and busy slots (i.e. “1”s) obtained from the binary matrix. If the ratio is higher than a threshold $R_{Threshold}$, the victim system can assume that the current idle slots are sufficient to enable the completion of data transmission with corresponding packet length. Otherwise, the victim should decrease the packet length and carry out a new energy detection. Since the length of idle slots is determined by the length of desired packets, and the objective of energy detection is to identify suitable communication slots, the pattern of interference and whether it is periodic or random, will not affect the energy detection result. $R_{Threshold}$ is used by the system to make judgment on the ratio of idle slot is a customized value. It expresses the possibility of the occurrence of suitable idle slots. For example, if the detected ratio is 50%, the victim can conclude that on average every one of two desired packets can be sent successfully. The selection of threshold value depends on the application requirements.

The interference mitigation strategy proposed in Chapter 4 is mainly for ensuring a single data packet to be successfully transmitted under the situation of interference. However, the strategy proposed in this chapter is to enable the victim system (i.e. IEEE 802.15.4 system) to locate a suitable packet length used by continuous data transfer for a relatively long period when interference is present.

5.4 Experiments

The tests implemented in this chapter are divided into two aspects: baseline test and evaluation test. The baseline test consists of hardware test and simulation. The purpose of the baseline test is to obtain the performance of IEEE 802.15.4 network communication when it is under 802.11b interference. The evaluation test is used to evaluate if the strategy can help IEEE 802.15.4 devices determine a suitable packet length to improve packet transmission under interference.

5.4.1 Baseline Test

The device deployment of the baseline test is shown in Figure 5.16.

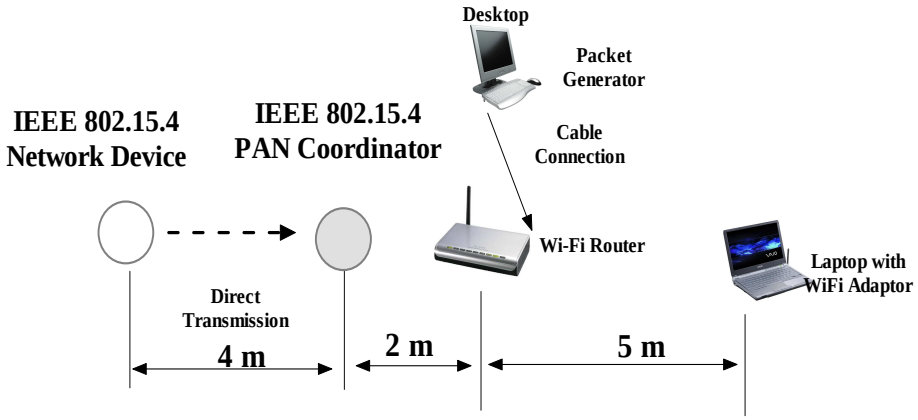

Figure 5.16 Device deployment in baseline test

In Figure 5.16, a desktop is connected to an IEEE 802.11b wireless router using a cable connection. A laptop with an IEEE 802.11b adaptor is located 5 meters away from the wireless router. An IEEE 802.11b packet generator is set to run on the desktop to generate the required 802.11b traffic. The distance between the IEEE 802.11b wireless router and the IEEE 802.15.4 device PAN coordinator is 2 meters. The IEEE 802.15.4 network device continues to send packets to the IEEE 802.15.4 PAN coordinator with different payloads. The amount of packets is determined by the results from baseline test I in Chapter 4, which ensures that the amount of data packets to be processed does not exceed the hardware limitation.

As mentioned in Chapter 3, the physical distance between the victim system and the interfering system can also influence the effect of interference. For example, if the distance between the PAN coordinator and the Wi-Fi router is large than 8 meters (Shin et al. 2007), the degradation of the Wi-Fi transmission power may reduce its interference effect on the transmission of the IEEE 802.15.4 data packet. The distance between the PAN coordinator and wireless router is set as 2 meters sufficiently short enough to enable the Wi-Fi transmission power to corrupt the IEEE 802.15.4 data packets. The wireless router works on IEEE 802.11b channel 4 (2427 MHz). The IEEE 802.15.4 network works on IEEE 802.15.4 channel 15 (2425 MHz).

A simulation using MATLAB was also implemented to make comparison with the baseline test using practical hardware. In the MATLAB simulation, the only opportunity for a successful IEEE 802.15.4 data packet transmission was that the transmission can complete within the interval between two IEEE 802.11b packets under given IEEE802.11b traffic. If the 802.15.4 packet transmission happens when an 802.11b transmission was in process, the 802.15.4 packet reception was thought to be failed. Table 5.3 summarize the result of the baseline test.

In Table 5.3, the column labelled “Wi-Fi Period” means the working period of the 802.11b system in milliseconds. Each 802.11b packet has a fixed packet length of 1024 bytes. For example, if the period is set as 3 milliseconds, the Wi-Fi generator will generate a packet every 3 milliseconds. Using 11 Mbps as a data rate, the Wi-Fi system will be in operation mode for (1024*8)/11000=0.744 (ms), and be quiet for the rest of (3-0.744) =2.256(ms). The column labelled “Wi-Fi Packet rate” corresponds to the value of the 802.11b period with unit of “packet/second”. The column labelled “P” and “S” denote the amount of successfully transmitted IEEE 802.15.4 data in bytes per second in the practical test and the simulation respectively. The first row expresses the different data payload of the IEEE 802.15.4 system varying from 2 bytes to 102 bytes.

Table 5.3 Practical and simulated processing capacity of IEEE 802.15.4 system in baseline test II with 802.11b interference

Packet Payload (Byte)		2	2	12	12	22	22	32	32	42	42	52	52	62	62	72	72	82	82	92	92	102	102
Wi-Fi Period	Wi-Fi Packet Rate	P	S	P	S	P	S	P	S	P	S	P	S	P	S	P	S	P	S	P	S	P	S
<1	>500	171	0	607	0	705	0	873	0	1220	0	1916	0	1959	0	2468	0	2821	0	1243	0	1969	0
2	500	245	272	728	802	797	246	988	0	1220	0	2086	0	2313	0	2407	0	1530	0	1339	0	2009	0
3	333	277	435	872	1894	853	2408	936	2241	932	1552	1984	465	1696	0	1412	0	2632	0	2111	0	2086	0
4	250	523	517	2467	2441	3773	3489	4679	3913	5287	3852	5597	3429	5532	2704	5381	1754	4700	605	4632	0	4278	0
5	200	601	566	2882	2769	4738	4137	4885	4916	7008	5232	7827	5208	8188	4892	8536	4369	8506	3649	8709	2789	8396	1800
6	167	602	599	2982	2987	4737	4570	6118	5585	7022	6152	7878	6394	8213	6350	8564	6071	8559	5679	8815	5115	8720	4423
7	143	645	622	3248	3143	5190	4879	6787	6062	7842	6810	8943	7241	9554	7390	10066	7358	10286	7129	10480	6777	10879	6299
8	125	644	639	3247	3260	5225	5111	6869	6420	7880	7302	8917	7876	9434	8172	10091	8293	10425	8215	10983	8022	10827	7704
9	111	666	653	3414	3351	5509	5291	7219	6699	8487	7685	9633	8371	10401	8779	11026	9020	11488	9061	11902	8991	12078	8798
10	100	680	664	3513	3424	5725	5435	7479	6922	8854	7992	10067	8766	10891	9266	11593	9601	12182	9738	12811	9767	12900	9671

Some of cells in the column labelled “S” have zero values as the required IEEE 802.15.4 packet sending time is longer than the intervals existing in the 802.11b traffic. Consequently, the simulator concludes that the 802.15.4 packet transmission could not succeed. In the practical test, the IEEE 802.11b transmitter may defer channel access if the energy activities of 802.15.4 packet transmission are detected. It is still possible for 802.15.4 systems to complete a few transmissions, even during the periods when 802.11b traffic is high. The results of the practical test are not exactly equal to the results obtained from the simulation test because of the hardware limitation in the practical environment. Both the Wi-Fi and IEEE 802.15.4 systems will defer the medium access upon the detection of the busy medium, which is completely random under such a case. And this procedure is unable to be simulated by the MATLAB simulator. Therefore, it is thought that the practical test results are reasonable as they accord with the trend of the results obtained from the simulation. From Table 5.3, it is clear that most of the survived data packets are those accomplished within the intervals of interfering packet transmission.

5.4.2 Evaluation Test

The evaluation test is designed to evaluate the proposed strategy. Figure 5.17 illustrates the hardware setting

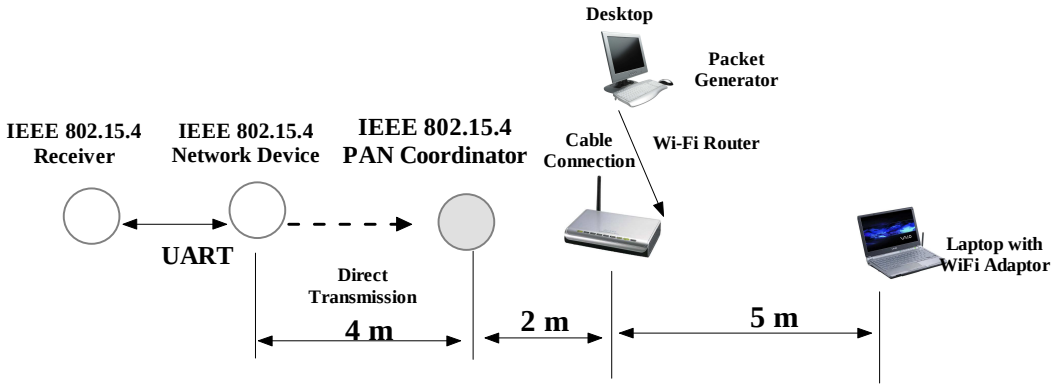

Figure 5.17 Evaluation test setting

In Figure 5.17, the test setting is similar to the hardware deployment in the baseline test. An additional IEEE 802.15.4 device is added. The device is used as

a receiver to implement energy detection when it is requested. The device connects to the 802.15.4 network device using a Universal Asynchronous Receiver/Transmitter (UART) connection.

Initially, the 802.15.4 network device starts to transmit data packets using the maximum data payloads (102 bytes), and acknowledgement is required. After a few seconds, the 802.11b traffic is implemented by the packet generator running on the desktop which connects to the Wi-Fi router.

If the IEEE 802.15.4 transmitter has detected a number of continuous events, which are caused by “no acknowledgement reception” or “CCA failure”, the system will start to implement the designed strategy by asking the 802.15.4 receiver to start energy detection. The centre frequencies of the IEEE 802.15.4 network and the IEEE 802.11b network are set at 2425 MHz (IEEE 802.15.4 channel 15) and 2427 MHz (IEEE 802.11b channel 4) respectively. The detection of the IEEE 802.15.4 receiver on the domain of frequency ranges from 2421 MHz to 2429 MHz, which can cover the whole IEEE 802.15.4 communication channel 15 and part of IEEE 802.11b channel 4.

As described in Section 5.3.1, the energy detection result is a matrix containing energy levels on the specified frequencies during a sampling period. For example, if the effective data payload of the IEEE 802.15.4 packet is 72 bytes, the energy detection sampling period is (72+15)*8*2/250kbps = 5.76 (ms), where 15 denote the length of packet header and 250 kbps is the data rate of the IEEE 802.15.4 system. If the times of energy detection is 10 and current Wi-Fi packet rate is 200packet/second, the energy matrix which can be obtained from the test is as follows:

$$\begin{bmatrix} -74 & -98 & -98 & -98 & -59 & -55 & -98 & -98 & -98 \\ -98 & -72 & -72 & -98 & -98 & -98 & -98 & -53 & -53 \\ -98 & -98 & -98 & -63 & -57 & -98 & -98 & -98 & -98 \\ -74 & -74 & -80 & -98 & -98 & -55 & -55 & -98 & -98 \\ -98 & -98 & -70 & -65 & -98 & -98 & -98 & -53 & -51 \\ -98 & -98 & -98 & -98 & -59 & -55 & -98 & -98 & -98 \\ -74 & -72 & -98 & -98 & -98 & -98 & -53 & -53 & -98 \\ -98 & -98 & -72 & -63 & -98 & -98 & -98 & -98 & -51 \\ -74 & -98 & -98 & -98 & -98 & -55 & -55 & -98 & -98 \\ -98 & -72 & -72 & -98 & -98 & -98 & -98 & -53 & -53 \end{bmatrix} \quad (5.4)$$

Each element in the matrix expresses the maximum energy level detected on the selected frequency during the sampling period in the unit of dBm. The next question is how to select $E_{Threshold}$ to determine if the detected energy level can cause interference on the PAN coordinator. If the required SNR is greater than 5 dB, the threshold $E_{Threshold}$ should be obtained as follows:

$$E_{Threshold} = E_{Receiver} - 5 \text{ (dBm)} \tag{5.5}$$

where $E_{Receiver}$ denotes the energy level of IEEE 802.15.4 signal falling within the bandwidth of PAN coordinator's receiver. If the detected noise energy level is greater than $E_{Threshold}$, it will be thought of as a "busy slot". However, there are two problems which require consideration: the distance between 802.15.4 transmitter and receiver, and the interfering signal's power spectral density.

- Distance between the 802.15.4 transmitter and receiver:

Even in a short-range 802.15.4 wireless communication, the transmitter is unable to know the distance between itself and the receiver. Consequently, the transmitter cannot estimate the actual value of 802.15.4 signal power which arrives on the PAN coordinator's receiver. In addition, the physical position of the IEEE 802.15.4 network device to the wireless router is further than the PAN coordinator in the practical test setting. Therefore the detected energy level is lower than the interference energy level which the PAN coordinator is suffering.

- Interfering signal's power spectral density:

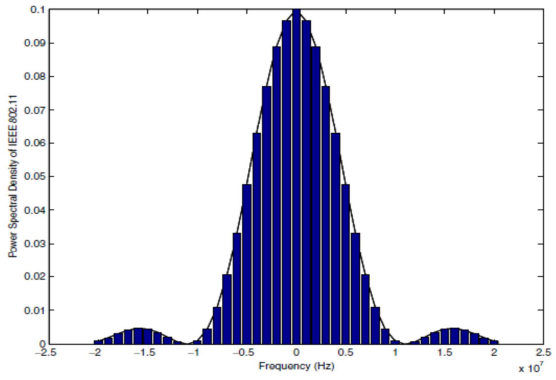

Figure 5.18 IEEE 802.11b power spectral density (Shin et al. 2007).

In Figure 5.18, the IEEE 802.11b signal power concentrates on the centre frequency of the used IEEE 802.11b channel. With the increment or decrement of frequency, the energy gradually attenuates. On the IEEE 802.15.4 transmitter side, the results of energy detection follow the same trend. Then the energy levels detected on different frequency will be different, although they express the same 802.11b signal.

The conservative way to set $E_{Threshold}$ is to use the minimum receiver sensitivity. It can be ensured that if any energy level detected on a channel is less than the minimum receiver sensitivity, the IEEE 802.15.4 communication can successfully be achieved. Therefore, the energy threshold $E_{Threshold}$ used in the evaluation test is set at -92dBm as it is the minimum receiver sensitivity specified in the used hardware manual. Then the energy matrix shown in Equation (5.4) can be converted into the binary matrix illustrated in Equation (5.5).

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix} \quad (5.5)$$

In Equation (5.5), the number of idle slots (zero value) and busy slots obtained from the binary matrix are 56 and 34. Then the ratio of idle slots to all detected slots is 56/ (56+34) =62.2%. If the critical ratio $R_{Threshold}$ was set at 50% (it is a user defined value which can be specified according to actual application requirements), the system can stop attempting to evaluate the interference with other payload lengths. Figure 5.19 illustrates the evaluation test results corresponding to different 802.11b traffic rate.

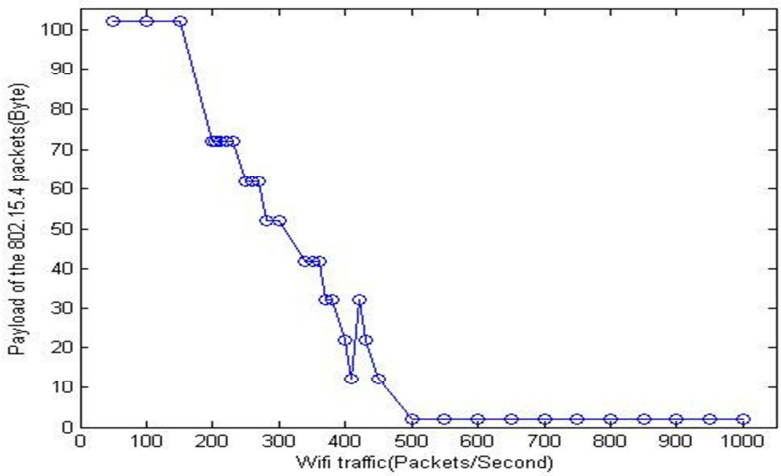

Figure 5.19 Results of the evaluation test

In Figure 5.19, the concluded data payload length given by the strategy increases with the decrement in the Wi-Fi traffic rate. The horizontal axis denotes the different Wi-Fi traffic generated by the wireless router. The vertical axis denotes the concluded payload length suitable for IEEE 802.15.4 packet use under corresponding Wi-Fi traffic. For example, when the Wi-Fi traffic rate is over 500packet/second, there is very little chance for the strategy to locate idle slots. Consequently, the suggested payload length for the IEEE 802.15.4 system is always 2 bytes, with which a higher packet rate can be achieved. When the Wi-Fi traffic is less than 100 packet/second, the 802.15.4 packet can utilize the maximum payload length of 102 byte as the Wi-Fi duty cycle is too low to affect 802.15.4 communications. When the Wi-Fi traffic is between 400 packets/second and 500 packets/second, the idle and busy slots are very difficult to determine because of the hardware limitation. In this situation the payload length suggested from the strategy has a small undulation. In general, if the Wi-Fi traffic rate becomes lower, the suggested 802.15.4 payload length increases accordingly. The reason is that more 802.11b idle periods are available under such situations.

An important note for consideration is that the idle ratio calculated by the proposed strategy is not equal to the Wi-Fi system's idle ratio. For example, the fixed length of a Wi-Fi packet in the evaluation test is 1024 bytes, the required sending time is (1024*8)/11Mbps = 0.74 milliseconds. When the Wi-Fi traffic is fixed at 200 packet/second and its working period is 5 milliseconds, the idle ratio

of Wi-Fi traffic is (5-0.74)/5=85.2%, which is larger than the idle ratio of 62.2% gained from the strategy. The reason is that the calculation in the proposed strategy is used to count the number of idle slots suitable for completing 802.15.4 packet transmission with a given payload length. The idle ratio of Wi-Fi traffic denotes the idle time between 802.11b packet transmissions. However, the idle ratio in the proposed strategy rises proportionately to the Wi-Fi system's idle ratio since the decrement in the Wi-Fi duty-cycle will introduce more idle time.

5.5 Discussion

The use of the proposed strategy is to enable the victim to understand the current interference status. It is clear that the interference existing in a real environment is a dynamic and complex phenomenon. In that case, the strategy is to help the victim make proper adjustments rather than precisely determine the interfering signals' information. For example, according to the 2 bytes suggested payload when the Wi-Fi traffic is over 500 packet/second, the IEEE 802.15.4 system is able to determine whether the interference is too high to enable transmission with large packet size to be successful. Figure 5.20 illustrates the comparisons of packet rates for different IEEE 802.15.4 packet payload lengths when Wi-Fi traffic is 500 packet/second. The values come from Table 5.3.

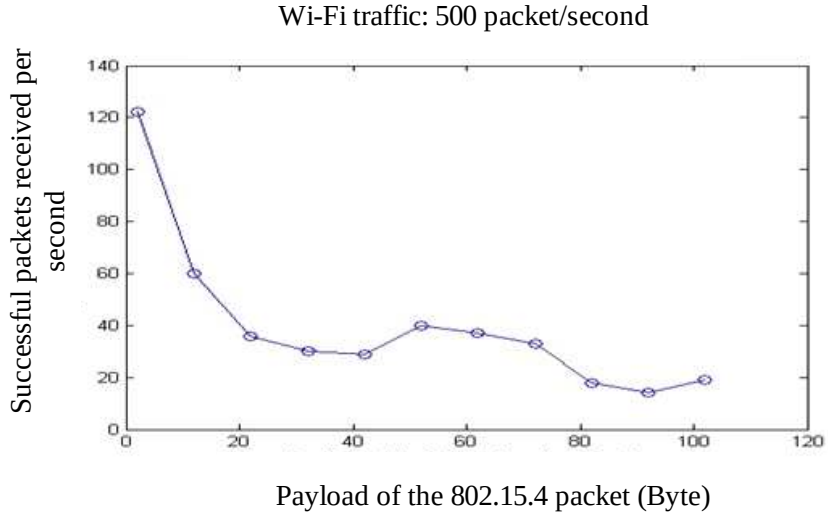

Figure 5.20 Packet rate of IEEE 802.15.4 system under Wi-Fi traffic (500 packets/second)

In Figure 5.20, the number of successfully received packet corresponding to short payload length is obviously higher than the packet with long payload within an unit time. On the basis of this trend, the IEEE 802.15.4 system can choose a short payload for each packet to maintain a high connection rate when serious interference is detected. Since the values used in Figure 5.20 are derived from the practical test, a small undulation (where payload length is between 40 bytes and 80 bytes) could be caused by the hardware limitations. This will be investigated in the future work.

If the Wi-Fi traffic is relative low, e.g. 200packet/second, the throughputs for packets with different payloads are considerably different. Figure 5.21 gives the graphic illustration of Table 5.3.

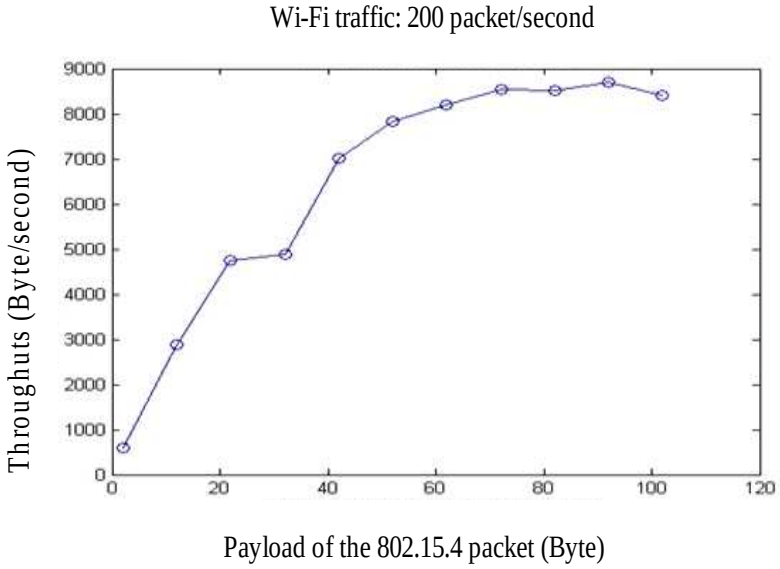

Figure 5.21 Throughputs of IEEE 802.15.4 system when Wi-Fi traffic is 200packet/second (refer to Table 5.3)

In Figure 5.21, the throughputs of packets with payload length which range from 52 to 102 bytes are similar. The throughputs for those packets with 2, 12 and 22 bytes payload length are quite low. If the IEEE 802.15.4 system can make dynamic adjustments by regularly implementing the strategy to monitor the interference status change, it can have a chance to increase the throughput once the level of interference decreases.

The disadvantage for using the proposed interference mitigation strategy is the difficulty of determining parameters. Due to the energy detection implemented on the side of the transmitter in communications, the key parameters of energy threshold $E_{Threshold}$ and idle ratio $R_{Threshold}$ are difficult to determine. For example, if the IEEE 802.15.4 signal falling within the bandwidth of receiver is -50dBm which could be achieved when the physical distance between 802.15.4 devices is short, the receiver should be able to tolerate noise whose energy level is less than -50dBm-(5dB)=-55dBm. With the conservative setting, using minimum receiver sensitivity (-92dBm in evaluation test), the interference energy level judgment will be over-restricted. When the strategy is applied for practical situations, systems can employ other ways to achieve information exchanges on both transmitter and receiver (e.g. a wireless mouse adaptor can regularly send information containing the received signal strength back to the wireless mouse). The selection of $R_{Threshold}$ is highly dependent on the application requirements. The application should decide a certain $R_{Threshold}$ to ensure the concluded payload length is suitable for system performance under interference.

Although the implementation of energy detection requires additional time consumption, it is unavoidable when a wireless communication system is under interference.

5.6 Summary

The proposed strategy in this chapter can be used as a complementary measure for IEEE 802.15.4 based WSN to mitigate the effect of interference. With the help of energy detection, the victim could locate the interval between two consecutive interfering signals and briefly estimate the pattern of interference generation. The means of enabling the desired packet transmissions within the interferer's idle slots can effectively increase a data packet transmission chance. Particularly, the proposed strategy gives the systems facing similar situations guidance on how to dynamically adjust transmission parameters when interference occurs. The strategy is flexible and achievable on existing hardware since it is purely a software solution.

Chapter 6 Reliable Multi-Hop Transmission in Ad Hoc WSNs

6.1 Background and Motivation

The deployment of WSNs often involves little or no infrastructure, which allows small, power-efficient, inexpensive solutions to be implemented for a wide range of devices (Gutierrez et al., 2003). For some applications, e.g. forest monitoring, multi-story building monitoring, star network is insufficient to establish an effective coverage area. With the ability to allow multiple hops to route message from any devices to any other devices on the network, IEEE 802.15.4 based ad hoc WSNs can be constructed and applied for applications requiring large-scale deployment. Due to the wide popularity of wireless products, it is inevitable that IEEE 802.15.4 devices might be affected by other systems employing different wireless technologies that work on the same 2.4 GHz free frequency band. When planning the design of an IEEE 802.15.4 ad hoc network supporting multi-hop data transmission, special consideration must be given to ensure the reliability of transmission. In this chapter, a strategy is proposed to improve the success rate of multi-hop transmissions under interference and tested in an experimental study. The strategy is achieved by employing a transmission speed control and data recovery mechanism. It can be easily implemented for existing IEEE 802.15.4 based WSNs require large-scale deployment.

6.2 Ad Hoc Network

The ad hoc network is a key factor in the evolution of wireless communications. In ad hoc networks, wireless hosts can communicate with each other. These networks typically consist of equal nodes that communicate over wireless links without central control (Wu and Stojmenovic, 2004). In an ad hoc network, each network device operates not only as a host, but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. If properly configured, an ad hoc network can be dynamically self-organized and self configured, with the devices in the network, and automatically establishing and maintaining mesh connectivity among themselves (Akyildiz et al., 2002).

However, one of the most important challenges in ad hoc networks comes from effectively maintaining reliable communications. The requirement of reliable multi-hop transmission is difficult to achieve due to the impact of interference (Tang et al. 2005). The multi-hop transmission is on the basis of peer-to-peer communications. If one or more communication links on the multi-hop transmission route are affected by interference, the desired data will not reach the destination.

The IEEE 802.15.4 standard supports both simple star network topology and peer-to-peer network topology. The star topology is mainly for applications operating within a short range. The peer-to-peer topology allows any device to communicate with other devices as long as they are in the effective wireless communication range. By adding an intelligent management system and capability for routing messages, devices that are compliant with the IEEE 802.15.4 standard can be used to construct self-organizing and self-healing ad hoc networks on the basis of communication infrastructure provided by the peer-to-peer topology (IEEE Std802.15.4-2003, 2003).

6.3 Multi-Hop Transmission and Interference Model

An ad hoc network applied for large-scale applications usually consists of a number of autonomous network devices. If the destination device of data communication is not within the effective communication range of the source device, the autonomous network devices existing between the destination device and source device can be organized in a certain way that provides service of message relay (i.e. implementation of routing protocol). The IEEE 802.15.4 technique offers peer-to-peer network topology for the use of device-to-device communication protocol in an ad hoc network. The technique of transmitting messages through multiple devices in an ad hoc network is called multi-hop transmission (Gomez et al., 2006).

6.3.1 Multi-Hop Transmission in IEEE 802.15.4 Ad Hoc Network

Under normal circumstances, an IEEE 802.15.4 data packet can be successfully received by the destination device through multi-hop transmission when both of the following two conditions are satisfied:

Condition 1: The route from the source device to the destination device has been selected.

The backbone of an IEEE 802.15.4 ad hoc network is composed of FFDs which are capable of implementing the complete protocol set. As specified in the IEEE 802.15.4 standard, a FFD can talk to RFDs or other FFDs, whereas an RFD can only talk to an FFD. Since each of the devices in a multi-hop transmission should be capable of establishing a communication link with its previous hop and next hop on the route, RFDs are not suitable to be involved in multi-hop transmission because of the communication limitations.

The selection of a route means some FFDs in the network are chosen and configured to act as intermediate devices. Each intermediate device relays the received data to the next intermediate device till it reaches the destination. The implementation of a routing protocol is normally the responsibility of the network

layer, which is above the IEEE 802.15.4 standard. For simplicity, it is assumed that the route selection has been completed before multi-hop transmission commences in the following sections of this chapter. Figure 6.1 illustrates a typical IEEE 802.15.4 network which is implementing multi-hop transmission.

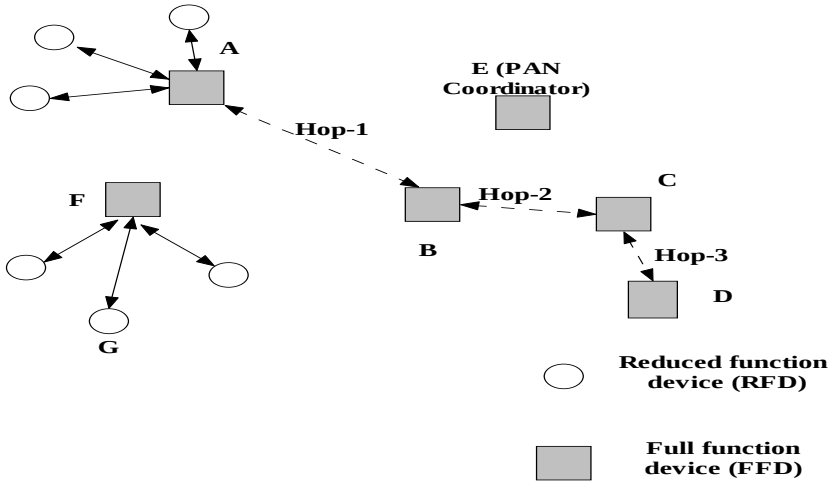

Figure 6.1 An IEEE 802.15.4 network with multi-hop transmission

In Figure 6.1, device E acts as the PAN coordinator responsible for starting an IEEE 802.15.4 network. Each RFD connects to the network by associating with a FFD. Once an RFD successfully joins the network, it can only talk to the FFD with which it associates. For example, device G can communicate with other devices in the network by means of device F, the FFD through which it joins the network. If other devices wish to establish communications with device G, the messages must be first sent to device F, and then relayed to device G. The FFDs in Figure 6.1 form the backbone of the IEEE 802.15.4 ad hoc network. Since a FFD can freely talk to other FFDs, multi-hop transmission can be achieved when the destination device is not within the communication range of the source device. For example, when FFD A is to send data to FFD D, the messages can be sent by travelling through devices B, C, and D, which are indicated in Figure 6.1 by the dotted line. Therefore, three hops are involved to complete the multi-hop transmission. The detail of the hop selection is normally scheduled by the network layer protocol.

Condition 2: Each intermediate device on the route can successfully implement data reception and relay.

The data reception and relay on an intermediate device is the main body of multi-hop transmission. In a non-beacon-enabled IEEE 802.15.4 network, each FFD listens on the selected working channel continuously. Once a data packet is received, the device will check the packet header to determine what action should be taken. If the packet requires relay, the device should find out the network address of the next hop and send the packet out. If there is no interruption existing during the implementation of multi-hop transmission, the data packet will be relayed hop by hop until it reaches the destination. The detailed procedure of sending data from one hop to another hop has been described in Section 4.3.

With the help of multi-hop transmission, data acquisition in an ad hoc network will not be limited by the radio's communication range. It is particularly useful for WSNs to enlarge the coverage area in monitoring applications. However, multi-hop transmission is sensitive to the effect of interference since the communication link failure on any hop can result in failure of the whole transmission.

6.3.2 Interference Model

When an interfering resource is physically located in the vicinity of an IEEE 802.15.4 FFD on the route of multi-hop transmission, it will affect the operation of the IEEE 802.15.4 receiver. From the view of the system level, the interference effect can be expressed as frequent packet losses. Figure 6.2 illustrates the multi-hop transmission being affected by a fixed source of interference.

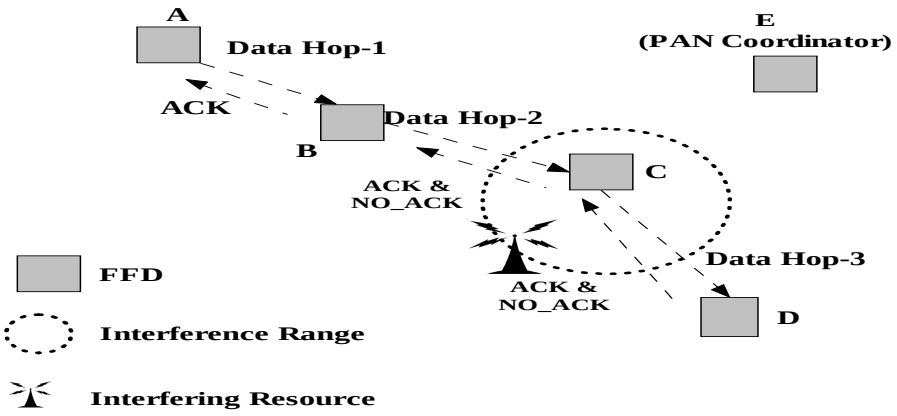

Figure 6.2 Multi-hop transmission affected by interference

In Figure 6.2, the multi-hop data transmission starts from device A to device D. The devices B and C are intermediate devices. Acknowledgement is required to confirm that the data packet is received by the next hop. An interfering resource is located close to device C. Assuming that only device C is affected by the interferer. If the multi-hop transmission is affected by the interfering resource, two situations will occur.

Situation 1: The expected acknowledgements sent from device C to device B are continuously lost, as the data sent from device B to device C are corrupted due to the effect of interference.

Situation 2: The number of acknowledgements sent from device D to device C decreases due to the same reason encountered in situation 1.

The main concern comes from situation 1. When the data are sent from device A to device B, the reception of acknowledgements is normal because device B is not affected by the interfering resource. If the acknowledgements are received, device A will clean the data from its buffer. When the data are relayed from device B to device C, the interference makes the data reception on the receiver of device C prone to failure. As the responsibility of device B in the multi-hop transmission is to relay message rather than processing, it will discard the unacknowledged data if there is no action specified. In such cases, it will be impossible to recover the data since the source device A has no copy left.

Figure 6.3 abstracts the situation of multi-hop transmission in an IEEE 802.15.4 ad hoc network when part of the selected route is affected by interference.

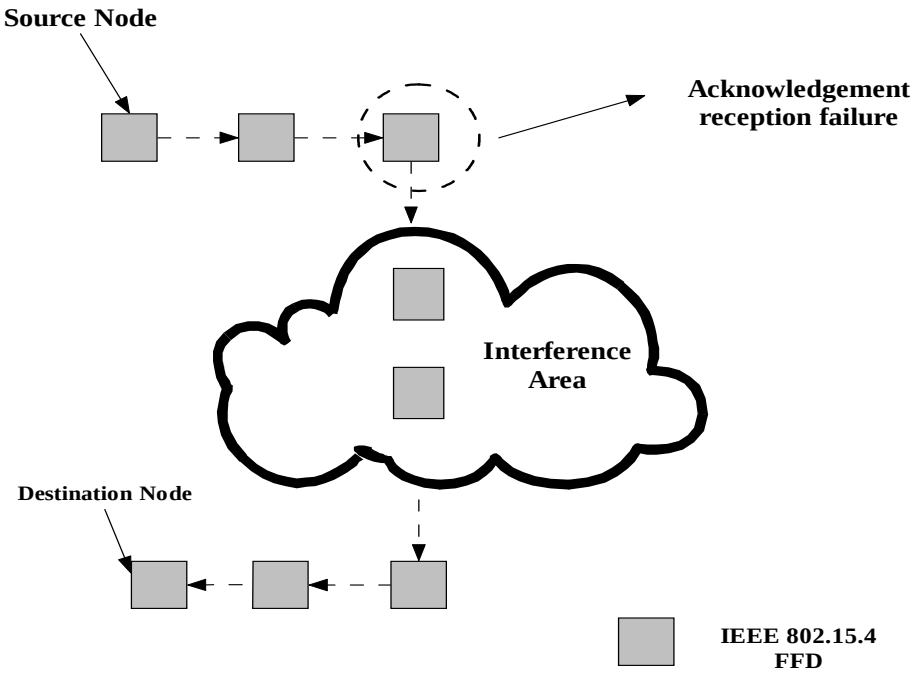

Figure 6.3 Interference model for IEEE 802.15.4 multi-hop transmission

In Figure 6.3, the affected intermediate nodes in the multi-hop transmission can be concluded into a special area, called “Interference Area”. When the “Interference Area” emerges, the acknowledgement receptions on the intermediate device which is one hop before the interference area will considerably decrease. Under such a circumstance, if the unacknowledged data can be temporally held on the intermediate device, and wait to be retrieved by other devices through a “secure” route not affected by interference, a reliable multi-hop transmission will be achieved. If multiple areas of interference exist in a practical network, the one which is the closest to the source device on the multi-hop transmission route will be taken into consideration since it is the first point from which data transmission becomes unstable.

6.4 Reliable Multi-Hop Data Transmission

Achieving reliable multi-hop data transmission in an IEEE 802.15.4 ad-hoc network means the whole transmission progress can be properly controlled and the lost data can, to a certain extent, be recovered.

6.4.1 Multi-Hop Transmission Control

When multi-hop transmission is required in an IEEE 802.15.4 ad hoc network, particularly for large volume data transfers, the setting of the transmission interval is the key point which decides the success of transmission. Compared with the procedures for implementing data transmission between a single pair of devices, multi-hop transmission has more factors to consider. Figure 6.4 illustrates a simplified model of multi-hop transmission.

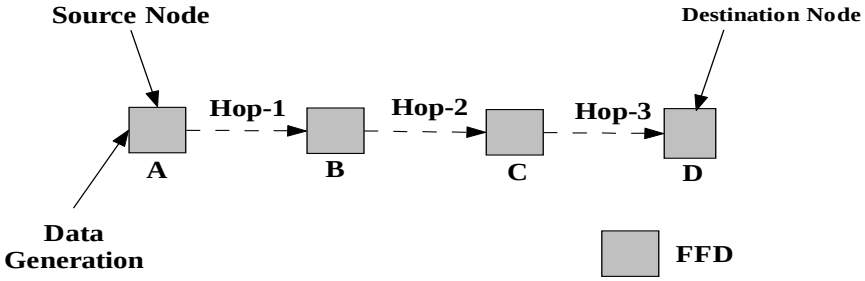

Figure 6.4 Simplified model for multi-hop transmission

In Figure 6.4, the model of multi-hop transmission can be described as a chain from the view of logic. The device A is the source device. The device D is the destination device waiting for data from device A. The metric used to measure the performance of multi-hop transmission is “Arrival Rate (AR)”. The AR expresses the ratio of data that successfully reaches the destination device to the total data sent from the source device.

According to the IEEE 802.15.4 standard, device A should complete three standard steps to ensure that the transmission is successful.

Step 1: Implement CSMA-CA to detect if the channel is clear for data transmission

Step 2: Send data to the next hop.

Step 3: Wait for acknowledgement from the next hop.

Devices B and C acting as intermediate devices on the route require four steps to complete the task of relay.

Step 1: Receive data sent from the previous node on the route, send back acknowledgement if required.

Step 2: Implement CSMA-CA to detect if the channel is clear for data transmission.

Step 3: Send data to the next hop

Step 4: Wait for acknowledgement from the next hop.

The device D, which is the destination device of the multi-hop transmission, needs to receive the data relayed from device C, and send back acknowledgement if required. A description of multi-hop transmission based on the same time line is illustrated in Figure 6.5.

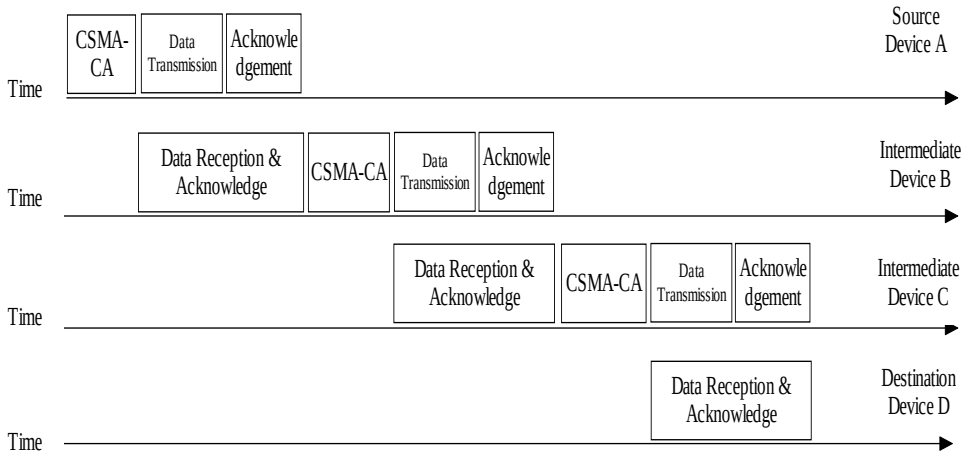

Figure 6.5 Completed multi-hop transmission based on the same time line

Figure 6.5 gives a comparison for actions taken by all involved devices in a multi-hop transmission on the same timeline. Theoretically, if the data have been successfully passed to device C by device B, the source device A can start a new data transmission for the following data packet. However, packet collisions will happen if the transmissions are not well scheduled. Wireless communication has

an important restriction that only one radio transceiver is allowed to emit radio signals within a given period if multiple transceivers exist in the same area (Golmie, 2006). It is well known that the conflict that happens during wireless communications has been concluded as the issues of “hidden node” and “exposed node” (Hwang et al. 2005; Koubaa et al., 2006). The situation in IEEE 802.15.4 ad hoc networks is different. The deployment of an IEEE 802.15.4 network in some application areas might be random, and there is no rule to follow. For example, an environment monitoring application needs the wireless devices to be located relatively close to each other in order to produce an effective monitoring area. Although the IEEE 802.15.4 standard specifies that the communication range for 802.15.4 devices is within 10 meters, the performance of actual products is far better than this limitation. For instance, the Jennic platform compliant with the IEEE 802.15.4 standard can provide typical receiver sensitivity at -96dBm, which can achieve effective communication range over distances of up to 50 meters within an indoor environment (Jennic Press Information, 2009). In addition, to ensure the reliable connectivity in the mesh network, it is unlikely to place adjacent devices in a 50 meter distance. In other words, routing protocols usually take various factors into consideration in the route selection, e.g. signal strength, device response time delay, the distance from the candidate to the destination device. Therefore, it is possible that intermediate devices selected for a route are within the same communication range from each other. In this chapter, the study focuses on the worst-case scenario in which all FFD devices involved in a multi-hop transmission are within a 1-hop communication range. Figure 6.6 illustrates an example IEEE 802.15.4 network deployment under the worst conditions.

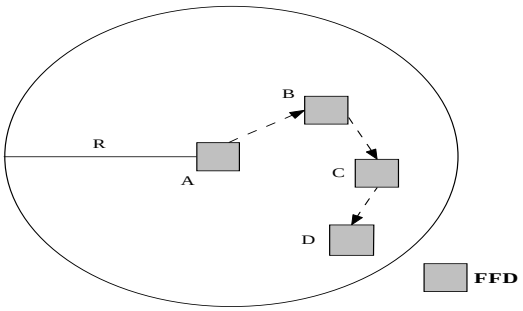

Figure 6.6 Deployment of IEEE 802.15.4 network under worst condition

In Figure 6.6, the radio communications range of device A covers a circle with the centre point of A, and the effective communication radius is R. The intermediate devices B, C and the destination device D are all within the range of this circle. By following the same process in Figure 6.5, if device A starts to send the second packet, whilst the first packet is being transferred from device C to the destination device D, it is possible that both of these two packet transmissions will fail in the worst case. Figure 6.7 shows the collision occurring under this circumstance.

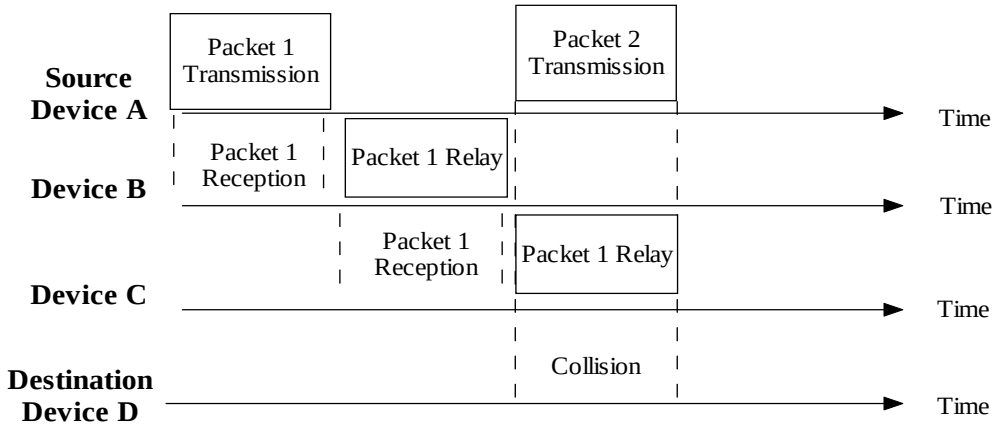

Figure 6.7 Packet collisions in multi-hop transmission

In Figure 6.7, the source device A starts to transmit packet 2 at the time point where device B has completed packet 1 relay. Since all devices are in the effective communication range with each other, it is possible for the transmission of packet 2 sent by the source device A to collide with packet 1 when the packet 1is being relayed from device C to the destination device D. Another possible case is that the action “Packet 1 Relay” starting from device B to device C and the action “Packet 2 Transmission” will cause channel contention. Then one of them should defer channel access and wait for a random delay before making the next attempt. If the transmission interval is not controlled properly on the source device A (e.g. interval is too small), the following packet transmission could cause a greater delay. The default retransmission mechanism for the IEEE 802.15.4 standard is less effective under such circumstance as it is implemented for the scenario where an expected acknowledgement is not received after data transmission. If more intermediate devices are involved in multi-hop transmission,

the collision and channel contention will be more complicated and unpredictable. The uncertainty of multi-hop transmission must be considered in the transmission protocol design.

To ensure the success of multi-hop transmission, the source device should control the interval between each packet transmission at a minimum level which should be equal to the time required by a packet travelling from the source device to the destination device. If the subsequent data transmission starts after the reception of previous data on the destination device, there will be little chance for collision and channel contention. The minimal interval is defined as follows

$$T_{MinimumInterval} = T_{Total}(L) * N_{Hops} \tag{6.1}$$

where $T_{Total}(L)$ from Equation (4.13) denotes the time consumed to send an L bytes packet from one device to another device in a single hop transmission. The N_{Hops} means the number of hops involved in the multi-hop transmission. By cooperating with the upper layers (e.g. the network layer and the application layer), it is easy for the MAC layer to set the minimum interval between each two consecutive source packets.

6.4.2 Hardware Based Data Recovery

One of the purposes of this research is to design a feasible data recovery strategy for an IEEE 802.15.4 ad-hoc network, in a situation where some of the data packets have been lost during multi-hop transmissions due to interference. Unlike the normal strategies which utilize the specified software algorithm to recover the data, the data recovery strategy mentioned in this thesis is hardware based, which focuses on the recovery of the lost data due to commination failure.

If interference occurs, the device whose physical location is one hop away from the interference area will be the first device to sense the situation change. If the desired packet has been successfully sent out by the device in front of the interference area, the next hop located within the interference area could have failed on packet reception. Consequently, no acknowledgement will be issued. Because of the half-duplex transceiver design, the IEEE 802.15.4 PHY layer is unable to detect whether the transmitted packet is corrupted or not.

The frequent indication of “NO_ACK” is the useful symbol for the system to judge if interference exists. When the primitive of “NO_ACK” is issued from a MAC layer on an intermediate device, its MAC layer should decide how to deal with the unsuccessful packets. Normally the MAC layer can have three options: simply discard the packet, attempt to retransmit, or request a higher layer to discover a new route and then attempt to retransmit.

Discard packet: Although discarding unsuccessful packets is the easiest way for the MAC layer to deal with such situations, if the content contained in the packet is important, the system will lose the chance to implement data recovery.

Attempt to retransmit: Since the primitive of “NO_ACK” is issued due to the failure to receive the expected acknowledgement frames, the success of retransmission is not assured. More importantly repeating the transmission of a packet during a period of multi-hop transmission might block subsequent packets.

Request higher layer interruption: Route discovery is normally performed by the source device rather than the intermediate devices employed on the route. If one of the intermediate devices can issue route discovery requests once a transmission problem is detected, the whole transmission would encounter considerable delay. Since the main function of the IEEE 802.15.4 MAC layer is to implement medium access and achieve peer to peer communications, the network layer on the source device should make the decision for new route discovery.

As discussed above the three options cannot achieve data recovery if they are implemented independently. Consequently, an adaptive speed control with a data recovery strategy working on the IEEE 802.15.4 MAC layer to provide reliable multi-hop transmission is proposed here. To make the lost packets recoverable and limit the used method to frequently require interruption from the upper layers, the strategy consists of two steps: slowing down transmission speed and retrieving packets which are not successfully transmitted.

Slow down transmission speed: Once the amount of unacknowledged packets exceeds a defined threshold on an intermediate device, the software running on its MAC layer will store the data packets, and issue a slowing down command to the previous intermediate device from which the unacknowledged data packet is received. This command will be passed back until it reaches the

source device. By slowing down the whole transmission speed, two objectives can be achieved:

1) If some intermediate devices are too busy to send out acknowledgements, the relative low transmission speed can allow more time for the system to handle the necessary processing. It is common for the MAC layer when more automatic retries are needed due to interference. The intermediate devices located within the interference area are often in a difficult situation to receive acknowledgements from the next hop. If the acknowledgements are not received within the defined time period, the system will retry transmission until the maximum retransmission time has been reached. Therefore, the outgoing queue will be occupied. As a consequence, the acknowledgement for the packets received from the previous hop in front of the interference area will be delayed, or even discarded if the queue is full. A low data transmission speed can give each intermediate device on the route more time to process these transactions.

2) If the interference is serious, the action of slowing down transmission speed can help the system reduce the data loss before scheduling a new route, which will subsequently increase the success rate of data recovery.

Retrieve lost packets: Although the intermediate devices can store the unacknowledged data packets in the local memory, the source device should stop using the affected route at an appropriate time point, reschedule a new route, and enable the destination device to request for the lost packets. Upon the establishment of a new route, the source device can inform the destination the number of packets which have been sent out. In comparison with the identification of the received packets on the local memory, the destination device should be able to determine how many packets were actually lost during previous multi-hop transmission, and then enquire the network about the lost packets. Once the intermediate devices on the old route receive the requests, they can send those

packets through an unaffected route. Figure 6.8 depicts the model of the proposed data recovery strategy.

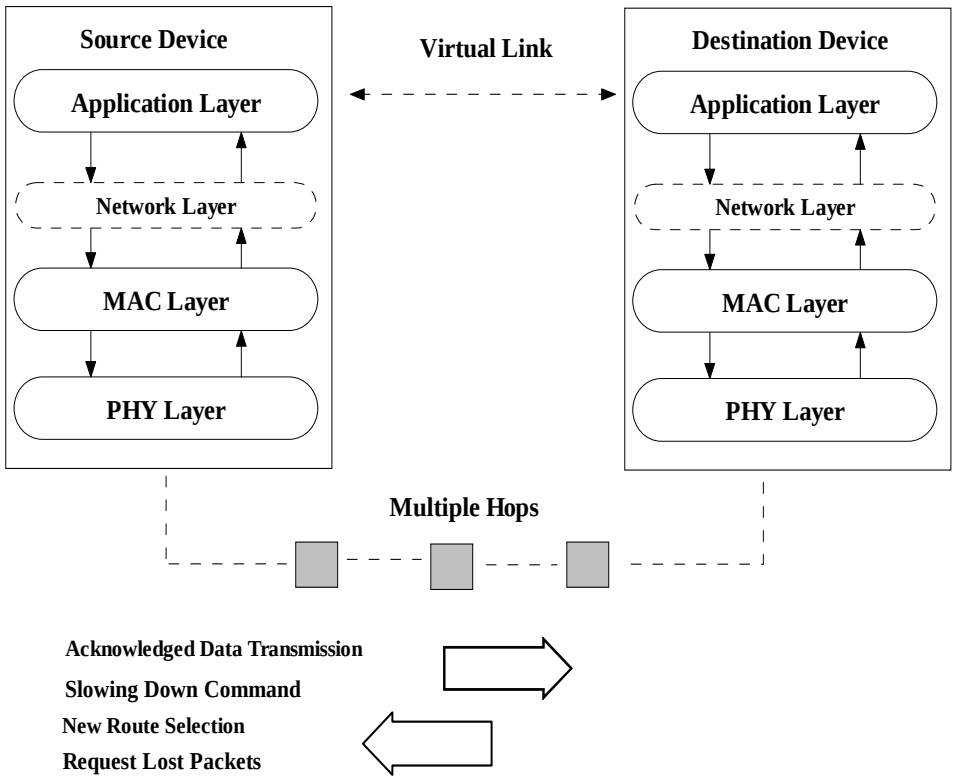

Figure 6.8 Proposed data recovery strategy

In Figure 6.8, the data communications between the source device and the destination device is completed by using multi-hop transmission. A virtual link is created at the application layers on both the source and destination devices. The default MAC layer acknowledgement in the IEEE 802.15.4 standard can indicate to an IEEE 802.15.4 device whether a packet previously sent by it has been successfully received by the next hop. If the network communication employs a multi-hop transmission, the source device will not know if the destination device has received the packet. The virtual link is responsible for helping the source device to monitor if the data packets are successfully delivered by asking the destination device to send an acknowledgement to the source device following the same multi-hop way. Acknowledgements sent by the destination device through the virtual link should be received by the source devices as a regular task to

confirm that a certain number of data packets have been successfully processed. Different from the acknowledgements at the MAC layer, the acknowledgement on the virtual link is based on the application layer, and requires application software to handle the acknowledgements. If a number of virtual link acknowledgements are missed, the source device must decide to reschedule a new route. Although the network layer is not defined in the IEEE 802.15.4 standard, for most applications requiring large-scale deployment, an appropriate network layer is necessary. It is assumed in the following test that the network layer is functional, and the implementation of routing protocol for multi-hop transmission is always available.

There are four types of information exchanging among the intermediate devices, which compose the main body of the proposed strategy:

- Acknowledged Data Transmission: It is used for normal multi-hop data transmission.
- Slowing Down Command: Once the amount of unacknowledged data packets increases, the MAC layer of the intermediate node automatically send out a slowing down command, which will be relayed to the source device. On receipt of the slowing down command, the MAC layer of the source device will increase the time interval for sending data packets.
- New Route Selection. It is implemented by the network layer on the source device when a number of acknowledgements on the virtual link are lost.
- Request Lost Packets. Intermediate devices will store the unacknowledged data packet in a local buffer. When a new route has been scheduled, the source device will inform the destination device how many packets have been sent out. After comparing with local memory, the destination device will send data requests to the network. If the previous intermediate nodes storing these demanded packets receive the requests, they will send the stored data using normal multi-hop data transmission, the route selection will be handled by the network layer on those intermediate devices. The requests sent by the destination device for retrieving the lost data can be handled by the network layer. To make it simple, broadcasting is used as an alternative method. After that, the source device can resume the data

transmission. The system starts the procedures for interference detection and data recovery again.

Except for the necessary support from the network layer, the proposed multi-hop transmission control and data recovery strategy requires no extra resource. The existing IEEE 802.15.4 stack can easily be programmed to achieve the desired purposes. The following tests use a practical IEEE 802.15.4 development kit to evaluate the proposed strategy.

6.5 Experimental Studies

The experimental studies consist of three tests: baseline test, interference test and data recovery test. The baseline test and interference test are mainly for addressing the transmit capability of multi-hop transmission in an IEEE 802.15.4 based ad hoc network with and without the presence of Wi-Fi interference. The data recovery test is designed to evaluate if the proposed strategy can improve the performance of multi-hop transmission by comparing with the results obtained from the baseline test and interference test. All experiments are carried out on the Jennic JN5139R1 platform (JN5139R1, 2009).

6.5.1 Baseline Test: Transmission Control on Multi-Hop Communications

In the analysis of multi-hop transmission, it is mentioned that a minimal interval between each transmission is needed to avoid overloading on intermediate devices. The baseline test is designed to validate if the setting of interval impacts the performance of multi-hop transmission.

- Test Bed Description:

The type of IEEE 802.15.4 devices used in the baseline test is a full function device. The deployment of test devices is illustrated in Figure 6.9.

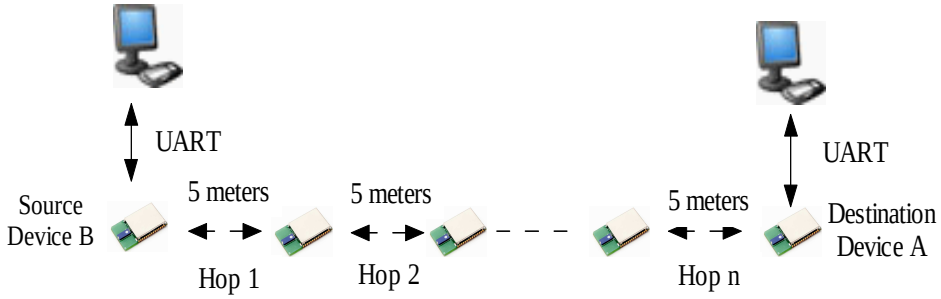

Figure 6.9 Hardware deployments in baseline test

In Figure 6.9, device A is a PAN coordinator responsible for starting an IEEE 802.15.4 network. Device B is the source device, which has data to send to the PAN coordinator. The devices located between device A and B are intermediate devices for relaying data. The transmission route has been manually scheduled and programmed into the intermediate devices. The source device B will send data by following the sequence of hops indicated in Figure 6.9 (Hop 1->Hop2->…->Hop n) until reaching the device A. In this test, the number of hops ranges from 2 to 6 hops. The software running on device A records the number of received data. When the data transmission is completed, device A will calculate how many no repeated data packets have been received. By comparing with the amount of data sent from device B, it is easy to figure out the arrival rate on device A.

To make it convenient for comparison, the payload length of each IEEE 802.15.4 packet is fixed at 50 bytes, which is half of the maximum MAC layer data payload length (*aMaxMACFrameSize = 102 bytes)* defined in the IEEE 802.15.4 standard. According to Equation (4.13), the time used to send a packet from one device to another device is determined as 4.032 milliseconds.

The total amount of data payload sent from device B is fixed at 1 MBytes, which means there will be 20,000 IEEE 802.15.4 data packets sent from device B. Figure 6.10 and 6.11 illustrate the baseline test results.

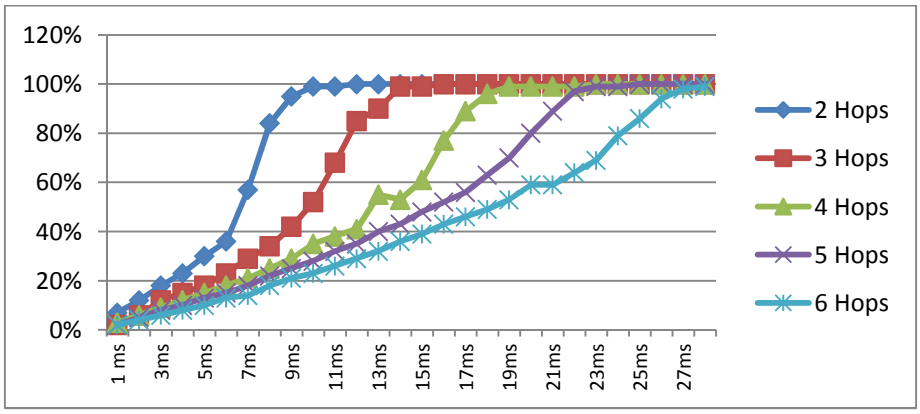

Figure 6.10 Results of baseline test

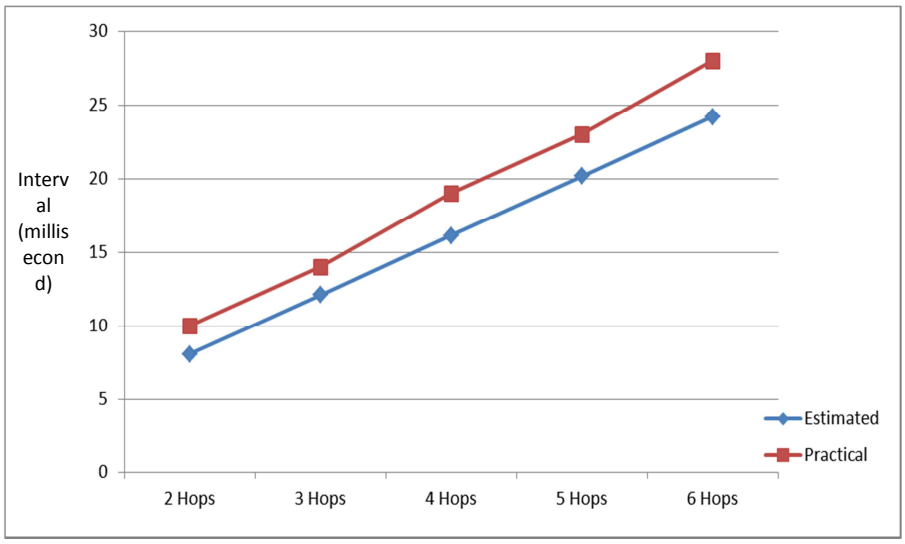

Figure 6.11 Comparison of estimated time intervals and practical results

In Figure 6.10, the horizontal axis expresses the time interval set on the source device for separating data transmission. The vertical axis expresses the corresponding data arrival rate measured on device A. The test result verifies that the arrival rate is obviously related to the number of hops involved in the multi-hop transmission. For example, to achieve a satisfied arrival rate (over 99%) for a 2-hop transmission, the minimal time interval is approximately 10 milliseconds, whereas a multi-hop transmission with 4 hops requires at least 19 milliseconds. It is clear that if more hops are employed in multi-hop data transmission, more time separation should be specified before sending the next data packet on the source device. Figure 6.11 shows the comparison between the analyzed time intervals

estimated according to Equation (6.1) and the practical results from the baseline test where the number of hops varies.

It is particularly important to consider the transmission interval when a large amount of data is needed to be sent to the destination device within a short period. Under this circumstance, the sender needs to arrange the data transmission with suitable interval, rather than continuously sending the packets.

6.5.2 Interference Test

When the parameter of interval between each packet transmission has been properly set, it is reasonable to assume that packet loss which happens during periods of multi-hop transmission is due to the consequence of interference. The interference test is designed to validate the effect of interference on the arrival rate of multi-hop transmissions. In the interference test, an IEEE 802.11b router was located close to one of the intermediate devices, and broadcast IEEE 802.11b signals using a fixed packet rate (e.g. 10packet/second, 100packet/second). During the period of IEEE 802.15.4 multi-hop transmission, every intermediate device recorded the amount of packets they successfully received. By comparing with the total number of packets sent from the source device, it will be clear how the interference affects multi-hop transmission. Figure 6.12 illustrates the hardware deployment in the interference test.

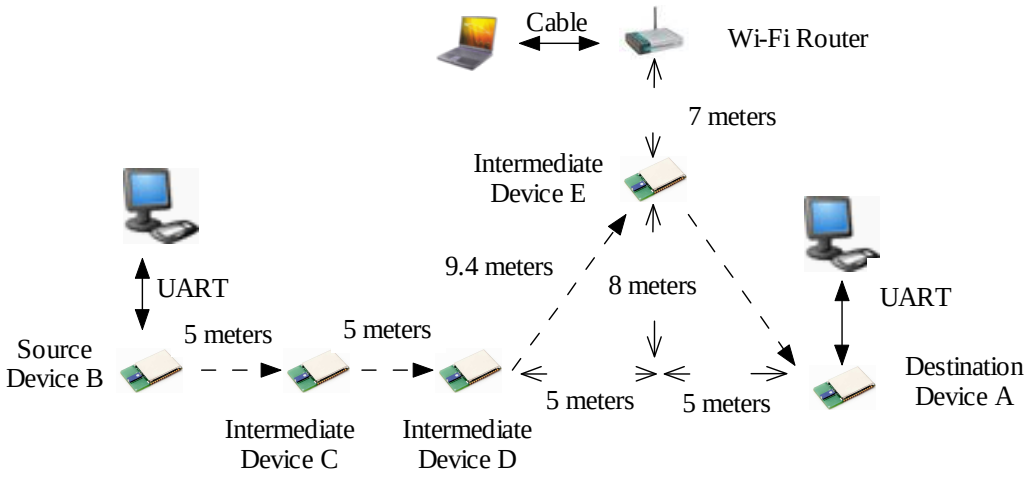

Figure 6.12 Hardware deployment in interference test

In Figure 6.12, an IEEE 802.11b Wi-Fi router working on communication channel 13 (2472 MHz) is connected to a laptop. A dedicated software based packet generator is set to run on the laptop. Due to the fact that the pattern of interference encountered by normal users in daily life has no fixed rules to follow, the packet generator broadcasts IEEE 802.11b signals with fixed rates as an alternative interference pattern to affect device E. During the interference test, the IEEE 802.15.4 ad hoc network uses 4 hops to complete multi-hop data transmission. To enable the wireless interference to take effect, the physical distance between the wireless router and the intermediate device E is 7 metres. The test conditions are: the IEEE 802.11b wireless router broadcasts signals, with the packet rate from 10 packets / second to 600 packets / second. The length of each IEEE 802.11b packet is 1024 Bytes. Four hops are employed by the IEEE 802.15.4 multi-hop transmission. Each IEEE 802.15.4 packet contains 50 bytes data payload. The total number of IEEE 802.15.4 packets sent from the source device is 20,000, the same setting as in the baseline test. The interval between each packet transmission on the source device is 22 milliseconds, which can achieve around 99% arrival rate in the baseline test. In this interference test, the intermediate device E is to be interfered by the IEEE 802.11b router. The IEEE 802.15.4 network works on communication channel 23 (2465 MHz), whose centre frequency is 7 MHz away from the centre frequency of the communication channel used by the IEEE 802.11b router. Figure 6.13 shows the test result from the interference test.

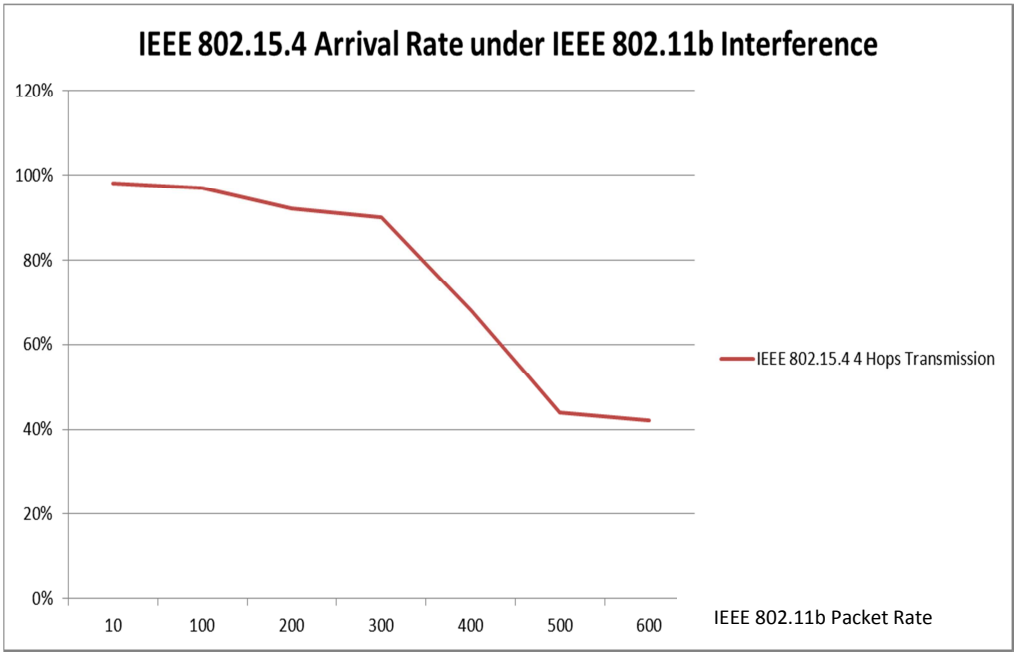

Figure 6.13 Result of interference test

In Figure 6.13, the horizontal axis expresses the IEEE 802.11b data rates generated by the packet generator. The vertical axis expresses the measured arrival rate on the destination device A. The result indicates that the interference coming from the IEEE 802.11b wireless router can cause considerable decrement on the IEEE 802.15.4 ad hoc network arrival rate when the IEEE 802.11b signal is working with a heavy duty-cycle. The number of successfully received data packets on each IEEE 802.15.4 device is recorded in Table 6.1.

Table 6.1 Summary of packet received on each device involved in IEEE 802.15.4 multi-hop transmission

IEEE 802.11b Packet Rate (packet/seconds)	IEEE 802.15.4 Device B (packet)	IEEE 802.15.4 Device C (packet) Arrival Rate	IEEE 802.15.4 Device D (packet) Arrival Rate	IEEE 802.15.4 Device E (packet) Arrival Rate	IEEE 802.15.4 Device A (packet) Arrival Rate
10	20000	19950 (99.75%)	19950 (99.75%)	19690 (98.45%)	19620 (98.1%)
100	20000	19999 (99.99%)	19974 (99.87%)	19798 (98.99%)	19382 (96.91%)
200	20000	19506 (97.53%)	19460 (97.3%)	18605 (93.03%)	18258 (91.29%)
300	20000	19608 (98.04%)	19552 (97.76%)	18331 (91.66%)	17870 (89.35%)
400	20000	19760 (98.8%)	19655 (98.28%)	14412 (72.06%)	13758 (68.79%)
500	20000	19478 (97.39%)	19301 (96.51%)	9810 (49.05%)	8812 (44.06%)
600	20000	19956 (99.78%)	19823 (99.12%)	9497 (47.49%)	8515 (42.58%)

In Table 6.1, the column labelled “IEEE 802.11b packet rate” means the level of traffic generated for the test. The second column “IEEE 802.15.4 Device B (packet)” denotes the number of packets sent from the source device B. Columns labelled “IEEE 802.15.4 Device X Arrival Rate” denote the number of successfully received packets on the measured device (C, D, E, A) and the corresponding arrival rate by comparing with the total packets sent from the source device. All devices except for the source device B are affected by the IEEE 802.11b interference due to its high power output. The number of successfully received data packets on each device decreases in different degrees. In a practical environment, it is unlikely that a 0% packet error rate (PER) will be achieved (Jennic AppNote1035). Usually, most IEEE 802.15.4 applications would be able to tolerate a PER between 1 and 10% if the application level retransmission are employed (Jennic, 2008). Therefore, the packet arrival rate measured on devices C and D are thought to be acceptable. However, it is clear that the obvious decrement starts from device E, which is supposed to be surrounded by the “Interference Area”. The worst situation is observed in the condition when the

wireless router works at 600 packets / second, and the corresponding arrival rate measured on the destination device A is only 42.58%.

If an acknowledgement is required for each transmission, the intermediate device D which is one hop away from the interference area will be the first device sensing the interference. The reason is that device E will send fewer acknowledgements for the packets relayed from device D to device E under the presence of interference.

6.5.3 Data Recovery Test

The data recovery test is implemented by integrating the proposed strategy into IEEE 802.15.4 application software to determine if the system can effectively retrieve the lost packets when interference occurs. The hardware deployment is illustrated in Figure 6.14.

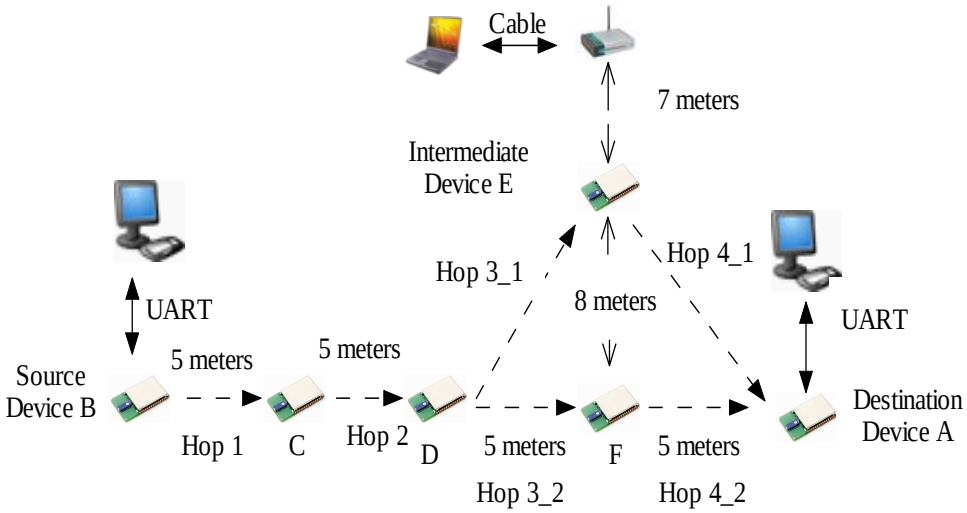

Figure 6.14 Hardware deployments in data recovery test

In Figure 6.14, the experiment device settings are the same as in the interference test except for the intermediate device F. The device F is also an IEEE 802.15.4 FFD device, and programmed to be an alternative to device E. Consequently, two routes are available in this test, Hop1->Hop2->Hop3_1->Hop4_1 and Hop1->Hop2->Hop3_2->Hop4_2. The distance between the wireless router and device F is 8+7=15 meters. If the virtual link between the source device and the destination device is thought to be broken, i.e. a number of

desired virtual link acknowledgements are lost; the source device will switch the route to maintain multi-hop transmission. After changing the hop, the system still needs to sense interference during data transmission. Once interference is detected again, route change and data recovery will be implemented correspondingly. The purpose for such settings is to verify if data recovery can be achieved when route switching is frequent. The settings of the IEEE 802.11b wireless router and the IEEE 802.15.4 network are the same as in interference test. The initial interval between each packet transmission on the source device is still set as 22 milliseconds. Other parameters are listed in Table 6.2.

In Table 6.2, “Initial interval” is used for normal multi-hop transmission. It is also used by the source device each time it has completed a route switch and starts multi-hop transmission. When an intermediate device has detected that the number of unacknowledged packet has reached the threshold (i.e. “MAC layer acknowledgement counter”), it will notify the previous hop to increase the transmission interval. On receipt of the slowing down command, the source will increase the interval as indicated by “Interval increment rate” till the “Maximum interval” has been reached. The “Virtual link acknowledgement set” means the source device puts requirement for virtual link acknowledgement every 20 packets. Then it waits for a “Virtual link waiting period” to confirm whether the acknowledgement from the destination device has been received or not. If a number of virtual link acknowledgements are not received (i.e. “Route switch threshold”), the source device will switch route, and inform the destination device on the new route, how many packets have been sent out. Then the source device waits for a “Waiting period” before resuming multi-hop transmission. Table 6.3 shows the result of data recovery test where the interference intensity varies.

Table 6.2 Parameter setting in data recovery test

Parameter	Value	Description
Initial interval	22 millisecond	Interval for normal multi-hop transmission
Maximum interval	1 second	The maximum interval allowed on the source device
Interval increment rate	2	The ratio for increasing interval when the source device is notified by intermediate devices
MAC layer acknowledgement counter	10 packet	For an intermediate device, if the number of consecutive unacknowledged packet has been 10, it will notify the previous hop in order to reduce interval, i.e. slow down the transmission
Virtual link acknowledgement set	20 packet	The source device sets an virtual link acknowledgement every 20 packets
Route switch threshold	3	If 3 consecutive virtual link acknowledgements are lost, the source device will switch its route
Virtual link waiting period	1 second	If the source device requires virtual link acknowledgement, it will wait for 1 second to check if acknowledgement is received
Buffer size	50	The maximum number of unacknowledged packets which can be stored on an intermediate device
Waiting period	3 second	The period for the source device to wait before resuming multi-hop transmission on a new route.

Table 6.3 Results of data recovery test

IEEE 802.11b Packet Rate (packets/second)	IEEE 802.15.4 Arrival Rate (without recovery strategy)	IEEE 802.15.4 Arrival Rate (with recovery strategy)	Recovery Rate
10	98%	98%	0%
100	97%	98%	1%
200	91%	97%	6%
300	89%	98%	9%
400	69%	95%	26%
500	44%	86%	42%
600	43%	82%	39%

In Table 6.3, the column “IEEE 802.11b Packet Rate” means the traffic made by the wireless router in order to generate interference. The column “IEEE 802.15.4 Arrival Rate (without recovery strategy)” means the measured packet arrival rate on the destination device A without using the proposed strategy. The values in this row are obtained from the previous interference test. The column “IEEE 802.15.4 Arrival Rate (with recovery strategy)” means the measured IEEE 802.15.4 packet arrival rate on the destination device A when the proposed strategy is used to enable data recovery. The column labelled “Recovery Rate” denotes the increment of data arrival rate by comparing the second and the third columns in Table 6.3. The proposed recovery strategy has less effect when the IEEE 802.11b packet rate is less than 200 packets / second. The reason is that the duty-cycle of the interference signal is relatively low which would not cause serious interference on the IEEE 802.15.4 network communications. When the packet rate of IEEE 802.11b signal is higher than 200 packets / second, the chance for the IEEE 802.11b signal to interfere with the IEEE 802.15.4 receiver increases. By using our strategy, the final arrival rates measured on the destination device arise to varying levels compared with the results of the previous

interference test. The maximum recovery rate (42%) is measured when IEEE 802.11b packet rate is 500 packet/second.

6.5.4 Discussion

Similar work carried out by Won et al. (2005) has been mentioned in the literature review in Chapter 3. In their work, the authors proposed that devices located within the interference area could temporarily change their communication channel once interference is detected. Since these devices cannot talk to other devices working on the previous communication channel, some special devices located around the interference area will frequently switch channel to exchange data for the devices affected and unaffected by interference. The measured success rate is between 97% and 86%, which is close to the success rate achieved in this work. However, it should be noticed that the IEEE 802.15.4 packet transmission rate employed by Won et al. (2005) is 1 packet / second, which is far slower than the rate used in our test, and their work was mainly on the basis of software simulation (i.e. NS2 simulator). Our strategy is more suitable for large volume data transmission required in a short period. The effeteness of the proposed strategy is verified by the hardware based experiment tests.

The performance of the data recovery strategy depends on many factors, which can be categorised into four aspects:

1. The range of interference area. In Section 6.3, the interference is assumed to affect some of the links existing on the IEEE 802.15.4 multi-hop transmission. If all communication links of IEEE 802.15.4 networks are being interfered with, multiple intermediate devices will try to store the unacknowledged data packets, and attempt to send these packets when the destination device requests. Consequently, unexpected collisions between these IEEE 802.15.4 devices will happen. As we have observed from the interference test, all of the intermediate devices are affected by the wireless router more or less. However, if a wide IEEE 802.15.4 network

deployment is applicable, the routing protocol running on the source device could find a new route to avoid the interference area.

2. Local buffer management. For intermediate devices which first sense the interference, the system may not be able to provide enough space to store the unacknowledged packets due to limited resource. In the data recovery test, each intermediate device is allowed to store up to 50 unacknowledged packets. In the data recovery test, if the local buffer is full, the new generated packets will simply be discarded. The buffer will be empty when the stored packets are retrieved by the destination device.
3. Redundant device searching. In the data recovery test, if the destination device is informed by the source device that some packets were lost, it will broadcast a data request command to the network. It is known that broadcasting to the network is normally not efficient, and probably causes more network collisions. If the intermediate devices holding the required data do not receive the requests, data recovery will fail. Since the IEEE 802.15.4 standard does not specify the use of a routing protocol, it is difficult effectively to complete this task on the MAC layer. However, if the routing protocol is integrated into an IEEE 802.15.4 based application, the destination device can locate the address of the intermediate devices on the previous route, and send date recovery requests to those devices on purpose.
4. Network deployment and data transmission setting. In the data recovery test, the interfering resource and IEEE 802.15.4 devices are deployed manually to meet test requirements (e.g. radio frequency separation, interference area range). The settings used in practical situations are usually full of uncertainty. Then the parameters listed in Table 6.2 should be adjusted accordingly. The data setting (i.e. 22 milliseconds interval, 1 MByte data capacity) in the test is set for the typical case. The IEEE 802.15.4 technique is not designed for high speed data transmission. Therefore, in practice a longer interval could be employed (e.g. a regular data packet required every 1 second). The objective of the test is to evaluate and demonstrate the proposed strategy when the system is experiencing a worst-case scenario.

At this point, the proposed strategy is suitable to work with the existing IEEE 802.15.4 stack as a supplementary mechanism to enhance multi-hop transmission reliability. When the strategy is integrated with an advanced network layer, and provided with essential information, e.g. the number of hops and the address of the intermediate devices containing the wanted packets, the success rate of data recovery can be further improved.

6.6 Summary

In this chapter, the process of multi-hop transmission in an IEEE 802.15.4 ad hoc network and the effect of interference on the IEEE 802.15.4 network communication links have been analysed in detail. It is observed from the interference test that once part of the communication link experiences interference, the data arrival rate of the IEEE 802.15.4 multi-hop transmission is affected. Since the failure of multi-hop transmission is normally detectable on the intermediate device close to the “Interference Area”, the proposed strategy fully utilizes the mechanism of acknowledgement provided by the IEEE 802.15.4 standard to sense the occurrence of interference, temporarily store the unacknowledged data, slow down the transmission speed, and help the destination device recover the lost data with best effort, which are also the major contributions of the research in this chapter. According to the results of the data recovery test, the effectiveness of the data recovery strategy was evaluated, and the result is positive. The whole strategy requires no change on the IEEE 802.15.4 standard. Therefore, the integration of our strategy into a practical IEEE 802.15.4 application is technically feasible.

However, the performance of the strategy does have some limitations. For example, the implementation of the strategy requires the involvement of other available intermediate devices unaffected by the interference to create a new route. And more potential issues need further investigation, including buffer management for storing unacknowledged packets, redundancy device searching for data recovery, and energy cost for strategy implementation. The objective of the research is to show that the strategy design is fundamentally feasible. The

future work focuses on the optimization of the strategy according to the requirements of practical applications.

Chapter 7 Application in Home Automation

7.1 Background and Motivation

The interference mitigation strategies proposed in Chapters 4 and 5, including consecutive data transmission and dynamic energy detection have been evaluated in the preliminary tests. However, many uncertain factors, such as system deployment, specific application requirements, should be taken into consideration when these strategies are adopted in a practical application.

An IEEE 802.15.4 based home automation system was developed and implemented as part of a Technology Strategy Board (TSB) funded project called "IndeedNET" (Integration and demonstration of energy efficient dwelling networks) (IndeedNET, 2007). The author was a member of the team responsible for designing and developing the technical part of the system. In particular, the author's contributions are focused on low level hardware driver development (e.g. smart sensors, miniature actuators, and wireless communication), system architecture, and software development. Other members of the IndeedNET team are responsible for hardware manufacturing, security mechanism development and end user interactions. The overall development is reviewed in the following sections that aim to provide a comprehensive understanding of the use of the IEEE 802.15.4 technique in a practical wireless sensor network. Since a home automation system usually employs the star topology to construct the communication network, the interference mitigation design in the IndeedNet

system adopts the strategy of consecutive data transmission proposed in Chapter 4, which is also the contribution 1 of this thesis.

7.2 Home Automation System

The idea of home automation is not a new concept. It has been used in day-to-day life for decades. Home automation consists of comprehensive categories, including environment monitoring, security, energy management, appliance control, and communications (Tidd, 1995). More specifically, the development of a home automation system is to devise a set of intelligent home appliances that can provide an awareness of the users' needs, providing them with a better home life experience (Park et al., 2003).

7.2.1 Existing Home Automation Technologies

There are many existing technologies for promoting the development of a home automation system. The X-10 system, which is achieved on the basis of "Powerline Communication", was developed in the late Seventies. It sends a 120 KHz signal at every zero crossing on a 60 Hz AC line with an effective baud rate of 60. The disadvantages of the X-10 system are relatively slow speed and non-effective noise immunity (Shwehdi and Khan, 1996). A java based home automation system was proposed by Al-Ali and Al-Rousan (2004), which utilizes the powerful Java language to construct communication link between remote users and a local system. However, the internal communications between the home server and home appliances still depend on complicated and high cost wired installation. In the work of Sriskanthan et al. (2002), a Bluetooth based home automation system with a relevant control protocol was proposed. The system includes a Bluetooth host device and several client devices. Both host device and client devices compose a Piconet within which the home automation commands can be exchanged using wireless communication. Considering the cost of the Bluetooth module, multiple device controllers are connected to a Bluetooth client device in order to reduce the number of Bluetooth devices employed. Each device controller can control more than one attached device (AD) using inter-integrated

circuit (I2C) bus. Although the primary communication in such a system can be completed with Bluetooth communication, the connection between home appliances (i.e. AD) is still complicated, and relies on wired installation.

7.2.2 IEEE 802.15.4 Technique in Home Automation

A home automation system usually requires a number of sensors and actuators to construct a communication network. For example, a single temperature sensor can only be sensitive to a small area around itself. Consequently, it is reasonable that more than one sensor is needed to generate a wide and effective monitoring area. Therefore, a low selling price for such application (i.e. home automation system) is crucial (Reinisch et al., 2007). The use of a wired system is becoming less attractive because of its high installation cost, especially when a large number of sensors are to be installed (Callaway et al., 2002).

Wireless home automation systems are becoming popular and moving from early research into practical application (Wheeler, 2007). Without the need to rely on cables as the communication carrier, a wireless network can reduce the installation price and maintenance cost. More importantly, physical location is no longer a restriction. From the view of technology, wireless home automation systems are facing the challenge of providing extremely low power consumption which is needed since frequently replacing batteries for sensor and actuator devices is impractical and uneconomical for domestic users. It is obvious that IEEE 802.11 and Bluetooth techniques are unsuitable for home automation systems due to their high power consumption.

The IEEE 802.15.4 technique originates in response to the need for robust, low-cost and low-power wireless control networks. It is widely supported by semiconductor manufacturers, including Ember, Freescale, Texas Instruments, California Eastern Laboratories (Howell, 2009).

The IndeedNet project selected the Jennic JN5139 (JN5139, 2009) module which is compliant with the IEEE 802.15.4 (2003) standard. Figure 7.1 illustrates a JN5139R1 wireless module.

Figure 7.1 JN5139R1 module

In Figure 7.1, JN5139R1 manufactured by Jennic is a complete system-on-chip (SoC) module which integrates microcontroller, modulation/demodulation module, and antenna into a single small printed circuit board (PCB).The SoC design is quite suitable for applications which do not require radio design as a core objective. The wireless communication module supporting IEEE 802.15.4 standard (2003) has the features of small size, low power consumption (operable with battery with active current at 37mA), and low cost (a minimum production cost can be less than $5) (Jennic Press Information, 2007).

7.2.3 IndeedNET Home Automation System Architecture

The main purpose of the IndeedNET project is to construct a home monitoring and control network in order to control energy consumption for domestic users. Based on this purpose, the system requirements can be classified into two main aspects: low-level hardware design and high level information processing system. The low-level hardware design mainly includes sensors actuators design, and wireless communications between sensors actuators and control unit. The high-level information processing system refers to smart control algorithms which are implemented according to the home environment changes.

The emphasis here is how to achieve reliable communications in such a wireless home automation system. Figure 7.2 illustrates the home automation system architecture designed for the IndeedNET system.

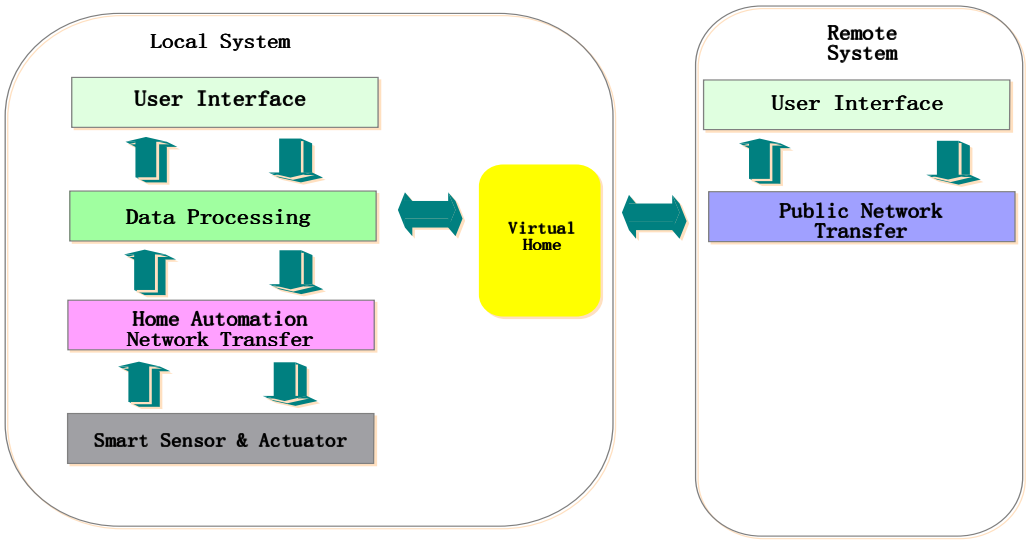

Figure 7.2 System architecture of home automation system (Fang et al., 2008)

In Figure 7.2, the first layer “Smart Sensor & Actuator” is responsible for information acquisition and actuator control. Modern micro-electro-mechanical system (MEMS) technology has accelerated the emergence of low-cost, highly reliable and easy programmable sensors. The benefits offered by such smart sensors include adopting the environmental changes and convenient home status monitoring. The selection of sensors depends on the purpose of the application. In the home environment, temperature, humidity, light level, and gas sensors are the most common types encountered. Many advanced miniature sensors can be powered by batteries that are vital for small sensor module design in a home automation system.

Actuators are the main mechanical parts in the home automation system to execute adjustments on home appliances. In the IndeedNET system, actuators are categorized into two groups: mechanical actuator and electronic actuator. Some home appliances’ adjustments can be achieved by applying mechanical force. For example, a radiator valve is driven by a motor. In addition to the mechanical actuator, some home appliances can be controlled by electronic actuators. A simple example of an electronic actuator is the use of a relay to control a light switch (see Figure 7.3).

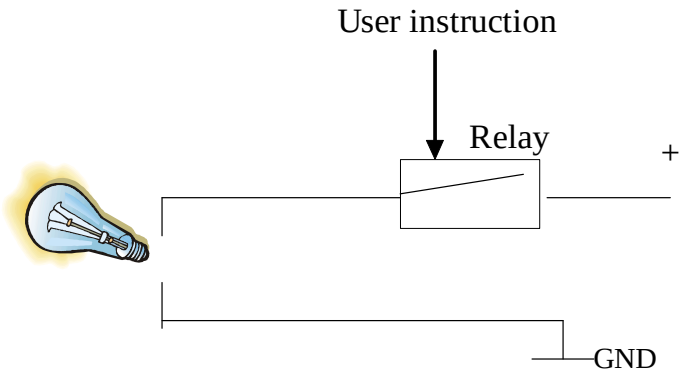

Figure 7.3 A light controlled by a relay

In Figure 7.3, a light is controlled by a relay located on its power circuit. On receipt of user instructions, the relay can execute the actions of switching the light on or off.

The second layer defined in the system architecture is the “Home Automation Network Transfer”. The function of this layer is to connect individual components within the home automation system. A home automation network can be constructed using either wired or wireless connectivity. Some home automation systems employ a wired network. However, the installation and maintenance cost will be higher comparing to a wireless system. In the IndeedNET system, the “Home Automation Network Transfer” layer is achieved wirelessly by the IEEE 802.15.4 technique as it features low power consumption, low installation and maintenance cost.

Upon the receipt of data from the “Home Automation Network Transfer” layer, the designed control algorithm running on the “Data Processing” layer is able to analyze home environment information, make decision for system adjustment, and then send out instructions to the relevant actuators & sensors. Domestic users are also given the capability of manually controlling the home automation system locally and remotely through the “User Interface” layer. The instructions from the remote users can be sent to the local home automation system through any kind of public network (e.g. Internet). Before being implemented in the local system, remote instructions will be first verified by the function of “Virtual Home” to ensure safety & security. (Yang et al., 2006)

In summary, in the architecture shown in Figure 7.1, the “Smart Sensor & Actuator” layer is responsible for sensor reading and actuator driving, the “Home Automation Network Transfer” delivery system instructions or sensor & actuator information to the desired destination. The layers “Data Processing”, “User Interface”, and “Virtual Home” are software relevant. The achievement of “Public Network Transfer” is based on the Internet or other public networks. Among these function layers, the “Home Automation Network Transfer” layer has direct connection with local wireless communications, which might possibly be affected by wireless interference in the home environment. Therefore, the research carried out in this chapter emphasizes the design and implementation of reliable wireless communication for home automation systems.

7.2.4 IndeedNET Home Automation System Components and Test-Bed

As part of the outcome from the IndeedNET project, a set of hardware was produced to complete sensing and adjustment tasks needed by the home automation system. It also offers a practical and complete test bed on which the interference and mitigation strategy evaluation tests could be carried out. The developed components which compose the IndeedNET home automation system are illustrated in Figures 7.4 to 7.10.

Figure 7.4. PAN coordinator

Figure 7.5 Local controller

Figure 7.6 Device with temperature, humidity, and light level sensor

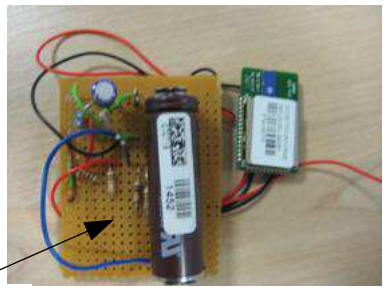

Figure 7.7 Device with carbon monoxide sensor

Figure 7.8 Light switch actuator

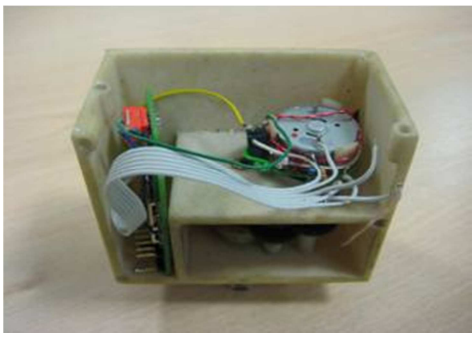

Figure 7.9 Radiator valve actuator

Figure 7.10 Power meter

In Figure 7.4, an IEEE 802.15.4 PAN coordinator with a LCD screen is used to start and maintain the whole wireless home automation network. As the network maintainer must operate without interruption, the PAN coordinator requires main power supply. Another IEEE 802.15.4 module together with some function keyboard and LCD screen is employed as a local controller to facilitate interactions between the home automation system and users (Figure 7.5). It is a battery-driven device. There are two sensor modules designed to execute environment monitoring tasks. One sensor module is equipped with temperature

sensor, light sensor, and humidity sensor (Figure 7.6). Another module is integrated with carbon monoxide sensor for safety monitoring purpose (Figure 7.7). These two sensor modules are also battery driven. A light switch (Figure 7.8) and a radiator valve (Figure 7.9) are developed to demonstrate how the normal home appliances can be adopted into the wireless home automation network. Figure 7.10 shows a power meter used to record the power consumption. Each sensor device or actuator device has an onboard Jennic IEEE 802.15.4 chip, by which the device can easily join the established IEEE 802.15.4 home automation network.

The IndeedNET project is designed to demonstrate wireless sensor/actuator networks for energy saving in a smart home environment. Therefore, periodical sensor reading and actuator status reporting compose the main body of the wireless communication (See Figure 7.11).

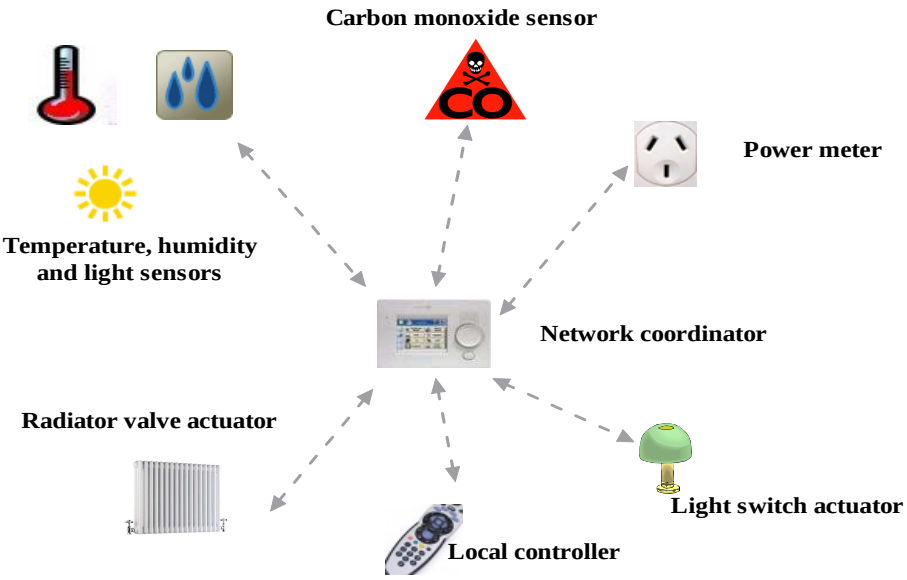

Figure 7.11 IndeedNET home automation network

In Figure 7.11, individual IndeedNET components connect to the network coordinator to construct a star home automation network. Except for the light switch, power meter, and PAN coordinator, other wireless sensor network devices are powered by battery. To conserve energy, the IEEE 802.15.4 modules

connecting to sensors and actuators are set to stay in a sleeping mode for most of time, and wake up to execute the designed task periodically. As a wireless module which is in sleeping mode most of time will not respond to radio communication, the network coordinator cannot directly contact these modules when it is requested. Therefore, the initiative of sending a sensor reading and an actuator status is controlled by the wireless modules. The local controller does not "talk" to a network device due to the same reason that an IEEE 802.15.4 communication module will not respond if it is in a sleeping mode. When a local controller is to request sensor reading, it asks for the PAN coordinator to obtain the latest record sent by the sensor device. If the local controller is to adjust an actuator, the instruction will be stored on the PAN coordinator. The actuator will ask for the PAN coordinator if there is any pending instruction for it when it wakes up. Some actuators are not restricted by power supply such as the light control actuator which is powered by mains power. The IEEE 802.15.4 communication module can share the same power source with the actuators to keep uninterrupted operations. The network coordinator can immediately relay instructions to such actuators. However, to ensure all network devices can follow the same communication rules, both battery and main power driven sensor/actuator devices will send their information to the PAN coordinator for recording. Figure 7.12 illustrates the information flow in the IndeedNET system.

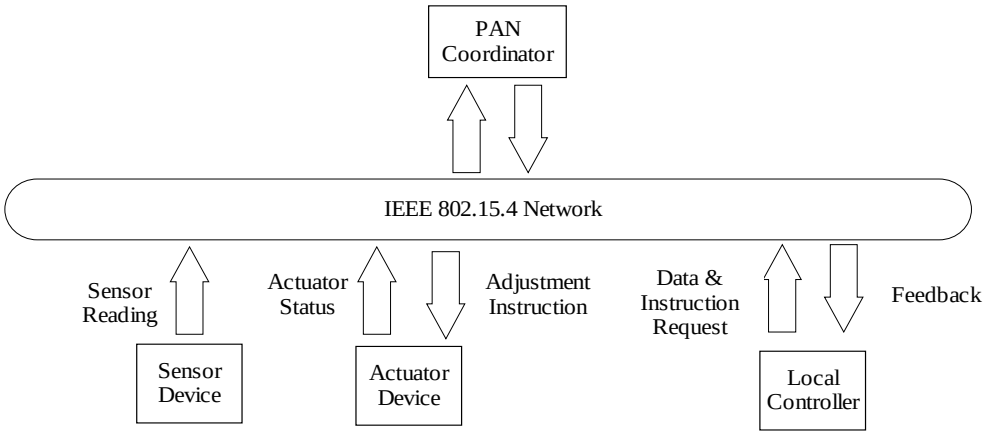

Figure 7.12 Information flow in the IndeedNET home automation network

In Figure 7.12, sensor devices are responsible for sending sensor readings to the PAN coordinator. Actuator devices also send actuator status to the coordinator, whilst they receive instructions sent by the PAN coordinator. The local controller directly sends data & instruction request to the PAN coordinator, and also receives the feedback from the PAN coordinator.

7.2.5 IndeedNET System Specification

The IndeedNET system consists of sensors and actuators used to monitor and control home environment. Table 7.1 summarizes the parameters used to configure sensors and actuators.

Table 7.1 defines the parameters for sensors and actuators. The temperature sensor, ambient light sensor, humidity sensor and carbon monoxide sensor are required to implement sensing task and send sensor readings to the central controller every ten minutes. Additionally, sensors implement self-checking every 1 minute to make sure that environment changes can be properly monitored. The self-checking result will not be sent to the network coordinator unless certain conditions are met (e.g. danger temperature is detected). Since temperature, humidity and light level sensors are integrated on the same wireless module, at least 9 bytes data size are needed for radio transmission.

Table 7.1 IndeedNET system parameters

Sensor & Actuator	Data Size (Byte)	Sampling Period	Description
Temperature Sensor (DS18B20)	3	• 1 minute for self checking • 10 minutes for system checking	• Measures temperature from -55°C to 125 °C • 1 byte for sensor reading • 2 bytes for control command
Ambient Light Sensor (TSL2500)	3	• 1 minute for self checking • 10 minutes for system checking	• Ambient light is divided into 7 levels ranges from 0 to 6 • 1 byte for sensor reading • 2 bytes for control command
Humidity Sensor (SHT11)	3	• 1 minute for self checking • 10 minutes for system checking	• Humidity reading ranges from 0% to 160% • 1 byte for sensor reading • 2 bytes for control command
Carbon monoxide Sensor (TGS5042)	4	• 1 minute for self checking • 10 minutes for system checking	• Sensor reading ranges from 0ppm to 10,000ppm • 2 byte for sensor reading • 2 byte for control command
Lamp Controller	2	• Always on	• 1 byte for lamp status • 1 byte for control command
Radiator Valve Controller	3	• 10 minutes for self adjustment and communication with	• 1 byte for temperature reading • 1 byte for set point

		central controller	• 1 byte for control command
Smart Power Meter	6	• Always on	• 2 byte for current • 2 byte for voltage • 2 byte for accumulated power consumption
Network Coordinator	N/A	• Always on	• Starts network, accepts network device, stores and relays message
Local Controller	N/A	• When requested by users	• Display home information and used by users to send commands

The lamp controller and smart power meter are connected to the main power and will be always on. Consequently their operations do not need to consider power consumption. Another similar component is a network coordinator, which is the PAN coordinator and it is an IEEE 802.15.4 based WSN. It should be connected to the main power to keep working as the message in a star network must be relayed by the network coordinator. The radiator valve controller communicates with the network coordinator to determine if a new set-point is sent by users, then makes adjustment according to the current temperature and set point. Except for the data size listed in Table 7.1 for sensor and actuator operations, more data size for additional settings (e.g. error correction, packet identification, reserved payload for system use, security setting) is also needed. Cosequently, packet transmission in the IndeedNET system takes 50-byte as a standard data size.

7.3 Interference Analysis in Home Automation System

The wireless interference issue has been considered in the development of the IndeedNET system. Most concerns come from the use of IEEE 802.11 devices which are well known as Wi-Fi. During the development period, the effect of

wireless interference was actually noticed. The distinct characteristic of interference phenomena is that the local controller often has a response from the PAN coordinator after a significantly long delay, or even loses a response when a Wi-Fi router is working nearby. The sensor device and actuator device encounter the same problem which is unable to be displayed on the local controller as they communicate with the PAN coordinator directly.

7.3.1 Home Automation Network Topology

An IEEE 802.15.4 star network can cover a typical house as depicted in Figure 7.13.

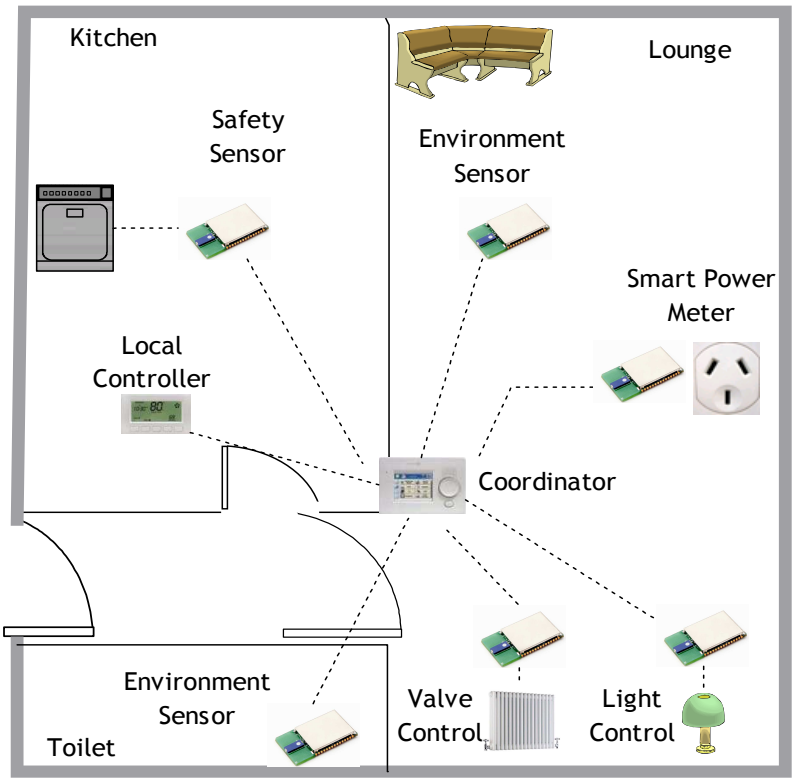

Figure 7.13 Star home automation network

In Figure 7.13, if the PAN coordinator has started and completed network initialization, other IEEE 802.15.4 devices will automatically join the established network by associating with the PAN coordinator. In other words, the individual devices do not need to consider deployment location. This is also the most

important advantage offered by the wireless technique. However, it is possible for these wireless home automation devices to be located in the vicinity of the interference source.

7.3.2 Wi-Fi Interference Source

According to the analysis in Chapter 4, the interfering source which can actually affect IEEE 802.15.4 network is the IEEE 802.11b/g network (i.e. Wi-Fi) working at a high duty cycle. Its relative wide bandwidth and high output power are essential factors causing the interference.

As wireless broadband is quite popular in the consumer market, many households prefer wireless networking as their home Internet access, which means the interference of Wi-Fi to IEEE 802.15.4 wireless sensor networks could be inevitable. Most Internet applications for domestic users work mainly in a downlink mode (e.g. Internet browsing, file downloading). The uplink mode is usually used to send a small number of data for requesting service (e.g. request a web page, or send an email). Consequently, the wireless router is the main interference resource under this situation. Normally, a household will have one wireless router.

There is another serious interferer, domestic wireless security camera, which usually employs the IEEE 802.11b/g technique. Unlike the wireless router connecting to the Internet, the domestic wireless security camera keeps working all the time and it might be requested to send video stream to the central server for monitoring purpose. The continuous IEEE 802.11b/g signal transmissions could continuously generate interference on the IndeedNET system.

7.3.3 Challenge in Home Automation System Installation

One of the challenges of avoiding interference in the home automation system is that the system installation should not impose too many “technical requirements” to users. In a business environment, a wireless system deployment can be done by professional staff and have an advance field test in order to ensure a safe distance between wireless devices. Domestic users are the end users of indeedNET system and most of them are not network experts. They are not likely

to have similar technology and knowledge for a proper radio environment measurement. Therefore, it is unrealistic to require end users to pay attention to deploying wireless network, e.g. where is a safe position unaffected by interference, how to allocate a channel. Consequently, the components of a home automation system might be put at any place in a house, which potentially increase the possibility for the IndeedNET system to be interfered by Wi-Fi.

The physical locations of the IndeedNET system devices are decided by the attached sensors or actuators. For instance, the radiator valve controller must fit on the radiator valve whose location was determined when the house was constructed. The sensor devices can be put anywhere in the house to monitor environment changes and provide the control algorithm running on the PAN coordinator with useful information. Therefore, their position will not be changed after installation. When Wi-Fi interference happens (e.g. Wi-Fi network channel moves to the frequency close to the home automation network channel), applying physical distance separation to avoid interference is usually not applicable. The strategy designed to mitigate interference should emphasise on software adjustment which does not require user interruptions.

7.4 Interference Mitigation Strategy

The interference mitigation strategy designed for the indeedNET system is on the basis of consecutive data transmission proposed in Chapter 4.

7.4.1 Interference Effect

The interference mitigation strategy is designed according to the characteristics of the IndeedNET system. The IndeedNET system is primarily for saving energy consumption for domestic users. Therefore, sensor and actuator devices are required to report the environmental data to the home network coordinator or execute appliance adjustments at a regular interval. To enlarge the lifetime of sensors and actuators, including the connected IEEE 802.15.4 wireless modules, the battery driven IndeedNET components need to keep in a deep sleeping mode in order to reduce power consumption during the period of “off

duty". In other words, battery driven IndeedNET components should keep a relative low duty cycle which can enlarge battery life. Consequently, domestic users do not have to frequently replace a battery. Figure 7.14 shows the state chart of an individual battery driven IndeedNET component.

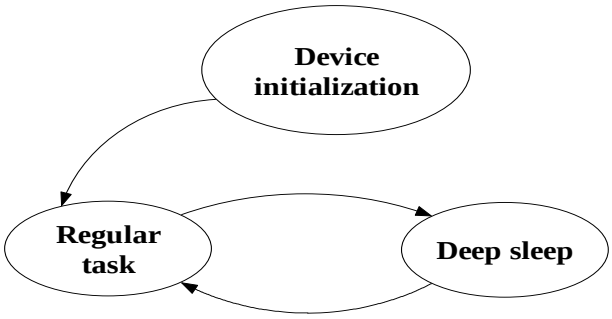

Figure 7.14 State chart of battery driven IndeedNET component

In Figure 7.14, an IndeedNET component starts to implement a regular task after the completion of system initialization. Then it will keep in the deep sleeping mode until the time for the next regular task. During the sleeping mode, the IEEE 802.15.4 module (i.e. transmitter and receiver) is inactive, which makes it completely untouchable from the PAN coordinator. If the PAN coordinator is sensitive to the emergence of interference, it cannot notify those components which are in the sleeping mode.

When the component wakes up from the deep sleeping mode, it will first implement the desired function (sensing task or appliance adjustment) and then report to the PAN coordinator. After that, the component should enter into the sleeping mode again to save energy. If the data transmission to the PAN coordinator failed, the component usually has two options: implement network rejoining procedure by scanning all available channels and then associate with the addressed PAN coordinator, or apply retransmission to make more tries on the current channel.

- Rejoining Network. According to the IEEE 802.15.4 standard, the network device which has lost connection with the PAN coordinator should issue an active scan by sending a beacon request command on a channel. Then the device enables its receiver and records the information contained in each received beacon. The

active scan should terminate on a channel when either condition is satisfied: the number of received PAN information has reached the maximum value (the maximum value is an implementation-specified number decided by manufacturers), or the specified scan period has expired. The definition for specified scan period T_{active_scan} is (IEEE Std802.15.4-2003, 2003):

$$T_{active\_scan} = [aBaseSuperframeDuration * (2^n + 1)] \quad symbols \qquad (7.1)$$

In Equation (7.1), T_{active_scan} is the scan period in the unit of symbol (a symbol is equal to 16 μs), $aBaseSuperframeDuration$ is a constant value equal to the number of symbols (i.e. 960 symbols) forming a superframe when the superframe order is equal to 0, n is a value between 0 and 14. Then $T_{active\_scan} \in [30.72ms, \quad 251673.6ms]$. If the minimum scan period is used (i.e. n=0), the total time consumed to scan all 16 channels on 2.4 GHz ISM band is equal to $30.72*16 = 491.52$ millisecond. Usually, to ensure that the waiting time is long enough to receive PAN information, the scan period n will be set as 3. Then the maximum time consumed to scan all 16 channels will be 2211.84 millisecond. Table 7.2 lists the required time to scan all channels when the exponent n ranges from 0 to 5.

Table 7.2 Time consumption for IEEE 802.15.4 device to scan channels

n	Scan Period for 16 Channels (millisecond)
0	491.52
1	737.28
2	1228.8
3	2211.84
4	4177.92
5	8110.08

In Table 7.2, column lapelled with “n” denotes the exponent in Equation (7.1). The second column is the calculated time consumption for IEEE 802.15.4

device to scan all channels with corresponding *n* value. Obviously, a large value of *n* will lead to a long scan period. Since the current consumption for using IEEE 802.15.4 transmitter and receiver is the same when the communication module is active, a long scan period will consume considerable battery energy.

Energy consumption is the most important metric to measure our strategy. As most of the IndeedNET components implementing sensing and actuator adjustment tasks are powered by batteries, the interference mitigation strategy should consume energy as little as possible.

- Applying retransmission at the application layer: Retransmission is a reasonable way for sensor/actuator devices to take when the expected acknowledgement is not received from the PAN coordinator within a certain time. However, it is difficult to determine an optimized value to be the maximum retransmission time, especially when the system is under interference.

7.4.2 Interference Mitigation Strategy

In Chapter 4, it has been evaluated that utilizing consecutive data transmission can significantly increase the success rate for a pair of IEEE 802.15.4 devices even under serious interference caused by a Wi-Fi transmitter. This strategy is suitable for the design of the IndeedNET system since the communications in the IndeedNET system only occurs between the network controller (i.e. PAN coordinator) and the network device. Additionally, the regular task to collect sensor information or adjust the actuator is needed every few minutes Applying a certain number of data retransmissions will not cause network congestion. A small modification is made in the original strategy proposed in Chapter 4. In the original strategy, an IEEE 802.15.4 device will select a small number as the maximum retransmission time after the first time failure of data transmission. If data retransmissions with the small maximum retransmission limitation still failed, the sender will choose to consecutively transmit data packets for 1 second. In the IndeedNET system, once the fist data transmission from a sensor / actuator device to the PAN coordinator failed, the sender will directly try to continue to send a data packet for 1 second. The interval between consecutive

transmissions is calculated according to the length of data packet. The purpose of modification is to limit the time consumed to implement retransmissions.

In the original strategy, the sensor device will regularly (for example. every 1 second) send a connection detection packet requiring acknowledgement to the PAN coordinator. If a certain number of acknowledgements are lost, the device will start to scan all channels in order to rejoin the network. In the IndeedNET system, the transmission of connection detection packet is not achievable by sensor/actuator devices as its transmitter is in a sleeping mode. To solve the problem, the PAN coordinator in the IndeedNET system sets a timer to monitor the data reception. If the expected data are not recorded during the specified period, the PAN coordinator will initiatively switch network channel to the one with least energy level. Figures 7.15 and 7.16 illustrate the flow charts of the strategies implemented in the IndeedNET system to mitigate interference.

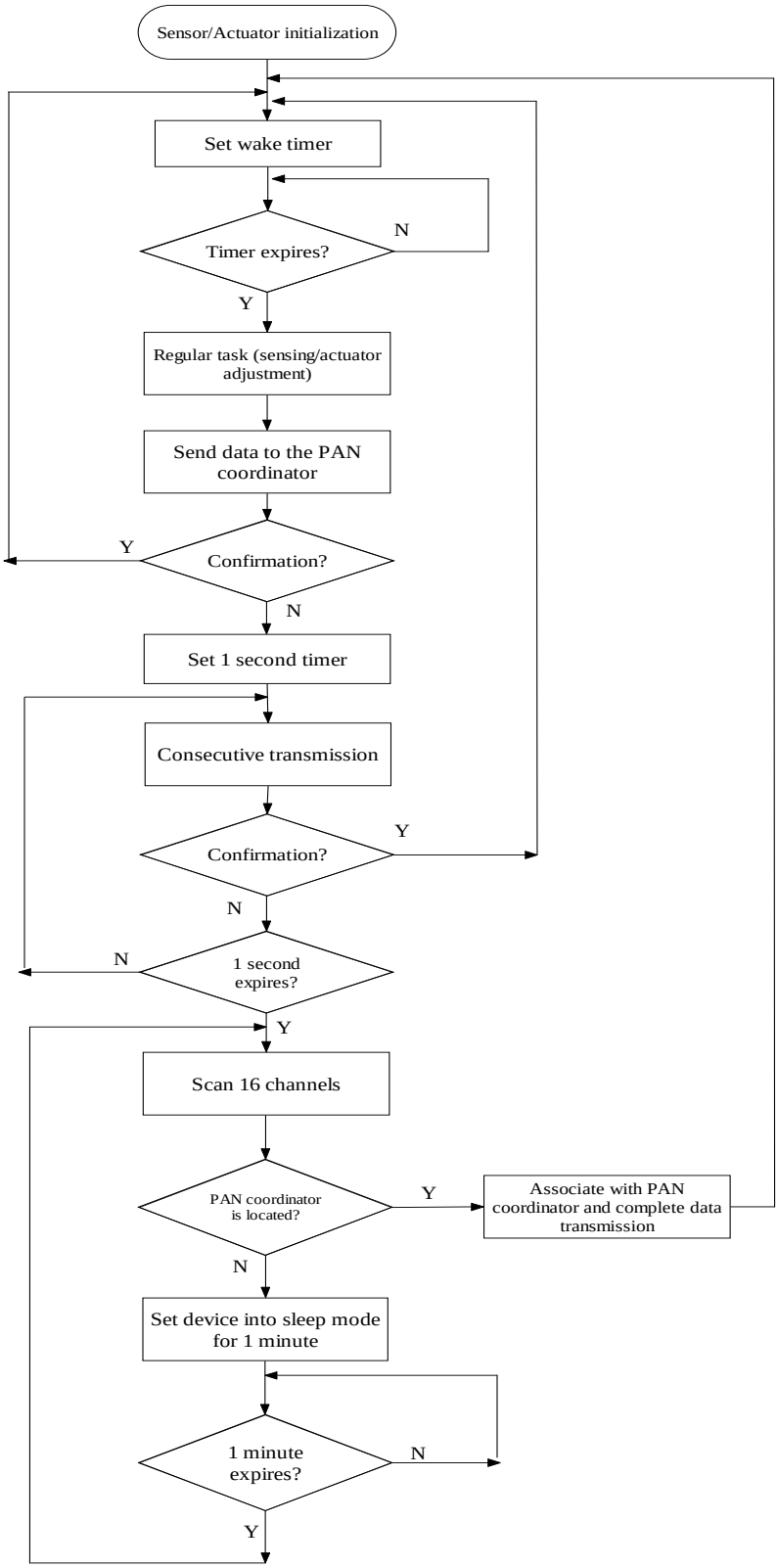

Figure 7.15 Flow chart of interference mitigation strategy implemented on sensor/actuator devices

In Figure 7.15, the workflow of the sensor/actuator device starts from system initialization. After successfully joining the network, the sensor/actuator will implement initial configuration. Then the device enters into the sleeping mode. When the wake timer expires, the device should execute the desired functions, including reading sensors or adjusting the actuator. The result of regular tasks will be sent to the PAN coordinator to make a record. If the confirmation from the PAN coordinator is received, the device can enter into the sleeping mode until the wake timer expires again. If the confirmation is not received, the device starts to send the packet to the PAN coordinator in the way of consecutive transmission. The transmission interval is decided by the length of the packet. For example, in the IndeedNET system, each data packet employs a fixed payload length whose size is 50 byte. According to Equation (4.13), the minimum time used to transmit such a packet is 4.032 millisecond. Therefore, the retransmission interval is 4.032 millisecond. If a confirmation is received from the PAN coordinator within the 1 second retransmission period, the device can stop retransmission and enter into the sleeping mode. If no acknowledgement is received and the 1 second retransmission period expires, the device should start to scan all channels in case the PAN coordinator has switched to other channels. If the PAN coordinator is located, the device should associate with it and complete the data transmission. Otherwise, the device should enter into the sleeping mode for a certain interval in order to save energy (we choose 1 minute here), and then wake up to search for the PAN coordinator. The procedure of “sleep for a short period and then search for PAN coordinator” will be repeated by the sensor/actuator device until it successfully joins the network.

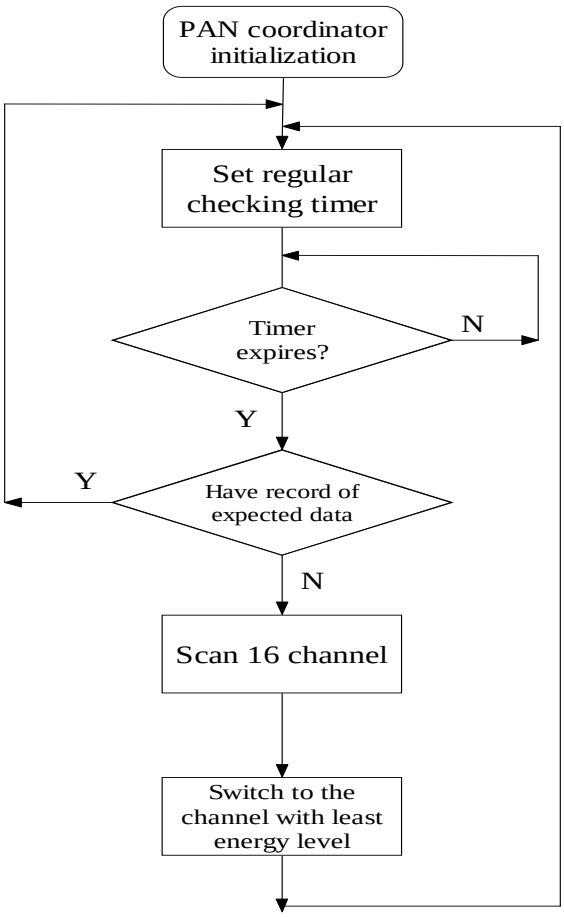

Figure 7.16 Flow chart of interference mitigation strategy implemented on the PAN coordinator

As shown in Figure 7.16, after initial configuration, the PAN coordinator sets a timer which is longer than the sensor/actuator device's working period. For example, if the sensors are required to report to the PAN coordinator every 10 minutes, the timer on the PAN coordinator can be 11 to 12 minutes, which is mainly for allowing errors of the timer running on sensor/actuator devices. When the timer expires, the PAN coordinator will check if expected data from all devices have been recorded during the last working period. If data have been recorded, the PAN coordinator can start the timer again. If some data are lost, the PAN coordinator should implement a channel scan and move the network to a clean channel which has the least energy level. Since sensor/actuator devices will implement the procedure of rejoining network 1 minute after the failure of communicating with the PAN coordinator, the home automation network will re-establish very quickly.

7.5 Evaluation Test

The test was carried out in a test house to evaluate the developed indeedNET system performance under interference. The deployment area is within a detached house locating in Holywell Park, Loughborough University (UK). It is a two-story house with complete home appliance settings. Figure 7.17 illustrates the test house.

Figure 7.17 Test house located in Loughborough University

Since the objective of this thesis is to discuss and study interference in a wireless sensor network, the main objective here is to evaluate the performance of wireless communication in such a home automation network when it is under interference.

7.5.1 Deployment of IndeedNET System in the Test House

The test house is a dedicated property built for research purposes. The Internet access is provided by an Asymmetric Digital Subscriber Line (ADSL) connection. The ADSL modem connects to a wireless router to establish a Wi-Fi network in the house. A laptop equipped with Wi-Fi adaptor is used as the client of the wireless router.

Since the test area is a two-story house, the central controller, which is also the PAN coordinator, is located on the ground floor. A lamp controller and a radiator valve controller are located in the longue. Two environment sensors are located in the kitchen and toilet respectively. A wireless camera, a wireless router and a laptop are also put in the lounge. A power meter is located on the first floor. Figures 7.18 to 7.26 illustrate the devices loations in the test house.

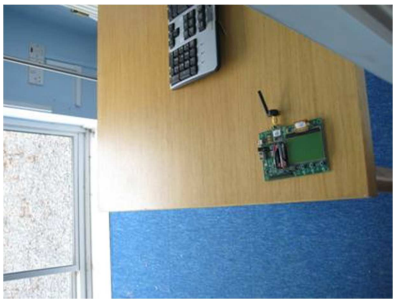

Figure 7.18 PAN coordinator locates on the ground floor

Figure 7.19 Wireless camera in lounge

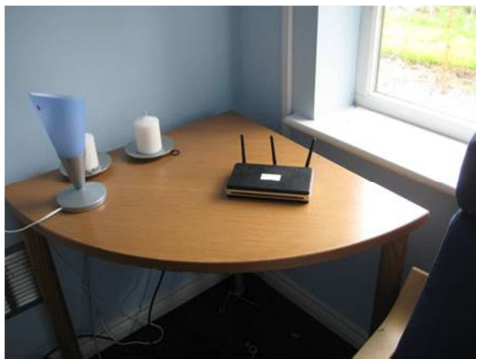

Figure 7.20 Wireless router in lounge

Figure 7.21 Local controller and laptop in lounge

Figure 7.22 Light controller in lounge

Figure 7.23 Radiator valve controller in lounge

Figure 7.24 Environment sensor in kitchen

Figure 7.25 Environment sensor in toilet

Figure 7.26 Power meter on the first floor

7.5.2 Measurement Methodology

The evaluation tests are performed with two components in the IndeedNET system. One component is the PAN coordinator to start the home automation network. Another component is an original sensor/actuator device in this system. Two locations are selected for this normal device. On the ground floor, we set it at a position which is 6 metres away from the coordinator. This is the average distance between devices on the ground floor to the coordinator. Another position is on the first floor. Figure 7.27 shows the deployment for the device at these two positions.

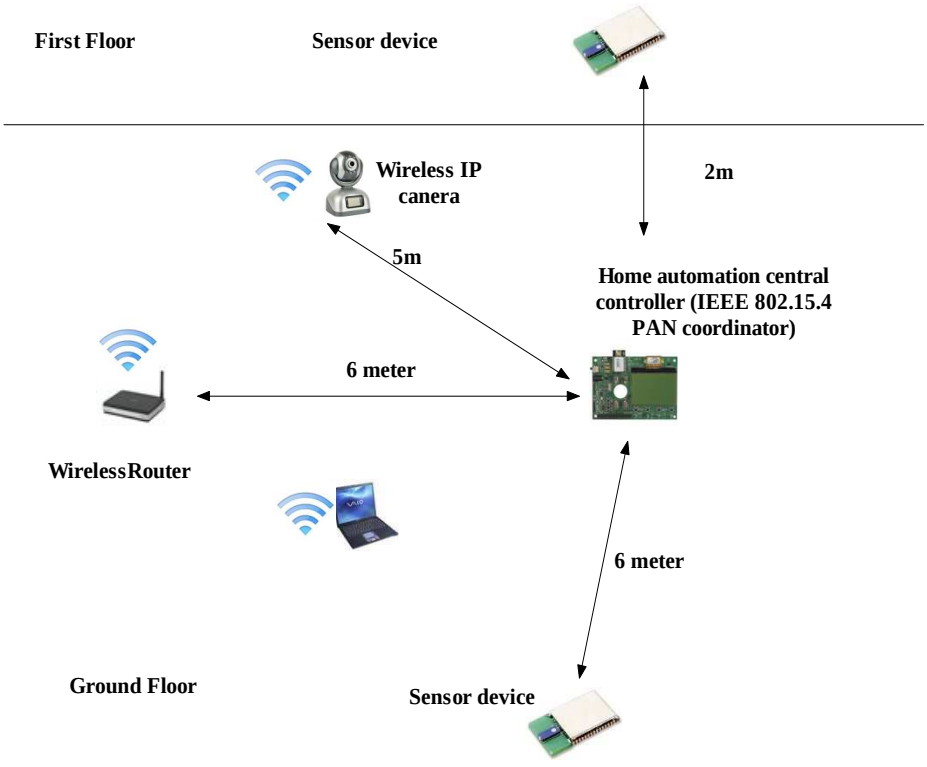

Figure 7.27 Deployment for the normal device at two positions

In Figure 7.27, the wireless router, a wireless IP (Internet Protocol) camera, a laptop, a home automation network coordinator and a sensor device are located at the ground floor. The distance between the wireless router and the network coordinator is 6 metres. Meanwhile, the wireless camera is set 5 metres away from the network coordinator. The distance of the sensor device located on the ground floor is 6 metres away from the network coordinator. The sensor device located on the first floor is about 2 metres from the network coordinator at the vertical direction.

After joining the established home automation network, the sensor device regularly sends sensor reading to the PAN coordinator every 1 minute. If the data transmission is successful, the sensor device enters into the sleeping mode and wakes up after 1 minute in order to execute its regular task. The tests are divided into two scenarios if data transmission is unsuccessful: 1) the sensor device enters into sleep without any action, or 2) the sensor device implements the proposed strategy described in Section 7.4. The test lasts for 20 minutes. A total of 20 sensor data packets were sent from the sensor device to the coordinator. The selection of interference sources adopts two devices: a web camera and a Wi-Fi router.

The tests run with three interference traffics: visiting wireless camera, browsing web page, and downloading file.

A. Web camera

The wireless router is set to work under the infrastructure mode, which means the acquired video stream generated on the web camera will be firstly relayed to the wireless router, and then sent to the laptop by the wireless router. In the web camera test, three different data rates supported by IEEE 802.11b standard (i.e. 2 Mbps, 5.5 Mbps and 11 Mbps) are used. Because such monitoring camera usually keeps working all the time for security purpose, it is probable that the wireless router will adapt the bit rate sometimes in order to support a noisy environment. Table 7.3 shows the settings for the wireless camera, the router, and the IEEE 802.15.4 network created by the PAN coordinator. The test result is shown in Table 7.4.

Table 7.3 Setting for the wireless camera, the router and the IEEE 802.15.4 network

Characteristics of Web Camera and Router		**Description**
Web camera manufacturer	LinkSYS	----
Effective Bandwidth on the router	2 Mbps, 5.5 Mbps and 11 Mbps	Configuration is made on the wireless router
Wi-Fi Mode on the wireless router and the camera	IEEE 802.11b	The camera only supports IEEE 802.11b mode
Wi-Fi Channel	11	Centre frequency 2462 MHz, ranges from 2451 MHz to 2473 MHz
IEEE 802.15.4 network channel	23	Centre frequency 2465 MHz, ranges from 2464 MHz to 2466 MHz

As indicated in Table 7.3 the wireless camera works at the IEEE 802.11b mode. The used Wi-Fi channel is 11, whose center frequency is 3 MHz from the channel used by the IEEE 802.15.4 network.

In Table 7.4, the column labelled “Data rate set on the wireless router” denotes different data rates configured on the wireless router. The columns labelled “Success rate of sensor device on the ground floor” and “Success rate of sensor device on the first floor” denote the success rate of data transmission from the sensor device located in different positions. The rate is obtained by counting the number of data packets whose transmissions are acknowledged by the coordinator. The row labelled “Without strategy” means the implementation does not include the proposed strategy. The row labelled “With strategy and retransmission time” means the consecutive retransmission strategy is implemented if data transmission failed. The value surrounded by brackets is the average retransmission time implemented by the sensor device when its first transmission after waking up from the sleeping mode was unsuccessful.

Table 7.4 Results of test using the wireless camera to generate interference

Data rate set on Wi-Fi router		**Success rate of sensor device on ground floor**	**Success rate of sensor device on first floor**
2 Mbps	Without strategy	30%	25%
	With strategy and retransmission time	100% (44)	95% (142)
5.5 Mbps	Without strategy	55%	50%
	With strategy and retransmission time	100% (40)	100% (30)
11 Mbps	Without strategy	85%	75%
	With strategy and retransmission time	100% (10)	100% (23)

For example, when the data rate of the wireless router is set at 2 Mbps, the sensor device located on the ground floor can achieve successful communication of a data packet by implementing 44 times retransmissions on average. The result shows that when a small data rate is set on the wireless router, the IndeedNET device requires more retransmission time. Since the retransmission interval set on the sensor device is 4.032 millisecond (refer to Section 7.4), the maximum retransmission time which will be attempted by the sensor device within 1 second is about $1000/4.032 = 248$ times. According to the measured success rate (with strategy implementation) listed in Table 7.4, the sensor device can achieve communication under most situations. The worst situation is that when the sensor device is located on the first floor and the Wi-Fi data rate is 2 Mbps, 5% data packets are still lost. However, the network coordinator moves to another channel very quickly when it detects that the data reception fails during the monitoring period. Consequently, the following data transmissions become normal. In other situations, a channel switch is not needed.

B. Browsing web page

In this test, the laptop is used to execute normal network operations, including browsing web page, sending/receiving email. The wireless router uses 11Mbps data

rate. The test result is shown in Table 7.5. No interference is found and retransmission strategy is not required.

Table 7.5 Result of test using normal Wi-Fi network operation to generate interference

Data rate set on Wi-Fi router		**Success rate of sensor device on ground floor**	**Success rate of sensor device on first floor**
11 Mbps	Without strategy	100%	100%
	With strategy and retransmission time	100% (0)	100% (0)

C. Downloading File

An additional computer is added into this test. The computer connects to the wireless router using a cable connection and has a file transfer protocol (FTP) server running on it. The laptop runs a FTP client to download a large capacity file from the FTP server. Different Wi-Fi traffic is generated by setting a download speed limit on the FTP server. The test result is shown in Table 7.6

In Table 7.6, the data transmission failure starts when Wi-Fi traffic rate is over 100Kbyte/second. The minimum success rate, which is 50%, is measured on the sensor device located on the first floor when Wi-Fi traffic is 500KBbyte/second. The retransmission strategy enables success rate to be 100% at most 37 retransmission times for a single packet.

Table 7.6 Result of test using FTP downloading to generate interference

Wi-Fi Traffic (KB/second)		**Success rate of sensor device on ground floor**	**Success rate of sensor device on first floor**
10	Without strategy	100%	100%
	With strategy and retransmission time	100% (0)	100% (0)
100	Without strategy	100%	95%
	With strategy and retransmission time	100% (0)	100% (21)
200	Without strategy	95%	90%
	With strategy and retransmission time	100% (6)	100% (21)
300	Without strategy	85%	75%
	With strategy and retransmission time	100% (20)	100% (37)
400	Without strategy	70%	65%
	With strategy and retransmission time	100% (25)	100% (23)
500	Without strategy	60%	50%
	With strategy and retransmission time	100% (16)	100% (23)

7.5.3 Discussion

In the test A- Web camera, the results show that the Wi-Fi traffic with low data rate causes significant interference on IEEE 802.15.4 network operation. The reason is that Wi-Fi packet requires more time to transmit if low data rate is employed. For example, if the Wi-Fi packet length is 1024 Byte. The wireless router needs $(1024*8)/(2*10^3) = 4.096ms$ to complete transmission if data rate is

2 Mbps. If the data rate is 11 Mbps, the transmission time is $(1024*8)/(11*10^3) = 0.744ms$, which is about one fifth of the time used by Wi-Fi transmitter with 2 Mbps data rate setting. As mentioned in Section 7.3, wireless security camera is a home appliance working at all time. Unless specified, the wireless router, which is the controller of a Wi-Fi network, may dynamically switch the Wi-Fi channel or shift the modulation scheme in order to maintain network performance when Wi-Fi network is under interference. Potentially, wireless camera has more chance to affect the developed IndeedNET home automation system. And we have encountered this problem in the field trial of the IndeedNET project.

For test B and test C, only 11 Mbps is chosen as the data rate setting on the wireless router. In test B, the Wi-Fi network does not generate obvious interference on the IndeedNET system during normal Internet operations (browsing web page, sending/receiving email, online chatting), which only require small data throughout. In test C, for the convenience of comparisons, fixed speed limits are applied on the FTP server. The test result indicates that the effect of interference caused by the Wi-Fi network becomes serious with the increment of download speed limit. During tests A, B, and C, our strategy has indicated that it can significantly increase the success rate of data transmission in the IndeedNET system.

The use of the consecutive data transmission strategy helps the home automation network device with the capability of maintaining communication whilst the battery consumption is also controlled. For example, in test C, when FTP speed limit is set as 300 KB/second, the sensor device located on the first floor needs 37 times retransmission to complete a data transmission. As the time consumed for each transmission is about 4.032milliseconds, the total operation time is 149.184 milliseconds. Table 7.7 lists the comparisons of time consumed by the sensor device with and without strategy implementation.

Table 7.7 Comparisons of time consumed by a sensor device with and without strategy implementation

Without Strategy Implementation		**With Strategy Implementation**	
First transmission	4.032 millisecond	First transmission	4.032 millisecond
Network rejoining (n=3)	2211.84 millisecond	Consecutive transmission for 37 times	149.184 millisecond
Data transmission after rejoining	4.032 millisecond	N/A	N/A
Total time consumption	2219.904 millisecond	N/A	153.216 millisecond

In Table 7.7, columns labelled “Without Strategy Implementation” and “With Strategy Implementation” denote the two situations that the sensor device will face when data transmission fails. If no strategy is used, the sensor device will scan all 16 channels and associate with the network coordinator again. The total time consumed for data transmission and network rejoining are 2219.904 millisecond. If the strategy is used, the communication will be achieved after 37 retransmissions which cost 153.216 millisecond. Therefore, the strategy implementation only requires $153.216 / 2219.904 = 6.9\%$ of time compared with the situation when no strategy is included. Consequently, 93.1% battery energy can be saved if the wireless module is active.

7.6 Summary

In this chapter, the proposed interference mitigation strategy was integrated into a practical home automation system in order to improve the system capability of maintaining communications during the times of interference. The strategy is specifically designed according to the characteristics of the home automation system. By applying consecutive data retransmission strategy, the sensor devices can effectively keep communications with the network coordinator

even under a serious interference condition, whilst the energy consumption is reduced compared with the normal procedures (e.g. scan channel and rejoin network) when the sensor device failed to send out a data packet.

Chapter 8 Application in Fire Safety Protection

8.1 Background and Motivation

In 2007, the local authority fire and rescue services attended 804,100 fires or false alarms in the United Kingdom. There were 445 fire-related deaths, including six fire fighters in 2007, and 268 fire fighters were injured during rescue service. The most common identified cause of death from a fire incident is being overcome by gas or smoke. In 2007, the fire and rescue service reported that 193 people died this way, accounting for 44% of all deaths. A further 88 (20%) deaths were attributed jointly to both burns and being overcome by gas or smoke, whilst 115 (26%) were due to burns alone". Figure 8.1 illustrates the overall statics of cause for fire-related death (Fire Statistic, 2007).

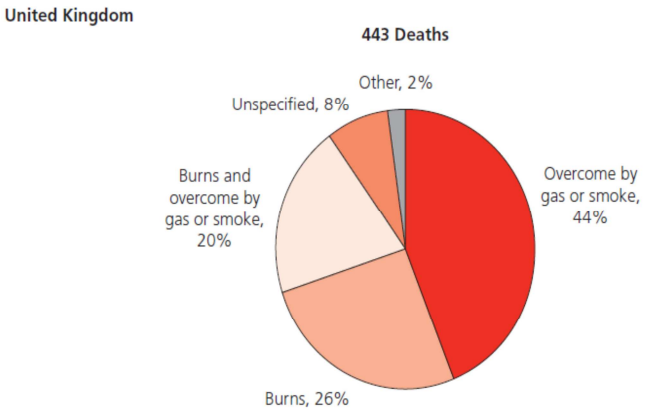

Figure 8.1 Overall statics of cause for fire-related death (Fire Statics, 2007)

The key point for effectively and efficiently implementing a fire rescue service and protecting fire fighters is to enable the command officer to clearly understand the emergency situation, by accessing real-time information collected from the scene of the fire incident (e.g. smoke distribution, gas density, temperature, and fire fighters' location). The best way is to deploy an innovative wireless sensor network to sense environment changes and report to on-site commanders before sending rescue personnel.

The Secure Ad hoc Fire & Emergency safety NETwork (SafetyNet, 2006) is a TSB funded project which provides an integrated first-responder support system achieving real-time data about the building and hazard conditions, including monitoring of responder location, floor-plan provision and critical conditions of environment changes. The author was a member of the technical team responsible for designing and implementing wireless communication module. Similar to the home automation system described in Chapter 7, the low level sensor information collection is accomplished by an IEEE 802.15.4 based wireless sensor network. The difference is that the SafetyNet system requires that the WSN should be applicable for large-scale deployment as the scope of a commercial building environment is usually unable to be covered by a single-hop star network. Therefore, WSN in the SafetyNet system employs a mesh network to achieve the purpose of adopting a large number of sensor nodes distributed within a given area into an integrated network, whilst the construction of such a network requires no infrastructure to be involved. The mesh network was developed based on the ZigBee technique (ZigBee, 2007).

It is common for offices in commercial buildings to have multiple Wi-Fi networks in daily work. As Wi-Fi networks work on the same 2.4 GHz ISM band, interference from these co-located networks becomes an increasing problem for ZigBee/IEEE 802.15.4 based WSNs. During the development of the SafetyNet system, interference issues were proposed by researchers and industrial partners from the point of view of practicality. It is concluded that the design challenges arise from uncertainty of interfering resource channel allocation, difficulty in predicting interference due to the wide coverage area of WSN in mesh topology, and existence of multiple interfering resources (i.e. multiple Wi-Fi networks). However, by monitoring the success rate of data transmission on sensor devices

and implementing districted energy detection, the controller of the SafetyNet system can determine the most suitable communication channel when WSN is under interference and then take further adjustment. The interference situation monitoring and multi-hop data transmission have been comprehensively studied in Chapters 5 and 6 as the contributions 2 and 3. An event driven strategy for interference detection and channel switch in the ZigBee network is proposed in this chapter with the adoption of contributions 2 and 3 in order to improve system performance under interference. The process of strategy design discussed in this chapter is also an overview of interference analysis and comprehensive utilization of measures in relation to moderating interference in WSNs.

8.2 Building Environment Monitoring System

Utilizing sensor networks to monitor building environments has been a mutual technology used in everyday life. It is quite common to have large numbers of smoke sensors, temperature sensors, etc installed in every corridor of buildings. Most of them are connected through a wired system to a central controller. The emergence of wireless sensor networks is accelerating the development of such a building monitoring system by reducing installation cost and improving deployment flexibility. To the best of the author's knowledge, the SafetyNET project was a first attempt to integrate smart wireless sensors, including environment sensors and location tracking sensors, into building monitoring for fire safety protection purpose. Figure 8.2 illustrates the infrastructure of the SafetyNET system (Yang and Frederick, 2006).

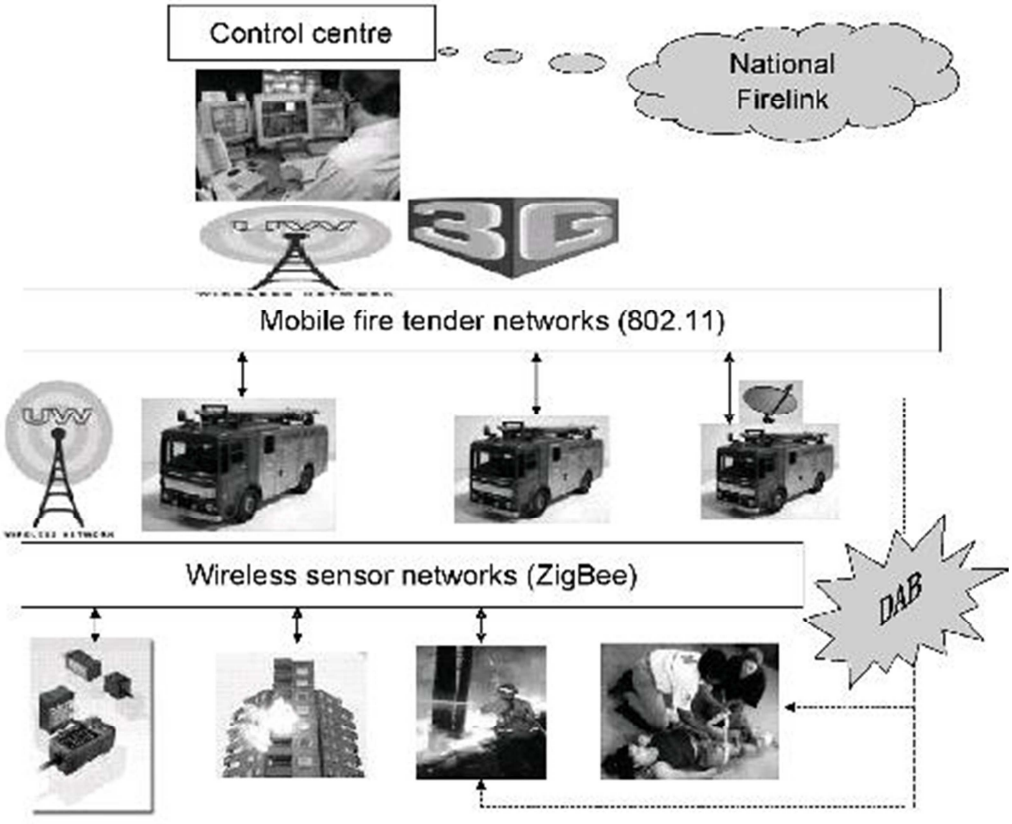

Figure 8.2 SafetyNet system infrastruture (Yang and Frederick, 2006)

The SafetyNet system provides an information structure to enable buildings, fire fighters, fire tenders, and their control centre to communicate efficiently during natural or man-made disasters by using sensor networks, wireless communications, Digital Audio Broadcasting (DAB) and 3rd generation (3G) technologies. The novel information infrastructure is comprised of three layers, as shown in the illustration above.

In Figure 8.2, the bottom layer comprises a robust wireless sensor network installed in the building. The sensor network utilizes robust sensor "motes" to detect any changes in the environment at specified locations. The sensor network can take the place of the existing fire alarm networks. Information collected from sensor devices flows over the sensor network and will then be transmitted to the fire tender network.

The middle layer comprises a vehicle-mounted mobile network installed on the fire tenders. It is achieved by upgrading the newly introduced vehicle-mounted mobile data systems (VMDS) and adding not only the up-link with the control centre but also the down-link with the sensor network. The real time

information about the building, occupants, and the locations of the fire fighters is collected from the sensor network, transmitted to and presented at the fire tender network. Up-to-date information about the building such as the floor plan and hydrant status is downloaded from the central database located at the control centre to the fire tender's network on their way to an incident. DAB is employed between the bottom and middle layers in order to maintain a time critical one way communication channel between the tenders and emergency personnel.

At the top layer is the central facility located at the control centre of a fire brigade. An emergency response management system at the control centre will provide the fire-fighters with up-to-date critical information and remotely monitor the latest development of incidents. The national FireLink radio communication system for the fire and rescue services will be connected with the top layer in the information infrastructure. The connection with FireLink allows the real-time situation in emergency situations to be available nationally.

According to the design plan, the IEEE 802.15.4 based ZigBee wireless sensor network will be deployed in the interior of building, and responsible for monitoring critical environment conditions.

8.3 IEEE 802.15.4 Based ZigBee Wireless Sensor Network in SafetyNet System

When a wireless sensor network is deployed in a large-scale application, the capability for network devices to automatically route messages is essential. Since the IEEE 802.15.4 standard does not support the network layer, SafetyNet system employs the ZigBee technique to implement wireless mesh sensor network construction.

8.3.1 ZigBee Standard

The ZigBee is a worldwide open standard (ZigBee, 2005). The main objective of ZigBee is to provide an open standard suitable for wide range of applications that perform monitoring or control functions.

ZigBee standard is an enhancement of IEEE 802.15.4 standard. Figure 8.3 illustrates the system architecture of ZigBee standard (ZigBee, 2005).

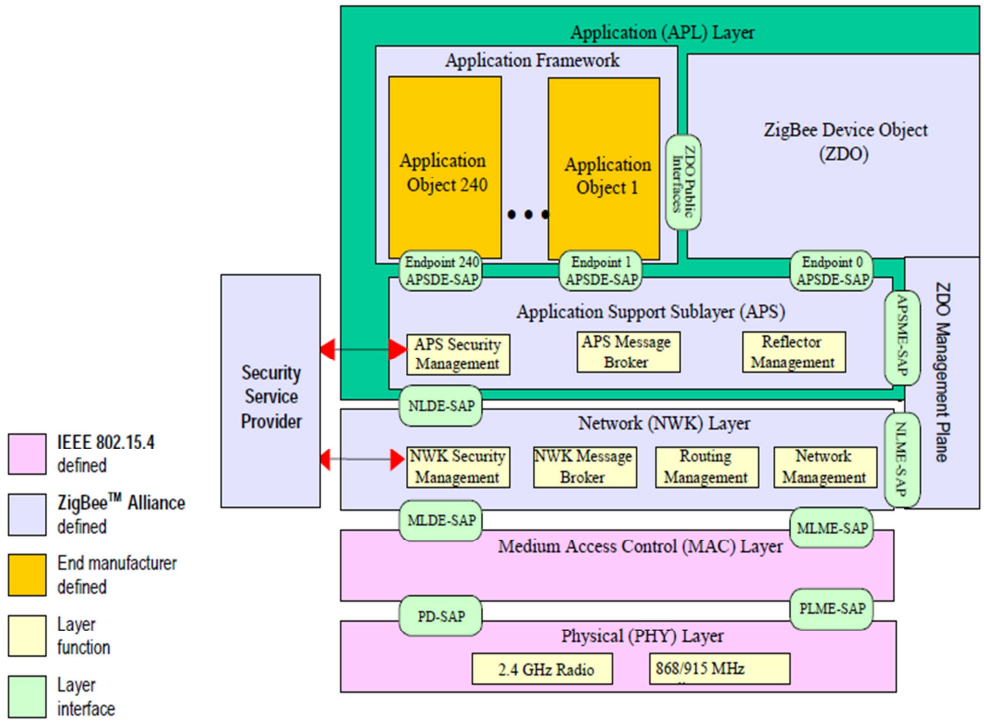

Figure 8.3 ZigBee stack architecture (ZigBee, 2005)

As shown in Figure 8.3, the ZigBee stack consists of four layers: PHY and MAC layers are defined by the IEEE 802.15.4 standard, the network and application layers are defined by ZigBee Alliance.

- PHY and MAC layers: The use of PHY layer and MAC layer in the ZigBee stack is to provide a ZigBee system with the capability of low power consumption wireless communication.
- Network Layer: ZigBee network layer is responsible for network topology construction and routing protocol implementation. The ZigBee standard utilizes the IEEE 802.15.4 standard to compose wireless communication part. The supported network topologies of ZigBee illustrated in Figure 8.4 are the extension of IEEE 802.15.4 infrastructure: star, tree, and mesh.

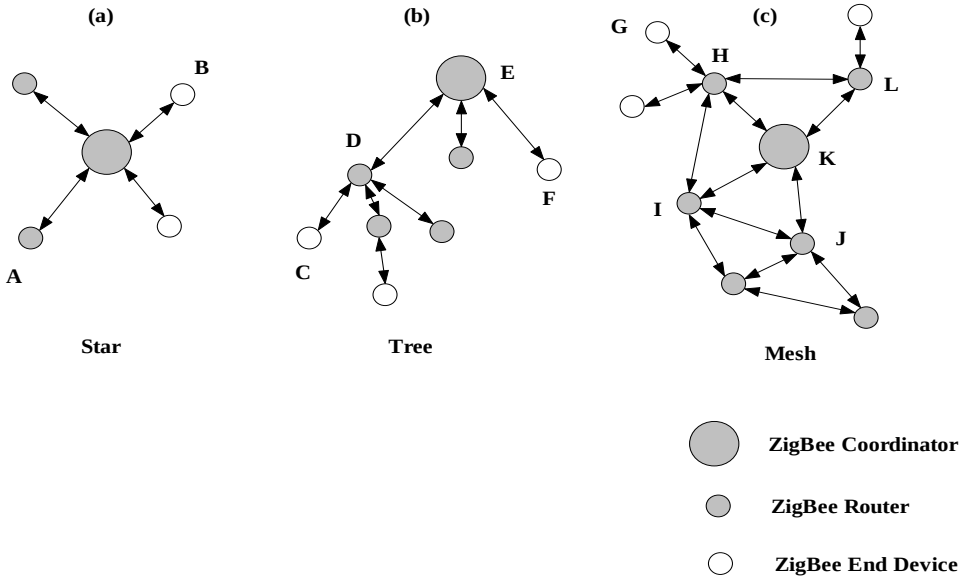

Figure 8.4 Supported topologies in ZigBee networks

The ZigBee standard defines three kinds of devices: ZigBee coordinator responsible for starting and maintaining the network, ZigBee router responsible for relaying network messages, and ZigBee end device responsible for implementing sensing or control tasks. In a ZigBee star network (Figure 8.4 a), either ZigBee router or ZigBee end device joins a ZigBee network by connecting to the ZigBee coordinator. Similar to the IEEE 802.15.4 star network, the network communications in a ZigBee star network is managed by the ZigBee coordinator. For example, if device A tries to send data to device B, the data must be sent to the ZigBee coordinator first, and then relayed to device B.

In a ZigBee tree network (Figure 8.4 b), a ZigBee router or a ZigBee end device router joins the ZigBee network through the ZigBee coordinator or the nearest ZigBee router which has already joined the network. The message transmission in a ZigBee tree network follows the route similar to the form of a tree. For example, if device C tries to send data to device F, the data must be sent to the device E, which is the common ancestor device of device C and F. Then device E relays the data to device F.

The process of forming a ZigBee mesh network is similar to the ZigBee tree network. The difference between the tree network and the mesh network is

the selection of message transmission route. In a ZigBee mesh network (Figure 8.4 c), if end device G tries to send data to device J, the data must be sent to the ZigBee router device H, through which end device G joined the network. Then the router device H can implement a routing protocol to find a route leading to device J. In Figure 8.4 c, the possible routes can be H->K->J, H->I->J, H->L->K->J, etc. All ZigBee router devices are completely equal in a mesh network, and capable to relay message. ZigBee end devices are not involved in any routing protocol.

The ZigBee network layer employs the same address mode inherited from the IEEE 802.15.4 standard, which uses a 16-bit short address to identify each device. Theoretically, around 65,000 devices can be contained in a single ZigBee network.

- Application Layer: The main objective of the ZigBee standard is to provide a standardized base set of solutions for monitoring and control systems (Kinney, 2003). Therefore, the design of the application layer introduces the concept of "Endpoint" applicable for a general purpose. Endpoint is a particular component which logically exists within a ZigBee stack. Each ZigBee device can have up to 240 such components. An endpoint can be used to identify a particular application running on a ZigBee device. Figure 8.5 illustrates the use of endpoints.

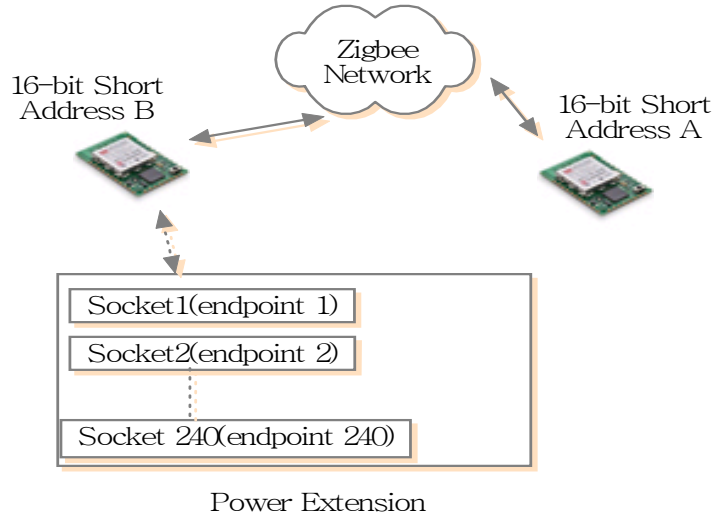

Figure 8.5 Use of Endpoint in ZigBee devices (Yao et al., 2008)

Figure 8.5 shows there is a ZigBee enabled power extension with multiple sockets. If other ZigBee devices want to communicate with a certain socket, the

communication message will reach the ZigBee power extension via a 16-bit address, and then use an endpoint identifier to locate the particular socket.

In a practical application, users only need to define the content of application (such as reading sensors and controlling actuators). The communications between different devices will be well managed by the ZigBee stack.

8.3.2 Wireless Sensor Nodes

The function of a ZigBee wireless sensor network is to provide real-time information within a building when required. According to the feedback obtained from the interviews with command officers, four types of sensor are essential for fire safety monitoring: temperature sensor, smoke sensor, flame sensor, and carbon monoxide sensor. Figures 8.6 to 8.9 show the sensors used. Figures 8.10 to 8.11 show the developed ZigBee router and ZigBee adaptor used to establish communication between computer and Zigbee network. Figure 8.12 illustrates the prototype of a sensor board integrating with these four sensors.

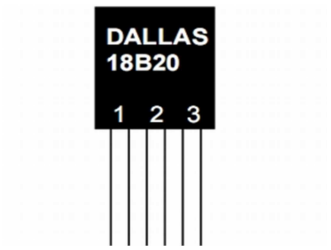

Figure 8.6 DS18B20 temperature sensor

Figure 8.7 Infrared smoke sensor

Figure 8.8 Infrared flame sensor

Figure 8.9 Carbon monoxide sensor

Figure 8.10 ZigBee router

Figure 8.11 ZigBee adaptor

Figure 8.12 Prototype of the ZigBee sensor board with four environment sensors

8.3.3 ZigBee WSN Deployment

A ZigBee wireless sensor network deployed within a commercial building for monitoring the environment is supposed to be able to adopt hundreds of sensor nodes. Meanwhile the effective communication range between a single pair of ZigBee devices is about 20-30 meters within an indoor environment. The star topology is not suitable for this application. Both the tree topology and mesh topology can generate a wide coverage area in a building environment. However, message transmission in a tree network might cause considerable delay as the data must be sent to the common ancestor of both source device and destination device, and then relayed to the destination device by following the branch of the tree. Therefore, we chose the mesh topology for the SafetyNet system. Figure 8.13 illustrates the developed ZigBee wireless sensor network in the SafetyNet system.

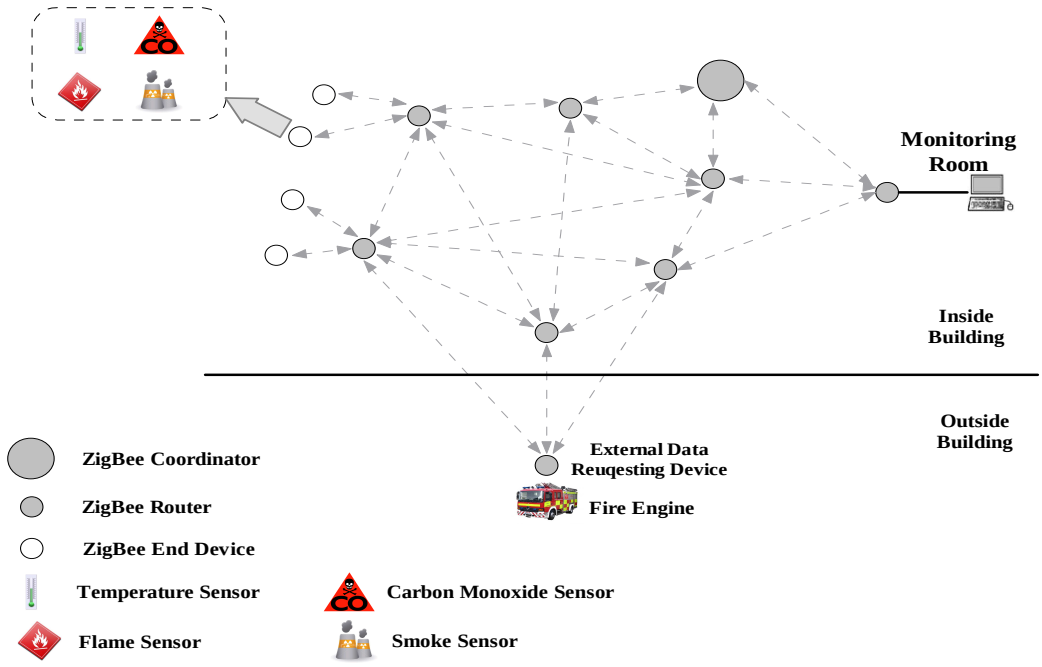

Figure 8.13 ZigBee wireless sensor network deployment

In Figure 8.13, a ZigBee coordinator and multiple ZigBee routers form a ZigBee mesh network, and are deployed inside a building. Each router can freely talk to other routers within its radio communication range. ZigBee end devices integrated with those four environment sensors join the ZigBee network through the nearest ZigBee routers. As mesh network does not have strict limitations on

physical locations of individual network nodes, ZigBee end devices can be installed at any position where at least one ZigBee router device is in its radio communication range. When sensor information is required by the monitoring room or the external fire engine, the corresponding ZigBee end device will send data to its parent device, i.e. the ZigBee router through which the end device joins the network, and then the ZigBee router takes responsibility of routing sensor information to the destination.

8.4 Interference in A ZigBee Mesh WSN

8.4.1 Interference Source

The most serious interference of WSN within a building environment is the coexistence of the ZigBee monitoring network and the IEEE 802.11 network. Typically there are multiple IEEE 802.11 networks existing in a building environment. To enable the convenience for employee or visitors to access networks (e.g. Internet, Intranet) inside offices, many IT services have made Wi-Fi networks as standard accessories of building network systems. In consideration of security and independency, it is quite common to have multiple IEEE 802.11 networks to work in the same area as required by different organizations, or departments. Figure 8.14 illustrates the deployment of multiple access points to meet the requirement of allowing multiple users to access a network over a large coverage area.

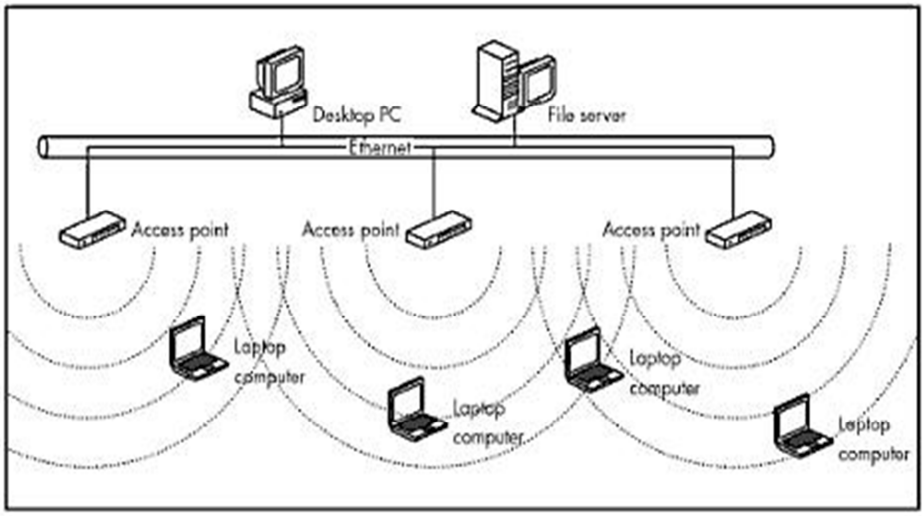

Figure 8.14 Multiple access points on a wired LAN (Ross, 2003)

In Figure 8.14, laptops connect to an Ethernet through wireless access points. In the office environment, mobile laptops usually work under the "downlink mode" in most cases, which means most IEEE 802.11 communications are issued from the access points to the laptops (e.g. browsing web page, email, ftp downloading). A possible interference scenario is illustrated in Figure 8.15.

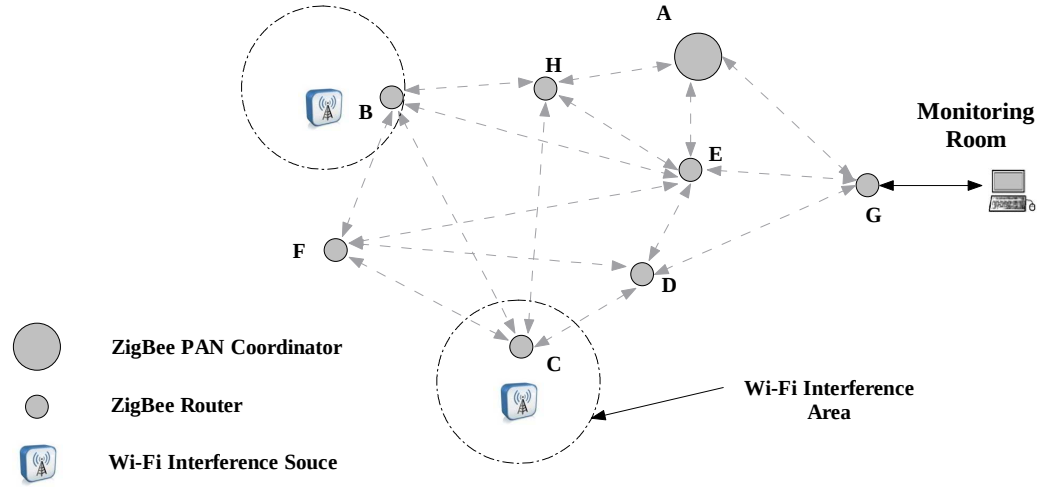

Figure 8.15 Interference scenario in ZigBee mesh network

In Figure 8.15, two Wi-Fi interference sources are located close to the ZigBee device C and device B. The receivers of device C and B will be affected by the Wi-Fi signals. If device F is to send data to device G connecting to monitoring room, the possible routes could be F->B->E->G, F->C->D->G, F->E-

>G, and F->D->G etc. The former two routes will be discarded by the routing protocol as devices B and C are unavailable due to interference. The communication can be achieved on other routes. However, if more ZigBee routers are affected by the Wi-Fi interference source, ZigBee communications in the mesh network still possibly fail due to the failure of route establishment. According to the purpose of the SafetyNet project, the developed ZigBee wireless sensor network is to monitor all areas in a building. It is inevitable to have some ZigBee devices coexist with Wi-Fi routers or access points.

Usually, Wi-Fi routers or access points are often static after installation. Therefore, ZigBee routers composing the backbone of the monitoring network can be located away from Wi-Fi transmitters with a safe physical distance. Meanwhile, proper centre frequency separation between the Wi-Fi interferers and the ZigBee network can also be helpful in interference avoidance.

8.4.2 Physical Distance and Channel Allocation

To reduce harmful interaction between Wi-Fi transmitters, proper physical and frequency separation is often taken into consideration when Wi-Fi networks were deployed. Usually, neighbour Wi-Fi routers are separated over 20 metres and employ different communication channels whose centre frequency separation is over 22 MHz, which is equal to the width of a complete Wi-Fi communication channel. As suggested in IEEE Std802.11b (2007), channels 1, 6, 11 or 1, 7, 13 are commonly used when multiple Wi-Fi routers are deployed. Figure 8.16 illustrates a possible Wi-Fi routers' deployment for the ZigBee mesh network.

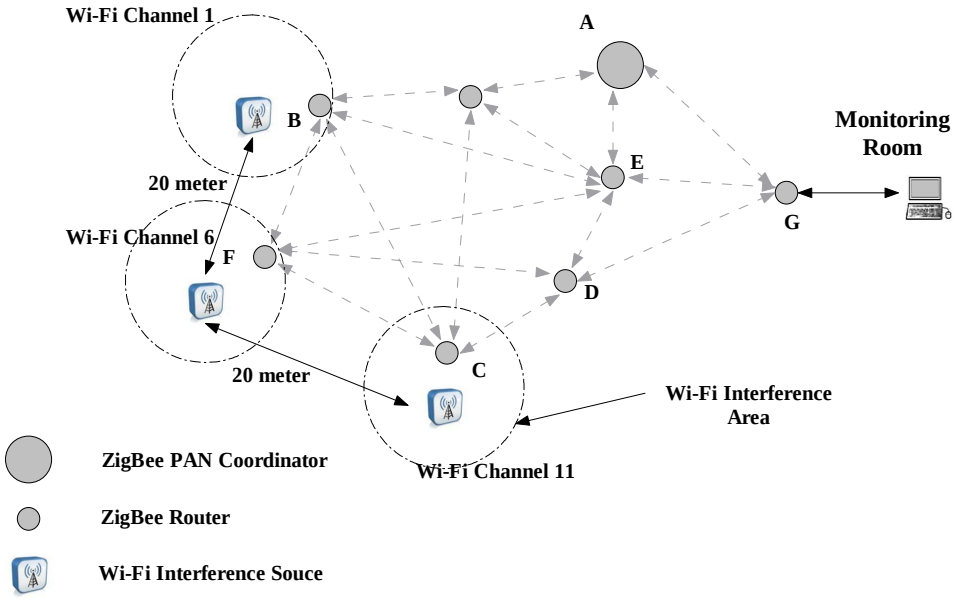

Figure 8.16 Wi-Fi routers deployment

In Figure 8.16, multiple Wi-Fi routers are deployed with a certain physical distance separation and channel separation. If a ZigBee device is located in the vicinity of a Wi-Fi router, it needs to consider the possible Wi-Fi interference avoidance from two aspects: distance separation and channel overlapping. The level of interference is decided by the signal strength of the interfering signal falling within ZigBee receiver's bandwidth. A Wi-Fi transmitter has a strong output power much higher than a ZigBee transmitter. According to the IEEE 802.11b standard, the initial output power on a Wi-Fi transmitter is around 20 dBm (i.e.100 milliwatt) whilst a ZigBee transmitter employs 0 dBm (i.e. milliwatt) output power. As the increment of propagation distance, Wi-Fi signal power will attenuate. If the remaining Wi-Fi power reaching a ZigBee receiver is still higher than the allowed noise level, the interference will affect the ZigBee communication. Channel allocation is also in relation to interfering energy attenuation. Figure 8.17 depicts Wi-Fi and ZigBee channel allocations on 2.4 GHz band.

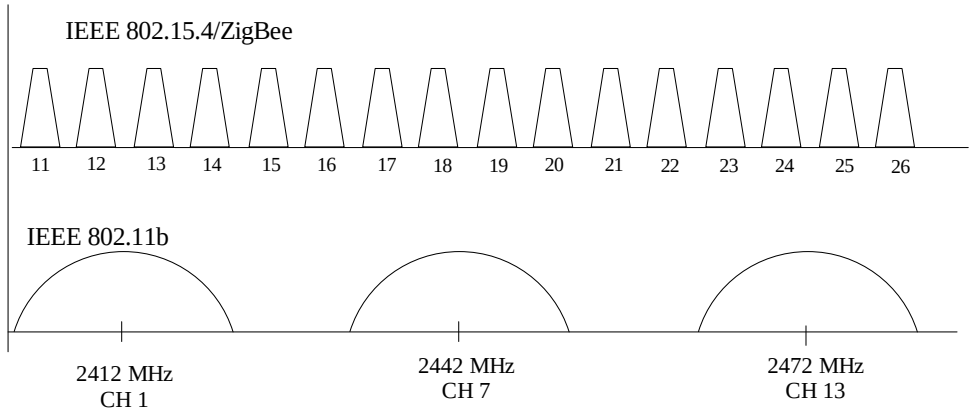

Figure 8.17 Wi-Fi and ZigBee channel allocations on 2.4 GHz band

Although ZigBee WSN can use up to 16 communication channels defined at 2.4 GHz band, a ZigBee network can only use one communication channel at any given time as it is not a frequency hopping technique similar to Blutooth. When the distributed Wi-Fi routers utilize non-overlapping channel settings (channel 1, 7, 13 as shown in Figure 8.17), some of the ZigBee channels will be affected. As most of the energy of the Wi-Fi signal concentrates on the central frequency of the employed Wi-Fi communication channel, a certain frequency separation between a Wi-Fi channel and a ZigBee channel can effectively reduce interference energy for ZigBee systems.

As the positions of Wi-Fi routers existing in a building environment are usually fixed, ensuring physical distance and channel separation for a ZigBee network to avoid Wi-Fi interference are achievable.

8.4.3 Dynamic Interference Source

After eliminating the possibility for static Wi-Fi routers to cause serious interference to a ZigBee sensor network, the interference source requiring sensor network developers to guard against is a dynamic interference source emerging during daily work. For example, a temporary Wi-Fi FTP server can be set up in an office as requested by a research project and keeps long term operations. These unexpected interference devices are not scheduled in the original Wi-Fi deployment and are not considered when establishing the ZigBee system. Due to the wide node distribution of the ZigBee sensor network, the ZigBee PAN

coordinator could be hundreds of meters away from the devices being affected by a dynamic interference source, which means the PAN coordinator is unable to be sensitive to the emergence in the dynamic interference area. Furthermore, the duration and level of interference caused by the dynamic interference source is unknown to the sensor network. Consequently the whole system cannot respond to interference in time without an effective mechanism.

In the following sections, the interference detection and mitigation strategy design is divided into two steps: for static interference detection and mitigation, and dynamic interference detection and mitigation.

8.5 Static Interference Detection and Mitigation Strategy Design

As mentioned in Section 8.4, the locations of most Wi-Fi routers or access points in a building environment are static during day-to-day operation. Then the ZigBee devices can avoid interference by being installed at positions which are a safe distance away from those Wi-Fi transmitters, and employing a suitable communication channel. It has been reviewed in Chapter 3 that generally if a ZigBee device is physically at least 7 meters away from Wi-Fi routers, or channel frequency separation between a Wi-Fi channel and a ZigBee channel is over 7MHz, the IEEE 802.11 signals reaching ZigBee receivers is tolerable. Consequently, the interference effect from the IEEE 802.11 signals can be ignored no matter what IEEE 802.11 traffic is.

A reasonable channel allocation is achievable as both Wi-Fi networks and ZigBee networks can be manually configured at the initial installation stage. The “safe distance” is not a fixed value as building layouts in different practical environments might be different. Before the installation of the SafetyNet system, measurements for detecting Wi-Fi routers’ interference range were implemented.

The measurement methodology explores the impact of different parameters on the SafetyNet system, including frequency offset and physical distance separation. At the application layer of communication protocol, packet loss is the direct consequence visible to the software developers. Therefore it is

used as the main metric. The purpose of designing interference energy measurement is to determine an optimized physical and frequency separation for the ZigBee mesh network to avoid interference from the static Wi-Fi network.

The installation of the ZigBee sensor mesh networks should not require changes on the locations of the Wi-Fi routers that have already been deployed in the same building. Therefore, the measurement starts from the point that the pre-installed Wi-Fi routers are static and have a limited interference range. Assuming the distance between a Wi-Fi router and a ZigBee receiver is fixed, the success rate of ZigBee communications will vary by changing the distance between the ZigBee transmitter and the ZigBee receiver. Frequency separation between the ZigBee and Wi-Fi networks are also considered. Figure 8.18 illustrates the set-up layout for the measurement testing.

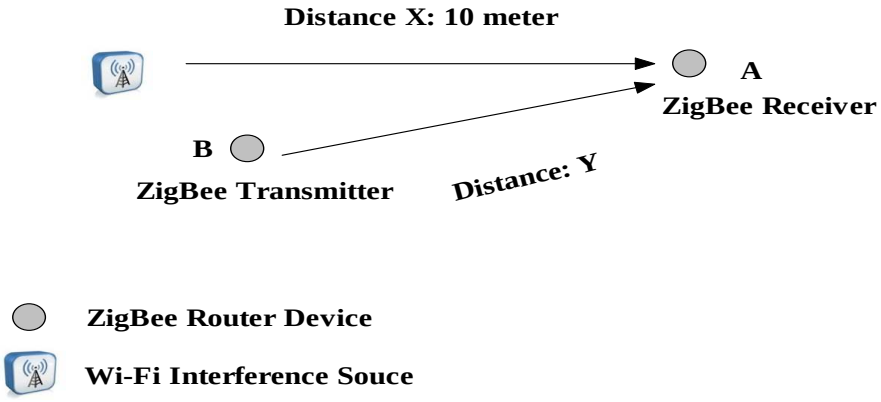

Figure 8.18 Devices deployment in static interference measurement

In Figure 8.18, the Wi-Fi interference source is fixed, and continues to transmit Wi-Fi signals in order to make the radio environment filled with the interference energy. The ZigBee device A and B are all ZigBee routers, and act as ZigBee receiver and transmitter respectively. The measurement is for testing the success rate of data transmission between device A and B. The distance X between Wi-Fi interference source and device A is fixed at 10 meter. The distance Y between device A and device B varies during measurement. The distance between the Wi-Fi interference source and device B is not considered here as the effect of interference on the receiver of device A is decided by the remaining

energy level of the interfering signal and desired signal. The measurement is divided into three steps: measuring Wi-Fi energy distributes on 2.4 GHz, measuring ZigBee signal strength falling within the ZigBee receiver bandwidth, and measuring the ZigBee communication success rate under the Wi-Fi interference with different distance Y.

A) Measuring the Wi-Fi energy distribution on the 2.4 GHz band

The experiment of measuring the Wi-Fi energy distribution on the 2.4 GHz band is to identify the Wi-Fi interfering energy level on each ZigBee communication channel when a Wi-Fi transmitter is in operation. In this experiment, the Wi-Fi interference source was set to work on Wi-Fi channel 11, whose centre frequency is 2462MHz. An energy detector compliant with the ZigBee/802.15.4 standard was placed at the side of device A, which is 10 meters away from the Wi-Fi router. The detector listened on 16 ZigBee channels and recorded the highest energy level on each ZigBee channel. Table 8.1 shows the measured results.

Table 8.1 Recorded energy level caused by Wi-Fi signal on all ZigBee channels

ZigBee Channel (Centre Frequency)	11 (2405 MHz)	12 (2410 MHz)	13 (2415 MHz)	14 (2420 MHz)	15 (2425 MHz)	16 (2430 MHz)	17 (2435 MHz)
Measured Energy (dBm)	-95	-96	-96	-92	-88	-82	-80

18 (2440 MHz)	19 (2445 MHz)	20 (2450 MHz)	21 (2455 MHz)	22 (2460 MHz)	23 (2465 MHz)	24 (2470 MHz)	25 (2475 MHz)	26 (2480 MHz)
-76	-65	-59	-36	-26	-20	-38	-57	-76

In Table 8.1, the row labelled “ZigBee Channel (Centre Frequency)” denotes the ZigBee communication channel and corresponding radio frequency on which the detector is listening. The row labelled “Measured Energy” means the highest energy level detected by the detector on a specified channel. Figure 8.19 shows the detected Wi-Fi interfering energy level on each ZigBee channel using the form of a bar chart.

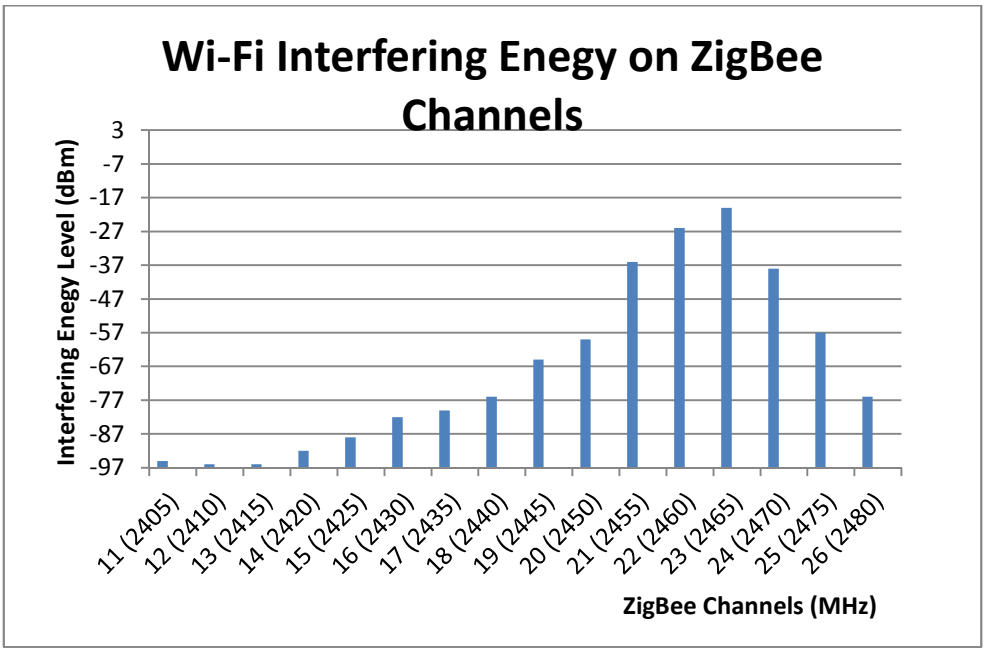

Figure 8.19 Wi-Fi interfering energy level

As shown in Figure 8.19, it is obvious that the detected Wi-Fi interfering energy level is higher in the ZigBee channels which are closer to the centre frequency of Wi-Fi channel (i.e. 2462 MHz).

B) Measuring ZigBee signal strength without Wi-Fi interference

The second measurement is to detect the ZigBee signal strength falling within the ZigBee receiver's bandwidth when no Wi-Fi interference is present. By changing the distance Y, the effective ZigBee signal strength measured on the receiver of device A is different. The measurement is taken by enabling device B to continue to send ZigBee packets to device A, whilst the energy detector records the average energy level at the side of the receiver of device A. According to the work of Rodriguez (2005), the attenuation of ZigBee signal strength can be calculated using Equation (8.1) as follows:

$$L = 20Log(f) + 20Log(d) + 32.44 \quad (8.1)$$

where:

L is the path loss in dB that the ZigBee signal strength will attenuate

f is the frequency in MHz that the ZigBee network works on

d is the distance in km between the ZigBee transmitter and ZigBee receiver

Then, the energy level measured on ZigBee receiver can be calculated as:

$$E_{\mathrm{Re}\,maining} = E_{Initial} - L \tag{8.2}$$

where $E_{\mathrm{Re}maining}$ is the energy level in dBm which finally reaches the ZigBee receiver after attenuating. $E_{Initial}$ is the output power from the ZigBee transmitter in dBm. In this experiment, $E_{Initial}$ is set at 0 dBm. Although the Equation (8.2) can be used to calculate the energy attenuation of the ZigBee signal strength after travelling over a certain distance, the practical situation is different as this equation is conducted on the basis of "Free-space", which means the effect of the indoor environment is not considered. Therefore, the Equation (8.2) is used in this experiment for the purpose of reference. For the convenience of comparison, the actual measured energy value and calculated energy level according to Equation (8.2) are listed in Table 8.2. Both the ZigBee devices A and B work on channel 23 (2465 MHz).

Table 8.2 Energy level on ZigBee receiver after attenuating

Distance Y (meter)	2	4	6	8	10
Measured Energy Level (dBm)	-47	-51	-53	-55	-57
Calculated Energy Level (dBm)	-46.30	-52.31	-55.84	-58.34	-60.28

In Table 8.2, the row labelled "Distance Y" denotes the distance between the devices A and B. The row labelled "Measured Energy Level" means the energy level measured by the energy detector. The row labelled "Calculated Energy Level" is the value obtained according to Equation (8.2). The experiment was taken place in an office environment. By considering the effect of indoor environment, such as shadow and reflection, the "Measured Energy Level" is thought to accord with the practical situation as a small error is reasonable.

C) Measuring ZigBee communication success rate under Wi-Fi interference with different distance Y

The experiment C is to determine at which level the Wi-Fi energy can cause significant interference on ZigBee communications when the distance between the Wi-Fi interference source and the ZigBee receiver is fixed at 10 meters.

In the experiment C, the Wi-Fi traffic is generated by a software packet generator. No limitation was applied on the packet generator in order to make Wi-Fi interference uninterrupted. ZigBee device B was set to send data packets to device A with a fixed packet rate at 200 packet/second. The ZigBee packets contained a fixed payload length at 50 bytes. ZigBee transmission lasts for 50 seconds, which means a total of 10,000 packets will be sent. The test results are shown in Table 8.3.

In Table 8.3, the column labelled “ZigBee Channel (MHz)” denotes the ZigBee communication channels on which the experiment C was carried out. Columns labelled “Distance Y”, “Centre Frequency Offset”, “Wi-Fi Energy on ZigBee Receiver” and “ZigBee Energy on ZigBee Receiver” denote the distance between device B to device A, the centre frequency offset between the Wi-Fi router and the ZigBee network, the measured Wi-Fi energy on the ZigBee receiver and the measured ZigBee signal energy on the ZigBee receiver respectively. Values in the columns of “Wi-Fi Energy on ZigBee Receiver” and “ZigBee Energy on ZigBee Receiver” are derived from the Tables 8.1 and 8.2 respectively. The column labelled “ZigBee Communication Success Rate” means the ratio of the received ZigBee packets to the total ZigBee packet number sent by device B. When the ZigBee network works on channels 23 and 24, the success rates are relatively low as the Wi-Fi energy falling within the ZigBee receiver’s bandwidth is always higher than the ZigBee signal energy. When the ZigBee network works on channel 25, the success rates are still relatively low when distance Y is 8 or 10 meters, although the ZigBee signal energy is equal or 2 dB higher than the Wi-Fi energy. Once the distance decreases and the ZigBee signal energy is higher than the Wi-Fi energy at least by 5 dB, the success rates become nearly 100%. It accords with the simulation results conducted by the IEEE 802.15.4 standard that

when the ZigBee signal measured on the receiver is about 4-5 dB greater than the noise level, the packet error rate will be less than 1% (IEEE Std802.15.4-2003, 2003). On the ZigBee channel 26, no interference was observed.

The conclusion drawn from experiments A, B, and C is that if a ZigBee router is installed 10 meters (i.e. distance X) away from the nearby Wi-Fi router, and the ZigBee network employs the communication channel whose centre frequency is at least 13 MHz away from the Wi-Fi communication channels, other ZigBee devices can be installed around the ZigBee router within a range of 8 meters. Although the success rate is about 89.9% when distance Y is 8 meters, the employment of data retransmission at the application layer can easily improve system performance. Figure 8.20 shows a possible deployment which is made according to the conclusion.

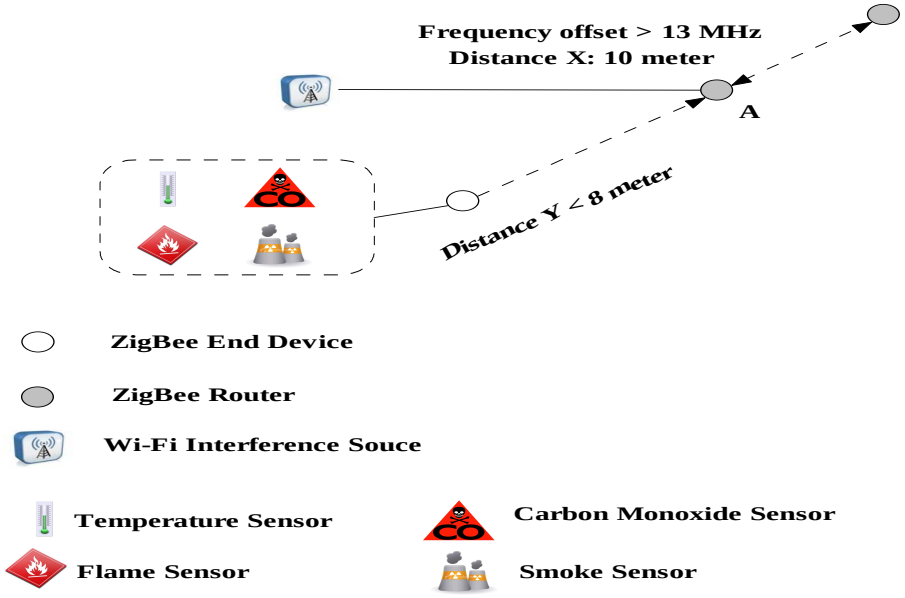

Figure 8.20 ZigBee router installation with safe distance

In Figure 8.20, the ZigBee router A is installed 10 meters away from the Wi-Fi interference source. Whilst the frequency offset between the ZigBee network and Wi-Fi router is greater than 13 MHz. A ZigBee end device connecting to multiple environment sensors is installed close to the ZigBee router with distance Y which is less than 8 meters. Under such circumstance, the success rate of data transmission from the ZigBee end device to the ZigBee router will not be less than 89.9%.

Table 8.3 Success communication rate of ZigBee devices during the period of interference

Wi-Fi Channel 11 (2462 MHz)					
ZigBee Channel (MHz)	**Distance Y (meter)**	**Centre Frequency Offset (MHz)**	**Wi-Fi Energy on ZigBee Receiver (dBm)**	**ZigBee Energy on ZigBee Receiver (dBm)**	**ZigBee Communication Success Rate**
23 (2465 MHz)	2	3	-20	-47	5.26%
	4	3	-20	-51	4.58%
	6	3	-20	-53	3.21%
	8	3	-20	-55	0.23%
	10	3	-20	-57	0.07%
24 (2470 MHz)	2	8	-38	-47	9.21%
	4	8	-38	-51	9.16%
	6	8	-38	-53	7.05%
	8	8	-38	-55	0.80%
	10	8	-38	-57	0.49%
25 (2475 MHz)	2	13	-57	-47	99.85%
	4	13	-57	-51	99.71%
	6	13	-57	-53	99.67%
	8	13	-57	-55	89.9%
	10	13	-57	-57	44.87%
26 (2480 MHz)	2	18	-76	-47	100%
	4	18	-76	-51	100%
	6	18	-76	-53	100%
	8	18	-76	-55	100%
	10	18	-76	-57	100%

The 10 meters physical separation and 13 MHz channel separation has been used as the basic criteria to design the SafetyNet system deployment scheme.

If the distance X (i.e. 10 meters) is changed, other parameters should be changed accordingly by following the same measurement methodology.

8.6 Dynamic Interference Detection and Mitigation Strategy Design

The physical distance separation and proper channel allocation can help ZigBee devices mitigate interference caused by static interference sources. However, the strategy design for detecting dynamic interference caused by unexpected IEEE 802.11 interferers faces new challenges, which can be concluded into three aspects: 1) Uncertainty of global interfering signal channel allocation. 2) Determination of interference level and 3) ZigBee network synchronization.

8.6.1 Uncertainty of Global Interfering Signal Channel Allocation

The unexpected interference source may operate on any ZigBee channel. If multiple interference sources employing different Wi-Fi communication channels emerge at different locations of a ZigBee network, the situation will become complicated (see Figure 8.21).

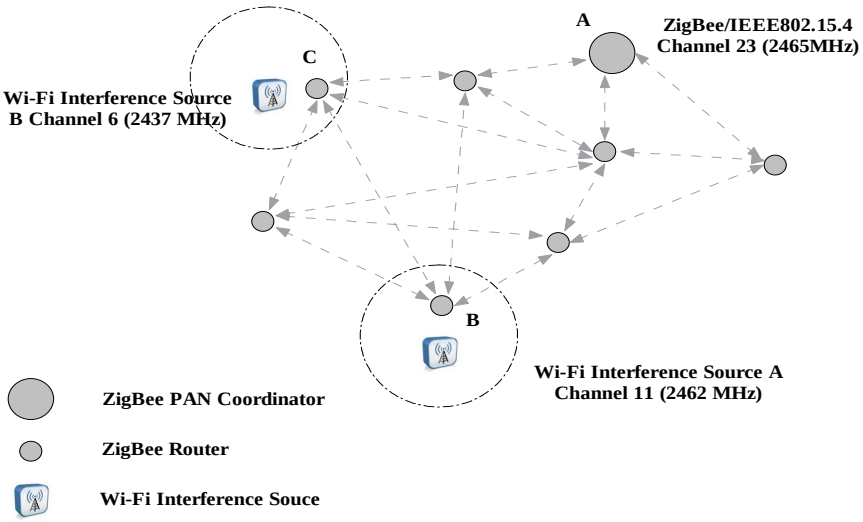

Figure 8.21 Multiple interference sources operating on different Wi-Fi channels

In Figure 8.21, Wi-Fi interference source A working on Wi-Fi channel 11 is interfering with the ZigBee network operating on ZigBee channel 23 as the centre frequency offset between two system is 3MHz. If the ZigBee PAN coordinator has sensed the interference caused by Wi-Fi interference source A, it might decide to switch to ZigBee channel 17 (2437 MHz) to avoid interference. However, another interference source, Wi-Fi interference source B, is working on Wi-Fi channel 6 (2437 MHz) and located in the vicinity of ZigBee device C. The interference avoidance for the ZigBee network might fail since the newly chosen ZigBee channel is too close to the frequency used by the second Wi-Fi interference source B. ZigBee network channel switch will be less effective if more interference sources are introduced.

8.6.2 Determination of Interference Level

Dynamic interference source could be temporary, or work at low duty-cycle which is insufficient to cause serious interference on ZigBee network operations. The strategy design should take interference tolerance into consideration in order to avoid overreaction. For example, a Wi-Fi interference source works at a relatively low traffic rate (e.g. less 100 KB/second). Even though the Wi-Fi signal can cause interference on ZigBee communications, ZigBee application software can easily overcome difficulty by employing retransmission at application layer.

8.6.3 ZigBee Network Synchronization

If the ZigBee PAN coordinator decides to move the network to an alternative channel when the current channel becomes noisy and communication becomes problematic, other ZigBee network devices also need to switch their network channel for the continuous sensor network communication. Unlike the beacon-enabled IEEE 802.15.4 network, a ZigBee mesh network does not employ beacon signal to synchronize network devices as spreading the beacon signal in a distributed mesh network is difficult to achieve. Therefore, a simple synchronization mechanism at the application layer is needed. In the SafetyNet system, each ZigBee device, including the ZigBee router and ZigBee end device,

is required to regularly send a detection packet requiring acknowledgement to its parent device, which previously allowed them to join the network. If a number of acknowledgements are lost, the ZigBee device shall restart the network joining procedure as the parent device has probably moved to a new channel due to the network channel switch. Figure 8.22 shows the flow chart of ZigBee device synchronization.

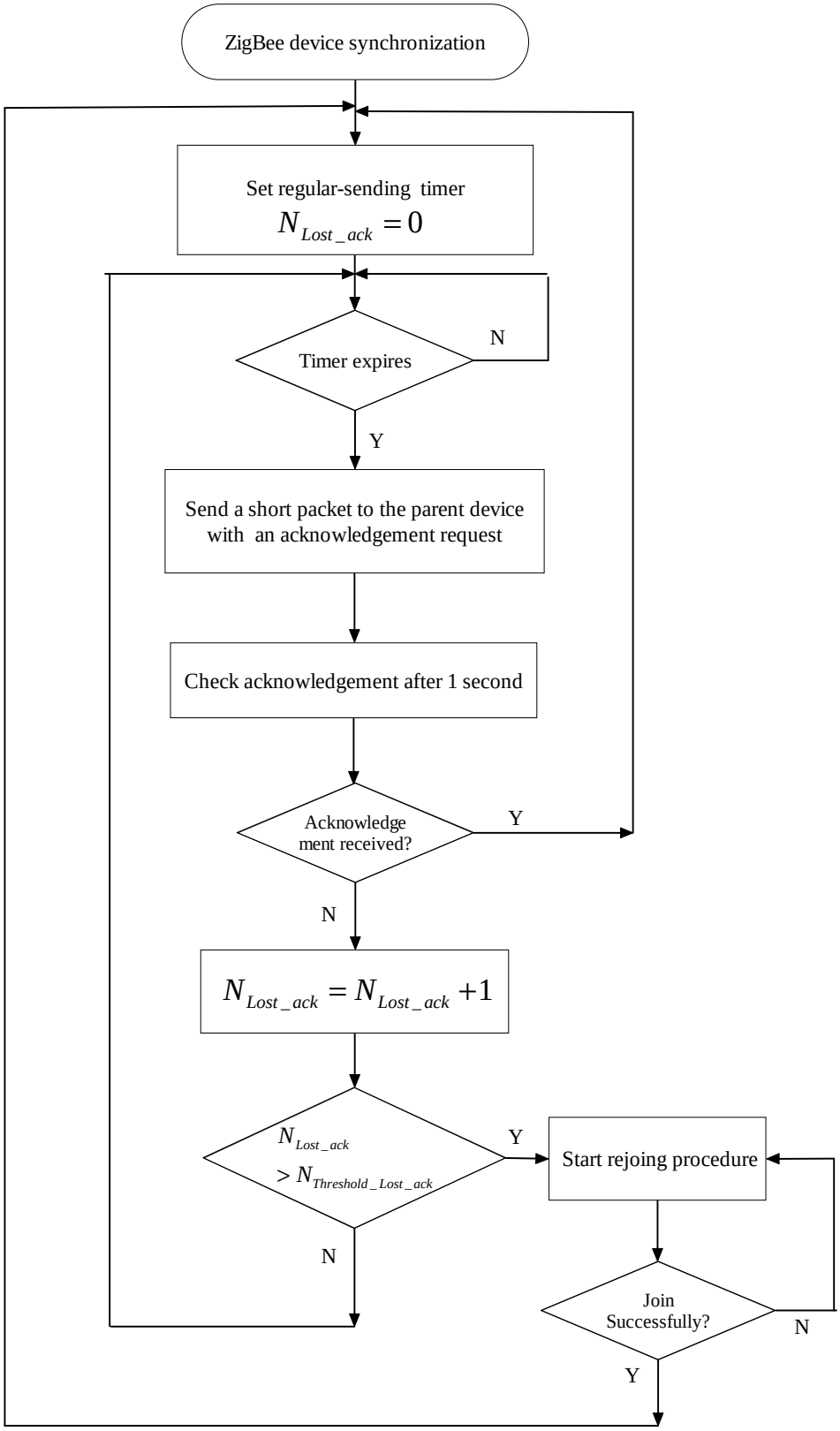

Figure 8.22 Flow chart of ZigBee device synchronization

In Figure 8.22, each ZigBee device sets a timer and counter, N_{Lost_Ack} to count the number of lost acknowledgements. When the timer expires, the ZigBee device will send a short packet requiring acknowledgement to its parent device. If the acknowledgement is received after 1 second, the counter will be reset to 0. If the acknowledgement is not received, the counter will be added by 1. If the counter has exceeded the threshold $N_{Threshold\_Lost\_ack}$, the ZigBee device should start the procedure of rejoining the network. If the counter is less than the threshold, the timer will be reset, but the counter value will remain.

8.6.4 Mitigation Strategy Design for Dynamic Interference

In order to the address the challenges concluded in the above sections, a comprehensive strategy was proposed during the development of the SafetyNet system to effectively improve the ZigBee network performance when dynamic interference occurs. The strategy consists of three steps: regular energy detection, employment of data retransmission and channel switch.

A) Regular Energy Detection

Each ZigBee router device is programmed to execute energy detection on all 16 channels as a regular task. Since the purpose of energy detection is to evaluate if the detected channels are available for ZigBee network communication, the strategy proposed in Chapter 5 can be used here after a proper modification. There are two parameters needed to implement energy detection: energy detection period $P_{Detection}$ on a single ZigBee channel and energy threshold $E_{Threshold}$ which is used to determine if the detected channel is suitable for use. The energy detection period is decided by the length of data packet. The longer the packet length is, the longer the detection period is needed. The value of $P_{Detection}$ can be calculated using Equation (4.13). In experiment C of Section 8.5, if the interfering energy level (i.e. the Wi-Fi signal strength) falling on a ZigBee channel is over -57 dBm, the ZigBee channel can be marked as a bad channel unsuitable for the ZigBee communication. Then the parameter $E_{Threshold}$ is set at -57 dBm in the SafetyNet system. The value of $E_{Threshold}$ depends on the practical system

setting (i.e. the distance between the ZigBee router to the Wi-Fi router). The regular energy detection results will be sent to the sink node located at the monitoring room to construct an up-to-date record for the whole ZigBee network. Figure 8.23 shows the flow chart for implementing energy detection on a ZigBee router.

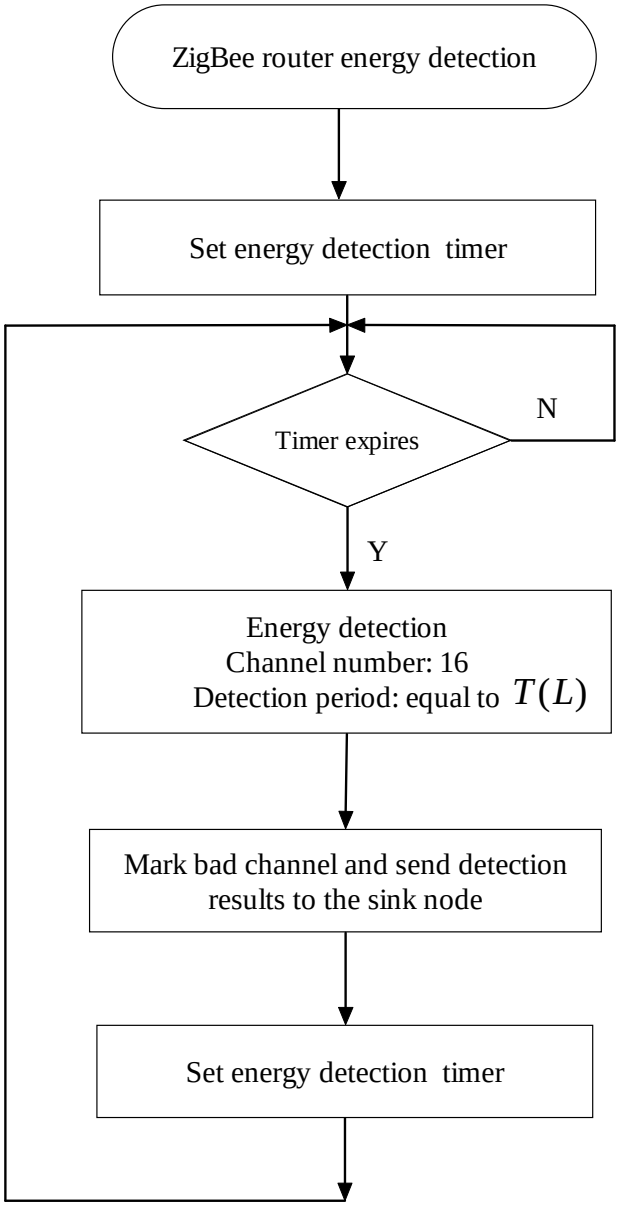

Figure 8.23 Flow chart of energy detection on a ZigBee router.

In Figure 8.23, after initialization, the router device sets a timer to implement regular energy detection. If the timer expires, the router will scan all 16

channels using detection period $T(L)$, which is equal to the time required to send a L byte length packet from a ZigBee device to another ZigBee device. The parameter $T(L)$ is derived from Equation (4.13). On the completion of energy detection, the router will mark the bad channels unsuitable for ZigBee communication and send the results to the sink node located in the monitoring room to build radio environment information. Then the router device sets a new timer and starts energy detection again when the timer expires.

B) Employment of Data Retransmission

The direct consequence of interference which is visible to application layer developers is packet loss. After successfully sending out a data packet, a ZigBee device is unable to know if the transmission is actually successful until an application layer acknowledgement is received. Therefore, the ZigBee device should wait for a certain period $T_{Waiting}$ and then check whether the acknowledgement has been received.

In ZigBee specification 2004 (ZigBee, 2005), a simple method named as "KVP_ACKNOWLEDGEMENT" (KVP stands for Key-Value Pair) is proposed to enable the recipient to issue an application layer acknowledgement to the sender on receipt of data frame. Figure 8.24 illustrates the use of "KVP_ACKNOWLEDGEMENT".

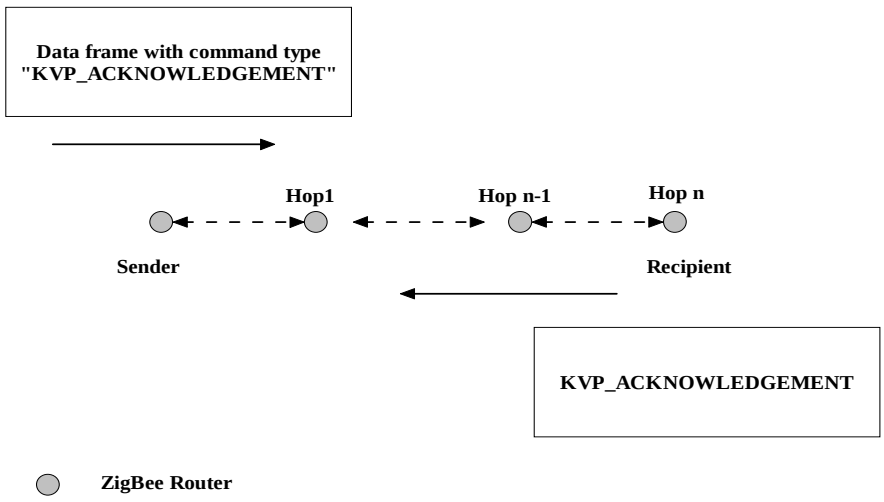

Figure 8.24 ZigBee data frame requesting KVP acknowledgement

In Figure 8.24, the sender puts the command "KVP_ACKNOWLEDGEMENT" into an outgoing data frame. On receipt of the data frame, the recipient will determine if the acknowledgement command is defined. If it is defined, the recipient will issue an acknowledgement and send it back to the sender through the multi-hop way.

A reasonable waiting period for a sender to check acknowledgement should be defined in the application layer. The waiting period is decided by the number of hops that the data frame and acknowledgement frame will experience. However, the route selection is invisible to the system developers. ZigBee protocol specifies a transmission parameter "RadiusCounter" to limit the maximum number of hops the router discovery operation should follow. Consequently, the number of hops experienced by actual data transmission will not exceed the value defined by "RadiusCounter". Therefore, $T_{Waiting}$ can be defined as follows:

$$T_{Waiting} \geq 2 \times T(L) \times RadiusCounter \tag{8.3}$$

where $T(L)$ derived from Equation (4.13) denotes the time needed to send a L bytes ZigBee packet from a ZigBee device to another ZigBee device. There are two possible reasons for the sender to lose acknowledgement: data frame is not successfully received by the recipient due to interference, or the acknowledgement frame is corrupted on the way to the sender due to interference as well. Therefore, a few settings should be made to help system analyze the situations.

When a sender is to send a data frame to the recipient, two elements should be put into the message: a unique packet sequence number and the number of retransmissions which have been tried till now. Under normal circumstance, the data packet should successfully reach the recipient, and the source device will receive an acknowledgement at the application layer after $T_{Waitting}$. On receipt of the data packet sent from the same source device with the same sequence number, the recipient will discard the duplicated one. However, the value of "number of tries" will be checked before discarding in order to determine if the packet is generated due to retransmission.

By analyzing the number of retries, the recipient can estimate that parts of the route employed by the sender to deliver the data frame might experience a difficulty. Assuming the factors of hardware failure and ZigBee signal collisions can be eliminated, the recipient can conclude that a possible interference area is emerging. When two conditions are satisfied: the number of retransmission for the same packet is over a threshold $N_{Threshold\_Retransmission}$, and the number of different packets sent from the same sender employing retransmissions is over threshold $N_{Threshold\_Packet}$, the recipient should try to contact the ZigBee PAN coordinator to switch channel in order to avoid the interference area. The value of $N_{Threshold\_Retransmission}$ and $N_{Threshold\_Packet}$ are related to application requirements. Recommended value for $N_{Threshold\_Retransmission}$ and $N_{Threshold\_Packet}$ in the SafetyNet system will be concluded in the corresponding evaluation tests. Figure 8.25 shows the flow chart for a sink node to follow when multiple retransmission from the same sender are detected.

In Figure 8.25, the sink node sets a counter for each sender. Its default value is 0. If a data packet is received from this sender, the content of the packet will be checked to determine is retransmission is employed. If retransmission is not used, the counter will be reset to 0. If retransmission is used, the sink will check if the retransmission times has exceeded threshold $N_{Threshold\_Retransmission}$. If it is not over the threshold, the counter will be reset to 0. If it is over threshold, the counter will be added by 1. If the counter value is greater than $N_{Threshold\_Packet}$, which means there are a certain number of different packets have employed retransmissions, the sink node will request the ZigBee coordinator to switch channel.

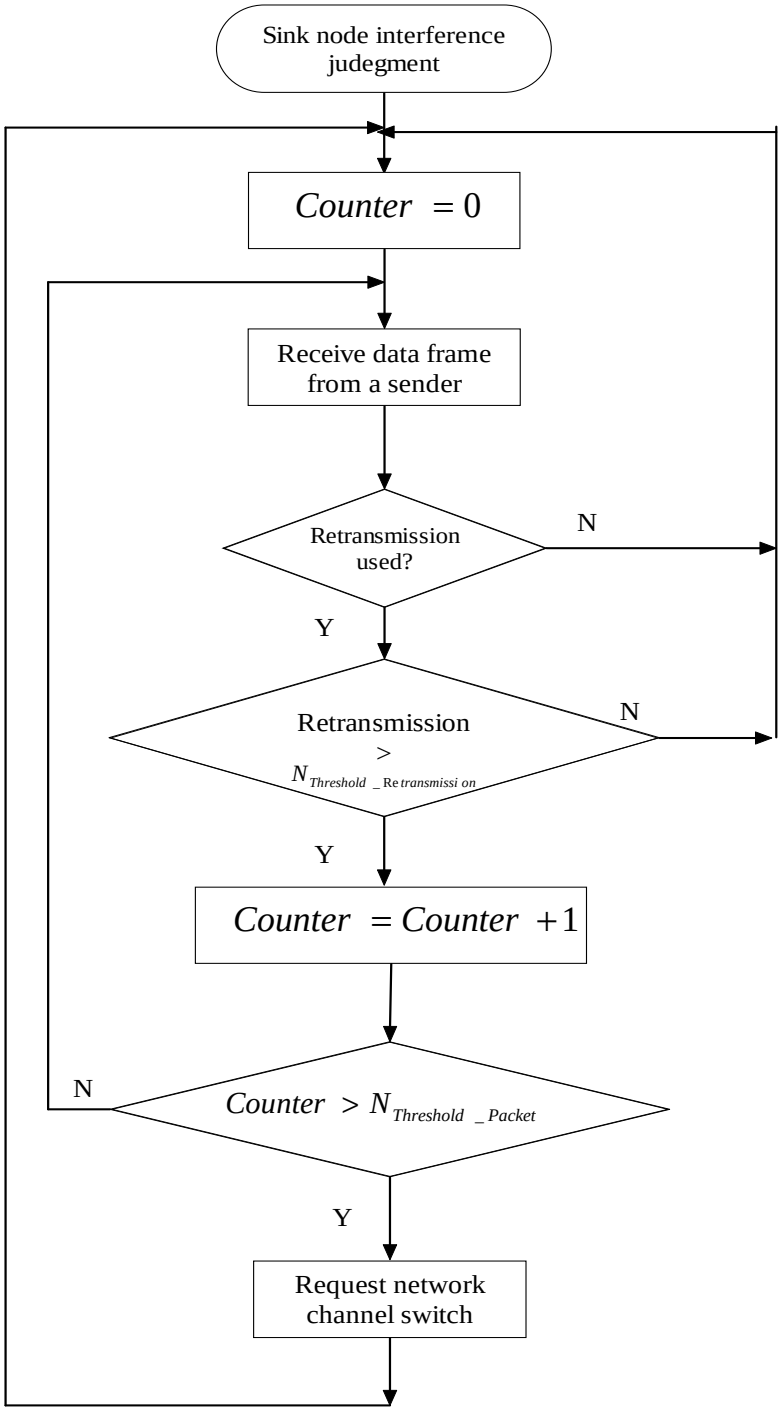

Figure 8.25 Flow chart of interference judgement on sink node when multiple retransmission are detected

Although the recipient can estimate the interference situation by analyzing the received data packet, it is insufficient as the recipient is probably unable to receive data frames when interference is too strong. Figure 8.26 illustrates a possible scenario for strong interference.

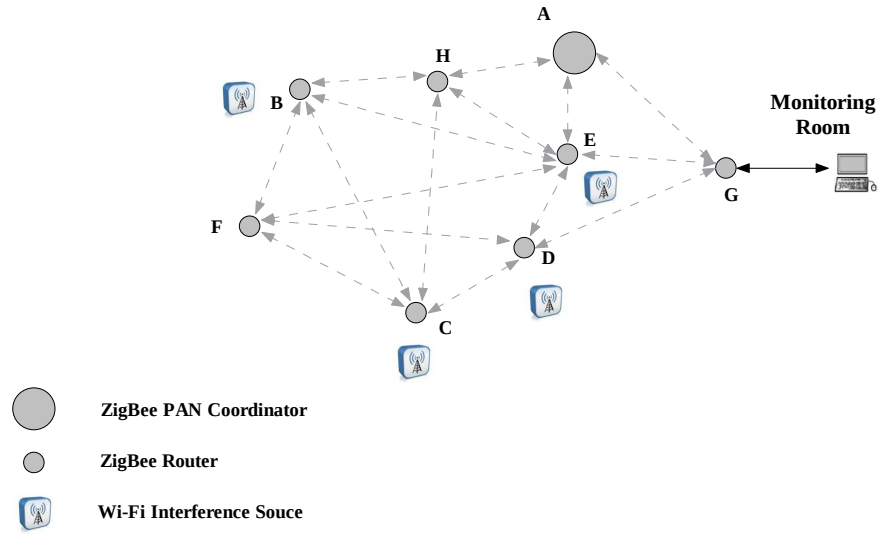

Figure 8.26 ZigBee network with strong interference

In Figure 8.26, ZigBee devices B, C, D, and E are all affected by Wi-Fi interference. Consequently, ZigBee device F will have no route available to send a data packet to device G located in a monitoring room. Under such a case, the only possible way for device G to sense the emergence of interference area is to build a record for each ZigBee sender to monitor the sensor readings' arrival rate. If a certain percentage of senders are lost within a certain period, device G should initiatively notify the ZigBee PAN coordinator to switch channel. The threshold $P_{Lost\_senders}$ for judging the percentage of lost senders should be defined according to the application requirements. Figure 8.27 shows the flow chart for a sink node to follow when some of senders are lost during a certain period.

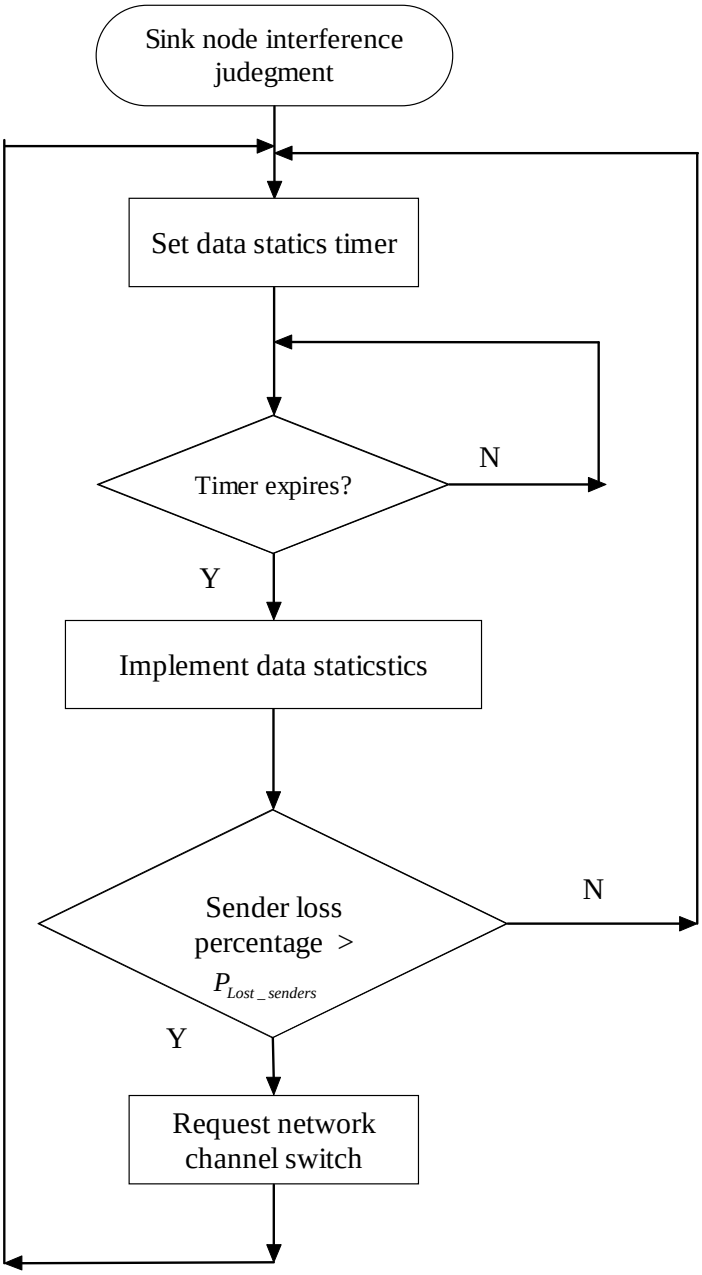

Figure 8.27 Flow chart of interference judgement on a sink node when some of senders are lost during a certain period

In Figure 8.27, the sink node sets a timer to implement a regular check. When timer expires, the sink node will check the number of received sensor readings before timer expiring. If a certain percentage (P_{Lost_Sender}) of sensor devices are found lost, the sink node will request the ZigBee coordinator for switch channel. If the percentage of lost sensor devices is smaller than $P_{Lost\_senders}$, the timer is reset. The determination of $P_{Lost\_senders}$ is decided according to the application requirements.

C) Channel switch

The ZigBee PAN coordinator executes the function of channel switch on the basis of global ZigBee network information. The information comes from the regular energy detection implemented by all available ZigBee routers not having been affected by interference. On the basis of a regular radio environment scan, an up-to-date radio environment information table is maintained on the central computer. A set of simple rules is proposed to assist the alternative channel selection by analyzing the recent energy detection results sent from the routers:

1. If the energy level of a channel is over threshold $E_{Threshold}$, the channel should be eliminated from available channel list.
2. If multiple channels remain in the available channel list, randomly select one channel as the alternative channel.
3. If there is no channel remaining in the available channel list, select the one with least energy level among all 16 channels.

By combining the detection strategies, the SafetyNet system can have a better performance when it is under dynamic interference.

8.7 Evaluation Tests

In the evaluation test, the sink node is also the ZigBee PAN coordinator for the convenience of operations. Three evaluation tests were implemented: data transmission in ZigBee network under interference without retransmission (test I), data transmission in ZigBee network under interference with a maximum 10 time retransmission (test II), and data transmission in ZigBee network under interference with proposed dynamic interference detection and mitigation strategies (test III).

8.7.1 Test I: Data Transmission in ZigBee WSN under Interference without Retransmission

Test I is for evaluating how serious a Wi-Fi interference source can affect ZigBee mesh network communications when the retransmission is not employed

at the ZigBee application layer. The employment of retransmission in a ZigBee application can be categorized into two types: automatic retransmission implemented by the ZigBee stack and manual retransmission implemented by the application layer. The ZigBee stack will automatically implement retransmission for a few times when the requested acknowledgements for the outgoing packets are not received within a certain period. However, this type of retransmission is managed by the encapsulated ZigBee stack and invisible to the application developers. Therefore, we choose to focus on the use of retransmission at the ZigBee application layer. Figure 8.28 illustrates the test set-up.

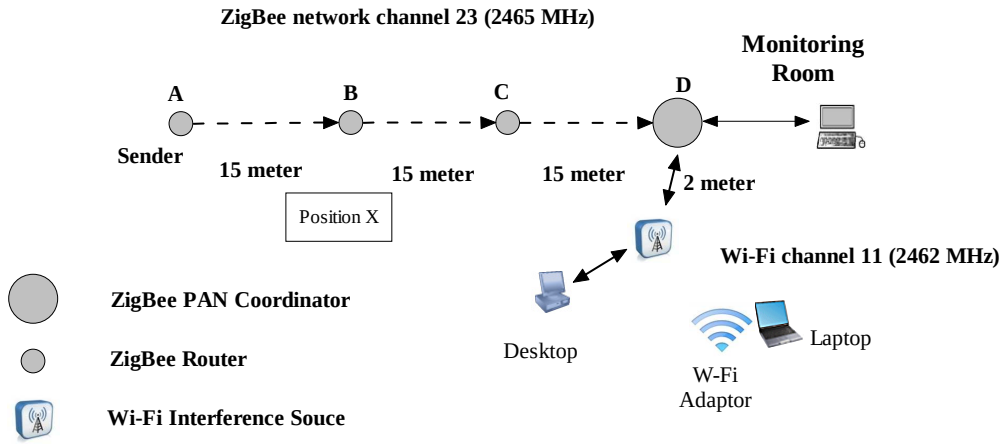

Figure 8.28 Test deployment in test I

In Figure 8.28, device A, B, and C are three ZigBee routers. They join the ZigBee network created by the ZigBee PAN coordinator. Device A sends a 50 byte length packet to the PAN coordinator every 10 seconds. A total of 20 packets are used in the test. The ZigBee stack automatically uses a routing protocol to select a suitable route for multi-hop data transmission. If the Wi-Fi interference source is located at position X which is near to device B, the next hop used by device A could be device C or the PAN coordinator as the effective communication range of ZigBee device is 50 meters within an indoor environment. Therefore, the Wi-Fi interference source is intentionally located close to device D in order to ensure that the receiver of the destination device of the ZigBee communication, the PAN coordinator, will be affected by the interference. The ZigBee network works at

channel 23 (2465 MHz), the Wi-Fi router works at channel 11 (2462 MHz) with data rate at 11 Mbps. The centre frequency offset between the two systems is 3 MHz. The distance between the Wi-Fi router and the PAN coordinator is 2 meters. A desktop connects to the Wi-Fi router and has a FTP server running on it. A laptop connects to the router through a Wi-Fi adaptor and downloads a big capacity file from FTP server. The Wi-Fi traffic is controlled by the FTP server. Table 8.4 summarizes the test I result.

Table 8.4 Test I result

Wi-Fi Traffic	**ZigBee Packet Success Rate**
100 KB/second	100%
200 KB/second	100%
300 KB/second	100%
400 KB/second	90%
500 KB/second	70%
600 KB/second	70%
700 KB/second	30%
No limitation	25%

In Table 8.4, the columns labelled “Wi-Fi Traffic” and “ZigBee Packet Success Rate” denote the generated Wi-Fi traffic on the Wi-Fi router and the ZigBee communication success rate measured on the ZigBee PAN coordinator. With the increment of the Wi-Fi traffic, the success rate of ZigBee communication decreases as expected.

8.7.2 Test II: Data Transmission in ZigBee WSN under Interference with Retransmission

The test II is for evaluating whether or not the employment of retransmission at the ZigBee application layer can be effective to the success rate of the ZigBee communications under interference. The test set-up is the same as

in test I (See Figure 8.28). Once the "KVP_ACKNOWLEDGEMENT" is not received by the sender, it will continue to send out packets till the maximum retry times is reached, or a "KVP_ACKNOWLEDGEMENT" is received. The retransmitted packets contain two parameters: sequence number, and number of retransmission which has been tried. The interval $T_{Waitting}$ for separating retransmissions is set at 500 millisecond, which is long enough to complete data transmissions and "KVP_ACKNOWLEDGEMENT" transmissions. In this test, the maximum retry number $N_{Retransmission}$ is set as 10, the number of ZigBee packets sent by device A is 20. Table 8.5 summarizes the test II results.

Table 8.5 Test II result

Wi-Fi Traffic	Total Packet	Received Packet	Total Retry Times	Average Retry Times	ZigBee Packet Success Rate
100 KB/second	20	20	0	0	100%
200 KB/second	20	20	0	0	100%
300 KB/second	20	20	0	0	100%
400 KB/second	20	20	9	0.45	100%
500 KB/second	20	20	12	0.6	100%
600 KB/second	20	20	15	0.75	100%
700 KB/second	20	17	29	1.7	85%
No limitation	20	17	50	2.9	85%

In Table 8.5, the columns labelled "Wi-Fi Traffic", "Total Packet", and "Received Packet" denote the generated Wi-Fi traffic on the Wi-Fi router, the total number of packets sent from the sender, and the total number of packets successfully received by the PAN coordinator respectively. The column labelled "Total Retry Times" denote the total retransmission times measured by counting the value of the parameter, "number of retransmission" contained in each received ZigBee packet on the PAN coordinator. The column "Average Retry Times" denotes the average retransmission times used to send a data packet from the

sender. The value in this column is derived from the columns “Received Packet” and “Total Retry Times”. For example, when the Wi-Fi traffic is 700 KB/second, the number of the received packet with unique sequence number on the PAN coordinator is 17, the total retry times obtained from this 17 packets are 29. Therefore, the average retry times are 29/17=1.7. Through test II, it is reasonable to conclude that parameter $N_{Threshold\_Retransmission}$ at 3 as the maximum average retransmission times measured in test II is 2.9. Therefore, if the PAN coordinator receives the packets containing the same sequence number from the same sender for more than 3 times, it can conclude that possibly interference is affecting the ZigBee network.

8.7.3 Test III: Data Transmission in ZigBee Network under Interference with Interference Detection and Mitigation Strategies

The aim of the test III is to evaluate if the ZigBee network can correctly respond to interference with the proposed strategies. When the PAN coordinator recognizes that the number of received data packets is less than the expected value, or a number of consecutive data retransmission is received, it can start a channel switch on the basis of regular energy detection executed by the ZigBee routers in the network. Once the channel switch is successfully completed, the success rate of ZigBee communication will become normal. Whether or not the PAN coordinator can select the most suitable alternative channel is the focus in test III. All routers implement energy detection every 5 minutes. Figure 8.29 illustrates the test III set-up layout.

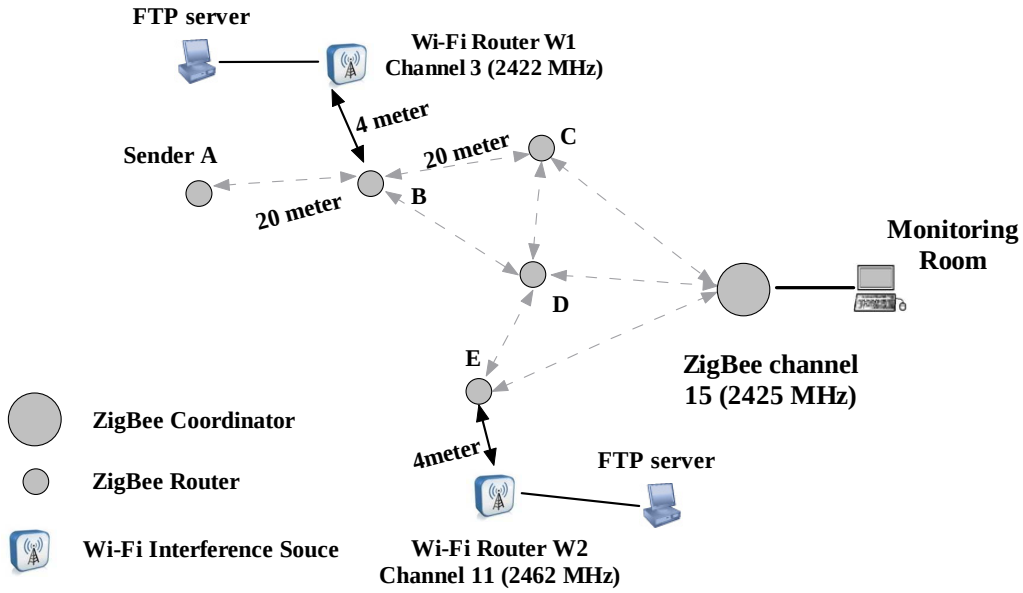

Figure 8.29 Test III deployment

In Figure 8.29, ZigBee router A acts as a sender to send data packets to the PAN coordinator. The ZigBee network works at channel 15 (2425 MHz). Two Wi-Fi interference sources, W1 and W2, are located 4 meters away from the vicinity of ZigBee routers B and E. W1works at Wi-Fi channel 3 (2422 MHz) and W2 works at channel 11 (2462 MHz). As the distance between the ZigBee router A and router C is 40 meters which is close to the maximum communication range, the data transmission issued from device A will employ device B as the next hop as it has stronger signal strength compared with device C. Other ZigBee devices are all out of the communication range of device A (It was tested and confirmed before implementing test III).

At the beginning of test III, ZigBee device A continued to send a data packet to the PAN coordinator every 10 seconds. Meanwhile, the FTP server running on the computer which connected to the Wi-Fi router W2 started to generate traffic at 700 KB/second. Since it worked at Wi-Fi channel 11, whose centre frequency was 37 MHz away from the frequency used by the ZigBee network, it did not affect the ZigBee network communication. After 10 minutes, all ZigBee routers should have reported the energy detection result to the PAN coordinator at least twice. After that the FTP server running on the computer which connected to W1 started to generate traffic at 700KB/second. Half a minute

later, the PAN coordinator detected that three different packets have employed more than 3 times retransmissions. Then the PAN coordinator checked the energy detection results. ZigBee routers C and D reported that all channels were available. However, devices B and E reported that some channels were marked as bad channels. Table 8.6 and 8.7 show the energy detection results obtained from device B and E.

Table 8.6 Energy detection result from device B

ZigBee Channel (Centre Frequency)	11 (2405 MHz)	12 (2410 MHz)	13 (2415 MHz)	14 (2420 MHz)	15 (2425 MHz)	16 (2430 MHz)	17 (2435 MHz)
Measured Energy (dBm)	-60	**-55**	**-38**	**-30**	**-30**	**-47**	-61

18 (2440 MHz)	19 (2445 MHz)	20 (2450 MHz)	21 (2455 MHz)	22 (2460 MHz)	23 (2465 MHz)	24 (2470 MHz)	25 (2475 MHz)	26 (2480 MHz)
-61	-65	-65	-74	-76	-82	-86	-96	-98

Table 8.7 Energy detection result from device E

ZigBee Channel (Centre Frequency)	11 (2405 MHz)	12 (2410 MHz)	13 (2415 MHz)	14 (2420 MHz)	15 (2425 MHz)	16 (2430 MHz)	17 (2435 MHz)
Measured Energy (dBm)	-96	-86	-82	-80	-80	-79	-82

18 (2440 MHz)	19 (2445 MHz)	20 (2450 MHz)	21 (2455 MHz)	22 (2460 MHz)	23 (2465 MHz)	24 (2470 MHz)	25 (2475 MHz)	26 (2480 MHz)
-74	-63	-63	**-32**	**-20**	**-20**	**-36**	-59	-61

In Table 8.6, row labelled “Measured Energy” indicates the energy level detected by router B on each ZigBee channel. The channels marked with a grey colour means they are unsuitable for ZigBee network communications. Since the Wi-Fi interference source located in the vicinity of device B works on channel 3 whose centre frequency is 2422 MHz, ZigBee channels unsuitable for communications are all found close to this frequency. Similar to Table 8.6, Table 8.7 is the result obtained from router E. Because the Wi-Fi interference close to device E works on Wi-Fi channel 11 (2462 MHz), the marked bad ZigBee channels are all around this frequency. Through analyzing the energy detection

results, the PAN coordinator can easily find out a suitable ZigBee channel from those channels not marked by gray colour. By using the proposed rules in Section 8.6.4, ZigBee channels 11, 17, 18, 19, 20, 25, 26 are all potential alternatives.

8.8 Discussion

The proposed interference detection and mitigation strategies consist of two aspects: strategies for static interference and strategies for dynamic interference.

The strategies designed for static interference focuses on the reasonable arrangements for deploying wireless systems. Installing a ZigBee WSN inside a building to monitor environment changes usually requires hundreds of sensor nodes to be involved. As the increasing usage of Wi-Fi systems in commercial office areas for convenient network access service, the statically deployed Wi-Fi access points or Wi-Fi routers become serious interference sources for any ZigBee WSN. However, static Wi-Fi access points or Wi-Fi routers can only affect a limited area due to wireless signal attenuation. Our strategies help the ZigBee WSNs locate the range of the interference areas, and then utilize physical distance separation and frequency separation to avoid interference. Since both Wi-Fi networks and ZigBee WSN are static after first installation, these measures are effective and easy to use.

The strategies designed for dynamic interference focuses on the analysis of events caused by interference and the design of a reasonable channel switch algorithm. Dynamic interference is the most serious interference source for any kind of wireless system as it is unpredictable and uncontrollable. The current method available to detect the existence of dynamic interference is to monitor the specified events relating to dynamic interference. In the SafetyNet case, the events are multiple data retransmissions, i.e. some ZigBee devices failed to send sensor readings and then resend them within a certain period. As the ZigBee mesh network is distributed inside the building, the ZigBee coordinator is unable to detect the position and strength of dynamic interference. Therefore, we propose dynamic energy detection, data retransmission monitoring, and percentage of lost ZigBee devices within a certain period, and channel switch to cooperate together

to detect and mitigate effect caused by dynamic interference in ZigBee WSN. It is difficult to evaluate the use of these strategies by numerical metrics. For example, for a ZigBee WSN affected by multiple dynamic interference sources, many other ZigBee devices are possibly to be interfered as well. Under such circumstance, monitoring the number of retransmissions might be less effective as those interfered devices are unable to complete data transmission successfully. Then the ZigBee PAN coordinator will not be sensitive to the existence of interference until a certain percentage of ZigBee devices are not recorded within a certain period. However, the threshold used to determine if such percentage is meaningful is purely dependent on user requirements. Other parameters proposed in the strategies have similar situations.

The SafetyNet system is designed for monitoring building environment changes, and provides real-time sensor information to users who are demanding such information. It can be used under either normal circumstance or in an emergency situation. However, when an emergency happens, the main power of the building is usually cut off automatically. Therefore, interference caused by Wi-Fi networks or similar wireless techniques are not analyzed in such a case.

8.9 Summary

The SafetyNet system is a comprehensive application which requires consideration for many practical factors, including static interference source, dynamic interference source, system requirements, etc. The proposed interference detection and mitigation strategies in this chapter fully consider the interference characteristics. Through arranging network deployment, enabling dynamic interference energy detection, and setting up corresponding adjustments, the interference inside a ZigBee WSN deployed within the building environment can be properly monitored, discovered, and responded to. The contribution in this chapter is to propose complete and feasible strategies for system developers' reference when they are designing WSNs which possibly encounters interference during the operations.

Chapter 9 Conclusions and Future Work

9.1 Contributions and Future Work

This thesis aims to enhance the operational capability of wireless sensor networks under interference. The research tasks of this thesis are to investigate the basis of interference, and design approaches to help wireless sensor networks avoid interference, or mitigate the effect of interference. The main contributions and findings from the research are listed below:

1. **The design of a consecutive data transmission mechanism to improve the wireless sensor network's capability to maintain communication without frequently changing network channel.**

Switching network channel is usually employed by wireless systems to avoid interference. However, if the whole frequency band is being interfered, the capability to sustain network communications via the currently employed channel is essential. Through proper control over the data transmission with a suitable interval, a consecutive retransmission mechanism can significantly increase the success rate of a wireless sensor network communication since the interval between interfering packets can be utilized to enable the completion of desired packet transmission. For particular applications such as home automation and industrial control, an extremely low duty cycle is usually employed. By applying consecutive data transmission, the network connectivity can be maintained when it is under interference. In the evaluation test, the wireless sensor network

communication can achieve almost 100% success rate until the interference reaches saturation.

2. The design of dynamic energy detection approach to help wireless sensor network device to estimate the status of interference and accordingly adjust transmission parameters to achieve optimized communication effectiveness.

During the period of interference, the affected wireless sensor devices are unable to recognize the type of interferers due to the different modulation/demodulation schemes. However, the energy activities generated by interferers can be captured by wireless sensor devices utilizing an energy detection function. This approach makes the wireless sensor device detect the idle slots existing between interfering packets, and identify an appropriate packet length with which the wireless sensor network communications can have a higher success rate. This approach is useful for applications that require consecutive data over a short period (e.g. computer mouse, toy controller, motion sensor). The evaluation test shows that energy detection can effectively express the change of interference traffic and provide wireless sensor devices with an estimation of packet length.

3. The design of an approach to enable reliable data transmission in an ad-hoc wireless sensor network.

The communication in an ad-hoc network relies on multi-hop transmission since the source device and destination device are usually not within effective radio communication range of each other. Interference which happens to any hop on the route from the source device to the destination can lead to the failure of the whole transmission. When interference occurs in an ad-hoc wireless sensor network, the interference effect will be undetectable by a single wireless sensor device. Consequently, the final data integrity will be affected. The proposed approach adds proper control to the MAC layer of a wireless sensor network to monitor the failure of data transmission, and uses redundancy to assist the implementation of data recovery. According to the calculation for the evaluation tests, up to 42% of the lost packet can be possibly recovered under certain conditions.

4. Implementation of the consecutive data transmission mechanism in a home automation application.

During the development of a home automation system, the proposed consecutive data transmission mechanism is adopted in order to improve the short-range wireless home automation network's capability to coexist with wireless interference within the domestic home environment. The implementation of strategy significantly increases the success rate of a wireless sensor network communications whilst the energy consumption is reasonably controlled.

5. A complete analysis and interference detection and mitigation strategies design in a practical WSN-based large-scale building monitoring system.

In the application of a building environment monitoring network, the widely distributed wireless sensor network dramatically increases the difficulty to design an effective strategy to sense the emergence of interference. A complete analysis was proposed for interference in such a wireless sensor network by starting from static installation to dynamic situation changes. The designed strategies fully consider the possible situations caused by unexpected interference source and make proper response according to interference situation. The process of analyzing interference and designing interference mitigation strategies can also be used by researchers to implement system design in similar areas.

In summary, this thesis has achieved all of the proposed objectives described in Chapter 1. Future work in studying interference in wireless sensor networks should focus on enhancing the analysis of interference characteristics in different scenarios (e.g. multiple interferers simultaneously affect the operations of WSNs), and designing approaches with more intelligence and efficiency for various applications. An optimal solution for deploying a large-scale WSN employing hundreds of wireless sensor nodes in a complex indoor environment and achieving a minimum interference and best performance are also particularly interesting in future study.

9.2 Summary

The concept of a sensor network is something that provides the end users with the capability to obtain environment information. The rapid development of microelectronic techniques in recent years enables the emergence of wireless sensors, which can be powered by battery and easily deployed without any restriction imposed by the need for cables. Typical applications requiring the use of wireless sensor networks include a building environment monitoring system, home automation system, location tracking system and asset management. The deployment of wireless sensor networks involving no fixed infrastructure can achieve the concept of "ubiquitous computation" which significantly improves the capability for human being to interact with the physical environment. However, communications over wireless signals are usually easily subject to interference as the communication medium, air, is available to potential wireless interferers and consequently such systems have no effective protection against interference unlike wired system. It is the major problem which obstructs the development of wireless sensor networks.

Recent research has developed theoretical analysis and primary tests to identify the factors that can cause interference on the operations of wireless sensor networks. Through the design and implementation of interference mitigation strategies, including keeping physical and frequency separations between the victim system and interferers, employing effective routing protocols, and allowing dynamic frequency agility etc., the possibility to overcome interference under certain conditions has been demonstrated. The analysis and approaches presented in this thesis are mainly based on experimental work and practical applications.

References

[1] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. & Cyirci, E.,"A Survey on Sensor Networks", *IEEE Communications Magazine*, Vol. 40, No. 8, pp. 102-114, 2002.

[2] Al-Ai, A.R., & Al-Rousan, M., "Java-Based Home Automation System", *IEEE Transactions on Consumer Electronics*, Vol. 50, No. 2, pp. 498 - 504, 2004.

[3] Baronti, P., Pillai, P., Chook, V.W.C., Chessa, S., Gotta, A., & Hu, Y.F., "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards", *Computer Communication*, Vol. 30, No. 7, pp. 1655-1695, 2007.

[4] Benini, L., Farella, E., & Guiducci, C., "Wireless sensor networks: Enabling technology for ambient intelligence", *Microelectronics Journal*, Vol. 37,No. 12,pp.1639– 1649, 2006.

[5] Beyer, S., Jaehne, R., Kluge, W., & Eggert, D., "A 2.4 GHz direct modulated 0.18um CMOS IEEE 802.15.4 compliant Transmitter for ZigBee", *IEEE Custom Integrated Circuits Conference*, pp.121 – 124, 2006.

[6] Bharathidasan, A., & Ponduru, V.A.S., "Sensor Networks: An Overview", *IEEE Potentials*, Vol. 22, pp.20–23, 2003.

[7] Callaway, E., Gorday, P., Hester, L., Gutierrez, J.A., Naeve, M., Heile,B., & Bahl, V., "Home Networking with IEEE 802.15.4: A Developing Standard for Low-Rate Wireless Personal Area Network", *IEEE Communications Magazine*, Vol. 40, No. 8, pp.70-77, 2002.

[8] Cardei, M., & Wu, J., "Coverage in Wireless Sensor Networks", *Handbook of Sensor Networks*, CRC Press, 2004.

[9] Cardei, M., and Wu, J., "Energy-efficient coverage problems in wireless ad-hoc sensor networks", *Computer Communications*, Vol. 29, No. 4, pp.413–420, 2006.

[10] CC2420 Data Sheet, 2007.

http://focus.ti.com/docs/prod/folders/print/cc2420.html

[11] Chandra, P., Dobkin, D.M., Bensky, D., Olexa, R., Lide, D., & Dowla, F., "WIRELESS NETWORKING, know it all", *Newnes*, 2007.

[12] Chiasserini, C.F., Rao, R.R., & Wlans. I., "Coexistence Mechanism for Interference Mitigation in the 2.4 0GHz ISM band", *IEEE Transactions on Wireless Communication*, Vol. 2, No. 5, pp. 590-598, 2002.

[13] Reinisch, C., Kastner, W., Neugschwandtner, G., & Granzer, W., "Wireless Technologies in Home and Building Automation", *Industrial Informatics, 5th IEEE Interference Conference*, pp. 93-98, 2007.

[14] Coskun, I., & Ardam, H., "A Remote Controller for Home and Office Appliances by Telephone", *IEEETransactions on Consumer Electron*, Vol. 44, No. 4, pp. 1291-1297, 1998.

[15] Cuomo, F., Luna, S.D., Monaco, U., and Melodia, T., "Routing in ZigBee: benefits from exploiting the IEEE 802.15.4 association tree", *IEEE International Conference on Communications*, pp.3271–3276, 2007.

[16] Demirkol,I., Ersoy,c., & Alagöz, F.,"MAC Protocols for Wireless Sensor Networks: a Survey", *IEEE Communications Magazine*, Vol. 44, No. 4, pp. 115–121, 2006.

[17] Elnahrawy, E., "Research Direction in Sensor Data Streams: Solutions and Challenges", *DCIS Technical Report DCIS-TR-527*, Rutgers University, 2003.

[18] Ergen, S.C.,"ZigBee/IEEE 802.15.4 Summary", Research Paper, University of Berkeley, pp.1-3, 2004, http://www.cs.wisc.edu/~suman/courses/838/papers/zigbee.pdf

[19] Fakatselis, J., "Processing Gain for Direct Sequence Spread Spectrum Communication Systems and PRISM", *Harris Semiconductor application note*, 1996.

[20] Fakatselis, J., "Processing Gain in Spread Spectrum Signals", *Harris Semiconductor application note*, 1998.

[21] Foschini, G.J., & Gans, M.J., "On Limits of Wireless Communications in a Fading Environment when Using Multiple Antennas", *Wireless Personal Communications: An International Journal*, Vol 6, No. 3, pp. 311–335, 1998.

[22] Freescale IEEE 802.15.4/ZigBee Software Selector Guide, 2007.

[23] Gast, M., "802.11® Wireless Networks: The Definitive Guide", O'Reilly, 2002.

[24] Gill,K., "Enhancing the Security of Wireless Sensor Network based Home Automation Systems", 2009.
https://dspace.lboro.ac.uk/dspace-jspui/handle/2134/5951

[25] Golmie, N., “Coexistence in Wireless Networks Challenges and system-level solutions in the unlicensed bands”, *Cambridge University Press*, Cambridge, 2006.

[26] Golmie, N., Cypher, D., & Rebala, O., “Performance Analysis of Low Rate Wireless Technologies for Medical Applications”, *Computer Communications*, Vol 28, No. 7, pp. 1266–1275, 2005.

[27] Gomez, C., Salvatella, P., Alonso, O., & Paradells, J., “Adapting AODV for IEEE 802.15.4 Mesh Sensor Networks: Theoretical Discussion and Performance Evaluation in a Real Environmnet”, *Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 159–170, 2006.

[28] Gutierrez, J.A., Callaway, E.H., & Barrett, R.L., “Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensors with IEEE 802.15.4", *IEEE Press*, 2003.

[29] Heusse, M., Rousseau, F., Berger-Sabbatel, G., & Duda, A., "Performance anomaly of 802.11b", Proceedings *of Twenty-Second Annual Joint Conference of the IEEE Computer and Communications (INFOCOM)*, Vol.2, pp. 836-843, 2003.

[30] Howell, R., “An Update on Short Range Wireless Technology”, *Technology Report from High Frequency Electronic*, Summit Technical Media, pp. 27-30, 2009.

[31] Howitt, I., & Gutierrez, J.A., “IEEE 802.15.4 Low Rate-Wireless Personal Network Coexistence Issues”, *IEEE Wireless Communications and Networking Conference (WCNC)*, Vol 4, pp. 1481–1486, 2003.

[32] Hwang, K., Yeo, S.S., & Park, J.H., “Adaptive Multi-Channel Utilization Scheme for Coexistence of IEEE 802.15.4 LR-WPAN with Other

Interfering Systems”, *2009 11th IEEE International Conference on High Performance Computing and Communications*, pp. 297-304, 2009.

[33] IEEE Std 802.15.1, "IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements Part 15.1: Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs)", 2005.

[34] IEEE Standard 802.11, 2007, “IEEE Standard for Information technology —Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.

[35] IEEE Std 802.15.2, “IEEE Recommended Practice for Information technology —Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands”, IEEE Computer Society, 2003.

[36] IEEE Std802.11b-1999, “Supplement to IEEE Standard for Information technology— Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band”, R2003.

[37] IEEE Std 802.15.4, 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 (LR-WPANs), 2003.

[38] IndeedNET, Integration and demonstration of energy efficient dwelling networks, Loughborough University, 2007 www.indeednet.org,

[39] Jennic Application Note, “Co-existence of IEEE 802.15.4 at 2.4 GHz”, 2008.

[40] Jennic Press Information: Jennic reduces bill of material cost for ZigBee/IEEE 802.15.4 reference designs to under US$5, Jennic 2007, http://www.jennic.com/files/press_releases/Sub_$5_module_28_Mar_07_2_.pdf

[41] Jennic Press Information: Jennic’s new single-chip wireless microcontroller sets benchmarks for ZigBee PRO and IEEE 80.15.4 wireless mesh networking, Jennic 2009.
http://www.jennic.com/files/press_releases/JN5148_PR_Mar_09.pdf

[42] JN5139 Data Sheet, 2009.
http://www.jennic.com/download_file.php?supportFile=JN-DS-JN5139MO-1v5.pdf

[43] Kang, M.S., Chong, J.W., Hyun, H., Kim, S.M., Jung, B.H., & Sung D.K., “Adaptive Interference –Aware Multi-Channel Clustering Algorithm in a ZigBee Network in the Presence of WLAN Interference”, *IEEE International Symposium on Wireless Pervasive Computing*, 2007.

[44] Kim, S.J., Seo, J.H., Krishna, J., & Kim, S.J., “Wireless Sensor Network based Asset Tracking Service”, *Proceedings of Conference on Technology Management for a Sustainable Economy (PICMET)*, 2008.

[45] Kinney, P., “ZigBee Technology: Wireless Control that Simply Works”, *Communications Design Conference*, 2003.

[46] Koubaa, A., Cunha, A., Alves, M., & Tovar, E.,“TDBS: a time division beacon scheduling mechanism for ZigBee cluster-tree wireless sensor networks”, *Real-Time System*, Vol. 40, No. 3,pp. 321–354, 2007.

[47] Koubaa. A., Alves. M. & Tovar. E., “IEEE 802.15.4: a wireless communication technology for large-scale ubiquitous computing applications”, *Proceeding of Conference on Mobile and Ubiquitous Systems (CSMU 2006)*, Guimarães, 2006.

[48] Krishnamurthy, V., & Sazonov, E., “Reservation-based protocol for monitoring applications using IEEE 802.15.4 sensor networks”, *International Journal of Sensor Networks*, Vol. 4, No. 3, pp. 155 –171, 2008.

[49] Hwang, L.J., Sheu, S.T., Shih,Y.Y., & Cheng,Y.C., “Grouping Strategy for Solving Hidden Node Problem in IEEE 802.15.4 LR-WPAN”, *Proceedings of First IEEE international conference on Wireless Internet (WICON)*, pp. 26-32, 2005.

[50] Latre, B., Mil, P.D., Moerman, I., Dhoedt, B., Demeester, P., & Dierdonck,N.V., “Throughput and Delay Analysis of Unslotted IEEE 802.15.4”, *Journal of Networks*, Vol. 1, No. 1, pp. 20-28, 2006.

[51] Lewis F., “Wireless sensor networks”, *Smart environments: technologies, protocols, and applications*, 2004.

[52] Lu,G., Krishnamachari,B., & Raghavendra, C S., “Performance Evaluation of the IEEE 802.15.4 MAC for Low-Rate Low-Power Wireless Networks”, *Proceedings of IEEE International Conference on Performance, Computing, and Communications*, pp. 701 - 706, 2004.

[53] Medepalli, K., Gopalakrishnan, P., Famolari, D., & Kodama, T., “Voice Capacity of IEEE 802.11b, 802.11a and 802.11g Wireless LANs”, *Proceedings of IEEE Globe Telecommunications Conference*, Vol. 3, pp. 1549–1553, 2004.

[54] Mishra, A., Shin, M., & Arbaugh, W., “An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process”, *ACM SIGCOMM Computer Communication Review, Vol. 33*, No. 2, pp. 93–102, 2003.

[55] Molisch, A.F., “Wireless Communications”, *John Wiley & Sons Ltd*, 2005

[56] Musaloiu-E.R., Liang,C.J., & Terzis.A., "Koala: Ultra-low power data retrieval in wireless sensor networks", *Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN)*, 2008.

[57] OPNET Technologies, Inc., Opnet Modeler Wireless Suite, 2010 http://www.opnet.com

[58] Pahlavan, K., & Levesque, A.H., “Wireless Information Networks 2nd Edition”, *John Wiley & Sons Ltd*, 2005.

[59] Park, S.H., Won, S.H., Lee, J.B., & Kim, S.W., “Smart home-digitally engineered domestic life”, *Personal and Ubiquitous Computing*, Vol. 7, No. 3-4 , pp. 189-196, 2003.

[60] Petrova, M., Riihijarvi, J., Mahonen, P., & Labella, S., "Performance Study of IEEE 802.15.4 Using Measurements and Simulations", *Wireless Communications and Networking Conference (WCNC)*, pp. 487–492, 2006.

[61] Pollin, S., Ergen, M., Dejonghe, A., Perre, L.V.D., Catthoor, F., Moerman, I., & Bahai, A., "Distributed cognitive coexistence of 802.15.4 with 802.11", *International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, pp. 1–5, 2007.

[62] Prasad, R., & Gavrilovska, L., "Research Challenges for Wireless Personal Area Networks" *Proceedings of 3rd International Conference on Information, Communications and Signal Processing (ICICS)*, 2001.

[63] Qi, H., Kuruganti, P.T., & Xu, Y.Y., "The Development of Localized Algorithm in Wireless Sensor Networks", *Sensors*, Vol. 2, pp. 286–293, 2002.

[64] Rodriguez, R., "MC1319x Coexistence", *Freescale Semiconductor Application Note*, AN2935, 2005.

[65] Ross, J., "The book of Wi-Fi: install, configure, and use 802.11b wireless networking", *No Starch Press*, 2003.

[66] SafetyNet, Secure Adhoc Fire & Emergency safety NETwork, Loughborough University, 2006.

[67] Schurgers, C., & Srivastava, M.B., "Energy Efficient Routing Wireless Sensor Networks", *Military Communications Conference on Communications for Network-Centric Operations: Creating the Information Force*, Vol. 1, pp. 357 - 361, 2001.

[68] Shin, S.Y., Park, H.S., & Kwon, W.H., "Mutual interference analysis of IEEE 802.15.4 and IEEE 802.11b", *Computer Networks*, Vol. 51, No. 12, pp. 3338–3353, 2007.

[69] Shuaib, K., Alnuaimi, M., Boulmalf, M., Jawhar, I., Sallabi, F., & Lakas, A., "Performance Evaluation of IEEE 802.15.4: Experimental and Simulation Results", *Journal of Communications*, Vol. 2, No. 4, pp. 29-37, 2007.

[70] Shwehdi, M.H., & Khan, A.Z., "A Power Line Data Communication Interface Using Spread Spectrum Technology in Home Automation",

IEEE Transaction on Power Delivery, Vol. 11, No. 3, pp. 1232-1237, 1996.

[71] Sikora, A., & Groza, V.F., "Coexistence of IEEE 802.15.4 with other Systems in the 2.4 GHz-ISM-Band", *IEEE Instrumentation and Measurement Technology Conference (IMTC)*, pp. 1786 - 1791, 2005.

[72] So, J., & Vaidya, N., "Multi-Channel MAC for Ad Hoc Networks: Handling Multi-Channel Hidden Terminals Using A Single Transceiver", *Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing*, pp. 222–233, 2004.

[73] Sriskanthan, N., Tan, F., & Karande, A., "Bluetooth based home automation system", *Journal of Microprocessors and Microsystems*, Vol. 26, No. 6, pp.281-289, 2002.

[74] Tang, J., Xue, G.L., & Chandler, C., "Interference-aware routing and bandwidth allocation for QoS provisioning in multihop wireless networks", *Wireless Communications and Mobile Computing Journal*, Vol. 5, No.8, pp.933–943, 2005.

[75] Thonet, G., Jacquin, P.A., & Colle, P., "ZigBee-WiFi Coexistence", *Schneider Electric White Paper and Test Report*, 2008.

[76] Tidd, J., "Development of novel products through intraorganizational and interorganizational networks: the case of home automation, *Journal of product Innovation Management*, Vol 22, No. 4, pp. 307-23, 1995.

[77] Vieira, M.A.M., Jr, C.N.C., Junior, D.C.D.S., and Mata, J.N.D., "Survey on Wireless Network Devices", *Proceedings of IEEE Conference on Emerging Technologies and Factory Automation*, Vol. 1, pp. 537 - 544, 2003.

[78] Wagenknecht, G., Anwander, M., Braun, T., Staub, T., Matheka, J., & Morgenthaler, S., "MARWIS: A Management Architecture for Heterogeneous Wireless Sensor Networks", *Wired/Wireless Internet Communications (WWIC)*, pp. 177-188, 2008.

[79] Webb, W., "Wireless Communications: The Furture", *John Wiley & Sons Ltd*, 2007.

[80] Weiser, M., "Some Computer Science Issues in Ubiquitous Computing", *Communications of the ACM*, Vol. 36, No. 7, pp. 75-84, 1993.

[81] Wheeler, A., “Commercial Applications of Wireless Sensor Networks Using ZigBee”, *IEEE Communications Magazine*, Vol. 45, No. 4, pp.70 – 77, 2007.

[82] Willig, A., Matheus, K., & Wolisz, A., “Wireless Technology in Industrial Networks”, *Proceedings of the IEEE*, Vol. 93, No. 6, pp. 1130-1151, 2005

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

[84] Wu, J., & Stojmenovic, I., “Ad Hoc Networks”, *IEEE Computer Society*, Vol. 37, No. 2, pp. 29-32, 2004.

[85] Xiao, Y., & Rosdahl, J., “Throughput and Delay Limits of IEEE 802.11”, *IEEE Communications Letters*, Vol. 6, No. 8, pp. 355–357, 2002.

[86] XBee Chip Data sheet, 2008. http://www.digi.com/pdf/ds_xbeemultipointmodules.pdf

[87] Yang, S., & Frederick, P., “SafetyNET: A Wireless Sensor Network for Fire Protection and Emergency Response”, *Measurement and Control*, Vol. 37, No. 9, pp. 218-219, 2006.

[88] Yang, L., Yang, S. and Yao, F., "Safety and Security of Remote Monitoring and Control of Intelligence Home Environment", *Proceedings of 2006 IEEE International Conference on Systems, Man, and Cybernetics (IEEE SMC 2006)*, Taipei, Taiwan, pp 1150-1153, 2006.

[89] Yao, F., Xia, B.K., and Yang, S.H., “A ZigBee Based Home Automation System Design and Implementation”, *The Journal of the Institute of Measurement and Control*, Vol. 41, No. 10, pp. 310-314, 2008.

[90] Yao, Y., & Gehrke, J., “The Cougar Approach to In-Network Query Processing in Sensor Networks” *ACM SIGMOD Record*, Vol. 31, No. 3, pp. 9–18, 2002.

[91] Ye,W., Heidemann, J.,& Estrin, D., "An energy-efficient MAC protocol for wireless sensor networks", *Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies*, Vol. 3, pp.1567-1576, 2002.

[92] Yilmaz, O., “Propagation Simulation For Outdoor Wireless Communications in Urban Areas”, 2002.

www.ee.bilkent.edu.tr/grad/ms-thesis/yilmaz-ms.pdf

[93] Yuan, W., Wang, X., & Linnartz, J.P.M.G., "A Coexistence Model of IEEE 802.15.4 and IEEE 802.11b/g", *14th IEEE Symposium on Communications and Vehicular Technology in the Benelux*, 2007.

[94] Zheng, J., & Lee, M.J., "Will IEEE 802.15.4 make ubiquitous networking a reality?: A discussion on a potential low power, low bit rate standard," *IEEE Communications Magazine*, Vol. 42, No. 6, pp. 140–146, 2004.

[95] Zhou, G., He, T., Stankovic, J.A., & Abdelzaher, T., "RID: Radio Interference Detection in Wireless Sensor Networks", *Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies*, Vol. 2, pp. 891 – 901, 2005.

[96] ZigBee Alliance, "ZigBee and Wireless Radio Frequency Coexistence", 2007.
http://www.zigbee.org

[97] ZigBee Alliance, ZigBee Specification 2004, ZigBee Alliance, http://www.zigbee.org, 2005.