



BOURNEMOUTH UNIVERSITY

Wireless Remote Patient Monitoring on General Hospital Wards

Yuanlong Liu

A thesis submitted in partial fulfillment of the requirements of
Bournemouth University for degree of
DOCTOR OF PHILOSOPHY

September 2010

© Copyright by Yuanlong Liu 2010

All Rights Reserved

Dedication

This thesis is dedicated to my parents, Piyao Liu and Yumei Liu, who have supported me all the way since the beginning of my studies.

Abstract

A novel approach which has potential to improve quality of patient care on general hospital wards is proposed. Patient care is a labour-intensive task that requires high input of human resources. A Remote Patient Monitoring (RPM) system is proposed which can go some way towards improving patient monitoring on general hospital wards. In this system vital signs are gathered from patients and sent to a control unit for centralized monitoring. The RPM system can complement the role of nurses in monitoring patients' vital signs. They will be able to focus on holistic needs of patients thereby providing better personal care.

Wireless network technologies, ZigBee and Wi-Fi, are utilized for transmission of vital signs in the proposed RPM system. They provide flexibility and mobility to patients. A prototype system for RPM is designed and simulated. The results illustrated the capability, suitability and limitation of the chosen technology.

Acknowledgements

First and foremost I want to thank my supervisor, Dr. Reza Sahandi, whose encouragement, guidance and support enabled me to develop a good understanding of the subject and finish my thesis.

I would like to thank Prof. Siamak Noroozi and Dr. Gelareh Roushan, who offered me many valuable suggestions in my research.

Special thanks to my friend Angel Torris Perez for his help on the hardware design in my research.

Also I thank my friends, Longjiang Niu, Meili Wang, Adil Saeed, etc, they helped me improved my thesis.

Lastly, I offer my regards and blessings to all of those who supported me in any respect during the completion of my PhD.

Table of Content

<i>Dedication</i>	I
Abstract.....	II
Acknowledgements.....	III
Table of Content	IV
List of Figures	VII
List of Tables	XI
Abbreviations.....	XII
1 Introduction.....	1
2 Patient Monitoring on General Hospital Wards	9
2.1 Introduction	9
2.2 Physiological monitoring on General Wards.....	9
2.3 Conventional Approach for Patient Monitoring on General Hospital Wards..	11
2.4 Development of PDA-based Patient Monitoring Systems	15
2.5 Summary.....	18
3 Evaluation of Sensors for RPM.....	19
3.1 Introduction	19
3.2 Sensors for Heart Rate Monitoring.....	19
3.2.1 Electrocardiograph (ECG) sensor	20
3.2.2 Heart-rate Chest Strap.....	22
3.2.3 Pulse Oximeter	23
3.3 Sensors for Measuring Blood Pressure.....	25
3.4 Sensors for Monitoring Respiration Rates.....	26
3.5 Sensors for Measuring Body Temperature	28
3.6 All-in-one Device for RPM	29
3.7 Summary.....	31
4 Wireless Network Technologies for RPM	32
4.1 Introduction	32
4.2 Bluetooth	33
4.2.1 Bluetooth protocol stack.....	33
4.2.2 Physical Layer	34
4.2.3 Topology and Medium Access Control	36
4.3 ZigBee	38

4.3.1	Physical Layer (PHY)	40
4.3.2	Medium Access Layer (MAC).....	42
4.3.3	Topologies.....	45
4.4	Comparisons between ZigBee and Bluetooth.....	46
4.5	IEEE 802.11 Wireless Local Area Network (WLAN)	49
4.5.1	IEEE802.11 MAC Layer.....	51
4.5.2	IEEE802.11 Physical Layer	53
4.6	Interference Issues of WLAN on WPANs.....	54
4.6.1	Interference of Wi-Fi on Bluetooth.....	55
4.6.2	Interference of Wi-Fi on ZigBee.....	57
4.7	Security Issue.....	60
4.8	Summary.....	68
5	RPM using Wireless Network Technologies	69
5.1	Introduction	69
5.2	Data Acquisition in RPM using Wireless Sensor Networks.....	70
5.2.1	Wireless Sensor Networks for Data Acquisition.....	70
5.2.2	Bluetooth and ZigBee-based Sensor Networks for Data Acquisition.....	71
5.3	The Use of Wi-Fi in RPM	78
5.4	Summary.....	80
6	Proposed Wireless RPM on General Wards.....	81
6.1	Introduction	81
6.2	Main Components of the Proposed RPM.....	82
6.2.1	Data Acquisition System.....	82
6.2.2	Data Transmission System.....	84
6.2.3	Central Control Unit.....	86
6.3	Some Relevant Issues	89
6.4	Summary.....	92
7	The Prototype RPM.....	93
7.1	Introduction	93
7.2	The Prototype Data Acquisition System	94
7.2.1	Design of a Simulated Wireless Biomedical Sensor (ZB)	94
7.2.2	Data Acquisition System (DAS).....	107
7.2.3	Data Transmission in ZigBee-based Networks	113
7.3	Data Transmission System based on a Wireless LAN	124

7.4	Prototype Central Control Unit.....	125
7.5	Summary.....	127
8	Simulations of Wireless RPM on General Wards.....	129
8.1	Introduction.....	129
8.2	Simulation tools.....	129
8.3	Simulations of ZigBee-based WPANs in RPM.....	132
8.3.1	Components and Configurations Used in Simulation.....	132
8.3.2	Alternative Approaches for ZigBee-based RPM.....	137
8.3.3	Simulation Results and Discussions.....	138
8.3.4	Channel Overlap Problems of ZigBee Networks for RPM.....	145
8.3.5	Simulation Results and Analysis of Channel Overlap.....	146
8.3.6	Realistic Transmission Intervals for RPM on General Wards.....	151
8.4	Simulations of WLAN in RPM.....	155
8.4.1	Components and Parameters Used in Network Modeling.....	155
8.4.2	Model of Hospital Network.....	167
8.4.3	Simulation results.....	168
8.5	Summary.....	179
9	Conclusion and Future Work.....	180
	References.....	186
	Appendix 1. Calculation of ZigBee Channel Capacity.....	214
	Appendix 2. PIC16F887 Specifications.....	215
	Appendix 3. Code of Programmed System for Micro-controller.....	216
	Appendix 4. Flow Chart of Programmed System for Micro-controller.....	219
	Appendix 5. Datasheet of Digi XBee Series.....	220
	Appendix 6. All Configurable Parameters Supported by XBee Series 2.....	222
	Appendix 7. Designed ZB.....	225
	Appendix 8. A Designed Database for the Central Control Unit.....	226
	Appendix 9. The Code Used by DAS Model for Transition Diagram.....	227
	Appendix 10. Theoretical Throughput of a WLAN.....	229
	Appendix 11. List of Publications.....	234

List of Figures

Figure 2.1 - Role of nurse in a patient monitoring process	11
Figure 2.2 - Information flow in a typical EWS system	14
Figure 2.3 - A Wireless PDA-based monitor	17
Figure 3.1 - A wireless 12-leads ECG	21
Figure 3.2 - A heart-rate chest strap.....	22
Figure 3.3 - A wireless oximeter based RPM system	24
Figure 3.4 - Wireless blood pressure sensor designed by IBM.....	26
Figure 3.5 - Wireless body temperature sensor	29
Figure 3.6 - AMON all-in-one device	30
Figure 4.1 - Bluetooth protocol stack	34
Figure 4.2 - Bluetooth basic operation mechanism – frequency hopping	35
Figure 4.3 - Overlapping Bluetooth Piconets (or Scatternets)	37
Figure 4.4 - ZigBee protocol stack	38
Figure 4.5 - Device Roles in the IEEE 802.15.4 and ZigBee Standard.....	39
Figure 4.6 - IEEE 802.15.4 operating channels in the 2.4GHz band.....	41
Figure 4.7 - Unslotted CSMA/CA algorithm	44
Figure 4.8 - Data transmission modes in a ZigBee WPAN	45
Figure 4.9 - Network topologies of ZigBee.....	46
Figure 4.10 - General 802.11 Frame Format	52
Figure 4.11 - Channel overlaps between Wi-Fi and Bluetooth channels	55
Figure 4.12 - Channel overlap between IEEE 802.15.4 and IEEE 802.11g.....	59
Figure 4.13 - Bluetooth security operation	63
Figure 4.14 - The use of encryption.....	64
Figure 4.15 - Basic authentication and authorization process used by Wi-Fi	68
Figure 5.1 - Architecture of a typical RPM system.....	69
Figure 5.2 - The architecture of a WPAN for data acquisition	71
Figure 5.3 - A single ZigBee network approach	75
Figure 5.4 - Multiple WPANs approach for RPM on a ward	76
Figure 6.1 - Framework of the proposed RPM system	82
Figure 6.2 - Architecture of a DAS.....	83
Figure 6.3 - An overview of the LAN-based data transmission system.....	85
Figure 6.4 - The architecture for central control unit in the RPM system	86

Figure 6.5 – A designed database for the control unit.....	87
Figure 6.6 - An operational overview of the proposed RPM.....	91
Figure 7.1 - A prototype of the proposed RPM.....	93
Figure 7.2 - System architecture of ZB.....	95
Figure 7.3 - Schematic diagram of the power unit.....	96
Figure 7.4 - Simulated sensing block (potentiometer).....	97
Figure 7.5 - Processing block of ZB.....	99
Figure 7.6 - ZigBee-based transmission module.....	100
Figure 7.7 - Schematic diagram of the communication unit.....	101
Figure 7.8 - Voltage conversion between the communication and the processing blocks..	102
Figure 7.9 - Interfaces of X-CTU for configuration.....	103
Figure 7.10 - Schematic diagram of local display.....	104
Figure 7.11 - The algorithm used for implementing local states indicator.....	105
Figure 7.12 - A ZB in operation.....	107
Figure 7.13 - Configuration of master node.....	110
Figure 7.14 - Configuration of ZigBee module of ZB.....	113
Figure 7.15 - Layout of the experiments.....	114
Figure 7.16 - Results of experiment of transmission range test.....	117
Figure 7.17 - Physical layout of the experiment of interference.....	119
Figure 7.18 - The experiment of interference.....	119
Figure 7.19 - The architecture of the proposed data acquisition system.....	122
Figure 7.20 - Experiment of the proposed data acquisition system.....	123
Figure 7.21 - Interface of display on the PC connected with the master node.....	123
Figure 7.22 - Experiment of using wireless LAN for data transmission.....	124
Figure 7.23 - Main panel of central control unit.....	125
Figure 7.24 - Designed GUI.....	126
Figure 7.25 - Graph for blood pressure.....	127
Figure 8.1 - Model of a master node.....	133
Figure 8.2 - Configuration panel of ZigBee master node.....	133
Figure 8.3 - Model of a ZigBee sensor (ZB).....	134
Figure 8.4 - Configuration panel of ZigBee master node.....	135
Figure 8.5 (a) - Attributes of wireless_tx (b) - Attributes of wireless_rx.....	136
Figure 8.6 - Supported packets types in simulation.....	136
Figure 8.7 - Transmission delay in a single WPAN RPM.....	140

Figure 8.8 - Data volume transmitted by sensors and received by the master node in a single WPAN RPM.	141
Figure 8.9 - Total volume of data transmitted by the sensors.....	142
Figure 8.10 - Comparison of successful data transfer	143
Figure 8.11 - (a) Data volume transmitted from the sensors to the master node in each WPAN (b) data volume received by the master nodes.....	144
Figure 8.12 - End to end delay for multiple WPAN RPM in each WPAN	145
Figure 8.13 - Comparison of data transmission and reception in each WPAN.....	148
Figure 8.14 - Successful data transfer rate.....	149
Figure 8.15 - Comparison of transmission delay through WPANs	150
Figure 8.16 - Comparison of transmission and reception in each WPAN.....	152
Figure 8.17 - Successful data transfer rate using longer transmission intervals.....	153
Figure 8.18 - Comparison of delays for transmission	154
Figure 8.19 - The DAS model used in simulation.....	157
Figure 8.20 - Attributes of a configured DAS	158
Figure 8.21 - Standard Network Application models	160
Figure 8.22 - Application Definition parameters.....	160
Figure 8.23 - Custom application parameters.....	161
Figure 8.24 - Custom application task table	161
Figure 8.25 - Profile configuration parameters	162
Figure 8.26 - DAS Application settings.....	163
Figure 8.27 - Access Point configuration parameters	164
Figure 8.28 - Server model used to simulate the central control unit.....	165
Figure 8.29 - Application attributes of server.....	166
Figure 8.30 - Switch Model	167
Figure 8.31 - Modelled Hospital Network for simulation.....	168
Figure 8.32 - Generated packet size and DAS application traffic sent	169
Figure 8.33 - Comparison of transmission data rate.....	170
Figure 8.34 - Total throughput of the modelled WLAN	171
Figure 8.35 - Average WLAN retransmission attempts.....	172
Figure 8.36 - Global average end-to-end delay	173
Figure 8.37 - Overall retransmissions on the modelled WLAN system.....	174
Figure 8.38 - Collision status on the WLAN when TCP is used	174

Figure 8.39 - The number of packets sent by all DASs and the number of packets received by the control unit	175
Figure 8.40 - Modified simulation scenario	176
Figure 8.41 - Video conference parameters.....	177
Figure 8.42 - WLAN and AP Throughput.....	178
Figure 8.43 - Data volume received by the central control unit.....	179

List of Tables

Table 2.1 - Some aspects in physiological monitoring on general wards.....	10
Table 2.2 - Comparative healthcare employment in five countries	13
Table 4.1 - Key features of Bluetooth.....	33
Table 4.2 - Frequency spectrum of Bluetooth	35
Table 4.3 - Power classes of Bluetooth.....	36
Table 4.4 - ZigBee specifications	40
Table 4.5 - Properties of Bluetooth, ZigBee and Wi-Fi	47
Table 4.6 - Summarized IEEE 802.11 standards.....	50
Table 7.1 - Main components of designed power unit.....	95
Table 7.2 - Key specifications of PIC16F887	98
Table 7.3 - Specifications of XBee series 2 ZigBee module	100
Table 7.4 - The range of vital signs used for display	104
Table 7.5 - Preset range used for local states indicator	106
Table 7.6 - Setting of serial port communication	108
Table 7.7 - Configured parameters of master node	109
Table 7.8 - Experiment result: the effect of Wi-Fi on ZigBee.	120
Table 7.9 - Parameters used in the experiment.....	122
Table 8.1 - Vital signs measured for RPM on general wards	139
Table 8.2 - Parameters used in simulation.....	139
Table 8.3 - Vital signs measured for patient monitoring.....	147
Table 8.4 - Parameters used in simulation.....	147
Table 8.5 - Vital signs transmitted in RPM with revised intervals	152

Abbreviations

ACK	Acknowledgement
AES	Advanced Encryption Standard
BPSK	Binary Phase-Shift Keying
CCA	Clear Channel Assessment
CFP	Contention-Free Period
CSMA-CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear to Send
DAS	Data Acquisition System
DSSS	Direct Sequence Spread Spectrum
ED	Energy Detection
EWS	Early Warning Score
FFD	Full-Function Device
FHSS	Frequency Hopping Spread Spectrum
GTS	Guaranteed Time Slot
IEEE	Institute of Electrical and Electronics Engineering
ID	Identifier
IP	Internet Protocol
IFS	Interframe Spacing
ISM	Industrial, Scientific, and Medical
LQI	Link Quality Indicator
MAC	Medium Access Control
MIC	Message Integrity Code
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit

NHS	National Health Service
O-QPSK	Offset Quadrature Phase-Shift Keying
PPDU	PHY Protocol Data Unit
QoS	Quality of Service
RF	Radio Frequency
RFD	Reduced Function Device
RPM	Remote Patient Monitoring
RTS	Request to send
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WHO	World Health Organization

CHAPTER ONE

1 Introduction

An ageing population and the associated prevalence of chronic disease continue putting increasing demands on medical and healthcare resources. There are currently more than 650 million people across the world over the age of 65, a number that will double over the next 10 years (Population Reference Bureau 2007). The rapidly growing ageing population has resulted in an increase of chronic age-related diseases, such as, congestive heart failure, arthritis and so on (Fass 2007). The World Health Organization (2010) indicates that elderly people, who frequently suffer from chronic disease, require a highly effective and efficient provision of care.

Health organizations and hospitals have been active in applying appropriate technologies to improve patient care; however there are still many areas, which can benefit from further improvement. National Institute for Health and Clinical Excellence (NICE) (2007) indicated that there are inefficiencies in patient monitoring, particularly on general hospital wards. This is supported by the Commission for Healthcare Audit and Inspection (CHAI) (2008), which indicated that patients on general wards in the United Kingdom (UK) believed that there was insufficient monitoring; some patients felt 'abandoned' whilst others experienced being left unattended for varying lengths of time. The CHAI (2009)

argues that the two major concerns of healthcare within the UK today are poor care of patients within general wards and inequality in treatment.

It is claimed that the healthcare system has long been plagued with problems, such as diagnoses being written illegibly on paper, doctors not being able to easily access patient information, as well as limitations on time, space, and personnel for monitoring patients (Meingast *et al.* 2006). These issues are compounded as healthcare organizations have to provide better quality services to a continually increasing number of patients within hospitals and nursing homes.

Medical personnel, nurses in particular, are fundamental to high-quality healthcare, as they have the greatest contact with patients over the twenty-four hour period (Department of Health 2008a). Part of this role within the hospital environment is the monitoring of patients, which will include gathering vital signs. Also, the frequency of nurses' visits depends upon patients' needs. These are based upon the severity of patients' conditions judged by nurses, which can be subjective.

Modern Intensive Care Units (ICUs) have employed an impressive array of technologically sophisticated instrumentation to provide detailed measurements of the physiological state of each patient (Heldt *et al.* 2006). This has been largely achieved utilizing Remote Patient Monitoring (RPM) systems; yet despite the success of this, the development of RPM on general wards is evolving at a rather slower pace. An RPM system for a general ward cannot replace the functions of

nurses; however, it can be used to complement them and improve efficiency in patient monitoring. A RPM system is perceived to be more convenient and cost effective than traditional care, since it enables healthcare organizations to monitor and manage patients remotely whilst being looked after professionally (Barlow *et al.* 2005). It is indicated that adopting RPM technologies could not only improve healthcare services, but also reduce nurses' visits by 30-50%, and it is claimed that this is very effective in terms of costs and time consumption (Kuraitis 2007).

Further, early detection of abnormalities of patients on general wards can improve recovery and reduce mortality rates during hospitalization. It is recognized that hospitalized patients who suffer cardiac arrest and require unanticipated admission to ICU often exhibit premonitory abnormalities in vital signs (Smith *et al.* 2006). Early detection of abnormalities of vital signs has significance in healthcare, particularly in patient monitoring. Many hospitals are now using a process called Early Warning Scores (EWS) in order to aid the early detection of patient deterioration; these operate by noting changes in patients' vital signs. However, it is argued that monitoring patients' vital signs is typically viewed as a mundane aspect of nursing care which is frequently delegated to healthcare assistants, whose varying levels of training provoke concerns regarding accuracy and interpretations of data (Al-Qahtani and Al-Dorz 2010).

It can be argued that innovation in healthcare ultimately has to be justified on three grounds, namely efficacy, efficiency and safety (Gardner *et al.* 2010). These three grounds determine the requirements of RPM on general hospital wards. In

spite of the complexity in analyzing the requirements, provision of the right information, in the right place, at the right time are the fundamental in RPM.

However, the current uses of wired sensing devices as well as their connections to network systems are not suitable for long-term RPM, as their usage restricts patients' mobility. Advances in biomedical sensors and wireless network technologies have made it possible to develop a wireless RPM system. Such a wireless RPM can provide enhanced mobility and comfort to patients during hospitalization. It will empower patients to be monitored

It should be highlighted that although some aspects of wireless RPM have already been developed, a fully automated RPM system for general hospital wards with the capability of monitoring a large number of patients for identifying abnormalities is yet to be developed. Moreover, a suitable wireless technology for networking of biomedical sensors to support RPM systems is yet to be determined. Bluetooth, ZigBee and Wi-Fi are possible technologies for wireless RPM systems. However their suitability and capability for RPM require further investigation.

Objectives of this research

- Analyze basic requirements for RPM on general hospital wards
- Investigate the suitability and reliability of wireless technologies to support RPM on general wards
- Propose a system framework for RPM on general wards
- Design a prototype to demonstrate the functionalities of the proposed RPM

- Evaluate the application of the proposed RPM system for general wards in a simulated environment

Research Methodology

In order to achieve the objectives, following methods were applied:

- Literature review

Extended literature review was conducted. In the initial stage, healthcare audit reports, surveys and review papers were used to identify problems in patient monitoring on general hospital wards. There were two key findings from literature review: 1) There was inefficiency in current approach of patient monitoring; 2) RPM had potential in improving patient monitoring and quality of patient care.

- Interview hospital staff

In order to verify the key findings, several hospitals were subsequently visited. Hospital staff was interviewed. They included doctors, nurses and hospital IT staff. During the interviews, pre-prepared questions were used, for example, what do you think about using RPM on general hospital wards; do you think RPM would improve patient care, etc.

The interviewees provided information about current approach of patient monitoring on general wards. They confirmed that RPM had not been utilized on general hospital wards in their hospitals; however they believed an

automated RPM had potential in improving patient monitoring on general hospital wards.

In addition, the requirements of using RPM on general wards were discussed with hospital staff. They indicated that a system would be validated on the premise of supporting long-term RPM as well as providing enough mobility and comfort to patients. Whilst they agreed that wireless RPM could provide enhanced mobility and comfort to patients. However usability and reliability were two main concerns.

- Experimental study

The experimental study was adopted to investigate technical feasibility of using wireless network technologies for data transmission in RPM. The focus was to study transmission reliability, especially in the presence of interferences and channel overlaps. A prototype system was used to explore distance range of the chosen wireless technology.

- Consultation of hospital staff

Hospital staff was consulted during the design of the prototype RPM and the result was discussed with them. They gave suggestion on further improvement of the prototype RPM system.

It should be noted that iteration of prototype design and consultation was carried out with intention to develop a RPM system to meet the required standard.

- Modelling and simulation of the proposed wireless RPM system

The focus of modelling and simulation was to investigate transmission reliability of using wireless network technologies in RPM. During the investigation, shortfalls of wireless technologies (e.g. ZigBee and Wi-Fi) were identified. Partial solutions for using these technologies in RPM are offered. Finally, a wireless RPM system for general hospital wards was proposed.

The organization of the thesis follows the sequence of achieved objectives. In addition to this chapter, there are eight other chapters:

Chapter 2 discusses patient monitoring on general hospital wards.

Chapter 3 evaluates available sensors which can be used in RPM.

Chapter 4 evaluates three types of wireless network technologies, Bluetooth, ZigBee and Wi-Fi in respect of suitability for RPM on general hospital wards.

Chapter 5 discusses the applications of wireless network technologies in RPM. Some of the existing technologies which can be used for wireless RPM are evaluated.

Chapter 6 discusses the proposed RPM system and its functional components. The relevant issues associated with the functionality and performances of the system are discussed.

Chapter 7 discusses the prototype which is used to demonstrate the functionality of the proposed RPM system. Some experiments based on the designed prototype are introduced and the results are evaluated.

Chapter 8 discusses the simulation of the proposed RPM system. The focus of the simulation is on the reliability of transmission using wireless network technologies in RPM. Simulation results are presented followed by the evaluation of the suitability of using the proposed RPM system on general hospital wards.

Chapter 9 concludes the thesis and highlights future research.

CHAPTER TWO

2 Patient Monitoring on General Hospital Wards

2.1 Introduction

Although many types of illnesses currently can be managed in an outpatient setting, there are clearly medical conditions that require more intensive care and treatment in a hospital. Generally, patients are either brought to an emergency or urgent care department for acute diagnosis and management or a general ward to receive non-urgent treatment. The diverse healthcare environments generate different requirements of health monitoring. These requirements should be carefully considered for further development in the healthcare system. In this chapter, basic requirements of patient monitoring on general wards will be discussed followed by the discussion of the approaches used for monitoring patients on general wards.

2.2 Physiological monitoring on General Wards

A general ward is a non-specialist hospital unit offering a range of treatments to a variety of patients. Advances in medical technology have led to patients living with much more complex health issues, leading to an increase in the variety of patients being managed within the general ward setting. Therefore, patients may require different level of care and attention; some require frequent visits by medical personnel whilst others who are in stable condition require less.

Physiological monitoring is an essential part of management and care of patients on general wards. The purpose is to identify and record changes that occur to vital signs, as this may be helpful in preventing deteriorations of patients' condition. The frequency of monitoring may also vary depending on the severity of the patient's condition. Varshney (2006) suggested some basic requirements that should be considered in physiological monitoring on general wards. Table 2.1 lists these requirements.

Table 2.1 – Basic requirements in physiological monitoring on general wards

Patient-related	Required vital signs Frequency for monitoring Patients' comfort and usability issues
Healthcare provider-related	Number of patients per provider and cognitive overload Liability and reliability issues Security and privacy of patient information Cost for deployment and maintenance

NICE clinical guidelines (2007) stated that as a minimum, the following vital signs should be recorded at the initial assessment and as part of routine monitoring:

- Heart rate
- Oxygen saturation
- Systolic blood pressure
- Respiratory rate
- Body temperature

NICE clinical guidelines (2007) also recommended that the vital signs should be monitored at least every 12 hours, unless a decision has been made at a senior level to decrease this frequency for an individual patient. Hospitals have made their own regulations to determine the frequency of monitoring of vital signs. Medical staffs confirmed that in spite of the variance of the regulations, the frequency of monitoring should increase if a symbol of deterioration is detected.

2.3 Conventional Approach for Patient Monitoring on General Hospital Wards

Practice at present is that in general a nurse or healthcare assistant visits a patient to observe and record vital signs and compare them with the data taken previously. The frequency of visits may relate to a suggested schedule. However, it may also depend on the severity of patient's condition, and the nurses' judgment, which can be subjective. In addition, when the nurse realizes that a patient's condition is deteriorating, it is most likely that the frequency of the visits will increase. This will only happen if the patient is monitored frequently and effectively. Figure 2.1 shows the role of nurses in this context.

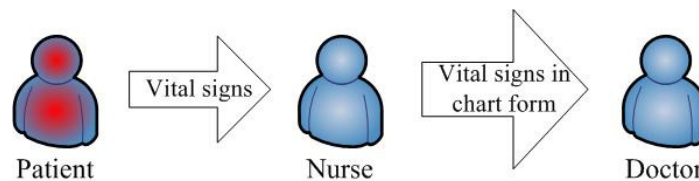


Figure 2.1 - Role of nurse in a patient monitoring process

Patient monitoring is a labour-intensive activity, and human resources are the most important input into this provision (Bloor and Maynard 2003). To record the patients' vital signs, it may take about 15-30 seconds to get pulse rate; another half minute for respiration rate and so on. The utilization of electronic instruments can improve the efficiency in vital signs measurement. However these instruments are commonly large in size and are not readily to move, which restricts their usage on general wards.

Vital signs are normally recorded in chart forms, which doctors often view daily during their ward rounds. In addition, other healthcare personnel may also view the charts and input their suggestions. Adler (2004) stated that "typical charts are 120 pages and viewed by 70 individuals in routine monitoring".

The ratio of medical staff to patient has also an impact upon the effectiveness of patient monitoring. This is more evident in small hospitals, where there is a smaller number of medical staff. This can result in many patients on general wards not receiving expected care and attention (Commission for healthcare audit and inspection 2008).

In the UK, the ratio of both medical and nursing staff to patient is relatively lower than in some other countries, where healthcare system are mainly funded by governments. Table 2.2 shows comparative healthcare employment ratios in five of these countries.

Table 2.2 - Comparative healthcare employment in five countries adapted from
(World Health Organization 2009)

Countries	Practicing physicians per 1000 population	Practicing nurses per 1000 population
Australia	3	10.7
France	3	6
Germany	3.4	9.6
Sweden	2.9	8.4
UK	1.8	4.5

Due to the low ratio of medical staff to patient, medical staffs have to work under pressure caused by the heavy workload. Occasionally extra work shifts need to be covered to address the lack of medical staff. It has been recognized that there is a potential link between increased medical errors and a cognitive overload of medical staff (Varshney 2006). Therefore, it can be argued that one major issue in patient monitoring is the number of patients per medical staff and the potential cognitive overload.

To improve patient care on general wards, Early Warning Scores (EWS) systems were introduced in many hospitals. These systems vary in terms of choice of physiological parameters, assignment of scores to physiological values and trigger thresholds. However they are trying to achieve the same mission, which is to ensure timely identification of patients with potential or established critical illness and to ensure early attendance by appropriately skilled staff (Department of

Health and NHS Modernization Agency, 2007). Figure 2.2 shows an overview of the information flow in a typical EWS system.

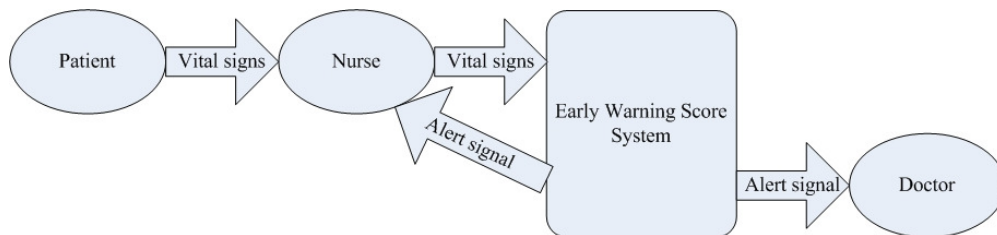


Figure 2.2 - Information flow in a typical EWS system

Most EWS systems are still paper-based and there are problems associated with them. For example, diagnoses are written illegibly on paper; doctors not having easy access to patient information, as well as time and personnel constraints for monitoring patients (Meingast *et al.* 2006). In addition, even when EWS systems are used, the recording of vital signs and completion of patient charts remain sub-optimal; in such a case vital signs are missing and charts are incomplete, which ultimately affects the validity of the system (Smith *et al.* 2006). Indeed, it is argued that most of the existing EWS systems provide inadequate sensitivities (Smith *et al.* 2008a), which seem to suggest that a high number of patients requiring intervention are likely to be missed. After reviewing the in-use EWS systems, Gao *et al.* (2007) indicated that incorrect/incomplete vital signs record or the record not being completed on time and inappropriate settings of the warning threshold are two main problems which lead to the inefficiency in existing EWS systems.

The paper-based EWS systems are gradually being replaced with electronic-based. Some hospitals, particularly in the United Kingdom, have adopted a PDA-based EWS system in critical care units (such as intensive care unit or high dependency care unit). This may be extended to general wards.

2.4 Development of PDA-based Patient Monitoring Systems

In recent years, healthcare providers have sought suitable methods for improving the efficiency of patient monitoring. Many approaches have been adopted to improve the processes of recording and disseminating patient's vital signs to medical personnel. PDAs with wireless capabilities have been introduced in hospitals to assist in vital signs recording and transmission.

In the UK, a pilot study of a PDA-based system, to record clinical data, concluded that the system presented a viable alternative to a paper-based one (Gardner *et al.* 2001). In using such a system, medical staffs carry PDAs to record patient's vital signs, which are then transmitted through a wireless network to a database in the hospital. This is an improvement upon paper-based patient recording, which can now be stored in PDAs and transmitted wirelessly.

Apart from easy recording of patients' vital signs, Lu *et al.* (2005) claimed that "PDA-based systems offer portable and unobtrusive access to clinical data, which could improve access to information and enhance workflow in patient monitoring". An implementation of a wireless network and PDA-based system at the Western General Hospital Trust, in Edinburgh was reported by Turner *et al.*

(2005). In addition to supporting medical staffs to use PDAs to download patients' record from a database, this system took advantage of ad-hoc wireless network, which allow medical personal to share patients' health information in a peer-to-peer mode (Turner *et al.* 2005). Thus, it provided increased access to patients' health information.

In addition an integrated patient monitoring and vital signs recording system based on PDAs was developed by Smith *et al.* (2006), which was an improvement to a paper-based EWS system. A set of EWS were integrated to the PDAs. When medical personnel input a patient's vital signs in to a PDA, it will do some calculation locally based upon the EWS. The output from the calculation can assist medical personnel to judge the condition of a patient. The PDA can also communicate with a central database through a wireless LAN system to upload patients' current record or download history record. Prytherch (2006) stated "this PDA-based system can facilitate vital signs recording as well as speeding up decision making".

Furthermore a conceptual plan of using PDA in health care has been presented by Akhgar (2009), which was to provide support for a portable diagnostic healthcare platform based on Lab-On-Chips technology. The concept is based on creating a host environment that combines mobile phones/PDAs with the Near Field Communication (NFC) wireless technology to further support mobile diagnostic healthcare applications.

PDA-based systems also have been used for gathering vital signs. The idea was to integrate biomedical sensors to a PDA. In such a case, the PDA can gather vital signs from the sensors automatically. A representative invention was introduced by Lin *et al.* (2005). In that system a PDA was connected to several biomedical sensors as shown in Figure 2.3. This system was used during transportation of patients within hospital. A nurse could use the PDA for local display of vital signs as well as sending a short period of recorded data wirelessly to a control room for RPM. Power consumption was a major issue in long-term operation; “the battery life could only last for a maximum of two hours in the test of gathering and displaying data continuously” (Lin *et al.* 2005).



Figure 2.3 - A Wireless PDA-based monitor (Lin *et al.* 2005)

PDA-based systems have advantages compared to the paper-based systems. However they cannot support real-time patient monitoring, which may be required on general wards. Although the system invented by Lin *et al.* (2005) has the

capability of automatic gathering of vital signs, the data was only displayed locally. A patient could not be monitored in the absence of a nurse. Therefore such a system is not suitable for patient monitoring on general hospital wards (Bardram *et al.* 2006). An automated RPM system is desired to gather vital signs from each patient in real-time for recording and analysis. In this respect, nurses would be able to focus upon the holistic needs of patients to improve quality of patient care.

2.5 Summary

Physiological data monitoring is a fundamental task in patient monitoring on general hospital wards. Approaches of patient monitoring on general wards were discussed in this chapter. The conventional approach is labour-intensive, human resources are the most important input into the provision of patient monitoring. The use of paper-based “Early Warning Score” system improves patient monitoring by ensuring timely identification of patients with potential deteriorations. PDA-based system is gradually replacing paper-based system; however, patient monitoring still relies on nurses’ visits. An automated RPM system would provide further improvement and holistic care to patients on general wards. In the next chapter, sensors that can be used to measure vital signs in RPM will be discussed.

CHAPTER THREE

3 Evaluation of Sensors for RPM

3.1 Introduction

Vital sign measurement is the initial and the most important task in RPM. The existing instruments are commonly equipped with cable-based sensors, which make them bulky, intrusive and inconvenient. These sensors may not suit for long-term monitoring of vital sign in RPM on general wards. To improve comfort and mobility of patients, wireless biomedical sensors are considered. They are normally small in size and have wireless communication capability. This chapter evaluates sensors that can be used to measure vital signs in RPM on general hospital wards.

3.2 Sensors for Heart Rate Monitoring

Heart rate is very important in patient monitoring. In traditional medicine, heart examination and monitoring was carried out by stethoscopes, through which medical personnel listened to a patient's heart sound and made decisions based on their knowledge and experience. The development of electronics and digital signals processing techniques have made it possible to use a small microphone to record cardiac sound and use a computer to analyze it. However noise cancellation is yet under research to ensure the accuracy of heart sound monitoring.

Budinger (2003) indicated that heart rate can also be measured by electrical waveform as well as pressure detection and electromagnetic flow. In this section, some sensors that can be used to measure heart rate are evaluated; they are ECG, heart-rate chest strap and oximeter.

3.2.1 Electrocardiograph (ECG) sensor

ECG is primarily a tool for examination of cardiac diseases (Dagtas *et al.* 2007). An ECG sensing device commonly consists of a group of electrodes to detect electrical events of a heart. Shnayder *et al.* (2005) indicated that the most prevalent ECG sensor involves the connection of 12 electrodes (also referred to as leads) to a patient's chest, arms and right leg via adhesive foam pads. The sensor records a short sampling (no more than thirty seconds) of the heart's electrical activity between different pairs of leads. Each pair of leads provides a unique and detailed picture of the cardiac rhythm by detect the change of electrical energy and referenced to a ground signal.

Pettis *et al.* (1999) indicated that computer-based applications and the development of wireless technology had allowed the transmission of 12-lead ECG waveforms from remote locations to a hand-held computer carried by a cardiologist. For example Khor *et al.* (2001) developed a wireless ECG sensor, which could send 12-lead ECG signal through Bluetooth or GSM for RPM. Figure 3.1 shows such a wireless 12-lead ECG. The hand-held device is for wireless transmission of ECG signal to a PC nearby or in remote location.

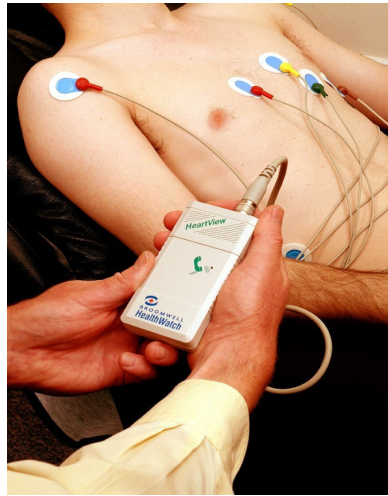


Figure 3.1 - A wireless 12-leads ECG (LifeSync 2010)

The 12-lead ECG is also called full-lead ECG. In some situations that do not need as much data recording, subsets of 12 leads ECG can be used. In RPM one or two leads ECG are commonly considered to reduce data transmission and increased flexibility. For example, Kho *et al.* (2005) employed a two-lead ECG in their Bluetooth-enabled ECG monitoring system. Yu *et al.* (2005) proposed a RPM system that includes a one-lead ECG sensor. A ZigBee-based ECG was designed by Auteri *et al.* (2007).

However there have been disadvantages of using ECG in RPM. Haghghi-Mood and Torry (1995) indicated that “the timing between electrical and mechanical activities in a cardiac cycle is not exactly constant for all patients due to a variety of pathological conditions”. In addition, Nigam and Priemer (2005) argued that the presence of a reference signal requires additional hardware that might not be readily available in using ECGs for RPM.

3.2.2 Heart-rate Chest Strap

Techchee (2010) stated that “current heart-rate chest strap is based on a tiny piezoelectric sensor to detect heart beat” (as shown in Figure 3.2). A micro-processor is integrated to transfer detected signal into heart rate. The heart rate is then sent by an integrated transmitter to a wrist-mounted device for display. The wrist-mounted device usually has local warning and wireless transmission capability. In the event that the wearer’s heart rate goes beyond the threshold of a preset safe range, the wrist-mounted device will warn locally as well as sending an alert signal to a physician. In contrast to ECG sensors, the strap can be simply placed on a patient’s chest for measuring heart rate without the assistance of skilled medical personnel. A heart-rate chest strap does not affect a patient’s mobility; however the comfort needs consideration for long-term monitoring. Currently it is mainly used for patients with some degree of chronic disease who may require regular exercises and self-monitoring (Casio 2010).

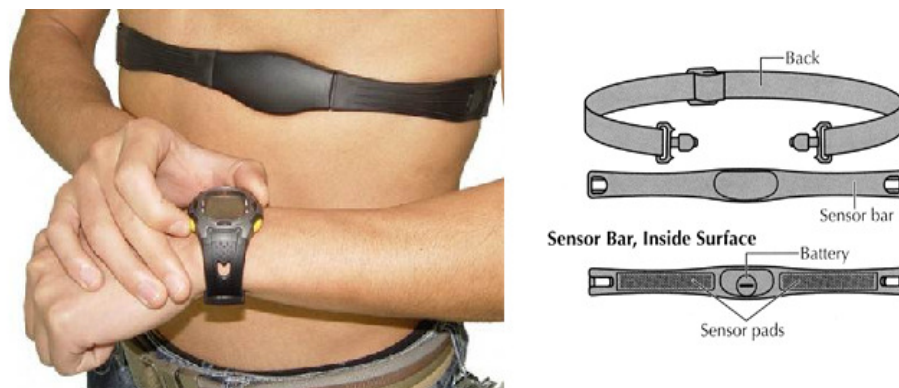


Figure 3.2 - A heart-rate chest strap (adapted from (Techchee 2010))

3.2.3 Pulse Oximeter

The pulse oximeter was invented for patient monitoring in the early 1970s (Tremper and Barker 1989). It can be used to examine two types of vital signs: heart rate and blood oxygen saturation (also referred to as SpO₂). These parameters yield critical information, particularly in emergencies when sudden changes in the heart rate or reduction in blood oxygen saturation can indicate a need for urgent medical intervention. With advanced warning, patients could get treatments to avoid hypoxemia before they manifests physical symptoms (Shnayder *et al.* 2005).

A pulse oximeter typically incorporates a plastic housing, which contains an array of LEDs and an optoelectronic sensor opposite. By detecting the amount of light absorbed by haemoglobin in blood with two different wavelengths (typically 650nm and 805nm), the level of oxygen saturation can be measured. In addition, heart rate can be determined from the pattern of light absorption over time, since blood vessels contract and expand with the patient's pulse. Computation of heart rate and SpO₂ from the light transmission waveforms can be performed using standard digital signal processing techniques.

There are two types of oximeters, transmittance pulse oximeters and reflectance oximeters. The applied position of transmittance pulse oximeters is limited to the peripheral tissue, such as the fingertip, ear lobe, or toe. On the other hand a reflectance oximeter can measure SpO₂ from various parts of the body such as the

forehead, cheek, wrist, etc. Nevertheless transmittance pulse oximeters are popularly applied in patient monitoring to obtain highly precise arterial oxygen saturation measurements (Severinghaus and Naifeh 1987).

Wireless oximeters are now available in the market, for example Nonin 4100, a Bluetooth-based oximeter (Nonin 2010). This type of oximeter can send measured data to a PC server, a PDA or a mobile phone wirelessly using Bluetooth. Then the data can be displayed or relayed on for RPM. Figure 3.3 shows a wireless oximeter for RPM.

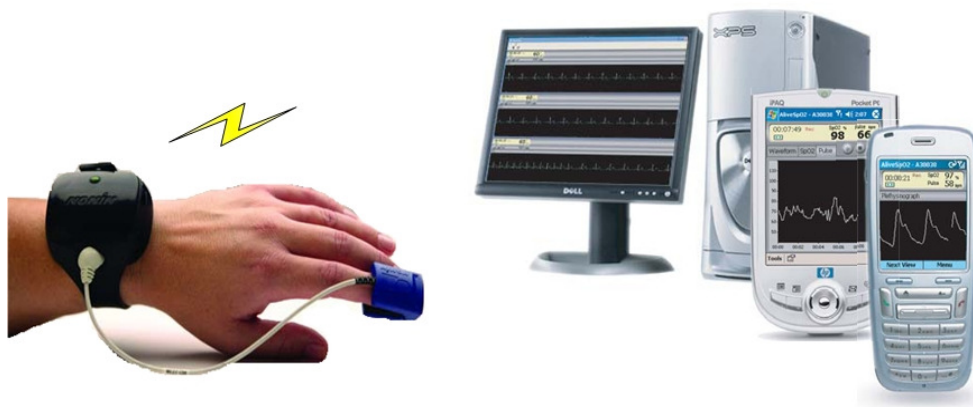


Figure 3.3 - A wireless oximeter based RPM system (Nonin 2010)

The pulse oximeter has advantages to be preferred for using in RPM. The major advantage is that one sensor provides two types of vital signs at a time. Hence it would offer more flexibility and convenience in RPM. An oximeter can be simply placed on a patient's finger for monitoring (as shown in Figure 3.3); professional skill is not required for placement compared to ECG sensors. Supported by an

appropriate wireless technology, pulse oximeter can be utilised in RPM on general hospital wards.

3.3 Sensors for Measuring Blood Pressure

Budinger (2003) indicated that “there are five common methods for measuring blood pressure: auscultation, palpation, flush, oscillation, and transcutaneous Doppler”. Furthermore Budinger (2003) pointed out that only the oscillation and transcutaneous Doppler can be adopted in remote monitoring by incorporation of sensors for pressure oscillations or Doppler shift in the pressure cuff around the wrist or finger.

Typical blood pressure sensors used in clinical are designed to measure systolic and diastolic blood pressures utilizing the oscillometric technique. A blood pressure sensor is usually used together with a pump bulb and a standard adult size adjustable cuff (typically 25 to 40 cm) that can inflate and deflate automatically (Omron 2010). In addition, wrist-worn blood pressure measuring device, which is portable and user-friendly, has already been utilized in current practice of patient monitoring. This type of device includes a memory storage that makes recording measurements easy, but they do not include communication capability for RPM.

Some efforts have been made to design a wireless sensing device for remote monitoring of blood pressure (Husemann 2004). A prototype has been built on a large wristwatch to measure blood pressure by IBM. It can measure blood

pressure and send it via Bluetooth to a mobile phone or a laptop of medical professional for RPM. Figure 3.4 shows the prototype of such a wireless blood pressure sensing device, which can be considered for RPM on general wards.



Figure 3.4 - Wireless blood pressure sensor designed by IBM (2004)

3.4 Sensors for Monitoring Respiration Rates

Respiration is also an important vital sign for patient monitoring. Cooley and Moser (1973) pointed out that “monitoring respiratory rates is ostensibly a simple task; the sensor needs to be neither linear nor accurate, but rather merely capable of recognizing respiration as such”.

The following provides information on respiratory rates and some of the sensors currently used for their measurement:

1. Brady *et al.* (2005) stated that “a pneumotachograph can be used to measure respiratory rates by detecting the rate of airflow to and from the lung”. When

using this clinical apparatus, patients need to wear a head-mounted respiration tube. This type of device has an advantage that it can provide detailed information on volume and direction of breath. However, it is too big to be employed in a portable RPM system.

2. A plethysmograph was introduced by Brady *et al.* (2007), which can be used to record respiration rates by measuring volume changes around the chest to determine lung capacity. However, though sophisticated, “these devices require hard-wired interconnections to external equipment and cannot be used outside a specialized clinical environment” (Brady *et al.* 2007).

3. A wearable sensor that can be used to measure respiration rate by combining wireless sensor with wearable technology is now available. The sensor has been tested with a range of 10-40 breaths per minutes and shown a satisfied performance in term of accuracy (Dunne *et al.* 2005). However, the wearable sensor has some limitations. One is that careful placement of the sensor is important for the quality of data gathered, since the position is crucial to their sensitivity. Furthermore movement during the monitoring phase may insurer incorrect result (Brady *et al.* 2007). But the potential of this kind of sensor should be realized, since it is wearable, mobile, and offer user much personal convenience.

4. Another approach was proposed by Johnston and Mendelson (2004) for extracting respiration rate from information gathered by a wearable pulse

oximeter. A pulse oximeter worn by a patient is used to record photoplethysmographic signal, which can then be processed by a time domain filtering and frequency domain Fourier analysis to extract respiration rate. Further investigation is required to validate its reliability. It could promote flexibility of a RPM system, since an oximeter can be used to measure three fifth vital signs, namely, oxygen saturation, pulse rate and respiration rate.

From the evaluations of respiration rate sensor, it can be concluded that currently wearable sensor may be an option for RPM on general wards with respect to accuracy of measurement and supported mobility. However more work may be required to address the issue of placement of respiration rate sensors.

3.5 Sensors for Measuring Body Temperature

Simpson and Greening (1965) summarized that body temperature can be measured by three types of sensors: resistance thermometer, thermocouple and thermistor. Among them, thermistors are widely used for portable devices in patient monitoring (Fogelson *et al.* 1996). They are resistance elements with a high negative coefficient of resistance. Some wireless body temperature sensors are based on it. Figure 3.5 shows a typical wireless body temperature sensor. It has wireless capability. When attached to a patient, it can measure the patient's temperature and send the measurement to a nearby instrument for display and monitoring.

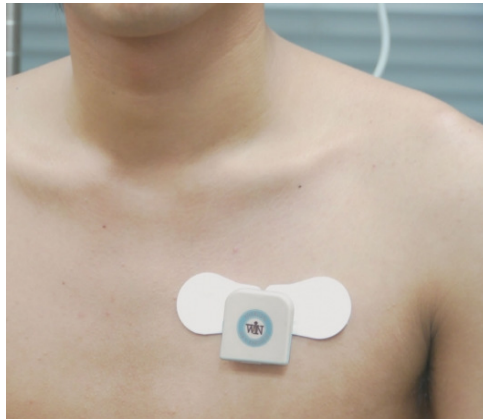


Figure 3.5 - Wireless body temperature sensor (Mobiitech 2010)

3.6 All-in-one Device for RPM

A device integrating several sensors for measuring vital signs from a patient has been proposed for RPM in recent years. These types of devices are usually defined as all-in-one. AMON is one of the best examples of all-in-one devices proposed by Anliker *et al.* (2004). It is a wrist-worn device (as shown in Figure 3.6) which includes sensors for blood pressure, skin temperature, SpO₂, and one-lead ECG. The device is capable of measuring vital signs and sends them to a remote clinical centre via GSM/GPRS. Although it can provide multiple measurements of vital signs, the accuracy of measurement is suboptimal. Varshney (2009) indicated that the skin temperature measured by AMON may not be a reliable estimate for body core temperature; one-lead ECG may not be able to produce high quality ECG signals needed for complex medical decisions. Therefore the AMON device may not be suitable for RPM on general wards, where high accuracy measurements of vital signs are fundamental.

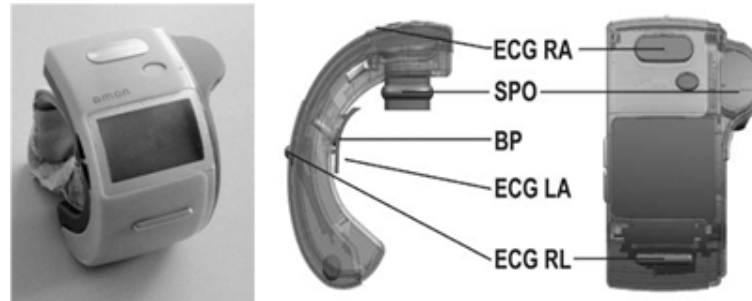


Figure 3.6 - AMON all-in-one device (Anliker et al. 2004)

WIHMD is a prototype of wrist-worn integrated health monitoring device proposed for RPM of elderly patients (Kang *et al.* 2006). Compared to AMON, WIHMD can also include respiration rate measurement. In addition it can be integrated with Global Position System (GPS). Patients' vital signs and their location can be sent through the commercial cellular phone network to medical professionals at a distance.

WEALTHY is another type of all-in-one device introduced by (Paradiso *et al.* 2005). It uses a textile wearable interface implemented by integrating sensors and connections in a fabric form. The sensors can measure respiration, three-lead ECG, temperature and movement activity. However it cannot measure all the five vital signs, which is required for RPM on general wards.

All-in-one monitors have advantages to be considered in RPM. They are capable of satisfying the demand of monitoring vital signs without affecting mobility of patients. An all-in-one device is easy to use, as it can be worn on the wrist like a watch. However accuracy of measurement and power consumption are two issues

need to be resolved. Although the “all-in-one” devices are likely to improve in their accuracy with further technological advances, using multiple wireless sensors for gathering vital signs may be suitable for RPM on general wards. In that case each sensor can be placed in an appropriate position focusing on one or two specific type of vital signs, which can lead to more precise measurement in monitoring.

3.7 Summary

Accurate and timely measurement of vital signs is vitally important in RPM. Relevant sensors that can be used to measure vital signs were discussed and evaluated in this chapter. These sensors can be used to measure patients’ heart rate, oxygen saturation, blood pressure, respiration rate and body temperature. All-in-one devices are capable of measuring multiple vital signs, which were also discussed. To achieve more precise measurement, multiple sensors are suggested to place in appropriate positions for measuring vital signs in RPM on general wards. In the next chapter, wireless technologies that can be utilized for networking biomedical sensors will be discussed.

CHAPTER FOUR

4 Wireless Network Technologies for RPM

4.1 Introduction

The advance of wireless technologies has led to the design, development and deployment of different types of wireless networks. These networks are usually classified by their capabilities and properties. Based on their characteristics, wireless network technologies can be used for specific applications. Wireless Local Area Networks (WLANs) based on Ethernet technology have been widely used to provide connectivity to hosts (computer, machinery or systems) that require rapid deployment in a local area environment. Low-power wireless network technologies were introduced to serve a more specialized purpose such as networking battery-powered sensing devices in healthcare. This type of technology permits short-distance communication. Therefore it is referred to as Wireless Personal Area Network (WPAN) technology. The application of WPAN technology in RPM has received increasing interest in recent years. It empowers patients to be monitored with enhanced mobility and comfort. In this chapter, three types of wireless network technologies are discussed. They include Bluetooth, ZigBee and Wi-Fi. Their technical aspects which are mainly summarized from the specifications of the IEEE standards are presented.

4.2 Bluetooth

Bluetooth is an industry standard developed by Ericsson, which later was adopted by the IEEE 802.15 work group as a WPAN standard, IEEE 802.15.1. It can enable several devices to communicate with each other, overcoming problems of synchronization. Bluetooth is specifically aimed at short-range ad-hoc networking without the need for a pre-determined infrastructure. A summary of some key features of Bluetooth is provided in Table 4.1, which is extracted from IEEE 802.15.1 specifications (2003).

Table 4.1 - Key features of Bluetooth

Connection	Spread Spectrum(Frequency hopping)
Frequency band	ISM 2.4 GHz
MAC Scheduling	FH-CDMA
Transmission Power	>20 dBm
Aggregate Data Rate	0.723-1 Mbps
Typical Transmission Range	1-10m
Supported Stations	8 active devices
Voice Channels	3
Data Security-Authentication key	128 bit key
Data Security-Encryption key	8-128 bits (configurable)

4.2.1 Bluetooth protocol stack

Figure 4.1 shows the Bluetooth stack layer. According to IEEE 802.15.1 (2003), the devices set up links, which are then managed by the Link Manager (LM) layer. This layer operates above the baseband layer and physical layer (PHY). It uses

Link Manager Protocol (LMP) to negotiate features, and administer connections between users. The data sent by user needs to be reformatted into small packets before transition over the Bluetooth link, which is one of the main responsibility of the Logical Link Communication and Adaptation Protocol (L2CAP).

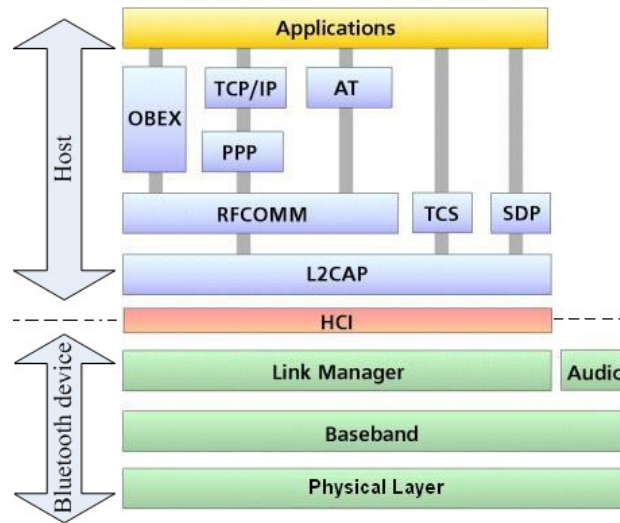


Figure 4.1 - Bluetooth protocol stack (adapted from (Rathi 2009))

4.2.2 Physical Layer

Bluetooth radio operates at Industrial, Scientific and Medical (ISM) 2.4 GHz frequency band. It uses frequency hopping (FHSS) technique to spread spectrum. This technique provides processing gain, which improves the chance of successful packet delivery in the presence of interference. Figure 4.2 shows the Bluetooth channel frequency hopping mechanism. 79 channels are used. Each channel has 1 MHz bandwidth. During communication, a Bluetooth system can make 1,600 hops per second evenly spread over the 79 channels according to a pseudorandom

pattern. Therefore if the system transmits on a bad channel, the next hop (which will occur $625 \mu\text{s}$ later), will hopefully be on a good channel (Gehrmann *et al.* 2004). In general, faster hopping between frequencies provides more spreading to resist interference. However, it will increase the complexity in implementation. Gehrmann *et al.* (2004) stated that “the hopping rate chosen for Bluetooth is considered to be a good trade-off between performance and complexity”.

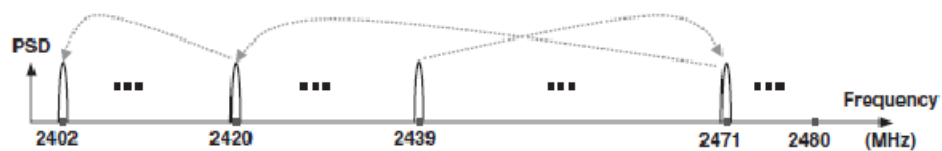


Figure 4.2 - Bluetooth basic operation mechanism – frequency hopping

It should be noted that the frequency hopping mechanism mentioned above is used in most countries. However some countries such as Spain and France have frequency range restrictions, therefore, they use special channel hopping algorithms. Table 4.2 lists the frequency range and the used channel frequencies in these countries and across the world.

Table 4.2 - Frequency spectrum of Bluetooth

Geography	Regulatory Range	Channels Frequencies (F)
Most countries	2.400-2.4835 GHz	$F=2402+ k \text{ GHz } 0 < k < 78$
Spain	2.445-2.475 GHz	$F=2.445+ k \text{ GHz } 0 < k < 23$
France	2.4465-2.4835 GHz	$F=2.4465+ k \text{ GHz } 0 < k < 23$

Gehrmann *et al.* (2004) stated that “a typical raw data transmission rate of Bluetooth is 1 Mbps, but due to various protocol overheads, the user data rates do not normally exceed 723 Kbps”.

Bluetooth supports three power classes, higher power class leads to longer transmission range. Table 4.3 lists the three power classes and their corresponding transmission range.

Table 4.3 - Power classes of Bluetooth

Class	Signal strength	Expected transmission range
Class 1	100 mw (20 dBm)	Long range up to 100m
Class 2	2.5 mw (4 dBm)	Ordinary range up to 10m
Class 3	1 mw (0 dBm)	Short range up to 10cm

4.2.3 Topology and Medium Access Control

A Bluetooth networks is often referred to as Piconet. A maximum of eight simultaneous devices can participate in a Piconet, which can comprise of one master device and one or more (up to seven active) slave devices. Each Bluetooth device is capable of assuming the master or slave role, depending on its configuration. The role of each device is determined during the initial connection. Usually a device that sends request for connection is determined as the master (i.e. the device that initializes the formation of the Piconet). Bluetooth provides both point-to-point and point-to-multipoint connections. Several Piconets can be connected together to form Scatternets (as shown in Figure 4.3). In a Scatternet,

one or more devices participate in more than one Piconet. However, they can only send and receive data in one Piconet at a time. In addition a master in one Piconet can be a slave in another Piconet.

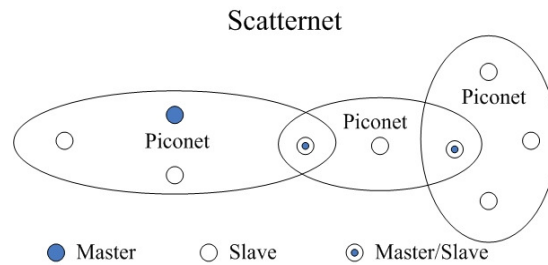


Figure 4.3 - Overlapping Bluetooth Piconets (or Scatternets)

Information exchange within the Piconet is accomplished by sending packets back and forth between Bluetooth-enabled devices (IEEE 802.15.1 2003). Full duplex communication is accomplished using a time division duplex mechanism. The master node within each Piconet determines which device can have access to the communication channel by addressing a slave. This slave will then have the right to send its data in the next time slot.

Bluetooth Piconet only permits master-to-slave and slave-to-master communication. Slave-to-slave traffic must go through a master. Gehrmann *et al.* (2004) argued that this property is suboptimal with respect to the aggregated system throughput.

In principle, a Bluetooth device can participate in more than one Piconet simultaneously (as illustrated in Figure 4.3). Different Piconets can work using time sharing scheme. “However it can cause practical problems, such as timing

issues and fulfilling Quality of Service (QoS) when a device is absent from the Piconet” (Gehrmann *et al.* 2004).

4.3 ZigBee

ZigBee conforms to IEEE 802.15.4 standard. The ZigBee alliance was formed prior to the formation of the IEEE 802.15.4 group. Later, the ZigBee Alliance and the IEEE 802.15.4 group decided to join forces and use ZigBee as the commercial name for this technology. However, the two groups still work on different parts of the technology. The IEEE 802.15.4 group has standardized the physical- (PHY) and the medium access control (MAC) layers (IEEE 802.15.4 2003), whereas the ZigBee alliance concentrates on the development of the upper layers and the overall development. Figure 4.4 shows the ZigBee protocol stack and the relations between IEEE 802.15.4 and the ZigBee Alliance in terms of the protocol.

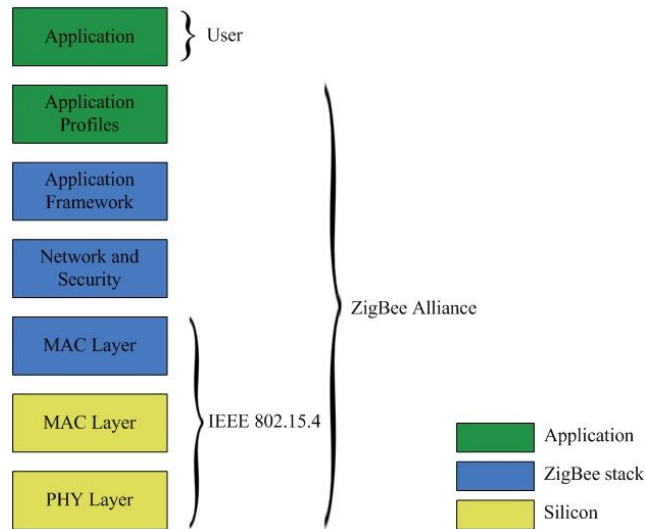


Figure 4.4 - ZigBee protocol stack

IEEE 802.15.4 defines two types of devices, Full Function Device (FFD) or a Reduced Function Device (RFD). An FFD can be configured to operate in three different modes: a coordinator, a router or an end device (IEEE 802.15.4 2003). An RFD on the other hand can only be used as an end device. Figure 4.5 shows device roles in the IEEE 802.15.4 and ZigBee standards. Today, most available ZigBee sensors are implemented as FFDs, which is also the case for the sensors used for experiments presented later herein. RFDs are intended to be even simpler, less expensive and more power efficient.



Figure 4.5 - Device Roles in the IEEE 802.15.4 and ZigBee Standard

In a ZigBee network, there is only one coordinator acting as a master node; all the other nodes including routers and end devices are slaves. The master node is in charge of channel selection and allocation to slave nodes. The reason being that a single radio transceiver is normally used, which cannot simultaneously work with more than one channel. To establish connection with end nodes or routers, the master node scans for channels that are not being used by other master nodes. If all channels have been occupied, the one which has the least energy level will be selected (IEEE802.15.4 2006). This channel will then be allocated for communication with the end nodes or the routers within the network. Thus to

communicate, the nodes in a ZigBee network use a single channel. Due to contention within the channel, transmission delay and data loss may occur. Therefore, it is important to limit the number of nodes in the network.

4.3.1 Physical Layer (PHY)

ZigBee standard offers three choices for the PHY for low-power operations. The differences in the choices lie in the frequency band used. They differ with respect to the data rate supported as shown in Table 4.4.

Table 4.4 - ZigBee specifications

Technology	ZigBee		
IEEE Specifications	802.15.4		
Frequency Band	868 MHz	915 MHz	2.4 GHz
Applied Area	Europe	America	Worldwide
Maximum Data Rate	20Kbps	40Kbps	250Kbps
Typical Range Indoor	10-100m		
Transmit Power	1-100 mW		
Receiver Sensitivity	-92dBm	-92dBm	-85dBm
Number of Channels	1	10	16
Channel Spacing	2M	2M	5M

It is worth noting that IEEE 802.15.4 introduced two optional specifications in 2006, which support high data rate up to 250 kbps, for the 868 and 915 MHz bands. However, due to their complexity in implementation and channel limitation, 2.4 GHz is popularly used for higher data rate. In the 2.4 GHz band,

the spectrum is divided into 16 equally spaced frequency channels as shown in Figure 4.6. Channels 1 to 11 are reserved for the lower frequency bands.

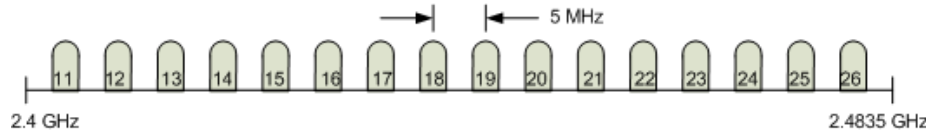


Figure 4.6 - IEEE 802.15.4 operating channels in the 2.4GHz band

The centre frequency of each band can be found from:

$$f_c = 2405 + 5 \times (k - 11) \quad (4.1)$$

where k is the channel number in the 2.4 GHz band (11-26).

The standard requires a receiver sensitivity of -85 dBm, and the defined transmit power from 0 dBm (1 mW) to -25 dBm (100 mW).

Transmission range relates to many factors including transmission power, and receiver sensitivity. Farahani (2008) calculated the estimated transmission range using:

$$R = 10^{\left[\frac{P_0 - F_m - P_r - 10 \times n \times \log_{10}(f) + 30 \times n - 32.44}{10 \times n} \right]} \quad (4.2)$$

P_0 : Transmit power (including the antenna gain, if any) in dBm

F_m : Fade margin in dB

P_r : Receiver sensitivity

n : Path-loss exponent

f : Signal frequency

For example, if a node transmits a 2450MHz signal with 0dBm (typical) output power to a receiver, whose sensitivity is -92 dBm (typical) in an environment with a path-loss exponent of 2.8 and a fade margin of 10dB, the estimated range is about 24 metres.

Increasing transmission power and improving receiver sensitivity can provide a longer transmission range; however, these will raise power consumption and complexity of sensor devices.

It should be noted that theoretically the highest data rate supported by a ZigBee channel is $C_p = 250$ kbps. However the calculation of this value does not take into account header bytes, CSMA waiting times, etc. Sun *et al.* (2005) stated the actual channel capacity (C) can be less than 142.86 kbps. The calculation of this value can be found in Appendix 1.

4.3.2 Medium Access Layer (MAC)

The MAC layer provides service to the upper layers, and enables the transmission and reception of MAC Protocol Data Units (MPDU) across the PHY data service. According to the IEEE 802.15.4 standard, features of the IEEE 805.15.4 MAC layer include beacon management, channel access, guaranteed time slots (GTS) management, frame validation, acknowledged frame delivery, association and disassociation.

Two different modes of operation are allowed; the beacon mode and the non-beacon mode. The latter is simpler, where the coordinator does not send out a

beacon. It should be noted that transmission of beacon will put extra payload on the network as well as consume more power. With intention of saving power and bandwidth, non-beacon mode is suggested for transmission of vital signs in RPM.

The channel access mechanism supported by the IEEE 802.15.4 MAC is Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) (IEEE802.15.4 2003). There are two types of CSMA-CA: slotted and unslotted. Slotted CSMA-CA is referred to as performing CSMA-CA while there is a superframe structure in place. A superframe divides the active period into 16 equal time slots. The back-off periods of the CSMA-CA algorithm need to be aligned to specific time slots for transmission. The unslotted CSMA-CA algorithm is used when there is no superframe structure; consequently, no back-off slot alignment is necessary. A nonbeacon-enabled network always uses the unslotted CSMA-CA algorithm for channel access.

In using the unslotted CSMA/CA algorithm to access the channel, before transmission, a ZigBee node performs Clear Channel Assessment (CCA) to sense the allocated channel to ascertain its availability. Some parameters (e.g. Maximum backoff number (NB) and Minimum backoff exponent (BE)) are used to control the number of attempts to sense the availability of the channel before declaring a channel access failure. More information on the effects of these parameters can be found in the work taken by Ko *et al.* (2006). Minimum back off exponent (BE) and maximum number of back offs (NB) are used to control the operations of CCA. If a sensor node detects the allocated channel is occupied, it

delays the transmission and waits for a random number (between 0 and $2^{BE}-1$) of unit periods to sense the availability of the channel again. NB controls the times of planned CCA operation. If a sensor still cannot access the channel when the value of NB get to its upper threshold (which is 4 in default), the sensor will declare a transmission failure and discard the waiting packet, resulting in data loss. Figure 4.7 illustrates the algorithm of unslotted CSMA/CA.

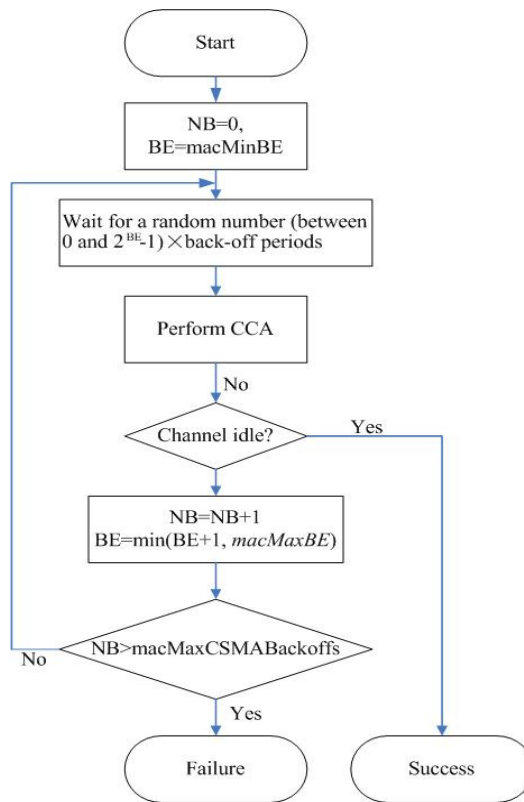


Figure 4.7 - Unslotted CSMA/CA algorithm

There are three main types of data transmission: from a coordinator to an end device, from an end device to a coordinator and between two coordinators. The

mechanisms for these transmissions depend on the mode. Figure 4.8 illustrates the data transmission mode between a coordinator and an end device, which is commonly used in a ZigBee WPAN.

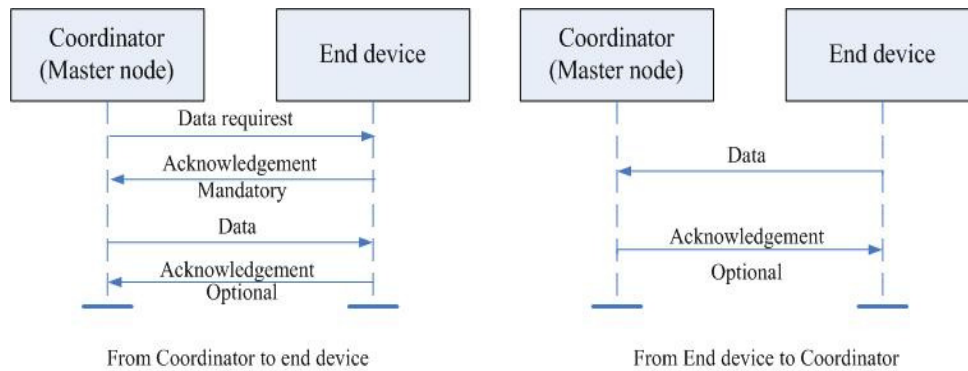


Figure 4.8 - Data transmission modes in a ZigBee WPAN

4.3.3 Topologies

The upper layers of ZigBee are responsible for the routing algorithms and for the gathering of data into packets. Two topologies are possible. They are Peer-to-Peer or Star. Based on Peer-to-Peer topology, ZigBee defines Mesh topology and Cluster Tree topology. Figure 4.9 shows these topologies.

Star topology is commonly used in RPM. A star-based ZigBee network uses the master (coordinator) and slaver (end devices) mode. The master node is usually put in the centre of a WPAN. It initiates the WPAN and control communication within the WPAN. Each WPAN has a unique WPAN Identifier (ID), which is used to distinguish data from other WPANs. A WPAN based on star topology is

commonly assisted by other communication networks like Ethernet to delivery information across distance.

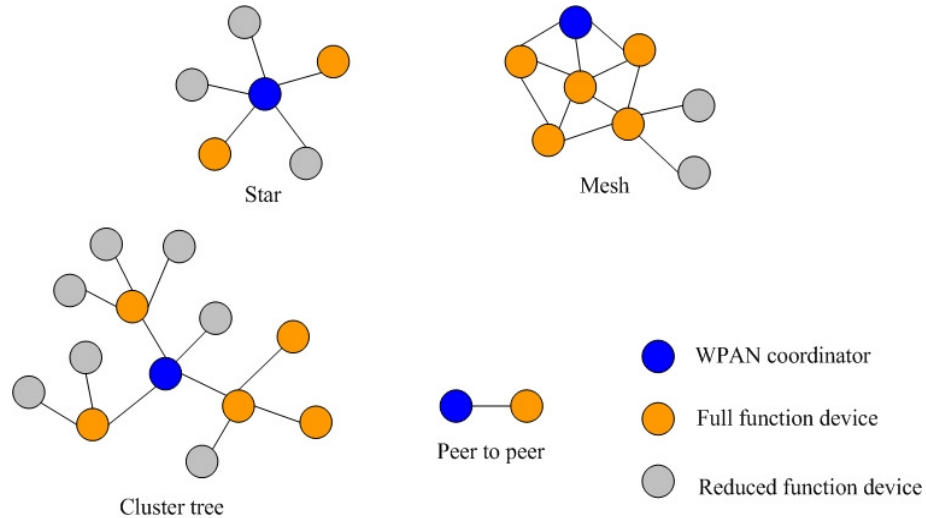


Figure 4.9 - Network topologies of ZigBee

Mesh network utilizes routers to relay message. This method can extend the range of the network. Sometimes it is referred to as multi-hopping because a message hops from one node to another until it reaches its destination. However the higher coverage comes at the expense of potential high message latency.

4.4 Comparisons between ZigBee and Bluetooth

Although ZigBee and Bluetooth are both short-rang communication technologies for WPANs, they have different characteristics. To understand the suitability of these technologies for RPM applications, several criteria need to be identified, such as: data rate, transmission range, power consumption and so on.

Comparisons of these aspects of Bluetooth and ZigBee can be found in Table 4.5. The table also includes the properties of Wi-Fi used in wireless LANs to illustrate possible frequency overlap, which is discussed later in this chapter. It can be observed that Bluetooth offers a higher data rate than ZigBee, it supports both data and voice communication. In contrast, ZigBee is designated for low-rate applications and it is not capable of sending large documents and audio. Both ZigBee and Bluetooth are short-range wireless technologies; however ZigBee have longer transmission range than Bluetooth. In addition ZigBee supports more active nodes in a WPAN than Bluetooth.

Table 4.5 - Properties of Bluetooth, ZigBee and Wi-Fi

Technology	Bluetooth	ZigBee		Wi-Fi (802.11g based)
IEEE Specifications	802.15.1	802.15.4		802.11
Frequency Band	2.4 GHz	868/915 MHz	2.4 GHz	2.4GHz
Supported data rate	1 Mb/s	250 Kb/s		54 Mb/s
Range (Indoor)	2-10 m	10-30m		38m
Support communication	data and voice	data		Mainly for data
Typical transmit power in mW	10	0.01-3.2		32-100
Size of stack	250kbits	4-32kbits		n/a
Basic cell	Piconet	Star		BSS
Max number of cell nodes	8	255		n/a

Low power consumption is a remarkable feature of ZigBee. A ZigBee node can survive for months powered by a primary battery making it suitable for some long-term self maintained applications. A ZigBee node sleeps most of the time

saving battery power, and then wake up, send data quickly, and go back to sleep again. Even sleeping nodes can achieve suitably low latency, because ZigBee can transition from sleep mode to active mode in 15 msec or less (Farahani 2008). In contrast, wake-up delays for Bluetooth are typically around three seconds, which is far larger than 15 msec.

By reducing the need for associated processing, ZigBee conserves still more power. ZigBee protocol stacks occupy very little memory that consumes less power than Bluetooth. The stack of a full function ZigBee device, as mentioned in the previous section, needs about 32 Kbits, and the stack of a reduced function device needs only about 4 Kbits. Those compare with about 250 Kbits for the far more complex Bluetooth technology (Legg 2004). In addition, ZigBee stack is free to public making it low-cost for implementation.

The ability to communicate with an Ethernet-based LAN allows WPAN devices to take advantage of services such as Internet access, file sharing and so on. Both Bluetooth and ZigBee have protocols that enable LAN access. Bluetooth has a profile that allows LAN access using the Point-to-Point Protocol (PPP). It does not provide LAN emulation or other methods of LAN access, just the features that are standard in PPP such as compression, encryption, authentication and multi-protocol encapsulation (Thraning 2005).

ZigBee supports LAN integration in order to send data to a longer distance. It can be argued that the increasing demand for integration of WPAN and WLAN may

drive the development of protocols for WPANs to enable access to wireless Ethernet directly. In current stage, a device that can be used as a bridge between ZigBee and LAN is required for integration. This type of devices normally includes two transmission modules to support ZigBee and LAN communication separately. Its size and power constraints may need further development to promote the integration.

Bluetooth and ZigBee, due to their characteristics, are suitable for different applications. In this section the comparison of them is restricted to the techniques that they employ. The suitability of their application in RPM will be further discussed in Chapter 5.

4.5 IEEE 802.11 Wireless Local Area Network (WLAN)

In contrast with technologies which use WPAN, wireless LANs have been used in a range of applications for many years. The IEEE 802.11 WLAN, also known as Wireless Fidelity (Wi-Fi), is mostly deployed for WLAN applications (Coleman and Westcott 2006).

A WLAN may either consist only of so called stations (STAs) running in ad-hoc mode, or it may consist of STAs and access points (AP) in infrastructure mode. These two modes are distinguished by the use of an access point (AP). An infrastructure Basic Service Set (BSS) networks has an AP to provide access to a wired LAN and distribution services like association within the WLAN. The AP

is used for all communications within the network, including communications between mobile nodes in the same service area.

Since the 802.11 has been standardized by IEEE, a number of task groups have been formed to add functionalities and improve performance of 802.11 WLAN. IEEE 802.11b, 802.11a, 802.11g and 802.11n are currently used for WLAN applications. Their key characteristics are summarised in Table 4.6.

Table 4.6 - Summarized IEEE 802.11 standards

	802.11b	802.11a	802.11g	802.11n
Spectrum	2.4GHz	5GHz	2.4GHz	2.4/5 GHz
Max data rate	11Mbps	54Mbps	54Mbps	144/300Mbps
Typical Power	30mW	25mW	30mW	30 mW
Protocol for Transmission	DSSS	OFDM	OFDM	MIMO-OFDM
Typical radius	38m	25m	38m	70m
Backward compatibility	With 802.11	None	With 802.11 and 802.11b	With 802.11a/b/g
Major advantage	Widely deployed High transmission range	Higher bit rate in a less crowded spectrum	Higher bit rate in 2.4 GHz/ Higher range than 802.11a	Highest bit rate Highest range 5 GHz mode enabled benefit low interference
Major disadvantage	Bit rate not enough for emerging applications	Smallest range of all 802.11 standards	Limited number of co-located wireless LANs	N/A
Current status	Widely Used	Limited use	Widely Used	Emerging

In this thesis, the focus is on the high bit rate extension, 802.11g (IEEE Std. 802.11g 2003), which allows for data rates of up to 54Mbps. The data rate is defined in terms of available bit rate, i.e. no overhead in the form of encapsulation

of data, collisions in the wireless media or processing delays in WLAN equipment are taken into account. The higher bit rates of 802.11g are achieved by using more advanced frequency modulation schemes, Orthogonal Frequency Division Multiplexing (OFDM). This scheme utilized multi-carrier modulation methods. A number of orthogonal sub-carriers are used to carry data to cope with severe channel conditions (e.g. narrowband interference, frequency-selective fading, etc.)

The IEEE 802.11n is an amendment to IEEE 802.11-2007 to improve network throughput over the two previous standards - 802.11a and g. It offers significant increase in the maximum raw data rate from 54Mbps to 600 Mbps by using Multiple Input and Multiple Output (MIMO) and 40 MHz channels. In addition, IEEE 802.11n can operate at 5GHz frequency band, which may benefit its usage in present of other wireless system using 2.4GHz, such as Bluetooth and ZigBee.

4.5.1 IEEE802.11 MAC Layer

The MAC layer of IEEE 802.11 is responsible for providing equal access to shared wireless media. Although the media is shared, two transmissions cannot occur at the same time, since both transmissions would probably fail because of interference. Access to the shared media is regulated by an Inter-Frame Space (IFS) time period that has to pass between the transmissions of each frame. The IFS takes on different values depending on the type of frame being sent. The operation of transmitting one frame is atomic, which means the operation has to finish before the next frame can be sent. A frame received from upper layers is

called a Service Data Unit (SDU), which is referred to as a MAC-SDU (MSDU) on the MAC layer. It is encapsulated by a header and checksum before being passed down to PHY as a MAC Protocol Data Unit (MPDU). The 802.11 general frame format can be seen in Figure 4.10.

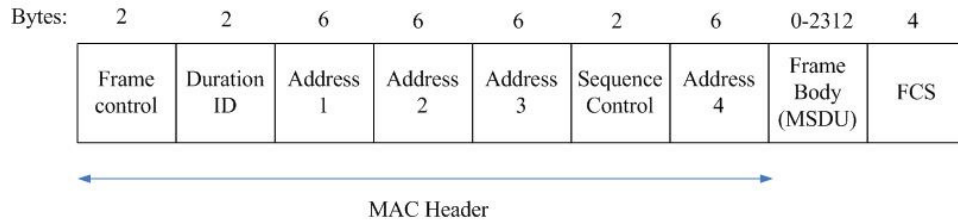


Figure 4.10 - General 802.11 Frame Format

There are three different frame types. Management frames, used for exchanging management information between STAs, control frames that controls the access to the media and data frames that are used for data transmission. The MAC layer is also responsible for encryption of the frames and fragmentation of the frames, if it is needed.

Two operating modes are offered, the Distributed Coordination Function (DCF) which is mandatory, and the Point Coordination Function (PCF) which is optional. In the simulation of using wireless LAN in RPM (in Chapter 8), only DCF is considered. DCF in turn offers two access methods, Basic Access (BA) which is mandatory and ready to Request/Clear to Send (RTS/CTS) which is optional.

DCF is sometimes referred to as contention mode, since each sender has to contend for access to the media. Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA) protocol is used to control media access, which is also utilized by ZigBee MAC layer (please refer to section 4.2.3). This protocol is designed to avoid collisions on the media by having a sender check whether the media is busy prior to sending data. However a collision could still occur because of the hidden STA problem. In addition severe contention on the transmission media will result in data loss and increased transmission delay, which will be discussed in Chapter 8.

Prioritized access may be useful in the contention mode. It is worth mentioning that the 802.11e group defined a set of Quality of Service enhancements for WLAN applications through modifications to the MAC layer. Priority of access to the wireless medium has been considered in this standard, which could be useful in some applications that data transmissions have different urgent levels. For example, in a hospital WLAN, transmission of patients' vital signs can be critical, which should get higher priority, compared to other applications like network printing.

4.5.2 IEEE802.11 Physical Layer

The Physical layer (PHY) of 802.11 acts as an interface between the MAC layer and the wireless media. As such, it is responsible for the actual transmitting of frames and for sensing whether the channel is idle or not and reporting this back

to the MAC layer. The 802.11 standard supports three different PHYs, of which the Direct Sequence Spread Spectrum (DSSS) is the most common used. DSSS works in conjunction with different modulation schemes to represent data bits as symbols before transforming and spreading the energy of the transmitted signal in a wider frequency range. This makes it easier for the receiver to pick up the signal and recover the frame sent.

Table 4.6 shows the specification of IEEE 802.11 standards. It can be found that IEEE802.11g uses ISM 2.4GHz frequency band and provides 13 channels. Among them, channels 1, 6 and 11 are commonly used, with 25MHz separation. Sharing the frequency band with other technologies (for example Bluetooth and ZigBee) can create interference.

4.6 Interference Issues of WLAN on WPANs

Operation in the 2.4 GHz ISM band provides the convenience of an unlicensed band with availability worldwide. Wireless devices used by WLAN and WPAN technologies (Bluetooth or ZigBee) operate on this frequency band, which can create interference. The interference will degrade the performance of the wireless system. In particular, due to higher power level used, Wi-Fi signals can create significant noise for the devices used in WPANs. Therefore careful consideration should be taken in using both WPAN and Wi-Fi technologies for transmission of vital signs in RPM. In this section, the interference issues caused by Wi-Fi on Bluetooth and ZigBee are discussed.

4.6.1 Interference of Wi-Fi on Bluetooth

Bluetooth and Wi-Fi have already been widely used to support various wireless applications. Both of them work at licence-free ISM2.4GHz band. Bluetooth uses the FHSS method to spread their signals, whereas Wi-Fi uses DSSS to provide processing gain, which improves the chance of successful packet delivery when interference is present. However, due to the higher transmission power used by Wi-Fi, it creates higher noise level to Bluetooth signal (Ullah 2009).

Figure 4.11 shows the channels used by Wi-Fi (a) and Bluetooth (b). It can be argued that a Wi-Fi channel has 22 MHz bandwidth which may cause interference on at least 22 Bluetooth channels. Therefore, if a nearby Bluetooth device is using all 79 channels for frequency hopping, the chance of interference between a single Wi-Fi STA and a Bluetooth node can be 22 out of 79 hops, which is approximately 28%.

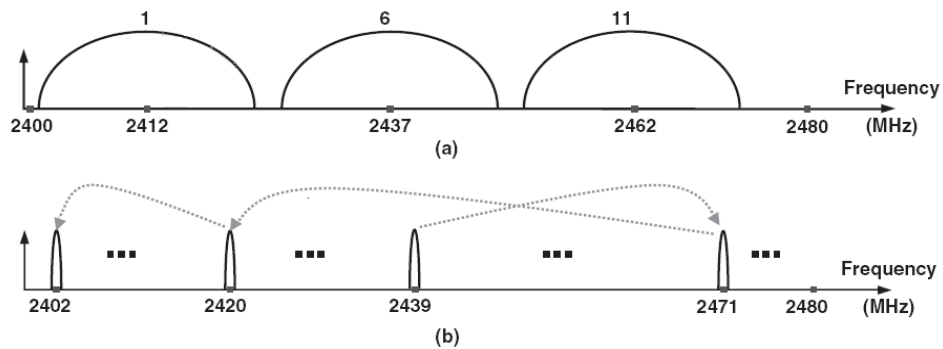


Figure 4.11 - Channel overlaps between Wi-Fi and Bluetooth channels (a) Wi-Fi channel (1, 6 and 11), (b) Bluetooth channel

The interference between Wi-Fi and Bluetooth does not entirely block each other's transmissions. However the interference can degrade the performance of both technologies. To improve the performance in the presence of interference, the IEEE 802.15 coexistence Task Group 2 (TG2) was formed in order to address the issue of coexistence of Bluetooth WPAN with WLAN (IEEE 802.15.2 2003). In addition, the Bluetooth Special Interest Group (SIG) formed its own task group to study techniques for alleviating the impact of interference (Golmie 2006).

A collaborative scheme called Bluetooth interference aware scheduling (BIAS) was proposed which intended for Bluetooth and IEEE 802.11 protocols to be implemented in the same device (Norgall *et al.* 2004). This scheme is based on MAC scheduling, for example the priority is given to Bluetooth for transmitting voice packets, while IEEE 802.11 is given the priority for transmitting data. However, an applicable solution is still required, which can allow the integration of Bluetooth and Wi-Fi network technologies for seamless data transmission.

Adaptive Frequency Hopping (AFH) technique was developed (Hodgdon 2004). It identifies the channels where interferences are present and marks these channels as "bad channels". Then the sequence of hops is modified such that the frequency channels with high-level interference are avoided. The bad channels in the frequency-hopping pattern are replaced with good channels via a lookup table. The Bluetooth master may periodically listen on a bad channel and if the interference has disappeared, the channel is remarked as a good channel. Bluetooth slaves can also send a report regarding the channel quality to the master

if necessary. The AFH method not only improves the performance of the Bluetooth network, it also reduces the effect of the Bluetooth network on other nearby networks working on 2.4GHz.

An experiment was carried by Golmie *et al.* (2005) to investigate the efficiency of AFH in the presence of Wi-Fi interference. The results showed that the packet loss rate of Bluetooth was 16.3% initially. By using AFH, it was dropped to 7.5%. Another study carried out by Shuaib *et al.* (2006) showed that Wi-Fi throughput dropped 4.6% due to Bluetooth interference, whilst Bluetooth throughput dropped 17% due to Wi-Fi interference. Both studies were carried with the assumption that Bluetooth devices worked alongside a Wi-Fi device (with distance 1-2 metres).

Therefore it can be argued that due to the high packet loss rate caused by the interference problem, Bluetooth is not suitable for transmission crucial information such as vital signs in an environment, where Wi-Fi signal may be present.

4.6.2 Interference of Wi-Fi on ZigBee

An IEEE 802.11b/g node has typical transmitter output power between 12 to 18 dBm, sometime it may be as high as 30 dBm (IEEE 802.11 2003). This is significantly higher than the typical output power of a ZigBee node (0 dBm). Therefore a WLAN can be the source of severer interference with a ZigBee network. However, Farahani (2008) indicated that ZigBee may utilize some methods to improve its coexistence performance, for example:

Dynamic RF Output Power Selection

This method is to adjust the RF output power of the transmitter based on the channel condition and the distance between the nodes. Typically, the RF output power is set to the lowest level which corresponds to an acceptable level of communication reliability. Reducing the transmitter output power decreases the interference with other nearby wireless devices, but the recipient of the signal becomes more susceptible to the interference. If several attempts to deliver a packet have failed, the transmitter RF output power can be increased to improve the signal to noise ratio. Increasing the signal power can improve the chance of successful packet delivery at the potential cost of increasing interference with other wireless nodes. However this method may cause decrease on battery life. It has been rarely employed by current industry.

Frequency Channel Selection

Changing the frequency channel when the energy of the interferer signal in the desired channel is unacceptable can be a simple way of addressing the interference problem. ZigBee Professional version (ZigBee Pro) provides frequency agility capability that allows the entire network to change channels in the face of interference (ZigBee Alliance 2007). However this version has not been widely adopted, most commercially available ZigBee modules do not support frequency agility.

Farahani (2008) stated “if the frequencies of operations and bandwidths of the interfering signals in the nearby networks are known, the frequency channel of the ZigBee network can be selected accordingly to minimize the effect of interfering signals”. For example, if three non-overlapping Wi-Fi channels 1, 6 and 11 are used, there are certain frequency bands that stay unoccupied and can be used by the ZigBee network. As shown in Figure 4.12, ZigBee channel 15, 20, 25 and 26 are four interference-free channels. With channel allocation mechanism, a ZigBee WPAN can easily find one of the four interference-free channels. In this case a ZigBee WPAN can operate alongside a WLAN, as well as communicating with them. Figure 4.12 also shows the channel overlaps between ZigBee and other Wi-Fi channels.

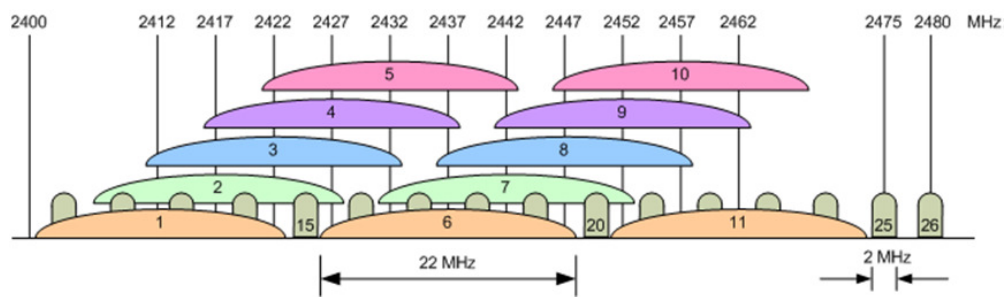


Figure 4.12 - Channel overlap between IEEE 802.15.4 and IEEE 802.11g

Collaborative methods

The above methods are called non-collaborative methods. There are collaborative methods for improving the coexistence performance of ZigBee networks. In collaborative methods certain operations of the ZigBee network and the other

network (e.g., an IEEE 802.11b/g network) are managed together. For example a ZigBee network and an IEEE 802.11b/g network are synchronized; every time one network is active, the other network stays inactive to avoid packet collisions. Fundamentally it is a Time Division Multiple Access (TDMA) method, which has been considered for implementation. For example, Jung *et al.* (2008) proposed to adopt an interference mediation scheme with a fairness-based TDMA scheme to optimize ZigBee network performance. This scheme could benefit ZigBee networks to work alongside Wi-Fi networks. However, Sahandi *et al.* (2010) believe the future replacement of current IEEE 802.11g with IEEE 802.11n could resolve this problem completely, because IEEE 802.11n can operate at 5 GHz. In that case, an integrated wireless RPM system can be developed for general hospital wards.

4.7 Security Issue

In a wireless network, the transmitted messages can be received by any nearby listener, including an intruder. In very simple applications the security might not cause serious problems, however in other applications an intruding device capturing the messages or resending modified messages can cause issues. In a wireless RPM system, patients' privacy can be violated if unauthorized people gain access to the server for storing patients' information at any time.

Security issue could be understood to encompass two aspects: confidentiality and integrity. Gehrman *et al.* (2004) indicated that confidentiality of data can be

implemented by transforming the original data (also referred to as the plaintext) into the ciphertext. After a parameterized transformation, the ciphertext does not reveal the content of the plaintext, while the plaintext can be recovered from the ciphertext. This transformation is called encryption.

“Integrity is about ensuring that data has not been replaced or modified by an eavesdropper during transport or storage” Gehrman *et al.* (2004). User authorization can be planned to improve data integrity.

Bluetooth Security

In general Bluetooth security aspects can be divided into three modes:

- Mode 1: non-secure
- Mode 2: service level enforced security
- Mode 3: link level enforced security

In Mode 1, a Bluetooth device does not take any security measures. In Mode 2, “security procedures, namely authentication, authorization and optional encryption, are initiated when a Logical Link Control and Adaptation Protocol (L2CAP) channel request is made” (Haataja, 2006). The difference between Mode 2 and 3 is that in Mode 3, the Bluetooth device initiates security procedures before the channel is established.

Bluetooth supports authorization and encryption for encoding exchanged information between two devices. In the initial stage of Bluetooth security option,

a Personal Identification Number (PIN) code (1~16 bytes in length) is used by two communicating devices which use Bluetooth (Haataja 2006). The devices then use this PIN with their Bluetooth 48-bits device addresses and an unencrypted 128-bit random number to generate an initialization key. The initialization key is then used for securing the generation of other 128-bit random numbers (link key) during the next phases of the event chain. A combination key is derived from this information of both devices. It is used in the next phase for challenge-response authentication. During each authentication, a new unencrypted random number is exchanged. The claimant returns a signed response to the verifier. The verifier compares the value of received signed response with its calculated value for authentication. If they are matched, both devices compute an authenticated ciphering offset, which is then used in generating an encryption key for symmetric encryption. Figure 4.13 illustrates the operation of Bluetooth security.

However, Scarfone and Padgett (2008) pointed out that Bluetooth has some security vulnerabilities. For example: short PINs are used for the generation of link and encryption keys, which can be easily guessed; PIN management is lacking. Link keys are stored improperly, that can be read or modified by an attacker etc. These vulnerabilities can be used for Bluetooth-related attack, for example Bluesnarfing, Bluejacking, Bluebugging and so on (Khan and Siddiqui 2009). It can be argued that the attacks are threatened to the safety of using a Bluetooth-based health monitoring system, where confidentiality and integrity of vital signs should be secured.

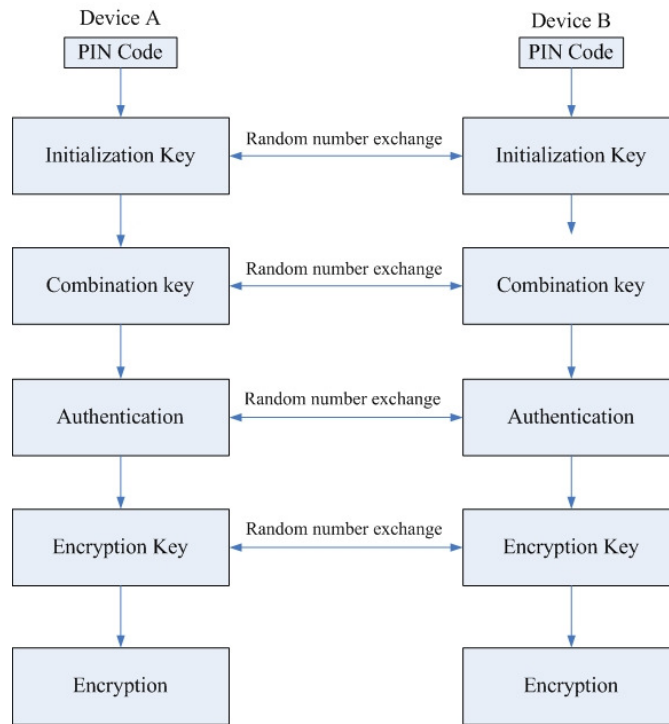


Figure 4.13 - Bluetooth security operation (adapted from (Haataja 2006))

ZigBee Security

The ZigBee standard supports the use of Advanced Encryption Standard (AES) (Farahani 2008). In AES, each encryption algorithm is associated with a key. The algorithm itself is public knowledge and available to everyone, but the value of the key in each transmission is kept secret. There are different methods to acquire a security key. For example, the key can be embedded in the device itself by the manufacturer. Alternatively, a new device that joins a network may get its security key from a designated device in the network. Figure 4.14 shows the concept of using encryption.

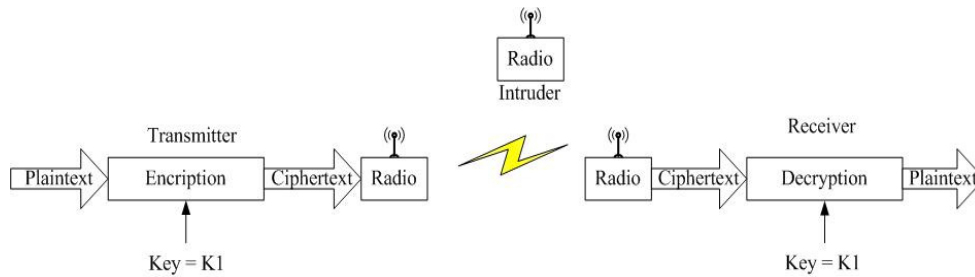


Figure 4.14 - The use of encryption

The key used for encryption is a binary number. The number of bits in a key will determine the level of security. ZigBee supports the use of 128-bit keys, which means there are 2^{128} (approximate 3.4×10^{38}) possible keys. Farahani (2008) believed that it is computationally infeasible to try 2^{128} different keys. Although it can be argued that rapid development of computing technique would support the calculation of the 128-bit keys in the future, new encryption approach may also be available to improve ZigBee security.

The receiver in Figure 4.14 is using the exact key as the transmitter to perform decryption, which is known as the symmetric key method. The ZigBee standard supports only symmetric key cryptography. The ZigBee standard provides methods to establish keys and share the keys between two or more devices. Considering that the algorithm itself is known by the potential intruder, the main effort is to ensure that the key is not distributed beyond the intended recipients.

The AES algorithm itself is a series of well-defined steps that use the provided key to shift and mix a block of data to create an encrypted version of the same block of data. In AES, the size of this block of data is always 128 bits. But the key

can be 128, 196, or 256 bits. The ZigBee standard uses the 128-bit key option. All these steps are invertible and the receiver that holds the correct key can perform the reverse steps to recover the original message. The AES has been announced as a standard by the National Institute of Standards and Technology (NIST) in 2001. According to the committee on national security systems, the design and strength of the AES algorithm is sufficient to protect even classified information up to the secret level (Sikora and Gorza 2005).

The ZigBee standard supports both device authentication and data authentication. The new device must be able to receive a network key and set proper attributes within a given time to be considered authenticated. In data authentication, the receiver verifies if the data itself has been altered or changed.

Any secure ZigBee network has a designated device called the trust centre that distributes security keys across the network. There is only one trust center in each network. The ZigBee coordinator determines the address of the trust center. In a star-based ZigBee network, the coordinator itself normally acts as the trust center. The device authentication procedure is performed by the trust center. When a device joins a secure network, it has the status of “joined, but unauthenticated.” If the trust center decides not to authenticate the newly joined device, the trust center will request the device be removed from the network.

In practice, ZigBee offers a security toolbox to ensure reliable and secure wireless communication. The security toolbox includes access control lists, data freshness

timer and 128-bit encryption as well as supported the use of a Message Integrity Code (MIC) (Thraning 2005). It consists of key management features that allow user remotely manage a ZigBee network. By using the security toolbox, a ZigBee network developer can choose the necessary security method for the application, providing a manageable trade-off against data volume, battery life, and system processing power requirements.

IEEE802.11 Security

In wireless LAN system, the data sent can be intercepted by anyone within signal range using compliant equipment. Also, a non-authorized user may gain access to network resources, especially since the AP in many WLANs uses the dynamic host control protocol (DHCP). To prevent these problems, wired equivalent privacy (WEP) was introduced with the 802.11 standard. It was supposed to offer a level of security comparable with wired LANs, where physical access is needed to intercept traffic or use network resources. WEP uses a pre-set 40 or 104-bit secret key known by each STA in a WLAN prior to transmission. It then adds a 24-bit Initialization Value (IV) to the secret key to form the encryption key to encrypt the data.

However, WEP may be easy to be decrypted by a non-authorized user, since the secret key is static and needs to be changed manually on every STA in a WLAN. Also, WEP provides weak support for authentication. If the WLAN uses DHCP, the association with an AP is automatic. By default, an AP sends out a so-called

Service Set Identifier (SSID) which is necessary for a STA to associate itself with the AP. Since the secret key may be broken, WEP provides no protection at all against non-authorized users. Three methods will make it harder to gain access to the WLAN: using only static IP addresses; using an access list based on MAC addresses of STAs in a WLAN; disabling the SSID broadcast. However, a non-authorized user still can eavesdrop on transmissions in the WLAN, and take over the identity of a STA in the WLAN.

IEEE802.11i provides better protection for WLAN. It employs an authentication server, an entity which participates in the authentication of two or more wireless nodes, including the access points. The authentication server can authenticate the nodes itself, or it provides material for use by wireless nodes to authenticate each other. After authentication, an 802.11i supported device must also gain authorization for further service access. The core requirement for WLAN access is the verification of a wireless client authorization to send and receive IP packets. Therefore, wireless networks need a back-end authorization infrastructure. To summarize, the authentication and authorization process includes three basic stages, as Figure 4.15 demonstrates:

1. An initial authentication mechanism used in order to identify valid client.
2. A key is exchanged and distributed to mutually agree on a secret key between the AP and the client (BS), which will be used for subsequent activities.
3. A data packet authentication protocol (based on the secret key) for subsequent data communication.

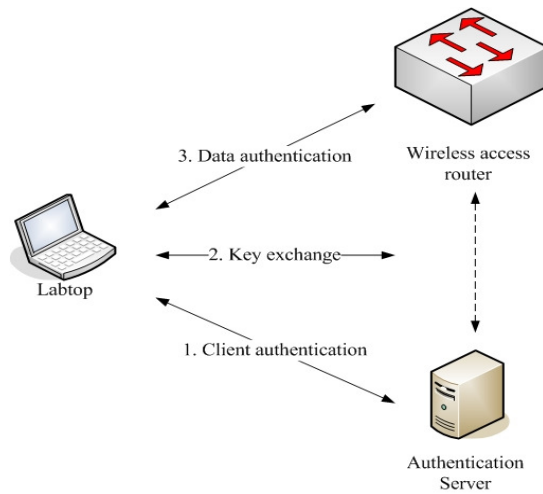


Figure 4.15 - Basic authentication and authorization process used by Wi-Fi

The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as WPA2, also called RSN (Robust Security Network).

4.8 Summary

Characteristics of three wireless network technologies were discussed. They included Bluetooth, ZigBee and Wi-Fi. ZigBee due to its low power consumption would be more suitable for long-term RPM compared to Bluetooth. Wi-Fi technology was also explored. Due to the same frequency band used by the three technologies, interference issues need to be taken in to consideration. In this chapter, some methods that could reduce the effects of interference were discussed. Finally, security issues when using wireless network technologies were discussed. In the next chapter, application of these wireless network technologies in RPM will be discussed.

CHAPTER FIVE

5 RPM using Wireless Network Technologies

5.1 Introduction

Application of wireless network technologies in healthcare have attracted increasing interests amongst researchers, healthcare providers, governments and so on. Their applications provide ubiquitous communication, making it possible to access information anywhere anytime. Remote Patient Monitoring (RPM) is a field that can benefit its further improvement from wireless network technologies. A typical RPM system (as shown in Figure 5.1) includes three functional parts implementing data acquisition, transmission and analysis. A bedside monitor in a data acquisition process obtains vital signs measured by sensors. The vital signs are then transmitted through a network to a control room, which is a centre for monitoring, analyzing and storage.

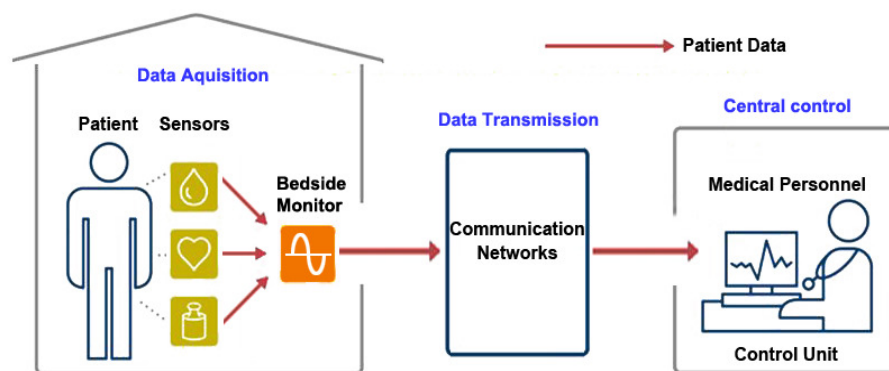


Figure 5.1 - Architecture of a typical RPM system

5.2 Data Acquisition in RPM using Wireless Sensor Networks

5.2.1 Wireless Sensor Networks for Data Acquisition

The sensors used in data acquisition are normally wired, which restricts mobility and comfort of patients. Application of wireless biomedical sensors can improve patients' comfort. Some sensors that are used to obtain vital signs have already been introduced in Chapter 3. They can be used in a wireless sensor network to support multiple-parameter monitoring of an individual patient.

Early research in the application of wireless sensor network in RPM saw the adoption of one or more wireless biomedical sensors which were attached to a patient. The sensors communicate directly with a controller (such as a PDA) in a star network (shown in Figure 5.2). The application of mesh-network was later introduced. Examples include Schwiebert *et al.* (2001), who examined power-efficient network topologies under the assumption that the sensor node positions were fixed. However, star-based sensor networks referred to as Wireless Personnel Area Networks (WPAN) are widely used in RPM. Some examples include:

- eWatch, a wearable platform sensing motion and temperature (Maurer *et al.* 2006)
- HealthGear system, which is used to the detection of sleep apneas events (Oliver and Flores-Mangas 2006)
- A wireless ECG monitoring system based upon a WPAN including wireless ECG sensors and a mobile phone (Hong *et al* 2007)

- Espina *et al.* (2008) developed a WPAN-based RPM system for continuous blood pressure monitoring.
- Haahr *et al.* (2008) used pulse oximeter, electromyography (EMG) sensors and a PDA to develop a WPAN for RPM.

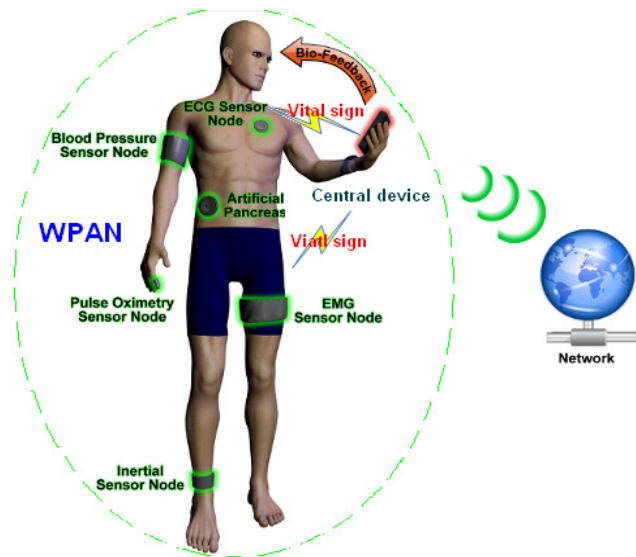


Figure 5.2 - The architecture of a WPAN for data acquisition

5.2.2 Bluetooth and ZigBee-based Sensor Networks for Data Acquisition

A wireless sensor network may be based on various technologies. Bluetooth and ZigBee are two suitable technologies for wireless sensor networks. Their technical properties have already been discussed in Chapter 4. In a RPM system, a Bluetooth or ZigBee based sensor network may communicate externally with other networks such as Wireless LAN (Wi-Fi), GSM, GPRS, etc., allowing a wide coverage area and offering the possibility of ubiquitous wireless connectivity.

Bluetooth-based sensor networks have already been used in RPM. They are based on star-topology. A PDA or Smartphone may be used as a central device in a Bluetooth WPAN. It gathers data from sensors attached to a patient and sends the data to medical personnel (please refer to Figure 5.2).

Since PDA and Smartphone are computing devices, they were also used to process patient's data locally and monitor the patient's condition as well as providing warnings in some RPM systems. For example, the Ubiquitous Monitoring Environment for Wearable and Implantable Sensors (UbiMon) is a project conducted by Imperial College London, UK (Lo and Yang, 2005). This project aimed to provide a continuous and unobtrusive monitoring for patients with arrhythmic heart disease. A Bluetooth-based WPAN worn by a patient was used to collect vital signs (ECG, SpO2 and temperature). Vital signs are gathered by a PDA (they referred to as Local Processing Unit) carried by the patient. The PDA processed the data in order to capture transient events of abnormalities. When an abnormality is identified, the PDA sounds an alarm. The patient then decides whether or not to send the data to medical personnel. In UbiMon system, the PDA acts as an intelligent local consultant and a gateway between WPAN and long-range mobile network (using GPRS service). Although the system can implement RPM, patient's manual operations are required and RPM is just a supplement of local monitoring and consultant.

A similar example is MobiHealth that aims to provide continuous monitoring of patients outside the hospital environment (MobiHealth 2008). It consists of a

Bluetooth-WPAN which comprised various biomedical sensors and a PDA. The PDA is used in the same way as in UbiMon. However it can automatically send notification to medical personnel through GPRS/UMTS message services, which minimized patient's manual operations. The system also supports medical personnel in respect of on-demand remote monitoring of a patient's live/historic data. A medical personnel located in a control room can send commands to the PDA and request data for observation. Although UbiMon was proposed to support continuous RPM, power supply was a major problem. Broens *et al.* (2007) proved that a UMTS terminal (e.g. Nokia telephone) transmitting data continuously would empty its battery in less than 2 hours (at best). Furthermore the Bluetooth WPAN can only work for 9 hours supporting continuous local monitoring (MobiHealth 2008).

In addition to high power consumption, Bluetooth has other limitations which have been discussed in Chapter 4. For example, a Bluetooth WPAN can only support up to seven active nodes for transmission in RPM. This limits the number of sensors for multi-parameter RPM. A Bluetooth WPAN is easy to be interfered by other Bluetooth WPANs and wireless systems working at 2.4 GHz. These limitations may also affect its usability for RPM on general hospital wards.

To respond to an overwhelming need for continuous monitoring of vital signs of patients within a general ward, a low-power WPAN with a common architecture and the ability to handle multiple sensors should be implemented. Low-power ZigBee sensor networks can meet this demand.

ZigBee technology conforms to IEEE 802.15.4 standard which is designed for simple, low-cost, low-power consumption WPANs (please refer to Chapter 4). In addition, the features make it more suitable for RPM on general wards are:

- Scalability: A ZigBee network is capable of supporting up to 65,534 nodes; a coordinator (master node) can manage up to 255 active nodes at a time.
- Data rate capacity: ZigBee provides the maximum data rates at 250 kbps in the 2.4 GHz band, 40 kbps in the 915 MHz band and 20 kbps in the 868 MHz band. These are sufficient for the transmission of vital signs of a patient, which normally require several kbps, e.g. Blood pressure and ECG require 1.2 kbps and 6 kbps respectively (Khan *et al.* 2008).
- Cost: Compared to Bluetooth, ZigBee can be treated as a cost-effective solution for its implementation and maintains in RPM (Vershny 2009).

Applications of ZigBee-based sensor network for continuous RPM have been considered in some projects. Khan *et al.* (2008) proposed a star-based ZigBee network for RPM on a general ward where four patients reside (as shown in Figure 5.3). The network consisted of a master node and twenty sensor nodes. The master node connected with a local PC through RS232 cable. It collected vital signs from the ZigBee-based sensor nodes and sent them to a database on the PC. Medical personnel could then retrieve the data remotely from the local PC. Khan *et al.* (2008) claimed that their system could easily be developed by integrating a ZigBee network with existing hospital Ethernet-based network.

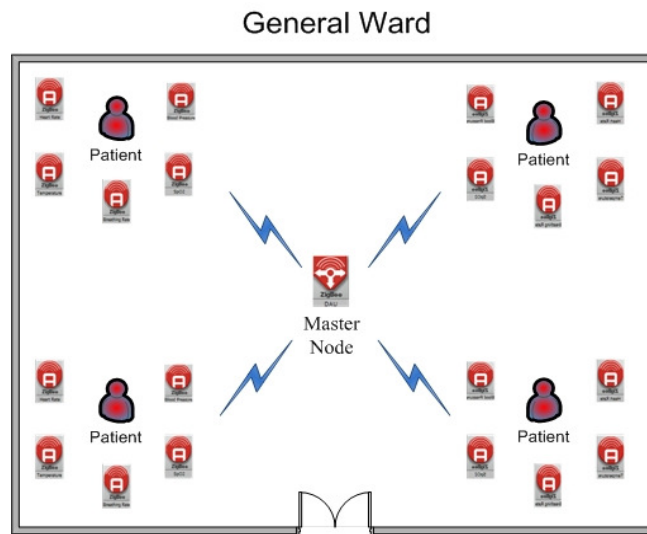


Figure 5.3 - A single ZigBee network approach

However, Sahandi *et al.* (2010) indicated that the system based on a single ZigBee network had limitations. For instance, the distance between the sensors and the master node can be an issue. A typical transmission range for ZigBee is 10 metres. Patients located outside this coverage area cannot be monitored. Khan *et al.* (2008) argued that “10 metres is sufficient for monitoring four patients residing in a ward”. However, some general wards can be larger, accommodating more patients. In those wards, a single master node will not be able to support data transmission of all the sensors attached to all the patients. Further, a master node within a WPAN normally communicates using a single channel. The maximum bandwidth for such a channel is 250 kbps (142.83 in reality, please refer to Appendix 1) that is shared by all the sensors in the WPAN. The communication of a large number of sensors using a single channel generates transmission delays due to the CSMA/CA mechanism used by the network. Therefore, it can be

argued that a single ZigBee network may be unable to support data transmission for all the sensors in a large ward with more patients.

A multiple ZigBee-WPAN-based RPM is proposed in this project. The difference between this and the single WPAN RPM is in the number of master nodes which are used. In a single WPAN only one master node is used for the entire sensor network. Whilst in the multiple-WPAN approach, a master node is used in every WPAN for each patient. Sensors within each WPAN gather vital signs from a patient and transmit them to their master node within this network. The master node collates the data received into a single packet for efficiency and transmits it through a network to a control unit for monitoring and storage. Figure 5.4 shows this multiple WPANs approach for RPM on a ward.

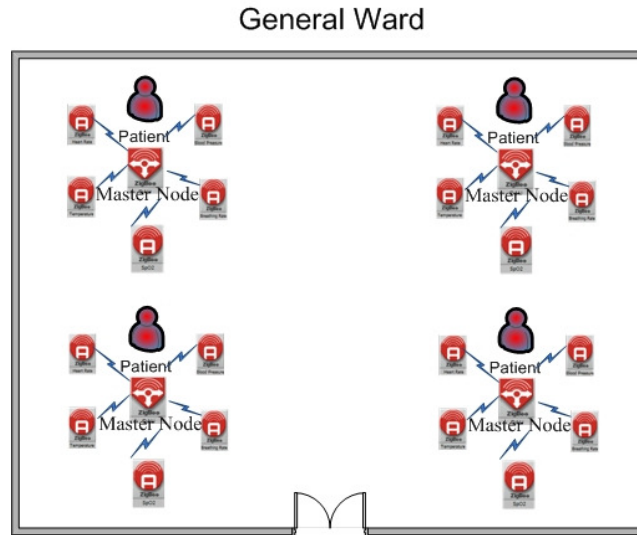


Figure 5.4 - Multiple-WPAN approach for RPM on a ward

Due to the short distance between the devices in this approach, the transmitted data will be received by the master node with sufficient signal strength, reducing the possibility of errors and data loss. To reduce interference and avoid frequency overlaps, the WPANs, particularly those adjacent to each other, will be using different transmission channels for communication between the sensors and the master nodes. This is facilitated by the ZigBee channel allocation mechanism. Further, the master nodes only communicate with the sensors within their own WPANs, thereby reducing the volume of traffic communicated as well as the latency. To compare the performance of single-WPAN approach and the proposed approach, both scenarios are simulated using network modelling and simulation tool, OPNET. Detailed information and simulation results are discussed in Chapter 8.

Although the implementation of multiple ZigBee WPANs in RPM will increase the cost, it provides higher reliability for data transmissions. Further allocating a master node per patient will improve data integrity in RPM. For instance, each master node can integrate patient identification with packaged data to avoid misrepresentation. Also, data transmission intervals can be adjusted based on individual patient's condition.

However the proposed multiple-WPAN approach may encounter the problem of channel frequency overlaps (Sahandi and Liu 2010). WPANs sharing a frequency channel may cause increased transmission delay and consequently data loss. Therefore the problem of channel frequency overlaps needs careful consideration

when using multiple WPANs. The channel frequency overlap problem was investigated in simulation, which will also be discussed in Chapter 8.

5.3 The Use of Wi-Fi in RPM

ZigBee is a short-rang wireless network technology. Therefore an additional network is required to deliver vital signs from ZigBee WPANs to the central control room which may be at a distance in a general ward. Ethernet-based Local Area Networks (LANs) is suitable for this task, which are also widely used in hospitals. Particularly since many hospitals with older structures and buildings may not have suitability for LANs. Wireless Ethernet LANs (Wi-Fi) by offering highly flexible means for data exchange can facilitate this.

Some works have already been done to use Wi-Fi in RPM in hospitals. For example, in the MedLAN project, a Wi-Fi based network was designed to transmit real-time video and audio from Accident & Emergency (A&E) units to a physician for remote monitoring and consultation (Banitsas *et al.* 2001).

At the Jikei University Hospital in Minato-Ku, Japan, a wireless reporting system was developed using Wi-Fi. The system consisting of a picture archiving and communication system, a diagnostic server and portable laptops, is used by radiologists, physicians and technologists to review prevalent radiology reports and images and instantly compare them with reports and images from previous examinations (Yoshihiro *et al.* 2002).

Wi-Fi also plays the key role in the PDA-based system which has been discussed in Chapter 2. As it was discussed, through Wi-Fi, PDAs can upload valuable data from the patients directly into the centralised monitoring system.

In addition, in a network based system, patients' information can be shared among medical personnel. For example, University of Aarhus in the AWARE project used Wi-Fi to share patient's record among 20 mobile medical personnel carry a PDA within a hospital (Hansen 2006). A doctor can use his/her PDA to download a patient's information stored on some other personnel's PDAs for display and review. He/she can also input new information or send text messages to some other medical personnel through Wi-Fi.

Widely adoption of Wi-Fi technology in hospitals has made it possible to use it together with ZigBee in RPM on general wards. In such a case vital signs can be sent from patient to medical personal wirelessly and seamlessly. Some problems need considerations to address the reliability of transmission in using wireless technologies for healthcare. Wi-Fi technology uses shared bandwidth which limits the capacity of the network. In the event of capacity overflow, vital signs cannot be delivered to the control unit, which will cause the failure of RPM. In addition, frequency overlaps between Wi-Fi and other technologies using ISM 2.4 GHz can cause interference problems, which can result in unacceptable delay and data loss. Moreover security issue should also be considered.

5.4 Summary

Wireless network technologies can be utilized for further improvement of healthcare service. In this chapter, some examples of their applications were discussed. This included examples of applications of wireless sensor networks in data acquisition. Bluetooth, due to its limitations, is unable to support long-term RPM, whereas low-power ZigBee can be used in RPM on general hospital wards. Two alternative approaches to use ZigBee networks were discussed. In addition, Ethernet LAN, particularly wireless Ethernet (Wi-Fi) was considered for supporting RPM on general hospital wards and some related issues were discussed. In the next chapter, a wireless RPM system proposed in this project will be discussed.

CHAPTER SIX

6 Proposed Wireless RPM on General Wards

6.1 Introduction

The design of a RPM system should be based on the specific requirements for patient monitoring. Although many efforts have already been made for the design of wireless RPM, the developed systems are either unsuitable or have many limitations. For instance, some systems like the UbiMon (Lo and Yang 2005) analyze vital signs locally. When patients receive warning signals, they need to inform their healthcare providers asking for assistance. Some systems like MobliHealth (MobliHealth 2008) enable medical personnel remotely access patients' vital signs on-demand. Research taken by Lorincz *et al.* (2004), Lin *et al.* (2004), Yu and Cheng (2005) etc. made some efforts on developing a RPM system for continuous automated monitoring. Their systems may not be suitable for supporting long-term RPM on general wards due to high-power-consumption WPAN used. Furthermore, these systems can only monitor individual or several patients, which may restrict their benefit for improving holistic care.

A wireless RPM system is proposed for general hospital wards in this project. Such a system can significantly improve patient monitoring and holistic care on general hospital wards. It can gather vital signs from each patient automatically and send them to a central control room for real-time monitoring. Benefit from the centralized and automated monitoring, all the patients on general wards can be

monitored; nurses can have the holistic view of patients' condition and work more efficiently. In addition, the use of wireless technologies provides more flexibility and mobility to patients during hospitalization. In this chapter the proposed RPM system is discussed.

6.2 Main Components of the Proposed RPM

The proposed system consists of three main components: Data Acquisition System (DAS), data transmission system and central control unit. Figure 6.1 shows the framework of the proposed system.

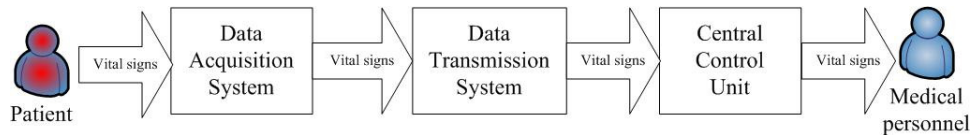


Figure 6.1 - Framework of the proposed RPM system

6.2.1 Data Acquisition System

The function of the DAS is to obtain vital signs from patients. Wireless sensors provide more comfort and mobility to patient. Each patient is allocated with five sensors which are capable of measuring vital signs (including heart rate, oxygen saturation, blood pressure, respiration rate and temperature). The sensors with wireless capability are networked ZigBee-based wireless network technology.

A master node is used per patient. The master node can be located on the bedside of a patient. The master node which is integrated with five sensors forms a WPAN. The master node controls the communication of the sensors within the WPAN. In

this thesis the WPAN which consists of a master node and five sensor nodes are referred to as a DAS. Figure 6.2 illustrates the architecture of a DAS.

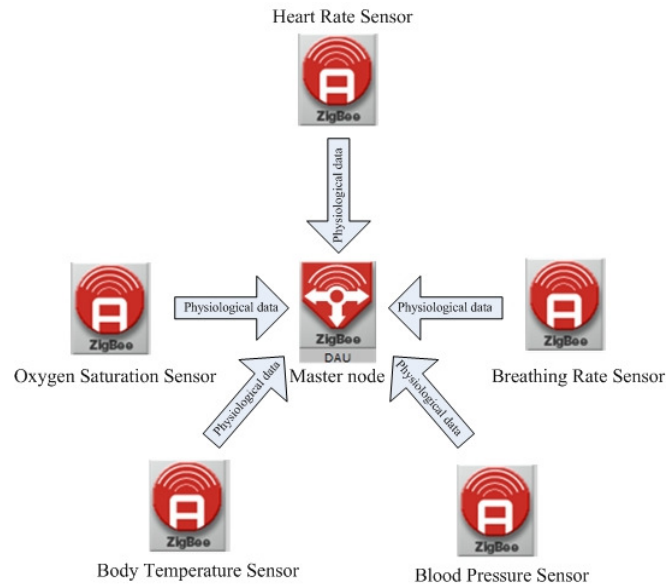


Figure 6.2 - Architecture of a DAS

It was discussed in Chapter 5 that ZigBee technology, due to its low-power consumption feature, is suitable for long-term RPM on general wards. Therefore the proposed DAS is based on a ZigBee WPAN.

Although there is an alternative approach of using single master node to receive data from all the sensors attached to all the patients on a general ward (please refer to Chapter 5 section 5.2.2). To overcome the limitations of the signal master node approach, multiple-WPAN approach is decided in this thesis. In such a case the sensors in a ZigBee WPAN will be within a short proximity of the master node communicating data with good signal strength, reducing the possibility of errors

and data loss. Moreover there will be a limited number of active sensors for generating vital signs for transmission in a ZigBee WPAN. Hence it can avoid transmission collision caused by a considerable amount of transmission using the limited bandwidth.

It is worth mentioning that the master node in the proposed DAS has more functionalities than a normal master node defined by the ZigBee standard (please refer to Chapter 4). The master node in the proposed DAS will be capable of collating and sending the received vital signs to a central control unit through a data transmission system. The design of the prototype DAS will be discussed in Chapter 7.

6.2.2 Data Transmission System

The data transmission system is used to transfer vital signs from all DASs to a control unit through a local area network for monitoring. In the proposed RPM, an Ethernet-based Local Area Network (LAN) will be utilized. Figure 6.3 illustrates an overview of the data transmission system. The arrows represent the direction of vital signs transmissions.

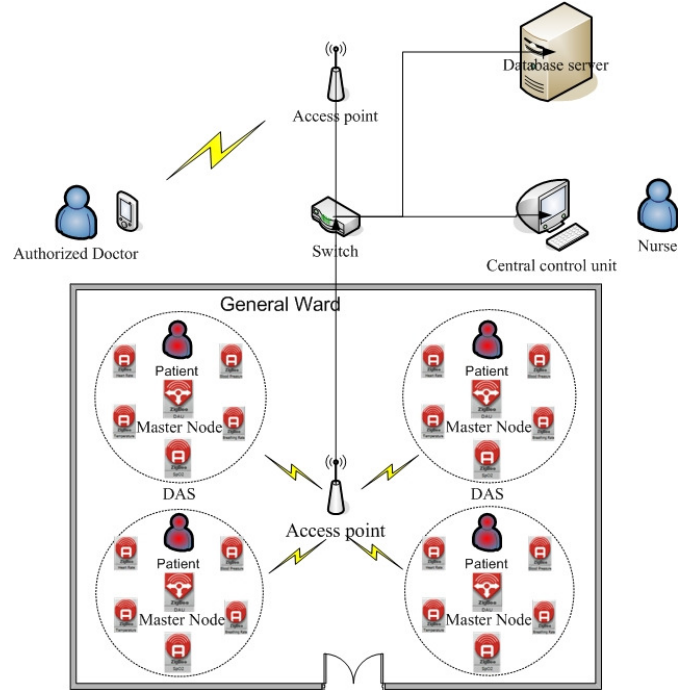


Figure 6.3 - An overview of the LAN-based data transmission system

A nurse in the central control unit can monitor patients' conditions in real-time. An authorized doctor can also access this information through a wireless LAN system.

However, the reliability of data transmission in the Ethernet LAN may be an issue requiring careful consideration. Ethernet LANs are non-deterministic and their performance can be affected by the number of active communicating devices as well as the volume of data communicated. The performance of wireless LAN in RPM will be studied in a simulation environment in Chapter 8.

6.2.3 Central Control Unit

A central control unit is proposed for the RPM on general hospital wards. This is the centre for processing of vital sign, analysis, display and storage. Figure 6.4 shows the architecture for this unit. Patients' vital signs received from the DASs are displayed graphically on-line in real-time. The data is analysed for a pattern of change to identify abnormalities. This can aid to prevent further deterioration of a patient's condition. An alarm may be raised when an abnormality is identified. A major benefit of this unit would be the ability to monitor patients' conditions continuously, especially at night, without disturbing their sleep. Doctors will also be able to access this information remotely through the LAN or World-Wide Web (WWW), especially if they are away from general wards. A database can be developed using the illustration shown in Figure 6.5

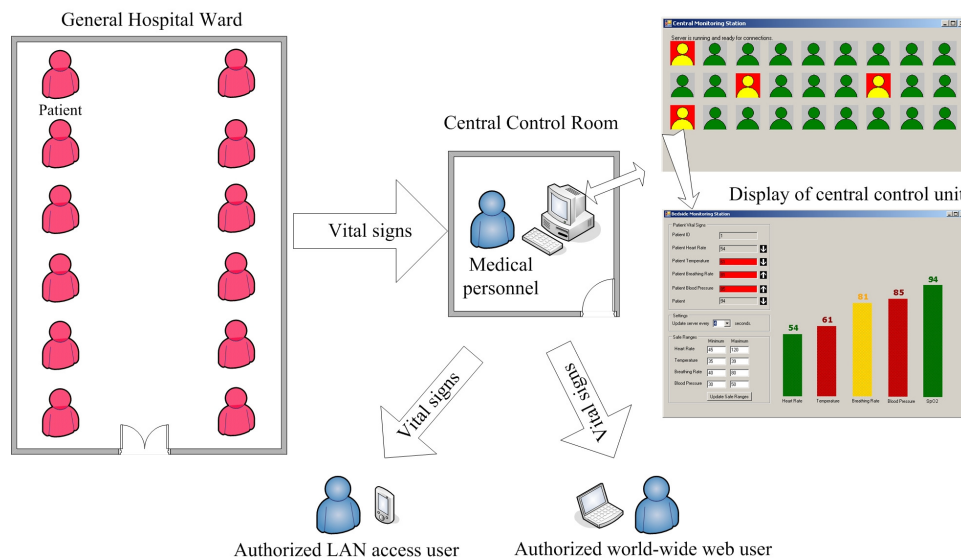


Figure 6.4 - The architecture for central control unit in the RPM system

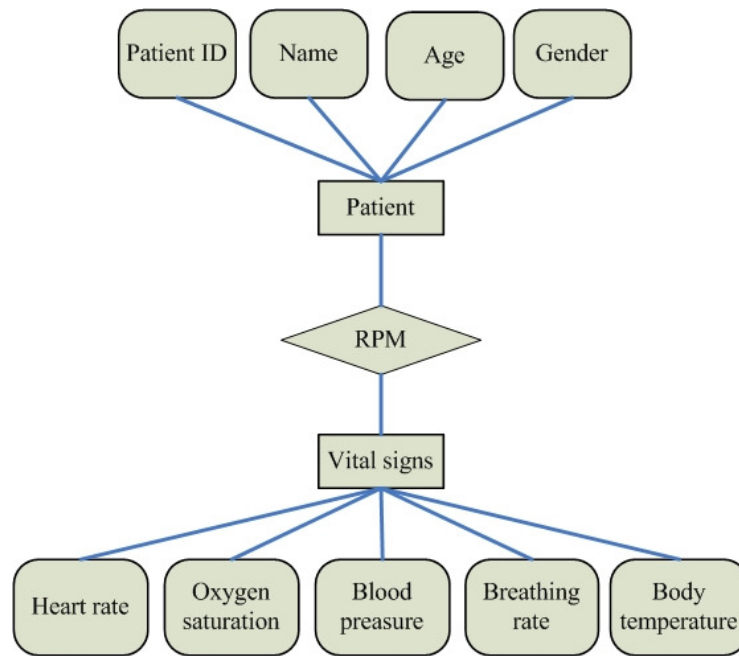


Figure 6.5 – A designed database for the control unit

To assist medical personnel to easily identify the patients who require attention, a three-colour-state mechanism is introduced to indicate patients' conditions. The use of three colours (green, amber and red) is to represent different state of patients' conditions in order to cause different level of attention of nurses (Sahandi *et al.* 2010). Figure 6.4 shows the architecture of the control unit. In the figure, the colour of the icon representing each patient indicates the condition of the patient. It should be noted that the three-colour-state which is proposed to facilitate the identification of patients' condition in RPM, may need further validation.

Furthermore, abnormality and rapid changes to vital signs can be indications of physiological deterioration. This may be detected by using predefined safe-range of vital signs which determines the upper and lower thresholds of a type of vital sign (e.g. heart rate). If the measurement of vital signs is out of the safe-range, the measurement may be treated as abnormality. In the proposed RPM system, the safe-ranges chosen are based on the consultation with hospital staff. However, due to the large variety of patients on general wards, further investigations are necessary to develop an algorithm for detecting abnormalities in vital signs.

State 1 (green): Assuming each patient on a general ward is in a stable condition; their icons will be displayed in green. The monitoring software applies an appropriate algorithm to the patient's vital signs which have arrived at the control unit to detect abnormalities. In a stable condition, the icon representing the patient will be shown in the green colour.

State 2 (amber): As soon as the monitoring software detects an abnormality in a patient's condition, the icon will change colour to amber and start blinking along with a gentle warning sound to raise the attention of staff. At this point, nursing staff are alerted to attend to the patient.

State 3 (red – alert): An abnormality is detected by the monitoring software which is regarded as severe and requires urgent attention. A request is made to alert the medical team.

6.3 Some Relevant Issues

Automatic identification of abnormalities

It may be possible to implement a detection system based on identification of sudden changes to vital signs, which may be used as an initial trigger in an automated RPM system. Several studies have shown that instability in vital signs is evidence of deterioration (Whittington *et al.* 2007). It is worth noting that automatic identification of abnormalities in a RPM system is a challenging task requiring a considerable amount of signal/data processing and medical expertise. This may be in the form of a rule-based system for identifying abnormalities as a large number of factors should be considered.

Vital signs of individual patients can also be stored for future use at the central control unit. Vital signs of a large population of patients stored over a period of time may be used to study patterns of change in vital signs, facilitating the identification of generic health problems of one or more patients.

Transmission interval

It should be noted that due to the nature of general wards, patients may require different levels of medical care and attention. Some patients may require frequent monitoring, whilst others may need less. Consequently, frequent transmission of vital signs of patients, who are in a stable condition, may put unnecessary pressure on the network. However, choosing long intervals for patients who require more attention may make the monitoring process ineffective. A RPM for general wards

should, therefore, have the facility to enable the transmission interval to be adjusted locally at the DAS or remotely from the central control unit. This is necessary as patients' conditions may change, resulting in more intensive monitoring being required.

Security and data integrity

The issue of security and data integrity also require attention due to potential detrimental consequences. Accordingly adoption of wireless technologies for transmitting medical data signifies greater need for security. Data transmitted through wireless networks should be encrypted to increase security. In addition, vital signs should be accompanied by Patient's Identification (ID) avoiding misrepresentation. For example, a ZigBee WPAN can use a unique Patient ID (PID) as WPAN Identification (WPANID) to distinguish data from other WPANs. The PID can also be used to check for data integrity. PIDs would accompany vital signs transmitted from each WPAN to the control unit. Details of this process are discussed in Chapter 7.

To increase security of data transmitted from a WPAN to the control unit, the data may also be encrypted. Encrypted vital signs and patient's IDs can then be communicated between WPANs and the control room.

Operational overview of the proposed RPM

At the initial point where patients are admitted to a general ward, wireless sensors are attached to them. A DAS is allocated to each patient on a general ward

forming a single ZigBee sensor network (WPAN). The DAS is then configured using the patient ID, allocated centrally, at which point an appropriate transmission time interval is also set, depending on the severity of the patient's condition. The patient ID is used during communication between the sensors and the master node to ensure data integrity. The patient's vital signs, gathered by the sensors, are accompanied by patient ID and are transmitted in an encrypted form to the master node within the WPAN. The master node subsequently transmits the encrypted data to the control unit through a local area network. Since the patient ID is allocated centrally, it will be recognized by the RPM system protecting data integrity. The vital signs of patients are recorded at the central control unit electronically for future use. In the control room each patients is represented using an icon on a display unit (please refer to Figure 6.4). Each icon will act as an entry point into the patient's live and recorded data, as well as medical history. In addition, as it was discussed in section 6.2.3, the icons can be colour coded to reflect patients' conditions. Figure 6.6 illustrates the operation overview of the proposed RPM system.

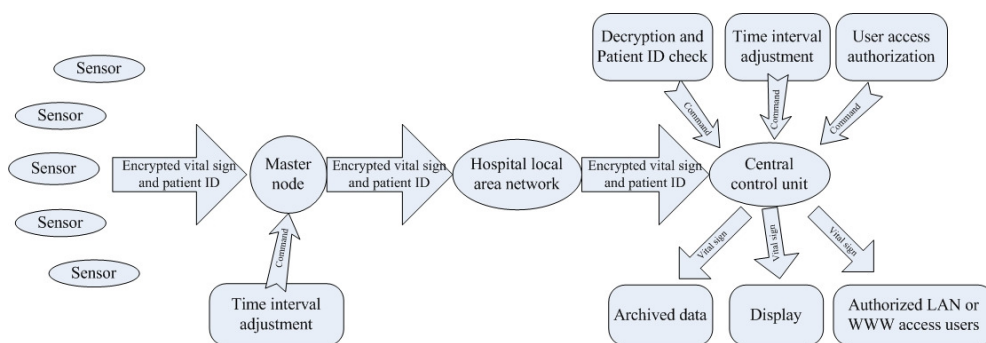


Figure 6.6 - An operational overview of the proposed RPM

6.4 Summary

The proposed wireless RPM system was discussed. This system utilizes a low-power ZigBee-based sensor network (WPAN) for each patient for data acquisition. A local area network is used for transmission of vital signs from patients to a central control unit. The control room is used to display, analyze and store the data. Vital signs are accompanied by patient ID to facilitate data integrity. They are also encrypted to provide security. The proposed system has the capability of monitoring a large number of patients and provides further improvement to holistic care of patients on general wards. Some relevant issues as well as an operational overview of the proposed RPM system were also discussed. A prototype system will be discussed in the next chapter.

CHAPTER SEVEN

7 The Prototype RPM

7.1 Introduction

A prototype system is designed to demonstrate the functionality of the proposed RPM system (illustrated in Figure 7.1). It consists of three main components: Data Acquisition System (DAS), data transmission system (based on a Local Area Network) and central control unit. The implementation of a ZigBee-based DAS is the majority part of the discussion in this Chapter. It includes the design of a ZigBee-based sensor network (WPAN) and the experiments based on the prototype. In addition, a prototype central control unit was designed for graphical and real-time display of vital signs.

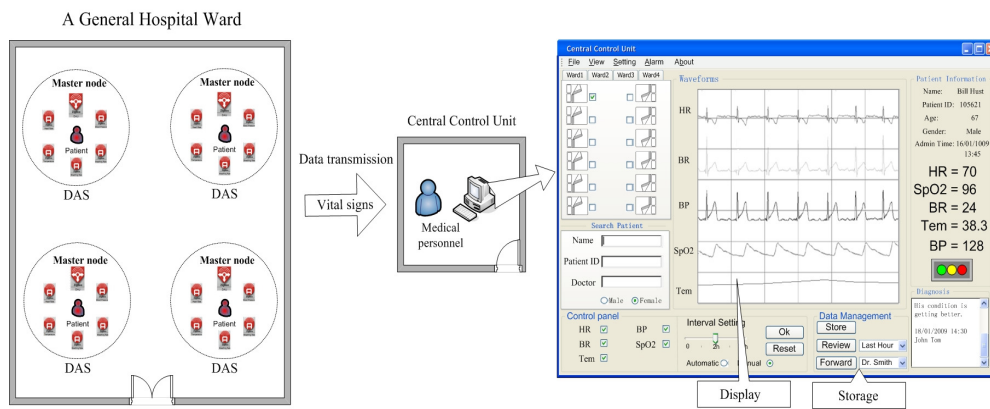


Figure 7.1 - A prototype of the proposed RPM

7.2 The Prototype Data Acquisition System

The DAS in the proposed RPM system is based on the star-topology using ZigBee-based sensors. It consists of a network of five ZigBee-based biomedical sensors. The sensors are responsible for obtaining vital signs, such as heart rate, respiration rate and so on and sending them to a master node in the DAS.

Currently ZigBee-based biomedical sensors are still under development. They are not readily available in the market. In this project, a device was designed to be used in the prototype RPM. This device will be referred to as ‘ZB’ in the rest of this thesis. Section 7.2.1 provides detailed information on ZB.

7.2.1 Design of a Simulated Wireless Biomedical Sensor (ZB)

Design of ZB is based on the architecture of a generic wireless sensor node which comprise of four basic blocks: power supply, communication block, data processing block and sensing block. The power supply block consists of a battery and a dc-to-dc converter to power ZB. The communication block consists of a ZigBee communication module. It is an XBee series2 sensor which can be configured as a ZigBee end device (ZigBee device can be of two main types, end device or a master node). The processing block consists of an Analog-to-Digital Converter, a microcontroller and memory. This block is used to receive signals from the sensing block and then process them using designated software stored in the memory. The functions of the sensing block depend on its application. In this project, it is simulating a biomedical sensor for measuring vital signs. The ZB also

has three additional blocks for local state indicator, local display and transmission interval adjustment. These blocks and their functions will be discussed in subsection 7.2.1.5 Additional blocks. Figure 7.2 shows the architecture of a ZB.

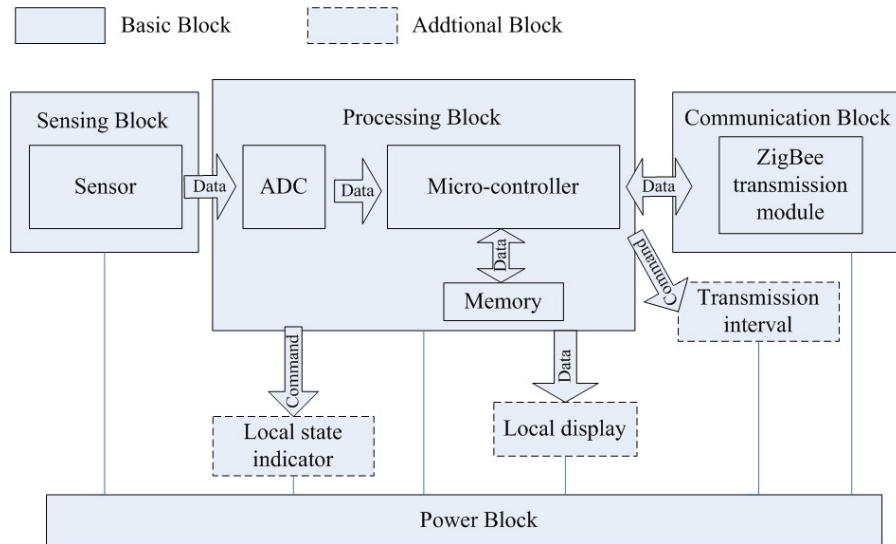


Figure 7.2 - System architecture of ZB

7.2.1.1 Power Block

The power block is responsible for supplying power to a ZB. Table 7.1 lists the main components and its function in circuit. Figure 7.3 is the schematic diagram of the power block.

Table 7.1 - Main components of designed power unit

	Component	Function
U4	Triple-pin regulator LM7805	Convert dc input to +5V output voltage
D1	Diode 1N4007	Reverse polarity protection
D2	Emitting LED	Show working status of the power block

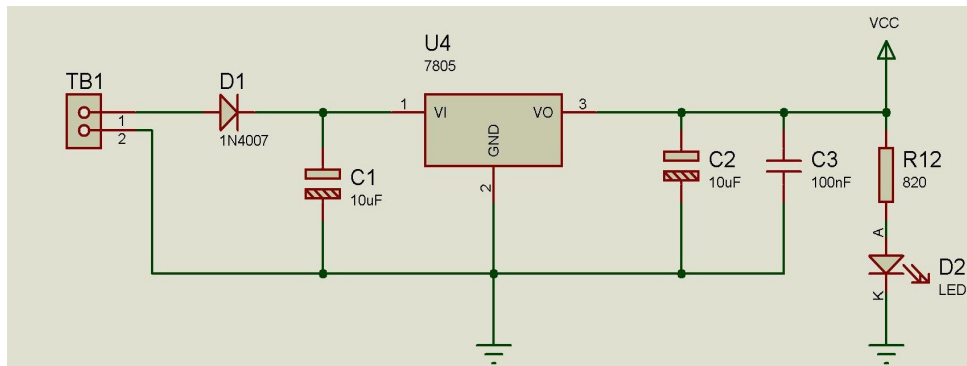


Figure 7.3 - Schematic diagram of the power unit

7.2.1.2 Simulated Sensing Block

This is referred to as simulated sensing block as it is not a practical biomedical sensor which can measure vital signs. Instead a potentiometer is used acting as a simulated sensor in this project. Its resistance can be adjusted to control the output voltage to the microcontroller (through the pin AD0 of PIC16F887), which is used to simulate reading/value for vital signs such as temperature. Figure 7.4 shows the schematic diagram of the simulated sensing block. Since the focuses of this thesis is not to develop wireless biomedical sensors for measuring vital signs, this simulated sensing block is utilized. This can simplify the design of ZB, because it can avoid complexity of building interfaces between biomedical sensors and ZigBee-based communication block.

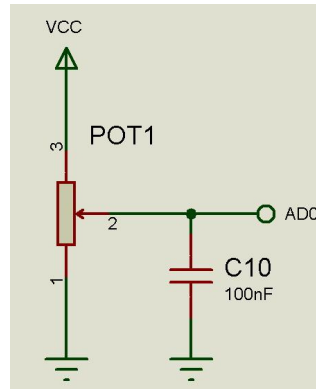


Figure 7.4 - Simulated sensing block (potentiometer)

A practical wireless biomedical sensor can be built together with ZB by replacing the potentiometer with a biomedical sensor. However, it should be noted that the range of measurement, resolution, the number of parallel output wiring may vary for sensors depending upon the vital sign that they measure. Also manufacturers support their own interfaces for their sensors. Therefore, standard interfaces for biomedical sensors are required for implementation in wireless biomedical sensors to be used for RPM.

7.2.1.3 The Processing Block

A processing block determines to a large degree both the energy consumption and the computational capabilities of a sensor node. It consists of a small size microcontroller with embedded programs. PIC16F887 microcontroller, due to its low power consumption and industry popularity, is utilized in the design of ZB. Table 7.2 lists its key specifications. Detailed specifications from can be found in Appendix 2.

Table 7.2 - Key specifications of PIC16F887

Memory Type	Flash
Program Memory	8K byte
Data Memory	368 byte
EEP Rom	256 byte
Number of I/O pins	40
Max CPU Speed	20MHz
ADC	14 channels, 10 bits
Request Power Range	DC 2~5V

The microcontroller (PIC16F887) has to be initialized before its utilization. The initialization is implemented using MPLAB IDE v8.46, which is C language-based software for programming embedded systems for microcontrollers. After being programmed, the microcontroller can perform multiple tasks. The main task is to simulate measurement of vital signs. As it was mentioned in subsection 7.2.1.2, an adjustable voltage controlled by the potentiometer (simulated sensing block) is the input to the microcontroller (PIC16F887). This signal is digitalized by an ADC. The sampling rate used by the ADC is 10 Hz ($1 \div (100\text{ms})$). The digitalized signal varies from 0 (0V) to 1023 (5V), which can be expressed by equation 7.1. This signal is then output to the communication block through a Universal Asynchronous Receiver Transmitter (UART) interface.

$$\text{Digitalized signal} = \frac{\text{Current input voltage}}{\text{Max input voltage}} \times (2^{10} - 1) \quad (7.1)$$

where current input voltage is from 0 to 5 volts; Max input voltage is 5 volts.

Figure 7.5 presents the pins description of PIC16F887 (U1) used in the design of ZB. The C code for the initialization of the microcontroller and the programmed system can be found in Appendix 3. The flow chart for this process can be found in Appendix 4.

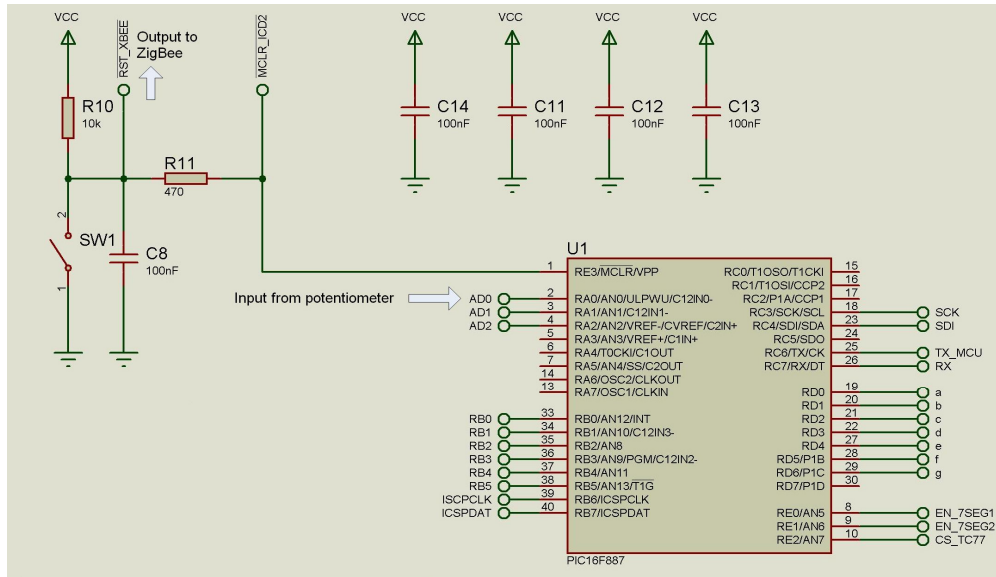


Figure 7.5 - Processing block of ZB

7.2.1.4 Communication Block

To send data in a wireless environment, a ZigBee transmission module is integrated with ZB. A ZigBee module (shown in right side of Figure 7.6) is an essential component for the communication block. Digi XBee series 2 module is utilized to support the communication function of ZB. This module has been extensively used in current application of ZigBee technology. Table 7.3 shows its

specifications. The manufacture datasheet of this module can be found in Appendix 5.

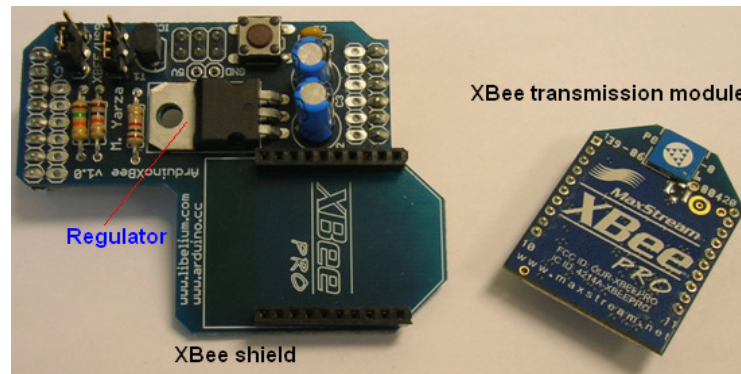


Figure 7.6 - ZigBee-based transmission module

Table 7.3 - Specifications of XBee series 2 ZigBee module

Frequency band	2.4 GHz
RF data rate	250 Kbit/sec
Indoor transmission rang	<40m
Transmit power	1.25 mW(+1dBm)
Receiver sensitivity (1% PER)	-95 dBm
Data integrity	PAN ID, 64-bit IEEE MAC
Encryption	128-bit AES
Support channel	16
Reliable packet delivery	Retransmission/Acknowledgement

It is worth mentioning that Digi XBee series 2 modules are updated from Digi XBee series 1 module. Digi XBee series 1 module can only support the features defined by IEEE 802.15.4 standard. It only allowed point-to-point communication

between two modules. Also the configuration of it is more complex than Digi XBee series 2. For instance automated channel scan and channel allocation are not permitted by Digi XBee series 1. A user has to manually choose a channel and allocate it to both transmitter and receiver in order to establish communication. However, the manually selected channel could be interfered with other devices using ISM 2.4GHz.

An XBee shield (shown on the left side of Figure 7.6) is used on ZB. It supports UART communication between the ZigBee module and the processing block. Figure 7.7 shows the schematic diagram of the communication unit.

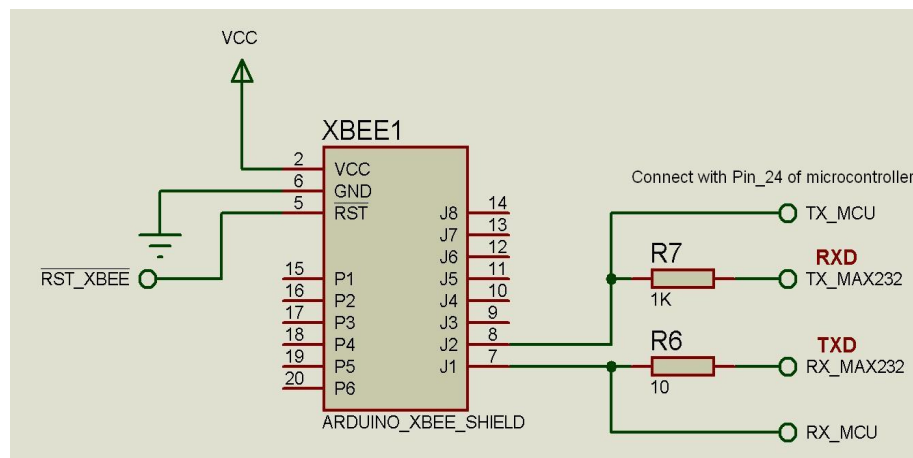


Figure 7.7 - Schematic diagram of the communication unit

It is worth mentioning that the maximum output range from the microcontroller is 5V. ZigBee module works at 3.3V. Therefore a regulator was used to convert voltage. However a module needs to be integrated to convert XBee output voltage to 5V, otherwise the microcontroller would not be able to process input signal from

the communication block. The circuit to implement the voltage conversion is shown in Figure 7.8.

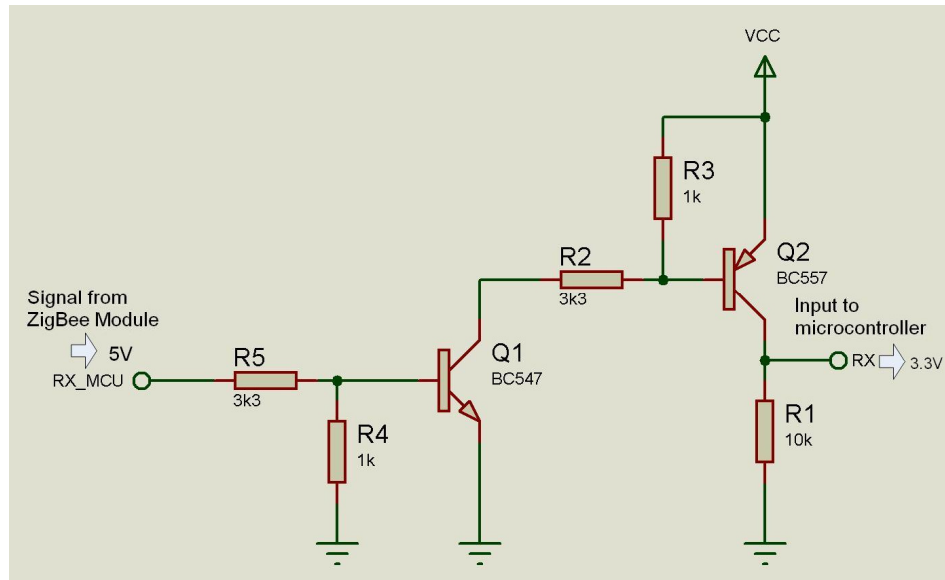


Figure 7.8 - Voltage conversion between the communication and the processing blocks on ZB

A ZigBee module needs to be configured before using it in a network. The configuration involves classification of the node (master or slave), network ID, destination address, the security option and so on. In the case of using XBee series 1 module, the channel used for transmission also needs to be set manually.

Manufacturers usually provide their own software for configuration. X-CTU (version 5.1.4.1) provided by Digi is used in this project for configuring the XBee series modules. Figure 7.9 shows the interfaces of X-CTU used for configuration (A table listing all the configurable parameters is included in Appendix 6). The

details of the configuration process are provided in section 7.2.2 Data Acquisition System.

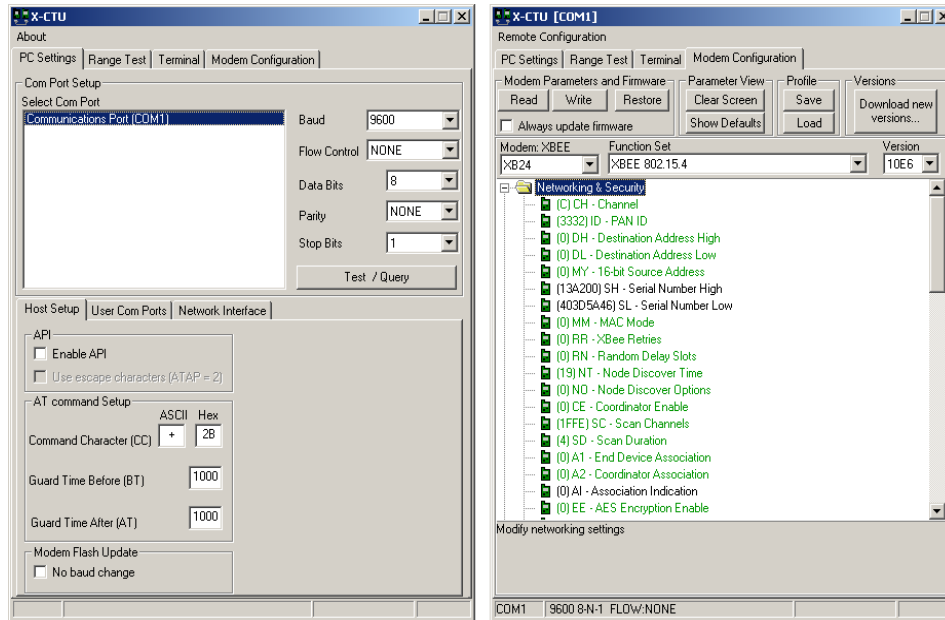


Figure 7.9 - Interfaces of X-CTU for configuration

7.2.1.5 Additional Blocks

In addition to generating and sending data, ZB has three additional blocks working together with the processing block performing the following functions:

Local display of current reading

ZB includes two seven-segment-LEDs to display local reading of data. Two seven-segment-LEDs are used to display current readings in decimal number.

Figure 7.10 shows schematic diagram of local display.

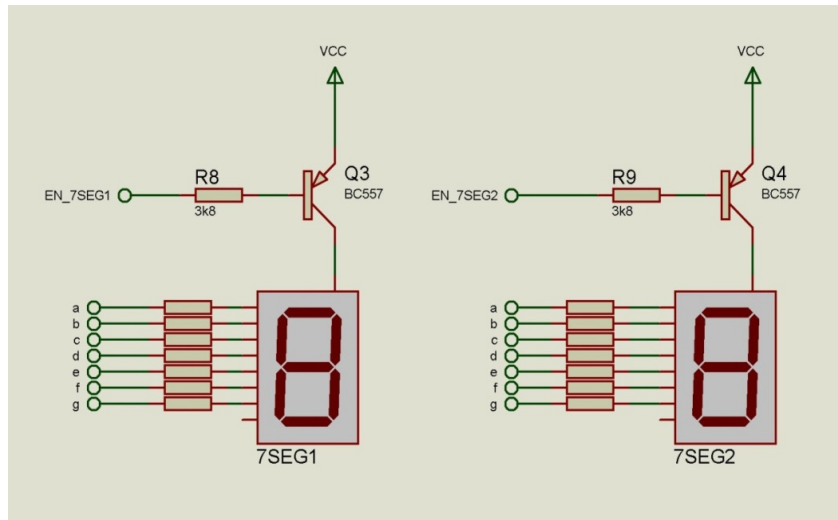


Figure 7.10 - Schematic diagram of local display

The microcontroller processes the input and converts it into a corresponding value for display. This value is used to represent simulated vital signs. This method for conversion and calibration is based on the equation:

$$\text{Vital sign}_{\text{current reading}} = \left(\frac{\text{Max input} - \text{Min input}}{\text{Max vital sign} - \text{Min vital sign}} \right) \times \text{Current input}$$

The range of voltage used for calculation is from 0 to 5V. The maximum and minimum values for vital signs are shown in the Table 7.4. The values correspond to the range of measurement are introduced for experiment. Further study should be carried out to develop a RPM system against the practice.

Table 7.4 - The range of vital signs used for display

Vital signs	Heart rate	BR	BP	SpO2	Temp
Min-Max	0-220	0-60	0-180	0-100%	0-42

Local States Indicator

ZB also has three light emitting diodes to illustrate local warning. The emitting diodes are in three colours: red, amber and green. The colours are used to indicate three different levels. Red means a patient' condition is critical; Amber means the patient require some attention; Green means the condition is normal. These functions are controlled by the microcontroller, which compares the value of input with a pre-set states ranges to determine the condition. Figure 7.11 shows the algorithm used for implementing the local states indicator. Table 7.5 lists the pre-set for the three states. It should be mentioned that the pre-set state ranges are not practical for clinical usages; they are just used for the purpose of experiments.

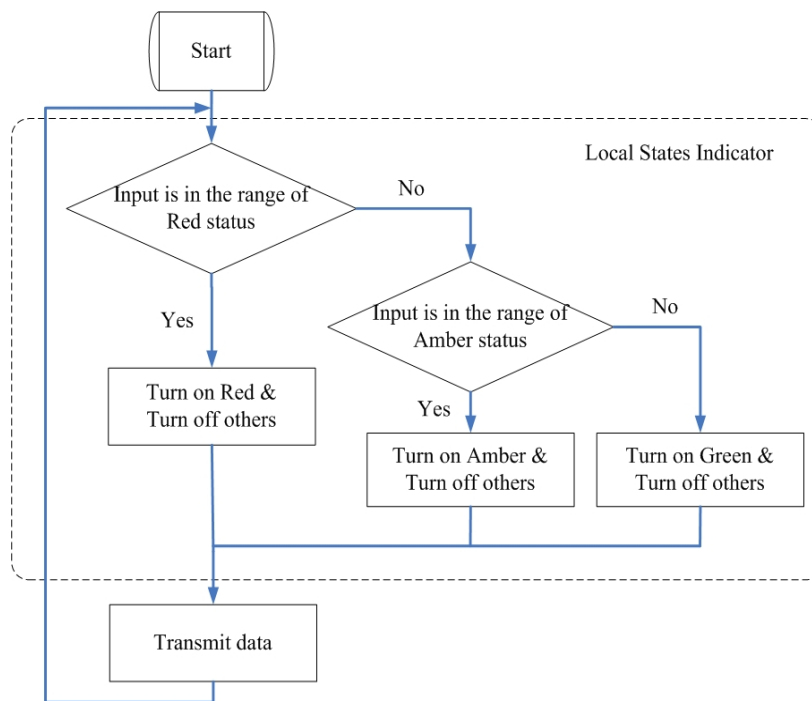


Figure 7.11 - The algorithm used for implementing local states indicator

Table 7.5 - Preset range used for local states indicator

Vital signs	Red states	Amber states	Green states
Heart rate (beat/s)	$[0, 60) \cup (160, 220]$	$[60, 65) \cup (120, 160]$	$[65, 120]$
Respiration rate(times/s)	$[0, 10) \cup (35, 60]$	$[10, 15) \cup (25, 35]$	$[15, 25]$
Blood pressure (pa)	$[0, 85) \cup (150, 180]$	$[85, 90) \cup (130-150]$	$[90, 130]$
Oxygen saturation (%)	$[0, 90)$	$[90, 95)$	$[95, 100]$
Temperature (°C)	$[0, 35) \cup (40, 42]$	$[35, 37) \cup (38-40]$	$[37, 38]$

Adjustable transmission intervals

ZB provides flexibility for adjusting transmission intervals for sending data from each master node to the control unit. This is necessary due to approach the nature of general hospital wards, where some patients need more care and attentions whilst others way needs less.

This function is implemented by changing the frequency of polling data. Transmission interval can be set in ZB from 1 second to 9 second. The default setting of transmission interval is 3 seconds. This can be changed by using two switches on ZB. One is for increasing the interval another is for decreasing. Every time the switch is pressed, the transmission interval changes by 0.1 second.

Figure 7.12 shows a ZB acting as a heart rate sensor in operation. Two seven-segment-LED shows the current reading is 60. This patient is presumed to be in a normal condition, therefore green light is emitting. It can be observed from Figure 7.12 that there are another two green light emitting diodes. These two diodes were

used to indicate the operation state of ZB. Once the ZB being powered, they will switch on.

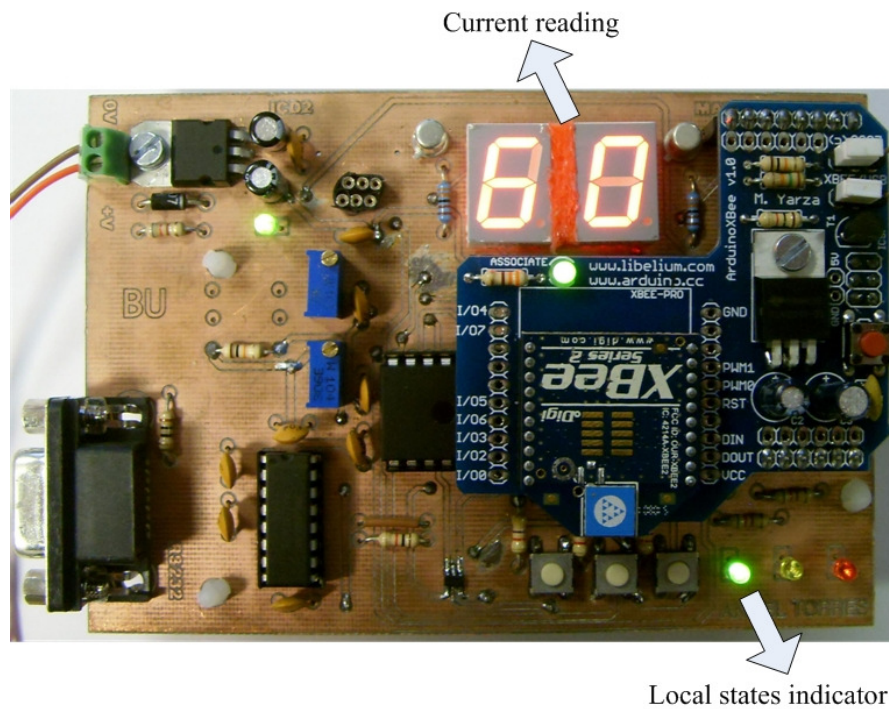


Figure 7.12 - A ZB in operation

More information of the design of ZB can be found in Appendix 7, which includes the completed diagram of the design.

7.2.2 Data Acquisition System (DAS)

The main functions of the DAS can be divided into two parts:

- To gather data (vital signs) from ZBs
- To send the data to the control unit

A prototype DAS is built based on two main parts:

- A ZigBee module (which has been configured to a ZigBee coordinator)
- A PC with both Ethernet network card and IEEE 802.11g wireless card. The PC is used for transmitting the data obtained from the ZigBee coordinator to the control room. This is required since the ZigBee coordinator cannot be directly connected to an Ethernet network.

The ZigBee coordinator is referred to as master node (please refer to Chapter 4) in the designed prototype. It initiates and controls the communication between the ZigBee-based sensors and itself. The PC is connected to the master node through a RS232 cable and receives data from the master node through this serial port. Table 7.6 indicates the parameters which were set for communication through this serial port.

Table 7.6 - Setting of serial port communication

Baud rate	9600
Flow control	None
Data Bits	8
Parity	None
Stop Bits	1

The PC can send the data received from the serial port to the control unit via either the wired or wireless Ethernet network.

Configurations of ZigBee Modules for Communication

Configuration is very important in application of ZigBee sensor networks. It involves many aspects such as selecting the node type, network address and so on. The X-CPU software was used to configure the ZigBee modules. This software contains many versions of firmware, which can be selected and written into a ZigBee module through RS232 or USB port. The configuration progress included two parts: configuration of a master node and configuration of the end devices.

Configuration of a master node

ZNET 2.5 coordinator firmware version 1047 was selected for configuring the master node. It is the latest coordinator version for configuring a Digi XBee series 2 modules. The parameters that have been configured are listed in Table 7.7. Figure 7.13 shows the menu used to configure the master node.

Table 7.7 - Configured parameters of master node

Configured Parameters	Settings
WPAN ID	234
Node Join Time	FF
Destination High and Low	0
Device Type Identifier	0
Power Level	4 (Highest) +3dBm
Power Mode	1(Improved Sensitivity)
Encryption Enabled	0 (Enabled)
AES Encryption Key	0123
All the Other Parameters	Default

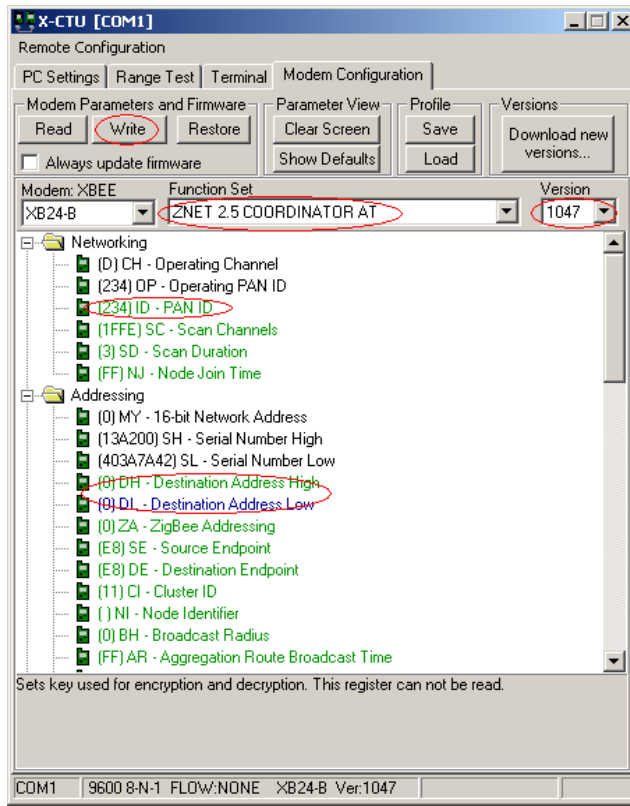


Figure 7.13 - Configuration of master node

Once being configured, the master node can automatically scans the air to select a communication channel using the mechanism introduced in Chapter 4. This channel cannot be changed during data transmission. The master node subsequently broadcast its address including a WPAN ID using this channel. Clients can then join this WPAN by sending their request to the master node through this channel. The WPAN ID can be changed to a number between 0 and 16383. It is used by the WPAN to distinguish the data transmitted by other WPANs. Each ZigBee module has a unique address allocated by its manufacture. This address contains two parts: serial high and low addresses (see Figure 7.13)

Node Join time (NJ) also needs to be set. An infinite join period is used, so that ZBs can join the master node at any time. In some cases, the master node can be configured to have a time-period during which nodes' joins are allowed. The infinite join provides more flexibility, as there is no time restriction for ZBs to send request for join a WPAN.

Configuration of ZigBee module for ZB

ZNET 2.5 end-device firmware (version 1247) was used for configuring ZigBee module on ZBs. Several features needed configuration to include channel verification, WPAN ID, destination address, node identifier and encryption key (see Figure 7.14). The features are discussed in detail in the following. All the other configurable features that use default settings are listed in Appendix 6 with brief introduction.

(1) Channel verification

This setting is only used by ZigBee end-devices. If it is enabled, an end-device (ZB) can verify whether a coordinator exists on the same channel to ensure its operation on a valid channel; it will leave, if a coordinator cannot be found (if NJ=0xFF). If channel verification is set disabled, the end-device (ZB) will remain on the same channel all the time. In this prototype, channel verification was enabled to ensure ZBs operate on a valid channel in the experiments.

(2) WPAN ID

The WPAN ID of a ZigBee module need to be as same as the one used by its master node, otherwise communication between the ZBs and their master node cannot be established. In this thesis, a unique Patient ID (PID) is used as WPAN ID, which has been discussed in Chapter 6.

(3) Destination address

ZigBee supports 64 bit destination address, which is divided into two parts. Upper 32 bits destination address and lower destination address. 0x000000000000FFFF is the broadcast address for the PAN. 0x0000000000000000 can be used to address the master node. In this prototype, both upper and lower destination addresses were set to 0, so that all the five ZBs recognize the master node as their default destination for transmission.

(4) Node Identifier

Node Identifier (ID) can be a series of numbers, words or a combination of numbers and characters. It can be used in a WPAN to distinguish data from different transmission modules. For instance, “Heart Rate” can be given as an ID to the ZB behaving as the heart rate sensor. In addition, an extended Node ID can be used as patients’ ID in RPM to improve data integrity in RPM.

(5) Encryption key

The encryption key can be used to provide security and privacy in the application of ZigBee WPAN in RPM. The key is a hexadecimal string set by the user. It should be used for both ZBs and the master node. The length of the key needs careful consideration since it will put extra load on the ZigBee network.

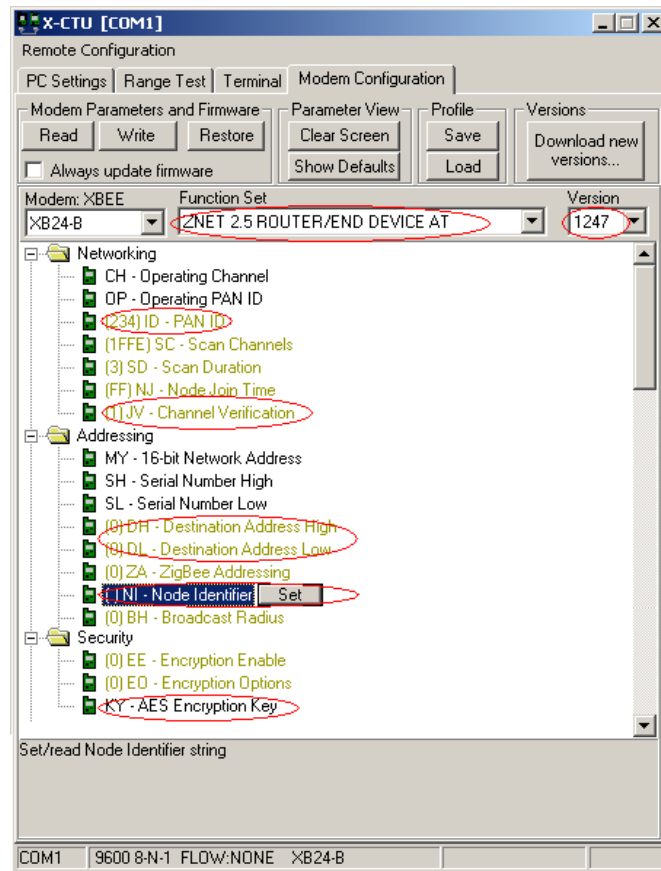


Figure 7.14 - Configuration of ZigBee module of ZB

7.2.3 Data Transmission in ZigBee-based Networks

A range of experiments were carried out in this project to investigate the feasibilities of using ZigBee sensor networks in RPM. The main purpose was to

validate transmission reliability. Several aspects were studied. They included channel verification, reliable transmission range and the impact of interference.

Two PC were used. One connected to a ZigBee master node; the other linked to a ZigBee module that was configured to an end-device (ZB). In that case, a simple ZigBee sensor network was formed. Data transmission between them was based on master-to-slave mode, which has been discussed in chapter 4. Connections between each PC and ZB were through RS232 cable. The PC connected to the ZB was set up to simulate a biomedical sensor. It generated data (vital signs) and sent them to the master node via ZB. The PC connected to the master node displayed the received data. Figure 7.15 illustrates the layout of the experiments.

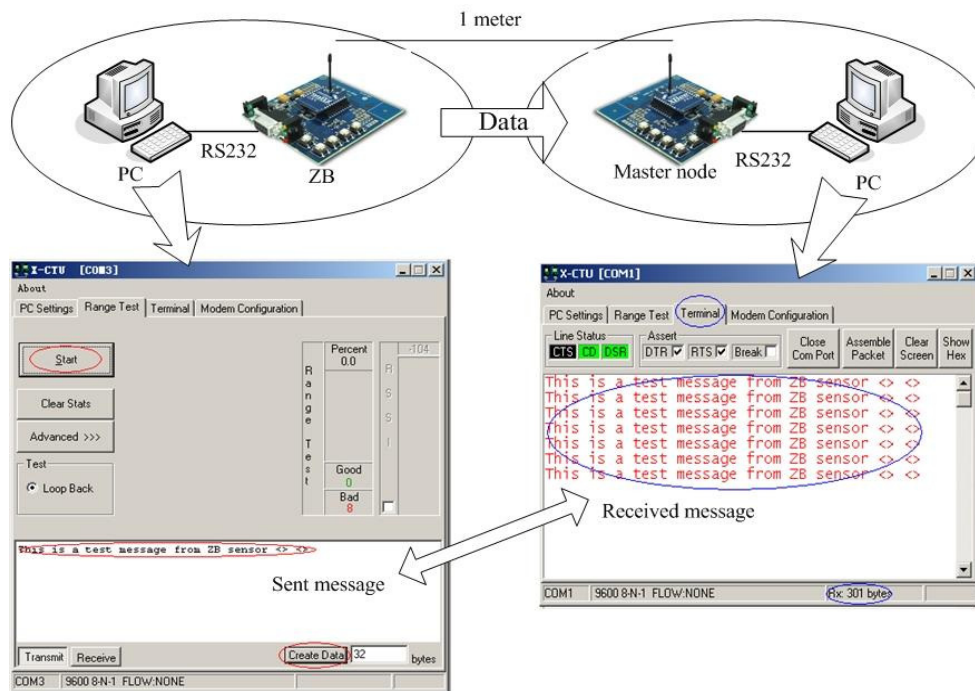


Figure 7.15 - Layout of the experiments

Channel Verification

Channel verification is important as it is the key to ensure a ZB works on a validate channel. Otherwise data transmission from ZB to the master node can not be implemented. It can cause data loss, which is not acceptable in RPM.

In the experiments, it was found that a ZB with channel verification enabled, still can communicate with its master node on the same channel every time when the master node or itself is restarted. However a ZB with channel verification disabled can lose connection with its master node due to the change of channels by its master node.

Transmission Range

Awareness of validated transmission range is crucial in using wireless technology for data transmission. It may have impact on transmission reliability. For example, two nodes may not be able to receive the entire information from each other, if they are out of the validated transmission range. Therefore, careful consideration should be taken in design of a wireless RPM.

Khan *et al.* (2008) claimed that a single master node could support RPM on a general hospital ward with the size of $10 \times 10 \text{ m}^2$, because ZigBee supports 10-100 metres typical transmission range. However, its data transmission can be affected by many factors such as transmission power, receiver's sensitivity, etc. Therefore, further study is needed to validate the reliable transmission range of ZigBee.

X-CTU provides the facility for testing ZigBee transmission range. It was applied in this experiment. XBee series 1 module was used since it supports manual selection of transmission channels.

The experiment was conducted in an office inside the university building. Two ZigBee transmission modules were put statically approximately 10 metres apart in order to validate the reliability of single-master-approach. The two transmission modules were configured using the following settings:

- Channel 26 was used to avoid possible interference with WLAN (Wi-Fi)
- Non-Beacon mode
- Transmit power is set to 0 dBm
- 200 package were sent from ZB sensor to the master node
- Each package was 12 bytes (the size of vital signs package)

Figure 7.16(a) illustrates the result of the experiment. It can be seen that the received signal strength indicator (RSSI) was -79 dBm. There were 19 packages lost during transmission; the data transfer rate was 90.5%. The data loss may be caused by many factors, for example the shape of the room, stuff between two transmission modules and so on.

Two ZigBee modules were then brought closer to a distance of approximate 2 metres. Figure 7.16(b) shows that the received signal strength indicator (RSSI) changed to -59 dBm. Data transfer rate increased to 100%.

It can be argued that the single-master-node approach may need further improvement and validation, since its reliability can be affected by the shape of the room, obstacles between two transmission modules and so on.

However, the experiments validated the proposed multiple-WPAN approach, because, in this approach, a master node can be put in a short distance (2 metres) from ZBs. The shape of the ward and some other factors may not impact the transmission. Signal sent from ZB can be received by the master node with enough power, so that it can avoid data loss.

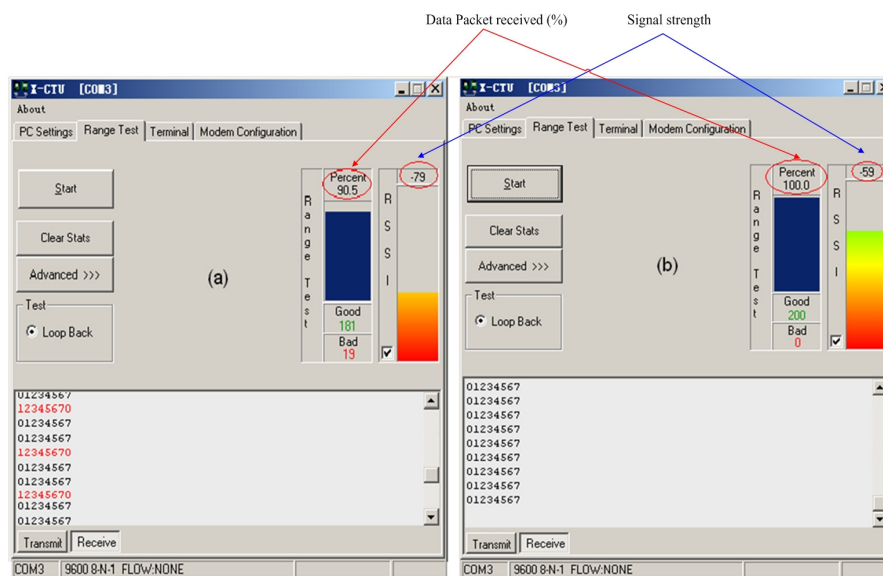


Figure 7.16 - Results of experiment of transmission range test

Interference

This test investigated the potential interference between wireless LAN (Wi-Fi) and ZigBee networks (WPAN) vice versa. Tests conducted were intended to

obtain experimental data transfer rates corresponding to the number of bytes correctly transferred without being affected by interferences between ZigBee and Wi-Fi signals. It is important to realize that a variety of scenarios are probable in realistic usage, each of them has its own characteristic. Therefore, tests should be conducted before the deployment of wireless RPM system on a ward.

In this project, the test was performed in an indoor office environment. A Belkin IEEE 802.11g access point (AP) and a Dell Latitude D600 laptop with an IEEE 802.11g interface card and a PC with a similar wireless card were used to generate data and transmit it through the wireless card. TCP traffic was generated and sent by the laptop to the PC through the AP. The traffic was generated using the “LanTrafficV2” software with packet payload size of 1460 bytes and a fixed inter-packet delay of 1 mini second. In the test, 60,000 Ethernet packets were transferred between the laptop and the PC.

At the same time, two Digi XBee series 1 sensors (a ZB sensor and a master node) linked to two PCs were used in a peer-to-peer communication where a 12-byte data packet (typical size of a vital sign measurement) were sent by ZB to the master node 3200 times with an inter packet delay of 200 mini second. The AP was placed 2cm to the master node which received ZigBee data. Figure 7.17 illustrates the physical layout of this test. Figure 7.18 shows the picture of the equipment in operation. The channels used by ZigBee modules and IEEE 802.11g AP were chosen depending on the test to be run, which will be specified in the following sections.

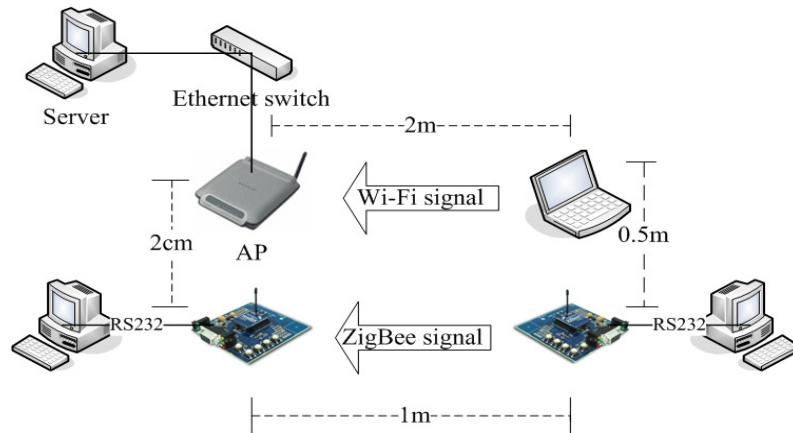


Figure 7.17 - Physical layout of the experiment of interference

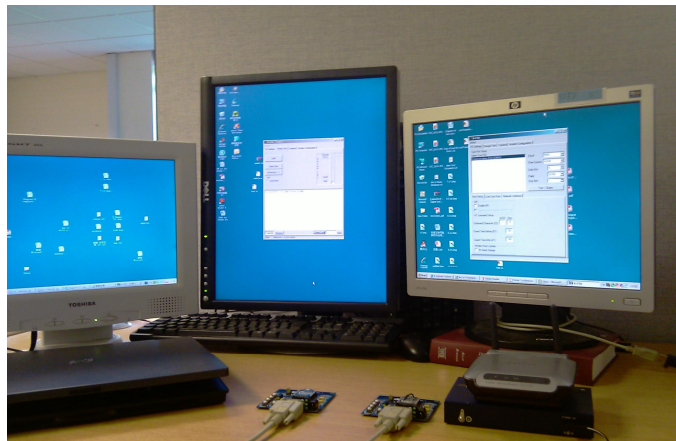


Figure 7.18 - The experiment of interference

The following shows the tests which were carried out:

(a) Using Non-overlapping Channels

In this test, the channel used was set to Wi-Fi channel 11, which has the central carrier frequency at 2462 MHz. The channel used by ZigBee modules was set to be ZigBee channel 11. Its central carrier frequency is also at 2405 MHz. In this

test, no interference effect was observed neither on the performance of the laptop with Wi-Fi card nor on the ZigBee modules. There is no data loss detected for both Wi-Fi and ZigBee transmission.

(b) Using Overlapping Channels

Test 1: In this test, Wi-Fi channel 6 and ZigBee channel 17 were used. These two channels are overlapping. The central carrier frequency of Wi-Fi channel 6 is at a 2437 MHz; the central carrier frequency of ZigBee channel is at 2435 MHz overlapping channels. The test was run ten times. It was found that ZigBee transmission did not generate significant effect on Wi-Fi transmission. However, ZigBee transmission experienced high data loss caused by Wi-Fi interference. Table 7.8 shows data loss rate in the tests.

Table 7.8 - Experiment result: the effect of Wi-Fi on ZigBee.

Sent package	Received package	Data loss rate
3200	2834	11.4%
3200	2881	9.9%
3200	2879	10%
3200	2738	14.4%
3200	2781	13.1%
3200	2790	12.8%
3200	2846	11.1%
3200	2771	13.4%
3200	2719	15%
3200	2828	11.6%
Average data loss		12.27%

From Table 7.8, it can be calculated that the mean received package volume and data loss rate were 2807 and 12.27% respectively.

Test 2: Another test has been conducted by moving the AP away from the ZigBee master node to 0.5 metre. This test was also run ten times. The results show reduction in data loss rate. The mean received package and data loss rate changed to be 2890 and 10% respectively. It can be concluded that frequency overlap between Wi-Fi and ZigBee can cause severe interference on transmission in ZigBee networks. To keep Wi-Fi enabled devices away from ZigBee transmission modules may reduce the effects of interference. However this may not be practical.

However XBee series 2 modules can automatically select channels with an attempt to avoid frequency overlaps. Therefore this type of modules was utilized in the prototype DAS. Careful consideration still needs to be taken to avoid frequency overlaps when ZigBee sensors are used in the presence of a Wi-Fi system. However if Wi-Fi signals arrive after the ZigBee channel being set, it can result in frequency overlap. The emergence of IEEE 802.11n technology that can operate at 5GHz will resolve the frequency overlap problem.

Establish a ZigBee-based WPAN

This experiment was carried out to demonstrate the operation of a WPAN, which would behave as a DAS in RPM. The hypothesis was that if the WPAN could function, ZigBee technology could be validated for RPM application. In the experiment, the ZigBee WPAN was established by using five ZBs, a master node

and a PC. The PC was used to display the received vital signs in the DAS. The purpose of the experiment was to demonstrate the functionality of the prototype DAS. Figure 7.19 shows the architecture of the DAS used in the experiment.

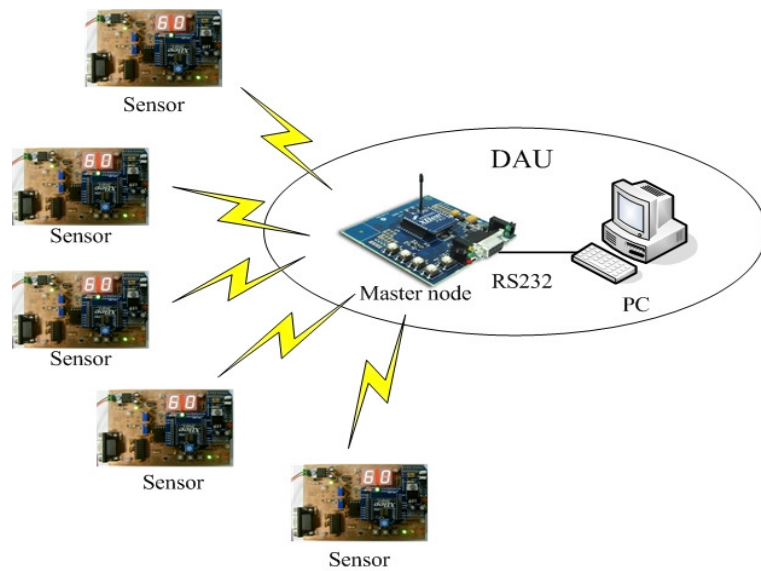


Figure 7.19 - The architecture of the proposed data acquisition system

Some parameters used in this experiment have been listed in Table 7.9. It should be noted that these parameters (e.g. transmission interval) may need further validation in the future.

Table 7.9 - Parameters used in the experiment

The number of used ZBs	5
Transmission interval	1s (changeable)
Used ZigBee channel	Channel 11
Experiment time	20 minutes
Distance between ZBs and the master node	10 – 50 cm

Figure 7.20 shows the equipment used. The master node receives data from the ZBs. Figure 7.21 shows the display of the current reading of vital signs received. The number at the bottom of each bar shows the current readings.

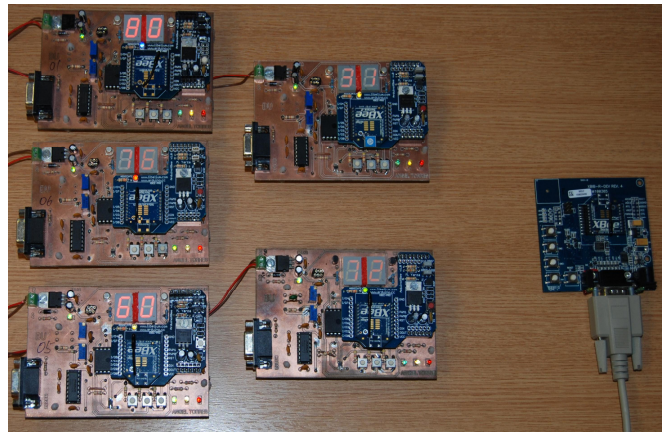


Figure 7.20 - Experiment of the proposed data acquisition system

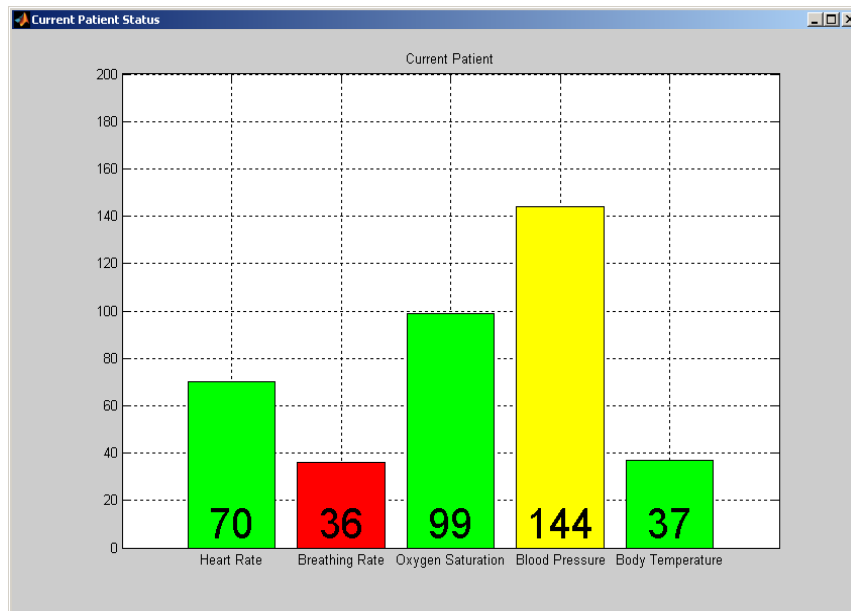


Figure 7.21 - Interface of display on the PC connected with the master node

7.3 Data Transmission System based on a Wireless LAN

It is anticipated that the proposed RPM system will utilize a wireless local area network for sending vital signs from DASs to the central control unit. An experiment has been conducted to test its feasibility. Figure 7.22 shows the equipments used in this experiment. Two PCs with wireless cards were used. They can communicate with each other using an AP in a Wi-Fi network. The left PC in Figure 7.22 was connected to the ZigBee master node. It sent the data received from the master node to the PC on the right hand side representing the server at the central control unit in RPM.

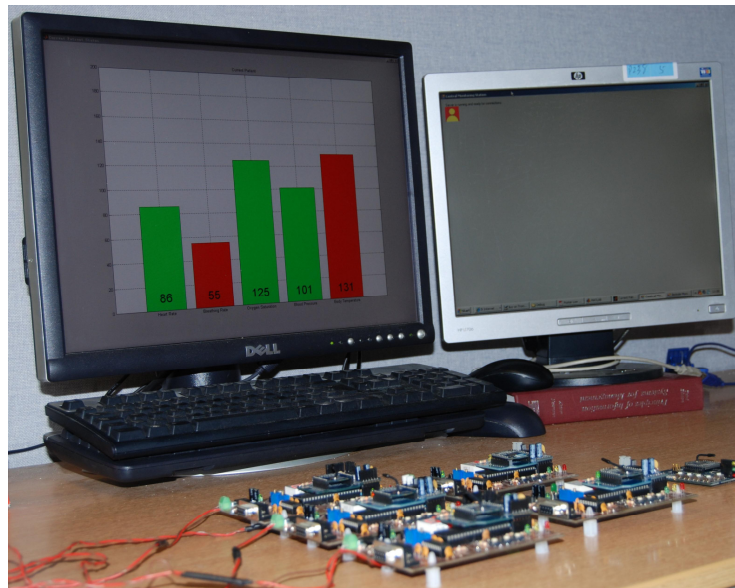


Figure 7.22 - Experiment of using wireless LAN for data transmission

In this experiment, Wi-Fi enabled devices use channel 11 for communication. Digi XBee series 2 modules were utilized. They automatically chose ZigBee

channel 11 for communication. It was already discussed in section 7.2.3 that ZigBee channel 11 does not overlap with Wi-Fi channel 11; hence Wi-Fi transmission between the two PCs did not generate interference on ZigBee transmission. Some other parameters used in this experiment were the same as those which are shown in Table 7.9.

7.4 Prototype Central Control Unit

The prototype central control unit is used to display the received vital signs in real-time. A user-interface has been designed to display patients' vital signs (as shown in Figure 7.23). Icons which include patient IDs are used to represent patients on general wards. The colour of the icons can change to reflect patients' states, which is in correspondence to the three-colour-states mechanism (please refer to Chapter 6).

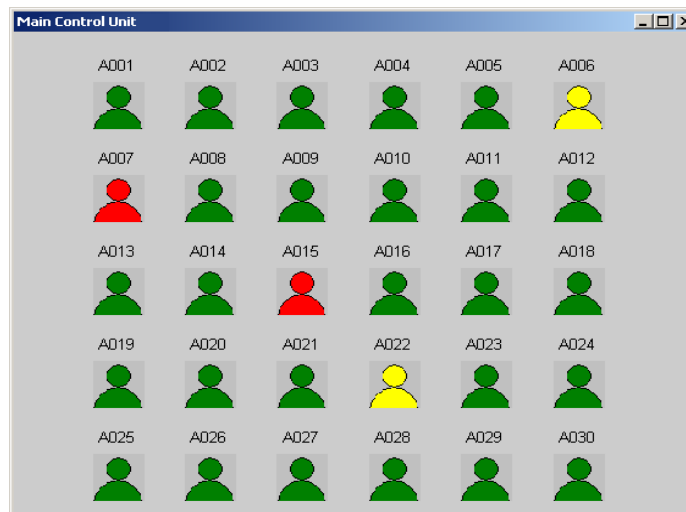


Figure 7.23 - Main panel of central control unit

By clicking on each icon, an individual patient's vital signs can be displayed in a separate interface as shown in Figure 7.24. Five vital signs are displayed in colour bars. The display also includes patient's name, patient ID, age and gender.

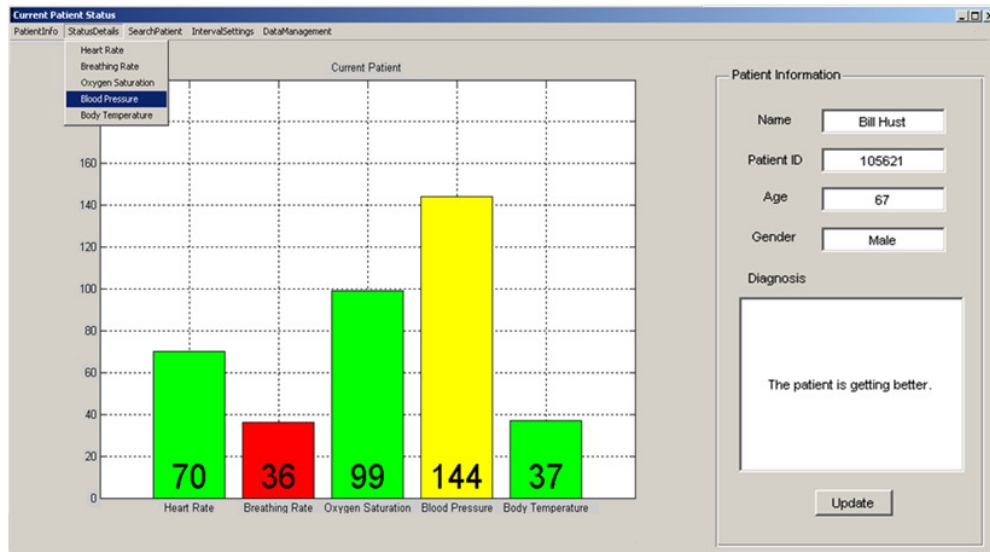


Figure 7.24 - Designed GUI

The colour of the bars indicates the patient's states. For example green means the patient is in a stable condition. It was used for the purpose of prototype design. The colours used for the display in the control unit may need further consideration (in respect of the ambient light, colour blinder etc) in consultation with hospital staff. The database in the control unit can also provide information on the history of the vital sign received from each patient over a period of time. By clicking on a bar, this data can be displayed. Figure 7.25 shows the history of a patient's blood pressure over a period of 10 hours. The designed database can be found in Appendix 8.

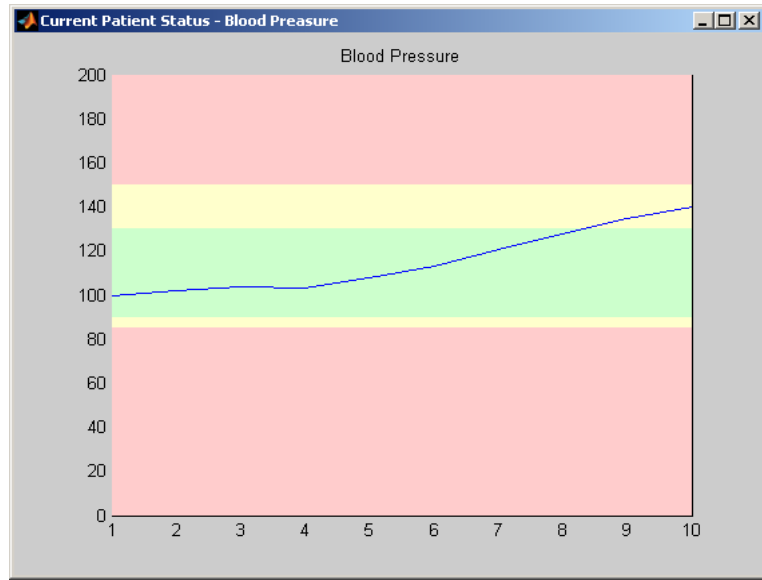


Figure 7.25 - Graph for blood pressure

7.5 Summary

This chapter described the implementation of the prototype RPM. This included three functional parts: data acquisition system, data transmission system and control unit.

The data acquisition system is based on a ZigBee sensor network. In order to implement the data acquisition system, a device called ZB was designed. Such a device was used to simulate a wireless biomedical sensor for obtaining and transmitting the data to a master node. A ZigBee master node and a PC were used to integrate with five ZBs to create a Data Acquisition System (DAS).

Configuration of ZigBee transmission module for both ZB and master node is crucial in the implementation of DAS. The method for configuration was

discussed. In addition two experiments were carried out to test the transmission range and the interference issues. It was found channel overlap problems between ZigBee and Wi-Fi caused degradation in the performance of DAS.

The data transmission system based on Wi-Fi was discussed. An experiment to test the usage of data transmission system was conducted using none-overlapping channels of the DAS. Reliable performance has been achieved.

The control unit is the centre for monitoring, analysis and store of patients' vital signs. A user interface was designed for real-time display patients' vital signs. Recorded vital signs for each patient can also be displayed on demand.

In the next chapter, simulation of vital sign transmission using the proposed RPM system will be discussed.

CHAPTER EIGHT

8 Simulations of Wireless RPM on General Wards

8.1 Introduction

Simulating the real world is an inexpensive way to test a system on a large scale (Hansen 2006). This method is applied in this research project to investigate the application of wireless networks for RPM on general hospital wards. The main purpose of simulation is to study the performance of the proposed system in transmitting vital signs for RPM on general wards.

Several software packages exist to simulate both wired and wireless communication systems like Wi-Fi and Ethernet-based system. However, only a few software providers have made IEEE 802.15.4/ZigBee a part of their simulation software. The following section looks at different simulation tools that have support or limited support for simulation of the ZigBee and Wi-Fi. A suitable simulation tool will be selected and used for modelling and simulations.

8.2 Simulation tools

OMNeT++

OMNeT++ is a discrete event simulation environment (OMNeT++ 2010). Its primary application area is the simulation of communication networks, but because of its generic and flexible architecture, it is successfully used in other

areas like the simulation of complex IT systems, queuing networks or hardware architectures as well. Its models are based on component architecture. Components are programmed in C++, and then assembled into larger components and models. Although OMNeT++ is not a network simulator itself, it is currently gaining widespread popularity as a network simulation platform in the scientific community as well as in industrial settings.

OMNeT++ does not provide models for simulation of IEEE 802.15.4/ZigBee. Customized models would have to be made to fit ZigBee standard. Although there are several discussed solutions from the community's on-line forum, a fully working contribution has not been found so far. Due to the lack of a functioning ZigBee model, the use of OMNeT++ was limited for this project.

OPNET Modeler

OPNET Modeler is a powerful tool for network modelling and development. It is designed by OPNET Technologies, Inc., which is a provider of management software for networks and applications (OPNET Technologies 2010). OPNET Modeler is an environment for network modelling and simulation, allowing design and study of communication networks, devices, protocols and applications with great flexibility and scalability.

Model development in OPNET Modeler can be carried out through graphical model creation and C++ programming. OPNET Modeler provides flexibility for modelling; systems of any dimensions may be modelled. The models are divided

into layers, Process model, Node Model and complete project model. This facilitates the building of layered network models, and by creating a simple Process model and Node model, a large scale Project model may be built with few adjustments. Besides placing models in a graphical user interface the object oriented C++ is used to program the functionality of the models at the bottom level. The OPNET model in its very core also consists of C++ code. These codes are compiled and executed just like a C++ program, and enables very detailed control of the model by the user (if the user is proficient in C++). When a model has been implemented, simulation parameters can be defined and monitored during simulation. OPNET Modeler also includes analysis tools for result evaluation and comparison.

The ability to simulate wireless systems requires the Wireless Module for OPNET Modeler. The standard library for OPNET Modeler with the Wireless Module includes the model for both the IEEE 802.15.4/ZigBee and IEEE 802.11g/Wi-Fi standards. It also provides vast pull-to-use device/node for ZigBee and Wi-Fi. Therefore, OPNET Modeler is utilized in this project to model and simulate the application of the proposed RPM on general hospital wards.

It should be noted that there are still some other software, like Java Simulator (J-Sim), and Sensor Network Simulator and Emulator (SENSE). However they have limitations for this project, for example, the interface of SENSE only accepts text using C++ and the results are provided in a text file. This contributes to the

efficient use of computational power, but greatly reduces the perceived user-friendliness.

8.3 Simulations of ZigBee-based WPANs in RPM

In Chapter 7, a ZigBee-based sensor network (WPAN) was discussed to be used for RPM. To investigate the feasibility of using ZigBee-based WPANs in RPM for multiple patients, a series of simulations were carried out using OPNET Modeler. The subsequent section introduces the components of a WPAN and their attributes used in simulations.

8.3.1 Components and Configurations Used in Simulation

A ZigBee-based WPAN consists of a master node and several sensors (ZBs). OPNET Modeler was used to simulate these devices.

8.3.1.1 Master Node

The model of master node used is shown in Figure 8.1. This model confines to ZigBee (IEEE802.15.4) and industrial standard which was provided by OPNET Modeler. It is worth mentioning that PHY and MAC layers of the model as defined by IEEE 802.15.4 can be customized based on the requirement of simulation, whereas the network and the application layers do not permit customization, which lead to some limitations in using OPNET for simulation of ZigBee network. Despite these limitations, OPNET is still the most powerful tool for ZigBee simulations at present.

Configuration of the master node includes multiple attributes including the transmission frequency band, the receiver sensitivity, network topology, network ID, etc. Relevant setting will be introduced based on different scenarios. Figure 8.2 shows the panel that was used to configure the attributes of a master node.

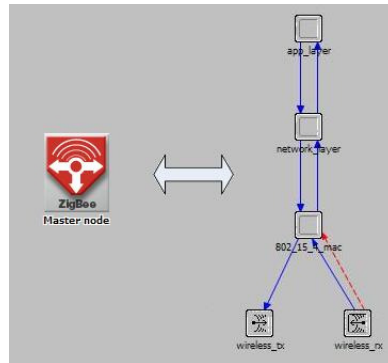


Figure 8.1 - Model of a master node

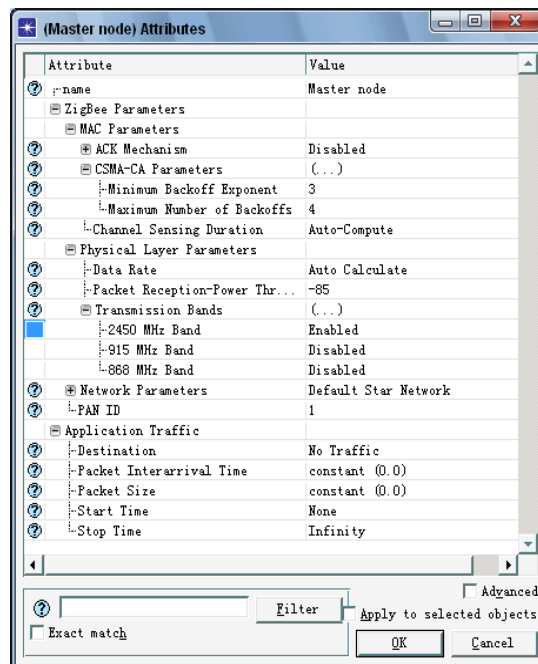


Figure 8.2 - Configuration panel of ZigBee master node

8.3.1.2 Sensor Node

The model of ZigBee sensor node (shown in Figure 8.3) provided by OPNET Modeler is similar to the model for the master node. However the attributes for them have some differences, which can be identified when comparing Figure 8.2 and 8.4. For example, master node model provides the option for setting network topology whereas sensor node model does not.

Configuration of application traffic is an important part in simulation. It includes setting the transmission interval, start transmission time, packet size and so on. These features are different for the master node compared to the sensors which are used to measure and transmit vital signs. In addition, these features were modified in different scenarios for the simulation. Figure 8.4 shows the panel for configuring the attributes for the sensors. Some attributes like frequency band, CSMA/CA parameters shown in Figure 8.4 have been used in simulation. Detailed configurations for the sensors will be discussed in the sections of describing the scenarios.

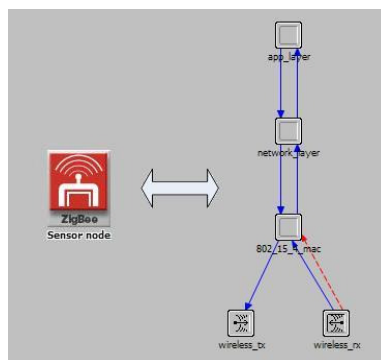


Figure 8.3 - Model of a ZigBee sensor (ZB)

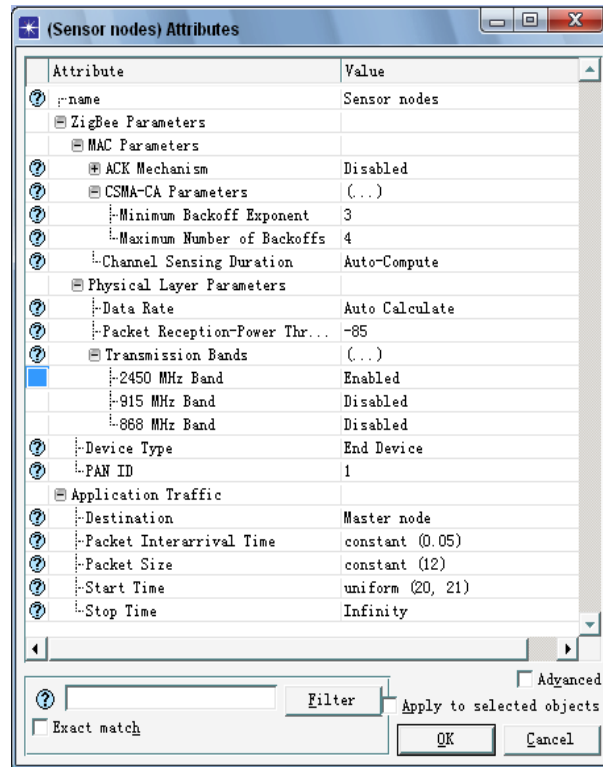


Figure 8.4 - Configuration panel of ZigBee master node

It is worth mentioning that the ZigBee model provided by OPNET Modeler needs modification before using it in a simulation. The attributes of wireless_tx and wireless_rx (two model blocks shown in Figure 8.3) need to be changed based on the specifications of ZigBee technology. The changes include data rate, packet format, frequency band, and modulation type. Number of rows (shown in both Figure 8.5 (a) and (b)) were set to 1, which means that dynamic change of channel was restricted in the simulation, since the existing ZigBee products do not support it. In addition, the types of packets supported for transmission are shown in Figure 8.6. The types of packets that are commonly used in ZigBee communications

were set to be supported-status. In simulation, ZigBee models can select an appropriate format from them automatically.

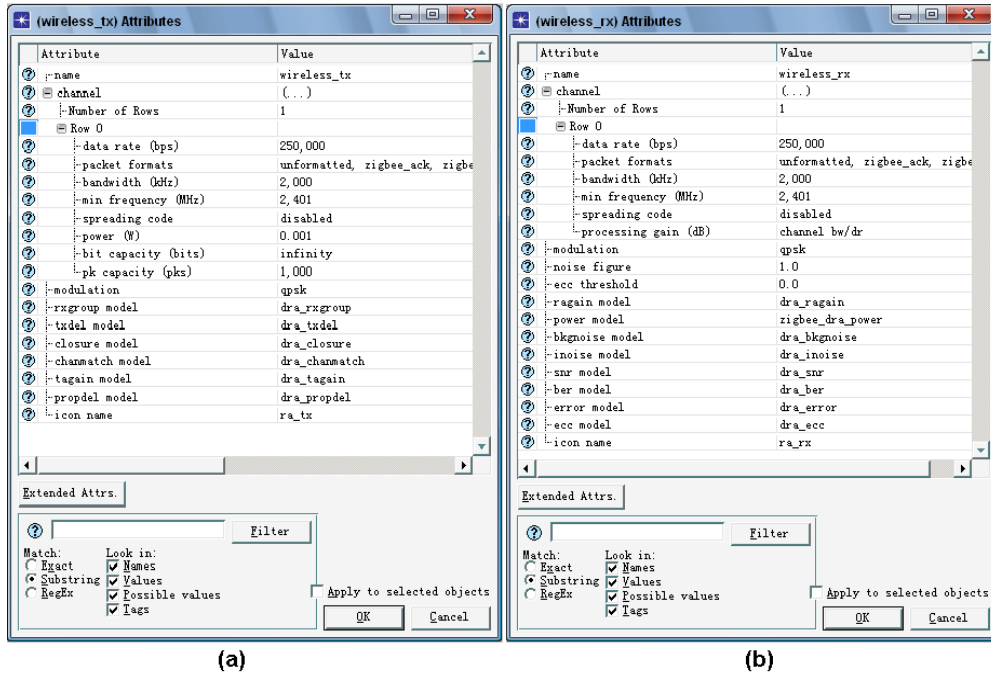


Figure 8.5 (a) - Attributes of wireless_tx (b) - Attributes of wireless_rx

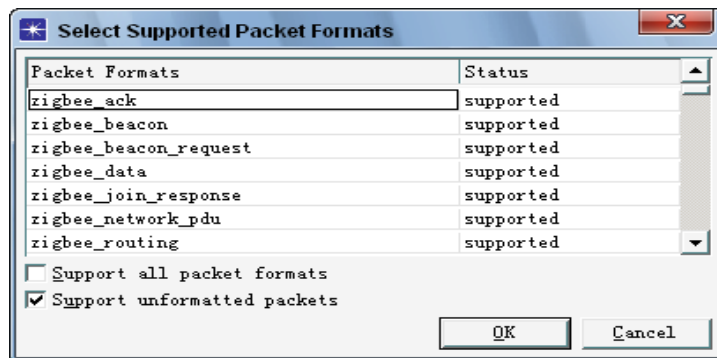


Figure 8.6 - Supported packets types in simulation

8.3.2 Alternative Approaches for ZigBee-based RPM

Two possible network structures may be considered for sensor networks (WPANs) on general wards for the transfer of data from the sensors. They are single ZigBee network approach and multiple ZigBee network approach as was discussed in Chapter 5. These two alternative approaches are simulated in the section below and the results are evaluated.

8.3.2.1 A Single ZigBee Network for Remote Patient Monitoring

In this approach a single WPAN based on ZigBee forms part of RPM as suggested by Khan *et al.* (2008). The WPAN is used to transmit vital signs gathered by sensors attached to all the patients on a general ward to a single master node. The master node may subsequently transmit the data through an Ethernet network to a control unit for monitoring.

It was claimed that this approach could improve the efficiency of transmission, as data from all the patients would be aggregated to a larger packet for transmission by the master node (Khan *et al.* 2008). This was also supported by Junnila *et al.* (2008), which stated that a single master node should be capable of supporting RPM in a multiple patients setting, as it can support 65535 network addresses for the sensors and other devices in this network.

8.3.2.2 Multiple ZigBee Networks for Remote Patient Monitoring

An alternative approach proposed in this project is to use a ZigBee WPAN for each patient. The sensors in each WPAN will be within a short proximity of a master node to control the devices and their communication in this WPAN. In such a case there will be a limited number of active sensors generating a moderate amount of data for transmission. Hence there will be no data loss due to channel capacity. To illustrate this, performances of the two network structures are evaluated in a simulation environment which is discussed in the following sections.

8.3.3 Simulation Results and Discussions

Both the two approaches discussed above may be used for RPM; however there is a major difference between their reliability. In order to evaluate their performance, OPNET Modeler was used to simulate two scenarios based on using the two approaches for RPM on a general ward. The focus of the simulations was to study the delay for the data transmitted by the sensors as well as the volume of data communicated.

In both scenarios, four patients were considered for each ward and five sensors for each patient. A rectangular room (10m× 8m) was considered for the ward and the patients were equally spaced in it.

Table 8.1 shows the type of vital signs selected, which were based on the recommendation in clinical guidance by the NICE (2007). NICE stated that as a

minimum, these five vital signs should be used for monitoring. Table 8.1 also shows the data rates used for the transmission of vital signs measured by the sensors for both the simulations. The parameters used in the simulations are summarized in Table 8.2.

Table 8.1 - Vital signs measured for RPM on general wards

Vital signs	Parameter Range	Data Rate (kbps)
Heart Rate (beats/min)	40-240	0.6
Respiratory Rate (breaths/min)	2-50	0.24
Blood Pressure (mmHg)	10-400	1.2
Oxygen Saturation (%)	90-100	0.48
Temperature ($^{\circ}$ C)	32-40	0.0024

Table 8.2 - Parameters used in simulation

Parameters	Value
Length of simulation run (sec)	600
Transmitted power (mw)	1
Number of patients	4
Number of sensor nodes	20

Figure 8.7 shows the increase in the time delay for the single WPAN RPM. The reason for this is due to all the ZigBee nodes using a single channel for communications. This channel can only provide 250 kbps bandwidth, which is shared by all the sensors.

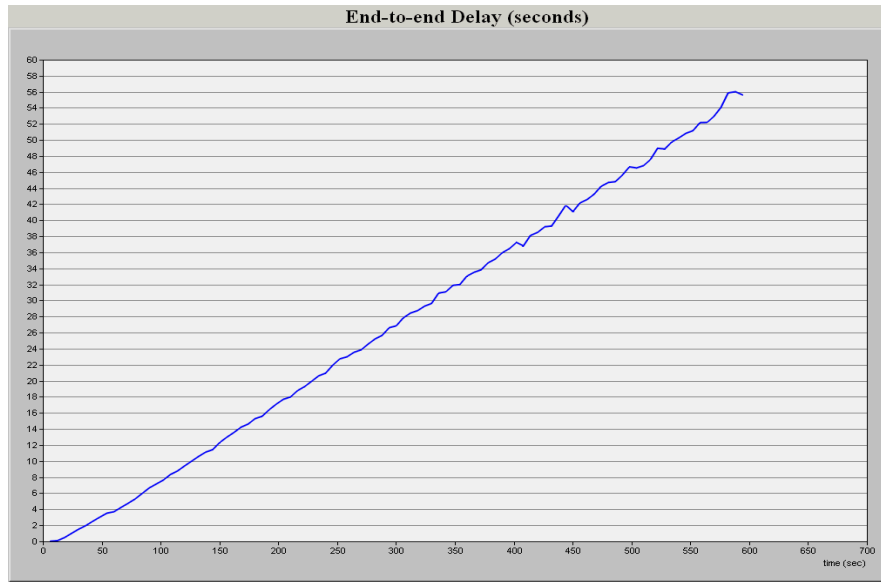


Figure 8.7 - Transmission delay from sensors to the master node in a single WPAN RPM

Figure 8.8 illustrates the volume of data transmitted by all the 20 sensors (Tx) and the volume of data received by the master node (Rx) in a single ZigBee WPAN RPM. The reason for the difference between the total volume of data received by the master node and the volume of data transmitted by all the sensors (shown in Figure 8.8) is due to the drop of data packets. When a last attempt for transmission of a packet is classified as a failure, the sensor node removes the waiting packet from its buffer. Increasing the buffer capacity of the sensors would reduce packet loss; however it will increase the transmission delay. It can be argued that the more the number of the patients who are monitored, the busier the traffic load and the higher the data loss. Data loss rate in this case as shown in equation 8.1 is:

$$\text{Data loss rate} = \frac{\text{Transmitted data} - \text{Received data}}{\text{Transmitted data}} = 26.2\% \quad (8.1)$$

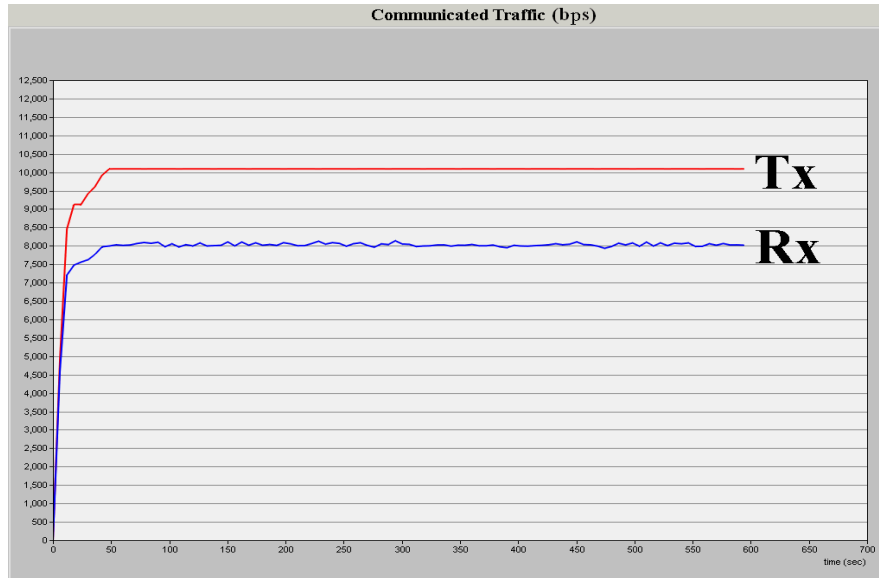


Figure 8.8 - Data volume transmitted by sensors and received by the master node in a single WPAN RPM. Tx - transmitted data by the sensors, Rx - received data by the master node

In summary, a single WPAN RPM has a higher data loss rate and high transmission delay. Therefore, it is not suitable for RPM on general wards in this scenario.

When using multiple WPANs, each master node selects a channel for its own WPAN, which provides more bandwidth per ZigBee sensor. Hence a sensor gets more chance to send its packets in the multiple-WPAN approach. Figure 8.9 provides a comparison between the total volume of data transmitted by the sensors in both single and multiple WPAN RPM. Graphs (a) and (b) in this figure show the total

volume of data transmitted in the single WPAN and multiple WPANs RPM respectively. In both cases, the same number of sensor was used. The increase in the data volume in (b) is due to the number of packets re-transmitted.

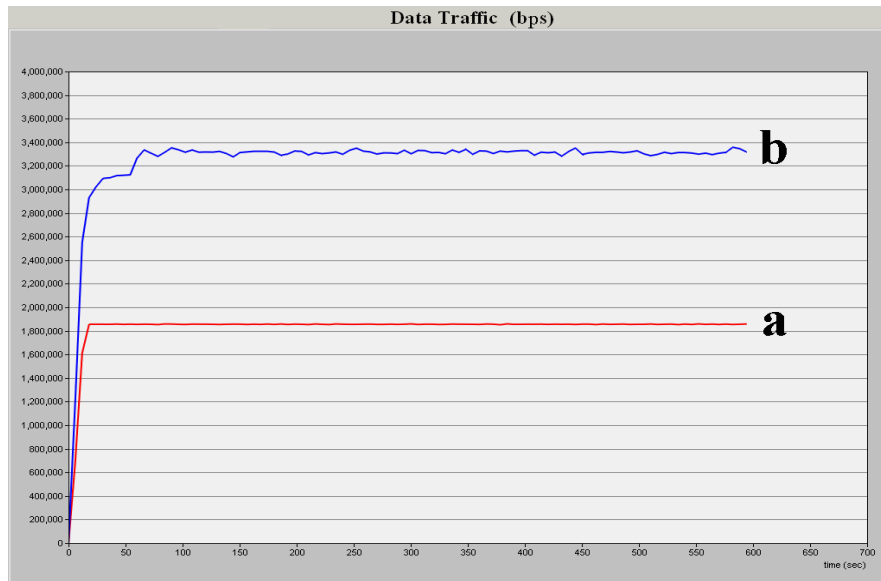


Figure 8.9 - Total volume of data transmitted by the sensors, (a) in a single WPAN and (b) in multiple WPAN RPM

A similar comparison was made in respect of the efficiency of data transfer. Figure 8.10 shows the successful data transfer in both single and multiple WPAN RPM. In both the scenarios the total volume of data captured by all the sensor nodes for transmission are the same. However, the volume of data received by the master node in the single WPAN RPM should be equal to aggregate volume of data received by all master nodes in multiple WPANs RPM. It can be observed that the graph (M) presenting multiple WPANs is much higher than the graph(S) for single master node (or single WPAN) RPM, which means that the multiple

WPANs provide a more efficient data transfer for RPM, compared to a single master node approach. Many of the data may have not reached the master node in the case of using a signal master node (S).

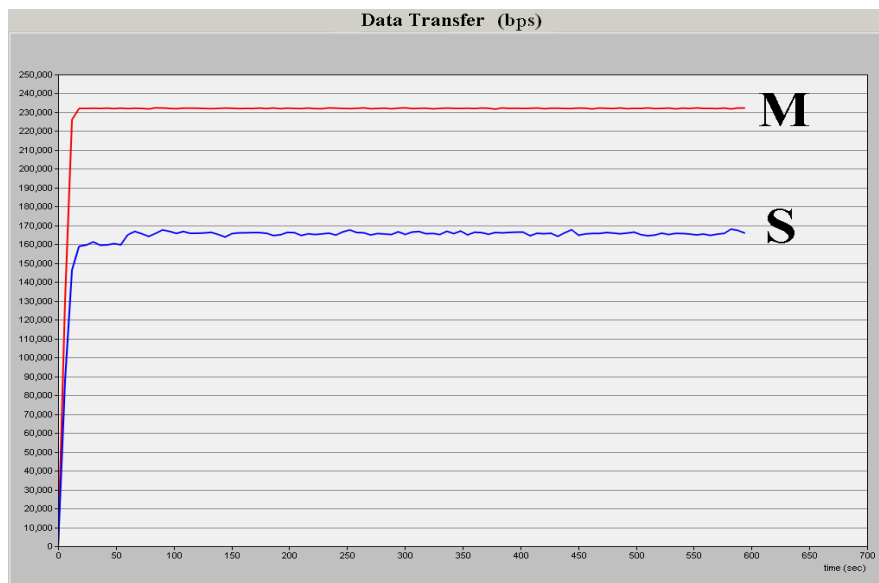


Figure 8.10 - Comparison of successful data transfer using a single and multiple WPAN RPM. M-multiple WPANs RPM, S-single WPAN RPM

Figure 8.11 shows the volume of data transmitted in the case of multiple WPANs. Figure 8.11(a) presents the data volume transmitted from the sensors to the master node in each WPAN; Figure 8.11 (b) shows the data volume received by the master nodes in each WPAN. The figures show the same volume of data communicated in each WPAN. They also illustrate that the volume of data transmitted by five sensors equal to the volume of data received by their master node in each WPAN. So there was no data loss in the communication in each WPAN.

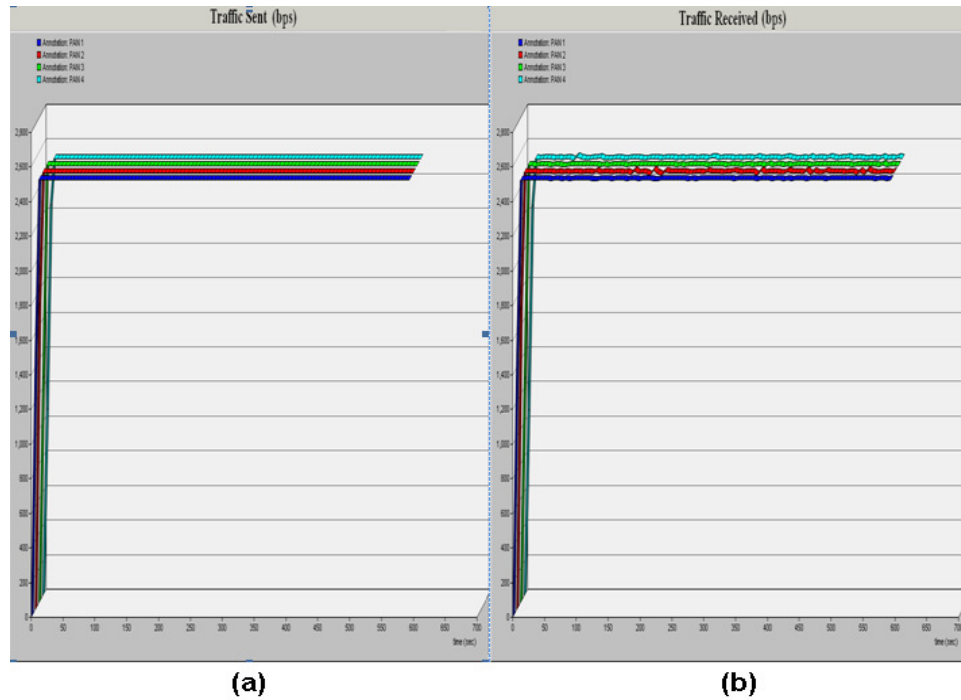


Figure 8.11 - (a) Data volume transmitted from the sensors to the master node in each WPAN (b) data volume received by the master nodes

Figure 8.12 presents the end-to-end delay profile for each WPAN. The end-to-end delay includes media access delay, pack delay and so on. The figure shows two of the WPANs in the system experience longer delays (14ms) than the other two (7ms). This is due to the WPANs using the same transmission channel; some sensors have to delay their transmissions due to waiting for the channel idle period. In this scenario, the effect of channel overlap is negligible. It was indicated by Soomro and Cavalcanti (2007) that the highest threshold for transmission delay in respect of medical applications is 300ms. Therefore, it can be argued that 14 ms end-to-end delay is acceptable in this scenario.

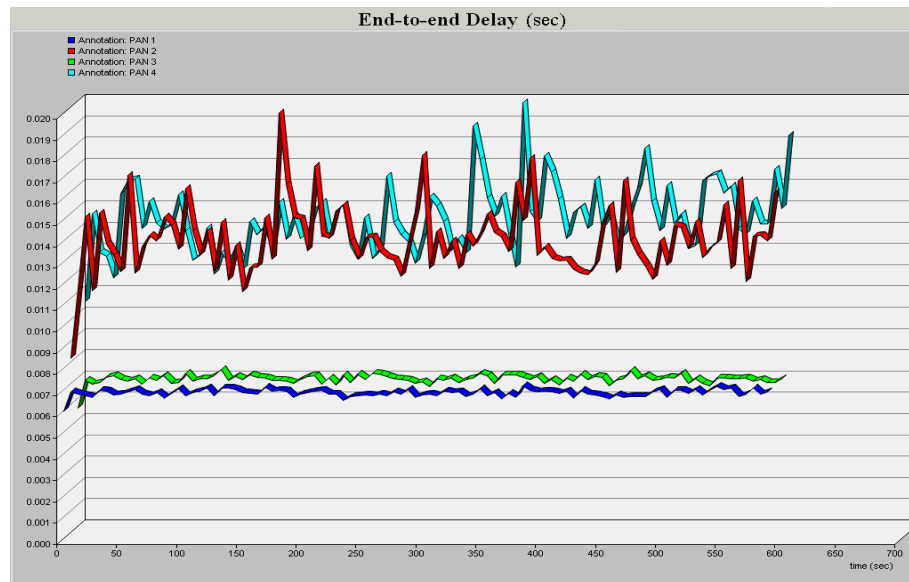


Figure 8.12 - End to end delay for multiple WPAN RPM in each WPAN

The simulation results show that the multiple WPAN approach provided more reliable performance than the single-master-node approach in data transmission. It may be more suitable than the latter for RPM on general hospital wards. Although the cost may be higher for deployment for multiple WPANs, it offers efficient and speedy data delivery as well as improved reliability.

8.3.4 Channel Overlap Problems of ZigBee Networks for RPM

The application of multiple ZigBee networks in RPM may generate channel overlaps. This is due to the limited number of channels used for data transmission by ZigBee networks. Networks using the same channel may experience contention, which can degrade their performance, as it is shown in Figure 8.12 in

last sub-section. WPANs using the same channel have higher transmission delays than those which do not.

To further evaluate performance of multiple sensor networks in a large general ward and to examine the effect of channel overlap between them, the performance of using 30 WPANs in RPM was evaluated. Each WPAN supported a patient utilizing five sensors. A rectangular room 40m×10m was considered for the ward and the patients were equally spaced in it. The results of this simulation are discussed in the next section.

8.3.5 Simulation Results and Analysis of Channel Overlap

To investigate the performance of multiple ZigBee WPANs in a situation where channel overlapping may occur, a model of a RPM system based on 30 ZigBee WPANs is simulated. The vital signs selected, are listed in Table 8.3. To test the capability of the WPANs in the presents of severe channel overlapping, a heavy traffic load is generated in simulation. In this situation, transmission intervals close to the sampling rates of the sensor devices were selected. The intervals for the transmission of data from the sensors to their master nodes are shown in Table 8.3. However, it should be noted that the transmission interval used in this project was for simulation purposes. Further study is required to validate them.

In this scenario, several WPANs used overlapping channels. Channel overlaps generated transmission delays and data loss, which are shown in Figure 8.13, 14 and 15.

Table 8.3 - Vital signs measured for patient monitoring

Vital Signs	Transmission Interval(S)	Sample Size(bits)	Data Rate(Kbps)
Heart Rate	0.02	12	0.6
Respiratory Rate	0.05	12	0.24
Blood Pressure	0.01	12	1.2
Oxygen Saturation	0.025	12	0.48
Temperature	0.5	12	0.024

In addition, other parameters used in the simulation are summarized in Table 8.4.

Table 8.4 - Parameters used in simulation

Parameters	Value
Length of simulation run (S)	600
Transmitted power (mw)	1
Minimum back off exponent (BE)	3 (default)
Maximum number of back offs (NB)	4 (default)
Number of patients	30
Number of sensor nodes for each patient	5

Figure 8.13 illustrates the volume of data attempted for transmission by the sensors and the data received by the master node in each WPAN. It can be observed that the volume of data received by the master nodes is far less than the volume of data attempted for transmission in most WPANs. This means that there is a considerable loss of data during the transmission process. The reason is that due to channel occupancy and contention, a large number of packets are

discarded. However Figure 8.13 also shows that some master nodes received all the data which was sent to them by their sensors. They included the 1st, 6th, 9th, 10th, 11th, 23rd, 25th and 28th WPANs. These WPANs did not share their channels with the other WPANs in communication.

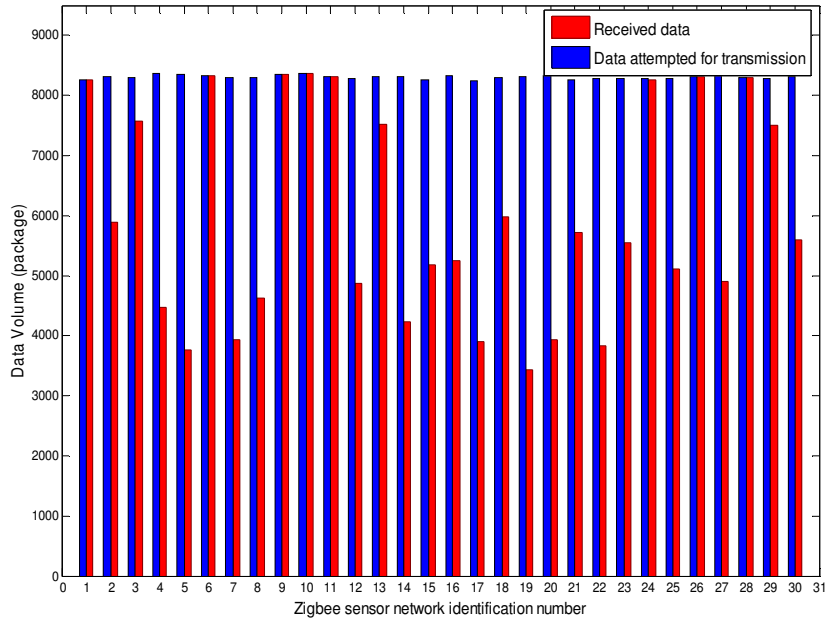


Figure 8.13 - Comparison of data transmission and reception in each WPAN

The ratio of data received by a master node to the data attempted for transmission to that master node can be expressed by following equation:

$$\text{Ratio} = \frac{\text{Received data}}{\text{Data attempted for transmission}} \quad (8.2)$$

Figure 8.14 illustrates this ratio for each WPAN. Only eight WPANs out of 30 received the data completely without any losses; more than half the WPANs missed over 25% of the data, which is unacceptable for RPM.

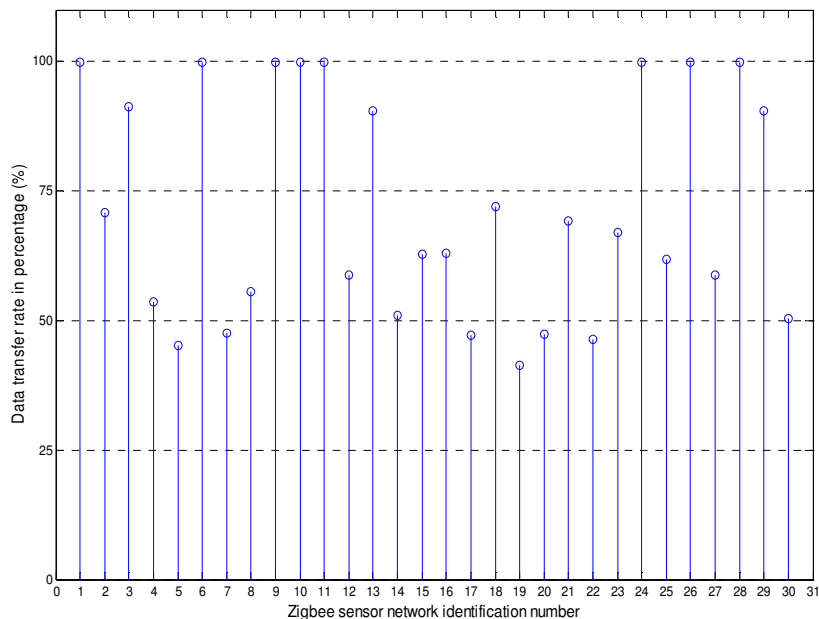


Figure 8.14 - Successful data transfer rate

The severity of loss of data depends on the number of WPANs which share the same channel. This can also affect the transmission delay caused by data waiting in the buffer prior to transmission. Figure 8.15 illustrates the transmission delays for four of the WPANs. In this simulation, WPAN1 shared its channel with only one other WPAN. Thus, the delay for transmission in WPAN1 remained relatively low, almost to zero. However, the delays have increased in time in the case of WPANs 2, 3 and 4 as they shared their channels with more WPANs. For example,

WPAN 2 shared a channel with five other WPANs; WPAN 3 with three other WPANs and WPAN 4, which had the worst performance, shared the channel with seven other WPANs.

In this simulation the total delay calculated is due to the waiting period that experienced by packets before transmission. According to OPNET Modeler (2009), this waiting period may be calculated using equation (8.3):

$$\text{Delay} = \sum_{NB=1}^4 2^{BE} - 1, BE \in [0, 3] \quad (8.3)$$

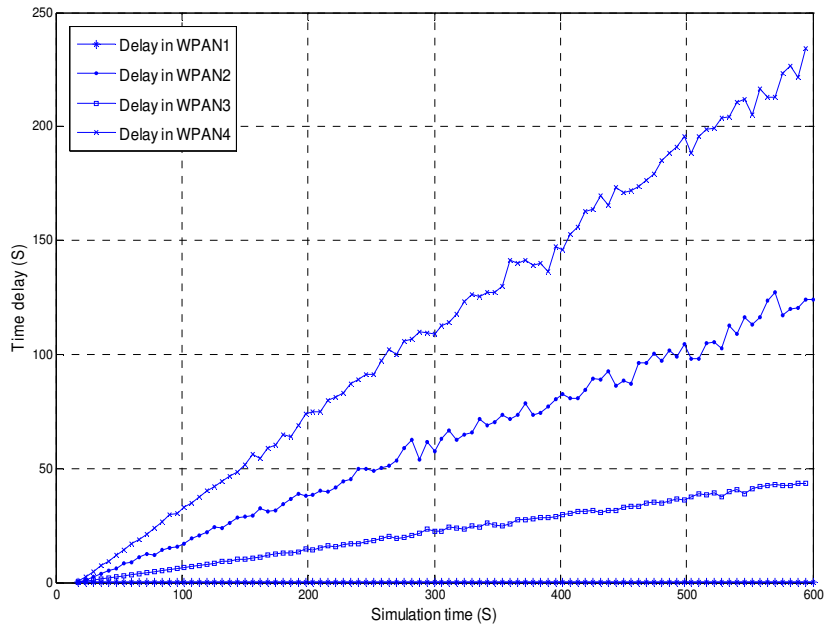


Figure 8.15 - Comparison of transmission delay through WPANs

Although in the above scenario, unrealistic and excessive volume of data was transmitted for testing the capability of WPANs under a severe transmission load,

timely and accurate transmission of vital signs of patients is crucial in RPM. When a large number of WPANs are used, the problem of channel overlapping may become unavoidable. Care should be taken to ensure that multiple ZigBee WPANs can operate effectively supporting RPM.

8.3.6 Realistic Transmission Intervals for RPM on General Wards

It can be seen from Table 8.4 that the chosen transmission intervals for the vital signs are very short. The frequent transmission of this data generates unnecessary traffic and increase contention in the channels. Patients on a general wards are normally in a stable condition and they may not require monitoring at this high rate. Intervals of 30 seconds or a minute would be more than adequate for the transmission of vital signs, even for patients who may require closer monitoring.

The transmission of vital signs using longer intervals reduces the traffic load on the channels thereby mitigating contentions. In such a case multiple ZigBee WPANs will be capable of supporting RPM for a general ward, even in the presence of overlapping channels. In order to validate this, a scenario is simulated based on the assumption that the sensor nodes send vital signs using the longer transmission intervals as shown in Table 8.5.

Although the channel overlapping problem still exists, the contention for the channels is considerably reduced. Sensor nodes are able to access a channel for transmission and data packets loss is significantly reduced, as it is shown in Figure 8.16. In contrast with Figure 8.13, there is no obvious difference between

the volume of data attempted for transmission by the sensor nodes and the volume of data received by the master nodes. This means vital signs were transferred from sensors to their master nodes successfully in almost all the WPANs.

Table 8.5 - Vital signs transmitted in RPM with revised intervals

Vital Signs	Trasmission Interval(S)	Sample Size(bits)
Heart Rate	0.2	12
Respiratory Rate	0.5	12
Blood Pressure	2	12
Oxygen Saturation	1	12
Temperature	5	12

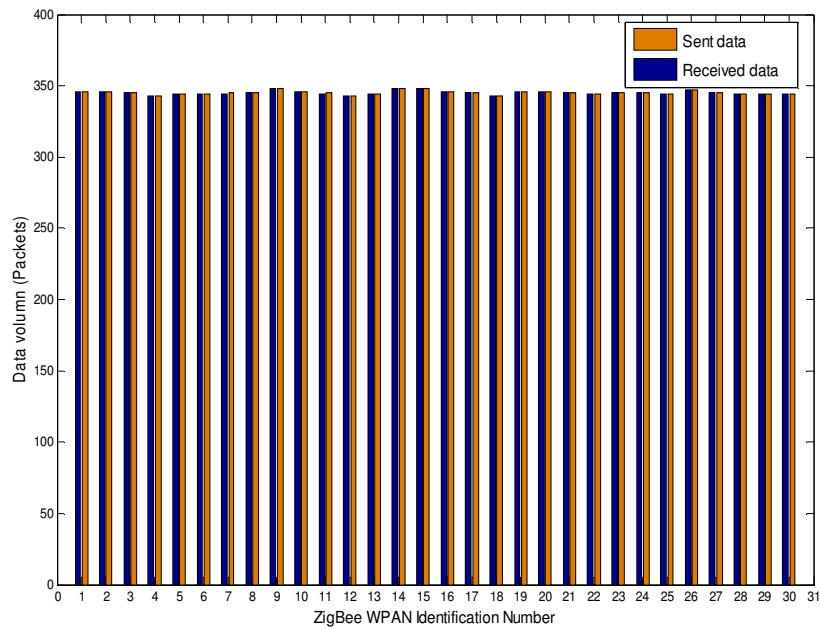


Figure 8.16 - Comparison of transmission and reception in each WPAN

The ratio presented by equation 8.2 in this scenario is shown in Figure 8.17. Most of the master nodes have received the data transmitted by the sensors in their WPANs. Data loss has only occurred in the 7th and 11th WPANs. This could also be attributed to data corruption caused by interferences or errors.

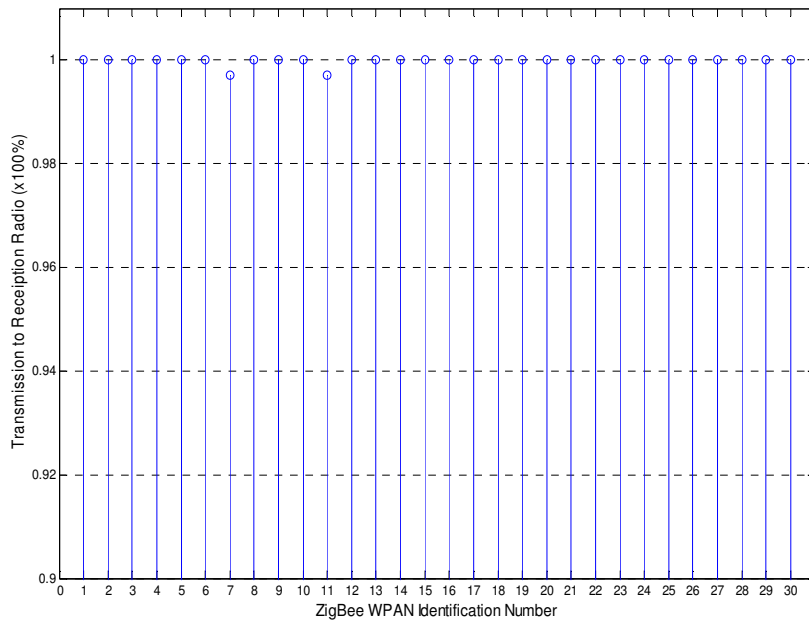


Figure 8.17 - Successful data transfer rate using longer transmission intervals

Figure 8.18 shows the delays for the longer transmission intervals for the same four WPANs which were shown in Figure 8.15. Figure 8.18 shows that data packet delays have been considerably reduced. Obviously, the reason for the improved performance of these WPANs is due to less contention for the channels.

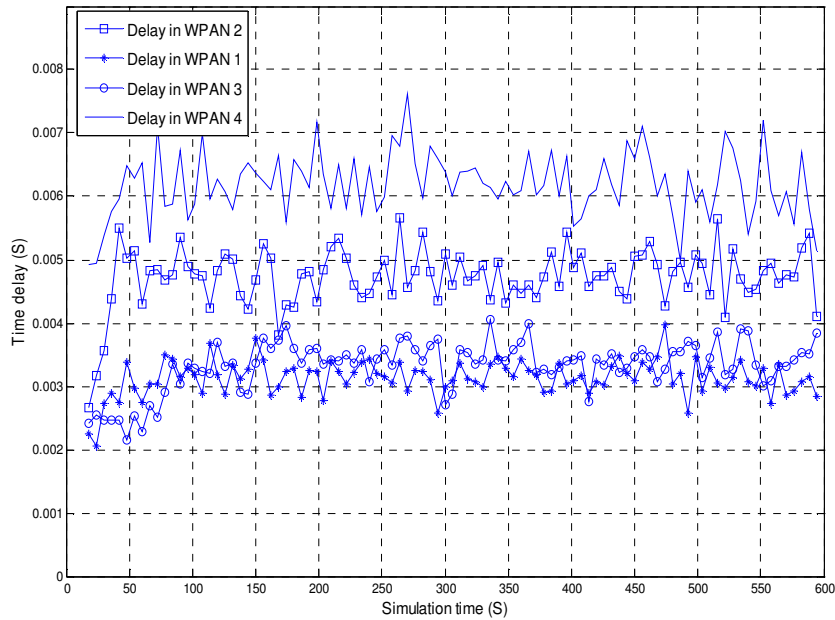


Figure 8.18 - Comparison of delays for transmission

Bearing in mind the above, it can be argued that multiple ZigBee WPANs can be used for RPM on general wards, as long as, changed transmission intervals are used. These intervals were chosen against realistic transmission. In the case of patients who are in stable conditions, even longer transmission intervals than those shown in Table 8.5 may be selected. This will enable the remaining channel capacity of WPANs be used for other medical applications.

It can be concluded that multiple WPAN approach can support RPM for general hospital wards. The intervals of transmission of vital signs should be selected appropriately in order to ensure reliable delivery. Further investigation may be required to develop a scheme for selection of appropriate transmission intervals.

8.4 Simulations of WLAN in RPM

The purpose of this section is to model a WLAN for supporting RPM of general hospital wards and evaluate its performance. The evaluation includes aspects such as transmission delay, throughput, re-transmission and so on. An assumption has been made that 100 patients were monitored. Each patient was allocated a DAS for sending vital signs to a server in a control unit. It should be noted that all DASs were static in the simulation since mobility and roaming issues were not the focuses of this research. An extreme case is used in modelling the WLAN system that all the traffic from 100 DASs to the server is through an AP. It is to investigate the capacity of the WLAN system for transmission vital signs in RPM on general wards.

Simulations are carried out by using TCP or UDP protocols for the transportation of patients' vital signs respectively. In addition, a worse case scenario is simulated where extra heavy traffic load are delivered using the WLAN to generate collision with vital signs transmission. The performance of the WLAN is evaluated. The following section introduces the components and attributes, which were used in modelling and simulation of the WLAN.

8.4.1 Components and Parameters Used in Network Modeling

The modelled WLAN data transmission system includes four types of components. They are DASs, AP, Ethernet switches and a control unit. Configuration of DASs is mostly important in the simulation, since its attributes determine the traffic load

and possible collisions on the simulated WLAN system, whereas the APs, Ethernet switches and the server in the control unit do not need much work on configurations; most attributes can adopt default setting provided by OPNET.

8.4.1.1 DAS and Configuration

WLAN workstation provided by OPNET is utilized to serve the DAS requirements. Its main task in the simulation is to generate data traffic for transmission through the WLAN. Each of the 100 DASs was assumed to generate 1500-byte (maximum size of an Ethernet package) vital sign packets per second for transmission. It should be noted that an Ethernet package contenting five types of vital signs can be smaller than 1500 byte as vital signs transmitted from sensors to a DAS are far less than 1500 bytes per package. The adoption of 1500 byte/second data rate in the simulation was to increase the manageability. In reality vital signs transmission from a DAS to the control unit should be based on some specified requirements of patient monitoring or some standards for RPM on general wards.

Figure 8.19 shows the icon of a WLAN workstation (DAS) and its model used to serve its usage in simulations. As it can be observed, it contains seven layers. Starting from the highest layer (Application layer) the model will invoke the application to get the patients' data. Then the data will be passed down to the transport layer. The transport layer will send the packet of information either over TCP or UDP. Then the "ip_encap" will encapsulate the packet in an IP datagram.

The ARP (Address Resolution Protocol) will map the DAS's IP address to its MAC address and will send the packet to the IEEE 802.11g MAC layer. The unique MAC address of every master node in a DAS will be automatically assigned by OPNET Modeler. Ultimately, the packet will be passed down to the DAS's WLAN transmit port (PHY layer) ready for transmission.

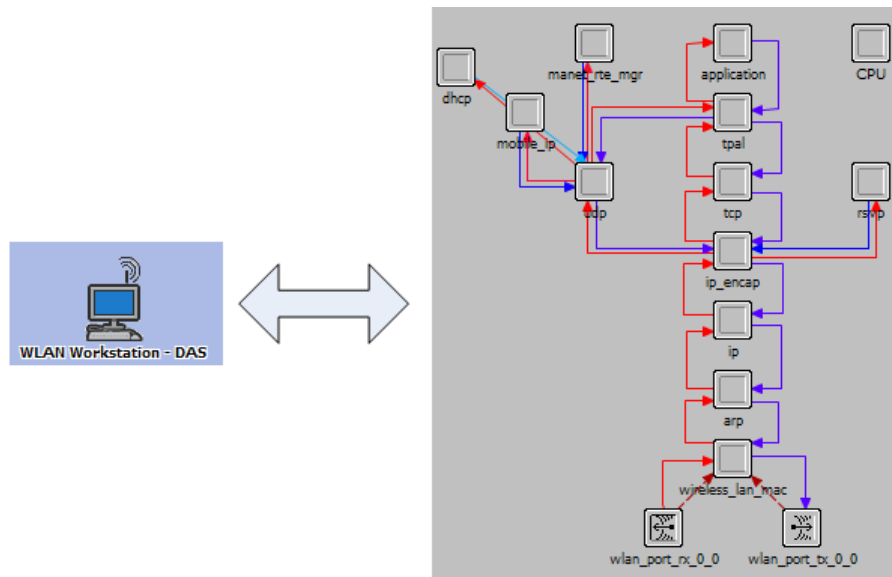


Figure 8.19 - The DAS model used in simulation

Configuration of PHY and MAC of WLAN components are important in the simulation, since the values selected can affect validation of the data transmission system. Figure 8.20 lists the parameters used for configuration of a DAS. These parameters were not varied in the simulation of different scenarios (except the setting of the channel number and BSS Identifier).

[-] Wireless LAN	
[-] Wireless LAN MAC Address	Auto Assigned
[-] Wireless LAN Parameters	(...)
[-] BSS Identifier	1
[-] Access Point Functionality	Disabled
[-] Physical Characteristics	Extended Rate PHY (802.11g)
[-] Data Rate (bps)	54 Mbps
[-] Channel Settings	(...)
[-] Bandwidth (MHz)	22
[-] Min Frequency (MHz)	2,401
[-] Transmit Power (W)	0.100
[-] Packet Reception-Power Threshold...	-65
[-] Rts Threshold (bytes)	None
[-] Fragmentation Threshold (bytes)	None
[-] CTS-to-self Option	Enabled
[-] Short Retry Limit	7
[-] Long Retry Limit	4
[-] AP Beacon Interval (secs)	0.02
[-] Max Receive Lifetime (secs)	0.5
[-] Buffer Size (bits)	1024000
[-] Roaming Capability	Disabled
[-] Large Packet Processing	Drop
[+] PCF Parameters	Disabled
[+] HCF Parameters	Not Supported

Figure 8.20 - Attributes of a configured DAS

MAC Specific Attributes of DAS

The DCF mechanism has been enabled with regular RTS/CTS frame exchange, whereas PCF is disabled (please refer to Chapter 4 for more information). The maximum number of transmission attempts for *Short Retry Limit* has been set to 7, while the same setting has been set to 4 for *Long Retry Limit*. Data frames that could not be transmitted after these attempts will be discarded from DAS.

The fragmentation threshold has been disabled, so transmitted data packet will be 1500 bytes size. The default maximum buffer size (1024 Kbits or 128 Kbytes) has

been adopted. Therefore the number of data packets that cannot be held by a DAS will be:

$$128,000 \text{ bytes} \div 1500 \text{ bytes/packet} = 85.3 \text{ packets} \quad (8.4)$$

These packets will be buffered when they cannot be transferred successfully. Once the buffer capacity is reached, data packets arriving from the higher layers will be discarded until some packets are removed from the buffer.

PHY Specific Attributes of DAS

The simulation was run using the standard data rate of IEEE 802.11g, 54 Mbps. This value specifies the data rate that was used by the MAC for the transmission of the data frames via the physical layer (OPNET 2009). The WLAN DAS model supports all the data rates specified in IEEE 802.11g standard. However, it will not scale back to support lower data rates at 48, 36, 24, 18, 12 and 9 Mbps when transmission range and signal quality become an issue. Thus, the transmission data rate will be fixed according to the setting, rather than changing with transmission distance. In addition, transmit power and packet reception power threshold have been set according to the 802.11g specifications.

Application Setting of DAS

OPNET Modeler allows the modeling of specific applications tasks and their profiles for every individual node. The DAS traffic model was defined using the OPNET Standard Network Application models. The Standard Network

Application models are a set of models that capture specific characteristics of the application that they represent. These include three objects; the “*Application Definition*”, the “*Profile Definition*” and the “*Task Definition*” object (shown in Figure 8.21).

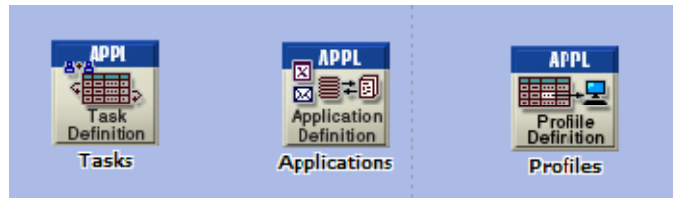


Figure 8.21 - Standard Network Application models

The “Application Definition” object model defines the applications of DASs. It offers a set of pre-defined applications, such as e-mail, FTP or HTTP. To fulfill the requirements of this study the pre-defined application types were disabled, while the full customized application was utilized (shown in Figure 8.22).

[-] Application Definitions	[...]
Number of Rows	1
[-] DAU Custom Application	
Name	DAU Custom Application
[-] Description	[...]
Custom	[...]
Database	Off
Email	Off
Ftp	Off
Http	Off
Print	Off
Remote Login	Off
Video Conferencing	Off
Voice	Off

Figure 8.22 - Application Definition parameters

The DAS custom application defines multiple parameters which can be used in simulations, for example the size of the transmitted packet in bytes, the transport protocol (TCP/UDP) and the destination of transmission (i.e. the control unit). Custom application parameters including their task description are shown in Figure 8.23 and Figure 8.24.

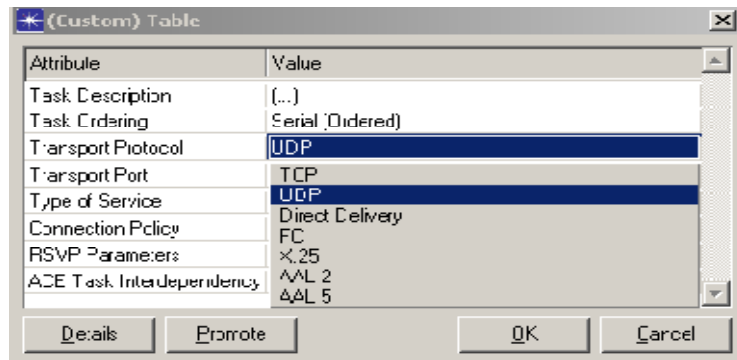


Figure 8.23 - Custom application parameters

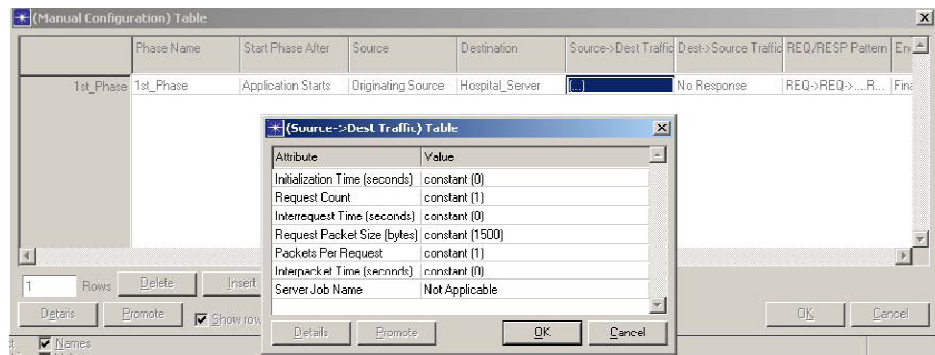


Figure 8.24 - Custom application task table

The profile definition describes the DAS's behavior including the specified applications and the amount of traffic each application generated. Although all the DASs implement the same application for sending vital signs, their Profile

Configurations were unique, since every DAS is a separate entity with its unique property. In the simulation, the Profile Configuration assigned a unique profile name to each DAS, the profile consists of a series of parameters, such as the start time and duration of the profile, the applications used in the profile, the application's operation mode (e.g. random, serial, or simultaneous), the application's repeatability and so on. The used profile parameters are shown in Figure 8.25.

The last step of the traffic modeling was to configure every DAS's application settings to link the device with the application traffic models described above. These settings include application and profile names, application destination and application protocol specification (please refer to Figure 8.26)

[-] Profile Configuration	[...]
Number of Rows	10
[-] UCP Profile	
Profile Name	UDP_Profile
[-] Applications	[...]
Number of Rows	1
[-] DAU Custom Application	
Name	DAU Custom Application
Start Time Offset (seconds)	No Offset
Duration (seconds)	End of Last Task
[-] Repeatability	Once at Start Time
Operation Mode	Serial (Ordered)
Start Time (seconds)	uniform (1, 60)
Duration (seconds)	End of Last Application
[-] Repeatability	[...]
Inter-repetition Time (seconds)	constant 601
Number of Repetitions	Unlimited
Repetition Pattern	Serial
[+] UCP_PROFILE_DAU2	...
[+] UCP_PROFILE_DAU3	...
[+] UCP_PROFILE_DAU4	...
[+] UCP_PROFILE_DAU5	...
[+] UCP_PROFILE_DAU5	...
[+] UCP_PROFILE_DAU7	...
[+] UCP_PROFILE_DAU3	...
[+] UCP_PROFILE_DAU3	...
[+] UCP_PROFILE_DAU10	...
[+] UCP_PROFILE_DAU11	...
[+] UCP_PROFILE_DAU12	...

Figure 8.25 - Profile configuration parameters

[-] Profile Configuration	(...)
[-] Number of Rows	101
[-] UDP_Profile	
[-] Profile Name	UDP_Profile
[-] Applications	(...)
[-] Number of Rows	1
[-] DAU Custom Application	
[-] Name	DAU CustomApplication
[-] Start Time Offset (seconds)	No Offset
[-] Duration (seconds)	End of Last Task
[-] Repeatability	Once at Start Time
[-] Operation Mode	Serial (Ordered)
[-] Start Time (seconds)	uniform (1, 60)
[-] Duration (seconds)	End of Last Application
[-] Repeatability	(...)
[-] Inter-repetition Time (seconds)	constant (60)
[-] Number of Repetitions	Unlimited
[-] Repetition Pattern	Serial
[-] UDP_PROFILE_DAU2	...
[-] UDP_PROFILE_DAU3	...
[-] UDP_PROFILE_DAU4	...
[-] UDP_PROFILE_DAU5	...
[-] UDP_PROFILE_DAU6	...
[-] UDP_PROFILE_DAU7	...
[-] UDP_PROFILE_DAU8	...
[-] UDP_PROFILE_DAU9	...
[-] UDP_PROFILE_DAU10	...
[-] UDP_PROFILE_DAU11	...
[-] UDP_PROFILE_DAU12	...

Figure 8.26 - DAS Application settings

It is worth mentioning that the processes in OPNET are expressed in a programming language called Proto-C. It consists of state transition diagrams (STDs), a library of kernel procedures, and the standard C programming language (OPNET 2009). Within each state, general logic can be specified using a library of predefined functions written in C language. The code used for the transition diagram in the simulation has been included in Appendix 9.

8.4.1.2 Access Point (AP)

In the WLAN system, AP was used to transmit the received vital signs from DASs to the control unit. An AP has two network interfaces, one wireless LAN interface (IEEE 802.11g) and a standard Ethernet interface which connects it to an

Ethernet switch. Thus it implements two MAC protocols, the Ethernet MAC and the wireless LAN MAC. Figure 8.27 shows the model of an AP.

Wireless LAN	
Wireless LAN MAC Address	Auto Assigned
Wireless LAN Parameters (...)	
BSS Identifier	1
Access Point Functionality	Enabled
Physical Characteristics	Extended Rate PHY (802.11g)
Data Rate (bps)	54 Mbps
Channel Settings	
Transmit Power (W)	0.100
Packet Reception-Power Threshold...	-65
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	1024000
Roaming Capability	Disabled
Large Packet Processing	Drop
PCF Parameters	Disabled
HCF Parameters	Not Supported

Figure 8.27 - Access Point configuration parameters

AP's MAC and PHY layers attributes were configured in the same way as the DASs. The only difference is the enabled access point functionality (shown in Figure 8.27). So it can periodically send beacon frames to announce its presence, maintain an array which stores the address of all the DASs and keeps DASs synchronized with the network.

APs have the capacity to buffer data for instances when transmission media are not free. If the traffic load through the AP exceeds its buffer capacity, the queue can increase. When the buffer reaches its saturation threshold, the carried load

will remain bounded to the maximum throughput value (Bing 2008). In that case the AP will start dropping new-coming packets causing data loss. Default value 102400 bits was used to set the buffer size. So an AP can buffer $102400 / (8 \times 1500) = 83$ packet at a time. In the simulation, the performance of the WLAN system was studied using different number of APs.

8.4.1.3 Central Control Unit

The central control unit was discussed in Chapter 6. An OPNET server model is used in the simulation to represent the control unit. It is the destination for transmission of all the DASs via the AP. In addition it supported other applications running over TCP/IP and UDP/IP. The model can support transmission speed of 10 Mbps, 100 Mbps or 1 Gbps. The transmission speed is determined by the link used between the model and other network components. The node model of the server deployed in this study is shown in Figure 8.28.

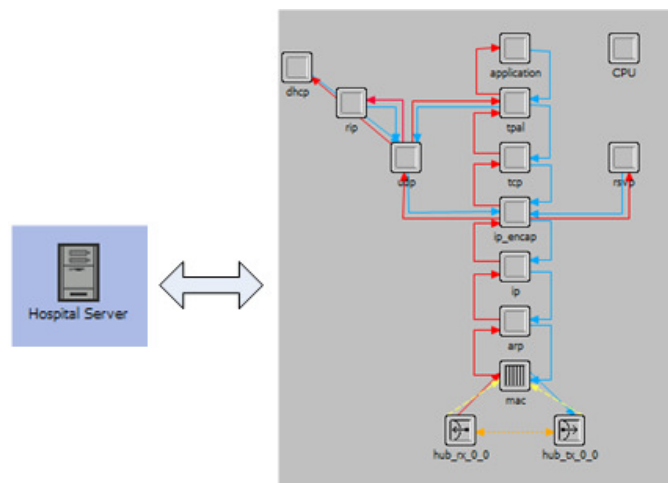


Figure 8.28 - Server model used to simulate the central control unit

The address of the control unit had to be specified. This address was used by the DASs for the destination to send patients' vital signs. Some of the attributes used to configure the control unit is shown in Figure 8.29.

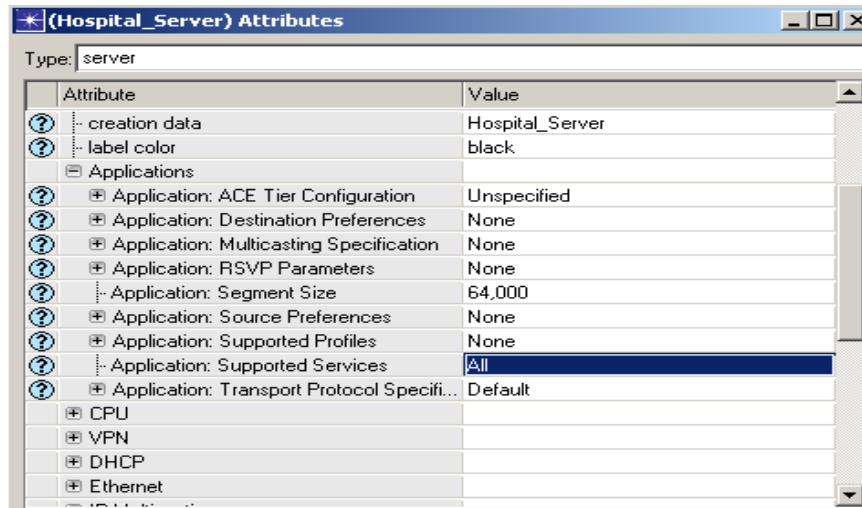


Figure 8.29 - Application attributes of server

8.4.1.4 Switches and Links between AP and Control Unit

Four Ethernet switches were used in modeling and simulation of the WLAN system in a hospital. They also contribute to the transmission delay. These switch models had to be specifically modified using the device creator. Interfaces have been created based on the needs of simulation. Figure 8.30 illustrates a switch model used in simulation. It includes a fiber optic interface and four Ethernet interfaces.

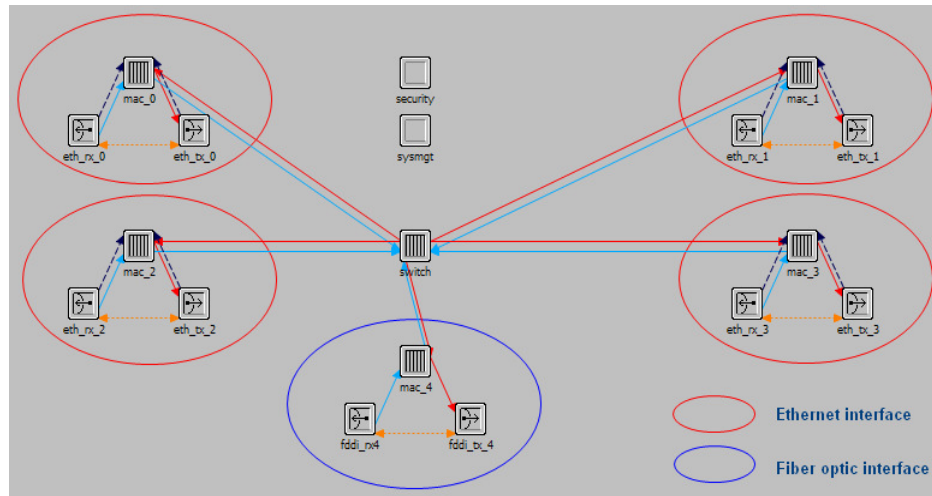


Figure 8.30 - Switch Model

100BaseT duplex Ethernet connection link was used to connect a switch with an AP and a control unit. This type of link can operate at 100 Mbps. Fiber optic cables (FDDI) supporting 100 Mbps data rate was used to link switches. The “delay” attribute of the links was “distance based”. This setting enabled the propagation delay within the cable, which will be determined based on the distance between the two nodes.

8.4.2 Model of Hospital Network

Using the components introduced above, simulations were carried out to investigate network and performance when using TCP and UDP respectively. Figure 8.31 illustrates the scenario. 100 DASs and an AP formed an infrastructure BSS. Vital signs sent from DASs to the control unit were through the AP.

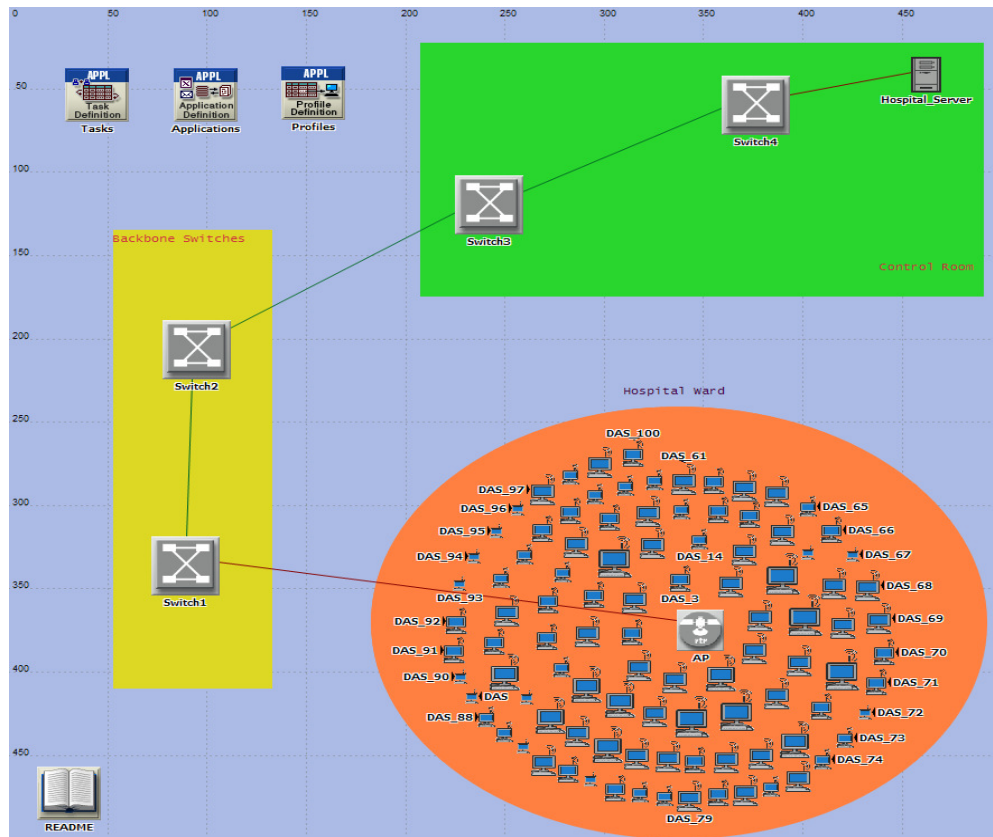


Figure 8.31 - Modelled Hospital Network for simulation

8.4.3 Simulation results

Figure 8.32 illustrates data generated and transmitted by a DAS. It can be observed that the size of generated packets remains stable at 1500 bytes throughout the simulation duration. Data traffic generated by a DAS for transmission is at a data rate of 1500 bytes/sec (or $1500 \times 8 \text{ bits} = 12,000\text{bps}$ or about 12Kbps) regardless of the protocol used (shown in the bottom of Figure 8.32).

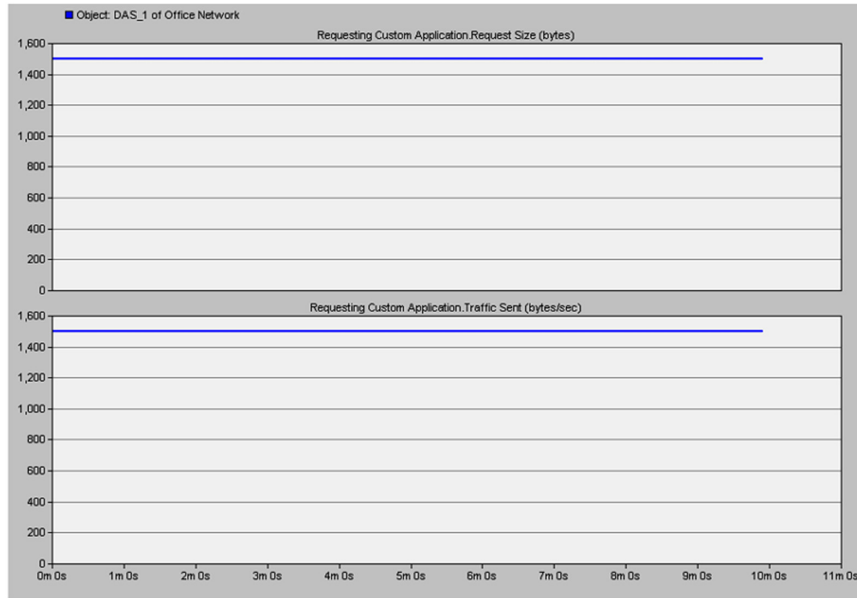


Figure 8.32 - Generated packet size and DAS application traffic sent

Therefore, the overall traffic generated by all the 100 DASs, as expected, should be 150,000 bytes/sec (1500 bytes \times 100). In another words, the transmission data rate should be:

$$150,000 \text{ bytes} \times 8 \text{ bits / seconds} = 1,200,000 \text{ bps} \approx 1.2 \text{ Mbps} \quad (8.5)$$

Figure 8.33 shows the overall traffic sent by all the DASs throughout the simulation. The simulation was run twice using UDP and TCP protocols respectively. The graphs for UDP and TCP are combined in Figure 8.33 to compare performance. It should be pointed out that packets generated by the DASs could not be sent completely at the beginning of the simulation when using TCP, since the transmission data rate did not reach 150,000 bytes/sec. This is because TCP is a connection oriented protocol which requires both DASs and the

control unit to agree to participate. The handshaking procedure needs to be taken before establishing a connection between a DAS and the control unit for the transmission of vital signs. However, UDP does not require handshaking. So using UDP, DASs can send the generated packets at the data rate of 150,000 bytes/sec through the simulation.

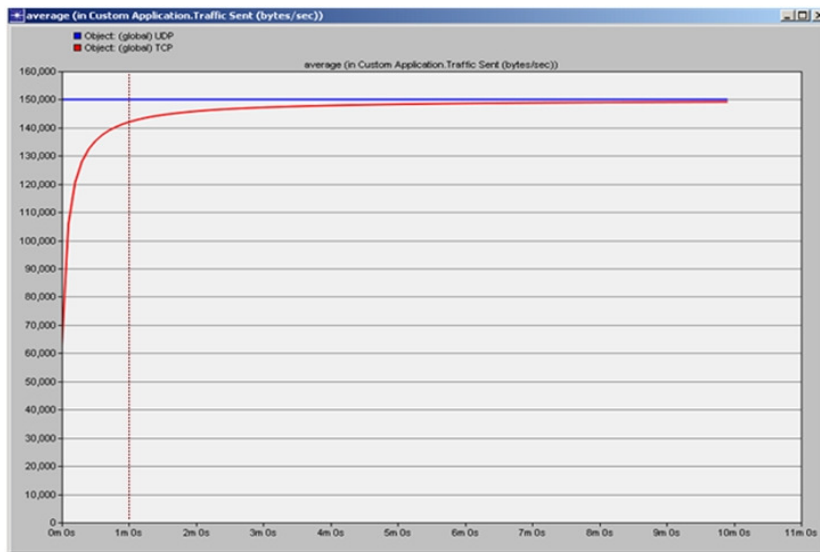


Figure 8.33 - Comparison of transmission data rate

It can be found from Figure 8.33 that a period was required for handshaking and establishing connection between all the DASs with the server for vital signs transmission when using TCP. Network performance was not considered during this period in the following discussion, since vital sign transmission can be scheduled after handshake process in practice of using a WLAN system. In this thesis one minute is considered for this handshaking period.

Figure 8.34 shows the comparison of overall throughput of TCP and UDP on the wireless LAN. It can be observed that UDP's throughput is stabilised at 1.2 Mbps, which is close to the value calculated in equation 8.5. An additional overhead of 20 Kbps is added to the vital signs because the UDP datagram contains a 16 bit header and 12 bytes checksum. In comparison, the average throughput is much higher (1.5 Mbps) than the generated data volume (1.2 Mbps) when TCP is used. This is due to the communication of acknowledgment (ACK) messages between the AP and the DASs. Therefore an extra 351 Kbps bandwidth is reserved when TCP is used in transmission of vital signs. In addition the exponential growth of TCP throughput follows the same pattern as the overall TCP application traffic sent by the DASs. So it can be noted that the used protocols for transmission can cause a major difference in the overall throughput and the bandwidth utilized in the WLAN system.

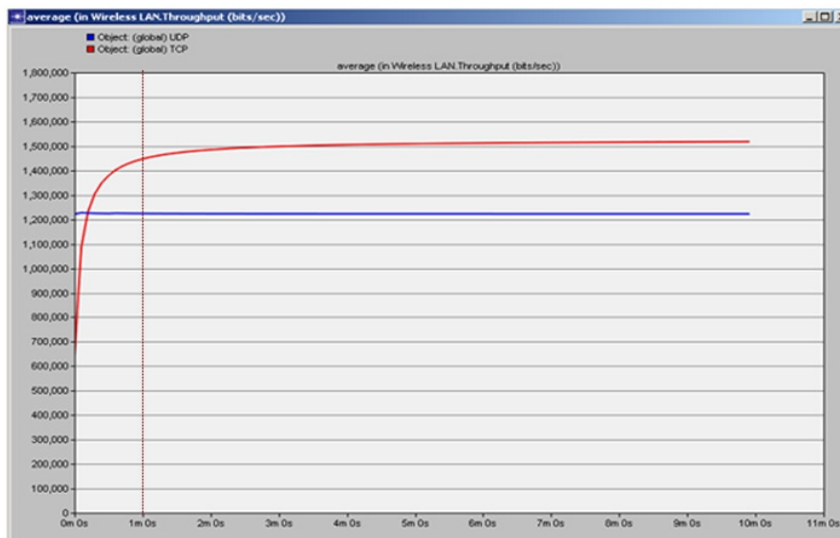


Figure 8.34 - Total throughput of the modelled WLAN

The graphs in Figure 8.35 show the average retransmission rate. UDP does not support retransmission of unsuccessful delivery, so the retransmission rate reported for UDP is zero. Whilst decreasing from 0.30, retransmission rate of TCP stabilized at 0.02, which means two out of 100 packets sent by the DASs will be retransmitted after the handshaking-period. This retransmission rate is acceptable, since 98% packets can be transferred once.

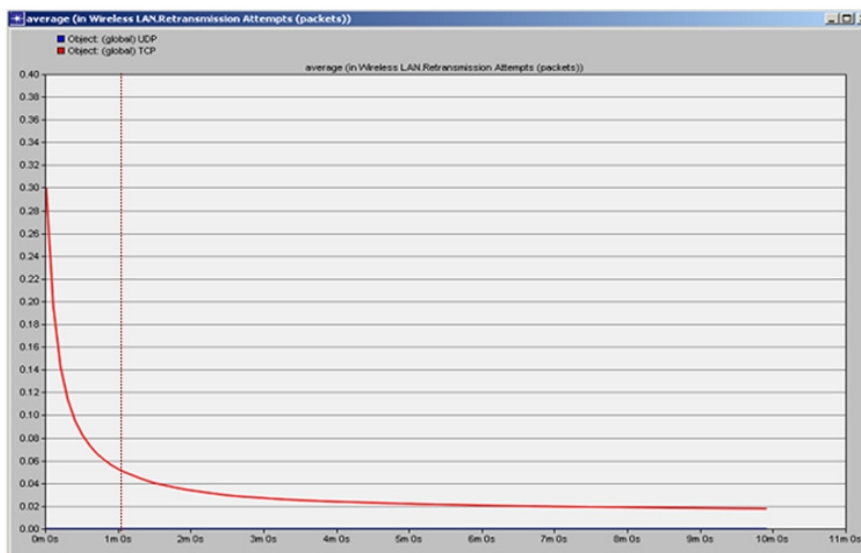


Figure 8.35 - Average WLAN retransmission attempts

Figure 8.36 shows the comparison of end-to-end delay of TCP and UDP transmission on the WLAN-based system. This feature calculated from the creation of a packet till the packet is received by the control unit. It can be observed that the delay of TCP is higher than delay of UDP. The difference between them is 30 μ s.

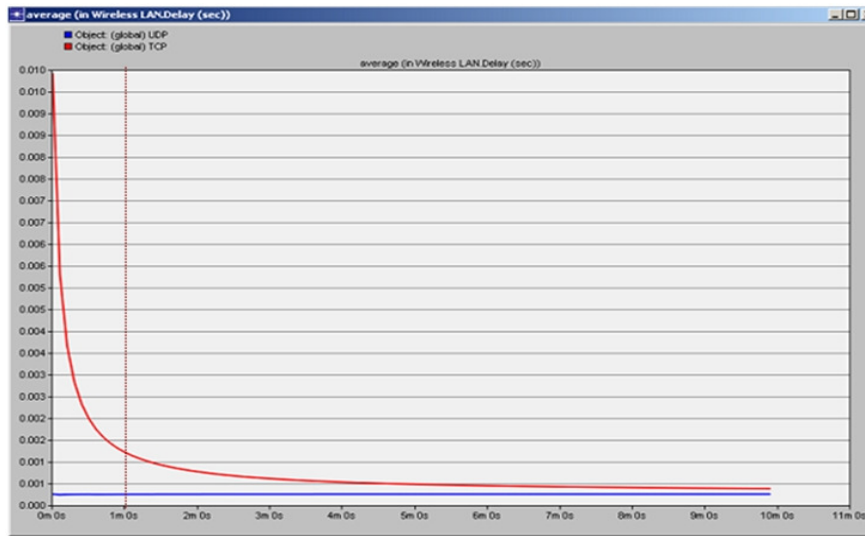


Figure 8.36 - Global average end-to-end delay

The rapid decrease of TCP delay at the beginning of transmission is caused by retransmissions during the period spent for establishing connection between AP and DAs, as collision is severer in that period when using TCP transmission. It should be noted that the retransmission includes ACK messages, RTS/CTS, vital signs and so on. Figure 8.35 only showed the retransmission of vital sign packets, Figure 8.37 shows overall retransmission on the WLAN using TCP. It can be seen that retransmission of ACK, RTS/CTS frames, etc. were the majority part in overall retransmissions. Therefore the settling-down period for handshaking is necessary at the start of communication session using TCP.

Due to using a single AP, the traffic load at the AP was heavy particularly at the beginning of the TCP transmission. Figure 8.38 shows the collision status of the AP, which is mostly due to retransmission. It should be noted that the simulated

scenario may be the worst case. In practice, application of more APs can reduce the traffic and mitigate collisions.

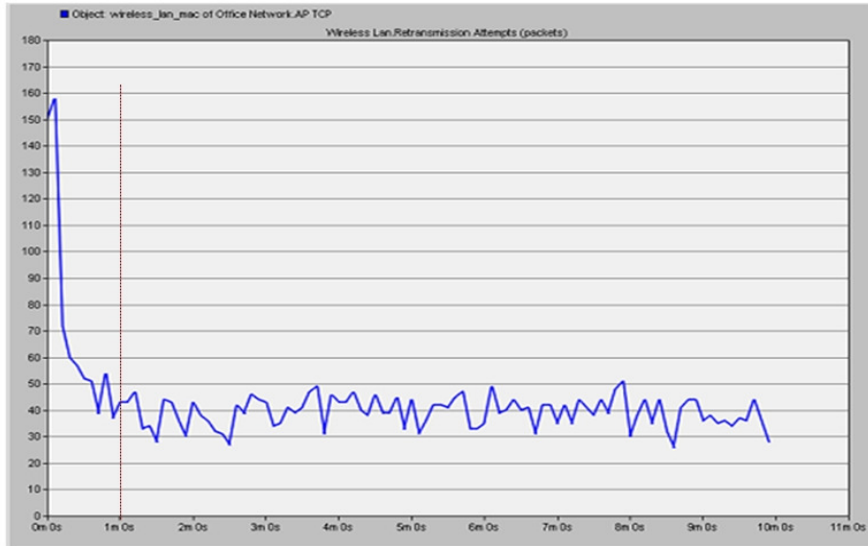


Figure 8.37 - Overall retransmissions on the modelled WLAN system

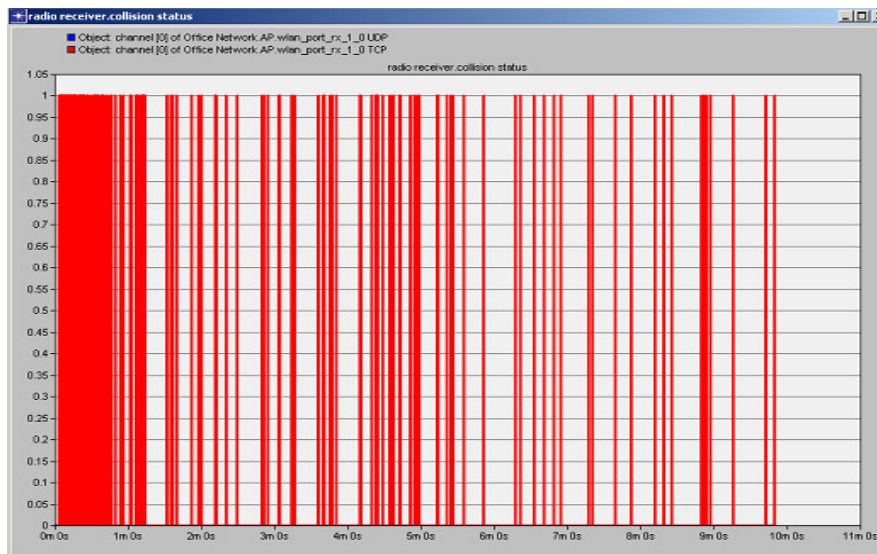


Figure 8.38 - Collision status on the WLAN when TCP is used

Although retransmissions caused by collision in using TCP, there is no consistent fail of retransmissions, which results in packets dropped. Figure 8.39 illustrated the number of packets sent by all DASs and the number of packets received by the control unit, which can be seen that the volume of transmission equal to the volume of reception for both TCP and UDP transmission.

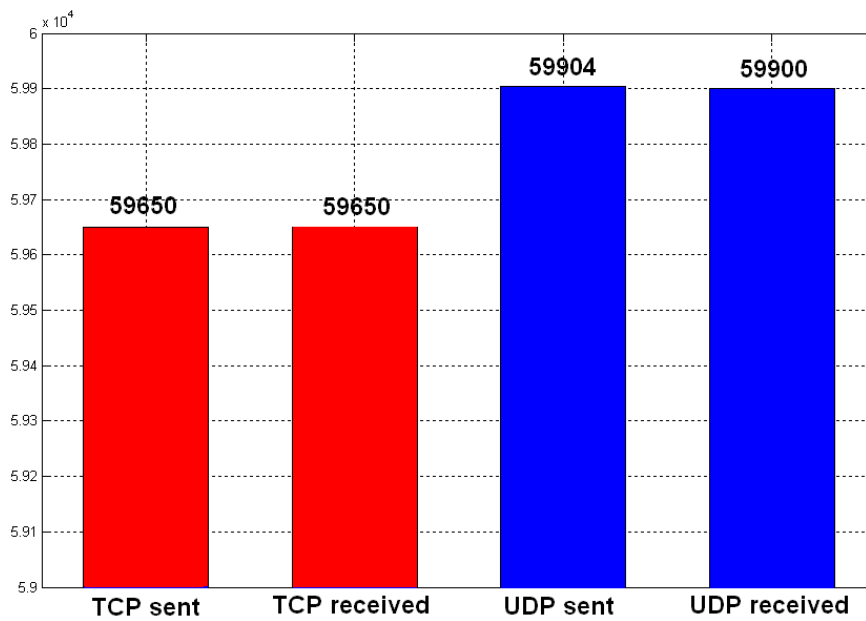


Figure 8.39 -The number of packets sent by all DASs and the number of packets received by the control unit

Due to the throughput (1.5 Mbps for TCP, 1.2Mbps for UDP shown in Figure 8.34) generated by all the DASs being far less than the available bandwidth (54 Mbps), transmission of patients' vital signs from DASs to control unit does not experience packets loss regardless of using either TCP or UDP. To further

investigate the performance of WLAN when using TCP and UDP, additional heavy traffic was generated to saturate the WLAN.

A Wi-Fi enabled device (Doctor_1) was placed close to the AP in the wireless network. The extra payload was added by implementing a client-server application between this device and another server (Hospital_Server_0) which was placed in the control room connected to the wired backbone of the hospital network. Figure 8.40 illustrates the changed scenario for simulation.

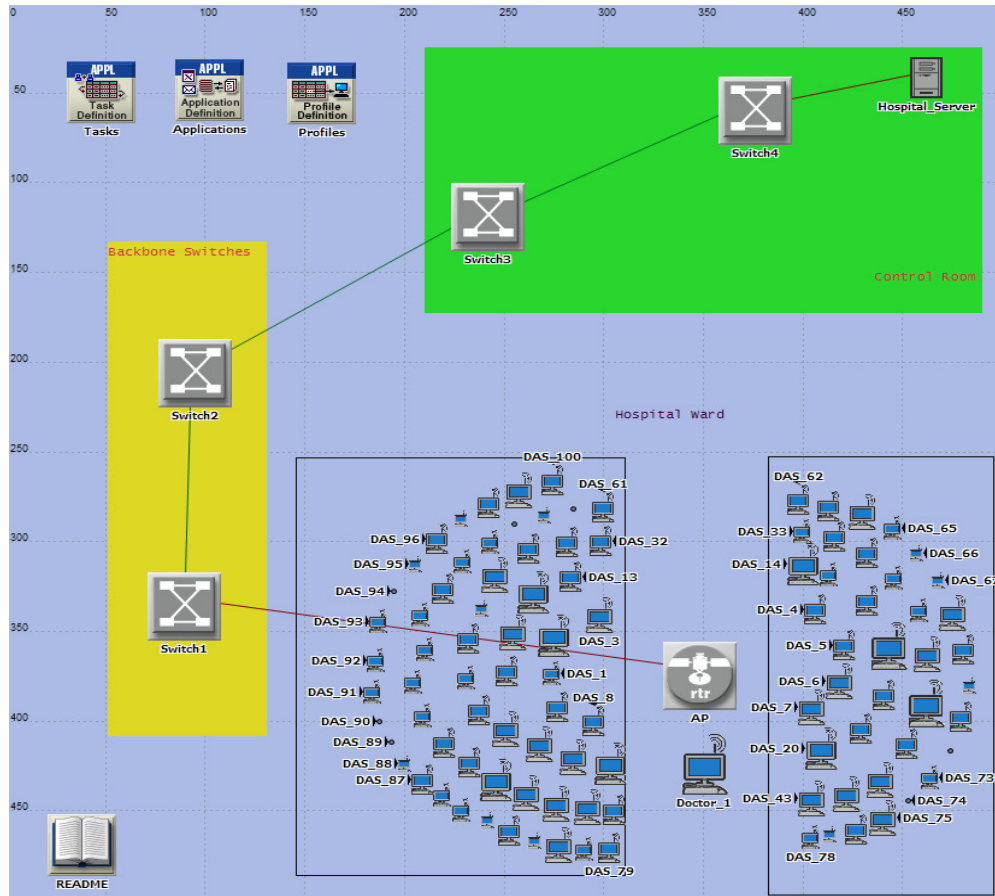
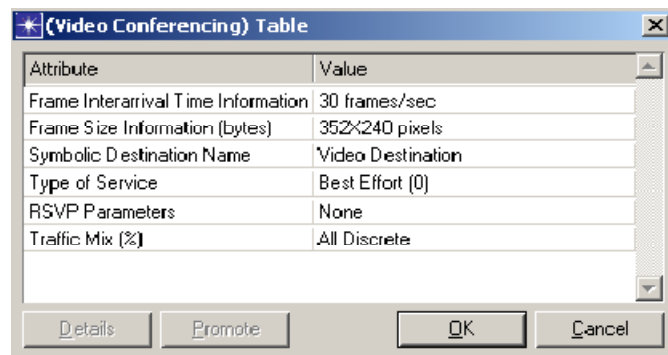


Figure 8.40 - Modified simulation scenario

Doctor_1 has been configured to transmit continuous video stream through the AP to Hospital_Server_0 using the same channel (channel 1) used by the AP and DASs. The configured parameters of video application are shown in Figure 8.41. It is worth mentioning that the modified scenario may be extreme in practice. It was just used to explore the capacity of a WLAN system.



Attribute	Value
Frame Interarrival Time Information	30 frames/sec
Frame Size Information (bytes)	352x240 pixels
Symbolic Destination Name	Video Destination
Type of Service	Best Effort (0)
RSVP Parameters	None
Traffic Mix (%)	All Discrete

Figure 8.41 - Video conference parameters

Figure 8.42 shows the overall traffic sent by all the DASs and Doctor_1 to the AP (WLAN throughput) and those sent by the AP to the server. As can be clearly seen, UDP provided higher and relatively stable throughput at 30.5 Mbps, whereas TCP's throughput was at 20.7 Mbps. These simulation results clarify the theoretical bandwidth provided by IEEE 802.11g. Appendix 10 shows a process for deducing the theoretical bandwidth of IEEE 802.11g when using TCP or UDP protocol.

It can be seen from the graph that the traffic volume sent by the AP to the server is far less than it received from DASs and Doctor_1. It means the AP could not process the total traffic received, it may have reached its processing saturation and

started to drop data packets. This was obviously occurred while the transmission of Doctor_1 started. After Doctor_1 stopped, data transmission between the AP and WLAN returned to a stable state.

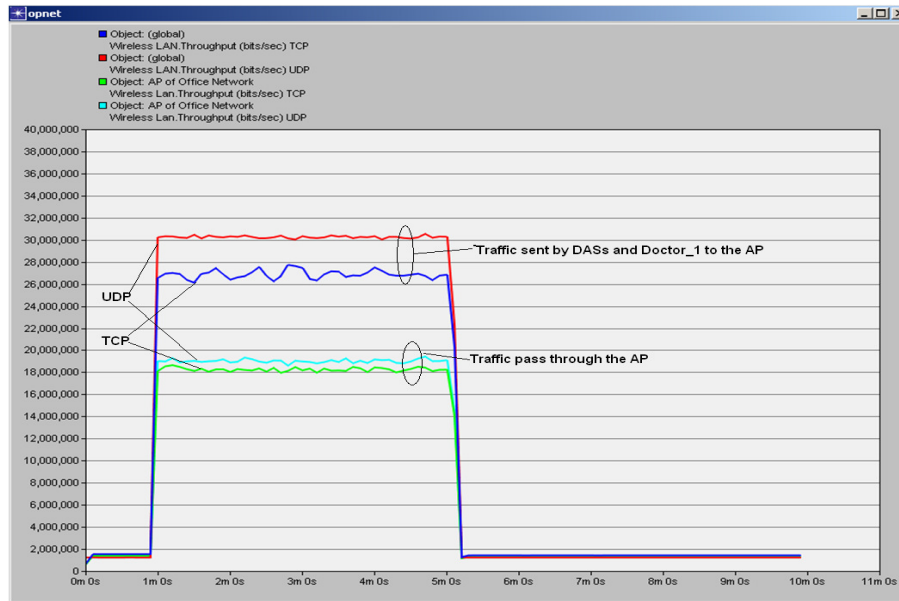


Figure 8.42 - WLAN and AP Throughput

Figure 8.43 shows the vital signs received by the server in the control unit. It can be seen when using UDP in transmission; the effect from Doctor_1 is severe. Data loss is obvious. On the country, vital sign transmission did not suffer huge data loss when using TCP. Because of the acknowledgement scheme used by TCP protocol, vital data got more reliable transmission. Therefore, it may be suitable for reliable transmission of vital signs in RPM. However, further study of application of Wi-Fi is required when the emerging 802.11n based network are widely deployed.

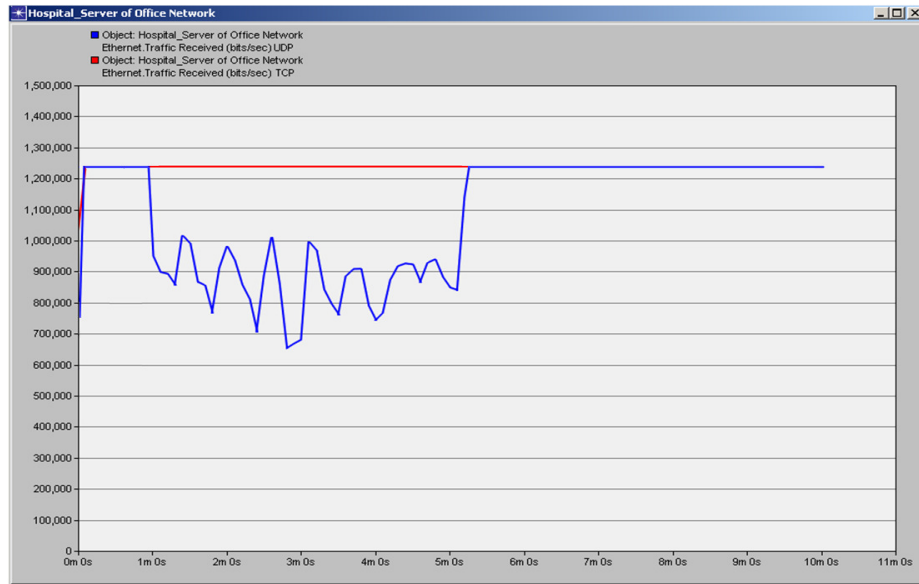


Figure 8.43 - Data volume received by the central control unit

8.5 Summary

In this chapter, the proposed RPM on general hospital wards was studied in a simulation environment using network simulation tool OPNET. The main aim of the simulation was to evaluate the feasibility of using wireless technologies in RPM on general hospital wards. Two alternative approaches of using ZigBee-based sensor networks were evaluated. The proposed multiple-WPAN approach showed better performance than the single-master-node approach. Channel overlaps between WPANs were investigated. In addition, the use of a wireless LAN based data transmission system was discussed and simulated.

CHAPTER NINE

9 Conclusion and Future Work

Patients on general wards are often monitored by healthcare personnel according to the severity of their conditions; however this is often based upon the nurses' judgment which is subjective. In addition, patient monitoring is a labour-intensive task; insufficient medical and nursing staff in some hospitals may result in patients on general wards not receiving the expected care and attention.

Progression in patient monitoring on general wards in many hospitals has resulted in the introduction of paper-based Early Warning Score (EWS) systems to ensure timely and appropriate responses to be taken for treatment. Furthermore, in recent years, some hospitals have implemented PDA-based systems for semi-automated recording and transmission of vital signs. Although this is an improvement to the paper-based monitoring systems, they cannot provide real-time patient monitoring. In this system, visits by nurses are still essential for patient monitoring.

An automated RPM system by providing real-time monitoring could go some way towards improving patient care on general wards. Such a system gathers patients' vital signs and sends them to a control room for centralized monitoring. It can provide opportunity to improve the efficiency of patient monitoring and holistic care on general hospital wards.

Sensors are important components in any RPM system. Relevant sensors that can be used in RPM were evaluated. The focus was on wireless sensors with the capability of measuring vital signs. A wireless sensor can offer enhanced mobility and comfort to patients during hospitalization.

The capability and suitability of two wireless network technologies, Bluetooth and ZigBee were examined. Due to low-power consumption and security features, ZigBee-based wireless sensor networks were adopted. Two alternative approaches of using ZigBee-based sensor networks were discussed. They differed from the network topology deployed as well as the use of master nodes that control the communication progress within the network.

A WPAN, referred to as Data Acquisition System (DAS) was considered for each patient. The WPAN includes a master node and five sensors. This approach can reduce traffic load on the limited bandwidth available in a ZigBee-based WPAN to improve transmission reliability.

In the proposed RPM, a DAS transmits vital signs through an Ethernet LAN to a central control unit. At the control unit, patients' vital signs will be recorded as well as being monitored in real-time for abnormalities. In addition, doctors can also access patients' vital signs through the Internet.

To demonstrate the functionalities of the proposed RPM, a prototype system was developed and evaluated. A number of experiments using the prototype were conducted. The focus of the experiments was on the transmission range,

interference issues caused by Wi-Fi. The experiment results verified the feasibility of using ZigBee-based sensor networks for Data Acquisition in RPM.

In addition, the proposed system was further investigated in a simulation environment using a network simulation tool, OPNET Modeler. Simulation results showed that the performance of proposed multiple-WPAN approach can out-perform the single-master-node approach for RPM on general wards.

However the multiple-WPAN approach can encounter the channel overlaps problems due to limited channels supported by ZigBee. WPANs sharing the same channel have to share bandwidth, which can cause performance degradation. This problem was investigated in a simulation environment where 30 patients were monitored. It was found that appropriate adoption of transmission interval for transmission of vital signs from sensors to their master node can rectify any possible bandwidth limitations.

The capacity and capability of a wireless Ethernet LAN for transmission of vital signs was investigated. 100 DASs were used to generate a heavy traffic load through the LAN. Both TCP and UDP protocols were used to evaluate performance. The results showed the wireless LAN could cope with such traffic.

Contribution to knowledge

- 1) Remote patient monitoring can play a key role in improving healthcare. It has already been used in homecare, emergency medical assistance, etc. This research expanded its application to general hospital wards. Although RPM

systems cannot replace the role of nurses, it will free their time to provide enhanced personal care to patients and focus upon their holistic needs. Therefore the proposed RPM can significantly improve patient monitoring and holistic care on general hospital wards.

- 2) This research investigated the technical feasibility of using ZigBee technology in the context of remote patient monitoring. The application of ZigBee in patient monitoring had been proposed in former research, where single-master-node approach was introduced. This project evaluated the single-master-node approach and highlighted its limitations for supporting RPM on general wards. Moreover, an alternative approach by using the multiple-WPAN was proposed in this research. The thesis has illustrated that the proposed approach is more practically appropriate for RPM on general hospital wards compared to previous approach.
- 3) In addition, this research identified shortfalls of ZigBee and Wi-Fi technologies for RPM applications. A partial solution has been offered to implement these technologies in RPM.

Limitation of the research

- 1) This research has investigated the technical feasibility in developing a wireless RPM system for general hospital wards. Due to ethic concerns, the investigation was restricted to a simulated environment. However, it is crucial to validate the designed prototype system on general hospital wards before its

deployment. Therefore, further investigation is required, which should include tests of ZigBee-based sensors and a master node integrated with the Wi-Fi system in hospital environment.

- 2) The impact of physical environment (shapes of wards, size, obstacles, etc) on the proposed RPM system should be further studied.
- 3) The detection of abnormality in vital signs is a fundamental task of the proposed RPM system. This process is implemented based on a basic algorithm, using safe-ranges of vital signs. Further development is required with more consultation from medical personnel.
- 4) Security is an important issue when using wireless RPM. Although some methods have been proposed for protecting the security of vital sign transmission, these methods have not been fully tested in the designed prototype system.

Area for Future Research

The objectives of this thesis, as expressed in Chapter 1, have been achieved.

However, there are some areas which could benefit from future works. They are:

- To test practical ZigBee-based biomedical sensors for data acquisition.
- The integration between Wi-Fi and ZigBee require further investigation.

- The emergence of IEEE802.11n standard for Wi-Fi has resolved the problem of channel frequency overlapping. However, this requires further investigation through practical testing.
- The software designed for the central control unit needs improvement to support access through the internet and World Wide Web.
- The algorithm used to detect abnormalities of vital signs should be further developed.
- The three-colour-state need to be validated.
- The integration between patient ID and the RPM system should be further developed. In addition, the issue of secure transmission of patient's data as well as patient's identification would require further research.

References

Adler, S., 2004. Enabling Wireless Applications the Way Forward, *3Com Solutions for Healthcare*. Available from: http://www.3com.com/solutions/en_US/casestudy.jsp?caseid=152101 [Accessed 14 September 2008]

Al-Qahtani, S. and Al-Dorzi, M. H., 2010. Rapid Response Systems in Acute Hospital Care, *Annals of Thoracic Medicine*, 5(1), 1-4. Available from: <http://www.thoracicmedicine.org/article.asp?issn=1817-1737;year=2010;volume=5;issue=1;spage=1;epage=4;aualast=Al-Qahtani> [Accessed 4 June 2010]

Anderson, K., 2004. *Proactive Health*, Intel: USA. Available from: <http://www.intel.com/research/prohealth/> [Accessed March 6 2008]

Anliker, U., Ward, J. A., Lukowicz, P., Troster, G., Dolveck, F., Baer, M., Keita, F., Schenker, E.B., Catarsi, F., Coluccini, L., Belardinelli, A., Shklarski, D., Menachem, A., Hirt, E., Schmid, R. & Vuskovic, M., 2004. Amon: A Wearable Multiparameter Medical Monitoring and Alert System. *Information Technology in Biomedicine*, 8(4), 415–427.

Anand, R. S., 2005. PC-Based Monitoring of Human Heart Sounds, *Computers and Electrical Engineering* 31(2), 166–173

Akhgar, B., Rahman, F., Jopek, L., Siddiqi, J. I., Atkinson, S., Savoldelli, A., DorisPrato, Montrucchio, S., Guella, F., James, B., Pinkerton, M. and Vilmos, A., 2009, Creating a LOC Based Portable Health-care Platform - Using a Universal Mobile NFC Host Environment, *Healthinf*, 38-42.

Akay, M., Akay, Y. M. and Welkowitz, W., 1994. Automated Noninvasive Detection of Coronary Artery Disease Using Wavelet-based Neural Networks, *Intelligent Engineering System Artificial Neural Network*, 14, 517-522.

Auricchio, A., 2003. Device-based Therapy and Remote Patient Management in Heart Failure, Available from: www.touchbriefings.com/pdf/33/gso31_t_biotronik.pdf [Accessed April 29 2008]

Baisa, N., 2005, Designing Wireless Interfaces for Patient Monitoring Equipment, *RF Design Magazine*, April, 1-5.

Banitsas, K. A., Istepanian, R. S. H., Tachakra, S. & Owens, T J, 2001. Modeling Issues of Wireless LANs for Accident and Emergency Departments, In: *the 23rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, October 2001 Istanbul. 3540-3543.

Barlow, J., Bayer, S., Castleton, B. & Curry, R., 2005. Meeting Government Objectives for Telecare in Moving From Local Implementation to Mainstream Services, *Journal of Telemedicine and Telecare*, 11(1), 49-51.

Barrett, M. J., 2005. Patient Self-management tools: an overview, *California healthcare foundation*, USA, 1-25

Biodevice, 2009. Available from: <http://www.biodevices.pt/> [Accessed 19 July 2010].

Bloor, K. and Maynard. A., 2003. Planning Human Resources in Health Care: Towards an economic approach - An International Comparative Review. Available from: http://www.fcrrs.ca/final_research/commissioned_research/programs/pdf/bloor_report.pdf [Accessed 6 April 2008]

Bluetooth SIG, Bluetooth specifications 1.0, 1.1, 1.2 and 2.0+EDR. Bluetooth SIG, technical specifications, 1999-2004. Available from <https://www.bluetooth.org> [Accessed 15 Many 2009]

Boyd, O. and Jackson, N., 2005. Clinical Review: How is risk defined in high-risk surgical patient management?, *Critical Care*, 9(4), 390-396.

Boyle, J., Bidargaddi, N., Sarela, A. & Karunanithi, M., 2008. Ambulatory Care Delivery for Chronic Disease Management, *In: Hierlemann A., ed. 6th IASTED International Conference, 12-16 February 2008, Innsbruck*. Zurich: ACTA Press, 384-389

Brady, S., Dunne, L. E., Tynan, R., Diamond, D., Smyth B. & O'Hare, G.M.P., 2005, Garment-based Monitoring of Respiration Rate Using a Foam Pressure

Sensor, In: *9th International Symposium on Wearable Computers, 18-21 October 2005* Osaka, JAPAN, Available from: ieeexplore.ieee.org/iel5/10396/33046/01550817.pdf [Accessed 11 July 2007]

Brady, S., Carson, B., O’Gorman, D., Moyan, N. & Diamond, D., 2007, Body Sensor Network Based on Soft Polymer Sensors and Wireless Communications, *Journal of Communications*, 2(5), 1-6.

Bratan, T. and Clarke, M., 2005. Towards the Design of a Generic System Architecture for Remote Patient Monitoring, In: *the 27th Annual EMBS International Conference, 1-4 September 2005, Shanghai, China*. IEEE, Available from: ieeexplore.ieee.org/iel5/10755/33900/01616353.pdf [Accessed 19 May 2007]

Bratan, T. and Clarke, M., 2006. Optimum Design of Remote Patient Monitoring Systems, In: *the 28th Annual EMBS International Conference, 30 August-3 September 2006, New York City, USA*. IEEE, Available from: ieeexplore.ieee.org/iel5/4028925/4030573/04398942.pdf [Accessed 21 May 2007]

Broens, T., Halteren, A. V., Sinderen, M. V. and Wac, K., 2007. Towards an Application Framework for Context-aware M-health Applications, *International Journal of Internet Protocol Technology*, 2(2), 109-116.

Bronzino, J. D., 2000. *The Biomedical Engineering Handbook*. 2nd ed. Boca Raton, FL: CRC.

Budinger, T. F., 2003. Biomonitoring with Wireless Communications, *Annual Review of Biomedical Engineering*, 5, 383-412.

Bulgrin, J. R., Rubal, B. J., Thompson, C. R. & Moody, J. M., 1993. Comparison of short-time Fourier, wavelet and time-domain analyses of intra-cardiac sounds. *Biomedical Sciences Instrumentation*, 29, 465–472.

Casino, 2010. Heart rate monitor, Available from: <http://www.casio-intl.com/wat/PHYS/heart/chr-100.html> [Accessed 16 May 2010]

Chigan, C. and Oberoi, V., 2006. Providing QoS in Ubiquitous Telemedicine Networks. In: the 4th Ann. *IEEE Conf. on Pervasive Computing and Communications Workshops*, 13–17 March 2006 Piza, Italy.

Clarke, M., Jones, R. W., Bratan, T., Larkworthy, A., 2004. Providing Remote Patient Monitoring Services in Residential Care Homes. *Current Perspective on Healthcare Computing*, 114-122.

Claveirole, T., Dias, D., Amorim, M., Abdalla, M. and Viniotis, Y., 2008. Securing Wireless Sensor Networks Against Aggregator Compromises. *IEEE Communication Magazine*, 46, 134–41.

Coleman, D. D. and Westcott, D. A., 2006. *CWNA: Certified Wireless Network Administrator Study Guide (Exam PW0-100)*. Indianapolis, Indiana: Wiley Publishing, Inc.

Commission for healthcare audit and inspection, 2008. *Are We Choosing Health?- The Impact of Policy on the Delivery of Health Improvement Program and Services*, London, UK, Concordat gateway number 137.

Commission for healthcare audit and inspection, 2009. *Care Quality Commission NHS Inpatient Survey 2009*, London: Commission for Healthcare Audit and Inspection. Available from: <http://www.nelm.nhs.uk/en/Categories/National-Health-Service/> [Accessed 15 June 2009]

Cooley, W. L. and Moser, K. M., 1973. A Simple Signal Processor for a Respiratory Rate Monitor, *IEEE Transactions on Biomedical Engineering*, 4, 309-310.

Cordeiro, C. M. and Agrawal, D. P., 2006. *AD Hoc Sensor Networks Theory and Applications*. Singapore: World Scientific.

Corman, R., 2000. Cedars-Sinai uses Pal0000m VIIs to Access Clinical Information: A New Item Reported, Available from: <http://www.handheldmed.com> [Accessed 12 May 2008]

Davidson, K. and Barber, V., 2004. Electronic Monitoring of Patient in General Wards. *Nursing Standard*, 18 (49), 42-46.

Deery, A., Chambers, D., Moriarty, D., Connolly, E. & Lyons, G., 2006. Clinical Trials of a Wireless LAN Based Patient Monitoring System, In: *the 19th IEEE Symposium on Computer-Based Medical Systems*, June 2006, Salt Lake City, UT, Available from: ieeexplore.ieee.org/iel5/10953/34552/01647616.pdf [Accessed 10 June 2007]

Denscombe, M., 2002. *Ground Rules for Good Research*, Maidenhead: Open University Press.

Department of Health and NHS Modernization Agency, 2003. *The National Outreach Report*, London.

Department of Health, 2008. *High Quality Care for All*, London.

Department of Health, 2008. *Framing the Nursing and Midwifery Contribution; Driving up the Quality of Care*, London.

Department of Health, 2008. *Confidence in Caring*, London.1-37.

Department of Commerce/N.I.S.T U.S., 2001. *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, Springfield, November 26, 2001. Available from <http://csrc.nist.gov/>.

Drazen, E., Wechsler, A., Wiig, K. & Little, A. D., 1975. Requirements for Computerized Patient Monitoring Systems, *Computer*, 8(1), 22-27.

Dunne, L. E., Tynan, R., O'Hare, G.M.P., Smyth, B., Brady, S. & Diamond, D., 2005. Coarse Sensing of Upper Arm Positions Using Body-garment Interactions, In: the 2nd *International Forum on Applied Wearable Computing (IFAWC 05)*, 17-18 March 2005 Zurich, Switzerland.

Espina, J., Falck, T., Muehlsteff, J., Jin, Y., Adan, M. A. and Aubert, X., 2008. Wearable Body Sensor Network towards Continuous Cuff-less Blood Pressure Monitoring In: *Int. Workshop on Wearable and Implantable Body Sensor Networks (BSN 2008) 1-3 June 2008 Hong Kong*, 28-32.

Fass, L., 2007. Patient Centric Healthcare, *3rd IET Int. Conf. on Medical Electrical Devices & Technology*, 2-3 October 2007 London.

Farahani, S., 2008. *ZigBee Wireless Networks and Transceivers*, Oxford: Elsevier.

Gao, T., Greenspan, D., Welsh, M., Juang, R. R. & Alm, A., 2005. Vital Signs Monitoring and Patient Tracking over a Wireless Network, In: *the 27th IEEE Annual EMBS International Conference, 1-4 September 2005 Shanghai, China*. Available from: ieeexplore.ieee.org/iel5/10755/33900/01616900.pdf [Accessed 19 May 2007]

Gardner, M., Sage M. and Gray, P., 2001. Data Capture for Clinical Anaesthesia on a Pen-based PDA: Is It a Viable Alternative to Paper?, In: A. Blandford, J. Vanderdonckt, and P. Gray (Eds.) *People and Computers XV* (Berlin: Springer).

Gao, H., McDonnell, A., Harrison, D. A., Moore, T., Adam, S., Daly, K., Esmonde, L., Goldhill, D. R., Parry, G. J., Rashidian, A., Subbe, C. P. and Harvey, S., 2007. Systematic Review and Evaluation of Physiological Track and Trigger Warning Systems for Identifying at-risk Patients on the Ward. *Intensive Care Medicine*, 33(4), 667-679.

GE Healthcare, 2007. Investigation of the Spectrum Requirements for Advanced Medical Technologies, Private Communication.

Gehrmann, C., Persson, J. and Ben, S., 2004. *Bluetooth Security*, Norwood: Artech House.

Goldhill, D. R., Worthington, L., Mulcahy, A., Tarling, M. & Sumner, A., 1999. The patient-at-risk team: identifying and managing seriously ill ward patients. *Anesthesia*, 54, 853-860.

Golmie, N., 2006. *Coexistence in Wireless Networks, Challenges and System-Level Solutions in the Unlicensed Bands*. Cambridge: Cambridge University Press.

Golmie, N., Cypher., D. and Rebala, O., 2005. Performance Analysis of Low Rate Wireless Technologies for Medical Applications, *Computer Communications*, 28, 1266-1275.

Golmie, N., Rebala, O. and Chevrollier, N., 2003. Bluetooth Adaptive Frequency Hopping and Scheduling, In: *Military Communications Conference*, 13-16 Oct. 2003 Gaithersburg, USA.

Guo, T., Zhang, L., Liu, W. and Zhou, Z., 2006. A Novel Solution to Power Problems in Implanted Biosensor Networks. In: *the 28th Ann. Int. Conf. IEEE Engineering in Medicine and Biology Society*, 31 August-3 September 2006, New York, USA. 5952–5955.

Haahr R G, Duun S, Thompsen E V, Hoppe K and Branebjerg J 2008 A Wearable 'Electronic Patch' for Wireless Continuous Monitoring of Chronically Diseased Patients. In: *Int. Workshop on Wearable and Implantable Body Sensor Networks (BSN 2008)* 1–3 June 2008 Hong Kong, 66–70.

Haataja, K. M. .J., 2006. Security in Bluetooth, WLAN and IrDA: a comparison. Available from: <http://www.cs.uku.fi/research/publications/reports/A-2006-1.pdf> [Accessed 18 July 2010]

Hajjar, I. and Kotchen, T. A., 2003. Trends in Prevalence, Awareness, Treatment and Control of Hypertension in the United States, 1988-2000. *ACC Current Journal Review*, 12(5), 32.

Hanada, E., Hoshino, Y., Oyama, H., Watanabe, Y. and Nose, Y., 2002. Negligible Electromagnetic Interaction between Medical Electronic Equipment and 2.4 GHz Band Wireless LAN, *Medical Systems*, 26(4), 301–308.

Hande, A., Polk, T., Walker, William. & Bhatia, D., 2006. Self-powered Wireless Sensor Networks for Remote Patient Monitoring in Hospitals, *Sensors*, 6, 1102-1117.

Hakemi, A. and Bender, J., 2005. Understanding Pulse Oximetry, Advantages and Limitations, *Home Health Care Manag Pract*, 17(5), 416-418.

Heldt, T., Long, B., Verghese, G. C., Sszolovits, P. and Mark, R. G., 2006. Integrating Data, Models and Reasoning in Critical Care. In: *the 28th IEEE EMBS Annual International Conference, 30 August – 3 September 2006 New York, USA*. 350-353.

Hodgdon, C., 2004. Adaptive Frequency Hopping for Reduced Interference between Bluetooth and Wireless LAN, Available from: <http://www.design-reuse.com/articles/5715/adaptive-frequency-hopping-for-reduced-interference-between-bluetooth-and-wireless-lan.html> [Accessed 26 June 2010].

Hodgetts, T. J., Kenward, G., Vlachonikolis I. G., Payne, S. & Castle, N., 2002. The Identification of Risk factors for Cardiac Arrest and Formulation of Activation Criteria to Alert a Medical Emergency Team. *Resuscitation*, 54, 125-131.

Hogan, J., 2006. Why don't Nurses Monitor the Respiratory Rates of Patients. *British Journal of nursing*, 15(9), 489-492.

Hong, J. H., Kim, J. M., Cham, E. J. and Lee, T. S., 2007. A Wireless 3-channel ECG Transmission System Using PDA Phone. In: *2007 Int. Conf. on Convergence Information Technology 21-23 November 2007* Hyдай Hotel Gyeongui, Korea. 462–5.

Husemann, D., 2004. Remote Monitoring of Health Conditions. *ERCIM News*, 56(1), 56.

IEEE Standard. 802.11g. 802 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band. 2003.

IEEE Standard for Information Technology Part 802.15.4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs). 2003.

IEEE, Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs), IEEE Standard 802.15.1-2005 (Revision of IEEE Std 802.15.1-2002), 1–580.

IEEE 802.15.2 IEEE Recommended Practice for Information Technology Part15.2: Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Bands. 2003.

IEEE, Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs), IEEE Standard 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003), 1–305.

IEEE P802.11n™/D9.0, 2009, Draft STANDARD for Information technology - telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements.

IEEE 802.19 Coexistence Technical Advisory Group (TAG), 2008. Available from: www.ieee802.org/19/ [Accessed 4 March 2010].

InfoLogix, 2007. Cisco Wireless Enhances Florida Hospital Patient Care. Available from: <http://whitepapers.silicon.com/0,39024759,60178434p,00.htm> [Accessed 20 January 2008]

Jasemian, Y. and Nielsen, L. A., 2005. Design and implementation of a telemedicine system using Bluetooth protocol and GSM/GPRS network, for real time remote patient monitoring, *Technology and Health Care*, 13, 199-219.

Javed, F., Venkatachalam, P. A. & Hani, A. F. M., 2006. A signal processing module integrated expert system for diagnosing heart diseases, In: *Proceedings of the Second IASTED International Conference on Telehealth*, 3-5 July 2006 Banff, Canada. 6-11.

Johnston, W. S. and Mendelson, Y., 2004. Extracting breathing rate information from a wearable reflectance pulse oximeter sensor, *Proc of 16th Annual*

International Conference of the IEEE EMBS, 1-5 September 2004 San Francisco, CA, USA, 5388-5391.

Jung, J., Ha., K. and Lee, J., 2008. Wireless body area network in a ubiquitous healthcare system for physiological signal monitoring and health consulting, *International Journal of Signal Processing, Image Processing and Pattern Recognition*, 1(1), 47-54. Available from: www.sersc.org/journals/IJSIP/vol1_no1/papers/06.pdf [Accessed 14 June 2009].

Junnila, S., Defee, I., Zakrzewski, M., Vainio, A. M. and Vanhala, J., 2008. UUTE home network for wireless health monitoring, *In: the International Conference on Biocomputation, Bioinformatics, and Biomedical Technologies*, R. Casadio, *et al.* eds. July 2008 Bucharest. 125-130.

Kang, J., Yoo, T. and Kim, H., 2006. A wrist-worn integrated health monitoring instrument with a tele-reporting device for telemedicine and telecare, *IEEE Transaction on Instrument Measurement*, 55(5), 1655-1661.

Karlof, C., Sastry, N. and Wagner, D., 2004. TinySec: A link layer security architecture for wireless sensor networks, *In: the 2nd Conference on Embedded Networked Sensor Systems*, Baltimore, MD, USA.

Khan, J. Y., Yuce M. R. and Karami, F., 2008. Performance evaluation of a wireless body area sensor network for remote patient monitoring, *In: the 30th*

Annual International Conference of the IEEE on Engineering in Medicine and Biology Society, August 2008 Vancouver, USA. 1266-1269.

Kho, T. K., Besar, R., Tan, Y. S., Tee, K. H. and Ong, K. C., 2005. Bluetooth-enabled ECG monitoring system, *In: TENCON 2005 IEEE Region 10th conference*, 21-24 November 2005 Melbourne. 1-5.

Ko, J. G., Cho, Y. H. and Kim, H., 2006. Performance evaluation of IEEE 802.15.4 MAC with different Backoff ranges in wireless sensor networks, *In: IEEE International Conference on Communication Systems*, October 2006 Singapore. 1-5.

Kohatsu, N. D., 2004. Characteristics associated with physician discipline. *Arch of Int Med*, 164, 653-658.

Koplow, M., Chen, A., Steingart, D., Wright, P. K. and Evans, J. W., 2008. Thick Film Thermoelectric Energy Harvesting Systems for Biomedical Applications *In: Int. Workshop on Wearable and Implantable Body Sensor Networks (BSN 2008)*, 1-3 June 2008 Hong Kong, 322-325

Kumar, S., Kambhatla, K., Hu, F., Lifson, M. and Xiao, Y., 2008. Ubiquitous computing for remote cardiac patient monitoring: A Survey. *International Journal of Telemedicine and Applications*, 4, 1-19.

Kuraitis, V., 2007. Five lingering questions holding back remote patient monitoring (RPM) adoption. Available from: <http://e-caremanagement.com/five->

lingering-questions-holding-back-remote-patient-monitoring-rpm-adoption/

[Accessed 18 April 2008]

Lahtela, A., Hassinen, M. and Jylha, V. 2008. RFID and NFC in healthcare: Safety of hospitals medication care, *In: the second international conference on pervasive computing technologies for healthcare*, 30 January - 1 February 2008 Tampere, Finland. 241-244.

LaRocca, J., 2002. *802.11 Demystified*. USA: McGraw-Hill.

Legg, G., 2004. ZigBee: *Wireless Technology for Low-Power Sensor Networks*, EE Times. Available from: <http://www.eetimes.com/design/communications-design/4017853/ZigBee-Wireless-Technology-for-Low-Power-Sensor-Networks> [Accessed 28 May 2010].

LifeSync, 2010. LifeSync System, Available from: Available from: <http://www.eetimes.com/design/communications-design/4017853/ZigBee-Wireless-Technology-for-Low-Power-Sensor-Networks> [Accessed 28 May 2010].

Lin, Y. H., Jan, I. C., Ko, P.C.I., Chen, Y.Y., Wong, J.M. & Jan, G.J., 2004. A Wireless PDA-based Physiological Monitoring System for Patient Transport, *IEEE Transactions on Information Technology in Biomedicine*, 8(4), 439-447.

Liu, Y. and Sahandi, R., 2008. Review of Sensors for Remote Patient Monitoring, *In: the 6th IASTED International Conference on Biomedical Engineering*, 12-14 February 2008 Innsbruck, Austria.

Liu, Y. L. and Sahandi, R., 2009. ZigBee network for remote patient monitoring, *In: XXII International Symposium on Information, Communication and Automation Technologies*, 28-30 October 2009 Sarajevo, Bosnia and Herzegovina. 1-7.

Lorincz, K., Malan, D., Fulford-Jones T. R. F., Nawoj, A., Clavel, A., Shnayder, V., Mainland, G., Moulton, S. & Welsh, Matt., 2004. Sensor Networks for Emergency Response: Challenges and Opportunities, *IEEE Pervasive Computing*, 3(4), 16-23.

Lo, P. L. B. and Yang, G. Z., 2005. Key Technical Challenges and Current Implementations of Body Sensor Networks, *the 2nd International Workshop on Body Sensor Networks (BSN 2005)* Available from: http://vip.doc.ic.ac.uk/bsn/public/UbiMonPapers/Key_Technical_Challenges_and_Current_Implementations_of_Body_Sensor_Networks.pdf [Accessed 24 July 2010]

Lu, Y. C., Xiao, Y., Sears, A. and Jacko, J. A., 2005, A Review and a Framework of Handheld Computer Adoption in Healthcare. *International Journal of Medical Informatics*, 74, 409 - 422.

Maurer, U., Rowe, A., Smailagic, A. and Siewiorek, D. P., 2006. eWatch: a Wearable Sensor and Notification Platform, In: *International Workshop on Wearable and Implantable Body Sensor Networks (BSN 2006)* 3-5 April 2006 Cambridge, Massachusetts, USA.

Malkary, G., 2003. Healthcare Without Bounds - Trends in Mobile Computing, Spyglass Consulting Group.

Malan, D., FulfordJones, T., Welsh, M & Moulton, S., 2004, *CodeBlue: An Ad Hoc Sensor Network Infrastructure for Emergency Medical Care*. Available from: www.eecs.harvard.edu/~mdw/papers/codeblue-bsn04.pdf [Accessed 26 March 2008]

Meingast, M., Roosta, T. and Sastry, S., 2006, Security and Privacy Issues with Health Care Information Technology, *In: the 28th IEEE EMBS Annual International Conference, 30 August – 3 September 2006 New York, USA*. 5453 – 5458.

MobiHealth, 2008. Available from: <http://www.mobihealth.org/> [Accessed 17 July 2010]

Mobiitech, 2010. Win Human Record will Monitor Your Health, Available from: Available from: <http://www.mobihealth.org/> [Accessed 17 July 2010]

Mora, F. A., Passariello, G., Carrault, G. & Pichon, J. P., 1993, Intelligent Patient Monitoring and Management system: a review, *IEEE Eng Med Biol M*, 12(4), 23-33.

Mower, W., Sachs, C., Nicklin, E. & Baraff, L., 1997. Pulse Oximetry as a Fifth Pediatric Vital Sign, *Pediatrics*, 99 (5), 681–686.

National Institute for Health and Clinical Excellence, 2007. Acutely ill patients in hospital- Recognition of and response to acute illness in adults in hospital, *NICE clinical guideline 50*, London, UK.

Neff, T., 1988. Routine oximetry: A fifth vital sign?, *Chest*, 94 (2), 227.

Neil, McCullen., 2009. Traffic Load Monitoring and Overload Prevention within a Wireless Environment. Dissertation, (BSc). Bournemouth University.

Nigam, V. and Priemer, R., 2005. Accessing heart dynamics to estimate durations of heart sounds, *Physiological Measurement*, 26(6), 1005-1018.

Nonin, Innovative Wireless Pulse Oximetry. Available from: <http://www.nonin.com/OEMsolutions/4100> [Accessed 15 May 2010]

Body Area Network - A Key Infrastructure Element for Patient Centred Telemedicine.

Norgall, T., Schmidt, R. and Von Der Grün, T., 2004. Body Area Network: a Key Infrastructure Element for Patient-centered Telemedicine. In: Lymberis, A. and Derossi, D., ed. *Wearable eHealth systems for personalized health management-state of the art and future challenges*. IOS Press, 142-148.

O'Donoghue, N., Kulkarni, S. and Marzella, D., 2006. Design and Implementation of Framework for Monitoring Patients in Hospitals Using Wireless Sensors in Ad Hoc Configuration, *Paper presented at the 28th Annual*

EMBS International Conference, 30 August-3 September 2006, New York City, USA. IEEE, Available from: ieeexplore.ieee.org/iel5/4028925/4030573/04398938.pdf [Accessed 29 May 2007]

Oliver, N. and Flores-Mangas, F., 2006. HealthGear: a Real-time Wearable System for Monitoring and Analyzing Physiological Signals, In: *International Workshop on Wearable and Implantable Body Sensor Networks (BSN 2006)* 3-5 April 2006 Cambridge, Massachusetts, USA. 4.

OMNeT++ Community Site, 2010. Available from: <http://www.omnetpp.org/> [Accessed 29 May 2010]

Omron, 2010. Omron Home Healthcare, Available from: Available from: <http://www.omnetpp.org/> [Accessed 29 May 2010]

OPNET Technologies, Inc, 2010. Available from <http://www.opnet.com/> [Accessed 29 May 2010]

Paradiso, R., Loriga, G. and Taccini, N., 2005. A Wearable Healthcare System Based on Knitted Integrated Sensors. *IEEE Transactions on IT in Biomedicine*, 9(3), 337-344.

Parissopoulos, S. and Kotzabassaki, S., 2005. Critical Care Outreach and the Use of Early Warning Scoring Systems, *ICUS Nursing WEB Journal*, 21(1), 1-13.

Park, S. H., Park, J. H., Ryu, S. H., Jeong, T, Lee H. H. & Yim, C. H., 1998. Real-time Monitoring of Patients on Remote Sites, *In: 20th Annual International Conference of the IEEE*, 29 October - 1 November 1998 Hong Kong. 1321-1325.

Park, T. R. and Lee, M. J., 2008. Power Saving Algorithms for Wireless Sensor Networks on IEEE 802.15.4, *IEEE Communication Magazine*, 46 148–55.

Pattichis, C. S., Kyriacou, E., Voskarides, S., Pattichis, M. S., Istepanian, R. & Schizas, C. N., 2002. Wireless Telemedicine Systems: An Overview, *Antennas Propagation Magazine*, 44(2), 143–153.

Pettis, K. S., Savona, M. R. and Leibrandt, P. N. 1999. Evaluation of the Efficacy of Hand-held Computer Screens for Cardiologist Interpretations of 12-lead Electrocardiograms. *Am Heart J*. 138(4), 765-70.

Population Reference Bureau, 2007. *2007 World Population Data Sheet*. Washington, DC: Population Reference Bureau. Available from: <http://www.prb.org/publications/datasheets/2007/2007worldpopulationdatasheet.aspx> [Accessed 20 October 2009].

Prasad, A. R. and Prasad, N. R., 2005. *802.11 WLANs and IP networking: security, QoS, and mobility*. Artech House. Available from: http://library.books24x7.com/book/id_14801/viewer.asp?bookid=14801&chunkid=839234241 [Accessed 11 October 2009].

Prytherch, D., Smith, G. B & Schmidt, P., 2006, Calculating Early Warning Scores - a Classroom Comparison of Pen and Paper and Hand-held Computer Methods. *Resuscitation*, 70, 173-178.

Rathi, S., 2009. Bluetooth Protocol Architecture, Microware Architect. Microware Systems Corporation. Available from: http://www.dedicated-systems.com/Magazine/00q4/2000q4_p028.pdf [Accessed 1 May 2009]

Raspin, C., 2009. What Makes Hospital Ward Staffing Costs Vary?. Available from: <http://www.hsj.co.uk/> [Accessed 20 April 2009]

Roman R, Lopez J and Gritzalis S 2008 Situation Awareness Mechanisms for Wireless Sensor Networks. *IEEE Communication Magazine*, 46, 102–7.

Rosenthal, K., 2006. Enjoy “Smarter” Patient Monitoring. *Nursing Management*, 37 (5), 52.

Sahandi, R. and Liu, Y., Channel Overlap Problem in ZigBee Based Remote Patient Monitoring on General Hospital Wards. *IEEE CMC2010*, 12-14 April 2010 Shenzhen, China. 259-263.

Sahandi, R., Noroozi, S., Roushanbakhti, G., Heaslip, V. & Liu, Y., 2010. Wireless technology in the evolution of patient monitoring on general hospital wards. *Journal of Medical Engineering and Technology*, 34(1), 51-63.

Seagull, F.J. and Xiao, Y., 2000. *Patient Monitoring Technology: Friend or Foe?*, USA. Available from: <http://hfrp.umm.edu/alarms/6.%20HFES2000-sym-1.pdf> [Accessed 6 May 2008]

Severinghaus, J. W. and Naifeh, K. H., 1987. Accuracy of Response of Six Pulse Oximeters to Profound Hypoxia. *Anesthesiology*, 67, 551–58.

Seyedi, A. and Sikdar, B., 2008. Modeling and Analysis of Energy Harvesting Nodes in Body Sensor Networks. In: *Int. Workshop on Wearable and Implantable Body Sensor Networks (BSN 2008), 1–3 June 2008 Hong Kong*, 175–178.

Sikora, A. and Groza, V. F., 2005. Coexistence of IEEE 802.15.4 with Other Systems in the 2.4 GHz-ISM-Band. In: *IEEE Instrumentation and Measurement Technology Conference*, 17-19 May 2005 Ottawa, Canada. 1786-1791.

Simpson, D.C. and Greening J. R., 1965. Patient Monitoring, *Phys. Med. Biol.*, 10(1), 1-16.

Smith, G., Prytherch, D. R., Schmidt, P., Featherstone, P., Knight, D., Clements, G. & Mohammed, M., 2006. Hospital-wide Physiological Surveillance –A New Approach to the Early Identification and Management of the Sick Patient. *Resuscitation*, 71(1), 19-28.

Smith, G., Prytherch, D. R., Schmidt, P. E., Featherstone, P. I., and Higginsc, B., 2008. A Review and Performance Evaluation of Single-parameter “Track and Trigger” Systems. *Resuscitation*, 79, 11-21.

Smith, G., Prytherch, D. R., Schmidt, P. E. and Featherstone, P. I., 2008. Review and Performance Evaluation of Aggregate Weighted “Track and Trigger” Systems. *Resuscitation*, 77(2), 170-179.

Shah, R.C., Roy, R., Jain S. and Brunette, W., 2003. Data MULEs: Modeling a Three-tier Architecture for Sparse Sensor Networks. In: *the 1st IEEE International Workshop on Sensor Network Protocols and Applications*, 11 May 2003 Seattle, WA, USA, 30-41.

Shnayder, V., Chen, B. R., Lorincz, K., Fulford-Jones T. R. F. and Welsh, M., 2005, Sensor Networks for Medical Care. *Technical Report TR-08-05*, Harvard University, USA.

Shuaib, K., Boulmalf, M., Sallabi, F. and Lakas, A., 2006, Co-existence of ZigBee and WLAN, A performance study. In: *Wireless Telecommunication Symposium*, April Pomona, CA, 1-6.

Soomro, A. and Cavalcanti, D., 2007. Opportunities & Challenges Using WPAN and WLAN Technologies in Medical Environments. *IEEE Communications Magazine*, 45(2), 114-122.

Stenhouse, C., Coates, S., Tivey, M., Allsop, P. & Parker, T., 2000. Prospective Evaluation of a modified Early Warning Score to Aid Earlier Detection of Patients Developing Critical Illness on a General Surgical Ward. *British Journal of Anaesthesia*, 84(5), 663.

Subbe, C. P., Kruger, M., Rutherford, P. & Gemmel, L., 2001, Validation of a Modified Early Warning Score in Medical Admissions. *QJM*, 94, 521—526.

Sun, T., Chan, L. J., Han, C. C., Yang, G. and Gerla, M., 2006. Measuring Effective Capacity of IEEE 802.15.4 Beaconless Mode. In: *IEEE Wireless Communications and Networking Conference*, 3-6 April 2006 Las Vegas, USA. 493-498.

Tan, K. S., and Hinberg, I., 2000. Effects of a Wireless LAN System, a Telemetry System and Electrosurgical Devices on Medical Devices in a Hospital Environment, *Biomedical Instruction Technology*, 34(2), 115–118.

Techchee, 2010. Wireless heart Rate Monitor Watch with a Chest Strap-on for Better Precision. Available from <http://www.techchee.com/2009/02/05/wireless-heart-rate-monitor-watch-with-a-chest-strap-on-for-better-precision/> [Accessed 16 May 2010]

Tremper., K. K. and Barker., S. J., 1989. Pulse Oximetry. *Anesthesiology*, 70(1), 98–108.

Turner, P., Garry, M., Manfred, K., Penman, Ian. & Turner S, 2005. Implementing a Wireless Network of PDAs in a Hospital Setting. *Pers Ubiquit Comput*, 9, 209-217.

Ullah, M. Z., 2009. *An Analysis of the Bluetooth Technology*. Dissertation (Master). Blekinge Institute of Technology

Varshney, U., 2006, Enhancing Wireless Patient Monitoring by Integrating Stored and Live Patient Information. In: *the 19th IEEE International Symposium on Computer-Based Medical Systems* 22-23 June 2006 Salt Lake City, USA. 501-506.

Varshney, U., 2009, *Pervasive Healthcare Computing: EMR/HER. Wireless and Health Monitoring*, Atlanta: Springer.

VitalJacket, 2008, VitalJacket: Heart Monitoring Shirt, *Internet Journal of Emerging Medical Technologies*. Available from: http://medgadget.com/archives/2008/04/vitaljacket_heart_monitoring_shirt.html [Accessed in May 2009].

Voigt, T., Österlind, F. and Dunkels, A., 2008. Improving Sensor Network Robustness with Multi-channel Convergecast, In: *2nd ERCIM Workshop on e-Mobility*. 30 May 2008 Tampere, Finland.

Whittington, J., White, R., Haig, K. M. and Slock, M., 2007, Rapid response systems: the stories - Using an automated risk assessment report to identify patients at risk for clinical deterioration. *The Joint Commission Journal on Quality and Patient Safety*, 33(9), 569-574.

World Health Organization (WHO), 2009. *Data and Statics*, Available from: <http://www.who.int/research/en/> [Accessed 12 June 2009]

World Health Organization (WHO), 2010. *Health Topics*. Available from: <http://www.who.int/topics/en/> [Accessed 19 May 2010]

Xiao, Y., 2008. Accountability for Wireless LANs, Ad Hoc Networks and Wireless Mesh Networks. *IEEE Communication Magazine*, 46, 116–26.

Yeatman, E. M., 2006. Rotating and Gyroscopic MEMS Energy Scavenging. In: *Int. Workshop on Wearable and Implantable Body Sensor Networks (BSN 2006)*, 3–5 April 2006 Cambridge, MA, USA.

Yu, S. N. and Cheng, J. C., 2005, A Wireless Physiological Signal Monitoring System with Integrated Bluetooth and WiFi Technologies. In: *the 27th Annual EMBS International Conference, 1-4 September 2005, Shanghai, China*. Available from: ieeexplore.ieee.org/iel5/10755/33900/01616900.pdf [Accessed 19 May 2007]

Yuce, M. R., Ng, P. C., Lee, C. K., Khan, J. Y. and Liu, Wentai, 2007, A Wireless Medical Monitoring Over a Heterogeneous Sensor Network. In: *29th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 23-26 August 2007 Lyon, France. 5894-5898.

Zeghdoud, M., Cordier, P. and Terre, M., 2006. Impact of Clear Channel Assessment Mode on the Performance of ZigBee Operating in a WiFi Environment. In: *the 1st Workshop on Operator-assisted (Wireless Mesh) Communality Networks*, 18-19 September Berlin, Germany. 1-8.

ZigBee Alliance, 2007. *ZigBee Health Care Public Application Profile*, Available from:

<http://www.zigbee.org/Products/DownloadZigBeeTechnicalDocuments.aspx>

[Accessed 10 July 2010].

Zhou, G., Lu, J., Wan, C. Y., Jarvis, M. D. and Stankovic, J. A., 2008. BodyQoS: Adaptive and Radio-agnostic QoS for Body Sensor Networks. In: *27th IEEE Conf. on Computer Communications, 13–18 April 2008 Phoenix, AZ, USA*, 565–73.

Zhu, Y., Keoh, S. L., Sloman, M., Lupu, E., Dulay, N. and Pryce, N., 2008. A Policy System to Support Adaptability and Security on Body Sensors. In: *Int. Workshop Wearable and Implantable Body Sensor Networks (BSN 2008)*, 1–3 June 2008 Hong Kong. 37–40

Appendix 1. Calculation of ZigBee Channel Capacity

The actual channel capacity, C , for a single hop connection in a non-beacon WPAN can be founded:

$$C = \frac{T_{packet}}{T_{packet} + T_{ack} + T_{header} + T_{wait}} \times C_p$$

where T_{packet} is the time used to transmit the actual data payload (Sun *et al.* 2005). Similarly, T_{ack} and T_{header} are the respective times used to send the ACK packet and the headers. T_{wait} is the minimum time that the radio has to wait before sending a packet. $C_p = 250$ kbps is the maximum data rate defined by IEEE 802.15.4 standard. The equations below show how to calculate the components in equation:

$$T_{packet} = \frac{S_{packet}}{C_p}, T_{ack} = \frac{S_{ack}}{C_p}, T_{header} = \frac{S_{header}}{C_p}$$

where S_{packet} is the size of the payload, S_{ack} is the size of the ACK packet, S_{header} is the total size of all headers.

To get the maximum transmission efficiency of the system, it should minimize the header/payload ratio and use the largest possible packets of 126 bytes (default). Deducting a total header size of 30 bytes, $S_{packet} = 96$ bytes. To find the maximum one hop capacity, the minimum wait time from CCA time, radio turnaround time and inter-frame spacing are used to calculate T_{wait} . This is defined by the IEEE 802.15.4 standard as default 1.152 ms. In this case, the upper-bound for the effective single hop capacity for one node is: $C \leq 142.86$ kbps.

Appendix 2. PIC16F887 Specifications



PIC16F882/883/884/886/887

28/40/44-Pin Flash-Based, 8-Bit CMOS Microcontrollers with nanoWatt Technology

High-Performance RISC CPU:

- Only 35 Instructions to Learn:
 - All single-cycle instructions except branches
- Operating Speed:
 - DC – 20 MHz oscillator/clock input
 - DC – 200 ns instruction cycle
- Interrupt Capability
- 8-Level Deep Hardware Stack
- Direct, Indirect and Relative Addressing modes

Special Microcontroller Features:

- Precision Internal Oscillator:
 - Factory calibrated to $\pm 1\%$
 - Software selectable frequency range of 8 MHz to 31 kHz
 - Software tunable
 - Two-Speed Start-up mode
 - Crystal fail detect for critical applications
 - Clock mode switching during operation for power savings
- Power-Saving Sleep mode
- Wide Operating Voltage Range (2.0V-5.5V)
- Industrial and Extended Temperature Range
- Power-on Reset (POR)
- Power-up Timer (PWRT) and Oscillator Start-up Timer (OST)
- Brown-out Reset (BOR) with Software Control Option
- Enhanced Low-Current Watchdog Timer (WDT) with On-Chip Oscillator (software selectable nominal 256 seconds with full prescaler) with software enable
- Multiplexed Master Clear with Pull-up/Input Pin
- Programmable Code Protection
- High Endurance Flash/EEPROM Cell:
 - 100,000 write Flash endurance
 - 1,000,000 write EEPROM endurance
 - Flash/Data EEPROM retention: > 40 years
- Program Memory Read/Write during run time
- In-Circuit Debugger (on board)

Low-Power Features:

- Standby Current:
 - 50 nA @ 2.0V, typical
- Operating Current:
 - 11 μ A @ 32 kHz, 2.0V, typical
 - 220 μ A @ 4 MHz, 2.0V, typical
- Watchdog Timer Current:
 - 1 μ A @ 2.0V, typical

Peripheral Features:

- 24/35 I/O Pins with Individual Direction Control:
 - High current source/sink for direct LED drive
 - Interrupt-on-Change pin
 - Individually programmable weak pull-ups
 - Ultra Low-Power Wake-up (ULPWU)
- Analog Comparator Module with:
 - Two analog comparators
 - Programmable on-chip voltage reference (CVREF) module (% of VDD)
 - Fixed voltage reference (0.5V)
 - Comparator inputs and outputs externally accessible
 - SR Latch mode
 - External Timer1 Gate (count enable)
- A/D Converter:
 - 10-bit resolution and 11/14 channels
- Timer0: 8-bit Timer/Counter with 8-bit Programmable Prescaler
- Enhanced Timer1:
 - 16-bit timer/counter with prescaler
 - External Gate Input mode
 - Dedicated low-power 32 kHz oscillator
- Timer2: 8-bit Timer/Counter with 8-bit Period Register, Prescaler and Postscaler
- Enhanced Capture, Compare, PWM+ Module:
 - 16-bit Capture, max. resolution 12.5 ns
 - Compare, max. resolution 200 ns
 - 10-bit PWM with 1, 2 or 4 output channels, programmable "dead time", max. frequency 20 kHz
 - PWM output steering control
- Capture, Compare, PWM Module:
 - 16-bit Capture, max. resolution 12.5 ns
 - 16-bit Compare, max. resolution 200 ns
 - 10-bit PWM, max. frequency 20 kHz
- Enhanced USART Module:
 - Supports RS-485, RS-232, and LIN 2.0
 - Auto-Baud Detect
 - Auto-Wake-Up on Start bit
- In-Circuit Serial Programming™ (ICSP™) via Two Pins
- Master Synchronous Serial Port (MSSP) Module supporting 3-wire SPI (all 4 modes) and I²C™ Master and Slave Modes with I²C Address Mask

Appendix 3. Code of Programmed System for Micro-controller

```
/*
*****
*/
/* Evaluation Board for Maxstream Xbee Series 2 Modules */
/* Program to be used in custom board */
/* Designer and programmer: Angel Torres */
/* Date: 17/02/2008 */
*****
#include "Billy_PIC16F887.h" #include "bcd7seg_2.h" #include "spi.h", long value; int
num_count; int count; int state1; int state2; int state3; int1 base_time; long per; int8 bcd; int8 aux;
int count_bcd=0; signed int16 temp; // Time thresholds according to base time.
#define UP_TH 90 #define LOW_TH 10 #BYTE PORTA= 0x05 #BYTE PORTB= 0x06
#BYTE PORTC= 0x07 #BYTE PORTD= 0x08 #BYTE PORTE= 0x09 #BYTE PIR1= 0x0C
#BYTE SSPBUF= 0x13 #BYTE SSPCON = 0x14
#define SSPIF 3 #define WCOL 7 #define T_BUFFER_SIZE 32
byte t_buffer[T_BUFFER_SIZE]; byte t_next_in = 0; byte t_next_out = 0;
#int_tbe
void serial_isr() {putc(t_buffer[t_next_out]);
t_next_out=(t_next_out+1) % T_BUFFER_SIZE;
if(t_next_in==t_next_out)
disable_interrupts(int_tbe);} // Overflow every 100ms
#int_TIMER1
void TIMER1_isr(void)
{ value = read_adc();
temp = medida_TC77();
set_timer1(15535);
count++;}
void bputc(char c) { short restart; int ni; restart=t_next_in==t_next_out; t_buffer[t_next_in]=c;
ni=(t_next_in+1) % T_BUFFER_SIZE;
while(ni==t_next_out);
t_next_in=ni;
if(restart)
enable_interrupts(int_tbe);}
void main()
```

```

{// Configuration of the internal clock 8MHz
    setup_oscillator(OSC_8MHZ);
    / set up the adc channels
    setup_adc_ports(sAN0lsAN1lsAN2lVSS_VDD); //clock polarity is low by default, data
transmitted in rising edge
    setup_spi(SPI_MASTER|SPI_L_TO_H|SPI_XMIT_L_TO_H|SPI_CLK_DIV_16);    //clock
polarity is high by default, data transmitted in rising edge
    setup_timer_0(RTCC_INTERNAL|RTCC_DIV_1);
    setup_timer_1(T1_INTERNAL|T1_DIV_BY_4);//
    Res=(1/(Fosc/4))*4*(2^16-1)=4/8E6*4= 2us *65535=131ms
    setup_timer_2(T2_DISABLED,0,1);
    setup_comparator(NC_NC_NC_NC);
    setup_vref(FALSE);
    setup_adc(ADC_CLOCK_INTERNAL);
    enable_interrupts(INT_TBE);
    enable_interrupts(INT_TIMER1);
    enable_interrupts(GLOBAL);
    set_adc_channel( 0 );
    num_count=30;
    state1=0; state2=0; base_time=0; // Overflow every 100ms
    set_timer1(15535);
    while(1)
    { if(count>=num_count)
        { // output the conversion values//
          printf("%X%X%2X%2X\n",0xAA,0x01,make8(value,1),make8(value,0));
          // send data without polling TXIF
          printf(bputc,"%X%X%2X%2X\n",0xAA,0x02,make8(value,1),make8(value,0));
          //printf("%X%X%2X%2X\n",0xBB,0x01,make8(temp,1),make8(temp,0)); //
          send data without pooling TXIF
          printf(bputc,"%X%X%2X%2X\n",0xBB,0x02,make8(temp,1),make8(temp,0));
          count=0; }
        if(temp>3800)
        { output_bit( PIN_B3, 0); output_bit( PIN_B4, 0); output_bit( PIN_B5, 1); }
        else if(temp>2500)

```

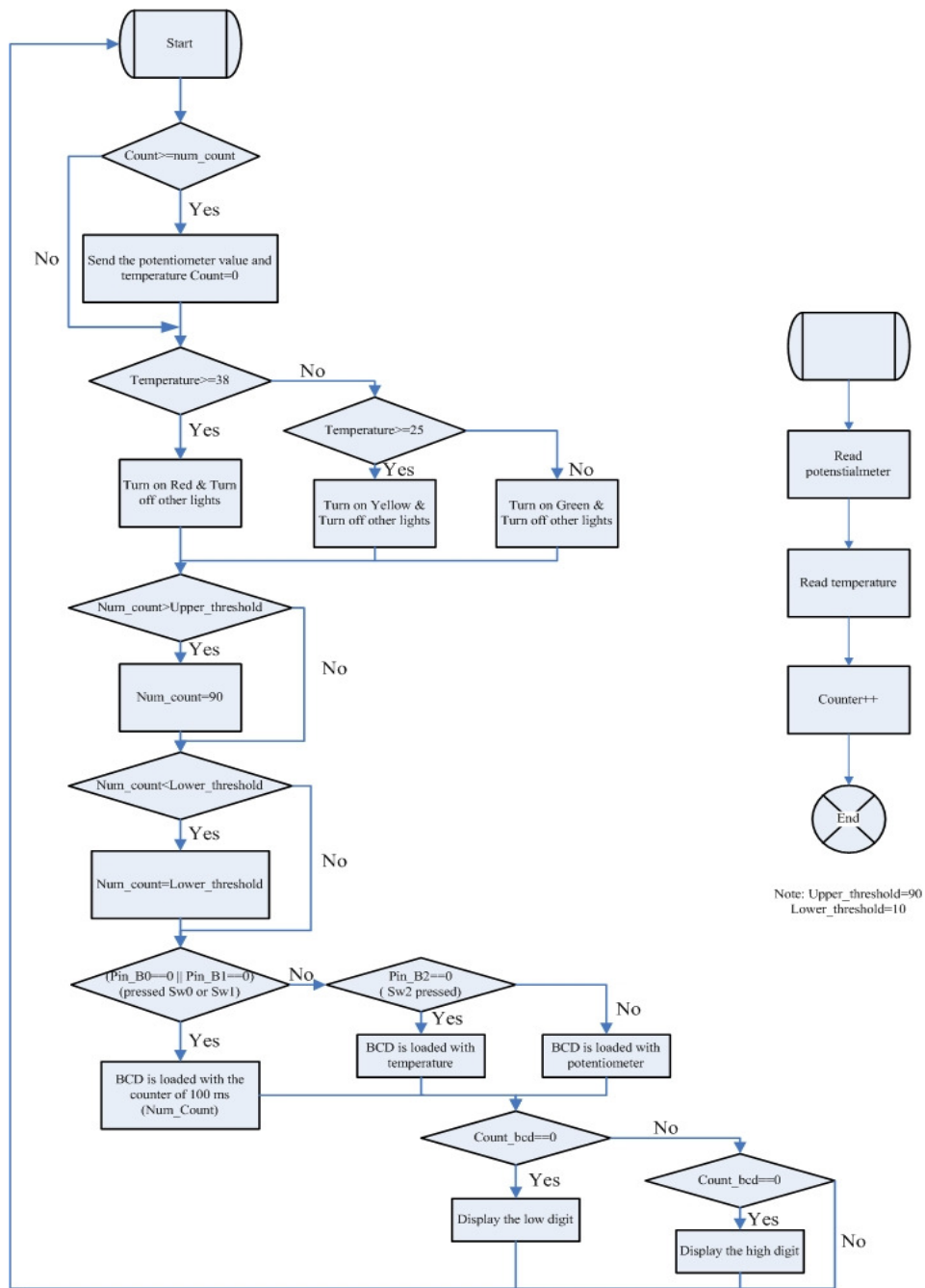


```

{output_bit( PIN_B3, 0); output_bit( PIN_B4, 1); output_bit( PIN_B5, 0);}
else
{output_bit( PIN_B3, 1); output_bit( PIN_B4, 0); output_bit( PIN_B5, 0);}
if( !input(PIN_B0) ) {state1=1;} if( !input(PIN_B1) ){state2=1 ;}
if( !input(PIN_B2) ){state3=1;}
if(state1==1){if( input(PIN_B0) ){state1=2;}}
if(state2==1){if( input(PIN_B1) ){state2=2;}}
if(state3==1){if( input(PIN_B2) ){state3=2;}}
if(state1==2){num_count++; state1=0;}
if(state2==2){num_count--; state2=0 ;}
if(state3==2){printf("Angel Torres"); state3=0;}
if(num_count>UP_TH) num_count=UP_TH; if(num_count<LOW_TH)
num_count=LOW_TH;
if( !input(PIN_B0) || !input(PIN_B1) )// saco el contador de tiempo
{bcd=(((num_count/10)<<4)|(num_count%10));} else if(!input(PIN_B2))
//Pushbutton for the temperature
{aux=temp/100; bcd=(((aux/10)<<4)|(aux%10));}
else// AN0 analog to digital conversion
// hexadecimal to decimal representation
per=value;
per=(per*25); // multiply by 100 and divide by 1024 --> ratio(25/256)
per=per>>8;
bcd=(((per/10)<<4)|(per%10)); //2 lower digits}
if (count_bcd==0)
{aux=bcd&0x000F;
display_seg(aux,0);
count_bcd=1;}
else if(count_bcd==1)
{aux=bcd>>4; display_seg(aux,1); count_bcd=0;}}

```

Appendix 4. Flow Chart of Programmed System for Micro-controller



Appendix 5. Datasheet of Digi XBee Series

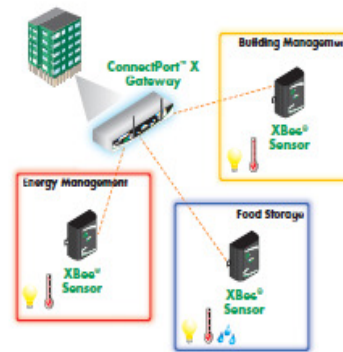
Product Datasheet



XBee® Sensors

Compact Battery Powered Sensors with Integrated ZigBee®

XBee sensors easily integrate into ZigBee networks, featuring long battery life and small size for unobtrusive installation anywhere.



Features/Benefits

- ZigBee wireless sensors
 - Temperature, humidity, light
- Small form factor can be mounted anywhere
- Long-life battery
- Easy to install/configure
- Easy to integrate with Digi's Drop-in Networking family of gateways, adapters and modules on a ZigBee network
 - Integrate with custom Python® development environment for events, triggers and data logging
- Applications include building automation and security, energy management, food management, freight/vehicle monitoring

Overview

ZigBee technology enables low-cost, low-power networking of sensors, controllers and other devices in self-configuring, self-healing wireless mesh networks. Part of Digi's Drop-in Networking solutions, XBee sensors offer the ability to provide real-time data from a variety of sensors (e.g., temperature, humidity, light) in a single solution for wireless communication across a ZigBee infrastructure.

Their small form factor and long-life battery power make XBee sensors easy to integrate with Digi's Drop-in Networking solutions to provide reliable, unobtrusive communications. Applications include building automation and security, energy management, food management, freight/vehicle monitoring and many more.

Installation is a snap. Simply insert batteries, add the XBee sensor to the ZigBee network, and configure the update interval. Next, mount the device in an out-of-the way location and start communicating.

XBee sensors can be used with ConnectPort™ X gateways, XBee embedded modules, XBee adapters or XBee wall routers to drop-in end-to-end device networks – without the need for a wired network infrastructure.



www.digi.com



Features/Specifications

FEATURES

- General**
- Frequency: 2.4 GHz (ISM)
 - Internal antenna
- Performance**
- Indoor/Urban range: 133 ft (40 m)
 - Outdoor (if line of sight range): 400 ft (120 m)
 - Transmit power output: 1.25 mW (-1 dBm) / 7 mW (-1 dBm) boost mode
 - RF data rate: 250,000 bps
 - Receive sensitivity (1% PER): -97 dBm (-98 dBm boost mode)
- Networking and Security**
- Networking topologies: Point-to-Point, Point-to-Multipoint, Peer-to-Peer, Mesh
 - Number of channels: 16 - 5 MHz channels (Direct Sequence Spread Spectrum)
 - Filtration options: PAN ID, Channel, 2^64 (64-bit) addresses
- LEDs**
- Power: Solid when powered and not associated to network.
 - Associate: blinks when unit is associated to network
- Push Button**
- Device reset
 - Configuration reset to factory defaults
 - Identification/Commissioning mode

INTERFACES

- ZigBee - compatible with:
 - Digi XBee ZNet 2.5 (formerly Series 2) module
 - EmberZNet 2.5x mesh stack

MODEL.....PART NUMBERS

Model	Worldwide
XBee Sensor - Battery powered temperature and light	XS-Z14-CB1RB
XBee Sensor - Battery powered temperature, humidity and light	XS-Z14-CB2RB

INTEGRATED SENSORS

- Temperature Sensor**
- Range: -18° C to +55° C (-0.2° F to +131° F)
 - Accuracy: +/- 2° C
- Ambient Light Sensor**
- Range of spectral bandwidth: 360 to 970 nm (similar to human eye)
 - Wavelength of peak sensitivity: 570 nm
- Humidity Sensor**
- Range: 0 to 100% RH
 - Interchangeability:
 - +/- 5 %RH (0% RH to 59%RH)
 - +/- 8 %RH (60% RH to 100%RH)
 - Accuracy: +/- 3.5% RH

ENVIRONMENTAL

- Operating temperature: -18° C to 55° C (-0.4° F to 131° F)
- Power requirements: 3 x AA alkaline 1.5V batteries (batteries not included)

BATTERY LIFE

Duty Cycle	Battery Life Estimate
1 read per 30 sec	1.5 years
1 read per minute	2.5 years
1 read per hour (or less frequent)	6 years

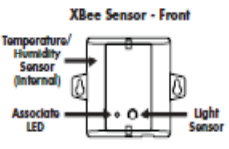
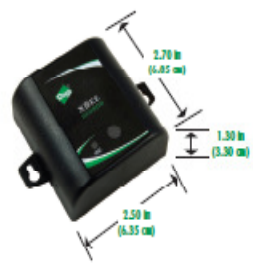
• Assumptions based on:
- Cyclic sleep enabled with single transmit per wake cycle
At 21° C

REGULATORY APPROVALS (pending)

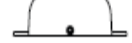
- FCC Part 15, Class B
- EN55022 Class B, EN 55024
- RoHS Compliant

DIMENSIONS

- Length: 2.70 in (6.85 cm)
- Width: 2.50 in (6.35 cm)
- Height: 1.30 in (3.30 cm)
- Weight: 0.35 lb (0.158 kg) w/batteries, 0.20 lb (0.091 kg) without batteries



XBee Sensor - Top/Bottom



DIGI SERVICE AND SUPPORT - You can purchase with confidence knowing that Digi is here to support you with expert technical support and a strong five-year warranty. www.digi.com/support



- | | | | |
|--|--|--|--|
| <p>Digi International
11001 Bran Road E.
Minnetonka, MN 55343
U.S.A.
PH: 877-912-3444
952-912-3444
FX: 952-912-4952
email: info@digi.com</p> | <p>Digi International France
31 rue des Potezonniers
92200 Neuilly sur Seine
PH: +33-1-55-61-98-98
FX: +33-1-55-61-98-99
www.digi.fr</p> | <p>Digi International KK
NES Building South 8F
22-14 Sakuragaoka cho,
Shibuya-ku
Tokyo 150-0031, Japan
PH: +81-3-5428-0261
FX: +81-3-5428-0262
www.digi-intl.co.jp</p> | <p>Digi International (HK) Limited
Unit 3206 - 08A, 32/F,
AIA Tower
183 Electric Road
North Point, Hong Kong
PH: +852-2833-1008
FX: +852-2572-9989
www.digi.cn</p> |
|--|--|--|--|

Digi International, the leader in device networking for business, develops reliable products and technologies to connect and securely manage local or remote electronic devices over the network or via the web. With over 20 million ports shipped worldwide since 1985, Digi offers the highest levels of performance, flexibility and quality.

www.digi.com

© 2008 Digi International Inc. All rights reserved. Digi, Digi International, the Digi logo, the When Reliability Matters logo, ConnectPort and XBee are either trademarks or registered trademarks of Digi International Inc. in the United States and other countries worldwide. All other trademarks are the property of their respective holders.

91001457
01/08



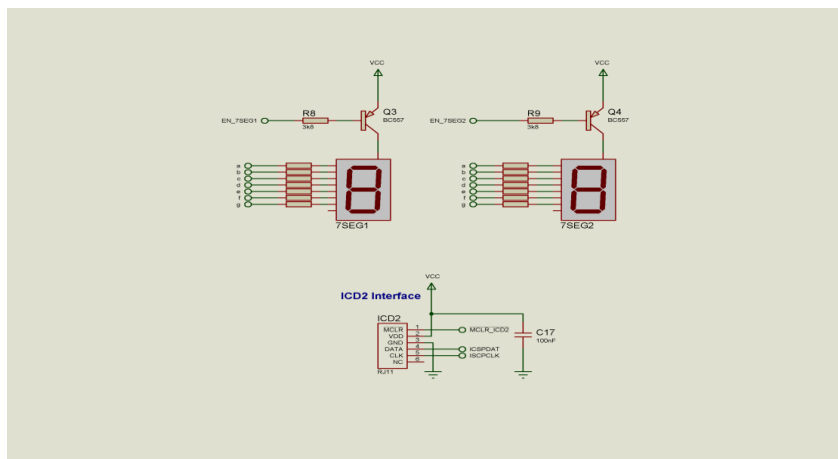
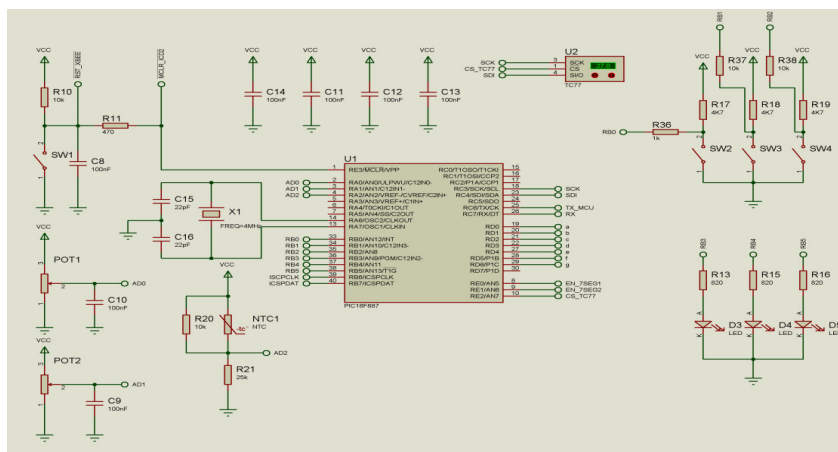
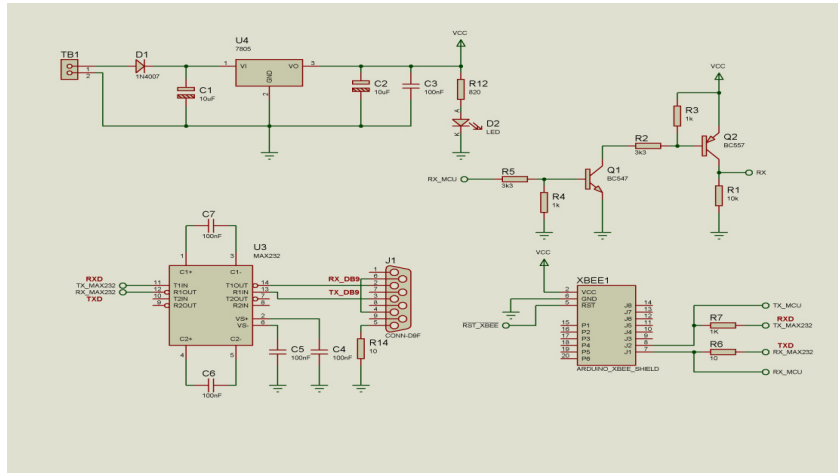
Appendix 6. All Configurable Parameters Supported by XBee Series 2

Networking	Operating Channel	Read the operating channel number (Uses 802.15.4 channel numbers).
	Operating PAN ID	Set the PAN (Personal Area Network) ID. Valid range is 0 - 0x3FFF. Alternatively, set ID=0xFFFF for the coordinator to choose a random Pan ID. RANGE:0-0xFFFF
	Scan Channel	Set/read list of channels to scan (active and energy scans) when forming a PAN as bitfield. Scans are initiated during coordinator startup: Bit 15 = Chan 0x1A . . . Bit 0 = Chan 0x0B RANGE:0-0xFFFF BITFIELD
	Scan Duration	Set/read the Scan Duration exponent. The exponent configures the duration of the active scan and energy scan during coordinator initialization. Scan Time = SC * (2 ^ SD) * 15.36ms. (SC=# channels) RANGE:0-0X07 EXPONENT
	Node Join Time	Set/read the Node Join time. The value of NJ determines the time (in seconds) that the device will allow other devices to join to it. If set to 0xFF, the coordinator will always allow joining. RANGE:0-0XFF X 1 SEC
Addressing	MY-16bit Network Address	Read the 16 bit Network Address for the modem. 0xFFFF means the device has not joined a PAN.
	Serial number high	Read high 32 bits of modems unique IEEE 64-bit Extended Address.
	Serial number low	Read high 32 bits of modems unique IEEE 64-bit Extended Address.
	Destination Address High	Set/read the upper 32 bits of the 64 bit destination extended address. 0x000000000000FFFF is the broadcast address for the PAN. 0x0000000000000000 can be used to address the Pan Coordinator. RANGE:0-0xFFFFFFFF
	Destination Address Low	Set/read the lower 32 bits of the 64 bit destination extended address. 0x000000000000FFFF is the broadcast address for the PAN. 0x0000000000000000 can be used to address the Pan Coordinator. RANGE:0-0xFFFFFFFF
	ZigBee Addressing	Set/read the ability to send transmissions using the ZigBee source and destination fields and cluster IDs (SE, DE, CI commands). RANGE:0-1

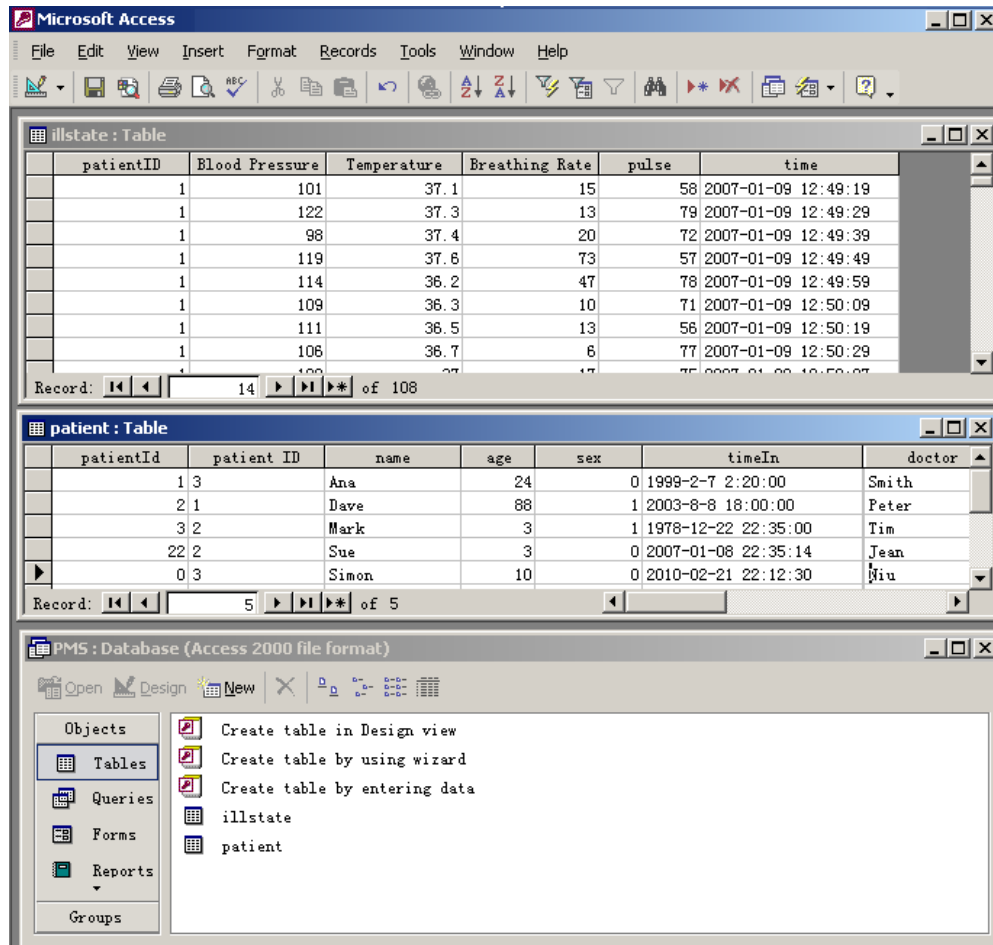
	Source Endpoint	Set/read the source endpoint used for serial data transmissions. This should only be changed if multiple endpoints must be supported. This command value is used in data transmissions only if ZA=1. RANGE:0X01-0XEF
	Destination Endpoint	Set/read the destination endpoint used for serial data transmissions. This should only be changed if multiple endpoints must be supported. This command value is used in data transmissions only if ZA=1. RANGE:0X01-0XEF
	Cluster ID	Set/read the cluster identifier value used for serial data transmissions. This should only be changed if multiple cluster IDs must be supported. This command value is used in data transmissions only if ZA=1. RANGE:0X00-0XFF
	Node Identifier	Set/read Node Identifier string
	Broadcast Radius	Set/Read the transmission radius for broadcast data transmissions. Set to 0 for maximum radius. RANGE:0-0X20
	AR-Aggregation Route Broadcast Time	Set/read the time between aggregation route broadcast times. This should be configured for no more than one node in a network to establish a route throughout the network to the node. Setting AR to 0xFF disables aggregation route broadcasting. Setting AR to 0 sends only one broadcast.
	Device Type Identifier	Set/read the device type identifier value. This can be used to differentiate multiple XBee-based products. RANGE:0-0XFFFFFFFF
	Node Discovery Backoff	Set/read Node Discovery backoff register. This sets the maximum delay for Node Discovery responses to be sent (ND, DN). RANGE:0X20-0XFF X 100 MS
	Node Discovery Option	Sets the node discovery options register. Options include 0x01 - Append DD value to end of node discovery, 0x02 - Return devices own ND response first. RANGE:0-3
RF interfacing	Power level	Select/Read transmitter output power. (XBee-PRO supports a fixed output power.) Approximate power levels (XBee): 0= -7dBm, 1= -3dBm, 2= -1dBm, 3= +1dBm, 4= +3dBm.
	Power mode	Select/Read module boosts mode setting. If enabled, boost mode improves sensitivity by 1dB and increases output power by 2dB, improving the link margin and range.
Security	Encryption Enable	Enable or disable ZigBee encryption.
	Encryption Option	Set the ZigBee Encryption options: Bit0 = Transmit security key on join, Bit1 = Use Trust Center RANGE:0-3 BITFIELD

	AES Encryption Key	Sets key used for encryption and decryption. This register can not be read.
Serial Interfacing	Baud Rate	Set/read the serial interface baud rate for communication between modem serial port and host. Request non-standard baud rates above 0x80 using a terminal window. Read BD register to find actual baud rate achieved.
	Parity	Configure parity for the UART.
	Packetization timeout	Set/read number of character times of inter-character delay required before transmission begins. Set to zero to transmit characters as they arrive instead of buffering them into one RF packet. RANGE:0-0XFF X CHARACTER TIMES

Appendix 7. Designed ZB



Appendix 8. A Designed Database for the Central Control Unit



Appendix 9. The Code Used by DAS Model for Transition Diagram

```
case WlanC_ERP_OFDM_11g:

    /* Set the slot time to 9E-6 seconds (short) initially. We will increase it to 20 usec (long)
    if we detect that we operate in an IBSS or in a BSS that also has non-ERP STAs
    associated. slot_time = 9E-06; Short interframe gap in terms of seconds. sifs_time = 10E-
    06; PLCP overheads, which include the preamble and header, in terms of seconds.
    Assume ERP-OFDM preamble.

    /*We will adjust the overhead amount if regular long or short DSSS preambles are used. /

    plcp_overhead_control = WLANC_PLCP_OVERHEAD_OFDM;

    plcp_overhead_data = WLANC_PLCP_OVERHEAD_OFDM;

    /* Minimum contention window size for selecting backoff slots. */

    /* Initially we pick the lower CWmin and increase it to 31 if we operate in an IBSS
    containing some non-ERP STAs or if we are associated with a non-ERP AP. cw_min =
    15;

    /* Maximum contention window size for selecting backoff slots. */

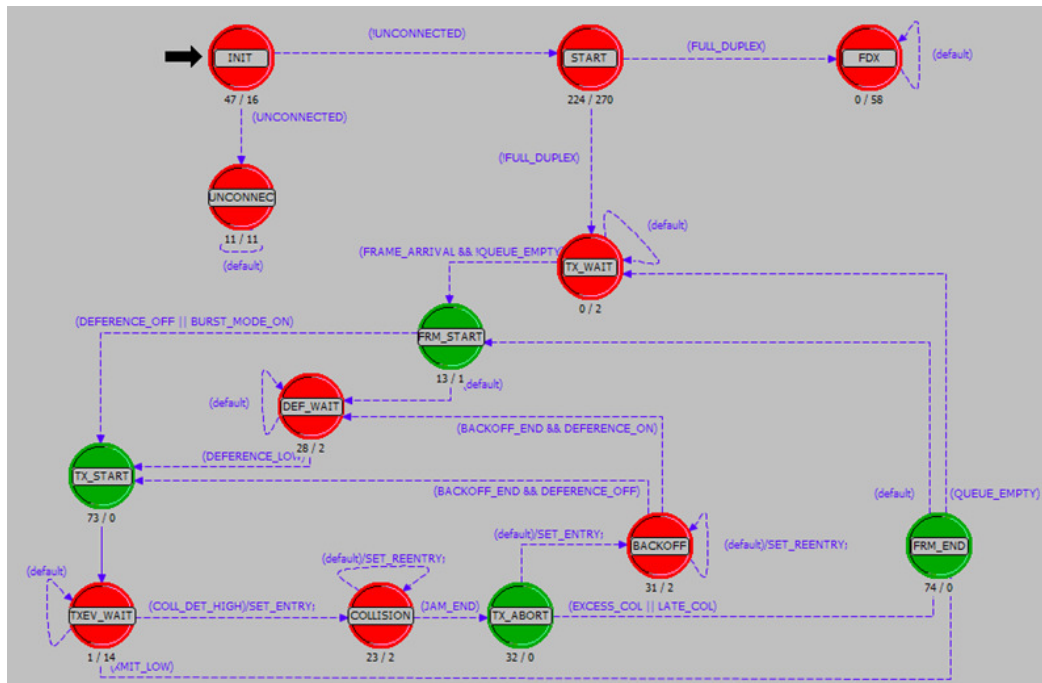
        cw_max = 1023;

        /* Set the PHY standard.

        phy_type = WlanC_11g_PHY;

        break;

    }
```



Transition Diagram (OPNET, Technologies 2009)

Appendix 10. Theoretical Throughput of a WLAN

An optimal WLAN should provide an appropriate throughput for dramatically growing demand from the side of the applications. Performance limit of a WLAN in terms of a maximum theoretical throughput is a key issue in network management and control traffic tasks.

It has been mentioned that the speed of 802.11 is defined in terms of available bit rate, encapsulation of data, collisions in the wireless media or processing delays in the wireless equipment are not taken into account. To calculate the theoretical throughput, it is necessary to make some simplifying assumptions. The only type of MAC frames considered are data and ACK frames (Figure 1), none of them are subject to corruption by interference or packet collisions. Fragmentation is not an issue, which normally would be the case since maximum-sized Ethernet frames are 1500 bytes, whereas 802.11 data frames may contain 2312 bytes of upper layer data. Figure 4.10 shows the MAC protocol data unit where it can be seen that an additional 34 bytes are added to the Ethernet frame. The MAC layer ACK has a simpler format which can be seen in Figure1. Both these frames are called physical layer convergence Protocol-Service Data Unit (PSDU) on the PHY layer (Figure 2).

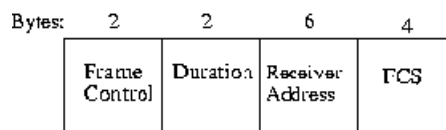


Figure 1 - ACK Frame Format

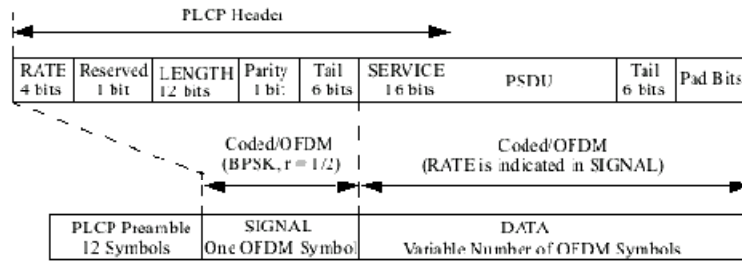


Figure 2 - PPDU frame format

Furthermore, propagation delay is not included, and there are always a continuous and sufficient number of frames to send in order not to drain nor overflow sending or receiving buffers. Other important factors are timing parameters, preamble and data rates, which vary between different extensions of the standard. As has been stated, the focus of the discussion on WLAN in this thesis are limited to 802.11g compliant equipment with maximum data rate of 54Mbps, a circumstance that admits the usage of shorter preamble and slot time. Also, one must consider the upper layer protocol, the total time to transmit one frame, its ACK and timing delays. For both UDP and TCP, the time to transmit one frame without timing delays can be described as shown in equation 1.

$$TX_{Time} = T_{Preamble} + T_{Signal} + T_{Sym} \times \left[\frac{(16+6+MPDU \times 8)}{N_{DBPS}} \right] + T_{Ext} \quad (1)$$

Where:

- $T_{Preamble}$ or preamble duration for the physical layer convergence protocol (PLCP) is $16\mu s$
- T_{Signal} or duration of the signal symbol is $4\mu s$

- T_{Sym} or symbol interval is $4\mu s$
- *MAC protocol data unit* (MPDU) in bytes is 1534
- N_{DBPS} or number of data bits per symbol is 216
- T_{Ext} or signal extension is $6\mu s$

Substituting these numbers into equation (1) yields

$$TX_{Time} = 16 + 4 + 4 \times \left[\frac{(16+6+1534 \times 8)}{216} \right] + 6 = 254\mu s \quad (2)$$

The MAC ACK in response to the frame is given by

$$TX_{ACK} = T_{Preamble} + T_{Signal} + T_{Sym} \times \left[\frac{(16+6+MACK \times 8)}{N_{DBPS}} \right] + T_{Ext} \quad (3)$$

where MACK is the size of the MAC acknowledgment frame, which is 14 bytes.

Substituting into (3) gives:

$$TX_{ACK} = 16 + 4 + 4 \times \left[\frac{(16+6+4 \times 8)}{216} \right] + 6 = 30\mu s \quad (4)$$

The transmission delay for each frame caused by timing is:

$$TX_{Delay} = T_{DIFS} + T_{SIFS} + T_{BO} \quad (5)$$

where

- T_{DIFS} is $28\mu s$,
- T_{SIFS} is $10\mu s$

- T_{BO} is the average back off time, $67.5\mu s$

which gives

$$TX_{Delay} = 28 + 10 + 67.5 = 105.5\mu s \quad (6)$$

So the total transmission time is:

$$TX_{Total} = TX_{Time} + TX_{ACK} + TX_{Delay} = 389.5\mu s \quad (7)$$

or 2567 transactions per second. For UDP, the maximum amount of useful data in every frame is 1472 bytes, and therefore the theoretical throughput becomes

$$UDP_{Throughput} = 1472 \times 8 \times 2567 = 30.2Mbps \quad (8)$$

For TCP, TCP ACK has to be considered, since it results in a MAC layer transmission. The size of a TCP ACK is 40 bytes so equation (1) becomes

$$TX_{Time} = 16 + 4 + 4 \times \left[\frac{(16+6+74 \times 8)}{216} \right] + 6 = 38\mu s \quad (9)$$

Also, equation (6) and (7) get doubled so that

$$TX_{Total} = 563\mu s \quad (10)$$

or 1777 transactions per second. The maximal amount of useful data is 1460 bytes which gives a theoretical throughput of

$$TCP_{Throughput} = 1460 \times 8 \times 1777 = 20.7 Mbps \quad (11)$$

Both UDP and TCP theoretical throughput are lower compared to the advertised data rate. It should be noted the calculation of theoretical throughput was based on some assumption. Changes in the assumptions can affect the calculated value. For example the value can be higher because used average BO is lower than estimated. Also, most of the time one ACK is sent for every two maximum sized Ethernet frames received (delayed ACKs), which would further increase the calculated value of the theoretical throughput.

Appendix 11. List of Publications

Material in this thesis has appeared in the following publications (presented in chronological order):

Sahandi, R., Noroozi, S., Roushanbakhti, G., Heaslip, V. & Liu, Y., 2010. Wireless technology in the evolution of patient monitoring on general hospital wards. *Journal of Medical Engineering and Technology*, 34(1), 51-63.

Sahandi, R. and Liu, Y., 2010. Channel overlap problem in ZigBee based remote patient monitoring on general hospital wards, In: *IEEE International Conference on Communications and Mobile Computing (CMC2010)*, 12-14 April 2010 Shenzhen, China. 259-263.

Liu, Y. and Sahandi, R., ZigBee network for remote patient monitoring, 2009. *IEEE 22nd International Symposium on Information, Communication and Automation Technologies*, 29-31 October 2009 Sarajevo, Bosnia & Herzegovina. 1-7.

Liu, Y. and Sahandi, R., 2008. Review of sensors for remote patient monitoring, In: the 6th *IASTED Biomedical Engineering Conference*, 13-15 February 2008 Innsbruck, Austria.

In addition, the research works have been presented at Annual Conference of Royal Institution of Physics, 15th Dec 2009, London and Bournemouth University Postgraduate Researcher Conference in 2009 and 2010.