High rate wireless personal area network

Lim, Cheng Chuan

2005

Lim, C. C. (2005). High rate wireless personal area network. Master' s thesis, Nanyang Technological University, Singapore.

<https://hdl.handle.net/10356/4655>

<https://doi.org/10.32657/10356/4655>

Nanyang Technological University

Downloaded on 26 Apr 2023 21:25:44 SGT

HIGH RATE WIRELESS PERSONAL AREA NETWORK

Lim Cheng Chuan

School of Electrical & Electronic Engineering

A thesis submitted to the Nanyang Technological University
in fulfilment of the requirement for the degree of
Master of Engineering

2005

TK
5103.2
L732
2005

ACKNOWLEDGEMENTS

The author would like to first and foremost thank his project supervisor, Associate Professor Patrick Ong Kian Seng for his insightful and invaluable advices throughout the duration of the project.

The author would like to further express his appreciation to Mr Lau Choon Poh and Mrs Irene Teng of the Computer Engineering Laboratory for the logistic support offered. The author would like to extend his gratitude to Mr Anthony Chong of the Network Technology Research Centre too for his enthusiastic help in terms of software support.

CONTENTS

LIST OF FIGURES	vi
LIST OF TABLES	viii
ABSTRACT	ix
CHAPTER 1 INTRODUCTION	1
1.1 Motivation	1
1.2 Objectives	2
1.2.1 Interference and Coexistence	2
1.2.2 Routing Algorithms for Ad-Hoc Wireless Networks	2
1.3 Scope	3
1.4 Major Contributions	3
1.5 Organisation of Thesis	4
CHAPTER 2 SURVEY OF WIRELESS COMMUNICATION NETWORKS	5
2.1 Fundamental Architecture of a Communication System	5
2.1.1 Call Modem	5
2.1.2 Answer Modem	6
2.2 Architecture of Wireless Local Area Network (WLANs)	7
2.2.1 Overview	7
2.2.2 PHY Layer	8
2.2.3 MAC Layer	10
2.2.4 Security	12
2.3 Architecture of Wireless Personal Network (IEEE 802.15.1)	13
2.3.1 Overview	13
2.3.2 Specifications	14
2.3.3 Security	18
2.4 IEEE 802.15.3 High Rate Data Wireless Personal Area Network (up to 55 Mbps)	18

2.4.1	Overview	18
2.4.2	Specifications	18
2.5	IEEE 802.15.3a Higher Data Rate WPAN	20
2.5.1	Overview	20
2.5.2	Theory of Impulse Radio	22
2.5.3	Advantages of UWB	27
2.5.4	Disadvantages of UWB	28
CHAPTER 3 COEXISTENCE		30
3.1	Coexistence of Bluetooth and WLAN	30
3.1.1	Overview	30
3.1.2	Collaborative Solutions	31
3.1.3	Non-Collaborative Solutions	32
3.2	Mathematical Modelling of Performance of Coexisting WPAN Devices in WLAN DSSS Environment	33
3.2.1	Overview	33
3.2.2	Greg Enni's Probability Model	33
3.2.3	Proposed Probability Model	35
3.3	Comparison of Proposed Model and Greg Ennis's Model	41
3.3.1	Comparison of Packet Error Rates	41
CHAPTER 4 ROUTING PROTOCOLS FOR UWB AD-HOC WIRELESS PERSONAL AREA NETWORK		43
4.1	Overview	43
4.2	Table-Driven Routing Protocols	43
4.2.1	Destination-Sequenced Distance-Vector Routing (DSDV)	43
4.2.2	Clusterhead Gateway Switch Routing (CGSR)	44
4.2.3	Wireless Routing Protocol (WRP)	45
4.3	Source-Initiated On-Demand Routing Protocols	45
4.3.1	Ad-Hoc On-Demand Distance Vector Routing (AODV)	46
4.3.2	Dynamic Source Routing (DSR)	47
4.3.3	Associativity-Based Routing (ABR)	48
4.3.4	Signal Stability Routing (SSR)	50

4.3.5	Temporally-Ordered Routing Algorithm (TORA)	51
4.4	Weighted-Factors for UWB WPAN	52
4.4.1	Factors for Consideration	53
4.4.2	Weighted-Factors Routing Protocol (WFRP)	55
4.4.3	Examples of WFRP in UWB Network	58
CHAPTER 5	SIMULATIONS	62
5.1	Coexistence of Bluetooth and IEEE 802.11b	62
5.1.1	Degradation Factor Modelling	62
5.1.2	Results	63
5.2	Simulation Environment and Setup for Routing Protocols	64
	Simulations	
5.2.1	Choice of NS2 as Network Simulator	64
5.2.2	Interference Model	65
5.2.3	Traffic Model Generation	66
5.2.4	Scenario Model Generation	67
5.2.5	Simulating UWB Conditions	68
5.2.6	Performance Metrics	69
5.3	Simulation Results for WFRP	69
5.3.1	Results for 10 Sources	70
5.3.2	Results for 20 Sources	73
5.3.3	Results for 30 Sources	77
5.3.4	Results for 40 Sources	80
5.4	Analysis	83
5.4.1	DSR Protocol	83
5.4.2	AODV Protocol	84
5.4.3	WFRP	84
5.5	Related Work	85
5.5.1	Overview	85
5.5.2	Packet Deliver Fraction	86
5.5.3	Routing Overhead	87

CHAPTER 6 CONCLUSION AND RECOMMENDATIONS	89
6.1 Conclusion	89
6.2 Recommendations	91
6.2.1 Creating a More Accurate UWB PHY Model	91
6.2.2 Election of Principal Factor in WFRP	91
BIBLIOGRAPHY	93

LIST OF FIGURES

Figure 2.1	V34 Call Modem	6
Figure 2.2	V34 Answer Modem	7
Figure 2.3	IEEE 802.11b Layers	8
Figure 2.4	PLCP Frame Format	9
Figure 2.5	IEEE 802.11b Back-off Algorithm	11
Figure 2.6	IEEE 802.11b MAC Frame Format	12
Figure 2.7	Bluetooth Architecture	13
Figure 2.8	Time-Division Duplex	15
Figure 2.9	Multi-slots Packets	15
Figure 2.10	Bluetooth Packet Format	16
Figure 2.11	Scatternet	17
Figure 2.12	IEEE 802.15.3 Superframe Structure	19
Figure 2.13	UWB Frequency Spectrum	21
Figure 2.14	Time Hopping Principle	24
Figure 2.15	Modulated PPM	26
Figure 3.1	MEHTA Engine	32
Figure 3.2	Greg Ennis's Time Overlap Model	34
Figure 3.3	Time Overlap of Bluetooth and IEEE 802.11b Packets	36
Figure 3.4	Time Overlap Figure (I)	38
Figure 3.5	Time Overlap Figure (II)	38
Figure 3.6	Time Overlap Figure (III)	39
Figure 3.7	Time Overlap Figure (IV)	39
Figure 3.8	PER of Greg Ennis's Model and the Proposed Model	42
Figure 4.1	Clusterhead Gateway Switch Routing	44
Figure 4.2	AODV Route Discovery	46
Figure 4.3	DSR Route Record Creation	48
Figure 4.4	Route Maintenance in ABR	50
Figure 4.5	Attaining a Higher Speed for UWB with More Hops	53

Figure 4.6	WFRP for Real-Time “Live” Multimedia Streaming	58
Figure 4.7	WFRP for Transmission of Large Files	60
Figure 5.1	Comparison of Degradation Factor	63
Figure 5.2	PDF Performances for 10 Sources	70
Figure 5.3	Average End-to-End Delay for 10 Sources	71
Figure 5.4	Normalised Routing Load for 10 Sources	72
Figure 5.5	PDF Performances for 20 Sources	73
Figure 5.6	Average End-to-End Delay for 20 Sources	
	74/75	
Figure 5.7	Normalised Routing Load for 20 Sources	76
Figure 5.8	PDF Performances for 30 Sources	77
Figure 5.9	Average End-to-End Delay for 30 Sources	78
Figure 5.10	Normalised Routing Load for 30 Sources	79
Figure 5.11	PDF Performances for 40 Sources	80
Figure 5.12	Average End-to-End Delay for 40 Sources	81
Figure 5.13	Normalised Routing Load for 40 Sources	82
Figure 5.14	PDF of Josh Broch et al.’s Work	86
Figure 5.15	Routing Overhead of Josh Broch et al.’s Work	87

LIST OF TABLES

Table 2.1	Bluetooth Transmit Power Classes	14
Table 2.2	Summary of Some Leading WLAN/WPAN Standards	22
Table 3.1	Bluetooth Packet Types	36
Table 4.1	Weight Table	55
Table 4.2	Calculations of Average Path Weight for Example 1	59
Table 4.3	Calculations of Average Path Weight for Example 2	61

ABSTRACT

In the report, various wireless communication standards are reviewed. IEEE 802.11b, Bluetooth and the upcoming IEEE 802.15.3 all operate on the unlicensed 2.4 GHz Industrial, Scientific and Medical (ISM) frequency band. These standards have different Medium Access Control (MAC), so interference is an inevitable issue to be addressed as degradation of the throughput will decrease the efficiency of the wireless systems. To look at the severity of interferences when Bluetooth devices coexist with IEEE 802.11b nodes, the author derived a probability model to investigate the Packet Error Rate (PER) of a Bluetooth piconet operating within close proximity (<0.5 m) of an IEEE 802.11b node.

Many coexistence ideas such as Adaptive Frequency Hopping (AFH) for Bluetooth devices are discussed in the report. One of the more hotly discussed alternatives is the use of Ultra-Wideband (UWB) to side-step the problem of co-existence of the narrowband wireless communication standards and is currently studied by IEEE 802.15.3a Working Group.

UWB offers variable high data rate depending on the distance. It can transfer data up to 1000 Mbps for distances shorter than 1 m, 200 Mbps at 4 m and 110 Mbps at 10 m. At longer distances, the data rate of UWB drops. This characteristic differs from the current wireless communication standards such as IEEE 802.11 and Bluetooth. As such, the current routing algorithms for ad-hoc wireless networks are not able to harness the full potential of ultra high data transfer rate of UWB. The author proposes a routing algorithm that best suits UWB-based networks.

CHAPTER 1

INTRODUCTION

1.1 MOTIVATION

Wireless technology has been around for many years. However, Personal Area Networking (PAN) became a buzzword when Bluetooth came around in 1999. Developers worldwide embraced the idea of no-frills ad-hoc interconnections of devices within a short range of 10m as a form of cable replacement. The potential of this short-range wireless communication technology is only limited by the creativity and imagination of the designer.

However, the take-up rate of Bluetooth, now also known as IEEE 802.15.1, was less than satisfactory after starting off with a bang in the 2nd quarter of 1999. One of the reasons is the relatively low data rate (1 Mbps) as compared to Wireless LAN, also known as IEEE 802.11b (11 Mbps). Bluetooth operates in the same 2.4 GHz unlicensed ISM (Industrial, Scientific and Medical) band as the IEEE 802.11b. However, unlike IEEE 802.11b, Bluetooth has a short range (10m as compared to 100m for IEEE 802.11b), requires low power to operate and low cost to produce.

In pursuit of a high rate WPAN, a task group was set up by the IEEE 802.15 Working Group to draft the standards of the High Rate Personal Area Networking (IEEE 802.15.3), targeted to achieve a data rate of 55 Mbps using the unlicensed 2.4 GHz ISM band. For multimedia applications, IEEE 802.15.3a Working Group was recently set up to investigate the feasibility of a higher rate WPAN PHY alternative to achieve up to 1000 Mbps in the form of UWB.

1.2 OBJECTIVES

The main objective of the research is to model the behaviour of data transmission within WPAN and to develop a suitable protocol for UWB-based WPAN.

1.2.1 Interference and Coexistence

The current status is that, the standard IEEE 802.15.3a is still being discussed and debated among the leading players e.g. INTEL, Motorola. As such, this project investigates the workings of Bluetooth and the extent of its interference with IEEE 802.11b WLAN. Many coexistence mechanisms are proposed. Collaborative methods are more efficient in avoiding interference, but non-collaborative methods are more desired as communication and collaboration between devices are not needed. One way to investigate the interference problem is to measure the performance of coexisting devices in the same band using a probabilistic model, which is proposed and developed in this thesis.

1.2.2 Routing Algorithms for Ad-Hoc Wireless Networks

There are many routing algorithms available for ad-hoc wireless networks currently, namely the Table-Driven Routing Protocols (DSDV, CGSR and WRP) and Source-Initiated On-Demand Protocols (AODV, DSR, ABR, SSR and TORA). Each of these routing protocols has their own merits and suits different kinds of networks configurations and traffic. However these routing protocols do not exploit the ultra high speed offered by UWB devices. As such, a new routing protocol to take advantage of the higher data rate of an UWB-based network is proposed.

1.3 **SCOPE**

The scope of the thesis will cover the following:-

- i. Survey of wireless transmission technologies.
- ii. Overview of WLAN and WPAN including the implementation of IEEE standards 802.11 and 802.15.3.
- iii. Address the issue of coexistence and its modelling using a probabilistic framework.
- iv. Survey of protocols for high data rate networks (IEEE 802.15.3) and highlights that existing network protocols are valid for up to 55 Mbps. There is a need to develop new protocols data rate in excess of 55 Mbps.
- v. The use of network simulation tool, ns2.
- vi. Proposed routing protocol for UWB-based WPAN and results of simulations.

1.4 **MAJOR CONTRIBUTIONS**

Greg Ennis's probability model on the interference between Bluetooth and WLAN is examined and refined for higher accuracy.

A new routing protocol, Weighted-Factors Routing Protocol that harnesses the ultra high data rate of an UWB network is proposed. Simulations are carried out and its performance is compared to 2 current routing algorithms, Dynamic Source Routing and Ad-Hoc On-Demand Distance Vector Routing.

1.5 ORGANISATION OF THESIS

Chapter 2 – Survey of Wireless Communication Networks reviews the fundamentals of a data network. Various wireless communication standards and WPAN standards are examined.

Chapter 3 – Coexistence examines the various collaborative and non-collaborative coexistence mechanisms for Bluetooth and IEEE 802.11b. The mathematical modelling of performance of coexisting WPAN devices in a WLAN DSSS environment are derived and improvements to existing models proposed.

Chapter 4 – Routing Protocols for UWB Wireless Personal Area Network lists the existing routing protocols for ad-hoc wireless networks. A new protocol, Weighted-Factors Routing Protocol to harness the potential of an UWB WPAN is proposed and discussed.

Chapter 5 – Simulations documents the implementation of the simulations carried out and records the results along with analysis.

Chapter 6 – Conclusions and Recommendations discusses the implications of the results and recommends future work to be done on this area.

CHAPTER 2

SURVEY OF WIRELESS COMMUNICATION NETWORKS

2.1 FUNDAMENTAL ARCHITECTURE OF A COMMUNICATION SYSTEM

To aid in the understanding of a digital communication system, a study is made of the V34 Modem [1], as the modem is a fundamental component in any communication system, be it wired or wireless. The architecture of this modem represents the generic model of a typical communication system. Although it is intended for use on the General Switched Telephone Networks (GSTN) and on point-to-point 2-wire leased telephone-typed circuits, its functions and principles are applied in all communication devices. The modem is essentially made up of the transmitter and the receiver.

2.1.1 Call Modem

The transmitter is made up of 4 logical units.

- i. The parser accepts binary input data sequence, scramble them and partition them into different groups to be passed to the next unit.
- ii. The point-select unit uses the parsed bits to select signal points from the constellation of 2D points.
- iii. The encoding unit consists of a precoder and a trellis encoder. The precoder applies a filter to the signal points to compensate for noise-whitening filter present in the V34 receiver. The trellis encoder reduce

bit error rate by ensuring the transmitted points corresponds to a proper trellis sequence.

- iv. The modulation unit performs QAM modulation of the signal points for transmission.

Figure 2.1 V34 Call Modem

2.1.2 Answer Modem

The receiver has 2 main functions, to demodulate and to decode. The received signal is first demodulated using the QAM method, transforming the analogue signal into digital points. After the Viterbi Decoder determines the sequence of transmitted points, the inverse of the receiver’s noise whitening filter is precoded much like what is done at the transmitter. Lastly, the inverse mapper recovers the input bits of an entire mapping frame.

Figure 2.2 V34 Answer Modem

2.2 ARCHITECTURE OF WIRELESS LOCAL AREA NETWORKS (WLANS)

2.2.1 Overview

In order to understand and develop new protocols in wireless personal area network, it is useful to have an insight into the basic working of a wireless network, using the tried and tested IEEE 802.11 WLAN as a reference model.

WLAN, as its name suggests, is a wireless communication standard based on the wired LAN technology. The current IEEE 802.11b supports data rates of up to 11 Mbps and uses Collision Sense Multiple Access with Collision Avoidance (CSMA/CA) [7] as the basic access method. IEEE 802.11b operates in the ISM 2.4 GHz unlicensed band. The IEEE 802.11b protocol that defines the PHY and MAC layers is shown below: -

Figure 2.3 IEEE 802.11b Layers

There are two operation modes in IEEE 802.11b. In Ad-hoc mode, wireless nodes form the network without any Access Point. Every node is able to communicate with every other node directly. Infrastructure mode consists of at least one Access Point connected to the wired network. The access points act as bridges between the wireless nodes to the wired network. The two service sets available in the infrastructure mode are Basic Service Set (BSS) and the Extended Service Set (ESS). For BSS, all wireless nodes communicate through the Access Point and don't communicate directly. ESS is a set of BSS structures where the Access Points communicate amongst each other to facilitate movement of wireless nodes between different BSSs.

2.2.2 PHY Layer

There are three specifications in the IEEE 802.11b PHY layer.

Frequency Hopping Spread Spectrum (FHSS)

79 channels that are 1 MHz apart are defined in the 2400 to 2483.5 MHz band. Using multi-level Gaussian Frequency Shift Keying (GFSK), 1 to 2 Mbps data rates can be achieved.

Direct Sequence Spread Spectrum (DSSS)

This uses 22 MHz passband, communicating with a throughput of up to 11 Mbps (using Complementary Code Keying (CCK) with Quadrature Phase Shift Keying (QPSK)).

Infrared

The most secure of the three as direct line-of-sight is needed for transmission, negating the threat of eavesdropping.

Frame Format

There are two sub-layers in the IEEE 802.11b PHY layer. The Physical Medium Dependent (PMD) sub-layer handles the wireless encoding. The Physical Layer Convergence Protocol (PLCP) sub-layer provides the carrier sense and the clear channel assessment.

The PLCP sub-layer frame format is shown below: -

Figure 2.4 PLCP Frame Format

- *PLCP Preamble*

- Synchronisation Field – 128 bits for long preamble and 56 bits for short preamble (optional; reduce overhead to maximise throughput).
- Start Frame Delimiter Field – 16 bits to mark the start of every frame.

- *PLCP Header*

- Signal (Data Rate) Field – 8 bits to indicate the speed of transmission
- Service Field – 8 bits reserved for future use.
- Length Field – 16 bits to indicate the length of the MAC Protocol Data Unit.
- Cyclic Redundancy Check (CRC) Field – 16 bits used to detect error.

2.2.3 MAC Layer

The MAC layer acts as an interface between the PHY layer and the device, supporting both infrastructure mode and ad-hoc mode.

Inter Frame Spaces

There are four types of inter frame spaces defined in the IEEE 802.11b standard.

- *Short Inter Frame Space (SIFS)* – used to separate transmissions in a single dialog. It is the period between the end of a packet transmission and the beginning of the ACK frame and is the minimum IFS. SIFS = 28 μ s for FHSS.

- *Point Coordination Inter Frame Space (PIFS)* – used by the Access Point to gain access before any other node. $PIFS = SIFS + 1$ slot time.
- *Distributed Inter Frame Space (DIFS)* – used when a node tries to start a new transmission. $DIFS = PIFS + 1$ slot time.
- *Extended Inter Frame Space (EIFS)* – used when a node could not understand a packet it received. It is used to prevent collision with a future packet belonging to the current dialog.

Exponential Back-off Algorithm

Like the Ethernet MAC, IEEE 802.11b MAC uses CSMA. However, unlike the wired Ethernet, it cannot detect collisions. Instead, it uses ACK frame for every received package to indicate a successful transmission. If the node does not receive an ACK from the recipient, it uses an exponential back-off algorithm and transmits again to avoid further collisions. Generally, the back-off algorithm is executed in the following scenarios: -

- if the node senses the medium to be busy before transmitting the packet.
- after each successful transmission
- after each retransmission

Figure 2.5 IEEE 802.11b Back-off Algorithm

Frame Format

Figure 2.6 IEEE 802.11b MAC Frame Format

- *Frame Control* – protocol version and frame type.
- *Duration/ID* – node ID used for power-save poll message frame type duration value used in Network Allocation Vector.
- *Address Fields* – up to 4 addresses.
- *Sequence Control* – fragment number and sequence number.
- *Data* – information in transmission.
- *Cyclic Redundancy Check* – 32-bit CRC.

2.2.4 Security

IEEE 802.11b employs Wired Equivalent Privacy (WEP) [7] to ensure security of the wireless network. Intruders would be unable to access the network when using similar WLAN equipment or eavesdrop.

An authentication key is used to prove the user’s identity in WEP to prevent unauthorised access to the network resources. The WEP prevents eavesdropping by using a shared secret key to initialise a pseudo random number generator to generate a sequence of pseudo random bits that are combined with the incoming or outgoing packets.

2.3 **ARCHITECTURE OF A WIRELESS PERSONAL NETWORK**
(IEEE 802.15.1)

2.3.1 Overview

Having reviewed the characteristics and operation of a WLAN, which has a coverage spanning large building interiors and adjacent outdoor areas, we are now ready to shift our focus to Wireless Personal Area Networks, WPANs – small scale networking architecture.

Bluetooth is a standard developed under IEEE 802.15.1, defining very short-range wireless communications. It is a lightweight, low cost and low power replacement for connecting-cables.

Bluetooth operates in the ISM (Industrial, Scientific and Medical) 2.4 GHz unlicensed band and uses frequency hopping to combat interference and fading.

The Bluetooth core specifications define the architecture protocol as shown below: -

Figure 2.7 Bluetooth Architecture

2.3.2 Specifications

Transmit Power

The original targeted reach of Bluetooth is 10m. However, provision for a longer range is provided too if needed.

Class	Power	Range
1	1mW (20dBm)	1m
2	2.5mW (4dBm)	10m
3	100mW (0dBm)	100m

Table 2.1 Bluetooth Transmit Power Classes

Channels

Bluetooth uses frequency-hopping spread-spectrum over direct sequence spread-spectrum to improve dynamic range and reduce near-far problem. It hops at 1600 hops/s (625μs time slots) at 79 frequencies (licensing restrictions limit Bluetooth to only 23 frequencies in Japan, France and Spain) selected in a pseudorandom manner.

The TDD (Time-Division Duplex) scheme is used and the channel is divided into time slots of 625μs each. The time slots are numbered according to the Bluetooth clock of the master device of the piconet. The numbering ranges from 0 to $2^{27}-1$ and is cyclic in nature.

The master and slave transmit packets alternately where the master starts its transmission in even-numbered time slots only and slaves in odd time-slots. Generally, one packet is transmitted per time slot with the option to extend to five time slots.

Figure 2.8 Time-Division Duplex

Figure 2.9 Multi-slots Packets

Each device has a unique 48-bit hard-wired device address and a 28-bit clock running at twice the nominal hopping frequency. Bluetooth uses binary GFSK (Gaussian Frequency Shift Keying) modulation. Its maximum data rate is 1Mbps, carrying 1 bit per symbol.

Links

Every Bluetooth device supports two types of link, ACL (Asynchronous Connection-less) link and SCO (Synchronous Communications-Oriented) link [10].

The ACL link supports a maximum data rate of 732.2bps in asymmetrical mode or 433.9kbps in symmetric mode. It uses a link-level ARQ algorithm where packets are retransmitted until the receiver sends a positive

acknowledgement to the sender. As such, no ACL data frames would be dropped in the physical channel.

The SCO link is a symmetric point-to-point link. The master device transmits on reserved slots while the slave transmits in the following slot. Received packets are accepted as they arrive with no flow control. In such a case, forward error control coding is used to lower the error rates. The SCO link is good for real-time applications such as voice.

Packets

The general packet format is shown below: -

Figure 2.10 Bluetooth Packet Format

The size of the access code and header are fixed at 72 bits and 54 bits respectively while the payload ranges from 0 to 2745 bits.

Service Discovery Protocol (SDP)

The SDP provides a way for devices to discover the availabilities of services and their characteristics within range. It provides only the information about the services available, but not the access to these services.

Piconets / Scatternets

When a master device is connected with one to seven slave devices, a piconet is formed. Bluetooth is a master driven centralised system. The master controls the scheduling for transmissions and Slaves are strictly synchronised to the

master. Considering the dynamic nature of devices entering and leaving the piconet, the roles of the master and slave can be exchanged.

There are four possible operational modes a slave device can be in: *Active*, *Sniff*, *Hold* and *Park*. In *Active*, *Sniff* or *Hold* modes, the slave has a 3-bit address (AM_ADDR), which is used when communicating with the master. As such, up to seven slaves can be connected to a master device. In the *Park* mode, the slave uses an 8-bit address (PM_ADDR, AR_ADDR), thus more than seven slaves can be connected. However, a slave in *Park* mode is inactive in the piconet. A *Parked* slave listens to the master periodically so as to remain synchronised. In the *Hold* mode, a slave is inactive for a fixed time interval while a slave in *Sniff* Mode wakes up periodically to listen for master transmission.

Scatternet [12] is formed when multiple piconets overlap each other. Each piconet can have only one master device. Slaves can however, exist in different piconets. Furthermore, a slave in one piconet can be a master in another piconet.

Figure 2.11 Scatternet

2.3.3 Security

Three different units are used to achieve security at the link layer [11]. The Bluetooth Device Address (BD_ADDR) is a unique 48-bit public address assigned to each Bluetooth unit. The second entity is a 128-bit secret key, which is the private user key used for authentication. The third entity is also a secret key. It has a configurable length of 8-128 bits used for encryption. Both the authentication key and the encryption key are derived during initialisation and are never disclosed.

2.4 **IEEE 802.15.3 HIGH RATE DATA WIRELESS PERSONAL AREA NETWORK (up to 55 Mbps)**

2.4.1 Overview

Similar to Bluetooth, IEEE 802.15.3 is a standard for low power, low cost, short range, peer-to-peer ad-hoc networking. On top of that, IEEE 802.15.3 boasts a high maximum data rate of 55Mbps and QoS [15]. As such, IEEE 802.15.3 is well suited for multimedia applications where high data rate and quality are essential. IEEE 802.15.3 signals occupy a 15 MHz bandwidth in the unlicensed 2.4GHz ISM band.

2.4.2 Specifications

Modulation and Coding

QAM is used in IEEE 802.15.3 with a symbol rate of 11 Mbaud. Without coding, a QPSK modulation is able to achieve 22Mbps. The data rates of 11, 33, 44 and 55Mbps can be achieved using trellis-coded QPSK, 16/32/64-QAM respectively [14].

Superframe

Figure 2.12 IEEE 802.15.3 Superframe Structure

The superframe consists of three parts:

- i. *Beacon* – Carries control information to the whole piconet, allocates GTS (Guaranteed Time Slots) per stream index to the current superframe and provides time synchronisation.
- ii. *Contention Period (CP)* – Used for authentication request/response, CTR (Channel Time Requests) and other command frames. The piconet controller (PNC) may replace the CP slot with Manage Time Slot (NTS) when necessary.
- iii. *Contention Free Period (CFP)* – Unidirectional GTS assigned by the PNC for asynchronous and isochronous data streams.

Guaranteed Time Slot (GTS)

Different GTSS may have different persistence. Dynamic GTSS have varying positions in different superframes. Pseudo-static GTSS may modify the position, but need to attain approval from both the Tx and Rx devices.

Management Time Slot (MTS)

MTSs are used in lieu of the CP to communicate commands. The number of MTS per superframe is allocated by the PNC.

Quality of Service (QoS)

QoS is attained through reservation. The device queries the PNC to see if the QoS requirements could be granted by the Channel Time (CT) Manager. Such a negotiation between the device and the PNC reduces the complexity.

2.5 IEEE 802.15.3a HIGHER DATA RATE WPAN

2.5.1 Overview

In order to cater for data rates in excess of 55 Mbps for WPAN, the IEEE has initiated a working group, IEEE 802.15.3a, which focuses on using UWB as a physical layer. UWB is also known as impulse or baseband radio as the transmission is carrier-free and uses narrow and extremely low power pulses typically on the order of nanoseconds, thereby spreading the radio signal very thinly [29]. As such the signal occupies a very broad spectrum. Having an extremely broad bandwidth makes the signal more robust to interferences and improves its time-of-arrival resolution.

The short pulses of UWB eliminate significant multipath fading and the fading margin in the link budget, thus achieving low transmission power operation [25]. The significantly large bandwidth also means that it can accommodate a large number of users. The fact that UWB is carrier-free implies that the cost of manufacturing is lower than the carrier-based systems. And the ability to operate in the lowest possible frequency enables it to penetrate solid material better.

UWB is currently being considered by IEEE 802.15.3a Work Group to be used for the PHY of IEEE 802.15.3a to support wireless data transfer of up to 500 Mbps (at 1m; 200 Mbps at 4m and 110 Mbps at 10m). It meets the three most important factors of a high rate WPAN, namely, low power, low cost and high data throughput. Another attribute of UWB that is useful in a WPAN is the capability to perform precise geo-location of other UWB devices within the network [25].

One of the advantages of UWB is that it appears to other RF technologies as noise, while supporting high data rates and offers data security. As such, coexistence between current various wireless technologies is achievable effortlessly.

Figure 2.13 UWB Frequency Spectrums

UWB is fundamentally different from other RF technologies currently available. While the current RF technologies use narrowband frequency carrier to transmit data, UWB transmits extremely short digital pulses (1 to 1000 picoseconds) across a spectrum of frequencies (3.1GHz to 10.6GHz as defined by the Federal Communications Commission). The Federal Communications Commission (FCC) allocates 7.5 GHz of unlicensed spectrum to the UWB band. UWB communications require -10 dB fractional bandwidth of more than 20% or a -10 dB bandwidth of more than 500 MHz [40]. Fractional bandwidth is defined by the expression $2(f_H - f_L)/(f_H + f_L)$.

Characteristics	IEEE 802.15.3.1 Bluetooth	IEEE 802.11.b WLAN	IEEE 802.11a WLAN	IEEE 802.15.3	IEEE 802.15.3a UWB
Max data rate	1 Mbps	11 Mbps	24 Mbps mandatory; 54 Mbps optional	11 Mbps (QPSK) to 55Mbps (64 QAM) mandatory: ≥ 22 Mbps	110 Mbps (10m) 200 Mbps (4m) mandatory; 500 Mbps (1m) optional
Max distance	10m	100m	50m	10m	10m
Frequency allocation	2.4 GHz (ISM)	2.4 GHz (ISM)	5 GHz UNII (5.15–5.35 + 5.725-5.825) GHz	2.4 GHz (ISM) 2.4-2.4835 GHz	3.1-10.6 GHz
Channel bandwidth	1 MHz	25 MHz	20 MHz	15 MHz	Min 500 MHz Max 7.5 GHz
Number of RF channels	79	3	12 US 8 EU 4 Japan	5	1-15
Modulation	GFSK	11 MBaud QPSK (CCK Coding)	COFDM BPSK, QPSK, 16 QAM	DQPSK 16/32/64 QAM	BPSK, QPSK
Spreading	DS-FH	CCK	OFDM	-	Multiband
Approx # PHY power consumption	BT (~40-100mW)	~4 BT	~6 BT	-	~2-3 BT
Approx cost #	BT (~5USD)	~4 BT	~5 BT	-	~1-2 BT

Table 2.2 Summary of Some Leading WLAN/WPAN Standards [41]

2.5.2 Theory of Impulse Radio

Impulse Radio has been utilised as the physical model in the design of the UWB transmission system (in [42] [43] [44]). Impulse Radio uses baseband pulses of very short duration, typically in the order of nanoseconds, thereby spreading the energy of the radio signal very thinly from near d.c. to a few gigahertz. Such transmission relies on a specific unchanging waveform to be transmitted in time with pulse position modulation. The monopulse waveform can be any single period wave that goes to zero at infinity. In order to create multiple accesses in impulse radio systems, a technique known as time hopping

allows transmitted pulses to have additional delays added, allowing only the receiver with the same delay codes to demodulate the signal.

Time-Hopping Format Using Impulses

The following formula shows the k th transmitter's output signal in a typical impulse radio:

$$S_{tr}^{(k)}(t^{(k)}) = \sum_{j=-\infty}^{\infty} \omega_{tr}(t^{(k)} - jT - c_j^{(k)}T_c - \delta d_{j/N_s}^{(k)}) \quad (2.1)$$

where,

- $t^{(k)}$ - k th transmitter's clock time
- ω_{tr} -transmitted pulse waveform
- T_f -pulse repetition time (frame time)
- $c_j^{(k)}$ -time hopping sequence (distinct time shift pattern)
- T_c -duration of addressable time bins
- j -indicates j th monocycle within each pulse train
- δ -Modulation index
- $d_{j/N_s}^{(k)}$ -data sequence

Every user k is assigned a distinctive time shift pattern $c_j^{(k)}$ (a time-hopping sequence), in order to prevent collisions due to multiple access. A time shift of $c_j^{(k)}T_c$ seconds to the j th monocycle in the pulse train can be provided. Typically, each frame time, T_f is a hundred to a thousand times the monocycle width.

Illustration of Time-Hopping Principle

To further explain the working principle of the impulse radio, a simplified model is used. The frame time T_f consists of 4 period of T_c (duration of addressable time delay). Only 3 frames are considered. T_f is also assumed to be an exact multiple of T_c . It must be noted in reality that the frame time is at least hundred times to thousandth times the monocycle width. The time interval to read the output of the monocycle correlator and to reset the correlator is assumed to be negligible. Within each T_c , the monocycle pulse will undergo a shift depending on the modulation index and data sequence.

Figure 2.14 Time Hopping Principle

For simplicity, there are only 2 transmitters in the example, user 1($k=1$) and user 2 ($k=2$). User 1 is allocated a code sequence, $c_j^{(k)}$ of 0, 3, 2 and user 2 is of 2, 1, 3. According to the given code sequence, user 1 and 2 will shift the pulses within each frame, for the same baseband pulse that illustrated in Figure 2.14(a). Each j th monocycle undergoes a shift of $c_j^{(k)}T_c$ seconds.

The first monopulse does not undergo any further shift since the code sequence is 0 (shown in Figure 2.14(b)). At $j=2$, the code for that frame is 3. Thus, the monopulse at that frame will shift by 3 periods of T_c . In the same way, the 3rd pulse is shifted by 2 periods of T_c . Accordingly, user 2 will shift each monopulse according to the time hopping code. The output is shown in Figure 2.14(c).

Figure 2.14(d) illustrates the combined received signal for the 2 impulse radios transmitting within range of a receiver. Negligible delay is assumed between transmission from user 1 and 2 and the reception shown in Figure 2.14(d) in order to simplify the example.

Illustration of Pulse Position Modulation Principle

The previous example explained how impulse radio systems accommodate multiple users and avoid interference. The next example will explain how data symbols are modulated on the waveform. Taking a simple example of binary data, the pulse waveform is shifted within the T_c to express the designated value.

In Figure 2.15(a), the pulse waveform within one period of T_c represents symbol of '0', while Figure 2.15(b) represents that of binary value '1'. The data modulation depends on implementation. The same 2 figures could represent symbol values of '-1' and '1' as well. In the same way, M-ary symbols could be represented within each period T_c with an appropriate time shift factored in.

Figure 2.15 Modulated PPM

Impulse Radio Receiver

For each impulse radio receiver in a multiple-access system, the composite received signal is as following:

$$r(t) = \sum_{k=1}^{Nu} A_k S_{rec}^{(k)}(t - \tau_k) + n(t) \quad (2.2)$$

The destination receiver does not only detect the signal by the source node, but also captures the signal energy by all other nodes within range of itself. A_k models the propagation attenuation that the signal suffers. The random variable, τ_k represents the time asynchronism between the clock of the transmitter k and the receiver. $n(t)$ represents other interference present at the receiver input.

2.5.3 Advantages of UWB

Low Power

UWB consumes significantly lower power than conventional narrowband RF systems as it transmits extremely short digital pulses rather than continuous modulated sine waves. On top of that, the transmitting power varies depending on distance. The transmitting power might even be negligible as it ranges in microwatts while the chipset itself consumes power in milliwatts.

Low Cost

Unlike traditional RF systems, UWB does not need high frequency carrier signal. This property also constitutes a low cost, low complexity radio system for the UWB.

High Data Throughput

UWB operates in the time domain and transmits ultra-short monocycles in a pseudorandom noise (PN) sequence, which results in ultra-wideband. Pulse Position Modulation (PPM) is used to transmit millions to billions of pulses per second in picosecond-range low power radio bursts, thus enabling UWB to reach throughputs of up to 1000 Mbps.

Immunity to Interference / Low Interference to Existing RF Technologies

Using such a wide bandwidth indicates that a pulse can only be disrupted if there is interference throughout the entire frequency spectrum it occupies. Thus, interferences from other narrowband signals are not threatening. Some other advantages of using such a wide bandwidth are wall-penetrating capability and high immunity to multi-path interference.

The power spectral density of UWB is below the thermal noise floor. To other RF technologies, UWB signals appear to them as noise and the interference threat is much like white noise.

High Level of Security

As described above, UWB transmissions appear to be like white noise to non-UWB receivers. As such, it is extremely difficult to decode UWB signals without knowing the PN sequence.

2.5.4 Disadvantages of UWB

Technical Difficulties

Implementing UWB is not without difficulties. It is challenging to detect a signal quickly and accurately below the thermal noise floor.

Near-Far Problem

UWB is susceptible to the near-far problem where a nearer UWB device might block the reception of a further UWB device.

Short Range

UWB is suited for short-range transmission, which is ideal for WPAN. As defined by IEEE 802.15.3a Work Group, the maximum distance to attain a speed of 100Mbps is 10m. The range can be increased further, but more power has to be consumed.

Interference with GPS and 3G/UMTS

Oppositions of UWB have pointed out that UWB would interfere with 3G/UMTS network. Proponents of UWB however is sceptical about the claim, arguing that there's no way UWB would interfere with UMTS if UMTS can even coexist with devices such as cordless phones, microwave oven or even IEEE 802.11b, which operate closer to the 3G frequency and have a million times transmit power higher than UWB.

The NTIA (National Telecommunications Information Administration) claimed that UWB could make it more difficult for GPS receivers to lock onto satellites while NASA suggested that UWB could interfere with flight instruments on planes.

CHAPTER 3

COEXISTENCE

3.1 COEXISTENCE OF BLUETOOTH AND WLAN

3.1.1 Overview

Both Bluetooth and WLAN use the ISM 2.4GHz band. Interference is inevitable especially if both devices are collocated, i.e. in a notebook PC. At closer range, the signal strength of the transmitter is higher, thus causing significant interference. The signal degradation is most severe at $<0.5\text{m}$ and decreases gradually till 2m. At $>2\text{m}$, the Bluetooth and WLAN do not interfere with each other [18].

Bluetooth is designed to exploit the entire spectrum with 79 hops that are 1 MHz apart from each other. While interference occurs, Bluetooth tries again by hopping to the next channel while WLAN issues Automatic Repeat Request (ARQ) and slows down to lower the Bit Error Rate (BER).

IEEE 802.11 has three different PHY specifications, namely, Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) and Infrared (IR). Similar to Bluetooth, the FHSS of WLAN has 79 channels (2400 to 2483.5 MHz) spaced 1 MHz apart. Using FHSS, WLAN can achieve rates of up to 2 Mbps. Interference is most serious when WLAN uses DSSS for higher data rates (up to 11 Mbps). DSSS occupies a relatively wideband of 22 MHz, thus is 22 times more likely to suffer from interference.

3.1.2 Collaborative Solutions

With collaborative methods, the Bluetooth device would have to exchange information with the WLAN device. In this way, an algorithm can be worked out to schedule the traffic of the devices to share the common channel. Collaborative methods are more suited to collocated configurations.

Dual-Mode Radio Switching

For collocated configurations, dual-mode radio switching alternates the operations of the different radio systems by suspending one of them while the other is transmitting. Only one of the radios is turned on at any one time, thus minimising the risk of interference to zero.

Although interference is minimal, the throughput suffers. The time used in stopping and initialising the radios posts a drop in overall performance. In addition, the SCO (voice) link of Bluetooth is time-sensitive and cannot afford to be interrupted with repetitive multiplexing.

MEHTA

The MEHTA [21] engine from Mobilian Corporation manages packet transmission requests and makes decisions on the transmission of a packet based on parameters such as signal strength and the difference between the centre frequencies of WLAN and Bluetooth. SCO links are possible.

Figure 3.1 MEHTA Engine (Source: Mobilian Corporation)

3.1.3 Non-Collaborative Solutions

Non-collaborative techniques do not require the communication between the two different systems. With no prior knowledge of other systems operating nearby, each system detects for excessive noise in the channel before deciding to send data packets.

Adaptive Frequency Hopping (AFH)

Adaptive Frequency Hopping allows a Bluetooth device to select and reduce the number of channels it hops across, freeing up channels for other devices. A typical Bluetooth device in AFH mode hops to around 15 channels and frees up 68 channels.

The AFH device pre-scans the channel during idle time and applies a score to each channel. Channels to be used are selected based on the scores given. Channels that experience little or no interference over an extended period of time will be labelled as clear channels. The clear channels are then selected for transmission.

Adaptive Packet Selection and Scheduling

This feature is a Bluetooth MAC level enhancement that uses a Frequency Usage Table to save statistics of channels that had encountered interference. From the data stored in the table, the packet scheduling algorithms schedule transmissions to happen only when a good channel is hopped onto.

3.2 MATHEMATICAL MODELLING OF PERFORMANCE OF COEXISTING WPAN DEVICES IN WLAN DSSS ENVIRONMENT

3.2.1 Overview

From findings of Mobilian Corporation, significant degradation of throughput occurs when Bluetooth and IEEE 802.11b operates within 0.5m of each other. To investigate the coexistence issue of Bluetooth and IEEE 802.11b in close proximity (less than 0.5m), the probability of collisions between the Bluetooth packets and the IEEE 802.11b packets is examined. A collision of the Bluetooth packets and IEEE 802.11b packets occur when frequency overlapping occurs during a time overlap.

3.2.2 Greg Ennis's Probability Model

In the widely accepted probability model [28] by Greg Ennis,

L	=	Dwell duration of an IEEE 802.11b packet
H	=	Dwell duration of a Bluetooth packet
d	=	Time from the last Bluetooth timeslot to the start of 802.11b packet

Figure 3.2 Greg Ennis's Time Overlap Model

Time Overlap

When a time overlap occurs, multiple Bluetooth packets would likely to be overlapped by the IEEE 802.11b packet. The number of Bluetooth packets overlapped, N , is determined by d . The equations below depict the probabilities: -

$$P(N = \lceil L/H \rceil) = \lceil L/H \rceil - L/H \quad , \text{ if } 0 \leq d \leq \lceil L/H \rceil \times H - L \quad (3.1)$$

$$P(N = \lceil L/H \rceil + 1) = 1 - \lceil L/H \rceil + L/H \quad , \text{ if } \lceil L/H \rceil \times H - L < d \leq H \quad (3.2)$$

where $\lceil x \rceil$ is the least integer $\geq x$

Using Figure 3.2 as an example,

$$P(N = \lceil 1.3H/H \rceil) = \lceil 1.3H/H \rceil - 1.3H/H$$

$$P(N = 2) = 2 - 1.3 = 0.7$$

$$P(N = \lceil 1.3H/H \rceil + 1) = 1 - \lceil 1.3H/H \rceil + 1.3H/H$$

$$P(N = 3) = 1 - 2 + 1.3 = 0.3$$

When $d > 0.7H$, 3 Bluetooth packets are overlapped. However, if $d \leq 0.7H$, only 2 Bluetooth packets will be overlapped.

Frequency Overlap

In the event of a time overlap, a frequency overlap has to occur too if a collision were to take place. The IEEE 802.11b DSSS can have 3 non-overlapping 22-MHz channels within the 83.5-MHz bandwidth of the 2.4 GHz frequency band [7]. At any given time, only 1 channel is in use. Thus in Greg Ennis's model [28], it is given that the probability that at any given time, a Bluetooth transmitter is on a narrowband channel outside a given wideband IEEE 802.11b DSSS channel is $2/3$. And if an IEEE 802.11b packet overlaps N Bluetooth dwell periods, the probability of no frequency overlap is $(2/3)^N$.

Probability of No Collision

Combining time and frequency overlapping probabilities, the probability of no collision can be derived: -

$$P(\text{no collision}) = (2/3)^{\lceil L/H \rceil} (\lceil L/H \rceil - L/H) + (2/3)^{(\lceil L/H \rceil + 1)} (1 - \lceil L/H \rceil + L/H) \quad (3.3)$$

3.2.3 Proposed Probability Model

Ennis's probability model [28] presented a simple probability model to estimate the probability of no collision during a time overlap. However, the model did not consider the idle time during a Bluetooth transmission. A collision during idle time will not result in any data lost or corrupted for that timeslot.

In Ennis's model, there is no idle time in-between the dwell durations of the Bluetooth packets. Thus, the packets are assumed to be 625 bits (at 1 bit/ μ s). However, Bluetooth has numerous packet types that have varying packet sizes [10] as shown in Table 2.2 below. A typical Bluetooth packet is taken to be 366 bits long.

Data Type	Payload Header (bytes)	User Payload (bytes)	FEC	CRC
DM1	1	0-17	2/3	Yes
DH1	1	0-27	No	Yes
DM3	2	0-121	2/3	Yes
DH3	2	0-183	No	Yes
DM5	2	0-224	2/3	Yes
DH5	2	0-339	No	Yes
AUX1	1	0-29	No	No
HV1	N/A	10	1/3	No
HV3	N/A	20	2/3	No
HV5	N/A	30	No	No
DV	1 for data	10+(0-9) for data	2/3 for data	Yes for data

Table 3.1 Bluetooth Packet Types

In this report, the author proposed a probability model that takes the idle time into account. With reference to Figure 3.3 below, only 2 Bluetooth packets would be overlapped if a time overlap occurs as opposed to 3 packets overlapped in Greg Ennis’s probability model. If the IEEE 802.11b packet starts only after the idle time of the first timeslot sets in, the Bluetooth packet in the first timeslot is unaffected.

- B_T

=

Duration of a Bluetooth timeslot (625μs based on 1600 hops/s)
- H

=

Dwell duration of a Bluetooth packet (typically 366μs)
- T_W

=

Dwell duration of a IEEE 802.11b packet
- x

=

Time from the last Bluetooth timeslot to the start of 802.11b packet

Figure 3.3 Time Overlap of Bluetooth and IEEE 802.11b Packets

Time Overlap

Generally, the duration of an IEEE 802.11b packet is longer than a Bluetooth timeslot. Thus, more than one Bluetooth packets could be corrupted when a time overlap occurs. The number of Bluetooth packets overlapped during a time overlap is dependent on three factors: -

- i. Dwell duration, T_w , of the IEEE 802.11b packet (dependent on fragment size and data rate).
- ii. Dwell duration, H , of the Bluetooth packet (dependent on the packet size).
- iii. Time offset, x , from the last Bluetooth timeslot to the start of the IEEE 802.11b packet.

To help simplify the study, the following assumptions are made. The packet size of the Bluetooth is 366 bits, thus $H = 366\mu s$. The highest data rate (11 Mbps) of IEEE 802.11b is used. And as the largest possible fragment size of an IEEE 802.11b packet is 1500 bytes, the maximum value of T_w to be taken into consideration in this study is calculated below.

$$\text{Max } T_w = \frac{1500 \times 8}{11 \times 1024 \times 1024} s = 1040 \mu s$$

Since $\text{Max } T_w$ is $1040\mu s$ which is $< 2B_T$, the number of Bluetooth packets overlapped, $n \leq 3$. The probability function differs with different conditions of T_w .

Condition I: when $0 < T_W \leq B_T - H$

Figure 3.4 Time Overlap Figure (I)

When T_W is shorter than the Bluetooth idle time, if the IEEE 802.11b dwell duration is within the idle time, no Bluetooth packet will be overlapped. Otherwise, 1 Bluetooth packet will be overlapped as shown in Figure 3.4 above. Thus, the probability function, $P(n)$, is shown below: -

$$P(0) = \frac{B_T - T_W - H}{B_T}, \text{ when } H \leq x \leq B_T - T_W$$

$$P(1) = \frac{H - 0}{B_T} + \frac{B_T - (B_T - T_W)}{B_T}, \text{ when } 0 \leq x < H \text{ or } B_T - T_W < x < B_T$$

$$= \frac{T_W + H}{B_T}$$

Condition II: when $B_T - H < T_W \leq B_T$

Figure 3.5 Time Overlap Figure (II)

When T_W is longer than the idle time but shorter than a Bluetooth timeslot, 1 or 2 Bluetooth packets would be overlapped as illustrated in Figure 3.5 above. The probability function, $P(n)$, is shown below: -

$$P(1) = \frac{B_T - T_W - 0}{B_T} + \frac{B_T - H}{B_T} \quad , \text{ when } 0 \leq x \leq B_T - T_W \text{ or } H \leq x \leq B_T$$

$$= \frac{2B_T - T_W - H}{B_T}$$

$$P(2) = \frac{T_W - B_T + H}{B_T} \quad , \text{ when } B_T - T_W < x < H$$

Condition III: when $B_T < T_W \leq 2B_T - H$

Figure 3.6 Time Overlap Figure (III)

$$P(1) = \frac{2B_T - T_W - H}{B_T} \quad , \text{ when } H \leq x \leq 2B_T - T_W$$

$$P(2) = \frac{H - 0}{B_T} + \frac{B_T - (2B_T - T_W)}{B_T} \quad , \text{ when } 0 \leq x < H \text{ or } 2B_T - T_W < x < B_T$$

$$= \frac{T_W - B_T + H}{B_T}$$

Condition IV: when $2B_T - H < T_W \leq 3B_T - H$

Figure 3.7 Time Overlap Figure (IV)

$$\begin{aligned}
P(2) &= \frac{2B_T - T_W - 0}{B_T} + \frac{B_T - H}{B_T}, \text{ when } 0 \leq x \leq 2B_T - T_W \text{ or } H \leq x < B_T \\
&= \frac{3B_T - T_W - H}{B_T} \\
P(3) &= \frac{T_W - 2B_T + H}{B_T}, \text{ when } 2B_T - T_W < x < H
\end{aligned}$$

General Time Overlap Probability Function

With the exception of Condition II, it can be observed that the upper bound limit of T_W for each of the conditions influence the respective probability functions. However, the probability function of Condition II is identical to Condition III. As such, Condition II is combined with Condition III, giving An extended condition of $B_T - H < T_W \leq 2B_T - H$. So let U be the upper bound limit of the T_W for each of the conditions. The general probability function can be written as: -

$$\begin{aligned}
P(n) &= \frac{U - T_W}{B_T} & \left| \begin{array}{l} \text{when } U = B_T - H, n = 0 \\ \text{when } U = 2B_T - H, n = 1 \\ \text{when } U = 3B_T - H, n = 2 \end{array} \right. \\
P(n+1) &= \frac{T_W + B_T - U}{B_T} & \quad (3.4)
\end{aligned}$$

Frequency Overlap

The IEEE 802.11b employs DSSS, which uses 22 of the 79 1-MHz channels while Bluetooth employs FHSS with 79 hops. Greg Ennis's model considered the 3 non-overlapping channels that the IEEE 802.11b DSSS occupies in the 2.4 GHz frequency band. However, there are complications when overlapping channels are taken in account (11 overlapping sub-channels are available for IEEE 802.11b DSSS across the 83.5 MHz of the 2.4 GHz frequency band) [21].

To avoid complications, the probability of no frequency overlap in event of a time overlap used in the proposed model in this report is 57/79. And if an IEEE 802.11b packet overlaps n Bluetooth dwell periods, the probability of no frequency overlap is $(57/79)^n$.

Probability of No Collision

Combining the time overlap and frequency overlap probability functions, the overall probability of no collision occurring is shown below: -

$$P(\text{no collision}) = (57/79)^n [P(n)] + (57/79)^{(n+1)} [P(n+1)] \quad (3.5)$$

3.3 COMPARISON OF PROPOSED MODEL AND GREG ENNIS'S MODEL

3.3.1 Comparison of Packet Error Rates

The Packet Error Rate (PER) is a better gauge of network performance than the probability of no collision. Assuming that a single corrupted bit is sufficient to corrupt an entire data packet, the PER is simply given by: -

$$PER = 1 - P(\text{no collision}) \quad (3.6)$$

For Greg Ennis's model, its $P(\text{no collision})$ is expressed in Equation 3.2. Thus,

$$PER = 1 - \left[(2/3)^{\lceil L/H \rceil} (\lceil L/H \rceil - L/H) + (2/3)^{(\lceil L/H \rceil + 1)} (1 - \lceil L/H \rceil + L/H) \right] \quad (3.7)$$

For the proposed model, its $P(\text{no collision})$ is expressed in Equation 3.6. Thus,

$$PER = 1 - \left[(57/79)^n [P(n)] + (57/79)^{(n+1)} [P(n+1)] \right] \quad (3.8)$$

Figure 3.8 PER of Greg Ennis’s Model and the Proposed Model

The PER plots of Greg Ennis’s and the proposed models are shown in Figure 3.8 above, according to the Equation 3.7 and 3.8. As expected, the proposed probability model has a lower PER than Greg Ennis’s probability model due to the consideration of idle time in the former.

The two probability models discussed in this section consider only the probability of overlapping of data packets in the time domain and frequency domain. To have an even more accurate model, more parameters such as number of devices within close proximity, distance between devices have to be considered.

CHAPTER 4

ROUTING PROTOCOLS FOR UWB AD-HOC WIRELESS PERSONAL AREA NETWORK

4.1 OVERVIEW

Ad-hoc network has no infrastructure and is mobile. All the nodes are mobile and are able to connect with each other dynamically in an arbitrary manner. Unlike infrastructured networks, there are no fixed routers in a wireless ad-hoc network as each and every node of an ad-hoc network functions as a router which discover and maintain routes to other nodes in the network.

Section 4.2 and 4.3 examine the 2 categories of existing routing protocols used for ad-hoc networks. Table-Driven Routing Protocols are discussed in Section 4.2 and Source-Initiated On-Demand Routing Protocols are examined in Section 4.3. Section 4.4 documents a proposed routing protocol targeted at ad-hoc networks for UWB to harness the full potential of an UWB network.

4.2 TABLE-DRIVEN ROUTING PROTOCOLS

Table-driven routing protocols require each and every node to maintain tables that contain consistent and up-to-date routing information between every node in the network.

4.2.1 Destination-Sequenced Distance-Vector Routing (DSDV)

For Destination-Sequenced Distance-Vector Routing (DSDV) [31], every node maintains a routing table that records all the possible destinations and number

of hops to each destination node within the network. Sequence numbers are assigned to each entry by the destination node. The sequence numbers help the nodes to differentiate fresh routes from the old ones and thus avoid routing loops. The tables are periodically updated throughout the network through “full dump” packets that carry all available routing information or smaller “incremental” packets that relay only information that has changed since the last full dump.

4.2.2 Clusterhead Gateway Switch Routing (CGSR)

Nodes in the Clusterhead Gateway Switch Routing (CGSR) by C.-C. Chiang *et al.* [32] belong to clusters where each cluster has a clusterhead that actually do the routing for all the other nodes in the cluster. All the nodes in a certain cluster are within 1 hop to the clusterhead. If a node exists in 2 clusters, it becomes a gateway node which links the 2 clusters together. Figure 4.1 shows how CGSR works.

Figure 4.1 Clusterhead Gateway Switch Routing

Although CGSR uses DSDV as the underlying routing scheme, CGSR is hierarchical with cluster heads and gateways as compared to a DSDV flat network. On top of routing tables, each node has to maintain a cluster member table which stores the destination clusterhead for each node in the network.

4.2.3 Wireless Routing Protocol (WRP)

In the Wireless Routing Protocol (WRP) [33], each node maintains 4 tables, distance table, routing table, link cost table and message retransmission list (MRL) table. Every entry in the MRL table records the sequence number of update messages, retransmission counter, list of updates sent and an acknowledgement-required flag vector with 1 entry per neighbour. Nodes inform each other of link changes via update messages between neighbouring nodes. Nodes learn the existence of their neighbours by receiving messages from them. If a node has no messages to send, a “hello” message has to be sent within a specified period of time to maintain connectivity.

WRP achieves loop freedom and avoids count-to-infinity problem by making every node perform consistency checks on information given by its neighbours.

4.3 SOURCE-INITIATED ON-DEMAND ROUTING

Source-Initiated On-Demand Routing [34] identifies routes only when the source node requires a route to its destination. Once the route discovery process is initiated, it will end only when a suitable route is found or when all possible route permutations are examined. When a route is established, it will be maintained by some form of route maintenance procedure until the destination becomes inaccessible or no longer desirable.

4.3.1 Ad-Hoc On-Demand Distance Vector Routing (AODV)

Ad-Hoc On-Demand Distance Vector Routing (AODV) [35] improves upon DSDV. Broadcasts are minimised by creating routes only on-demand compared to maintaining a complete list of routes as DSDV requires. Nodes that are not selected within the path do not have to maintain any routing information or tables.

The path discovery process is initiated at the source node when there is no current valid route from the source node to the destination node. Route request (RREQ) packets are broadcast to its neighbours which in turn forward the request to their neighbours until the destination node or an intermediate node with a fresher route to the destination node is found [34] (Figure 4.2(a)). Again, sequence numbers are used to ensure that all the routes are loop-free and have the most updated route information. Each node has its own sequence number and broadcast ID which is incremented for each RREQ the node initiates. The broadcast ID and sequence number uniquely identifies the RREQ. Intermediate nodes which have routes to the destination with corresponding destination sequence number greater than or equal to that contained in the RREQ can reply to it with a RREP.

Figure 4.2 AODV Route Discovery

When forwarding the RREQ, the intermediate nodes record the address of their neighbours which the first copy of the broadcast packet is received, thus establishing the reverse path. When the RREQ finally reaches the destination node or an intermediate node with a fresher route, a route reply (RREP) packet is unicast back to the neighbour it receives the RREQ from (Figure 4.2(b)). When the RREP is unicast back to the source node along the reverse path, nodes along the path set up forward route entries in their route tables, pointing to the node from which the RREP came from. These forward route entries denote an active forward route.

4.3.2 Dynamic Source Routing (DSR)

Nodes using Dynamic Source Routing (DSR) [36] maintain route caches. The route information is continually updated as soon as new routes are discovered. When a node needs to send a packet to some destination, it first checks with the route cache for existing route. If there is an existing route which has not expired, the route will be used to send the packet. If there is no existing route to the destination, a route discovery process will be initiated by broadcasting a route request packet which contains the address of the destination, the address of the source node and a unique identification number. Upon receiving the route request packet, each node will check whether if it knows a route to the destination. If there is no known route, it adds its own address to the route record of the packet and forwards it to other nodes. During this process, the sequence of hops is also recorded.

Figure 4.3 DSR Route Record Creation

Once the route request reaches the destination or an intermediate node which knows an unexpired route to the destination, a route reply is generated. Route maintenance is carried out by sending of route error packets along with acknowledgements.

4.3.3 Associativity-Based Routing (ABR)

Associativity-Based Routing (ABR) [37] selects route based on the degree of associativity of stability of the nodes where each node periodically generates a beacon to signal its existence. For every beacon received, the associativity tick of the current node with respect to the beaconing node is incremented. The associativity stability is defined by the connection stability of a node with respect to another node over time and space. A node with low mobility has a high degree of associativity stability and vice versa. When the node or its any of its neighbours move out of proximity, the associativity ticks are reset. The objective is to derive longer-lived routes for the network.

The route discovery process is a broadcast query (BQ) and await-reply cycle (BQ-REPLY). The source node broadcasts a BQ message to find nodes that have a route to the destination. All the intermediate nodes that receive the BQ message add their addresses and their associativity ticks with their neighbours along with the QoS information to the query packet. An intermediate node deletes its upstream neighbour's associativity tick entries and retains only the entry concerned with itself and its upstream node. Thus each packet that arrives at the destination node contains the associativity ticks of the nodes along the route to the destination and the destination node selects the best route after examining the associativity ticks along each path. If there are multiple paths with the same degree of associativity stability, the route with the least number of hops will be selected. Once a route is chosen, the destination node sends a reply packet back to the source along the path and each node along this path marks their route as a valid route.

In event of an invalid route erasure, partial route discovery, valid route updates and new route discovery, a route reconstruction process is initiated. When the source node is moved, a new BQ-REPLY process is initiated as shown in Figure 4.4(a). At the same time, the route notification (RN[1]) message is sent to notify the downstream nodes to erase the route entries. When the destination node is moved, the immediate upstream node delete its route and determines if the node is still to be reached by a localised query (LQ[H]) process (H is the number of hops from the upstream node to the destination node). If the destination is able to receive the LQ packet, it implies that it has found the best partial route (refer to Figure 4.4(b)). If the destination node is not able to receive the LQ packet, the process backtracks to the next upstream node. The RN[0] message is sent to the upstream node to erase invalid route and at the same time inform the node to start the LQ[H] process. If the backtracking spans more than half the initial nodes involved, the LQ process stops and a new BQ process is initiated from the source again.

When a route is no longer needed, the source node broadcasts a Route Delete (RD) message so that all the nodes along the route and the route tables are updated.

Figure 4.4 Route Maintenance in ABR

4.3.4 Signal Stability Routing (SSR)

Signal Stability Routing (SSR) decides on which route to take based on the signal strength between nodes and on the stability of a node’s location. SSR can be sub-divided into 2 co-operative protocols namely, Dynamic Routing Protocol (DRP) and Static Routing Protocol (SRP).

DRP maintains the Signal Stability Table (SST) and the Routing Table (RT). Through periodic beacons from the link layer of every neighbouring node, the SST records the signal strength of neighbouring nodes. The transmissions are received and processed in DRP, after which the received packets are passed on to the SRP after the DRP updates all the appropriate table entries. Signal strength is classified as either strong or weak.

The SRT passes the packets up the stack if it is the intended recipient or look up the Routing Table for the destination node and forward it if it is not the intended recipient. If there is no entry for the destination in the Routing Table, a route-search process is initiated to find a route. Route requests are sent throughout the network, but are only forwarded to the next node only if the

signal strength is strong and has not been processed previously so as to prevent looping. The route in which the packet reaches the destination node first is deemed to be the shortest or least congested and thus is selected to be used. The DRP then sends a route reply message back to the source via the reverse path.

When no route reply is received by the source within a specific timeout period, the source changes the *PREF* field to indicate that weak channels are also acceptable as they may be the only links over which the packet can be transmitted.

4.3.5 Temporally-Ordered Routing Algorithm (TORA)

Temporally-Ordered Routing Algorithm (TORA) [38] is based on the concept of link reversal. It is highly adaptable, loop-free and is suitable for highly dynamic mobile networking environment. This is due to the localisation of control messages to a very small set of nodes near the occurrence of a topological change; nodes maintaining routing information about adjacent nodes. The three main functions of TORA is route creation, route maintenance and route erasure.

In route creation and route maintenance processes, nodes use a “height” metric to establish a Directed Acyclic Figure (DAG) rooted at the destination. The links are then assigned an upstream or downstream direction based on the relative height metric of neighbouring nodes.

When nodes move, the DAG route is broken and has to be re-established by performing route maintenance. Upon failure of a downstream link, the node generates a new reference level which results in the propagation of that reference level by neighbouring nodes, thus coordinating a structured reaction to failure. The links are reversed, showing the change in adapting to the new reference level.

4.4 WEIGHTED-FACTORS FOR UWB WPAN

UWB offers variable high data rate depending on the distance. It can transfer data up to 1000 Mbps for distances shorter than 1m, 200 Mbps at 4m and 110 Mbps at 10m. As such, the high data rate potential of UWB is compromised if the nodes are far apart. One way to harvest the high data rate of UWB is to use multi-hopping in a mesh network.

In WPAN terms, a typical ad-hoc wireless device has a range of 10m and although 10m is the range considered for UWB in data communications, Although UWB is capable of transmitting data at distances greater than 10m, it is not advisable as speed has to be sacrificed. Thus by using multi-hop, the range of the network can be indefinitely expanded as long as there are intermediate nodes within 10m range of each other to act as links. The efficiency of multi-hopping in a mesh network lies on the routing algorithm to select the best path from source to destination. However, unlike other wireless standards such as IEEE 802.11, the path with the lowest link cost may not be the best path in terms of QoS and maintaining higher speed by keeping distances between nodes small to utilise the ultra-high speed offered by UWB at short distances.

In view of different forms of transmissions, different factors take precedence in priority. For example, 'live' streaming of high quality digital video signals requires constant transmission of data at high speed (32 Mbps for Digital Video and 15 Mbps for MPEG2 [30]) and high fidelity for smooth playing of the multimedia. In this instance, the two most important factors would be high data rate and fixed power supply of nodes to support the transmission of the digital video over a lengthened period. Consequently, factors such as distance between intermediate nodes and power take higher priority over the other factors. For a simple transmission of a small fixed-sized data file from a handheld PDA to a desktop computer, the number of hops to the intended node should take precedence over the other factors (distance, power level and signal strength) to ensure a quick and simple transmission. Figure 4.5 demonstrates how having more hops in an UWB network can result in a higher throughput, which benefits the transfer of large files.

Figure 4.5 Attaining a Higher Speed for UWB with More Hops

4.4.1 Factors for Consideration

Discovering routes is just the preliminary phase. Several factors have to be taken into consideration in choosing a most suitable route to use. Below are the factors considered and used as weights for determining suitable routes in WFRP.

- i. **Distance Between Nodes** – Distance between nodes directly affects the data rate of UWB transmissions. Instances where high data rate is required would require the distance between nodes to be set to be given a higher weight.
- ii. **Power Level** – The power level of a UWB node has to be taken into consideration when transmission has to be sustained over a long period of time. For a device that draws power from a fixed power source, the power level is considered as unlimited whereas mobile or ad-hoc devices are most likely running on batteries and would

have limited power. In cases where there is no node with fixed power supply, the power level of the batteries has to be taken into consideration.

- iii. **Number of Hops** – The number of hops between the source node and the target node denotes the simplicity of data transmission. Involving more intermediate nodes can lead to more complications such as sudden exit of nodes from the network.
- iv. **Signal Strength** – Weak signal strength may result in high errors in data received and affect the fidelity of data. This subsequently affects the overall transfer speed as retransmission is required for data packets with errors.
- v. **File Size** – Transmission of data that are small in size implies a short and quick session. If the file size is big, factors such as distance and signal strength are important to facilitate a faster transfer with high fidelity.
- vi. **Streaming** – If there is “live” streaming to be done, factors such as power level and signal strength are very important as “live” streaming typically demands low error rate over a lengthened period of time. If it is digital multimedia “live” streaming, the distance factor takes high priority too.

The factors listed above are by no means exhaustive and flexibility can be exercised to consider more factors. However, for the work covered in this thesis, only the above listed factors are considered.

4.4.2 WEIGHTED-FACTORS ROUTING PROTOCOL (WFRP)

Fundamentally, a Source-Initiated On-Demand Routing is performed to discover and examine all the possible routes to the destination from the source node. Each node has individual ratings for respective factors such as Power Level and Signal Strength. The number of hops required to reach the destination from source node is recorded during the process of route discovery. Distance between neighbouring nodes can be detected as UWB possesses the geo-location feature that can determine the position and distance of other UWB devices.

When a data transmission is required, the nature of transmission has to be determined first before embarking on a route discovery process. The first 2 criteria to consider are whether the transmission is real-time “live” streaming and the amount of data to be transmitted. These criteria help to determine what weights to assign to each of the 4 factors (distance, power level, number of hops and signal strength) which ultimately determine which path is to be picked at the end of the route discovery process.

The overall weights of the 4 factors add up to 10. Depending on the nature of the data transmission, different weights are assigned to the 4 factors to reflect their priority in the delivery of the data. Table 4.1 shows a typical weight table with some sample weights distribution for 4 kinds of data transmissions. The weight distribution is adaptive and can be re-assigned as needed.

Category	Distance (Speed) W_D	Power Level W_P	Signal Strength W_S	Number of Hops W_H
“Live” Streaming	3	4	1	2
Large Files	5	2	1	2
Small Files	1	1	1	7
Voice	2	2	4	2

Table 4.1 Weight Table

The route discovery process is initiated via a broadcast of route request (RREQ) packets to all the source node's neighbours. Upon receiving a RREQ packet, the node first determines and get the node information, i.e. that the properties of the distance, strength and power level of the node. It determines whether the path specified in the routing table is better or the new path specified is better. This is done by calculating the average path weight taken by the packets. If the average path weight is better, then the routing table is updated with the better path sequence. If the node is the destination node as requested by the source node, a route reply (RREP) packet is then sent back to the source node via the path with the highest weight value. If the receiving node is not the destination node, the RREQ packet is then forwarded again to its neighbouring nodes and continues until the RREQ packet reaches the destination node.

Like the AODV, the WFRP requires only the nodes on the selected path to maintain routing tables and exchange routing information. During the route discovery process, in addition to the routing tables, a node table which contains the node information is maintained. The node table of each individual node records the overall node weight of the 3 factors, distance, power level and signal strength. The number of hops factor is added and recorded to the routing table as path information.

The individual node weight is calculated at each node as shown in Eq 4.1 and stored in the node table. The 3 factors considered here are graded from 1 to 10 each to give an even and fair node weight. For distance, every metre would increment by a grade of 1 to the maximum of 10m. For power level, a maximum grade of 10 is awarded for a device with fixed power (plugged to a power point), 9 for a fully charged depletable power source (i.e. batteries) and minimum grade of 1 for a device critically low in power. Signal strength is graded from 1 to 10 based on how strong the signal strength is at each node.

$$Node\ Weight = \left(\frac{W_D \times 10}{Distance} \right) + (W_P \times Power) + (W_S \times Signal\ Strength) \quad (4.1)$$

In addition, the path weight and the average path weight are also calculated (see Eq 4.2 and Eq 4.3 respectively) and stored in the routing table.

$$Path\ Weight = Node\ Weight + \left(\frac{W_H \times 10}{Number\ of\ Hops} \right) \quad (4.2)$$

$$Average\ Path\ Weight = \frac{(Average\ Path\ Weight)_{n-1} + (Path\ Weight)_n}{2} \quad (4.3)$$

At the destination node, the path with the highest Average Path Weight value is selected and the RREP packet is sent back to the source node via this path.

4.4.3 Examples of WFRP in UWB Network

Example 1: Real-Time “Live” Multimedia Streaming

Figure 4.6 WFRP for Real-Time “Live” Multimedia Streaming

For the real-time “live” multimedia streaming scenario given in Figure 4.6, the weights assigned to the 4 factors are $W_D = 3$, $W_P = 4$, $W_S = 1$ and $W_H = 2$ as given in Table 4.1. Using these assigned weights on equations 4.1, 4.2 and 4.3, a path to the destination is selected as shown in Table 4.2 below.

Current Node	Next Node			Current Sub-path				Current Average Path Weight
	Next Node	Power (P)	Signal Strength (SS)	Distance (D)	No. of Hops (H)	Node Weight	Path Weight	
Source	Node 1	3	8	3	1	25.0	45.0	45.0
Node 1	Desti-nation	10	9	7	2	53.3	63.3	49.1

(a) Path 1

Current Node	Next Node			Current Sub-path				Current Average Path Weight
	Next Node	Power (P)	Signal Strength (SS)	Distance (D)	No. of Hops (H)	Node Weight	Path Weight	
Source	Node 2	10	7	3	1	57.0	77.0	77.0
Node 2	Node 3	10	6	4	2	53.5	64.5	70.3
Node 3	Desti-nation	10	9	4	3	56.5	63.2	66.8

(b) Path 2

Table 4.2 Calculations of Average Path Weight for Example 1

Thus comparing the Average Path Weights, Path 2 is a superior path, with an Average Path Weight of 66.8 as compared to Path 1’s Average Path Weight of 49.1. Path 2 is preferred because of the priority given to principally the Power Level and to a lesser extent, Distance (Speed). The nodes along Path 2 have Power Level ratings of 10 which imply the nodes are plugged to a power point for constant power supply. As the real-time “live” streaming of multimedia data might take place over a long period of time, the power level of the intermediate nodes become the most important factor, followed by Distance which is to maintain high speed and consequently, the QoS of the transmission.

Node 1 has a Powel Level rating of 3 which indicates that it is on depletable power source and is low in power. If Path 1 was to be chosen, Node 1 may run out of power and shut down before the end of the transmission. In such a scenario, the link breaks down and causes the “live” streaming some down time while a new path it tries to discover a new path.

Example 2: Very Large File

Figure 4.7 WFRP for Transmission of Large Files

Figure 4.7 shows the scenario of WFRP in operation for a data transmission of a very large file. The weights assigned to the 4 factors are $W_D = 5$, $W_P = 2$, $W_S = 1$ and $W_H = 2$ as given in Table. 4.1. Using these assigned weights, a path to the destination is selected as shown below.

Current Node	Next Node			Current Sub-path				Current Average Path Weight
	Next Node	Power (P)	Signal Strength (SS)	Distance (D)	No. of Hops (H)	Node Weight	Path Weight	
Source	Node 1	9	9	3	1	43.7	63.7	63.7
Node 1	Node 2	8	5	3	2	37.7	47.7	55.7
Node 2	Node 3	6	7	3	3	35.7	42.4	49.1
Node 3	Node 4	7	8	3	4	38.7	43.7	46.4
Node 4	Desti-nation	10	9	3	5	45.7	49.7	48.1

(a) Path 1

Current Node	Next Node			Current Sub-path				Current Average Path Weight
	Next Node	Power (P)	Signal Strength (SS)	Distance (D)	No. of Hops (H)	Node Weight	Path Weight	
Source	Node 5	8	5	10	1	26.0	46.0	46.0
Node 5	Desti-nation	10	9	10	2	34.0	44.0	45.0

(b) Path 2

Table 4.3 Calculations of Average Path Weight for Example 2

In this scenario, Path 1 has an Average Path Weight of 48.1 and is chosen over Path 2 which has an Average Path Weight of 45. Higher weight is assigned to Distance to attain a higher speed for the transfer of a very large file so as to complete the transmission in the shortest time possible.

CHAPTER 5

SIMULATIONS

5.1 COEXISTENCE OF BLUETOOTH AND IEEE 802.11b

5.1.1 Degradation Factor Modelling

The Degradation Factor is the ratio between the actual time taken to transmit a packet and the minimum time it takes to do the same. The probability models derived in Section 3.2.2 and Section 3.2.3 are used to develop the Degradation Factor Model to observe the effects of Bluetooth interference on IEEE 802.11b transmissions.

The simulation is set up in an environment where the IEEE 802.11b and the Bluetooth are both active at the same time. However, the utilisation setting of the Bluetooth transmission is set at 50%, meaning only 50% of the Bluetooth slots contain Bluetooth packets. As for the IEEE 802.11b packets, the transmission is constant and the other components of a frame such as PLCP preamble, PLCP header, SIF, etc (See Section 2.2.2 and Section 2.2.3) are also included as parts of the packets transmitted.

A 100 MB file is simulated to be sent using IEEE 802.11b at 11 Mbps with interference from Bluetooth which is at 50% utilisation. The simulations investigate the extent of degradation against fragment size of the IEEE 802.11b packets during transmission while being interfered by Bluetooth traffic. The transmission of the 100 MB file is repeated using different fragment sizes ranging from 100 bytes to 1500 bytes to obtain the graph shown in Figure 5.1.

5.1.2 Results

Figure 5.1 Comparison of Degradation Factor

Both probability models exhibit similar behaviour of having extremely high Degradation Factor when the fragment sizes of the IEEE 802.11b packets are very small. This is due to the inclusion of the MAC and frame format (i.e. PCLP preamble, PLCP header, etc) overheads that the IEEE 802.11b packet contains. For very small fragment sizes, the 100 MB file gets divided into many small parts each with its own MAC and frame format overheads. Thus the effect of these overheads on Degradation Factor is much more obvious.

At the other end of the graph where the fragment size is 1500 bytes (meaning there is no fragmentation), the Degradation Factor for Greg Ennis's model is 3.95 times while the proposed model is 3.35 times. As expected, the proposed model yields a lower Degradation Factor much like the comparison of PER between these 2 models in Section 3.3 since the expected number of collisions and packets corrupted is lesser than that of Greg Ennis's model.

Another observation that can be made from the results is that in presence of Bluetooth interference, fragmentation of the IEEE 802.11b packets is beneficial as can be seen from the steady drop in Degradation Factor of both curves as the fragment size is reduced from 1500 bytes to 600 bytes gradually. However, fragmentation of the packets into too small a size will outstrip the benefits of fragmentation as explained earlier. This phenomenon is evident when the fragment size is gradually reduced from 600 bytes to 100 bytes as can be seen in Figure 5.1.

Overall, the proposed model has a lower Degradation Factor than Greg Ennis's model as expected since the proposed model considers the idle time when no collision is possible. However at around 300 bytes fragment size, the proposed model has a lower than expected Degradation Factor which might suggest that 300 bytes is the optimal fragment size.

5.2 SIMULATION ENVIRONMENT AND SETUP FOR ROUTING PROTOCOLS SIMULATIONS

5.2.1 Choice of NS2 as Network Simulator

NS2 is the network simulator used in the project. It is an object-oriented, discrete event driven network simulator which can simulate IP networks. It implements network protocols, traffic source behaviour, Telnet, Web and CBR (Constant Bit Rate), router queue management mechanism and many other network processes. NS2 also can implement multicasting and some of the MAC layer protocols for LAN simulations.

Several basic factors affect the choice of this network simulator as following:-

- Open source and hence changes can be made to source codes
- Large user base and active mailing list
- Zero cost
- Available mobile ad-hoc simulation model

The simulation package can be run on any Unix machine (Linux, Solaris, BSD) or on a PC running Windows operation system with a Linux emulator like *cygwin*.

There are also many other advantages to use such a common simulation platform as NS2. One important factor is that by sharing the methodology with other like-minded researchers, the simulation package can be critically assessed, constantly. Most functions of the simulators have been correctly implemented. Therefore, more time can be allocated to design the simulation setup, rather than cast doubts over the project results due to the existing bugs and inconsistency of the simulation package in use.

5.2.2 Interference Model

The MAC protocol of the mobile allows only 1 pair of nodes to communicate with each other within the sensing range of the nodes. In event of multiple incoming packets that arrive at the same time, the receiving node has to decide which packet to accept. The in-built interference model in the network interface of each mobile node handles this function.

When 2 incoming packets collide, the receiving node executes a decision-making process. The energy levels of the 2 colliding packets are compared. If the difference in energy level is higher or equal to the Capture Threshold (in dBm), the packet with the higher energy level will be correctly received. Otherwise, both packets will be discarded and marked as lost. Capture

Threshold (CPThresh) is the parameter in the network interface that defines the signal ratio required to maintain receiver capture of incoming packet during a collision.

5.2.3 Traffic Model Generation

Before running the simulation, a traffic model that depicts the conditions of the traffic is to be generated. The tcl code to carry out this task is found in the file found at `~ns/indep-utils/cmu-scen-gen/cbrgen.tcl`. The syntax of the command line is shown below:-

```
ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] [-seed seed] [-mc connections][  
-rate rate] > [outdir/movement-file]
```

`[-type cbr|tcp]` defines the connections, typically Continuous Bit Rate (CBR) or Transmission Control Protocol (TCP) between the wireless nodes. `[-nn nodes]` depicts how many nodes there are in the wireless network. The role of `[-seed seed]` is to randomise the parameters. A particular seed value will generate a set of random sequence. A different seed value will produce another different set of random sequence, such that a different set of experiment using the pseudo random number can be repeated. The overall results can be obtained by averaging these different set of results. `[-mc connections]` specifies how many nodes within the network are actually source nodes. `[-rate rate]` defines the number of packets sent every second.

An example of the command line where the traffic model to be generated and saved to an output file, `cbr.txt`, is of CBR nature, consists of 50 nodes, has seed value of 1, maximum connections of 20 sources and a rate of 1kbps is as shown below:-

```
ns cbrgen.tcl -type cbr -nn 50 -seed 1 -mc 20 -rate 1 > cbr.txt
```

5.2.4 Scenario Model Generation

To simulate the conditions of a mobile wireless network, a scenario model is generated to define node movements within the network. The node movement generator is made up by `setdest.cc`, `setdest.h` and `Makefile` found in the `~ns/indep-utils/cmu-scen-gen/setdest` directory. The syntax of the command line is as below:-

```
./setdest [-v 1] [-n nodes] [-p pause time] [-M max speed] [-t simulation time]
[-x max X] [-y max Y] > [outdir/movement-file]
```

`[-v 1]` depicts the version of `setdest` used (in this project, version 1 is used). `[-n nodes]` defines the number of nodes within the network. In this project, 50 mobile nodes are used. `[-p pause time]` sets the length of time the nodes wait before moving to another destination. A pause time of 0 indicates that the various nodes will be in constant movement; moving to its new destination position once it reaches its current position. And a system with a pause time of 60 indicates that the node will stop at its current position for 60 seconds before moving on to its next intended destination. `[-M max speed]` sets the maximum speed for nodes to move about. The movement speed of the nodes range from 0-20 m/s. `[-t simulation time]` is the length of the simulated period. `[-x max X]` `[-y max Y]` define the size of the topology of the simulation. An elongated shape is used instead of a square topology such that the probability of nodes using multi-hop transmission is higher than using a balanced topology.

For example, a scenario model with 50 nodes, 20sec of pause time, maximum speed of 10m/s, simulated time of 100sec and a topological boundary of 60m x 12m can be generated and output to a file, `scenario.txt`, by running the command line,

```
./setdest -v 1 -n 50 -p 20 -M 10 -t 100 -x 60 -y 12 > scenario.txt
```

5.2.5 Simulating UWB Conditions

As the UWB models are not yet available in ns2, modifications are made to the IEEE 802.11 model to emulate the characteristics of an UWB model. The changes based on the parameters proposed by the Multiband OFDM Alliance [45], are made in the tcl script and are listed below:-

```
Mac/802_11 set dataRate_ 110e6           #Data Rate
Mac/802_11 set basicRate_ 55e6           #Basic Rate
Phy/WirelessPhy set CStresh_ 8.912509381e-12 #Receiver Sensitivity
Phy/WirelessPhy set RXThresh_ 3.548133892e-11 #Receiver Power
Phy/WirelessPhy set Pt_ 9.332543e-5       #Avg Transmission Power
Phy/WirelessPhy set freq_ 3.882e+9        #Center Frequency
Phy/WirelessPhy set L_ 1                  #Loss
```

In addition, the maximum transmit range for IEEE 802.11 is set at 250m in ns2 by default, whereas the transmit range for UWB is 10m. To rectify this, the RANGE value in the setdest.cc file is changed from 250m to 10m. After making the changes, the setdest.cc is recompiled by running the following command in the directory ~ns/indep-utils/cmu-scen-gen/setdest:-

```
$> gcc setdest.cc
$> make depend
$> make
```

5.2.6 Performance Metrics

The following three important metrics are used to characterise the performance of the system:-

- i. ***Packet Delivery Fraction (PDF)*** - Packet delivery fraction is the ratio of the data packets delivered to the destinations to those generated by the sources. This metric gives an immediate idea of the efficiency of the system that is being evaluated.
- ii. ***Average End-to-End Delay*** - Average end-to-end delay is the sum of all the delay contributed by every data packets divided by the total number of packets received. The magnitude of delay represents the time that a packet spends traversing the network from a sender to a receiver.
- iii. ***Normalized Routing Load*** - This metric evaluates the efficiency of the routing protocol when used on the system. It is the number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission.

5.3 SIMULATION RESULTS FOR WFRP

The performance metrics are plotted against pause time. The pause time is the period of time which the nodes will wait before moving to another destination. Thus a low pause time indicates a scenario of high mobility while a high pause time reflects a scenario of low mobility.

The performance of WFRP is compared against the performances of AODV and DSR routing protocols in a series of NS2 simulations based on the performance metrics given in Section 5.2.6.

The number of nodes is set at 50 with each node having a moving speed ranging from 0 to 20 m/s. The simulation time is set at 300 seconds and the data rate is fixed at 1 packet per second. The topology defined is 60 x 12 metres. The 2 parameters that are varied are pause time and number of connections (sources).

5.3.1 Results for 10 Sources

Figure 5.2 PDF Performances for 10 Sources

With 10 sources, the DSR protocol performs the worst among the 3 routing protocols except marginally better performance than the AODV protocol and the WFRP around the pause time of 25 sec, with approximately 5.1% and 6.0% PDF increase, respectively, as shown in Figure 5.2. On average, the AODV protocol delivers the highest PDF. It outperforms the WFRP and the DSR protocol by approximately 3.8% and 4.1% PDF increase. The WFRP fared only marginally lower than the AODV protocol with approximately 7.0% maximum difference of around 40 sec.

All the 3 protocols' PDFs rise sharply from 0 to 25 sec pause times and gradually increase to 90% and above when the pause time reaches 50 sec.

(a)

(b)

Figure 5.3 Average End-to-End Delay for 10 Sources

Comparing the AODV protocol and the WFRP as shown in Figure 5.3(a), the Average End-to-End Delay is significantly lower for the WFRP as compared to the AODV protocol for most of the pause times, except around the pause time of 60 sec where they are of the same value. On average, the WFRP's Average

End-to-End Delay is approximately 27.6% lower than that of the AODV protocol. This indicates more efficient routes are chosen by the WFRP over the AODV protocol as less time is spent traversing the network from the sender to receiver. The Average End-to-End Delays for both the AODV protocol and WFRP drop gradually until they stabilize at the pause times of 60 sec and 45 sec respectively.

For the DSR protocol, the Average End-to-End Delay is excessively high at the lower pause time, especially ranging from 0 to 25 sec, as shown in Figure 5.3(b). In this range, the dynamic ranges of the Average end-to-End Delay values of both the WFRP and the AODV protocol do not exceed 0.11 sec, while the maximum Average End-to-End Delay of the DSR protocol reaches approximately 17 sec. This has shown that the DSR protocol's ability to choose an efficient route is compromised when the nodes are moving at higher speed while the AODV protocol and the WFRP are more dependable, with the WFRP being the most effective.

Figure 5.4 Normalised Routing Load for 10 Sources

With 10 sources, the DSR protocol exhibits extremely high Normalised Routing Load as compared to the AODV protocol and the WFRP as illustrated by Figure 5.4. While the AODV protocol and WFRP are on par with each

other, having Normalised Routing Loads that peak at 0 pause time with 22 packets, the DSR protocol's Normalised Routing Load peaks at 132 routing packets at 0 pause time. Although it is expected for the Normalised Routing Load to be higher at lower pause time as nodes are moving faster, causing a need for more routing packets to be transmitted to maintain accurate route information, the DSR protocol's excessively high Normalised Routing Load at low pause time is far from satisfactory as compared to the other 2 routing protocols. However, beyond the pause time of 25 sec, the Normalised Routing Load is at a satisfactorily low level which is even lower than those of the AODV protocol and the WFRP.

5.3.2 Results for 20 Sources

Figure 5.5 PDF Performances for 20 Sources

With 20 sources now, the DSR protocol displays a better PDF performance (compare Figure 5.5 to Figure 5.2) on average than when there are only 10 sources, approximately 11.4% and 5.6% higher on average in PDF over the WFRP and the AODV protocol around the pause times of 25 to 40 sec with 20 sources, respectively. However at 0 sec pause time, the DSR protocol performs worse with a PDF of 61% than when there are only 10 sources with PDF of

51%. While the AODV protocol and the WFRP maintain similar PDF performances (See Figure 5.5) as when with 10 sources, the DSR protocol outperforms both the protocols at 18 sec pause time and above, with the difference most significant when the pause times range from 20 to 50 sec.

The PDF of the DSR protocol rises the most sharply from 51% to 95% when the pause time is from 0 to 25 sec. Although the PDFs of the AODV protocol and the WFRP are higher than the PDF of the DSR protocol at 0 sec pause time, they stabilise at PDF of 90% and beyond only at the pause time of 50 sec and above.

(a)

Figure 5.6 Average End-to-End Delay for 20 Sources

From Figure 5.6(a), it can be seen that with 20 sources, the Average End-to-End Delay for the AODV protocol is lower than when there are 10 sources. The highest Average End-to-End Delay for the AODV protocol dropped from 0.109 sec with 10 sources (see Figure 5.3(a)) to 0.088 sec with 20 sources (see Figure 5.6(a)). An interesting observation made from Figure 5.6(a) is the sudden dip in the Average End-to-End Delay for the AODV protocol at the pause time of 45 sec. A clue for the occurrence of this unexpected sharp drop can be found in Figure 5.3(a) around the pause time of 50 sec with the same Average End-to-End Delay. Anyhow, this sharp drop can be avoided when the resources reach 30 and above, which will be illustrated later.

The WFRP's Average End-to-End Delay starts off marginally higher as compared to the 0 sec pause time of the scenario with 10 sources (compare Figure 5.6(a) with Figure 5.3(a)). The Average End-to-End Delay decreases more gradually until it stabilises below 0.01 sec at 122 sec pause time. Again, the WFRP performs significantly better than the AODV protocol with approximately 33% lower Average End-to-End Delay, except the previously mentioned sharp drop.

As shown in Figure 5.6(b), the Average End-to-End Delay of the DSR protocol is again extremely high at low pause times again, registering a 20 sec delay at 0 sec pause time. The readings drop sharply from 0 to 19 sec pause times before it stabilises to become on par with the AODV protocol and the WFRP.

Figure 5.7 Normalised Routing Load for 20 Sources

Figure 5.7 shows that the Normalised Routing Loads for the AODV protocol and the WFRP have the same performance as what happened in the scenario with 10 sources (see Figure 5.4). The Normalised Routing Load of the DSR protocol also exhibits the same characteristic as with the scenario with 10 sources (see Figure 5.4) except for lower Normalised Routing Load at very low pause times (108 data packets at 0 sec pause time).

5.3.3 Results for 30 Sources

Figure 5.8 PDF Performances for 30 Sources

With 30 sources, the DSR protocol continues the trend of starting worse off at 0 sec pause time as compared to scenarios of lesser sources, having a PDF of 45% as shown in Figure 5.8, but increases very sharply from 0 to 25 sec pause times. The PDFs of the DSR protocol are slightly higher than the scenario where there are only 20 sources. Same as the earlier scenarios with lesser sources, the PDF performance of the DSR is significantly worse off than the other 2 routing protocols at very low pause times, but outperforms the AODV protocol and the WFRP beyond 25 sec pause time.

The PDF performances of the AODV protocol and the WFRP are very similar as compared to their performances when there are only 20 sources.

(a)

(b)

Figure 5.9 Average End-to-End Delay for 30 Sources

The Average End-to-End Delay for the AODV protocol at 0 sec pause time is again lower than the previous scenarios with lesser sources, recording a 0.72 sec delay. At 22 sec pause time, The AODV protocol experiences a sudden increase with approximately 125% higher Average End-to-End Delay then that of the WFRP as shown in Figure 5.9(a). The previously mentioned sharp drop

around 50 sec disappears. Other than that, the Average End-to-End Delay gradually decreases over the remaining range of pause time.

The WFRP's Average End-to-End Delay starts off at a lower delay of 0.07 sec at 0 sec pause time (see Figure 5.9(a)) as compared to the Average End-to-End Delays of WFRP with 10 and 20 sources (see Figures 5.3(a) and 5.6(a)). The Average End-to-End Delay of the WFRP gradually decreases and goes below 0.02 sec at 100 sec pause time and above. Once again, the WFRP performs better than the AODV protocol. However at 80 sec pause time and above the superiority of the WFRP over the AODV protocol diminishes as both have approximately the same Average End-to-End Delay values.

As for the DSR protocol, the Average End-to-End Delay curve for 30 sources behave almost identically to the curve for 20 sources as shown in Figures 5.9(b) and 5.6(b) respectively.

Figure 5.10 Normalised Routing Load for 30 Sources

From Figure 5.10 above, it can be observed that the AODV protocol and the WFRP yield the same results with the scenarios of 10 and 20 sources. Similarly, for the DSR protocol, the Normalised Routing Load has a lower peak of 80 data packets at 0 sec pause time as compared to the scenarios of 10

and 20 sources. The Normalised Routing Load of the DSR protocol dropped sharply until it stabilises after 20 sec pause time and is lower than the Normalised Routing Loads of the AODV protocol and WFRP.

5.3.4 Results for 40 Sources

Figure 5.11 PDF Performances for 40 Sources

The PDF of the DSR protocol is once again lower (42% PDF as shown in Figure 5.11) at 0 sec pause time as the number of sources increases to 40 as compared to the scenarios with lesser sources. However, the PDF rises even more sharply than the earlier scenarios of lesser sources, exceeding 90% at 20 sec pause time and attains higher PDF than the other 2 routing protocol thereafter.

Referring to Figure 5.11, the PDF performances of the AODV protocol and the WFRP remains consistent with the scenarios with lesser sources (see Figures 5.2 and 5.5)

(a)

(b)

Figure 5.12 Average End-to-End Delay for 40 Sources

The Average End-to-End Delay for the AODV protocol peaks at 0.079 sec at 0 sec pause time and gradually decreases. At 60 sec pause time and above, the rate of decrease of the Average End-to-End Delay slows down, decreasing from 0.029 sec to 0.005 sec over the range of 60 to 300 sec pause times.

For the WFRP, the Average End-to-End Delay with 40 sources is consistently lower than the AODV protocol. Its Average End-to-End Delay is 0.051 sec at 0 sec pause time. The curve generally decreases gradually over the length of pause time.

Figure 5.12(b) shows that the DSR protocol once again performs almost identically as its scenarios of 20 and 30 sources in terms of Average End-to-End Delay.

Figure 5.13 Normalised Routing Load for 40 Sources

Once again, the AODV protocol and the WFRP perform nearly identically as compared to scenarios of 10, 20 and 30 sources. The Normalised Routing Load of the DSR protocol stabilises at 25 sec pause time again and has a lower peak Normalised Routing Load of 71 data packets as compared to the scenarios of lesser sources. Please see Figure 5.13 above.

5.4 ANALYSIS

5.4.1 DSR Protocol

Based on the results collected from the series of simulations, it is observed that the DSR protocol performs the worst when the pause times are low, indicating that is less reliable when nodes are moving about at short intervals. However, the PDF of the DSR is higher than the PDF of the other 2 routing protocols as can be seen from Figures 5.5, 5.8 and 5.11.

Although it is expected for the PDF of a routing protocol to be lower at low pause time (nodes moving frequently), the PDF of the DSR protocol is significantly lower than the AODV protocol and the WFRP as observed from Figures 5.2, 5.5, 5.8 and 5.11. This make the DSR protocol a less reliable candidate for use with an ad-hoc UWB WPAN network as compared to the other 2 routing protocols.

The performance of the DSR protocol in terms of Average End-to-End Delay is abysmal at low pause time (25 sec and below). The worst case can be seen at Figure 5.12(b) where the Average End-to-End Delay is 20 sec at 0 sec pause time. Comparatively, the Average End-to-End Delays of the AODV protocol and the WFRP have never exceeded 0.11 sec. In this department, the weakness of the DSR protocol at low pause times is once again exposed.

The DSR protocol fares badly yet again at low pause time of 25 sec and below for Normalised Routing Load, reaching the highest value of 132 routing packets at 0 pause time for 10 sources as shown in Figure 5.4. With such a high routing overhead (packets), it can be concluded that the DSR protocol is inefficient at low pause time.

5.4.2 AODV Protocol

The AODV protocol has the best PDF at 0 sec pause time of all the 3 routing protocols. The PDF increases gradually with the increase of pause time up to 50 sec pause time where the increase slows down and the curve becomes gentler in gradient. In comparison to the DSR protocol, the AODV is far more reliable at low pause times, offering at least 70% PDF approximately (see Figures 5.2, 5.5, 5.8 and 5.11).

For Average End-to-End Delay, the AODV protocol performs reasonable well, not exceeding 0.11 sec for its worst case at 0 sec pause time with 10 sources (see Figure 5.3(a)).

The Normalised Routing Load of the AODV protocol is moderate at low pause time (22 data packets at 0 sec pause time) and gradually decreases to a low level of 5 data packet and below with higher pause time (50 sec and above). Refer to Figures 5.4, 5.7, 5.10 and 5.13 for the curves.

Overall, the AODV protocol appears to be a stable choice for an ad-hoc UWB WPAN network, giving steady performances in all the 3 performance metrics. It is also able reliable when node mobility is high (low pause time).

5.4.3 WFRP

In terms of PDF, the WFRP performs marginally (1~2%) worse off than the AODV protocol. Otherwise the PDF curve of the WFRP exhibits similar characteristics as the PDF curve of the AODV protocol. Refer to Figure 5.2, 5.5, 5.8 and 5.11.

The WFRP outperforms the AODV protocol in the Average End-to-End Delay department. The WFRP performs consistently better than the AODV at different mobility rate of the nodes. Under the heaviest traffic and most

stressful conditions at 0 pause time with 40 sources, the WFRP has an Average End-to-End Delay 40% lower than the AODV. This indicates that the path chosen by the WFRP is more efficient than the path chosen by the AODV and the difference is more apparent when the traffic is heavier or when the nodes in the network have high mobility.

For Normalised Routing Load, the WFRP performs almost identically as the AODV protocol as can be seen at Figures 5.4, 5.7, 5.10 and 5.13.

From the overall results of the simulations, WFRP appears to be a very good candidate for a routing protocol for an UWB WPAN, even edging ahead of the popular AODV protocol. Although the DSR has better performances at low mobility, its poor performance at high mobility hurts its credential as a good candidate for a routing protocol for an UWB WPAN.

5.5 RELATED WORK

5.5.1 Overview

In an investigation carried out by Josh Broch *et al.* [46], four protocols namely DSDV, TORA, DSR and AODV are examined. 50 wireless nodes are simulated, moving about at a uniformly distributed speed between 0m/s to 20m/s over a 1500m x 300m flat space for 900 seconds of simulated time. The simulations were carried out for 7 different pause times of 0, 30, 60, 120, 300, 600 and 900 seconds. 20 of the 50 wireless nodes were chosen to be constant bit rate (CBR) sources, sending out 4 data packets with sizes varying from 64 bytes to 1024 bytes per second. The simulations were carried out using the MAC of IEEE 802.11. The Packet Deliver Ratio which is equivalent to the Packet Delivery Fraction (PDF) used in this project and the Routing Overhead are the main performance metrics measured.

5.5.2 Packet Delivery Fraction

Figure 5.14 PDF of Josh Broch *et al.*'s Work

The DSR protocol has a better performance in the Packet Delivery Fraction than the AODV protocol across all pause times as depicted in Figure 5.14.

The results of Josh Broch *et al.*'s work are similar to the findings of this project. The DSR protocol has a slight advantage in PDF performance over the AODV protocol. However for the simulations done in this project, the PDF performance of all the routing protocols suffered a considerable drop in performance at very low pause times as opposed to Josh Broch *et al.*'s findings that the performances are more or less the same than that of higher pause times.

As it is expected of the PDF to be significantly lower especially for the DSR protocol [47] at very high mobility where the network is more volatile and the signals are more unstable, the graph shown in Josh Broch *et al.*'s work

indicated otherwise as shown in Figure 5.14. The PDF of the DSR and AODV protocols at very low pause times are more or less the same as of other pause times, never dipping below 95%. Furthermore, the TORA protocol's PDF at very low pause times (from 0 to 60 sec) is even higher than that of higher pause times (from 60 to 300 sec). The reason for this strange phenomenon was not explained in the published paper.

5.5.3 Routing Overhead

Figure 5.15 Routing Overhead of Josh Broch et al.'s Work

The AODV protocol has significantly higher routing overheads than the DSR protocol for all pause times especially at lower pause times as shown in Figure 5.15.

The results of Josh Broch *et al.*'s findings are similar to the findings of this project except for very low pause times of 0 to 30 sec. In the simulations carried out in this project, the DSR protocol has lower routing overheads

compare to the AODV protocol only at pause times of 30 sec and beyond. At pause times of 30 sec and below in this project, the normalised routing overhead of the DSR protocol is much higher than that of the AODV protocol whereas Josh Broch *et al.*'s DSR protocol has lower routing overheads than the AODV protocol for all pause times.

Since the DSR protocol uses route cache to store route information to aid its selection of the shortest path instead of a route table as used by the AODV protocol [47], the routing overhead of the DSR protocol is generally lower than the AODV protocol as there is no need for periodic route advertisement and neighbour detection packets to be sent [46].

Although the DSR protocol boasts a lower overall routing overhead than the AODV protocol, the routing load of the DSR protocol is actually relatively high as the routing load is dominated by RREP packets due to multiple replies from the destination [47]. As such, the excessively high normalised routing overhead at very low pause times exhibited in the simulations of this project can be explained by the nature of the small topography.

The topography of the simulations carried out in this project is defined to be 60 x 12 metres, whereas Josh Broch *et al.*'s simulations were run in a space of 1500 x 300 metres. Given the much smaller space defined for the simulations in this project, when the nodes are highly mobile, the route information changes rapidly and frequent updates to the routing cache which contributed to the high normalise routing overhead of the DSR protocol at very low pause times. Over a much larger space of 1500 x 300 metres, such an effect is greatly reduced in significance.

CHAPTER 6

CONCLUSION AND RECOMMENDATIONS

6.1 CONCLUSION

In the simulations carried out for the routing protocols, the WFRP has shown the potential to be a stable and efficient routing protocol. Although the DSR protocol yields favourable results compared to the WFRP and AODV at higher pause times. However, the results of DSR dip sharply when the mobility of the nodes in the network is high as shown from the figures in Section 5.3 at 0 pause times. The poor performance at high mobility of the mobile nodes is the Achilles' heel of DSR and renders it unreliable for an UWB ad-hoc wireless personal area network.

While the WFRP is on par with AODV in terms of Normalised Routing Load and is marginally lower (1~2%) than AODV in terms of Packet Delivery Fraction (PDF), the WFRP performs much better (up to 38%) in the Average End-to-End Delay. The notably better performance in Average End-to-End Delay by the WFRP eclipses the marginally lower PDF when compared to AODV. On top of that, the WFRP is designed to tap the ultra high speed offered by an UWB network at short distances.

The performance of the DSR protocol is significantly worse off than WFRP and AODV at 0 pause time (very high mobility of nodes). The Packet Delivery Fractions (PDF) of WFRP and AODV are 50% higher than the DSR. Although the PDF of DSR increases sharply after 0 pause time to above 95%, which is even higher than the PDF of WFRP and AODV, its poor performance at 0 pause time impairs the reliability for use in an UWB ad-hoc network.

The WFRP and AODV have more stable PDF than DSR. The AODV protocol yields a PDF of approximately 70% at 0 pause time and its PDF gradually and steadily improves as the pause time increases. As observed from the figures, the PDF of WFRP is only marginally lower (1~2%) than AODV, making WFRP as reliable as the AODV. The slightly lower PDF experienced by the WFRP can be explained by some of the longer paths chosen compared to AODV as the probability of packet errors increases if the route is longer. Although some of the paths chosen may be longer, WFRP offers the benefit of higher transfer speeds which are offered at smaller distances between nodes in an UWB-based network outweighs the extra number of hops the route may take.

The WFRP outperforms the AODV in the department of Average End-to-End Delay. The WFRP performs consistently better than the AODV at different mobility rate of the nodes. Under the heaviest traffic and most stressful conditions at 0 pause time with 40 sources, the WFRP has an Average End-to-End Delay 40% lower than the AODV. This indicates that the path chosen by the WFRP is more efficient than the path chosen by the AODV and the difference is more apparent when the traffic is heavier or when the nodes in the network have high mobility. The DSR protocol scores badly at 0 pause time again in terms of Average End-to-End Delay. At 0 pause time, the delay can go up to as high as 20 seconds, which is highly undesirable.

On the overall, the WFRP offers a relative more reliable and better performance than the popular DSR and AODV protocols. The strength of the WFRP will be even more distinct if the simulated environment is able to exhibit the trait of variable data rate according to proximity between nodes that a real UWB environment should really have.

The mathematical probability model for coexistence of Bluetooth and IEEE 802.11b by Greg Ennis has been investigated too in this project. Although this model gives a simple and clean outlook to the probability of collision when the Bluetooth and IEEE 802.11b coexist, some important details are overlooked

which would cause inaccuracy of the model. In this project, improvements to Greg Ennis's model are proposed and investigated.

6.2 RECOMMENDATIONS

6.2.1 Creating a More Accurate UWB PHY Model

The simulation results are satisfactory when compared to the AODV and DSR protocols. However, the lack of an accurate UWB PHY model has to be taken into consideration. The distinctive difference between UWB and other wireless communication standards such as IEEE 802.11 is the varying data rate at different distances. The lack of this distinctive feature in the UWB PHY model used in the simulations adversely affects the results of the WFRP. With an accurate UWB PHY Model, the strengths of the WFRP can be better presented during simulations.

6.2.2 Election of Principal Factor in WFRP

Although the WFRP has performed well in the simulations carried out in Part V as compared to the AODV and DSR, there are more room for improvements. The WFRP performs path selection by comparing the average path weight at the destination node. The efficiency of the route discovery process can be further improved by electing a principal factor. The principal factor should be the most critical factor to consider in the selection of path. By identifying the principal factor, the route discovery process can be shortened by discarding paths that exceeds the threshold limit of the principal factor. For example, the number of hops factor is elected as the principal factor and its threshold limit is set at 5. Any path that exceeds 5 hops before reaching the destination node will not be pursued any further.

The method to choose a principal factor varies. One method is to choose the factor with the highest weight as the principal factor. This method is good when there is a factor which weight is distinctively higher than the other

factors. However, if the weight values of all the factors are near, this method of choosing the principal method might not be desirable. Finding and implementing an effective method for choosing a principal factor calls for creativity. And how well the method can improve the performance of the WFRP is open for further studies.

BIBLIOGRAPHY

- [1] Texas Instruments, 'V.34 Transmitter and Receiver Implementation on the TMS320C50 DSP', *Application Report*, SPRA159, June 1997
- [2] Lee-Fang Wei, 'Trellis-Coded Modulation with Multidimensional Constellations', *IEEE Transactions on Information Theory*, Vol. 33, No. 4, pp. 483-501, Jul 1987
- [3] Lee-Fang Wei, 'Rotationally Invariant Trellis-Coded Modulations with Multidimensional M-PSK', *IEEE Journal on Selected Areas in Communications*, Vol. 7, No. 9, pp. 1281-1295, December 1989
- [4] G. David Forney Jr, Lee-Fang Wei, 'Multidimensional Constellations – Part I: Introduction, Figures of Merit and Generalized Cross Constellations', *IEEE Journal on Selected Areas in Communications*, Vol. 7, No. 6, pp. 877-892, August 1989
- [5] Amir K. Khandani, Peter Kabal, 'Shaping Multidimensional Signal Spaces – Part I: Optimum Shaping, Shell Mapping', *IEEE Transactions on Information Theory*, Vol. 39, No. 6, pp. 1799-1808, November 1993
- [6] 802.11 Planet, www.80211-planet.com
- [7] Phani K. Neelakantham, Pallegadda Kistareddy, 'Wireless Networking... IEEE 802.11 Specification',
<http://www30.homepage.villanova.edu/phani.neelakantham/Comm%20Nets/Wireless%20Networking%20802.11.htm>
- [8] IEEE 802.11 Specifications for Wireless Communication,
<http://mama.indstate.edu/users/kantamneni/ECT680/fall02/RenePhilippe.html>
- [9] Kanoksri Sarinnapakorn, IEEE 802.11b "High Rate" Wireless Local Area Networks,
<http://alpha.fdu.edu/~kanoksri/IEEE80211b.html>
- [10] The Bluetooth Specifications, <http://www.bluetooth.org/specifications.htm>
- [11] Anthony C Davies, 'An Overview of Bluetooth Wireless TechnologyTM and Some Competing LAN Standards', *Proceedings of 1st IEEE International Conference on Circuits and Systems for Communications*, pp. 206-211, 2002

- [12] Manish Kalia, Sumit Garg, Rajeev Shorey, 'Scatternet Structure and Inter-Piconet Communication in the Bluetooth System', *IEEE National Conference on Communications 2000*, New Delhi
- [13] David Harris, Michael Roberts, 'Quantifying Bluetooth Piconet Mutual Interference', *Highland Systems Inc*,
<http://www.highsys.com/products/Bluetooth%20Mutual%20Interference.pdf>
- [14] Jeyhan Karaoguz, 'High-Rate Wireless Personal Area Networks', *IEEE Communications Magazine, In-Home Networking*, pp. 96-102, December 2001
- [15] Pierre Gandolfo, James Allen, '802.15.3 Overview/Update October 2002', *The WiMedia Alliance*,
http://www.wimedia.org/events/docs/05_802.15.3_Overview_WiMedia_Oct_2002.pdf
- [16] Chatschik Bisdikian, Pravin Bhagwat, Brian P. Gaucher, Frank. J. Janniello, Mahmoud Naghshineh, Puneet Pandoh, 'WiSAP: A Wireless Personal Area Network for Handheld Computing Devices', *IEEE Personal Communications*, Vol. 5, No. 6, pp. 18-25, December 1998
- [17] Prashant Krishnamurthy, Joseph Kabara, Tanapat Anusas-amornkul, 'Security in Wireless Residential Networks', *IEEE Transactions on Consumer Electronics*, Vol. 48, No. 48, pp. 157-166, February 2002
- [18] Wang Feng, Nallanathan Arumugam, Garg Hari Krishna, 'Performance of a Bluetooth Piconet in the Presence of IEEE 802.11 WLANs', *The 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications 2002*, Vol. 4, pp. 1742-1746
- [19] Carla F. Chiasserini, Ramesh R. Rao, 'Performance of IEEE 802.11 WLANs in a Bluetooth Environment', *IEEE Wireless Communications and Networking Conference 2000*, Vol. 1, pp. 94-99
- [20] Marko Hannikainen, Tapio Rantanen, Jani Ruotsalainen, Markku Niemi, Timo Hamalainen, Jukka Saarinen, 'Coexistence of Bluetooth and Wireless LANs', *International Conference of Telecommunications 2001*, Bucharest, Romania, Vol. 1, pp. 117-124, June 4-7 2001
- [21] Mobilian Corporation, 'Wi-Fi™ and Bluetooth™: An Examination of Coexistence Approaches', www.mobilian.com

- [22] Jim Lansford, 'Working Towards the Peaceful Coexistence of Wireless PANs, LANS and WANS', *presented on Communication Design Conference, San Jose, CA*, September 2002
- [23] Beatriz Bardon Rodriguez, Matilde P. Sanchez Fernandez, Ana Garcia Armada, 'Discrete Channel Simulation of Bluetooth Piconets',
http://www.projectmesa.org/ftp/TSG_SYS/Workshops/01_Broadband_Access_Sept2002/Accompanying_papers/Rodriguez.doc
- [24] Wenzhen Li, Masayuki Tomisawa, 'A New Receiver Architecture for Joint Carrier, Channel and Data Estimation for High-Rate WPAN Systems', *IEEE Proceedings of 56th Vehicular Technology Conference*, Vol. 3, pp. 1637-1641, 2002
- [25] The UWB Workgroup; <http://www.uwb.org>
- [26] Nicholas Cravotta, 'Ultrawideband: The Next Wireless Panacea?',
<http://www.uwb.org/files/October2002/EDNOct1702.pdf>
- [27] Terry Mitchell, 'Broad is the Way', *IEE Review* January 2001, pp. 35-39
- [28] Greg Ennis, 'Impact of Bluetooth on 802.11 Direct Sequence Wireless LANs', September 1998,
<http://grouper.ieee.org/groups/802/Regulatory/Regulatory%20Filings/831947a-Impact-of-Bluetooth-on-80211.pdf>
- [29] Saikat Ray, 'An Introduction to Ultra Wide Band (Impulse)', 18 Oct 2001
- [30] M. Nakagawa, Honggang Zhang, H. Sato, 'Ubiquitous Homelinks Based on IEEE 1394 and Ultra Wideband Solutions', *IEEE Communications Magazine*, Vol. 41, April 2003, pp. 74 - 82
- [31] C. E. Perkins, P. Bhagwat, 'Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers', *Computer Communications Review*, pp. 234-244, October 1994
- [32] C.-C. Chiang, H. K. Wu, W. Liu, M. Gerla, 'Routing in Clustered Multihop, Mobile Wireless Network with Fading Channel', *Proceedings of IEEE SICON'97*, pp. 197-211, April 1997
- [33] S. Murphy, J. J. Garcia-Luna-Aceves, 'An Efficient Routing Protocol for Wireless Networks', *ACM Mobile Networks and Applications Journal*, Special Issue on Routing in Mobile Communication Networks. Pp. 183-197, October 1996

- [34] Elizabeth M. Royer, C. K. Toh, 'A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks', *IEEE Personal Communications*, April 1999, pp. 46-55
- [35] C. E. Perkins, E. M. Royer, 'Ad-hoc On-Demand Distance Vector (AODV) Routing', *Proceedings of 2nd IEEE Workshop on Mobile Computing Systems and Applications*, February 1999
- [36] D. B. Johnson, D. A. Maltz, 'Dynamic Source Routing in Ad-Hoc Wireless Networks', *Mobile Computing*, ed. T. Lmielinski, H. Korth, Kluwer Academic Publishers, pp. 153-181, 1996
- [37] C-K Toh, 'A Novel Distributed Routing Protocol To Support Ad-Hoc Mobile Computing', *Proceedings of the 1996 IEEE Fifteenth Annual International Phoenix Conference on Computers and Communication*, pp. 480-486, March 1996
- [38] V. D. Park, M. S. Corson, 'A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Network', *Proceedings of INFOCOM'97*, April 1997
- [39] G. Racherla, J. L. Ellis, D.S. Furuno, S. C. Lin, 'Ultra-Wideband Systems for Data Communications', *ICPWC 2002*, pp. 129-133, December 2002
- [40] Federal Communications Commission Report FCC 02-48, Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband Transmission Systems, First Report and Order,
http://www.fcc.gov/Bureaus/Engineering_Technology/Orders/2002/fcc02048.pdf
- [41] D. Porcino, W. Hirt, 'Ultra-Wideband Radio Technology: Potential and Challenges Ahead', *IEEE Communications Magazine* July 2003, pp. 66-74, July 2003
- [42] F. Legrand, I. Baille, S. Hethuin, L. Nardis, G. Giancola, M-G. Benedetto, L. Blazevic, P. Rouzet, 'U.C.A.N.'s Ultra Wide Band System: MAC and Routing Protocols', *Proceedings of the 2003 International Workshop on Ultra Wideband Systems, IWUWBS 2003*, June 2-5, 2003
- [43] P. Baldi, L. Nardis and M-G. Benedetto, 'Modeling and Optimization of UWB Communication Networks Through a Flexible Cost Function', *IEEE Journal On Selected Areas In Communications*, Vol.20, No.9, December 2002

- [44] J-Y. Boudec, R. Merz, B. Radunovic, J. Widmer, 'A MAC Protocol for UWB Very Low Power Mobile Ad-hoc Networks Based in Dynamic Channel Coding with Interference Mitigation', 2004,
http://cwww.epfl.ch/publications/documents/IC_TECH_REPORT_200402.pdf
- [45] A. Batra, 'Multi-Band OFDM Physical Layer Proposal for IEEE 802.15 Task Group 3a', 15 September 2003
- [46] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu Jorjeta Jetcheva, 'A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols', *Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'98)*, October 1998
- [47] Adrija Biwasa, 'Comparison of Two On-Demand Routing Protocols, DSR and AODV',
<http://comet.ctr.columbia.edu/~jaekwon/E6768/Adrija-presentation.pdf>