UNIVERSITY OF CALGARY

PERFORMANCE ANALYSIS OF IEEE802.11 WLANs WITH EXPOSED NODES

by

Yagazie O. Uhuegbulem

A THESIS SUBMITTED TO THE FACULTY OF GRADUATE STUDIES IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTERS OF SCIENCE

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

CALGARY, ALBERTA

APRIL 2004

UNIVERSITY OF CALGARY

FACULTY OF GRADUATE STUDIES

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies for acceptance, a thesis entitled "Performance analysis of IEEE802.11 WLANs with exposed nodes" submitted by Yagazie O. Uhuegbulem in partial fulfillment of the requirements for the degree of Masters of Science.

Supervisor, Dr. A. O. Fapojuwo,
Department of Electrical and Computer Engineering

Co-supervisor, Dr. A. B. Sesay,
Department of Electrical and Computer Engineering

Dr. B. H. Far,
Department of Electrical and Computer Engineering

Dr. Y. Gao,
Department of Geomatics Engineering

April 23, 2004
Date

Abstract

Mobile stations (MS) using the IEEE802.11 establish virtual connections so as to be able to transmit and receive data over a wireless channel. IEEE802.11 transmissions over the wireless channel are restricted by physical constraints like the available radio spectrum, high error rates of the wireless channel, and that MS can only transmit in the half-duplex mode. The transmissions can also be affected by access problems like the hidden node and exposed node problems. The purpose of this thesis is to investigate the impact that the exposed node problem has on the performance of the IEEE802.11 Wireless Local Area Network (WLAN). The Intelligent Request To Send (RTS) control Algorithm is proposed to solve the exposed node problem and a mathematical analysis of its performance is performed. Simulations are used to validate the analytical performance results. A virtual network is built using the OPNET simulator to test the performance of the Intelligent RTS under different network loads and different mobility ratings. For the Intelligent RTS approach, a 15% channel throughput improvement is observed with a better average frame delay compared to the conventional RTS that incorporates no intelligence. The Intelligent RTS improves the efficiency of the wireless channel by allowing more successful data traffic utilization than the conventional IEEE802.11.

Acknowledgement

I would like to acknowledge TRLabs for providing me with the opportunity and funds to undertake this research and the Cornell Wireless Networks Laboratory for the use of the ZRP routing protocol. OPNET is also acknowledged for allowing the use of their software and for providing technical support.

Dedication

First and foremost I thank GOD for guiding me and giving me strength throughout this thesis work. I dedicate this work to my parents, Sir and Lady B. S. C Uhuegbulem, my brothers Mecky and Iyke and my sisters Ada, Ugy and Chioma for their moral support. I would also like to say thank you to my supervisors Dr. A. O. Fapojuwo and Dr. A. B. Sesay for their patience and for also pointing me in the right directions.

Table of Contents

List of Tables

List of Figures

List of Acronyms, Notations and Symbols

A.I Abbreviations

ACK	Acknowledgement
AP	Access Point
AODV	Ad Hoc On-demand Distance Vector
BRAN	Broadband Radio Access Networks
BS	Base Station
BSS	Basic Service Set
CRC	Cyclic Redundancy Code
CS	Carrier Sensing
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
DCF	Distributed Coordinated Function
DIFS	Distribution Coordination Function InterFrame Spacing
DS	Distribution Systems
DSDV	Destination-Sequenced Distance-Vector
DSSS	Direct Sequence Spread Spectrum
EIFS	Extended InterFrame Spacing
ETSI	European Telecommunications Standard Institute

FCS	Frame Check Sequence
FH	Frequency Hopping
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
IEEE	Institute of Electrical and Electronics Engineers
IR	Infrared
ISM	Industrial, Scientific and Medical band
LAN	Local Area Networks
MAC	Medium Access Control
MS	Mobile Station or wireless device
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency Duplex Multiplexing
PC	Personal Computers
PCF	Point Coordinated Function
PCMA	Power Controlled Multiple Access
PDA	Personal Digital Assistant
QoS	Quality of Service
RSN	Robust Security Network
RA	Receiver Address
RTS	Request To Send
SIFS	Short InterFrame Spacing
SIR	Signal to Interference Ratio
SNR	Signal to Noise Ratio

TA	Transmitter Address
TKIP	Temporal key Integrity Protocol
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless-Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPAN	Wireless Personal Area Networks
WWAN	Wireless Wide Area Networks
ZRP	Zone Routing Protocol

A.II Symbols

a = Normalized propagation delay

$\overline{B}$ = Busy period

c = Normalized transmission time of a control frame

$\overline{C}$ = Average length of the contention period

f = Successful channel time

f_{ctrl} = Time spent transmitting a control frame

f_{data} = Time spent transmitting a data frame

G = normalized offered load

$\overline{I}$ = Idle period

K = Maximum backoff period

P_{CS} = Probability that there is no other transmission in the channel during $[0,2\tau]$

P_{ES} = Probability of success under exposed node condition

P_S = Probability of a success transmission

R = Average number of unsuccessful transmission attempts

S = Throughput

τ = Propagation delay

T_S = Successful transmission delay

$\hat{T}_S$ = Normalized successful transmission delay

$\overline{U}$ = Successful period

X = Average length of the vulnerable period

Z = Backoff period

$\hat{Z}$ = Normalized backoff period

CHAPTER ONE

INTRODUCTION TO MOBILE DATA NETWORKS

1.1 Overview of Mobile Data Networks

The widespread popularity of the Internet and cellular networks like Global System for Mobile Communications (GSM), have led to a demand for mobile data access. The Internet is a means by which a large number of computers can be interconnected like a giant web with the sole purpose of distributing data across the network. The Internet was initially designed as a wired network and was not designed with any form of mobility in mind. All the computers in the network were physically connected to the network and were also stationary devices. The cellular networks completely revamped the telephony industry changing the way people interact with each other. The cellular industry proved that wires were no longer compulsory in order for one device to communicate with one or more other devices. Mobile data networks are a hybrid of the Internet and Cellular technologies. Devices known as Mobile Stations (MS) are able to provide data services to users while on the move. Mobile data networks are categorized into three different networks depending on their coverage area. The different groups of mobile data network are briefly described in the following sections:

1.1.1 Wireless Personal Area Networks

The Wireless Personal Area Network (WPAN) devices have been designed to operate up to a distance of 10 metres. WPAN is designed for normal use in personal and home networking. A WPAN consists of a network of MS's associated with an individual person over a short range. A typical WPAN scenario has an image taken from a camera in a Personal Digital Assistant (PDA) downloaded to a Personal Computer (PC), which in turn connects to a printer to print the image. The IEEE is pushing the IEEE802.15 [1], based on the Bluetooth technology [2], as the standard for WPAN.

1.1.1.1 Bluetooth Technology

Bluetooth uses frequencies around the 2.4GHz range, which is part of the unlicensed Industrial, Scientific and Medical (ISM) band. Bluetooth is being marketed as a low cost and low power device that provides data rates up to 1Mb/s. MS's using the Bluetooth technology are normally organized into clusters called piconets. The number of MS's in a piconet can range from a minimum of 2 to a maximum of 8. A piconet consists of a single master and one or more slave MS's, data is transmitted when the master MS polls the slave MS. The coverage area of the Bluetooth technology can be expanded when an MS belongs to more than one piconet and acts as a bridge that connects these piconets to form a scatternet.

1.1.2 Wireless Local Area Networks

Wireless Local Area Network (WLAN) devices have a distance limitation of 300 metres. The market being targeted by WLAN is the home and office network and is seen as the logical replacement of the Ethernet cable. The Ethernet cable provides the last link of high speed Internet access to the PC and is also used in setting up a peer-to-peer network. WLAN has two competing standards, IEEE802.11 [3] in North America and HiperLAN [4] in Europe. The Institute of Electrical and Electronics Engineers standardized the IEEE802.11 as the North American standard. The European Telecommunications standard Institute (ETSI) under the Broadband Radio Access Networks (BRAN) project standardized HiperLAN as the European standard.

Table 1.1 shows a brief summary of the attributes supported by IEEE802.11 and HiperLAN at the physical and Medium Access Control (MAC) layers. IEEE802.11 and HiperLAN are relatively similar at the physical layer; both use the 5Ghz range of the unlicensed ISM band. The IEEE802.11a/g and HiperLan use Orthogonal Frequency Division Multiplexing (OFDM) as one of their modulation schemes and provide data rates up to 54Mb/s.

Table 1. 1 MAC and Physical layer attributes for IEEE802.11 [3] and HiperLAN [4]

	IEEE802.11			HiperLAN
Current Series	a	b	g	1, 2
Frequency (ISM) band	5GHz	2.4GHz	2.4GHz	5GHz
Max Data Rate (Mb/s)	54	11	54	54
Modulation Scheme	OFDM	Direct Sequence Spread Spectrum (DSSS)	OFDM	Gaussian minimum shift keying, OFDM
MAC	Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)	CSMA/CA	CSMA/CA	Centralized Control Multiple Access

The IEEE802.11 and HiperLAN use different protocols at the MAC layer to access the channel.

1.1.2.1 IEEE802.11

IEEE802.11 implements two different access mechanisms to transmit data, Distributed Coordinated Function (DCF) and Point Coordinated Function (PCF) at its MAC layer. PCF is contention free and is an infrastructure-based network where a centralized base station (BS) coordinates all the traffic in the network while DCF is an infrastructureless based network and MS's contend for the channel using the CSMA/CA protocol to physically sense the channel. In DCF, if the channel has been free for a time equal or greater than a DCF interframe spacing (DIFS), the MS can acquire the channel and then transmit its data. If the channel is sensed busy, the MS defers its transmission until the end of that transmission and then

chooses a random backoff period. The next time the MS is able to contend for the channel is at the end of the backoff period.

The MS uses virtual carrier sensing (CS), where the transmitting and receiving MS's exchange control frames to acquire the channel. The transmitting MS then acquires the channel for a period equal to the duration of transmitting a data frame and receiving a positive acknowledgement. MS's are allowed to contend for the channel when it becomes free.

1.1.2.2 HiperLAN

HiperLAN uses a centralized multiple access scheme. If the channel is sensed free for a certain length of time the MS can transmit its data frame. If the channel is sensed busy, an MS then uses three phases to gain access of the channel namely prioritization, elimination and yield. A synchronization slot follows the end of a transmission. The slot length of the synchronization, prioritization and elimination are the same while that of the yield is smaller. The prioritization phase begins at the end of the synchronization and has 1 to 5 slots. An MS having a frame with priority p transmits a burst in priority p+1 if no higher priority burst was heard. The aim of the priority phase is to allow MS's with the highest priority to contend for the channel.

Only MS's that transmitted a burst in the prioritization phase can contest in the elimination phase. In the elimination phase an MS transmits a burst for a geometrically distributed number of slots and listens for one slot time. If another burst is overheard during the listening period the MS defers transmission. The

MS's with longest burst during the elimination phase move on to the yield phase. In the yield phase the MS's defer transmission for a geometrically distributed number of slots and if any transmission is overheard the MS defer their transmission.

1.1.3 Wireless Wide Area Networks

Wireless Wide Area Networks (WWAN) cover a wide area with ranges up to tens of kilometres. The earlier generations of WWAN supported mainly voice and little amount of data traffic. Supported data traffic is provided at very low data rates. Recent and future generations of WWAN are being designed to offer high data rates for data traffic and still handle voice traffic. For example, the 2.5 generation e.g., General Packet Radio Service (GPRS) and 3rd generation e.g., CDMA2000 are mobile data and voice networks and provide high speed data services. Due to the demand of mobile high-speed data the 2.5-generation was deployed to bridge the data speed deferential between the available low speed 2nd generation and the deployment of the high speed 3rd generation WWANs.

The focus of this thesis is on WLANs. There is an increasing popularity in the use and deployment of WLANs because of its cheap equipment and operating cost. The use of the unlicensed ISM band has contributed in keeping the cost of WLANs down. Also, WLAN devices are affordable with most devices equipped with easily understandable configuration wizards for easy installation, which helps to reduce labour cost. Although the future forecast for WLANs looks very rosy there are still outstanding issues that need to be resolved.

1.2 Research Areas at the IEEE802.11 MAC

Areas in the IEEE802.11 MAC generating a lot of research interests are security, power consumption and MAC channel access. In this thesis, the focus is on MAC channel access.

1.2.1 Security

Security is an area of great concern since the WLAN is used, at certain times, to transmit very sensitive information that would be dangerous in the wrong hands. Also, if the security of the WLAN is breached, a malicious intruder can cause enough havoc that can potentially result in the shut down of the WLAN. Protecting a WLAN is difficult since transmissions are over the wireless channel and any individual with a sniffer can eavesdrop on the ongoing transmission. The security specifications provided by IEEE802.11 standard, the Wired Equivalent Privacy (WEP) [5] have been found to be inadequate for WLANs. WEP uses secret keys, for encryption of data, data integrity and client authentication deployed on both the MS and AP. A major problem with WEP is that it uses a 40-bit secret key size and this is considered to be easily crackable. Even, the longer 104-bit secret key size is also crackable. Other issues with WEP include no effective key management solutions and one-way authentication.

One of the major driving forces for the creation of the Wi-Fi Alliance [6] was to provide a security solution that would be adequate for IEEE802.11 WLANs. Wi-Fi Protected Access (WPA) [7] is the security solution proposed by the Wi-Fi and is compatible with WEP. WPA adds mechanisms for two-way authentication and

provides secure key management. WPA also implements the Temporal key Integrity Protocol (TKIP) to plug the vulnerabilities of WEP and improve the security of IEEE802.11 WLANs. Key sizes made available in TKIP consist of 128-bit for data encryption and 64-bit for data integrity check.

1.2.2 Power consumption

A key selling point for IEEE802.11 is the freedom of movement it gives to users, offering "a world without wires". This freedom does come at a price though, since an MS would have to be battery operated to benefit from the lack of boundaries provided by the mobility features. Currently, batteries have a finite lifetime and would have to be either replaced or recharged at the end of its life cycle. An inefficient MAC protocol could hasten the rate at which an MS would have to power down. The IEEE802.11 MAC supports two modes, active and power saving.

In the active state the MS is fully powered and can either transmit or receive but while in the power saving state the MS is dormant and only wakes up at a periodic interval to check for incoming packets from the AP. An AP periodically transmits beacon frames at fixed beacon intervals. The beacon frame is used to inform MS with frames at the AP to change their mode to active and the remaining MS to change their mode to power saving. The standard did not provide adequate power savings for MS's operating in DCF.

In [8], the MS power consumption is improved when any of the three asynchronous power management protocols proposed is used. The first protocol

proposes an approach whereby an MS remains active long enough for neighboring MS's to become aware of each other. The second approach designs two beacon intervals; one interval has a minimum active window and occurs regularly while the other interval's active window is extended to the maximum occurring at periodic intervals. The final approach is quorum based. Here, a power saving host only sends a beacon as a fraction of all the beacon intervals. The power saving method in [9], tries to find a good balance between the transmitting power and the MAC retransmissions. Increasing the transmitting power produces less MAC retransmissions but more energy is required. On the other hand, reducing the transmitting power results in more retransmissions at the MAC and the channel time is wasted handling unsuccessful transmissions.

1.2.3 Channel Access

An MS has to first gain access to the wireless channel before any type of data can be transmitted. The channel access technique for the IEEE802.11 WLAN is implemented at the MAC layer. In the IEEE802.11 standard, different modulation schemes are proposed at the physical layer but only one access method is proposed. This was done deliberately to allow interconnection between the different physical layer modulation schemes.

The CSMA/CA protocol using virtual CS is the channel access technique accepted for use at the IEEE802.11 MAC, however, the virtual CS is an option that can be turned on or off in an actual deployment. The CSMA/CA is used to prevent the occurrence of collisions because it is expensive to implement collision

detection while the MS is transmitting. The CSMA/CA with virtual CS has been found [10] to have a lower utilization of the channel bandwidth due to the processing overhead for RTS and CTS control frames in some network configurations. New schemes are being proposed as either stand alone or as an enhancement of the existing IEEE802.11 MAC channel access technique.

The IEEE802.11 MAC was designed for MS's to monitor, receive and transmit over a single channel. Due to the wide but limited spectrum available for WLANs, most of the schemes being proposed are in favour of splitting the available channel into multiple sub-channels. The Power Controlled Multiple Access (PCMA) scheme proposed in [11] utilizes busy tone and data channels and also changes the virtual CS specified in IEEE802.11 MAC. The virtual CS implemented at the IEEE802.11 MAC is used to acquire the channel over a fixed transmission range, e.g., 300 metres. In the PCMA scheme the virtual CS is used to exchange power control information. Multiple MS's are able to gain access to the channel simultaneously as long as the power required for the new transmission does not exceed a certain power threshold.

The sending and destination MS exchange request-power-to-send (RPTS) and acceptable-power-to-send-respectively (APTS), to determine the minimum transmission power for successful data frame transmission. An acknowledgement (ACK) frame is sent when the data is received successfully. The RPTS-APTS-DATA-ACK frames are sent in the data channel. The receiving MS sends pulses in the busy tone channel at periodic intervals advertising the additional noise it can tolerate before the ongoing transmission is disrupted or corrupted. Any MS that

needs to transmit alongside the ongoing transmission monitors the busy channel to determine the channel transmission power threshold. The MS can transmit at the minimum transmission power as long as 4 constraints are met:

- Is the transmission power within its parameter range?
- Will the received power at the destination be equal to or greater than the minimum received power threshold?
- Is the observed signal-to-noise ratio (SNR) for the transmission equal to or greater than the minimum signal-to-interference ratio (SIR) threshold?
- Will the addition of a new transmission exceed power transmission threshold of the channel?

The scheme proposed in [12] modifies the existing IEEE802.11 MAC single channel into one common access control channel and multiple traffic channels. MS's in the network monitor the common access channel and maintains a table of the traffic channels that have been reserved for data frame transmissions, as well as the sending and receiving MS's that reserved the traffic channels. The table also contains the time at which the current reservations of the traffic channels expire. MS's exchange control frames over the common access channel and embed in the control frame the traffic channel to use. The sending and destination MS's switches to the specified traffic channel for the transmission of the data frame and accompanying ACK frame.

1.3 Thesis Objectives and Contributions

1.3.1 Thesis Objectives

The radio spectrum allocated for use in IEEE802.11 WLANs is finite. As more users switch from wired LANS to IEEE802.11 WLANs, this can result in the radio bandwidth being oversubscribed. IEEE802.11 WLANs require MAC layers that will utilize the available radio bandwidth efficiently.

The motivation behind this research is to find ways that improve the utilization of the IEEE802.11 MAC. Another key focus of the work presented in this research is to maintain the existing framework of the IEEE802.11 MAC and especially retain the single channel approach currently being used. The objectives of this thesis include:

- Investigate known access issues in the IEEE802.11 MAC protocol [13] that cause the underutilization of the radio resources.
- Propose a viable solution that can resolve the access issues with little or no modification to the existing IEEE802.11 MAC access algorithm.
- Analyze (using renewal theory) the performance of the proposed solution.
- Develop a system level simulation for IEEE802.11 WLANs and modify the tool to evaluate the performance of the proposed solution.
- Compare the performance of the proposed solution with the existing IEEE802.11 MAC access algorithm.

1.3.2 Summary of Contributions

This thesis contributes mainly to the resolution of known access issues in the IEEE802.11 MAC layer. The contributions made in this thesis include:

- The proposal of a modified IEEE802.11 MAC access algorithm.
  - Adding Intelligence to the RTS control frame.
  - The proposed algorithm changes the way the MAC interprets the RTS control frame.
  - By introducing intelligence to the RTS control frames, the performance of the wireless channel is improved.
  - The proposed modified MAC algorithm introduces a higher MAC processing overhead.
- Mathematical Analysis of the proposed MAC algorithm
  - 15% improvement to the channel throughput.
  - Reduction in the end-to-end delay.
- Simulation Analysis of the Proposed MAC algorithm
  - The simulation is used to validate the results obtained from the mathematical analysis.
  - Simulation is also used to test how the proposed MAC algorithm performs under real life scenarios without actually building a WLAN.

1.4 Thesis Outline

The remainder of this thesis is organized as follows: Chapter 2 takes a more detailed look at the IEEE802.11 MAC layer and the access problems that affect the MAC layer. The modified IEEE802.11 MAC access algorithm and the analysis of the proposed algorithm are presented in Chapter 3. In Chapter 4 the developed simulation model of the proposed modification to IEEE802.11 MAC access algorithm is presented. Finally, Chapter 5 presents the main conclusions and suggestions for future work.

CHAPTER TWO

IEEE802.11 MEDIUM ACCESS CONTROL LAYER

2.1 Introduction

This chapter provides a general view of the North American standard for Wireless Local Area Networks (WLANs), known as IEEE 802.11 [14]. The current and future series operating at the 802.11 physical layer are briefly examined. The main focus of this chapter is on the Medium Access Control (MAC) layer. The chapter elaborates on the MAC issues affecting the bandwidth of 802.11 networks and the solutions used to fix these problems. The two 802.11 operating configurations, infrastructure-based and infrastructureless-based 802.11 networks are discussed. Emphasis is placed on the infrastructureless-based 802.11 network and the access algorithm used is described.

2.2 IEEE802.11 Physical Layer

At the physical layer [14] of a transmitting Mobile Station (MS) the data frame, containing information received from high layers of the OSI, is encoded for transmission. The encoded data frame is sent via the wireless channel at a predetermined data rate to the receiving MS. The received data frame is decoded at the physical layer of the receiving MS. The decoded frame, if received correctly, is then sent to the higher layers of the OSI.

The 802.11 physical layer currently has 4 different series operating at various frequencies and at various data rates, as listed in Table 2.1. The first 802.11 physical layer approved operated at the 2.4 GHz range which is the license-free ISM band. This series has two operational data rates of 1Mb/s and 2Mb/s and can operate over radio and infrared media. The radio based WLAN uses Frequency Hopping (FH), DSSS modulation techniques. The next series that became available was the popular Wireless – Fidelity (WI-FI) IEEE802.11b [15], which operates at the 2.4GHz range and uses the DSSS modulation scheme but provides data rates up to 11Mb/s.

Following the IEEE802.11b series, came the IEEE802.11a [16] series operating at 5GHz frequency with amazing data rates of 54Mb/s due to use of the Orthogonal Frequency Duplex Multiplexing (OFDM) modulation scheme. The downside of the IEEE802.11a is that at the operating frequency of 5GHz the pathloss is higher than what is experienced at 2.4 GHz. The consequence is that more IEEE802.11a access points are required to cover a geographical area in contrast to the number of IEEE802.11b access points needed for the same area, this increases the cost of deployment. The IEEE802.11g [17] released recently combines the best features of both IEEE802.11a and b standards. This series operates at the 2.4GHz range, capitalizing on the cost savings available in this radio spectrum range and the OFDM scheme is implemented to provide data rates up to 54 Mb/s.

Table 2. 1 The IEEE802.11series suit

	Modulation Scheme	Supported Data Rate	Frequency Band
IEEE802.11	FH	1Mb/s and 2Mb/s	2.4GHz
	DSSS		
IEEE802.11a	OFDM	6Mb/s, 9Mb/s, 12Mb/s, 24Mb/s, 36Mb/s,48Mb/s and 54Mb/s	5GHz
IEEE802.11b	DSSS	Same as IEEE802.11, also 5.5Mb/s and 11Mb/s	2.4GHz
IEEE802.11g	OFDM	Same as IEEE802.11a	2.4GHz

The 802.11 has several future series, example include 802.11e and 802.11i

I. 802.11e [18] adds Quality of Service (QoS) features and multimedia support to the existing 802.11b and 802.11a wireless standards and maintains full backward compatibility with these standards

II. 802.11i [19] features an upgrade to the Wired Equivalent Privacy (WEP) [20] being currently used by 802.11 devices. WEP is the data encryption algorithm used in 802.11 and it has been proven to be unreliable. Data transmission utilizing the WEP algorithm can be intercepted and easily decrypted by a malicious MS. 802.11i provides two types of encryption: Wi-Fi Protected Access (WPA) and Robust Security Network (RSN) to provide better security for data frames on the channel.

2.3 IEEE802.11 Medium Access Control Layer

To allow for the possibility of connecting between the different series, the 802.11 standardization committee approved only one Medium Access Control (MAC) layer. One of the major issues faced by the 802.11 committee was how MS's were going to interact via the wireless channel. The committee decided to adopt a variant of the contention-based Carrier Sense Multiple Access (CSMA) [21] protocol. The Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is the protocol used to gain access to the wireless channel.

This protocol is required because the wireless channel operates in a half duplex mode: an MS can either receive or transmit at one instant in time and not both. If an MS is receiving a data frame from different MS's, this will result in the combination of the multiple data frames and the MS will not be able to successfully retrieve the transmitted data. The occurrence of this situation is known as a collision and it reduces the efficiency of the wireless channel.

To determine the current status of the channel, an MS uses the CSMA/CA protocol. If the channel is sensed idle, the sensing MS gains access to the channel and transmits its data frame. However, prior to sending the data frame, an MS waits a short period before it actually transmits its data. The waiting time prior to data frame transmission is to prevent collision with a transmission already in the channel because it takes a finite amount of time for that transmission to propagate to all the MS's in the network, due to finite signal velocity.

On the other hand, when an MS senses the channel busy, the MS refrains from transmitting and changes its state from active to backoff. This is necessary to

avoid subsequent collisions. In the backoff state, an MS refrains from monitoring the channel for a random period of time.

There are two situations when an MS changes its current state to the backoff state:

i. When the channel is sensed busy.

ii. When a collision is detected.

In the backoff state, the MS synchronizes the start of the next contention period after a specified time has elapsed since the end of the last frame was detected. The time is divided into time slots where each transmission starts at the beginning of a time slot. An MS chooses a random slot and waits for that time slot to transmit its data, all slots are equally possible for an MS.

Although the implementation of the CSMA/CA protocol would aid an MS in gaining access to the wireless channel, some access issues have arisen from the use of this protocol. The typical access problems identified with the CSMA/CA protocol are discussed in the following sub-sections.

2.3.1 Hidden Node Problem

The sensing range of the CSMA/CA protocol is finite and due to this, an MS is not able to correctly determine the state of the wireless channel resulting in the hidden node problem. The hidden node problem [22, 23] occurs when an MS is out of sensing range but within interference range of another MS. In Fig 2.1, MS A is aware of the presence of MS B but oblivious to the existence of MS C in the wireless network while MS C is only aware of MS B's presence in the network. In

this scenario MS A and MS C are "hidden" from each other. If MS C was to transmit to MS B at approximately the same time as when MS A was transmitting to MS B, a collision is observed at MS B.

The occurrence of the hidden node problem in a wireless network results in collisions, which in turn reduces the efficiency of the wireless channel.

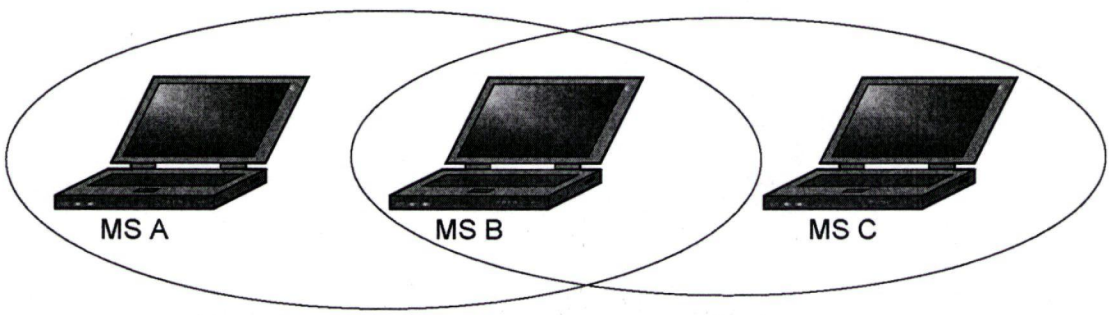

Figure 2. 1 The Hidden Node Problem

2.3.1.1 Solution Approaches to the Hidden Node Problem

Virtual carrier sensing [21] is used to solve the hidden node problem. This approach requires the handshaking of control frames between two MS's in order to acquire the channel. Additional function of the control frames is to inform other MS's within the sender's sensing range of its intention to utilize the channel. The 802.11 uses three types of control frames:

2.3.1.1.1 Request To Send frame

An MS with a data frame to send tries to acquire the channel by broadcasting a Request To Send (RTS) control frame into the channel. The

broadcasted RTS frame notifies all MS's within the sender's sensing range that the channel would be acquired for a certain period of time. The MS's in the network respond to this request by suspending any attempt to acquire the channel. The broadcasted RTS is also used to inform the intended destination MS to be prepared to receive the data frame.

Fig. 2.2 shows the RTS control frame structure and its control field. The frame control, duration, transmitter address (TA) and the receiver address (RA) are called the MAC header.

I. The frame control is 16 bits long and contains the following fields [14]:
   a. Protocol Version field is 2 bits long and it functions as a way to alert MS's to the presence of an incompatible MS in the network.
   b. Type field is 2 bits long and the Subtype field is 4 bits long and are used to indicate what type of frame is being sent or/and received. Typical frame types are data frames, control frames and management frames.
   c. To DS field is 1 bit long and is set to 1 in data type frames destined for the distribution system (DS). The DS is used to interconnect WLANs to integrated local area networks (LANs).
   d. From DS field is 1 bit long and is set to 1 in data type frames exiting the DS. It is set to 0 in all other frames.
   e. More Frag field is 1 bit long and is set to 1 when the sent data has more fragments, else the value is 0.

f. Retry field is 1 bit long and is set to 1 when the data frame to be sent is a retransmission of an earlier unsuccessful transmitted data frame. Otherwise, the retry field has a value of 0.

g. Pwr Mgt is 1 bit long, is set to 1 when an MS is in power saving mode and 0 when the MS is in active mode.

h. More Data is 1 bit long and is used in infrastructure-based WLAN to inform an MS in power saving mode that there is more data for it.

i. WEP is 1 bit long and is set to 1 if the WEP algorithm has processed the data frame.

j. Order is 1 bit long and is set to 1 if a data type frame that contains a fragment is being transferred using the StrictlyOrdered service class.

II. Duration field is 16 bits long and is used to update the Network Allocation Vector (NAV) and its value is the time it takes to transmit a Clear To Send (CTS) frame, the pending data frame, an ACK frame and three short interframe space (SIFS) intervals.

III. Receiver address (RA) field is 32 bits long and contains the IEEE MAC address of the MS where the RTS frame is destined.

IV. Transmitter address (TA) field is 32 bits long and contains the IEEE MAC address of the MS that the RTS frame originated from.

The frame check sequence (FCS) contains an IEEE 32-bit cyclic redundancy code (CRC) and is used to check the integrity of the frame received. The FCS helps a destination MS determine if a collision occurred.

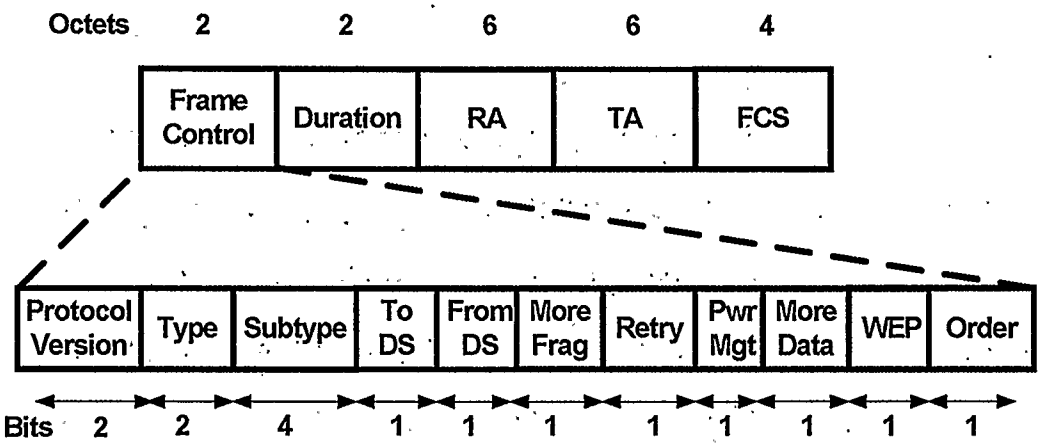

Figure 2. 2 RTS Control Frame Structure

2.3.1.1.2 Clear To Send frame

The Clear To Send (CTS) frame, like the RTS, is used to inform all the MS within the sender's sensing range that the channel will be occupied for a certain length of time. The main function of the CTS control frame is to inform the MS from whence the RTS originated that the destination MS is prepared to receive the data frame.

The frame structure and fields of the CTS control frame, shown in Fig. 2.3, are the same as that of the RTS control frame but with one exception; there is no TA field. The RA of the CTS frame is copied from the TA field of the RTS frame to which the CTS frame is a response. The duration value is the value obtained from the duration field of the RTS frame being replied. It is the time to transmit the pending data frame, an ACK frame and two SIFS intervals.

Octets	2	2	6	4
	Frame Control	Duration	RA	FCS

Figure 2. 3 CTS Control Frame Structure

Only upon the completion of this handshaking can the data frame be broadcasted into the channel. After the RTS control frame has been transmitted the sending MS expects the CTS control frame to indicate successful handshaking. If the CTS control frame is not received within a specified time the CTS control frame times out. The sending MS enters the backoff state and the exponential backoff algorithm is implemented to choose the backoff period. The backoff algorithm chooses a random integer from a uniform distribution over the interval [0, contention window (CW)]. The size of the contention window varies depending on whether the frame to be transmitted is a new transmission or a retransmission.

The CW has an initial size of 7 for IEEE802.11 and up to 31 for IEEE802.11b. The CW increases after each unsuccessful transmission to a maximum permitted by the standard for 0-255 for IEEE802.11 and up to 0-1023 for IEEE802.11a. Once the maximum value for the contention window is reached, the CW will stay at this value until the data frame is successfully transmitted or discarded when the maximum number of retransmission attempts is reached.

The backoff time is obtained by multiplying the random integer with the duration of a slot for the particular IEEE802.11 series. The backoff slot begins after the channel has been idle for a time greater or equal to the DIFS period. Slot

duration is set to 9 and 50 microseconds in IEEE802.11a and IEEE802.11b, respectively. The backoff procedure will decrement its backoff timer by a slot duration, if no activity is sensed in the channel. The backoff timer is suspended when any activity is sensed in the channel with the backoff timer resuming after the channel has been sensed idle for a time greater or equal to the DIFS period. The transmission is started when the backoff timer reaches zero. After the data frame is successfully transmitted the CW is reset back to the initial size.

2.3.1.1.3 Acknowledgement frame

The Acknowledgement (ACK) frame is broadcasted upon the successful receipt of the data frame and is used to acknowledge a successful data transmission. If the ACK is not broadcasted within an ACK time limit, the sending MS assumes that a collision has occurred and enters the backoff state. The MS would have to contend for the channel before it can retransmit the data frame.

Fig. 2.4 shows the frame structure and fields of the ACK frame. The bits of the frame control field are the same as that described in Fig. 2.2. The More frag bit (a sub-field of frame control field) is set to 1 when there are more fragments of the message (being acknowledged) to be transmitted. If the More frag bit is set to 1, the value of the duration field becomes the time to transmit the new data frame, the corresponding ACK frame and a SIFS interval. The duration field and the More frag bit are set to 0 when there are no more fragments of the message expected.

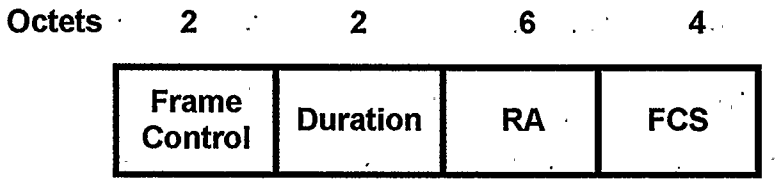

Figure 2. 4 ACK Control Frame Structure

Fig 2.5 illustrates the use of the control frames to solve the hidden node problem. Using the earlier scenario depicted by Fig. 2.1, MS A broadcasts an RTS and then waits for the CTS from MS B. After a little while MS C, unaware of RTS transmission by MS A, also sends an RTS to MS B. MS B first receives the RTS from MS A before receiving that from MS C. MS B then sends a CTS to MS A accepting its request. MS C receives the CTS from MS B to MS A and stops its attempt to acquire the channel for a certain period of time. MS A sends the data frame after receiving the CTS frame and MS B sends the ACK frame after the data frame has been received.

2.3.2 Exposed Node Problem

The exposed node problem [13, 23], unlike the hidden node problem, has not been addressed in the 802.11 standard. The exposed node problem occurs when an MS is within sensing range but out of interference range of another MS. The exposed node problem is further intensified by the use of the control frames. Fig 2.6 is used to show two scenarios when the exposed node problem can occur.

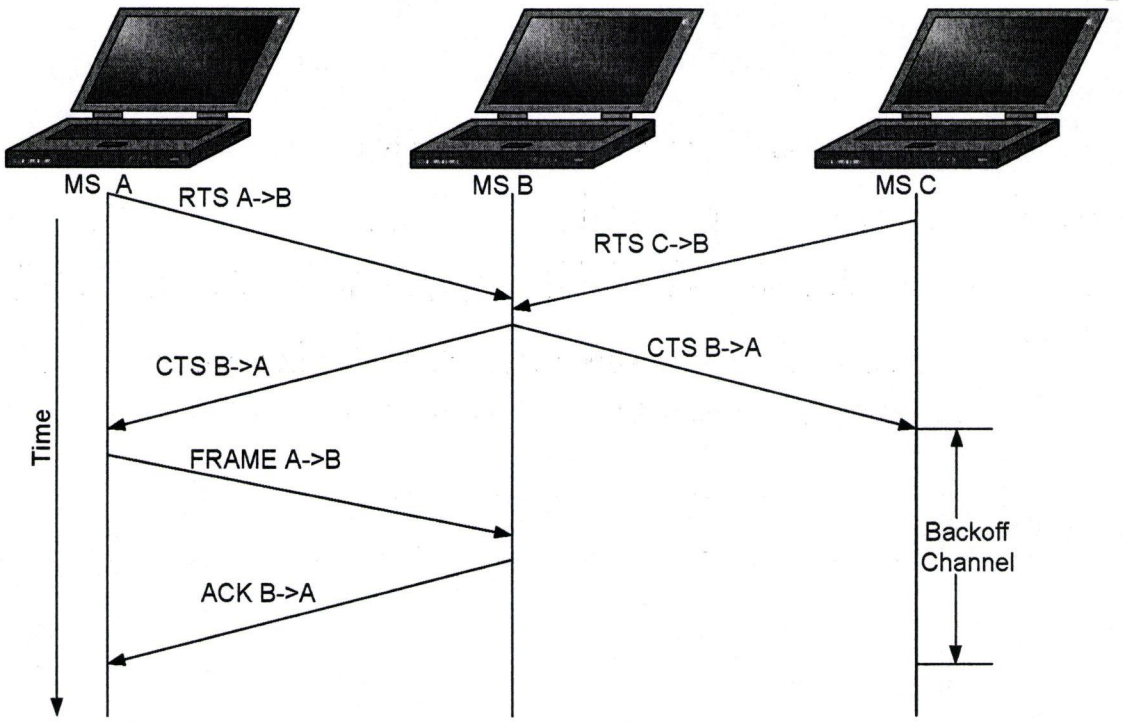

Figure 2. 5 Timing diagram illustrating the use of RTS and CTS frames to solve the hidden node problem

In scenario 1, MS C is transmitting to MS D and MS B can physically sense MS C's transmission in the channel. The CSMA/CA protocol stipulates that if the channel is sensed busy, the sensing MS must backoff from the channel to prevent the occurrence of collision.

From Fig. 2.7, MS B senses MS C's transmission before receiving a CTS from MS A. MS B should be able to successfully transmit to MS A without interfering with MS C's transmission in the channel but instead refrains from transmitting. MS B is "exposed" to the transmission of MS C. The transmission by

MS B to MS A will then have to be rescheduled and MS B would have to contend for the channel before it can transmit the rescheduled frame. The effect is underutilization of the wireless channel.

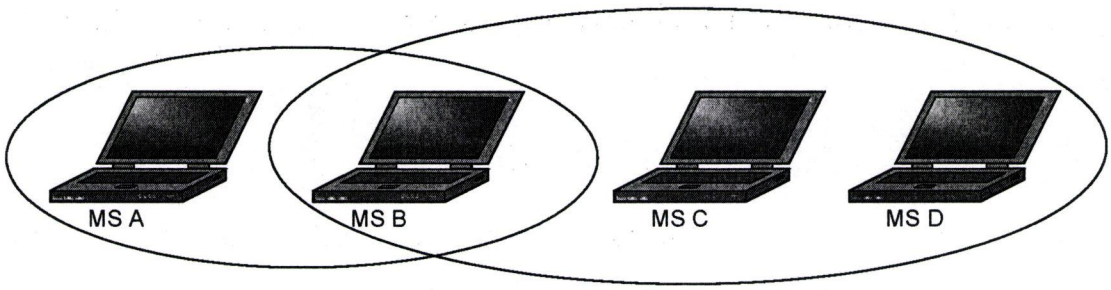

Figure 2. 6 A WLAN with the exposed node problem

In scenario 2, MS D is transmitting to MS C but MS B is "hidden" from MS D and cannot sense this transmission. If virtual carrier sensing is used to acquire the channel, and solve the hidden node problem, MS B now becomes "exposed" to the CTS transmission by MS C to MS D. In Fig. 2.8, MS A has successfully negotiated the channel but before MS B can receive the data frame, the CTS from MS C to MS D arrived.

MS B then backs off from the channel. MS A, not aware of the change in the channel, transmits its frame to MS B. Although MS B has backed off the channel, it would receive the frame from MS A but does not send an ACK frame to MS A acknowledging receipt of the data frame. MS A, after waiting for a period of time without receiving the ACK frame, reschedules the data frame for retransmission.

MS A then contends again for the channel to retransmit an already successful transmitted frame instead of transmitting a new frame.

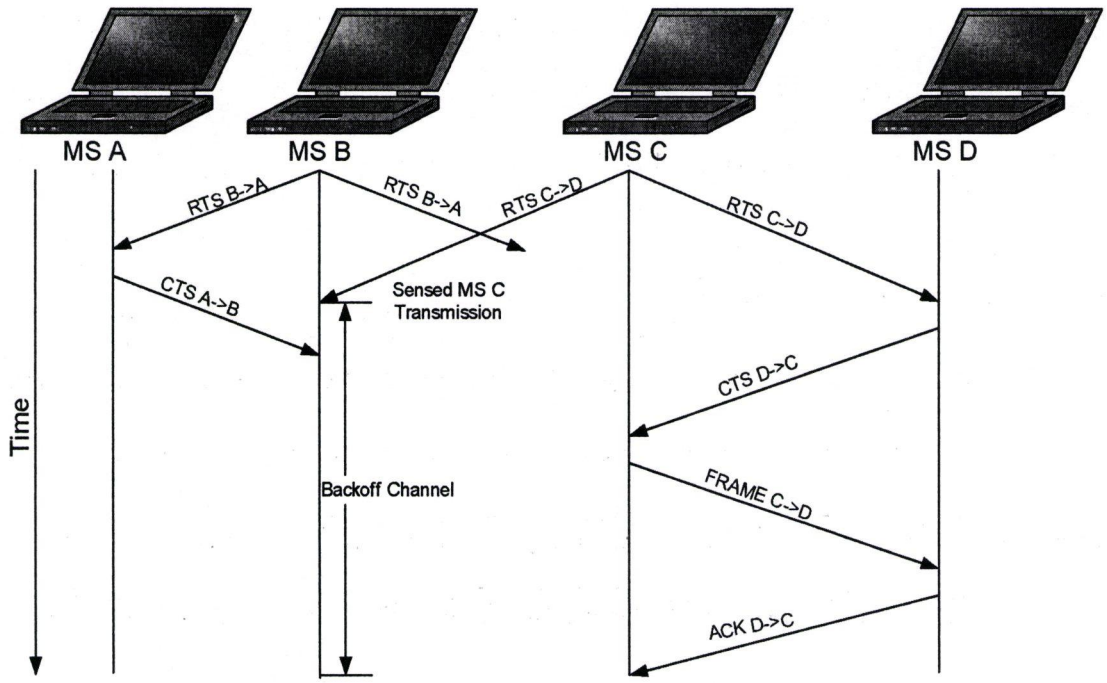

Figure 2. 7 Timing diagram illustrating exposed node caused by the CSMA/CA protocol

The exposed node problem causes the underutilization of the channel bandwidth. With the popularity and continuous deployment of the 802.11 networks, the exposed node problem stands to be a major hindrance if not addressed. There is further need to optimize 802.11 networks because the radio spectrum available for wireless networks is limited.

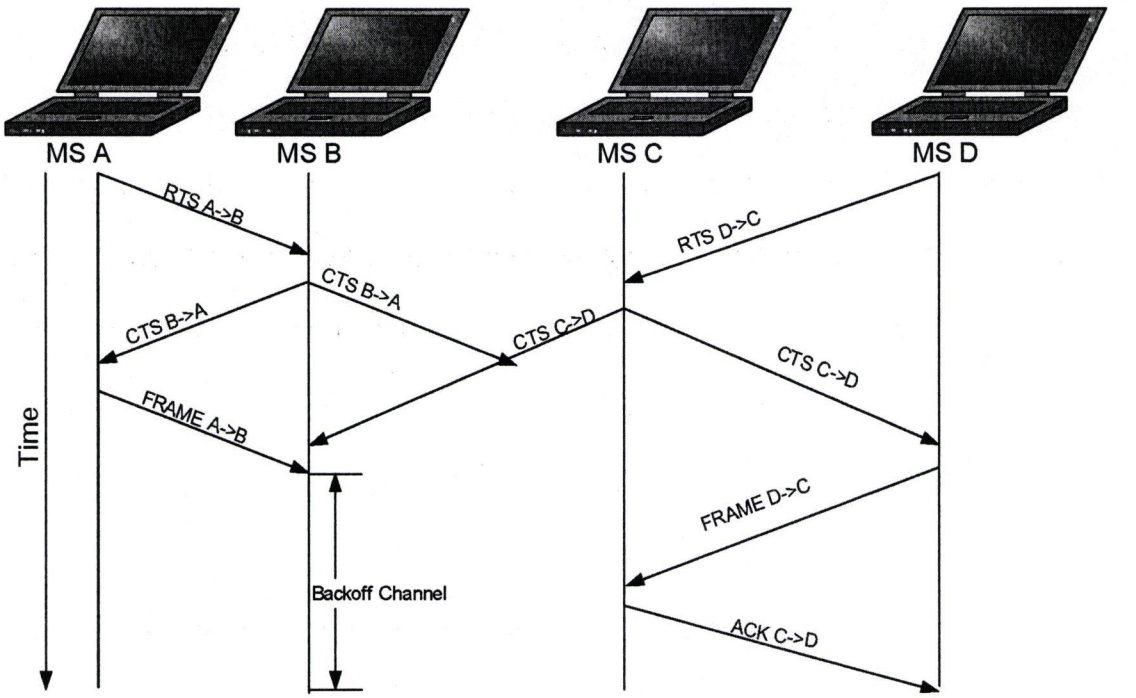

Figure 2. 8 Timing diagram illustrating exposed node problem observed from virtual carrier sensing

2.4 Types of 802.11 Networks

There are two types of 802.11 network configurations available for data transfer. These two configurations are used under different operating conditions. The configurations are explained below:

2.4.1 Infrastructure-based 802.11 WLANs

The infrastructure-based [14] WLAN is a borrowed concept from the Wireless Wide Area Networks (WWAN) and WLANs. The WWANs have a BS that coordinates all traffic within a certain region called a cell. Only one BS can exist in

a cell. This is the same with the infrastructure-based WLAN, which has an Access Point (AP) that all MS's in a certain region called a basic service set (BSS) must communicate through. The AP routes data to MS's within its BSS. If the destination MS is not within the BSS, the AP tries to locate the AP where this MS is located and then routes the data to that AP which then transmits the data to the destination MS. All MS's, on entering a BSS, must register with the serving AP so that the MS's can be associated with that AP before it can be allowed to send data.

In Fig. 2.9, MS A, MS B and MS C are associated with the AP in the BSS. MS A generates a frame for MS C and sends the frame to the AP, which then checks if MS C is in its BSS table. Since MS C is already associated with the same BSS, the AP then sends the frame to MS C.

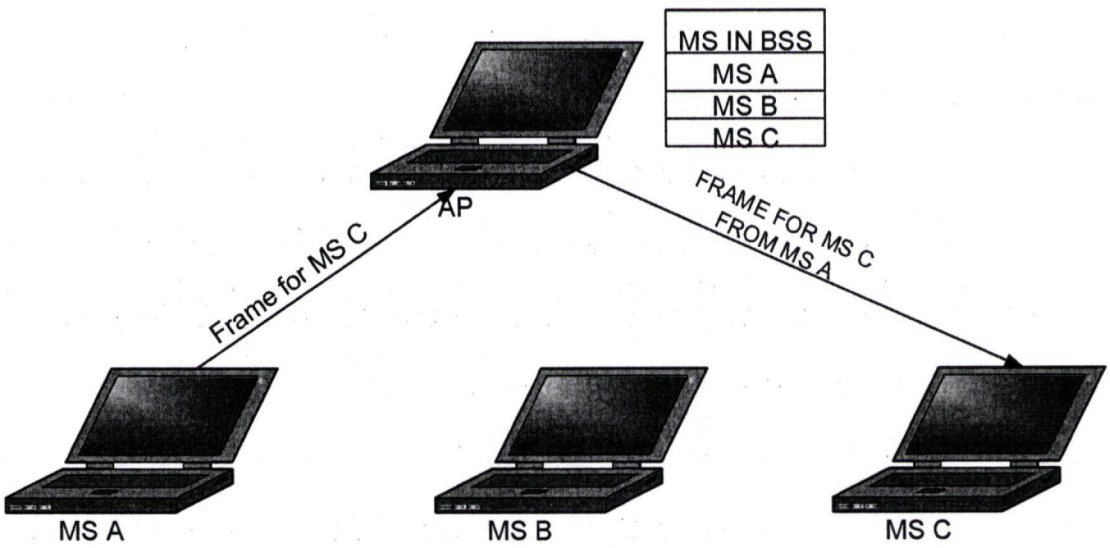

Figure 2. 9 Illustration of an infrastructure-based WLAN, (one BSS)

2.4.2 Infrastructureless-based 802.11 WLANs

The infrastructureless-based [14] networks, as the name implies, have no centralized AP. In this type of networks, shown in Fig. 2.10, an MS can transmit to or receive data by directly communicating with the receiving or sending MS. Also, if the destination MS is not directly reachable, the sending MS creates a virtual map to the destination MS that includes one or more intermediary MS's. The MS then routes the data to the destination, via the MS's in the virtual map.

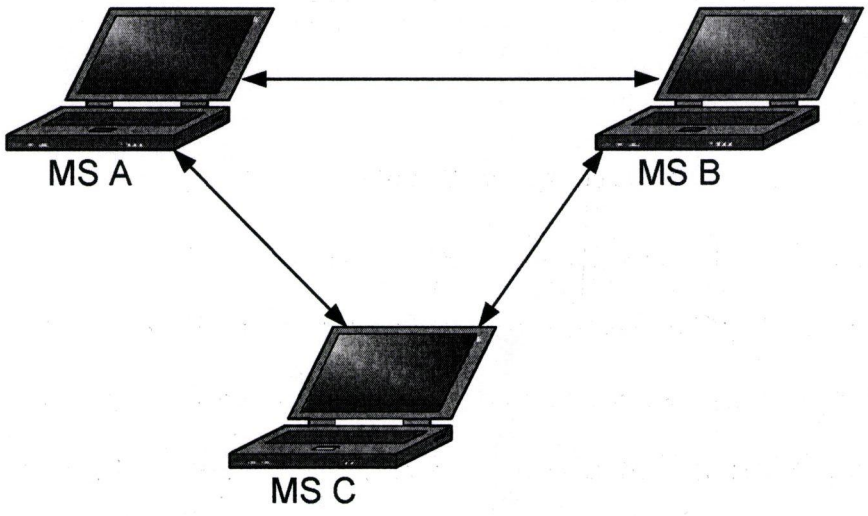

Figure 2. 10 Illustration of an infrastructureless-based network

The infrastructureless-based networks can implement different types of routing protocols to aid in constructing the virtual network map, stored in a routing table. There are three ways a routing table can be constructed:

2.4.2.1 *Proactive Routing Protocol*

Proactive routing protocols are also known as table driven routing protocols. Networks create a routing table and this table is consulted to determine the location of the destination MS before the data can be transmitted. The routing table is constructed at the time of entering into the network and is updated at periodic intervals or if there is a change in the network topology. The proactive routing protocols are effective in a network with a constant topology with less periodic updates required. Proactive routing protocols are not very efficient in a network with a changing topology, for every change in the topology results in an update of the routing table. This can result in the network being flooded with routing information and less time spent on actual data transfer. The Destination-Sequenced Distance-Vector (DSDV) [24] routing protocol is an example of proactive routing.

2.4.2.2 *Reactive Routing Protocol*

The reactive routing protocol can also be called on-demand routing. The reactive routing protocol does not maintain a routing table but creates a route only when required. These types of routing protocols are usually used in networks with changing topologies and less routing information are sent into the channel but suffer from the delay in setting up the routes. This protocol is less favourable in a network with no mobility because the same route will have to be rediscovered each time before the data can be transmitted. The Ad Hoc On-demand Distance Vector (AODV) [24] routing protocol is an example of reactive routing.

2.4.2.3 *Hybrid Routing Protocol*

The hybrid routing protocol combines both proactive and reactive routing protocols to build efficient routing tables regardless of the network topology. The hybrid routing uses the proactive routing to construct a routing table for its direct neighbours. This helps when there is a topology change and the amount of routing information sent into the channel is reduced compared to only using a proactive routing protocol. Also, there is no need to request the route for the direct neighbor as would have been the case if a reactive protocol is implemented. The hybrid routing protocol uses the reactive routing protocol to route its data to MS's that are out of range from direct communication. The Zone Routing Protocol (ZRP) [25] is an example of hybrid routing.

The infrastructureless-based networks can be used to extend the coverage of an infrastructure-based network or can be used to set up a network where an infrastructure-based network is not available. Infrastructureless-based network are easy to setup and are usually temporary (or ad-hoc) networks.

The MAC layer issues discussed earlier in this chapter, hidden node and exposed node problems, are more pronounced under the infrastructureless network configuration. The work carried out in this thesis is focused on the infrastructureless network configuration.

2.5 802.11 Medium Access Control Algorithm for Infrastructureless-based Networks

This section describes the IEEE802.11 MAC layer algorithm [14]. An MS listens to the channel to access the current state of the channel before it can attempt to transmit any data. If the channel is physically sensed busy the MS defers its transmission. The channel is presumed idle, after the Distributed Coordinated Function interframe space (DIFS) has elapsed without interruption since the last frame detected in the channel was received correctly. If the last frame was not received correctly, the channel is considered idle after the extended interframe space (EIFS) has elapsed without interruption.

At the end of the DIFS, if the channel is still sensed free, virtual carrier sensing is used to establish a virtual connection. Virtual carrier sensing uses the RTS/CTS frames to perform handshaking between the sending and receiving MS's. The sending MS transmits an RTS frame to the destination MS. When the RTS has been received successfully, the destination MS sends a CTS frame to the sending MS. The sending MS then transmits each data frame to the destination, which sends an ACK after receiving each data frame successfully. If no ACK is received, the sending MS has to retransmit the data frame at a later time and also has to go through this handshaking scheme each time it tries to transmit. No actual data transmission can commence without the full completion of the two-way handshaking scheme. The algorithm used when the channel is sensed idle is shown in Fig. 2.11.

The channel is a broadcast channel and the control frames are also used to warn other MS's linked to the channel of the channel's current status. Any MS, other than the MS's negotiating the virtual connection, upon hearing the RTS frame in the channel defers its attempt of using the channel. The deferring MS's then adjusts their Network Allocation Vector (NAV) if the time specified in the RTS frame is greater than the current NAV time. The NAV time indicates to the deferring MS's how long the ongoing transmission will occupy the channel. The same procedure is performed if the deferring MS's received the CTS frame. The NAV time of the MS receiving the CTS frame is shorter than the MS that received the RTS frame. An MS that is kept from using the channel has to contend for the channel before making another attempt to use the channel.

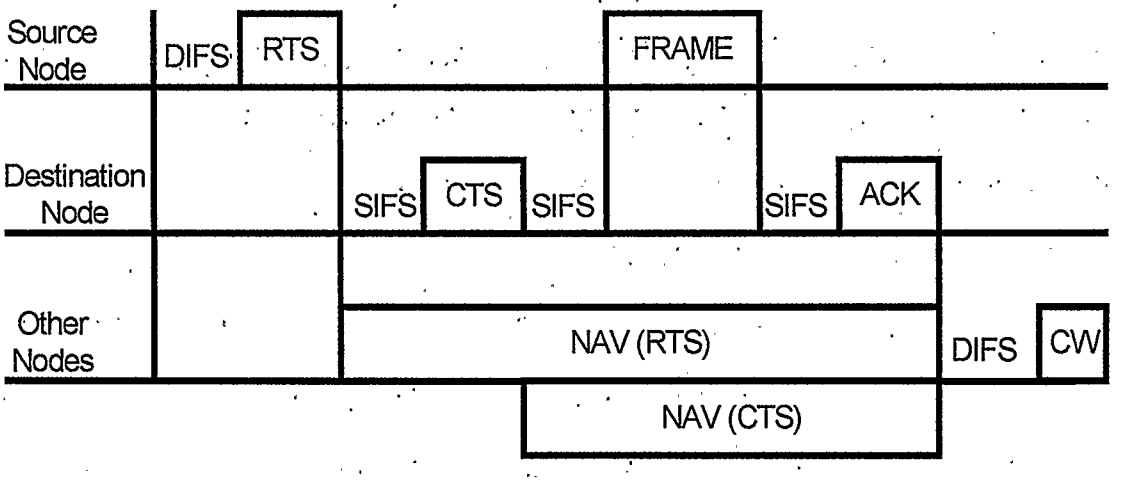

Figure 2. 11 IEEE802.11 Algorithm when channel is sensed idle

If the channel is sensed busy, each deferring MS shall enter the backoff state and randomly selects an integer from the contention window. The backoff timer is determined by multiplying the random integer with the slot time. The deferring MS would choose the corresponding backoff slot after the channel is sensed idle for a period greater than the DIFS or EIFS time. The MS reduces the backoff timer by a factor of the slot time, whenever the backoff slot is physically sensed idle. If the backoff slot is sensed busy, the MS suspends the backoff timer and does not reduce the timer for that slot. The backoff timer would not resume until the channel has been sensed idle for a period greater than the DIFS or EIFS. The MS attempts to set up a virtual connection with the destination MS when the backoff time reaches zero. Fig. 2.12 shows the steps taken by an MS before it can attempt to transmit its frame if the wireless channel was sensed busy [14].

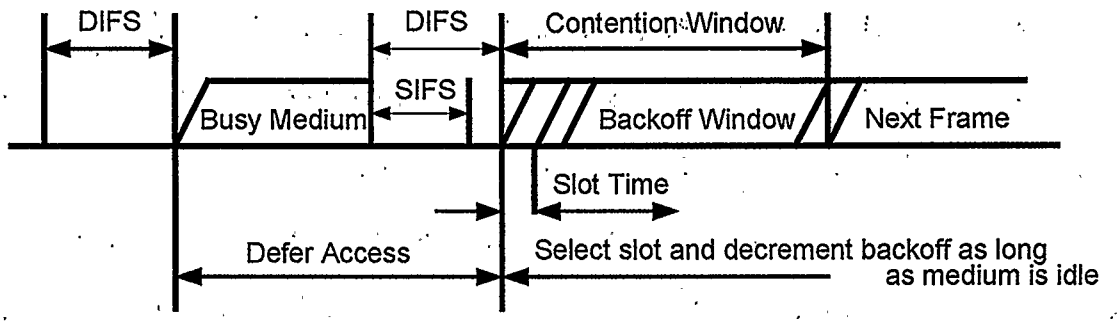

Figure 2. 12 IEEE802.11 Algorithm when channel is sensed busy

2.6 Summary

This chapter presented an overview of the IEEE802.11 standard. The data rates and the operating frequency available for the different 802.11 series at the physical layer were described. Next, the MAC layer is described and the issues affecting the bandwidth utilization, namely, the hidden node and exposed node problems are presented. The mechanism used to solve the hidden node problem is discussed but the exposed node problem is yet to be addressed and the IEEE has proposed no solution. The 802.11 networks can operate under two different configurations, infrastructure-based and infrastructureless-based networks. It is explained that the exposed node problem is more pronounced in the infrastructureless-based network because there is no central MS and all MS's in the network have to coordinate their transmissions. The next chapter presents the proposed solution to the exposed node problem in IEEE802.11 networks.

CHAPTER THREE

PROPOSED ENHANCEMENT TO IEEE802.11 MEDIUM ACCESS CONTROL ALGORITHM

3.1 Introduction

In this chapter an algorithm is proposed that improves the performance of IEEE 802.11 networks. The main features of the algorithm are presented, followed by a description of its operation. A mathematical analysis of the performance of the proposed algorithm is presented. Numerical results obtained from the mathematical analysis are presented and discussed.

3.2 Proposed Enhanced 802.11 MAC Algorithm

3.2.1 Features

The main feature of the proposed algorithm is to add an extra function to the RTS-CTS control frames. MS's will use the channel access information obtained from this new function to interpret the current channel condition. In the IEEE802.11 algorithm the key control frames channel access functions include:

I. Setting a virtual connection between the transmitting and receiving MS's.
II. Informing the neighboring MS's that the channel is occupied.
III. Informing MS's how long the channel will be occupied.

The purpose of the added function is to add intelligence to the ways MS's interpret the RTS control frames. MS's will use transmitted control frames to help decide if it is safe to transmit when activity has already been sensed in the channel. The MS will rely on the RTS control frame not only for information about the ongoing transmission in the channel but also a major component in determining whether the MS is an "exposed node". By implementing this new function to the IEEE802.11 algorithm the exposed node problem can be tackled. The rest of the chapter describes the proposed algorithm and the mathematical analysis to evaluate its performance.

3.2.2 Intelligent RTS Algorithm

In this approach an exposed MS listens to the control frames in the channel and from this information decides whether it can attempt establishing a connection with another MS. This proposed solution modifies the existing MAC layer protocol as follows.

The exposed MS compares the address from the RA field and the TA address field contained in the RTS control frame, with the address of its destination MS in determining whether to transmit. If any of the addresses in the control frame is the same as that of its intended destination address, the exposed MS refrains from using the channel. However, if the addresses are different the exposed MS can use the channel alongside the transmission in the channel.

An MS, on receiving an RTS control frame, first checks the RA field contained in the control frame. If the MS is not involved in the ongoing channel

negotiations and has no data frame to send, the MS enters and sets its NAV time or stays in the backoff state. If a data packet arrives from the higher layers, the MS retrieves the address information stored from the control frame received for the ongoing transmission(s) in the channel. It then compares the RA and TA obtained from the RTS control frame with its intended destination. If any of the addresses match, the MS remains in the backoff state and completes the backoff routine. The MS will contend for the channel, as stipulated in IEEE802.11 MAC algorithm when next the channel is deemed idle.

If none of the addresses match, the MS waits an additional DIFS time as a precautionary measure to ascertain that it is up to date with the channel activity. If a new RTS control frame is received within the waiting period, the MS will have to repeat the whole procedure. The MS will execute the backoff routine if a CTS frame is received. The CTS frame only contains the RA field and the MS will not be able to accurately access the channel. If no further control frame is received, the MS will then attempt to establish a virtual connection with its intended destination. Fig. 3.1 shows the new MAC algorithm used when the channel is sensed busy. The italics in bold font indicate the modification in the algorithm that an MS would have to execute to solve the exposed node problem.

3.2.2.1 Optimized Intelligent RTS

Introducing a destination preventive scheme optimizes the Intelligent RTS algorithm. The destination preventive scheme prevents an exposed MS from transmitting its data frame if its intended destination MS is within transmission

range of an ongoing transmission. Before this scheme can be implemented, each MS would have to make a table of the MS's it can access and this table can be broadcasted in the channel with the routing information. An MS on receiving the table creates a new table called the neighbor's table that keeps track of the MS neighbors and that neighbor's neighbors. The ZRP routing protocol creates and maintains a proactive routing table at each MS, which contains the address of MS's that are 1 hop reachable. The routing protocol can be modified to broadcast the routing table at periodic intervals or if there is a change to the routing information.

From Fig. 3.1, an exposed MS implements the exposed routine after comparing the contents of RA and TA fields with its intended destination MS. The exposed MS consults the neighbor's table and then retrieves the addresses of the MS's that are the neighbors of the destination MS. The exposed MS compares the neighbors addresses of the destination MS with the RA and TA. The exposed MS continues to process the exposed routine, if none of the addresses match. On the other hand if a match is found, the backoff exponential algorithm (section 2.3.1.1.2) is executed.

Step 1

Receive RTS control frame.

Step 2

Retrieve RA from the RA field.

Step 3

If the RA is the same as the MS address, send CTS frame.

If RA is not the same as the MS address, check if any data frame to transmit.

Step 4

If no data frame to transmit, execute backoff routine.

Step 5

Execute exposed routine, if there is a data frame to transmit.

Step 6

/*Exposed routine*/

Retrieve TA from TA field.

Compare TA and RA with destination address.

If the destination address matches either the TA or RA, execute backoff routine.

If the destination address matches neither the TA nor RA, wait DIFS.

If a new RTS frame is received before the DIFS expire, go to step 1.

If CTS frame received, execute backoff routine.
If DIFS expire without receiving a new control frame, use channel.

Figure 3. 1 Proposed MAC Algorithm for solving the exposed node problem

3.3 Impact of Proposed Algorithm on IEEE802.11 Network Elements

This section looks at the impact of introducing RTS control frame intelligence to the IEEE802.11 Elements. The areas being looked at where the proposed algorithm would have an impact include:

- The IEEE802.11 MAC Layer: As no new control frames or control frame element is being introduced, there will be no added processing overhead in the channel. The cost to be paid will be the additional processing required when the intelligent algorithm is implemented. The proposed intelligent MAC and IEEE802.11 MAC algorithms access the channel the same way when the channel has been sensed idle hence there will be no increase to the processing cost. In the case when the channel is busy and the proposed intelligent MAC algorithm is enabled, there is an increase of up to 400% to the computing process. This increase is mainly due to the additional steps that have to be processed in the proposed intelligent MAC algorithm. With the processing speed of microprocessors on the rise, the increased processing cost will not hamper the MAC layer.
- Compatibility with the IEEE standard: The proposed intelligent MAC algorithm can be implemented via a software patch and should not require external hardware. The virtual CS is an integral part of the proposed intelligent MAC algorithm and has to be always on. In networks where the virtual CS is switched off the Intelligent RTS cannot be implemented. There are no compatibility issues if the virtual CS is switched on.

3.4 Performance analysis of the Intelligent RTS algorithm

The performance of the proposed MAC algorithm is evaluated using the original CSMA/CA with virtual CS but is modified to account for the features of the proposed enhancements. This approach simplifies the performance analysis of the

MAC protocol but produces results that should hold for all MAC protocols that implement CSMA/CA with virtual CS. The key metrics of the performance, channel throughput and average frame delay, are analyzed mathematically.

3.4.1 Analysis Assumptions

The assumptions used for the performance analysis are listed below:

A1. Frame arrivals to the channel are random and follow a Poisson process.

A2. A complete channel cycle time consists of a busy period and an idle period, where the idle period can have a time length of zero.

A3. RTS/CTS frames are used to acquire the channel.

A4. The propagation delay, τ, is the maximum time it takes for all nodes within hearing range to hear the transmission on the channel.

A5. Two or more stations can successfully acquire the channel simultaneously.

A6. All transmissions after the channel has been acquired using the RTS-CTS control frames are successful.

A7. RTS and CTS have the same length.

A8. Maximum backoff limit is fixed.

3.4.2 Throughput analysis

The throughput, S for the Intelligent RTS algorithm is obtained using renewal theory arguments [26]:

$$S = \frac{\bar{U}}{\bar{B} + \bar{I}} \tag{3.1}$$

where $\overline{U},\overline{B},\overline{I}$ are the average length of successful, busy and idle periods, respectively. In CSMA/CA with virtual CS the probability of a successful transmission, P_{CS}, is the probability that there is no other transmission in the channel during $[0,2\tau]$. The time interval 2τ is the time taken to send a RTS frame and receive a CTS frame acknowledging successful channel acquisition. Based on the Poisson arrival process, the expression for P_{CS} is given by:

$$P_{CS} = e^{-2G\tau/f} \tag{3.2}$$

where *G* is the channel normalized offered load, τ is the propagation delay and f is the successful channel time. The successful channel time, f, is the sum of transmission time of the RTS and CTS control frames required to acquire the channel and the actual data frame transmission time, f_{data}.

For the exposed node scenario the probability of success changes, since an exposed node occurs when a node has a frame to transmit and should be able to transmit but defers transmission because the channel is sensed busy. The probability of success under exposed node condition, P_{ES}, is the probability of at least one transmission already in the channel during $[0,2\tau]$ and the probability that the new transmission is successful. Mathematically,

$$P_{ES} = (1-e^{-2G\tau/f})e^{-2G\tau/f} \tag{3.3}$$

Note that P_{ES} only considers the occurrence of exposed nodes, but this does not give a complete analysis of the channel since there are situations where only one node has a frame to transmit and the other nodes within hearing range are idle. With these in mind, the channel probability of success, P_S, becomes the probability that the channel is idle when a frame arrives or that at least another node within hearing range is transmitting and the new arrival is successful. Hence,

$$P_S = P_{CS} + P_{ES} \tag{3.4}$$

Substituting Equations (3.2) and (3.3) into (3.4) gives

$$P_S = e^{-2G\tau/f} + (1 - e^{-2G\tau/f})e^{-2G\tau/f} \tag{3.5}$$

The average length of successful transmission period, $\bar{U}$ is given by:

$$\bar{U} = f_{data}(e^{-2G\tau/f} + (1 - e^{-2G\tau/f})e^{-2G\tau/f}) \tag{3.6}$$

An idle period occurs when there are no arrivals in the channel or after the conclusion of a busy period. The idle period ends as soon as the first arrival enters into the channel. By assumption A1, the arrivals into the channel follow a Poisson process and the channel also inherits the memoryless property of the Poisson process. The average wait time for a new arrival from any random chosen point is equal to the mean of the inter arrival time distribution. The station also waits an

additional time greater or equal to τ before transmitting in the channel, preventing its frame from colliding with an ongoing transmission. The average idle period is then given by:

$$\bar{I} = (f/G) + \tau \tag{3.7}$$

In analyzing the busy period, two types of busy period are considered: successful transmission and contention busy periods. A successful transmission is the successful exchange of control frames (RTS+CTS) followed by the successful transmission of the data and ACK frames. In the analysis, the ACK frame is ignored since by assumption A6 once the control frames are successful the data is transmitted without errors. Hence, channel time f is the sum of transmission times for control frames and the data frame,

$f = f_{data} + 2f_{ctrl}$, where f_{data} is the transmission time for a data frame and f_{ctrl} is the transmission time of a control frame.

The contention period is the period when the channel is vulnerable and any interfering arrival can corrupt the frame in the channel. The control frame in the channel is vulnerable until all stations within hearing range sense the control frame, the time it takes for the stations to sense a control frame is known as the propagation delay, τ. The length of f_{ctrl} is assumed to be as long as τ, but much smaller than f_{data}, $\tau \leq f_{ctrl} \ll f_{data}$ so that as little time as is necessary is spent

exchanging control frames. The expression for the average busy period $\overline{B}$ is then written as:

$$\overline{B} = P_S(f+\tau)+(1-P_S)\overline{C} \tag{3.8}$$

where $\overline{C}$ is the average length of the contention period. In the analysis of the contention period, the length of the vulnerable period is considered to be less than or equal to the total length of the control frames. The vulnerable period is random and has an average length denoted by $\overline{X}$. The average contention period $\overline{C}$ is hence given by,

$$\overline{C} = \overline{X}+\tau \tag{3.9}$$

The random variable X is calculated when any interfering arrival or arrivals collides with the control frame being sent or received by an MS trying to acquire the channel. The distribution function for the random variable X, $F_x(x)$ is defined as $P(X \le x)$, where $0 \le x \le 2\tau$. The maximum vulnerable time length of 2τ is the time it takes for a sending MS after sending a RTS control frame to successfully receive a CTS control frame. The average vulnerable period $\overline{X}$ is derived as:

$$\overline{X} = \tau\left\{\frac{1}{g}\left[\frac{1-e^{-g}}{1-e^{-2g}}\right]-\frac{e^{-g}}{1-e^{-2g}}\right\} \tag{3.10}$$

In Equation 3.10, $g = G\tau / f$.

Hence,

$$\overline{C} = \tau\left\{\frac{1}{g}\left[\frac{1-e^{-g}}{1-e^{-2g}}\right] - \frac{e^{-g}}{1-e^{-2g}} + 1\right\} \tag{3.11}$$

Substituting Equations (3.5) and (3.11) into (3.8) the average busy period gives Equation (3.12) below:

$$\overline{B} = \left(e^{-2g} + \left(1-e^{-2g}\right)e^{-2g}\right)\left(f+\tau\right) + \left(1-\left(e^{-2g} + \left(1-e^{-2g}\right)e^{-2g}\right)\right)\tau\left\{\frac{1}{g}\left[\frac{1-e^{-g}}{1-e^{-2g}}\right] - \frac{e^{-g}}{1-e^{-2g}} + 1\right\} \tag{3.12}$$

Finally, substituting Equations (3.6), (3.7) and (3.12) into (3.1) and after simplifying gives Equation (3.13) where *a* represents the normalized propagation delay τ/f and *b* is the normalized frame transmission time f_{data}/f.

$$S = \frac{GbP_S g\left(1-e^{-2g}\right)}{g\left(1-e^{-2g}\right)\left(1+\left(g+Ps\left(G+g\right)\right)\right) + g\left(1-P_S\right)\left(1-e^{-g}-ge^{-g}+g\left(1-e^{-2g}\right)\right)} \tag{3.13}$$

From Equation 3.13, the key parameter that affect the throughput of the CSMA/CA algorithm with the proposed enhancement to mitigate the exposed node problem is the normalized propagation delay, a.

3.4.3 Delay analysis

Obtaining the average frame delay [26] for the CSMA/CA model with exposed node is basically straightforward, it is the time spent sending a successful frame and the time the frame has to be retransmitted due to retransmissions. The time to send a successful frame is the average transmission delay, T_S. A frame that does not collide with any other control frame spends at minimum the transmission delay. Hence,

$$T_S = f + \tau \tag{3.14}$$

or

$$\hat{T}_S = 1 + a \tag{3.15}$$

where $\hat{T}_S$ is the normalized successful transmission delay.

A data frame is unsuccessful at time of arrival if either one of the conditions listed below occurs:

I. The channel is sensed busy at the time the frame arrives at the MAC layer from the upper layers, the frame transmission is deferred for a random

amount of time by the MS. This deferred period is also known as the backoff period.

II. The data frame collides with another data frame causing corruption of the frame. The frame will have to be retransmitted and the MS defers the channel for a random backoff period.

The backoff period Z is a random number uniformly distributed over [0, k] where k is any integer greater than zero.

The average backoff period is given by [27],

$$\overline{Z} = \left(\frac{k+1}{2}\right) f \qquad (3.16)$$

whose normalized value is $\hat{Z} = \frac{\overline{Z}}{f}$

The average delay is the average successful transmission time and the average delay spent on retransmissions. Hence,

$$\overline{D} = 1 + a + R(\hat{Z} + 2c + 2a) \qquad (3.17)$$

where R is the average number of unsuccessful transmission attempts, c is the normalized transmission time of a control frame, f_{ctrl}/f and $(2c+2a)$ is the

maximum time taken for a transmission to be deemed unsuccessful, barring the channel being successfully acquired. Finally, the expression for R is given by [26]:

$$R = \left(\frac{G}{S} - 1 \right) \tag{3.18}$$

where $\frac{G}{S}$ is the average number of transmission attempts to successfully transmit a frame. From Equation 3.17, the key parameters that affect the delay of the CSMA/CA algorithm are

1) Normalized propagation delay, *a*.

2) Maximum backoff period, k.

3.5 RESULTS AND DISCUSSION

The assumed parameter values used in obtaining the results presented in this thesis are comparable with values used in other literature analyzing the performance of CSMA based protocols [26, 27].

Fig. 3.2 shows the throughput obtained when the MAC algorithm is modified to offer stations in the exposed node situation access to the channel. The result shows an improvement in the efficiency of the channel when intelligence is introduced to the RTS control frame. This result indicates that stations using CSMA/CA with virtual CS to gain access to channel underutilize the available channel spectrum by about 15%. The proposed algorithm changes the way

stations react upon observing the channel busy and also having a frame to transmit. The changes help mitigate the occurrence of the exposed node problem and thus improve the channel capacity [28].

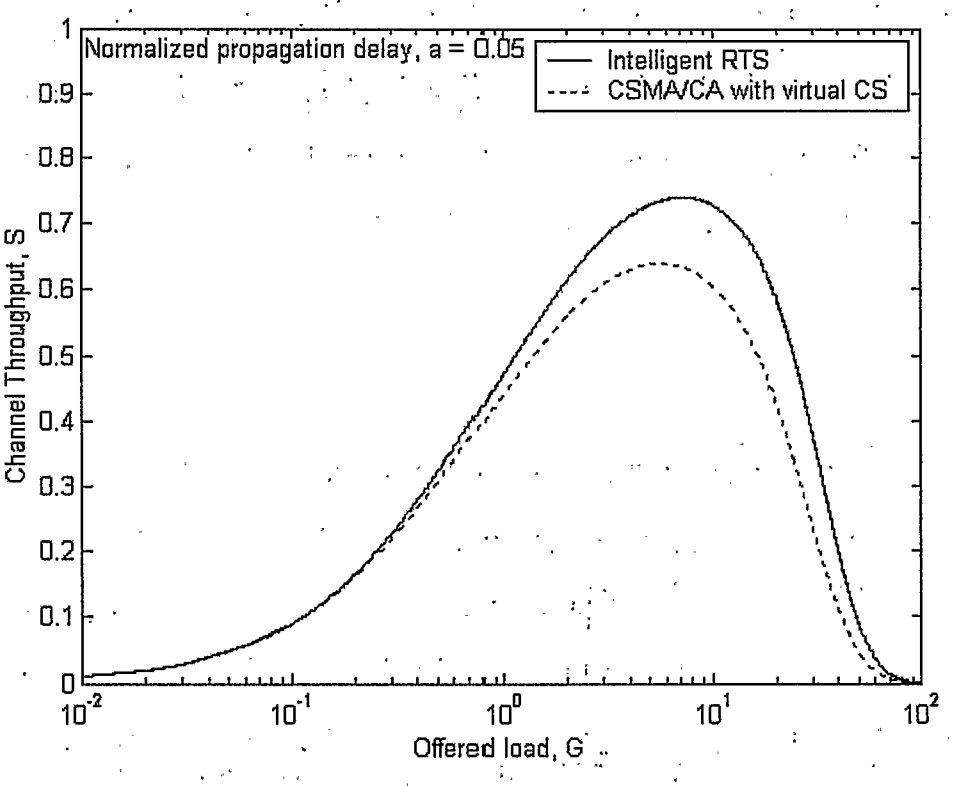

Figure 3. 2 Channel throughput performance

Fig. 3.3 illustrates the effect of the normalized propagation delay, a, on the maximum channel throughput. It is observed that small values of a corresponds to a higher throughput and there is little difference between the standard and modified MAC algorithms. As a increases the performance of the modified MAC algorithm starts to outperform that of the standard MAC algorithm. The results indicate that the performance of the channel is dependent on the distance between stations in

the network. When stations are close together, detection of frame transmission is almost instantaneous. When the distance between stations gets larger, it takes the channel a longer time to transmit a frame and this in turn reduces the channel throughput. The modified algorithm allows more than one sending station, within hearing range of each other to use the channel simultaneously. This in turn eliminates the exposed node problem and improves the efficiency of the channel [28].

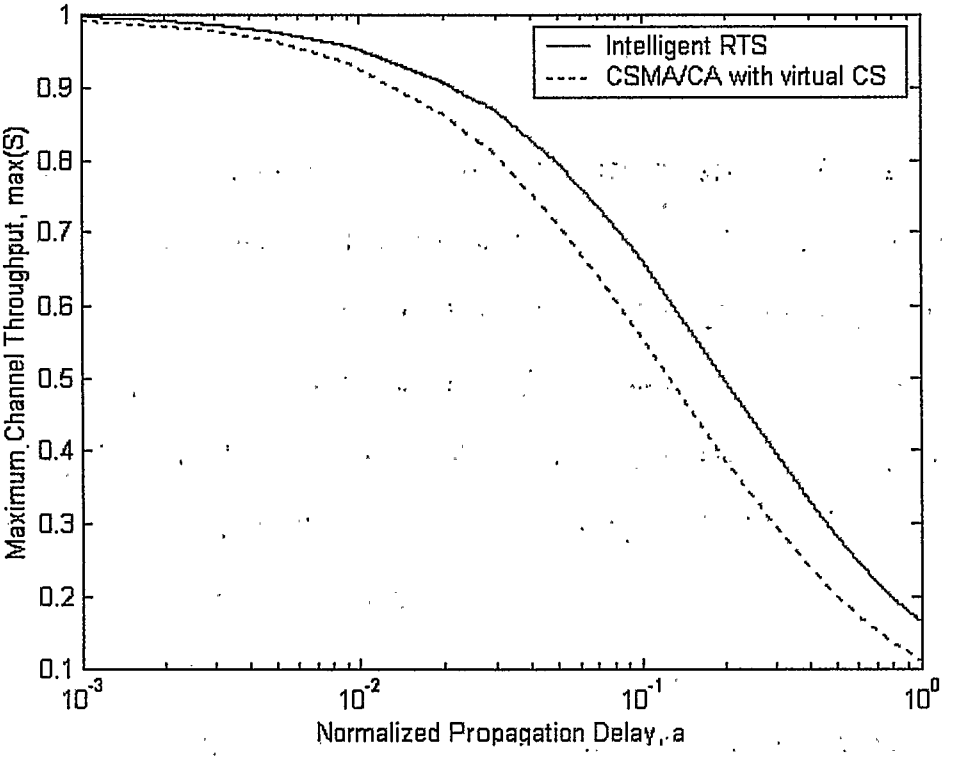

Figure 3.3 Impact of normalized propagation delay on maximum channel throughput

Fig. 3.4 displays the results for the average frame delay for the standard and modified MAC algorithms. It is noted from Fig. 3.4 that, as the throughput increases, the average transmission delay experienced by a frame increases, this is caused by frame retransmissions and backoff periods. It is also observed that the proposed enhanced MAC algorithm has a lower average frame delay than the standard algorithm and this is possible because of a decrease in frame retransmissions thus reducing the contention for channel access [28].

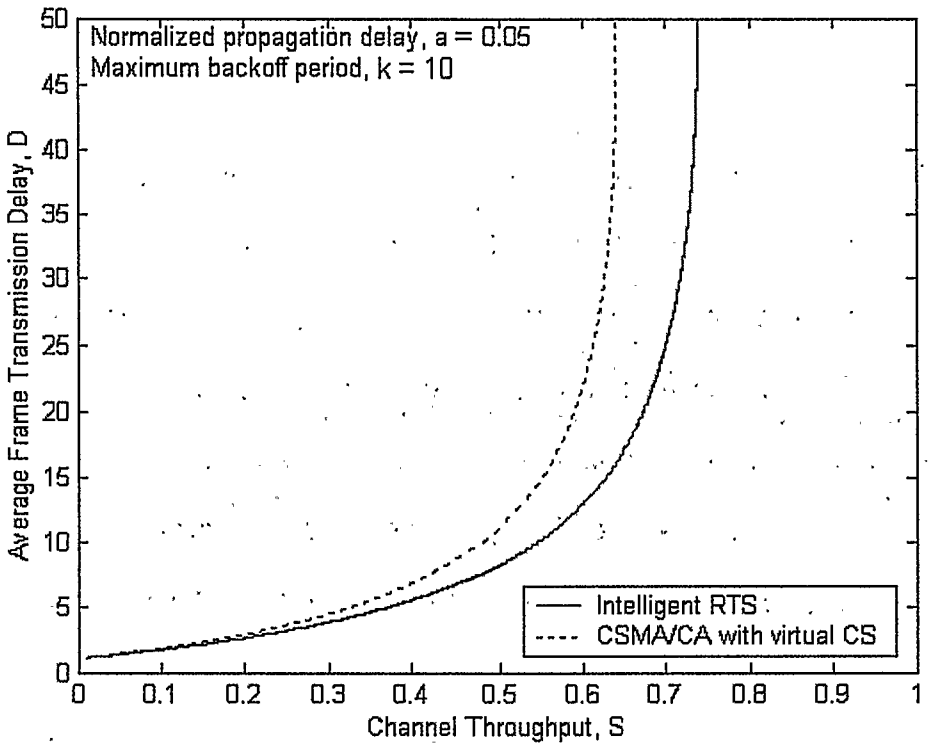

Figure 3. 4 Average frame transmission delay performance

In Fig. 3.5 increasing the maximum backoff period, k, changes the average backoff period $\bar{Z}$. The average delay, $\bar{D}$, increases with increasing k. The higher

the value of k the less the probability of collision but this translates to a longer backoff time. If a station sensing the channel busy picks a long backoff period, the station does not check the channel until the end of the backoff period. If the channel becomes free before the end of the backoff period the station would not contest for the channel and this means the channel resources are wasted and adds unnecessary delays to the network.

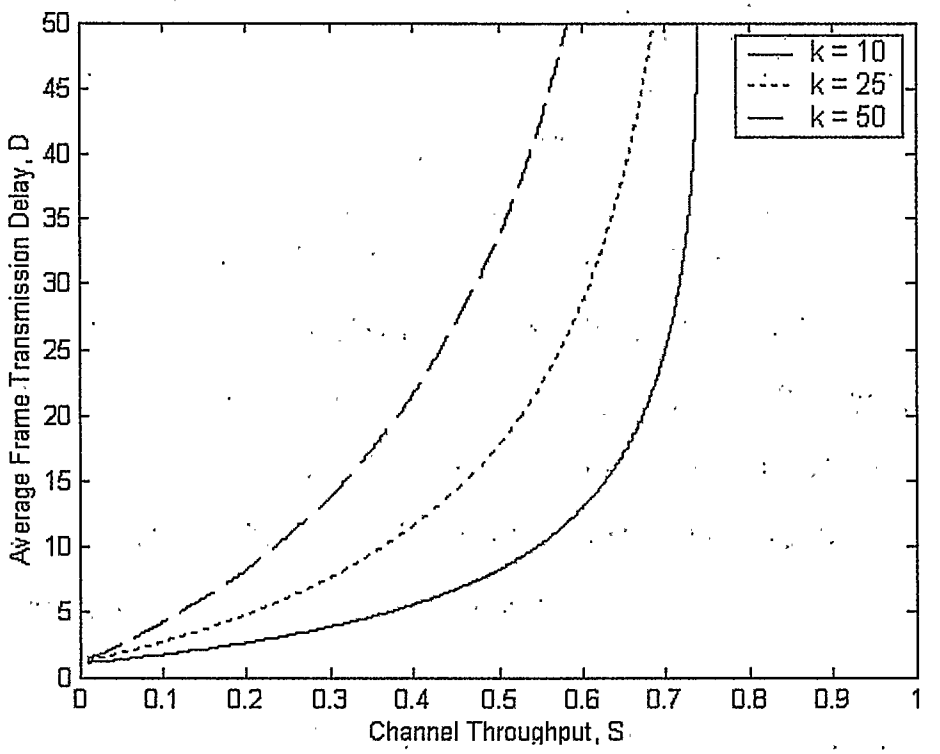

Figure 3. 5 Effect of maximum backoff period on the average frame transmission delay

Fig. 3.6 studies the effect of changing the normalized propagation delay on the average frame transmission delay. As observed from the throughput

performance results, the lower the propagation delay the better delay performance achieved by frames transmitted on the channel. This makes sense because if the propagation delay is small, all stations are immediately aware of the channel condition hence reducing the amount of time needed for the exchange of control frames and more of the channel time is spent on transmission of data frames.

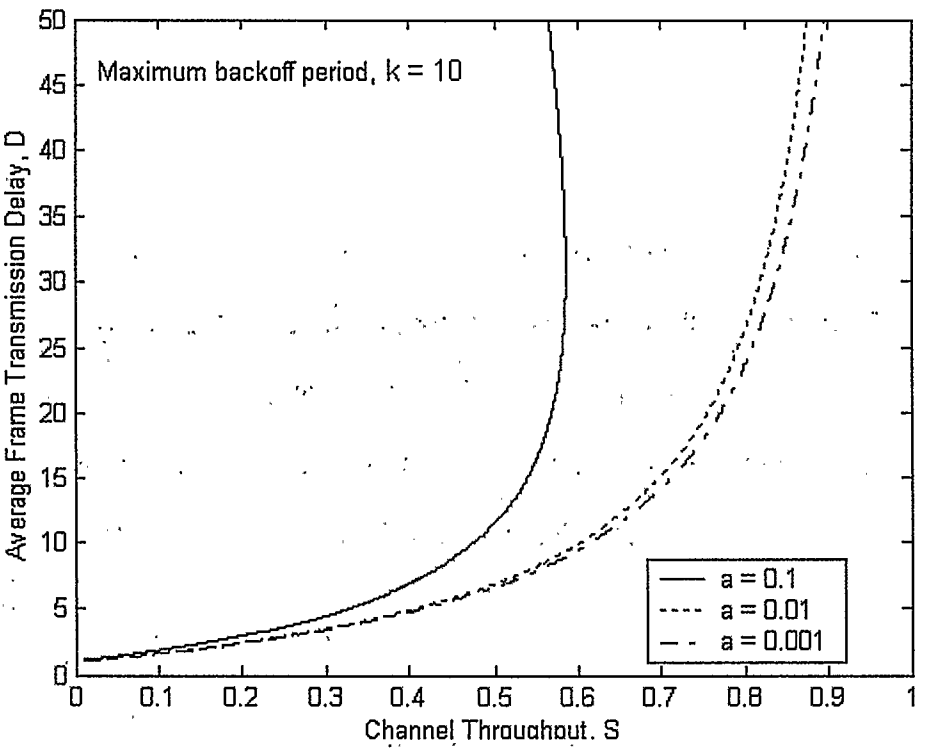

Figure 3. 6 Effect of propagation delay on the average frame transmission delay

As the popularity of WLAN increases and the channel becomes oversubscribed implementing the proposed algorithm, improves the efficiency of the channel. This is important because the radio spectrum assigned for WLAN is

fixed and all transmissions must be curtailed within this radio spectrum. Thus, by allowing more transmissions in the channel the point at which the channel begins to saturate can be increased. This in turn improves the performance of the wireless channel and also reduces the number of transmissions contending for the channel.

3.6 Summary

This chapter proposed an algorithm for improving the channel performance in 802.11 networks. The Intelligent RTS algorithm added an extra function to the control frames currently being used in the IEEE802.11 MAC to solve the exposed node problem. MS's will be able to use information obtained from the control frames to create a virtual picture of the channel state. An exposed MS can then implement the proposed algorithm to gain access of the channel. With the implementation of this algorithm more multiple MS's can simultaneously use the channel. A performance evaluation of the proposed algorithm is also presented. The obtained results are then compared with the CSMA/CA with virtual CS protocol, the same protocol used in IEEE802.11 MAC. The performance of the proposed algorithm shows an improvement in the key channel performance metrics of throughput and delay. Although the proposed algorithm results in an increase in its processing cost, this should not be a major issue with faster processors available.

CHAPTER FOUR

SIMULATION ENVIRONMENT

4.1 Introduction

In chapter three the mathematical analysis for the proposed enhancement to the MAC algorithm was presented. In this chapter, the mathematical results will be validated by means of discrete-event computer simulation. By developing a computer-based simulation, the proposed algorithm can be tested under a more realistic operating environment. The virtual network environment will be created using the optimized network performance modeler (OPNET) [29].

4.2 OPNET Modeler

There are different simulators used in simulating the WLAN environment but the two commonly used are the Network Simulator 2 (ns-2) [30] and OPNET. Ns-2 is free simulator and different modelers develop most of its model but the ns-2 simulator does not provide any end user support. Unlike ns-2, the OPNET simulator is not free and requires the end user to pay for a license before being able to gain access to the simulator. The acquired license also gives the end user access to OPNET support center.

The MAC simulator will be implemented under the OPNET modeler environment, due to the amount of support available. The OPNET modeler uses a

three stage step to simulate any network: Network Domain, Node Domain and Process Domain, as illustrated in Fig. 4.1.

4.2.1 Network Domain

The Network domain defines the top-level characteristic of the network to be investigated, type of devices, number of devices, topology, network size, et cetera. The interfacings required between the different network components are defined in the Network domain. This stage can also be considered as the testing stage of the simulator, where different devices are connected to simulate different types of network. The network performance parameters to be investigated can include delay, throughput, and so on, and these are set and the results collected in the Network domain. The OPNET simulator allows for multiple scenarios to be created and simulated consecutively with little import from the user, after the initial configuration have been stated for the first scenario, and this is accomplished by using the Simulation Sequence tool.

4.2.2 Node Domain

The Node domain is used to define the specific elements or modules that make up a device defined in the Network domain and the hierarchy in which these modules are connected. Queues can also be implemented in this domain. The node domain has different types of connections.

The Node Domain can be regarded as the implementation stage where different modules when connected make up a device that is then tested in the Network Domain.

4.2.3 Process Domain

The Process domain defines the finite state machine describing each module of the node domain. The logic of each state and transitions is implemented in C/C++ code. In the Process domain all the processes for the modules defined in the node domain are executed. The Process Domain is the point where all the functions for the different modules are designed. The process domain uses state machines to model the stages required by the module.

4.3 Network Configuration

The MAC simulator will be implemented on a network structure that supports a single channel with multiple users as obtained in a practical IEEE802.11 WLAN. The essence is to capture a network topology that emulates an MS behavior in a WLAN. The Mobile Ad Hoc Network (MANET) environment requires the MAC simulator to operate in the Distributed Coordinated Function (DCF) mode. The MAC simulator modifies the IEEE802.11 MAC to reduce the probability of exposed nodes occurring, recall that exposed nodes occur when stations are within hearing range but out of interference range.

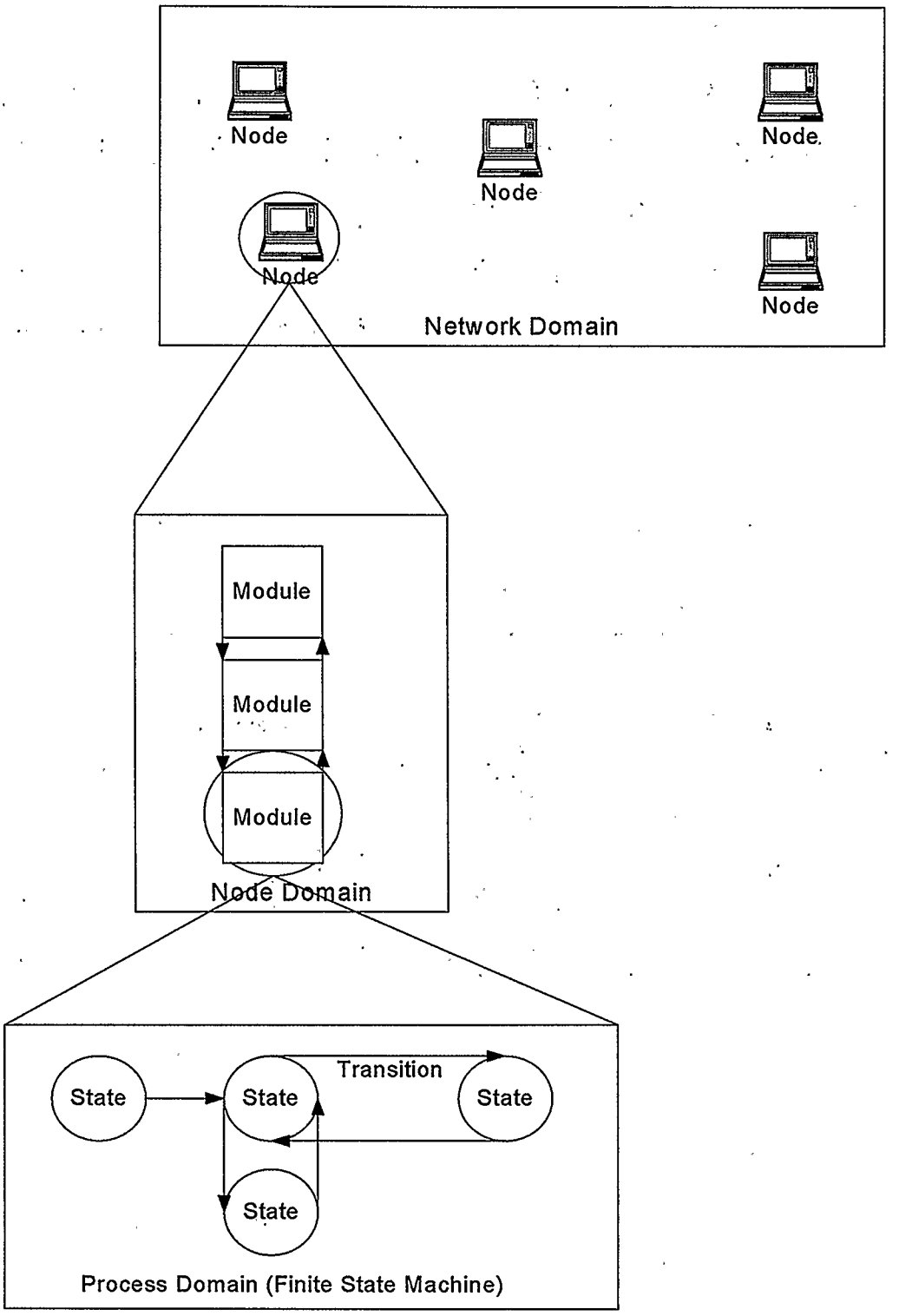

Figure 4. 1 OPNET modeling configuration

4.3.1 Node Model for MAC Simulator

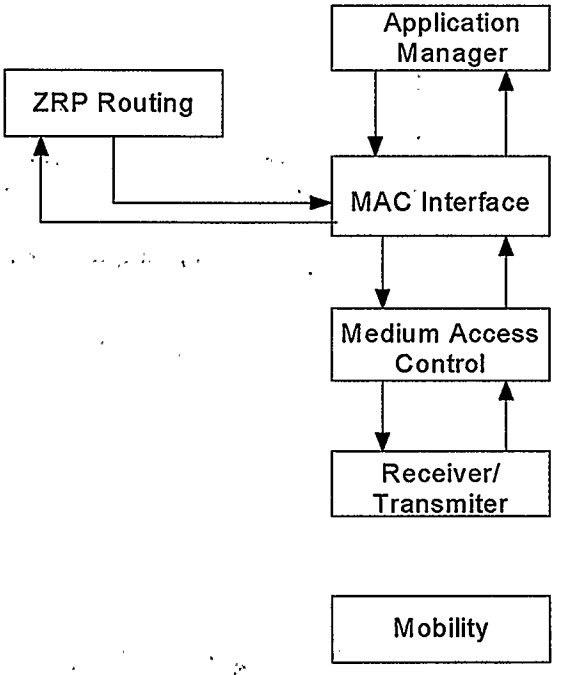

Figure 4. 2 Node Model structure in OPNET

Figure 4.2 illustrates the node model structure for each MS in the IEEE802.11 WLAN implemented for MAC simulator. The relevant layers of the OSI stack and their functionalities are captured in the model.

The Application manager is in charge of generating the traffic load that will be used in the simulation. MS's in the network are designed to support only data traffic and the data traffic is composed of file transfer using file transfer protocol (ftp). The application manager randomly chooses an MS and then generates traffic that will be sent to that MS. The application manager is the end point of all data traffic in the network excluding dropped data traffic. The session inter-arrival time for the data traffic is exponential because a data session is assumed to arrive

following a Poisson process, Table 4.1. The mean number of packets per session is 300 per node second and a reading time of 1 second between sessions. Two frame arrival rates of 10 frames/sec and 1000 frames/sec are used to generate light and heavy network loads, respectively. In addition, the number of MS's in the network generating traffic in the network is varied to increase the offered traffic, at a fixed mean session arrival rate. A fixed packet size of 2048 bytes was chosen to increase the load on the channel; packet sizes greater than 2048 bytes did not produce significant impact on the channel throughput.

Table 4. 1 Data Traffic Parameters

Parameter	File Transfer (ftp)
Session arrival process	Poisson
Number of packets per session	300
Mean inter-arrival time between frames	100ms, 1ms
Time between sessions	1s
Packet size	Fixed – 2048 bytes

The MAC interface handles incoming data packets from the upper and the lower layers. When data is received from the application manager the MAC interface queries the ZRP routing process to obtain a valid route to the destination MS. Similarly, if a data packet is received from the lower layer that has a different MS as its final destination, the MAC interface also queries the ZRP routing process for a valid route. If the data packet is received from the lower layer and is destined to this MS, the MAC interface forwards the packet to the application manager.

The functions of the ZRP routing process, with parameters shown in Table 4.2, include maintaining a routing table of MS's that are a hop away, finding valid

routes to MS's that are not within 1 hop to the MS, removing stale routes from the routing table, broadcasting a beacon at specific intervals to alert other MS's of its presence in the network.

Table 4. 2 ZRP Routing Information

Routing Parameters	Value
Periodic broadcast beacon update	1s
Number of periodic updates missed before route link broken	3
Table hop limit	1 hop

The Transmitter process is a physical layer process and it gives MS's the capabilities of transmitting data frames in the channel. The transmitter process defines the physical layer characteristics such as the transmitter power, the channel transmitting rate and the transmitting frequency. Table 4.3 shows the parameters for data transmission.

Table 4. 3 Transmitter Parameters

Transmitter Parameters	Value
Transmitting Frequency	2.4 GHz
Maximum data rate	11 Mbps
Transmitter Power	100 mW

Every frame transmitted by an MS is transmitted at the operating frequency of 2.4 GHz and with a power of 100mW. These parameters correspond to the specification of the IEEE802.11b standard.

The operating frequency and the transmission rate of the receiver and the transmitter have to match to setup a virtual connection between the MS's in the

network. The Receiver process is also a physical layer process and its main functionality is to receive data frames from the channel. The characteristics defined at the receiver include the receiver power, the signal-to-noise (SNR) ratio, bit error rate (BER) and any other factor that affects the reception of the data frame. Table 4.4 lists the models used at the receiver.

Table 4. 4 Receiver parameters

Receiver Parameters	Value
Receiver Frequency	2.4 GHz
Maximum data rate	11 Mbps
Receiver Power	dra_power
SNR	dra_snr
BER	dra_ber
Interference noise	dra_inoise

The received power is calculated using the dra_power model, which utilizes free space propagation because the environment being looked at is an office layout and the major cause of degradation will be path loss. The dra_snr model calculates the strength of the frame signal over the background noise seen in the channel. The interference caused by other frame transmissions is obtained from the dra_inoise model. The dra_ber model calculates the probability of a bit being received in error.

4.3.2 MAC Simulator Process Model

The MAC simulator process model, Fig. 4.3 models all the functionalities of the IEEE802.11 MAC and also models the proposed modification to the MAC that are implemented when the exposed node problem arises.

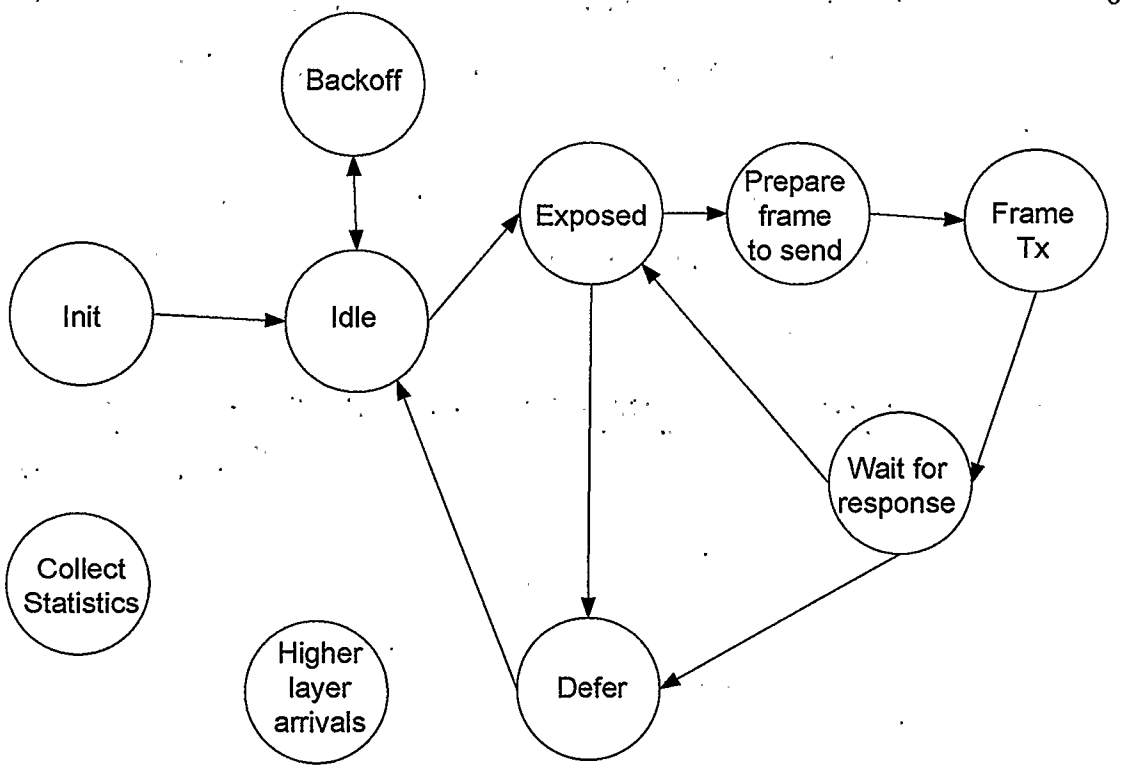

Figure 4. 3 Process model structure in OPNET

A description of the states and transitions is given as follows:

A. Initialization (Init)

All simulation parameters, variables, constants, characteristics, et cetera, are initialized in this state.

B. Idle

The idle state is entered when an MS is idle and is not receiving or transmitting any frame. The idle state is returned to if the buffer is empty.

C. Higher layer arrivals

When a packet is sent from the higher layer to the MAC interface, the higher layer state is called. Packets received from the higher layer are then placed in the MS's buffer. The buffer system implemented is the First In First Out (FIFO) queue system. The buffer is of finite size and has a finite size limit of 1.4 Megabytes. Packets are dropped if the buffer size is exceeded. Based on a packet size of 2048 bytes (from Table 4.1), the buffer can accommodate a total of 716 packets.

D. Prepare frame to send

This state is executed just before a frame can be transmitted. The main purpose of this state is to format the next transmission into a legal frame format. Legal frames sent to the transmitter process include RTS, CTS control frames, DATA frame (Fig. 4.4) and ACK frame.

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

Figure 4. 4 DATA Frame Structure

E. Frame TX

The frame transmission (TX) is used to deliver formatted frames to the transmitter process for immediate transmission. An MS switches to this state under

the condition that the channel is idle or the MS is "exposed" to an ongoing transmission.

F. Wait for response

After a frame is transmitted the MS waits in this state until either the right response frame is received or a frame timeout is reached, whichever comes first.

G. Backoff

The backoff state is implemented when an MS has to contend for the channel. The backoff period is uniformly distributed between [0, CW - 1], where $CW \in \{CW_{min},...,CW_{max}\}$ where CW depends on the number of times the MS has tried to transmit the data frame. For IEEE802.11b, CW_{min} and CW_{max} are 31 and 1023, respectively. The MS sets a timer that decreases the backoff interval after each idle slot with the timer expiring at the end of the backoff period. The timer is suspended if a frame is received during backoff period. The backoff state is exited at the expiration of the backoff timer or if the backoff timer is suspended.

H. Defer

The defer state is executed when the MS has to defer transmission for a period of time. The length of the defer period is dependent on the NAV time. If a frame arrives from the receiver process while in the defer state, the frame is ignored.

I. Exposed

When a frame is received from the receiver process and the defer state has not been invoked, the exposed state is executed. The exposed state implements the Intelligent RTS algorithm and resolves the conditions under which an MS can transmit when a control frame is received from the receiver process. The conditions are listed below:

- The received frame is an RTS frame and the MS is the destination MS and a CTS reply is needed.
- The received frame is an RTS frame and both the source and destination addresses contained in the RTS frame do not match the destination address of the next outbound transmission from the MS.

J. Collect Statistics

This state collects the statistics that will be required in analyzing the overall performance of the IEEE802.11 WLAN.

Transition of one state to another is triggered by different events without any simulation time passing. The events that trigger the state transition are as follows:

- The collect statistics and higher layer arrivals are global states and can be triggered within any state.
- The simulation starts from the initialization state and then proceeds to the idle state.

- The Idle state transition to the exposed state is triggered when there is a data frame to transmit and under either of this conditions:
  - The channel has been idle for a period equal to or greater than the DIFS period.
  - The RTS control frame is received from the channel.
- The Exposed state changes its state to the Prepare frame to send state to format the frame that has to be sent.
- The Prepare frame to send state moves to the Frame Tx state after the frame to be sent has been formatted.
- The Frame Tx state to the wait for response state occurs after the frame has been transmitted.
- If a frame is received within the specified time period, this triggers the transition of states between the wait for response and the Exposed states.
- The Wait for response and defer states are triggered by a frame timeout.
- A match of the RA and TA fields with destination MS or if the frame received is not the expected frame switches the Exposed state to the Defer state.
- The Defer state to the Idle state occurs after the NAV time has expired.
- The Idle state to the backoff state is triggered when there is data to transmit and the MS has to contend for the channel.
- The transition back to the Idle state from the backoff state is done after the expiration of the backoff timer or if the backoff timer is suspended.

4.3.3 MAC Simulated Network Environment

Figure 4.5 shows an example network structure of the simulated WLAN, configured with parameters listed in Table 4.5.

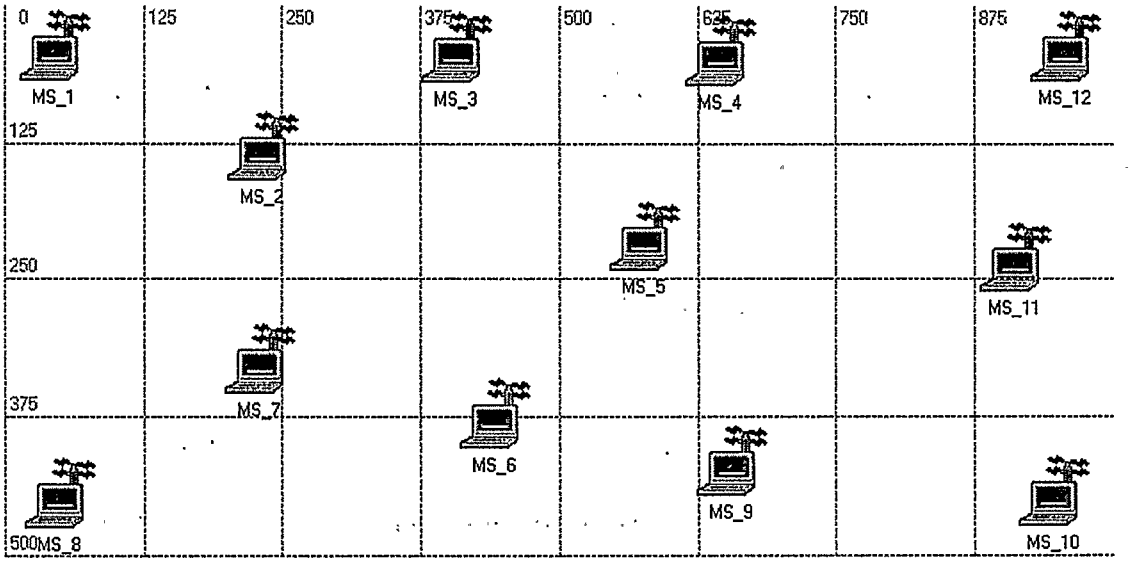

Figure 4. 5 Simulated WLAN Structure showing the initial node placement (Distance Unit is in meters)

Table 4. 5 OPNET Network Simulation Parameters

Network Parameters	Index
MS	12 (maximum)
MS transmitting	Variable [3,6,9 and12]
Data frame size	Fixed – 2048 bytes
Topology	Office
Size	1000mx500m
Wireless range	250m
Routing Protocol	ZRP
MAC	1. 802.11 DCF 2. MAC simulator (Thesis proposal)
Mobility	Random waypoint mobility
Inter-arrival rate	Variable - 100 ms, 1ms
Max speed	Variable [0, 1, 3, 5 m/s]

4.4 MAC and Channel Simulation Parameters

4.4.1 Radio Channel Environment

The distance between the transmitter and the receiver, as well as the office layout affects transmissions over the wireless channel. As the distance increases, the more likely the transmissions become vulnerable to phenomena's like path loss, multi-path, etc. The WLAN configuration being simulated only considers transmission distortion due to path loss. Table 4.6 specifies the propagation model chosen and its path loss coefficient.

Table 4. 6 Simulated Channel Parameters

Radio Channel Parameter	Value	Comment
Free space propagation	2	Assuming an office environment

4.4.2 Simulation Parameters, Definitions and Representative Values

Table 4.7 lists the major parameters of the MAC simulator specifying their representative values, and comments where necessary. The values for the parameters for the IEEE802.11b are taken from [14, 15].

Table 4. 7 Simulated IEEE802.11b Parameters

Physical Layer Parameter	Value	Comment
Slot time	20μs	
SIFS time	10μs	
DIFS time	50μs	
Min. Contention Window	31	
Max. Contention Window	1023	
Backoff	Random [0,CW - 1] * Slot time	$CW_{min} \leq CW \leq CW_{max}$ Min.
Data Frame rate	11Mb/s	
RTS	20 octets	
CTS	14 octets	
DATA	2048 octets	Support for variable data frames without preamble 0-2312 octets
ACK	14 octets	

4.5 IEEE802.11 MAC-level Performance Metrics

The required performance metrics from the simulation are as follows:

- System throughput
- Frame delay

The formulas for calculating these metrics are as follows:

$$system\ throughput = \frac{Total\ correctly\ received\ frames}{Simulation\ time} \quad (4.1)$$

$$Average\ frame\ delay = \frac{Frame\ delivery\ time - Frame\ arrival\ time}{Total\ correctly\ received\ frames} \quad (4.2)$$

4.6 Verification of Simulation Software

Verification of the simulation software is necessary to ascertain that the simulation model is performing as desired. The simulation sequence was verified

by tracing the simulation steps for a small fraction of time to make sure the simulator was performing the right functions at each point in time. The simulation was run with random seeds to ensure the simulation was in the steady state region before the results were collected.

Simulation runs of duration 600, 900, 1800, 3600 minutes were performed, the simulation output obtained between 1800 and 3600 minutes varied between +/- 10%. The simulation was deemed to be in steady state region between these regions and a simulation length of 3600 minutes was chosen. The simulation parameters counters are reset after 1800 minutes and data for analysis is collected in the steady-state period.

4.7 Validation of Simulation Outputs

The simulation outputs were validated by comparing with the results obtained through mathematical analysis in Chapter 3. A confidence interval of 95% for the simulation results was used when comparing with the mathematical analysis. Fig. 4.6 shows the plot of the throughput obtained through mathematical analysis and the simulation throughput with a 95% confidence interval. Fig. 4.7 also shows the same type of plot for the transmission delay. It can be observed from Fig. 4.6 and Fig. 4.7 that the analytical results fall mostly within the 95% confidence limits of the simulation. In Fig. 4.7, it is seen that, at high throughput, the simulation results are different from the analytical results. This is expected because the system is experiencing instability resulting in high delays. In the stable

region, there exists very good agreement between the analytical and simulation results.

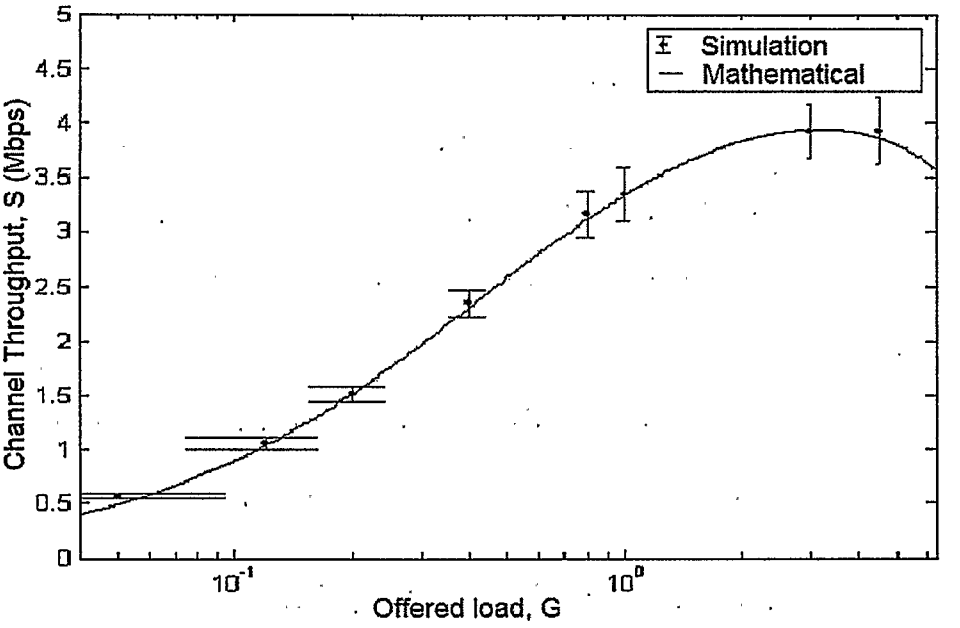

Figure 4. 6 Validation of throughput performance

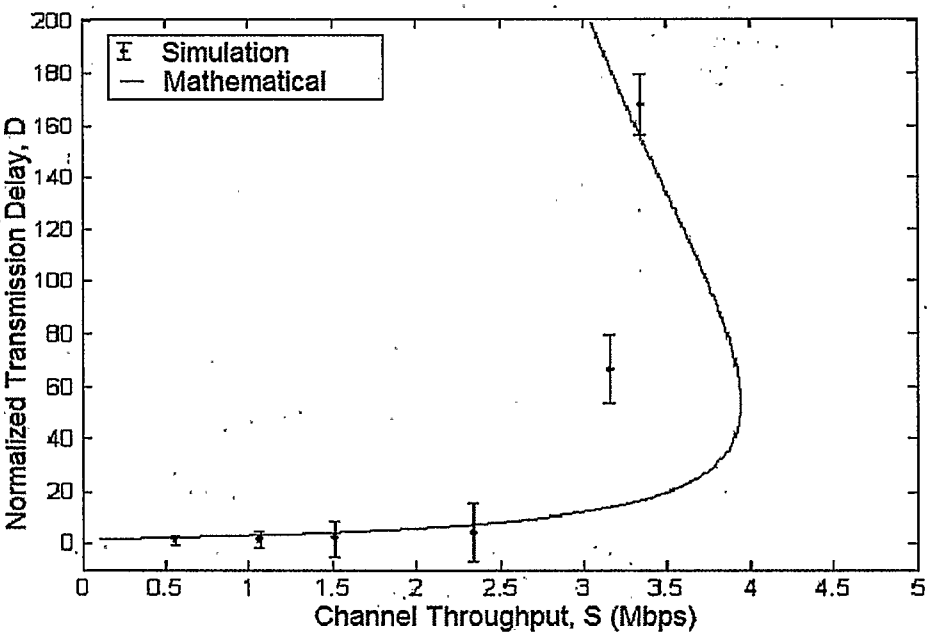

Figure 4. 7 Validation of delay performance

4.8 Simulation Experiments

Two results were designed and conducted to study the performance of the proposed MAC algorithm. The experiments are summarized as follows:

Experiment #1: Impact of the proposed MAC enhancement algorithm on network performance of the IEEE802.11b

Objective: Determine the effect of the Intelligent RTS algorithms on the efficiency of the wireless channel and the influence on the average frame delay.

Experiment #2: Impact of mobility on the Intelligent RTS algorithm.

Objective: Investigate the performance of the network when mobility is introduced.

4.9 SUMMARY

This Chapter describes the environment that will be used to run and obtain results from the simulation scenarios. First the OPNET simulator, which is used to build the virtual WLAN, is described with detailed explanation provided for the different stages implemented. Next, the network configuration to be simulated is outlined along with the simulation parameters used. This Chapter shows how the performance metrics, channel throughput and average frame delay, will be collected. The simulation logic was verified using tracing technique and the

simulation outputs are validated by the results obtained from the mathematical performance analysis. Finally the Chapter concludes by outlining the simulation experiments that were performed to generate performance results for the proposed MAC algorithm. Presentation and discussion of the results form the topic of the next chapter.

CHAPTER FIVE

SIMULATION RESULTS AND DISCUSSION

5.1 Introduction

The objective of this Chapter is to present the simulation results obtained from the experiments performed in Chapter 4. This Chapter graphically presents the key WLAN performance metrics of throughput and delay collected for different network loads and for different mobility levels. Also, the factors that attribute to the variations in the simulation are discussed.

5.2 Results and Discussion

5.2.1 Lightly-loaded Network

The results obtained from simulating a lightly loaded network are shown in Figs. 5.1 to 5.4. The goal is to study the network performance as the probability of the MS's vying for the channel at the same time increases while MS's remain stationary. From Fig. 5.1, it is observed that the channel throughput performance increases as the number of MS's generating traffic increases for the algorithms presented. The channel throughput rate of change is approximately identical for the three algorithms and this similarity is attributed to the frame arrival rate. The frame arrival rate is low with 10 frames arriving every second and hence reducing the

probability of the channel being occupied when a frame arrives. Since each MS is likely to transmit its frame when it arrives, the network channel throughput increases linearly as the load increases.

While Fig. 5.1 does not show any difference in the channel, the opposite is the case for the transmission delay normalized with respect to successful channel time, presented in Fig. 5.2. It is observed from Figure 5.2 that as the number of MS transmitting increases the average delay a frame sees increases. Also, as the number of MS transmitting increases the delay performance of the proposed algorithms is better than that of IEEE802.11. Since the proposed algorithm is modified to solve the exposed node problem the improvement can be attributed to the probability of exposed node being small in the simulated network configuration.

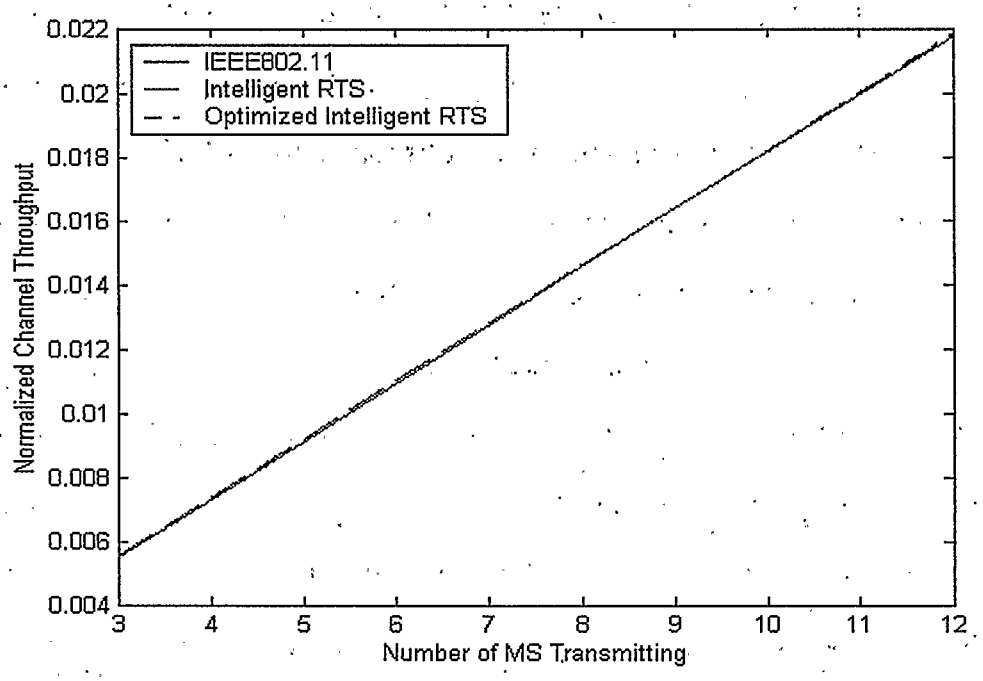

Figure 5. 1 Channel throughput (low load)

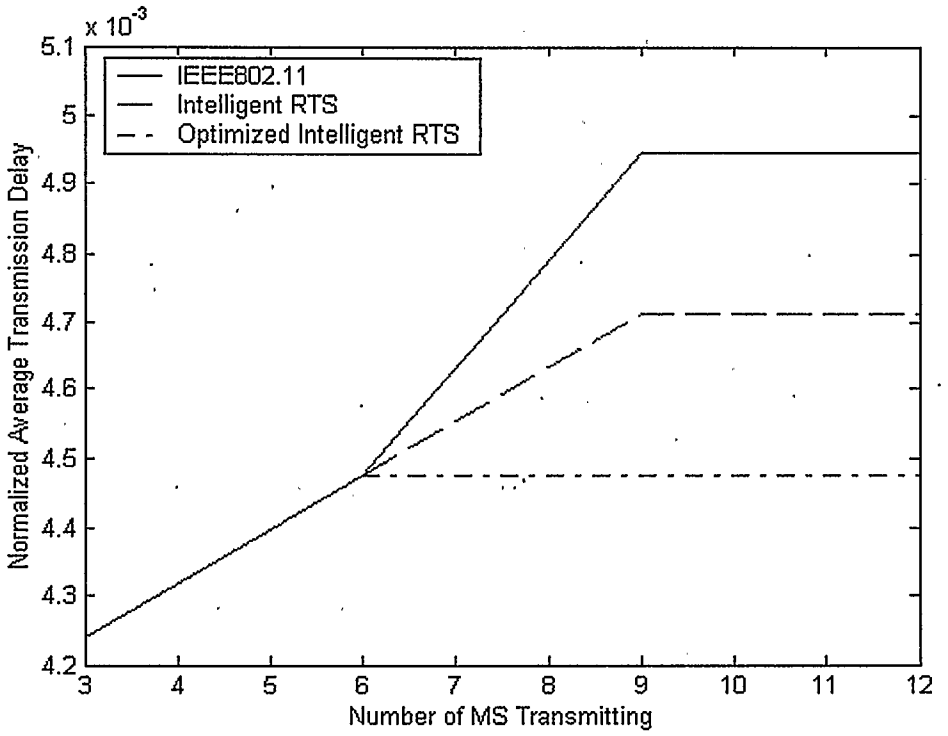

Figure 5. 2 Average frame delay (low network load)

Figs. 5.3 and 5.4 examine the network performance when 12 MS's are transmitting but mobility is introduced into the network. In Fig. 5.3, the channel throughput drops as the speed of the MS increases. By allowing MS's to move randomly in the network makes it difficult for virtual connections to be set up between MS's. This could be due to different factors such as MS's moving out of transmission range, increase in the probability of exposed node, invalid routing information, and increase in the probability of collisions if an MS moves within interference range of an ongoing transmission. From Fig. 5.3, there are 1.4% and 1.5% improvement over the IEEE802.11 channel throughput using the Intelligent RTS and the optimized Intelligent RTS approaches, respectively. Although this

shows a small improvement, it is noted as the network begins to change the modified algorithms are able to take advantage of the exposed algorithms to improve their throughput performance.

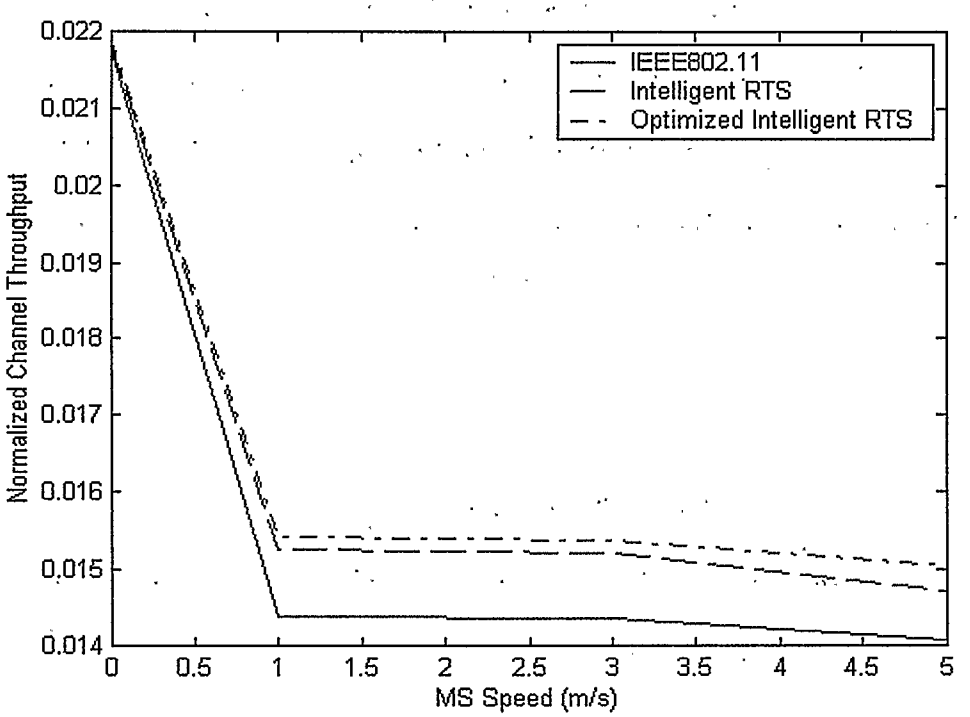

Figure 5. 3 Channel throughput with mobility (low network load)

Fig. 5.4 shows that the average frame delay increases as MS speed increases. In addition, Fig. 5.4 shows a better average delay performance with the Intelligent RTS and the optimized Intelligent RTS compared to the IEEE802.11. The two proposed enhancement algorithms have very similar average frame delay. This affirms the earlier conjecture that the probability of exposed nodes occurring in this network configuration is small.

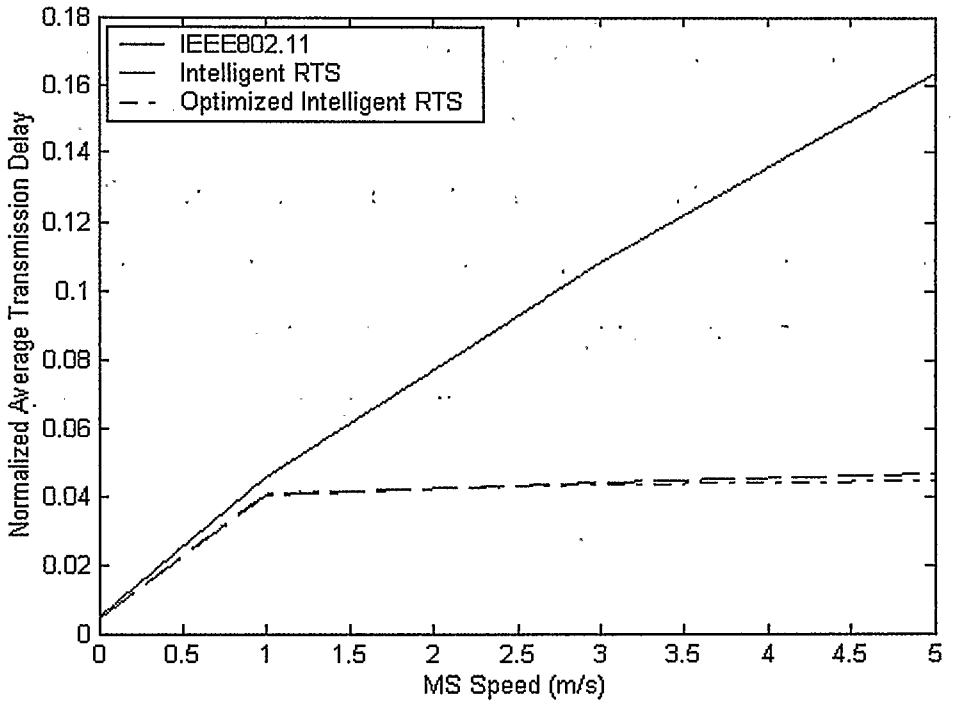

Figure 5. 4 Average frame delay with mobility (low network load)

5.2.2 Heavily-loaded Network

Figs. 5.5 to 5.8 investigate the effects the exposed node problem has on the performance of a heavily loaded network. In Fig. 5.5, the channel throughput increases as the network load increases and the Intelligent RTS and Optimized Intelligent RTS show a throughput improvement of 4% and 6% respectively. The frame arrival rate for a heavily loaded network is 1000 frames/second and thus the probability of exposed node occurring increases.

From Fig. 5.6, it is observed that as the load increases there is a rise in the average frame delay. The Optimized Intelligent RTS and Intelligent RTS algorithm offer a better average frame delay performance as opposed to the IEEE802.11.

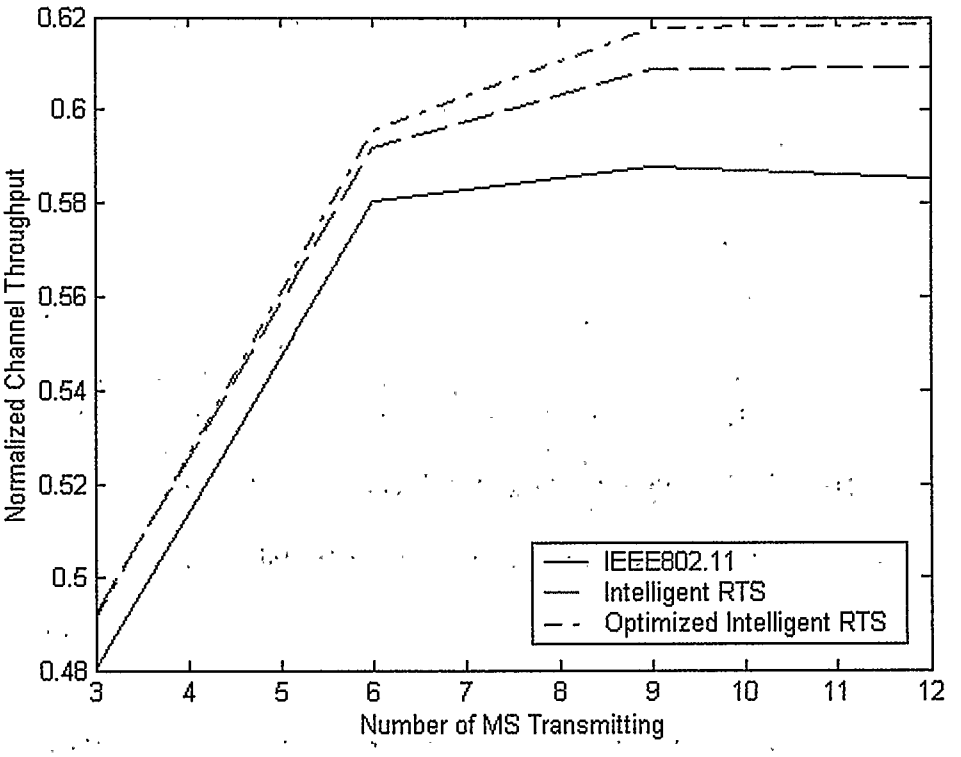

Figure 5. 5 Channel throughput (high network load)

Figs. 5.7 to 5.8 look at the highly loaded network when MS's are allowed to move about in the network at different speeds. It is observed that the network performance of the network deteriorates. The channel throughput (shown in Fig. 5.7) drops and the average delay (Fig. 5.8) increases as the MS speed increases.

In Fig. 5.7 an improvement of 59% in the channel throughput is observed for both the Optimized RTS and the Intelligent RTS as MS speed increases. The Optimized Intelligent RTS and Intelligent RTS also show performance improvement in the average frame delay, as seen from Fig. 5.8. This shows that as the MS speed increases the probability of exposed node occurring also increases.

From the results shown in this Chapter, it is concluded that the exposed node problem has a negative impact on the performance of the IEEE802.11 WLAN network, the network performance worsening with increased network load and introduction of mobility. By implementing the Optimized Intelligent RTS and the Intelligent RTS exposed node problem is solved, demonstrated through an improvement in the efficiency of the WLANs.

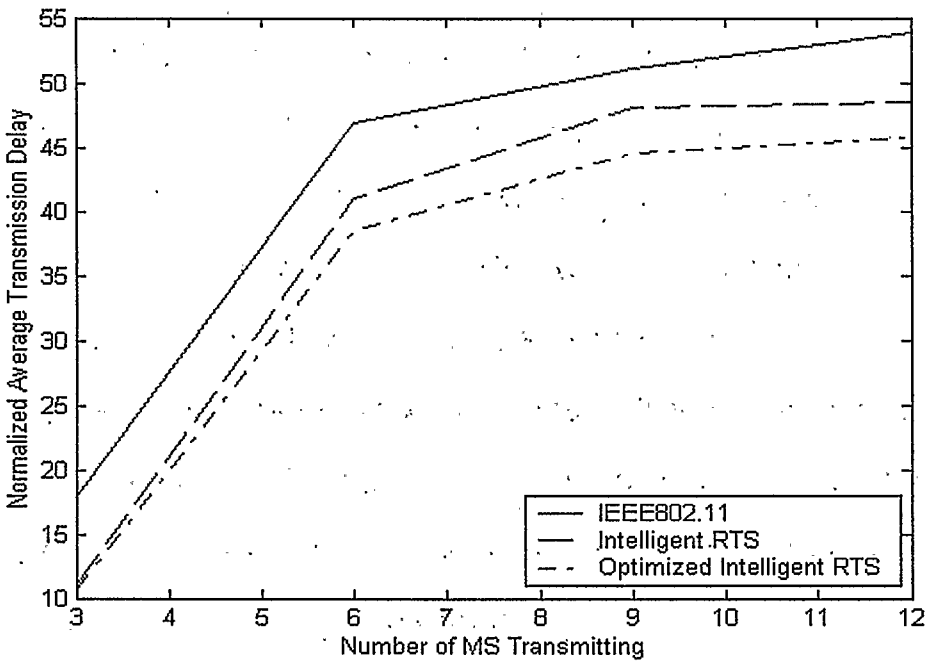

Figure 5. 6 Average frame delay (high network load)

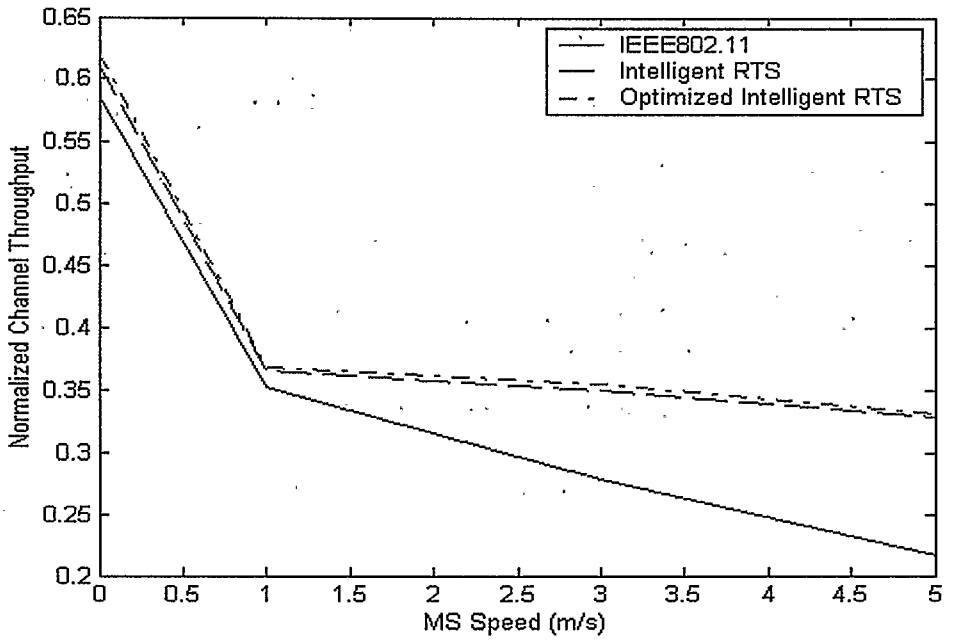

Figure 5. 7 Channel throughput with mobility (high network load)

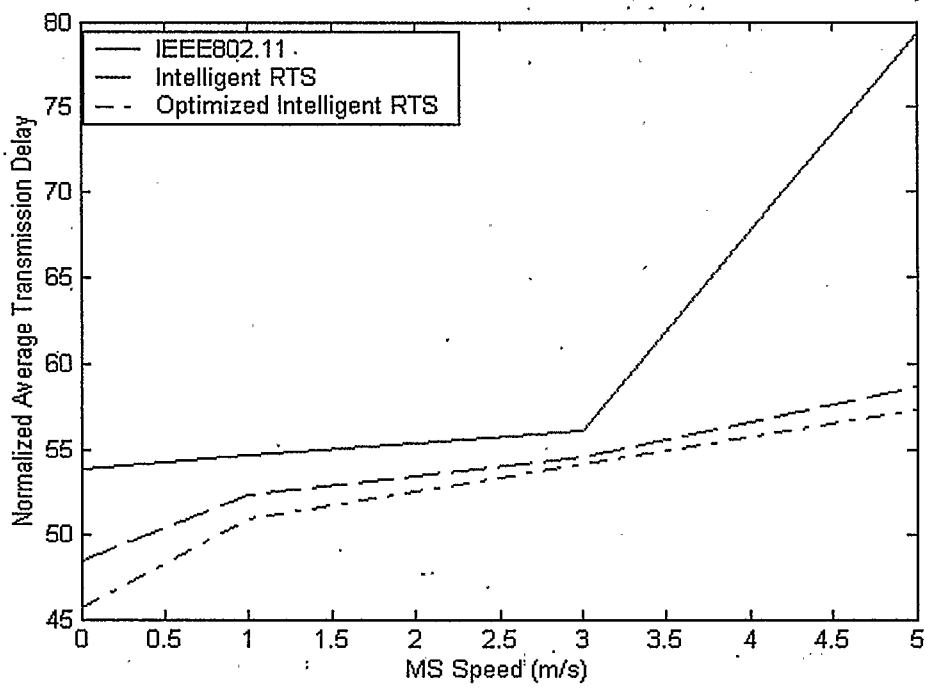

Figure 5. 8 Average frame delay with mobility (high network load)

5.3 Summary

This Chapter presents and discusses the results obtained from the simulation environment. The results presented looked at how the channel throughput and the average frame delay were affected by exposed node problem when different network loads were used. Also investigated was how the exposed node problem affected the network performance when the mobility feature was included. The proposed MAC algorithm exhibit an increase of up to 1.5% and 6% in the channel throughput for a lightly-loaded network and a highly-loaded network, respectively compared to the IEEE802.11. Increase in the channel throughput was also accompanied with better average frame delay. These results signify that by implementing the proposed MAC algorithm the network performance efficiency of WLANs is improved.

CHAPTER SIX

CONCLUSIONS

6.1 Thesis Summary and Conclusions

In this thesis, the access problems affecting the performance of the IEEE802.11 WLANs are addressed. There are two known issues: the hidden node and exposed node problems that have an effect on how MS's gain access to the channel. The IEEE802.11 standards committee has proposed a solution to the hidden node problem, however the exposed node problem remains to be solved. The purpose of this thesis is to investigate the impact the exposed node problem has on the IEEE802.11 by proposing a technique, the Intelligent RTS to solve the exposed node problem.

The Intelligent RTS uses information stored in the RTS control frame to determine if its intended destination is the same as that in the TA and RA fields. The MS then decides if a new transmission can be established alongside an ongoing transmission. A mathematical performance analysis on the Intelligent RTS is performed. One of the performance metrics investigated was the throughput, which showed a theoretical improvement of 15% to the maximum throughput achieved by CSMA/CA with virtual CS, the protocol used by IEEE802.11. The other performance metric investigated was the average frame delay, which also showed a reduction in average frame delay when compared with IEEE802.11. The

Intelligent RTS is optimized by also using routing information to assist in predicting the destination identity.

A virtual WLAN was built using the OPNET simulator to investigate the network performance of the Intelligent RTS and optimized Intelligent RTS under real-life conditions. The network performance was tested with varying network loads and also with different levels of mobility. The simulated results obtained showed that as the network load increased the maximum channel throughput improved by up to 4% and 6% for the Intelligent RTS and optimized Intelligent RTS, respectively. With the improved channel throughput, a reduction in average frame delay is obtained with optimized Intelligent RTS scheme.

When mobility is introduced into the network, a drop in the channel throughput is observed. This drop in channel throughput performance can be attributed to MS moving out of range and MS having stale routing information. The optimized Intelligent RTS and Intelligent RTS adapt better to the changing network environment providing up to 59% improvement in throughput compared to IEEE802.11 networks. The optimized Intelligent RTS and Intelligent RTS approaches provide a finite average frame delay as the MS speed increases. In contrast, for the IEEE802.11 scheme, the average frame delay increases with MS speed.

Based on the results obtained for the Intelligent RTS and optimized Intelligent RTS schemes, it is concluded that the proposed schemes offer solution to the exposed node problem resulting in improved efficiency of the IEEE802.11 WLAN. IEEE802.11 WLANs utilize the unlicensed ISM band, which has a finite

radio spectrum regardless of the network load and by implementing the proposed algorithms more network traffic can be handled. The limitations of the proposed algorithms include:

- Higher processing cost
- Requires the virtual CS to be always switched on.

6.2 Suggestions for Future Work

In this section, future works that can be performed on the modified algorithms are suggested as follows:

- Building a WLAN test bed and implementing the proposed algorithms.
- Redoing the mathematical analysis to account for the DIFS and SIFS times assigned by the IEEE802.11.
- Analyzing the impact of the modified algorithms on the power consumption of IEEE802.11 devices.
- Study the effect of changing the CTS control frame Structure to include a TA field and introducing intelligence to both the CTS and RTS control frames.

References

1. V. A. Dubenorf, "Wireless Data Technologies", First Edition, Wiley, 2003.
2. S. Baatz, "Bluetooth scatternets: an enhanced adaptive scheduling scheme", Infocom 2002 Twenty-First Annual Joint Conference of the IEEE Computer and Communication Societies, Proceedings IEEE, vol. 2 June 2002, pp. 782-790.
3. B. P. Crow, I. Widjaja, J. G. Kim, and P. T. Sakai, "IEEE802.11 Wireless Local Area Networks", IEEE Communications Magazine, pp. 116-126, September 1997.
4. B. H. Walke, N. Esseling, J. Habetha, A. Hettich, A. Kadelka, S. Mangold and J. Peetz, "IP over Wireless Mobile ATM – Guaranteed Wireless QoS by HiperLAN/2", Proceedings of the IEEE, pp. 21-40, January 2001.
5. J. S. park and D. Dicoi, "WLAN Security: Current and Future", IEEE Internet Computing, vol. 7,issue 5, Sept-Oct 2003, pp. 60-65.
6. Wi-Fi Alliance, www.wi-fi.org
7. U. Varshney, " The Status and Future of 802.11-based WLANs", IEEE Computer, vol. 36 issue 6, June 2003, pp. 102-105.
8. Y-C. Tseng, C-S. Hsu and T-Y. Hsieh, "Power-Saving Protocols for IEEE 802.11-based Multi-Hop Ad Hoc Networks", Infocom 2002 Twenty-First Annual Joint Conference of the IEEE Computer and Communication Societies, Proceedings of IEEE Infocom, vol.1 June 2002, pp. 200-209.

9. J-P. Ebert and A. Wolisz, "Combined Tuning of RF power and Medium Access Control for WLANs", Journal of Mobile Networks & Applications (Monet), vol. 6, no. 5, September 2001, pp. 417-426.

10. S. Ray, J. B. Carruthers and D. Starobinski, "RTS/CTS-Induced Congestion in Ad Hoc Wireless LANs", IEEE Wireless Communications and Networking, 2003, vol. 3, March 2003, pp. 1516-1521.

11. J. P. Monks, V. Bharghavan and W-M. W. Hwu, "A Power Controlled Multiple Access Protocol for Wireless Packet Networks", IEEE Infocom 2001, pp. 219-228.

12. J. Li, Z. J. Haas, M. Sheng and Y. Chen, "Performance Evaluation of Modified IEEE802.11 MAC for Multi-Channel Multi-Hop Ad Hoc Network", The International Conference on Advanced Information Networking and Applications (AINA), March 27- 29, 2003.

13. S. Xu and T. Saadawi, "Does the IEEE802.11 MAC protocol work well in Multihop Wireless Ad Hoc Networks?", *IEEE COM. Mag.*, vol. 39, no. 6, June 2001, pp. 130-137.

14. IEEE802.11 Working Group Home Page, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", IEEE Std 802.11, http://grouper.ieee.org/groups/802/11/, 1999 Edition.

15. IEEE802.11 Working Group Home Page, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band", IEEE Std 802.11b, http://grouper.ieee.org/groups/802/11/, 1999 Edition.

16. IEEE802.11 Working Group Home Page, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band", IEEE Std 802.11a, http://grouper.ieee.org/groups/802/11/, 1999 Edition.

17. S. Kerry and K. McCabe, "Popular wireless local area networks gain large boost in speed", IEEE website, http://standards.ieee.org/announcements/80211gfinal.html, June 2003.

18. A. Grilo, M. Macedo and M. Nunes, "A scheduling algorithm for Qos support in IEEE802.11E Networks", Wireless communication, vol. 10, no.3, June 2003, pp.36-43.

19. IEEE802.11 Working Group Home Page, "(D8) Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security", IEEE Std 802.11i, http://grouper.ieee.org/groups/802/11/, 2004 Edition.

20. J. Geier, "802.11 WEP: Concepts and vulnerability", Wi-Fi planet, http://www.wi-fiplanet.com/tutorials/article.php/1368661, June 2002.

21. M.S. Gast,"802.11 Wireless Networks", First Edition, O'Reilly.

22. L. Kleinrock and F. A. Tobagi, "Packet switching in radio channels: Part II-The Hidden Terminal Problem in Carrier Sense multiple Access and the Busy-Tone Solution", *IEEE Trans. Com.*, vol. COM-23, no. 12, Dec. 1975, pp. 1417-1433.

23. A. J. Goldsmith and S. B. Wicker, "Design challenges for energy-constrained Ad Hoc Wireless Networks", *IEEE Wireless Communications Magazine,* August 2002, pp.8-27.

24. E. M. Royer, C-K Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", IEEE Personal Communications, vol. 6, no. 2, April 1999, pp. 46-55

25. Z. J. Haas and M. R. Pearlman, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks", draft-ietf-manet-zone-zrp-04.txt, July 2002.

26. L. Kleinrock and F. A. Tobagi, "Packet switching in radio channels: Part I-Carrier Sense Multiple-Access modes and their delay characteristics", *IEEE Trans. Com.*, vol. COM-23, no. 12, Dec. 1975, pp. 1400-1416.

27. J. Spragins, J. Hammond and K. Pawlikowski, "Telecommunications Protocol and Design", *Addison-Wesley Publishing*, 1991.

28. Y. Uhuegbulem, A, O. Fapojuwo and A. B. Sesay, "Performance Analysis of IEEE802.11 WLANs with Exposed Nodes", Wireless 2003 The Fifteenth International Conference on Wireless Communications Proceedings, vol. 2, July 2003, pp. 344-350.

29. OPNET Technologies, "The OPNET Modeler Documentation," version 9.0 2002.

30. VINT Project, "The *ns* Manual", http://www.isi.edu/nsnam/ns/doc/index.html