NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

IEEE 802.11 MAC PROTOCOL PERFORMANCE EVALUATION IN OPERATIONAL ENVIRONMENTS

by

Kacha Jitpanya

March 2002

Thesis Advisor:	Robert Ives
Co-Advisor:	Murali Tummala

Approved for public released; distribution is unlimited.

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
29 Mar 2002	N/A	-

Title and Subtitle IEEE 802.11 MAC Protocol Performance Evaluation in Operational Environments	**Contract Number**
	Grant Number
	Program Element Number
Author(s) Jitpanya, Kacha	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Naval Postgradaute School Monterey, California	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes The original document contains color images.	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 73	

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2002	Master's Thesis

4. TITLE AND SUBTITLE IEEE 802.11 MAC Protocol Performance Evaluation in Operational Environments

5. FUNDING NUMBERS

6. AUTHOR (S) Jitpanya, Kacha

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the U.S. Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public released; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(maximum 200 words)***

The IEEE 802.11 MAC protocol is widely used for wireless local area networks. Consequently, it is important to examine the protocol performance in operational environments. This thesis presents a simulation study of the performance of the IEEE 802.11 MAC protocol in multihop, jamming, and mobile node environments. The effects of the request-to-send mechanism and fragmentation in these environments are also studied. The average throughput and delay are obtained from the simulation and these results are then used to analyze the protocol performance.

14. SUBJECT TERMS
Mobile Ad Hoc Network, Optimum Network Performance, 802.11, Medium Access Control, Jamming, Multihop, Node Velocity

15. NUMBER OF PAGES 73

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500 **Standard Form 298 (Rev. 2-89)**
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public released; distribution is unlimited.

IEEE 802.11 MAC PROTOCOL PERFORMANCE EVALUATION IN OPERATIONAL ENVIRONMENTS

Kacha Jitpanya
Ensign, Royal Thai Navy
B.S., University of Washington, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
March 2002

Author: Kacha Jitpanya

Approved by: Robert Ives, Thesis Advisor

Murali Tummala, Co-Advisor

Dan C. Boger, Chairman
Information Sciences Department

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The IEEE 802.11 MAC protocol is widely used for wireless local area networks. Consequently, it is important to examine the protocol performance in operational environments. This thesis presents a simulation study of the performance of the IEEE 802.11 MAC protocol in multihop, jamming, and mobile node environments. The effects of the request-to-send mechanism and fragmentation in these environments are also studied. The average throughput and delay are obtained from the simulation and these results are then used to analyze the protocol performance.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS

ACK	Acknowledgement
AP	Access Point
BER	Bit Error Rate
BSS	Basic Service Set
CFP	Contention-Free Period
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
DCF	Distributed Coordination Function
DIFS	DCF Interframe Space
DS	Distribution System
DBPSK	Differential Binary Phase Shift Keying
DQPSK	Differential Quadrature Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
DTIM	Delivery Traffic Indication Message
ECC	Error Correction Control
EIFS	Extended Interframe Space
ESS	Extended Service Set
FHSS	Frequency-Hopping Spread Spectrum
FTP	File Transfer Protocol
GFSK	Gaussian Frequency Shift Keying
IEEE	Institute of Electrical and Electronics Engineers
IR	Infrared
IFS	Interframe Space
JTRS	Joint Tactical Radio System
MAC	Medium Access Control
MANET	Mobile Ad Hoc Network
MPDU	MAC Protocol Data Unit
NAV	Network Allocation Vector

OPNET	Optimum Network Performance
PC	Point Coordinator
PCF	Point Coordination Function
PIFS	PCF Interframe Space
PPM	Pulse Position Modulation
RTS	Request To Send
SIFS	Short Interframe Space
SNR	Signal-To-Noise Ratio
TCP	Transport Control Protocol
WLAN	Wireless Local Area Network

ACKNOWLEDGEMENTS

This thesis is dedicated to my parents and my loving wife, Chanokporn, for their constant supports. I would also like to thank our daughter, Kanisa, for being such a wonderful kid.

I would like to thank my thesis co-advisors, Dr. Robert Ives and Dr. Murali Tummala, for their guidance and encouragement. I would also like to thank Dr. Supachai Sirayanone for his consultant.

Finally, I would like to thank the Royal Thai Navy for giving me an opportunity to pursue a master's degree in systems engineering.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

This thesis presents results from a simulation study evaluating the performance of the Institute of Electrical and Electronics Engineers (IEEE) 802.11 medium access control (MAC) protocol in operational environments. By using the OPNET software as the simulation tool, the study evaluates the protocol performance in three operational environments.

A. BACKGROUND

A mobile ad hoc network (MANET) consists of wireless nodes, which may be mobile and operable even without an infrastructure [1]. This type of network is easy and fast to deploy making it favorable in situations where an infrastructure is not available or even practical. A MANET can be efficiently applied to personal area networking, military environments, civilian environments, or emergency operations [1]. One example of MANET in military environments is the joint tactical radio system (JTRS). The JTRS is basically sought for scalable, interoperable networks operating in radio frequency band to provide secure and non-secure voice, video and data communications using multiple narrowband and wideband waveforms [2].

Moving from wired to wireless networks, the main difference is the physical medium. Since the wireless medium is shared and unprotected, interference from noise or other signals is unavoidable. This makes the wireless medium significantly less reliable [3]. To increase certain quality of services, a medium access protocol greatly impacts on the performance of such a network. The IEEE 802.11 MAC protocol has been suggested as a possible MAC protocol for JTRS. The IEEE 802.11 MAC protocol is specified in the IEEE 802.11 standard, approved in 1997 and revised in 1999 [4]. The standard also includes specifications for three physical layers: direct sequence spread spectrum (DSSS), frequency hopping spread spectrum (FHSS), and infrared (IR).

B. OBJECTIVES

The objective of this study is to evaluate the 802.11 MAC protocol in operational environments in an attempt to establish a performance benchmark. The effects of node velocity, multihop, and jamming are specifically examined with File Transfer Protocol (FTP) network traffic. These three scenarios are considered to be common in an operational environment. Multihop is useful when the destination station is out of transmitting range; with multihop, the source station can use its neighbor nodes to relay a packet. If the protocol performs well in this environment, then each network node is acting effectively as both a workstation and router.

Another scenario of interest is when nodes are moving. In real-world scenarios, individual soldiers on foot, in helicopters, or in tanks, traveling with different velocities, would be able to communicate with one another effectively. As a consequence, the study of effects of node velocity on the performance of the protocol would be able to identify whether the protocol is suitable for this type of environment.

Jamming is another anticipated, unavoidable military scenario, which is considered a potential problem to JTRS [2]. A good network protocol should operate reasonably well under jamming.

C. RELATED WORKS

Since there are many parameters that are left to designers, many studies have been carried out to evaluate and optimize the performance of the IEEE 802.11 MAC protocol. The multihop environment study by Xu and Saadawi has found that Transport Control Protocol (TCP) experienced instability and unfairness problems caused by the IEEE 802.11 MAC protocol [5]. They concluded that the protocol's ability to work in multihop environment was doubtful. They also provided a thorough analysis of the problems. However, using a different simulation tool and network traffic characteristic in similar environment, this study will focus mainly on the overall performance of the IEEE 802.11-based networks. This study aims to verify whether the protocol would work sufficiently well in military tactical operations.

The effect of mobility studied by Khurana et al. found a significant effect on performance [6]. Other studies related to this MAC protocol identify effects of a request-to-send (RTS) handshake and fragmentation in regular, fixed network configurations [3], [6], [7]. However, the current study will focus more on military-oriented network environments using three scenarios most common in the operational environment. Finally the effect of jamming on the protocol performance will be studied.

D. ORGANIZATION

This chapter presented background information and the objectives of this study along with a discussion of some related works. The next chapter gives a summary of the IEEE 802.11 standard. It mainly focuses on the MAC sublayer functions of the standard. Chapter III begins with an overview of OPNET simulation software and its Wireless Local Area Network (WLAN) model used in this study followed by an explanation of simulation environments and network configurations. Chapter IV presents and discusses the results of the simulation and the final chapter, Chapter V, presents conclusions and recommendations.

THIS PAGE INTENTIONALLY LEFT BLANK

II. IEEE 802.11 MAC PROTOCOL

The summary of the IEEE 802.11 standard is given in this chapter. The chapter introduces the network configuration defined in the standard proceeded by a description of the MAC sublayer function. This chapter concludes with a specification of the physical layers. Detailed descriptions of the complete standard can be found in [4] and [8], which provide the basis of this chapter.

A. IEEE 802.11 NETWORK CONFIGURATION

The IEEE 802.11 MAC protocol is the first international standard for wireless local area networks (WLAN) [4]. The basic network configuration is called a basic service set (BSS). The BSS consists of two or more wireless stations, which are further classified into two types, independent and infrastructure. In the independent BSS, stations can communicate directly among themselves. Figure 1 shows two BSSs, each with two wireless stations.

On the other hand, the infrastructure BSS also contains an access point (AP) to provide access to other networks, which can be either wireless or wired networks. In this way, stations in one BSS can communicate not only among themselves but also with stations in another BSS. This configuration is called an extended service set (ESS). As shown in Figure 1, APs communicate with one another using a distribution system (DS) that extensively provides connectivity among and between BSSs and other 802.x networks.

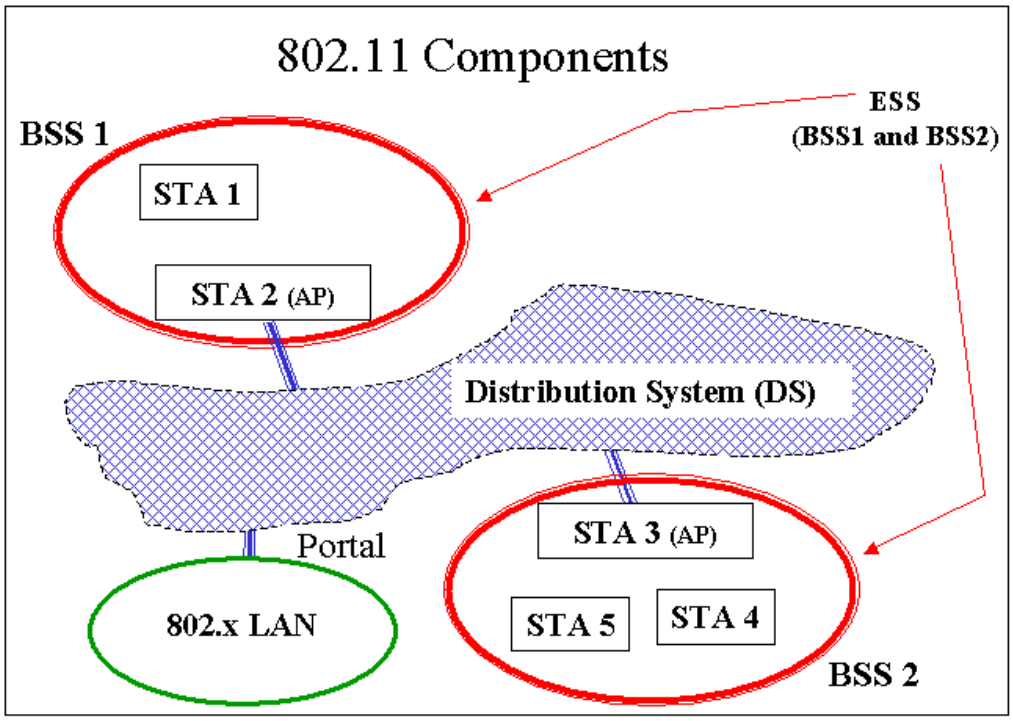

Figure 1. IEEE 802.11 Network Configuration (After [1])

B. MAC SUBLAYER ARCHITECTURE

The basic medium access method of the IEEE 802.11 MAC protocol is the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) [8]. Figure 2 illustrates the MAC architecture indicating the Distributed Coordination Function (DCF) and Point Coordination Function (PCF) as two main components of its architecture.

A DCF is used in both independent and infrastructure networks; whereas, a PCF is an optional access method and used only in infrastructure network configurations. In the infrastructure network a point coordinator (PC) controls access to the medium permitting the DCF and PCF to coexist.

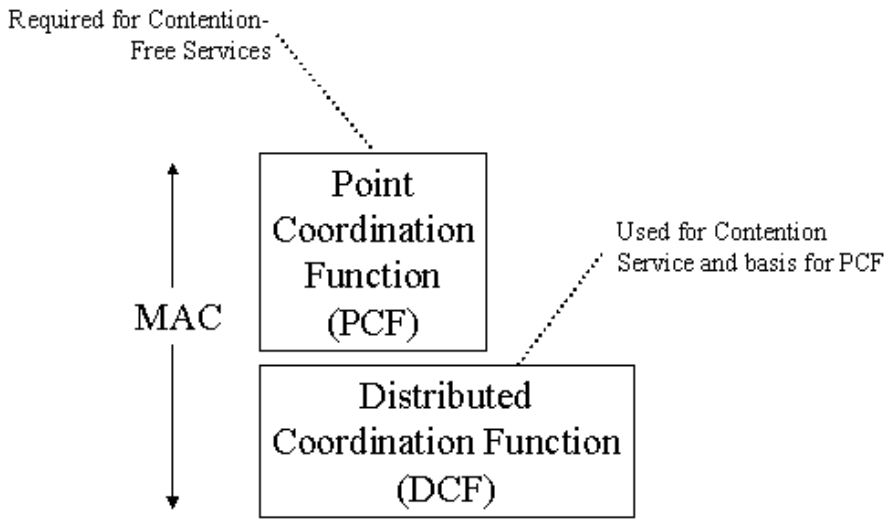

Figure 2. MAC Sublayer Architecture (After [1])

C. DISTRIBUTED COORDINATION FUNCTION

A DCF is the basic medium access method using CSMA/CA and a random backoff time following a busy medium condition [8]. Since a wireless station cannot hear its own transmission, it cannot detect the collision [7]; therefore, the CSMA/CA algorithm is used. A positive acknowledgement is also needed for each transmitted frame. If an acknowledgment is not received, a retransmission takes place.

1. Carrier Sense Mechanism

Both physical and virtual carrier sense mechanisms are used in determining the condition of the medium (busy or idle). The medium is idle only when both mechanisms indicate such a condition. The physical layer performs a physical carrier sensing and forwards the information to the MAC. The MAC layer uses the network allocation vector (NAV) to implement the virtual carrier sense mechanism, which reserves the medium for transmitting a data frame and its acknowledgment. The NAV values tell other stations how long the current transmission might take after which those stations can try to access the medium again. Reserving the medium is accomplished in two ways: by using a Duration/ID field in the request-to-send (RTS) and clear-to-send (CTS) frames, or using the Duration/ID field in directed frames.

2. MAC-Level Acknowledgments

A positive acknowledgment requires that a station receiving certain kinds of frames must respond by sending an acknowledgment back to the transmitting station. If the transmitting station does not receive the acknowledgment, it will assume that an error has occurred and will automatically retransmit the frame. An error can occur in transmitting either the data frame or the acknowledgment frame.

3. Interframe Space (IFS)

After sensing that the medium is idle, a station must wait for a certain interval of time, called an interframe space (IFS), before attempting to transmit. There are four different types of IFS, which prioritize a station in accessing the medium. The first type is a short interframe space (SIFS), used in sending an acknowledgement, CTS, and the second or subsequent frames of a fragment burst. During the contention-free period (CFP), a station also uses a SIFS when it responds to a poll while a point coordinator (PC) may use a SIFS for any type of frame. A SIFS is the shortest interframe space; consequently, it gives a particular station the highest priority in gaining access to the medium.

The second type is a PCF interframe space (PIFS). Except when responding to the poll, a station will use PIFS during the CFP. The third type is a DCF interframe space (DIFS), which is used under the DCF. DIFS is the longest interframe space. Hence, a station waiting a DIFS period has the lowest priority. A point coordinator is guaranteed to gain and maintain control of the medium to start the CFP by employing PIFS instead of DIFS. The fourth type of IFS is an extended interframe space (EIFS), used when the first attempt to transmit a frame has failed. Since the EIFS is shorter than DIFS, a retransmission has higher priority than a normal transmission.

4. DCF Access Procedure

a. Basic Access

Basic access is a core mechanism in accessing the medium. Under the DCF access method, the basic access operates as follows. A station may transmit a frame when the medium is idle for DIFS following a successful frame transmission, or for EIFS

following an unsuccessful frame transmission. However, if the medium is sensed to be busy, a station needs to wait for a specified length of time after the medium is idle again as described below.

b. Backoff Procedure

With CSMA/CA, a station senses the medium before it transmits a data frame. If the medium is busy, a station defers accessing till the end of the current transmission. When the medium becomes available again, many stations could attempt to transmit a frame but may cause collisions. To minimize these collisions a station must wait a random backoff time before attempting to transmit again.

After sensing the medium is idle for DIFS (if the last transmission was successful), or for EIFS (if the last transmission was not successful), a station begins a backoff procedure. A station starts the backoff procedure by setting its backoff timer to a random backoff time, which is equal to a random number multiplied by a fixed time slot duration. During the backoff, a station senses the medium every slot time and decrements the backoff timer by one slot time if the medium is sensed to be idle. On the other hand, the backoff timer will not be decremented if the medium is sensed to be busy. With this procedure, a station with the smallest backoff time will gain access to the medium first.

c. Recovery Procedures and Retransmit Limits

Errors can occur if the transmitting station does not receive a CTS frame after sending an RTS frame, or an acknowledgment frame after sending the data frame. To recover from an error, a station will retransmit the frame. If the retry limit is reached before a successful transmission is achieved, the frame is dropped.

d. Setting and Resetting the NAV

Using the NAV is the way the standard implements the virtual carrier sensing mechanism. As shown in Figure 3, except for the source and destination station, all other stations should set their NAV when they receive a valid frame. In this figure, a source station (denoted *Source*) would transmit an RTS frame after the medium is sensed idle for a DIFS period. Stations located near the source station (denoted *Other*) will receive an RTS frame and set their NAV according to the duration information in the

frame. The receiver (denoted *Destination*), however, responds with a CTS frame after a SIFS period. Other stations that are too far away from the source but can receive the CTS (also denoted *Other*) will set their NAV using the information in a CTS frame. However, the station will not reset the NAV if the new value is smaller than the current NAV value.

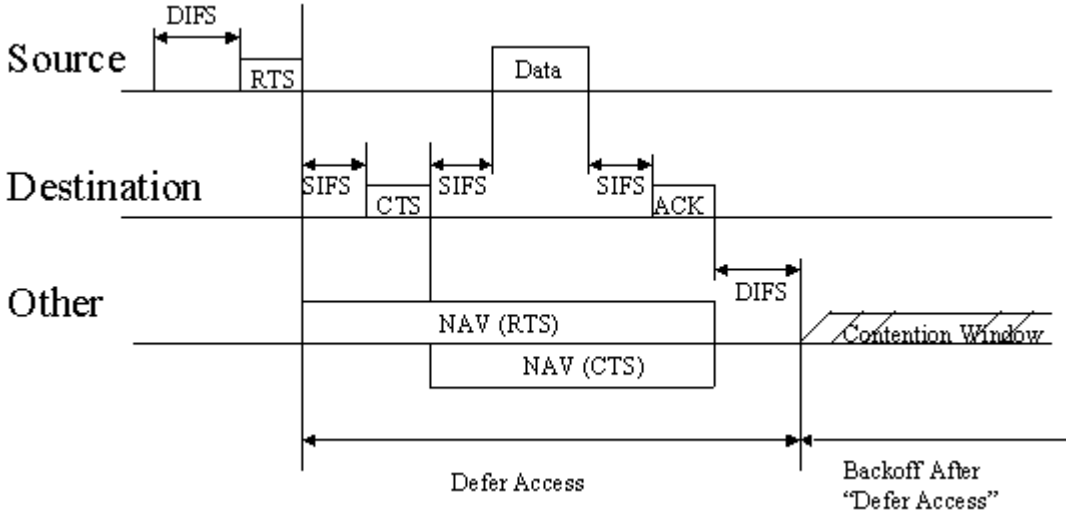

Figure 3. NAV Setting (After [1])

e. RTS/CTS Usage with Fragmentation

In some conditions of the medium and network configurations, transmitting a large frame might be less successful or even impossible. Fragmenting and defragmenting a frame and transmitting smaller frames individually may increase the success of transmitting a large frame. The original frame is rebuilt once all fragments are received.

Virtual carrier sensing using RTS/CTS with fragmentation operates as follows. Only one exchange of RTS/CTS frames occurs for transmitting all fragments of a particular frame. As shown in Figure 4, the channel reservation information in the Duration/ID field of the RTS/CTS frames is set for transmitting the first fragment and its acknowledgment. The duration information in each fragment and its acknowledgment specifies the duration of the next fragment and acknowledgment, and so on. However, the duration information of the last fragment is for its acknowledgment, whose duration information will be zero.

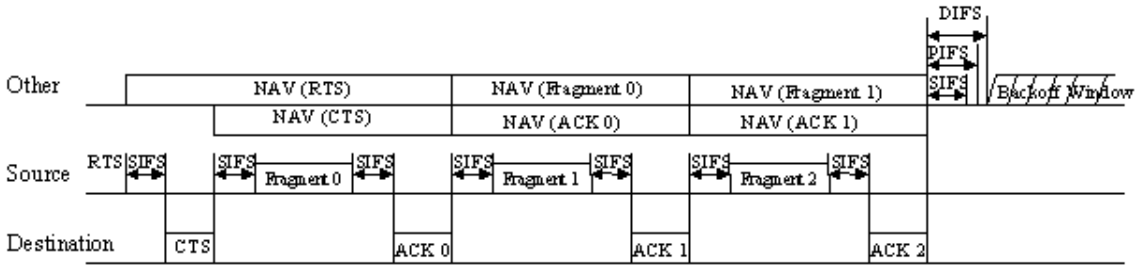

Figure 4. Timing of Using RTS/CTS with Fragmented Data Frame (After [1])

f. CTS Procedure

When transmitting an RTS frame, a source station will wait for the destination station to send back a CTS frame. After the duration of CTSTimeout, if the transmitting station does not get the CTS frame back, it will assume that the exchange of RTS/CTS frames is not successful and go into a backoff procedure.

A destination station will reply with a CTS frame when it receives an RTS frame addressed to it and the carrier sensing mechanisms indicate that the medium is available. However, if the medium is not available, it will disregard that RTS frame.

5. Acknowledgement Procedure

After transmitting a frame that requires an acknowledgment, a station will wait for the acknowledgment frame. It will wait up to the acknowledgement timeout interval. If it does not receive the acknowledgment frame after this interval, it assumes that the transmission was unsuccessful. Therefore, the station must follow the backoff procedure before it can retransmit.

A receiving station sends back an acknowledgment frame after a SIFS period if the received frame is valid and requires an acknowledgment. In transmitting the acknowledgment frame, the state of the medium is not considered.

6. Duplicate Detection and Recovery

A station uses a *sequence control* field in a frame to check for duplicated frames. The *sequence control* field consists of a sequence number and fragment number. All fragments of a particular frame have the same sequence number. A frame that has the retry bit set in the *frame control* field and the same sequence number and fragment

number as a previously received frame is a duplicate. When there is a duplicate of a frame, a receiving station will disregard the duplicate. Nonetheless, if the received frame is a valid frame and requires to be acknowledged, the station needs to send back an acknowledgment.

D. POINT COORDINATION FUNCTION (PCF)

A PCF offers a guarantee of access to the medium for stations in a BSS [8]. This is beneficial for time-bound application traffic, such as voice or video. This section explains the contention-free period structure, the access procedure, and the transfer procedure.

A PCF consists of a point coordinator (PC) and stations that can respond to the contention-free (CF) polling frame. The PC controls the access of the medium during the contention-free period. Once polled, a station may transmit only one frame to any station. All stations, including the PC, may "piggyback" the acknowledgment using data frame subtypes to increase the efficiency of the CFP.

1. Contention-Free Period Structure and Timing

As shown in Figure 5, a beacon frame with a delivery traffic indication message (DTIM) element marks the beginning of each contention-free period. The PC controls the length and rate of the CFP. The CFP typically ends at the specified length; however, available traffic and size of the polling list may cause the PC to terminate it earlier.

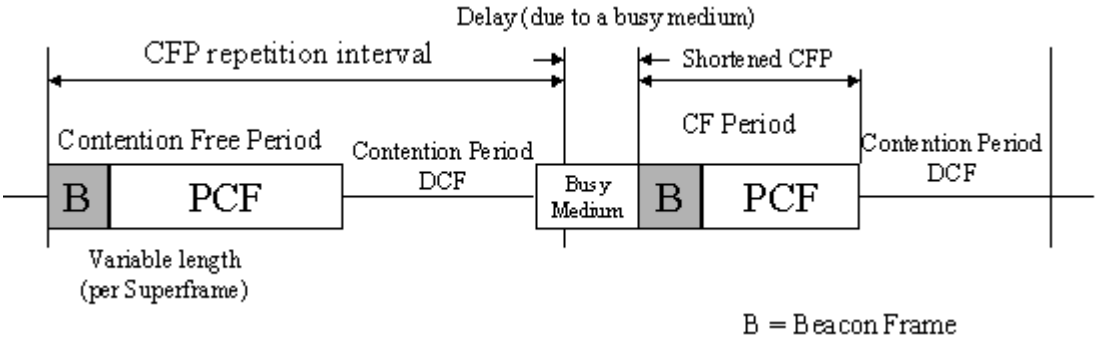

Figure 5. Timing Diagram of CFP (After [1])

2. PCF Access Procedure

The polling scheme is the building block for the contention-free transfer protocol. The PC performs polling to allow other stations to transmit a frame. At the start of the CFP, the PC is guaranteed access to the medium using the DCF access procedure by using a shorter interframe space, PIFS instead of DIFS. Once taking control of the medium, the PC maintains control for the entire CFP. This results in requiring all other stations to set their NAVs to the length of the CFP, as shown in Figure 5.

During any of the CFPs shown in Figure 5, after sensing the medium is idle for one PIFS period, the PC transmits a beacon frame containing the CF parameter set element and a DTIM element. The PC then transmits a data frame, a CF-Poll frame, a Data + CF-Poll frame, or a CF-End frame one SIFS period later. After these steps, if the PC has no traffic buffered and no polls to send, it will immediately end the CFP by sending a CF-End frame. If the PC does send those frames, a station that is addressed by the PC starts the transfer procedure, explained in later sections.

At the beginning of the CFP, each station, except the PC, sets its NAV to the maximum length of the CFP. This prevents stations from taking control of the medium. The length of the CFP is contained in the CF Parameter Set element within beacon frames. At the end of the CFP, the PC will transmit either a CF-End or CF-End + ACK frame. These frames tell other stations to reset their NAV.

3. PCF Transfer Procedure

Since the PC controls the access to the medium during the contention-free period, it controls both the order of transmissions and stations allowed to transmit. After gaining access to the medium, the PC starts the CFP by sending a beacon frame. It then transmits Data, CF-Poll, CF-ACK, Data + CF-ACK, Data + CF-Poll, Data + CF-Poll + CF-ACK, CF-Poll + CF-ACK, or any management frame after a SIFS period. A station receiving a CF-Poll may transmit a data frame after a SIFS period without resetting its NAV. The PC can send an acknowledgment along with a data frame even if the station expecting the data and the one expecting the acknowledgment are not the same. This is called "piggybacking" which can improve the efficiency of the CFP. A station expecting the acknowledgment will look at the subtype of the frame.

If a transmission of a poll fails, the PC will transmit its next frame after a PIFS period. The collisions are avoided since a station may have responded after a SIFS period. A station responds with a Null frame or CF-ACK (no data) if it has no data to send. Then the PC ends the CFP by sending a CF-End and the stations reset their NAVs.

E. PHYSICAL LAYER

Three physical layers have been recommended in the IEEE 802.11 standard: direct sequence spread spectrum (DSSS), frequency hoping spread spectrum (FHSS), and infrared (IR) [4]. This section briefly discusses their specifications.

1. Direct Sequence Spread Spectrum (DSSS)

The DSSS physical layer operates at the 2.4 GHz industry scientific and medical (ISM) radio band [4]. In North America, there are 12 channels, each with a bandwidth of 22 MHz. The data rate is set to be 1 Mbps or 2 Mbps. A differential binary phase shift keying (DBPSK) modulation scheme is specifically used for the 1 Mbps data rate while differential quadrature phase shift-keying (DQPSK) is used for the 2 Mbps data rate. The maximum allowable transmit power for North America is 1,000 mW.

2. Frequency Hoping Spread Spectrum (FHSS)

The FHSS physical layer also operates at the 2.4 GHz ISM radio band, with a bandwidth of 1 MHz for each channel [4]. In North America, the first channel operates at 2.402 GHz and the last channel at 2.495 GHz. A minimum of 2.5 hops per second for a minimum hop distance of 6 MHz is required. Two data rates are supported, 1 Mbps and 2 Mbps. Two-level Gaussian frequency shift-keying (GFSK) is used for 1 Mbps, and four-level GFSK for 2 Mbps.

3. Infrared (IR)

The IR physical layer uses near-infrared light as its transmission medium [4]. The IR is good for indoor communication; however, unlike radio media, it cannot penetrate through a wall. The IR physical layer supports both 1 Mbps and 2 Mbps. Pulse position modulation (PPM) is used to transmit data. Sixteen level PPM is specifically used for 1 Mbps, and four level PPM for 2 Mbps.

F. SUMMARY

This chapter has provided a summary of the IEEE 802.11 standard. The network configurations, MAC sublayer functionality, and specifications of the physical layer are explained. The two main components of the MAC architecture, DCF and PCF, were discussed. The next chapter, Chapter III, will present a description of the protocol model implemented in OPNET and the simulation environments.

THIS PAGE INTENTIONALLY LEFT BLANK

III. WIRELESS LAN (WLAN) SIMULATION AND MODELING

This study uses OPNET Modeler, version 8.0, on a Windows 2000 platform. The WLAN Model, available with the software package, is used as a tool since the model is based on the IEEE 802.11 standard [9] making it very convenient in evaluating the IEEE 802.11 MAC protocol. Most of the protocol parameters can be modified to check its effect on the performance, allowing the simulation results to be readily obtainable. However, the actual physical layer specification is not simulated in this model [9].

Choosing OPNET Modeler as a simulation tool is based on its availability. In addition to its graphical user interface, OPNET is very effective and convenient in duplicating a network configuration so different settings can be explored. Other simulation tools, such as Matlab and the C-programming language, can also be used.

A. OPNET WLAN MODEL

This section covers details on implementing the WLAN model. The OPNET modeling philosophy is described first, followed by a brief discussion on how the state diagram of the MAC protocol works. Finally, this section gives details of the radio communication mechanism used in OPNET. All information in this section is taken from [9].

1. OPNET Modeling Architecture

Modeling in OPNET is organized into a hierarchy similar to real network systems. As shown in Figure 6, modeling can be done in three different layers: network, node, and process domain. A network model consists of communicating nodes and links, which are examples of node and link models, respectively. A network can further be used as a subnetwork in another network. Subnetworking makes it simple to model a large and complex network. In this structure, the hierarchy can be nested to any depth.

Node models are composed of modules and connections. Modules are sources, sinks, or processors of information; whereas, connections are the controller of information movement between modules. Users can define behavior of modules using a

process model, coded in Proto-C. A Proto-C process is a combination of graphical state-transition-diagrams, embedded C/C++ language data items and statements, and a library of Kernel Procedures used for programming in Proto-C. Process parameters, called attributes, can be created to avoid hardwiring of some specifications of a process. Each attribute has a name, a value, and properties. Users can extensively control the behavior of objects by customizing their attributes. Every object in each modeling domain has a set of attributes, which can also be "promoted" so that their values can be specified in upper layers. At the topmost layer, object attributes become the attributes of the simulation.

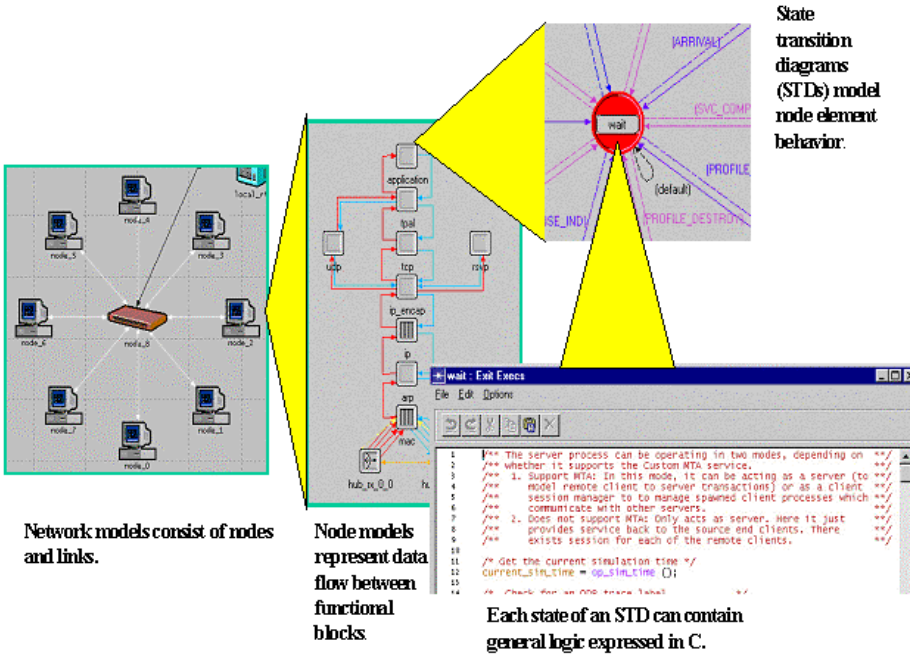

Figure 6. OPNET Modeling Domains (After [9])

Information is carried between communicating objects in a packet, which can be transferred between objects in the Node and Network domains. Each network has its own packet format.

Any OPNET simulation automatically creates output vectors, output scalars, and animations. Output vectors collect simulation data as a function of simulation time. Scalar statistics are single values of a simulation data of interest for each simulation run. These values are obtained from vector statistics as an average, peak value, final value, or

other statistical values. Statistics of an object are called local statistics, while those of the whole system are called global statistics. Application-specific statistics are also provided. Moreover, modelers can create a program to collect a specific simulation output.

The Analysis Tool not only displays data stored in output vector and output scalar files in the form of graphs, or traces, but also provides a variety of methods for processing output data and computing new traces, such as histograms, probability density functions, cumulative density functions, and confidence intervals.

2. WLAN Node Architecture and Parameters

The current OPNET implementation of the WLAN MAC protocol has simplified, omitted, or deferred some part of the IEEE 802.11 MAC protocol [9]. The implementation mainly focuses on the distributed coordination function (DCF) of the protocol. The MAC protocol is implemented using a module, called *wireless_lan_mac*, which is described in detail later.

a. Wireless stations

A wireless station is implemented using the *wireless_lan_mac* module and other modules for different parts of the TCP/IP protocol stack. The physical layer is implemented using a radio transmitter and receiver, which will be discussed in detail later.

As shown in Figure 7, the *wireless_lan_mac* module is connected to three different modules: address resolution protocol, radio transmitter, and radio receiver modules. Both the transmitting and receiving antenna are omnidirectional, eliminating the need for an antenna module.

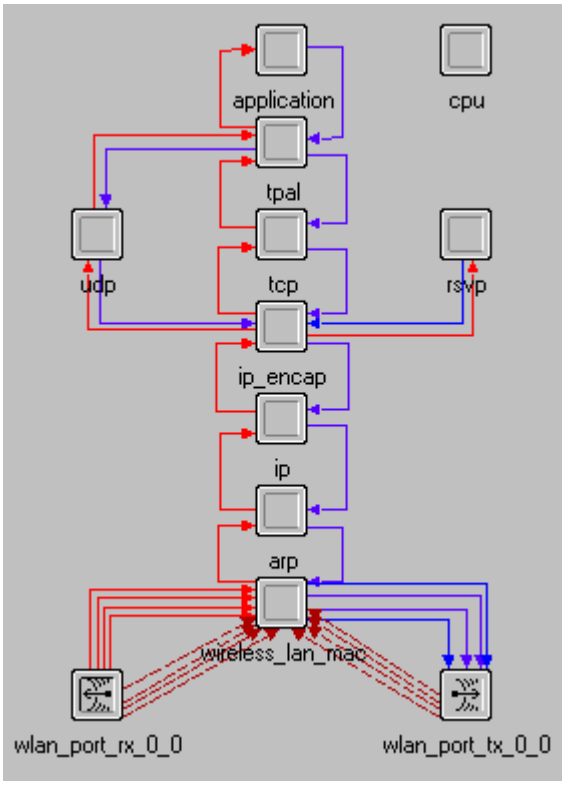

Figure 7. Workstation Module

b. Wireless Router (or Access Point)

The wireless routers provide local stations access to other networks. They have either two wireless interfaces, or one wireless interface and one wired interface. Consequently, the connected networks can be another wireless LAN or other wired networks, such as Ethernet, FDDI, frame relay, etc.

As shown in Figure 8, routers primarily have three layers: physical, MAC, and network; additionally, they also have a number of routing protocols. Figure 8 displays the module for a wireless-Ethernet router.

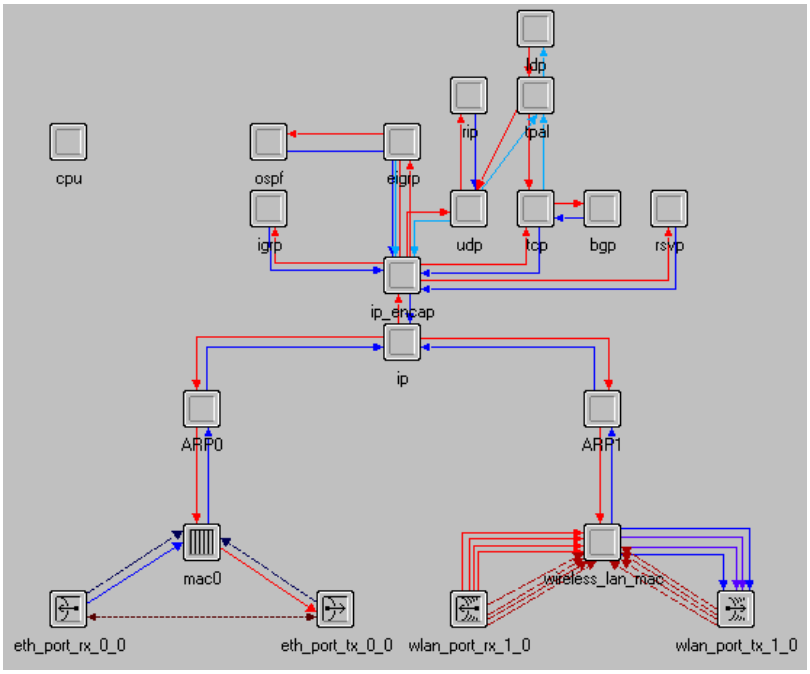

Figure 8. Ethernet-WLAN Router Module

c. WLAN Parameters

Like other modeling objects, a *wireless_lan_mac* module has a number of attributes so that users can customize their network requirements. The users configure attributes, via a graphical user interface, for the WLAN Parameters as shown in Figure 9.

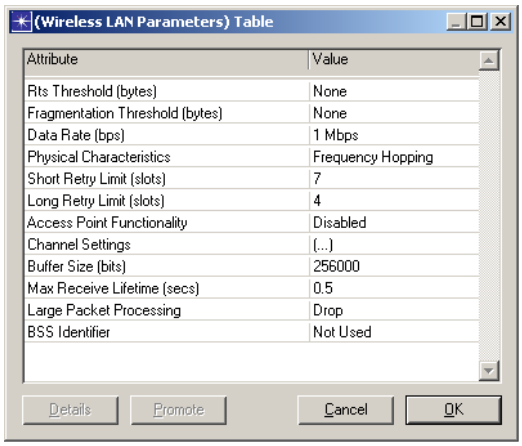

Figure 9. WLAN Parameters

Most of these parameters correspond to those defined in the IEEE 802.11 standard. Note, however, that the Physical Characteristics parameter here is only used as a flag indicating to the *wireless_mac* process the slot duration, SIFS, minimum and maximum contention window sizes. For example, for the direct sequence spread spectrum physical layer, the slot duration is $2x10^{-5}$ seconds, SIFS is $1x10^{-5}$ seconds, minimum contention window is 31, and the maximum contention window size is 1023.

3. MAC State Diagram

The 802.11 MAC protocol is implemented in Proto-C as a process called *wlan_mac*. The *wlan_mac* module consists of a graphical state-transition-diagram, embedded C/C++ language data items and statements. Actions are performed in states while transitions indicate when to change state. Once an interrupt occurs, every transition condition is checked. The state-transition-diagram of the module is shown in Figure 10.

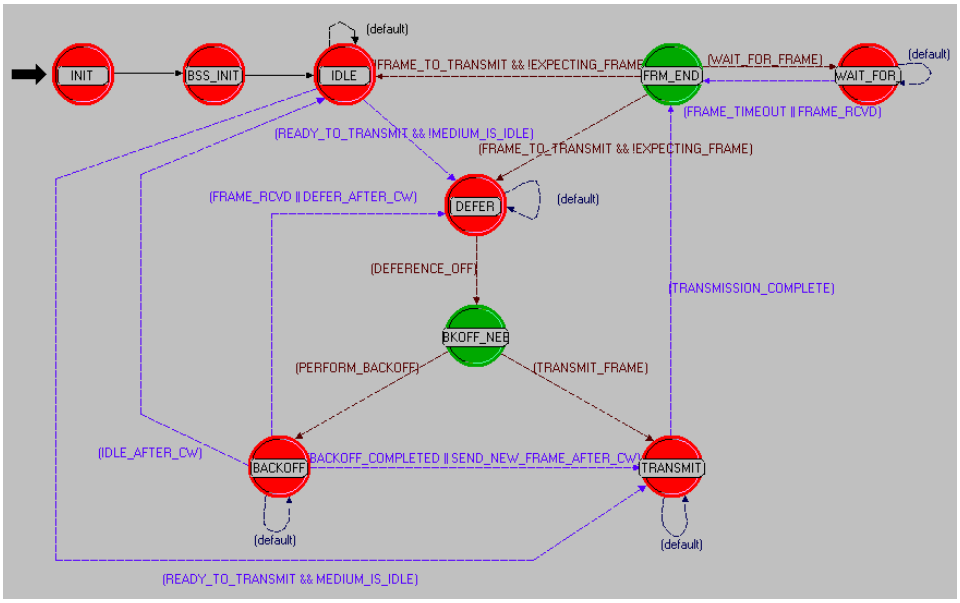

Figure 10. A *wlan_mac* State Diagram

As shown, the *wlan_mac* has 9 states and a number of transitions. After initializing, the module enters the IDLE state waiting for a frame from the higher layer for transmitting or from the lower layer for receiving. When the frame from the higher

layer arrives, the access mechanism takes place. At this point, the module checks the medium condition. If the medium is idle, the frame exchange sequence takes place. The module moves to the TRANSMIT state and transmits the frame. If fragmentation is needed, it is done in this state. After completing the transmission, the module moves to the FRM_END state. At this point, it knows if the frame requires an acknowledgment, if a retransmission is needed, or if the transmission is complete. If an acknowledgement is needed, it will move to the WAIT_FOR_RESPONSE state. If there are other frames waiting or the recovery mechanism is needed because the reception of the acknowledgement failed, the module moves to the DEFER state; otherwise, it moves back to the IDLE state.

When a higher layer frame arrives and the medium is not available, the deference and backoff mechanism are needed. The module will move to the DEFER state where it decides if it needs to backoff. If the backoff is needed, the module makes a transition to the BACKOFF state; otherwise, it can transmit the frame in the TRANSMIT state as described above. Frame reassembly and detection of duplicate packets are performed when an interrupt in the IDLE state indicates that a frame has been received from the physical layer by functions *wlan_data_process* and *wlan_tuple_find*, respectively.

4. Physical Layer Modeling

OPNET implements the physical layer of the IEEE 802.11 standard using a radio transmitter module, radio receiver module and a 14-stage pipeline. These components are described in the following sections.

a. Radio Transmitter and Receiver Modules

The radio transmitter module is a built-in module, which cannot be programmed by users, although its attributes may be customized by the users as shown in Figure 11. Since OPNET does not model the medium as an object, some of the medium attributes are associated with the transmitter while others with the receiver. There are six radio pipeline stages associated with the transmitter, which will be discussed in detail next. The channel attribute specifies bandwidth, data rate, base frequency, packet formats, power, and spreading code. The modulation attribute specifies the modulation table used in transmitting data.

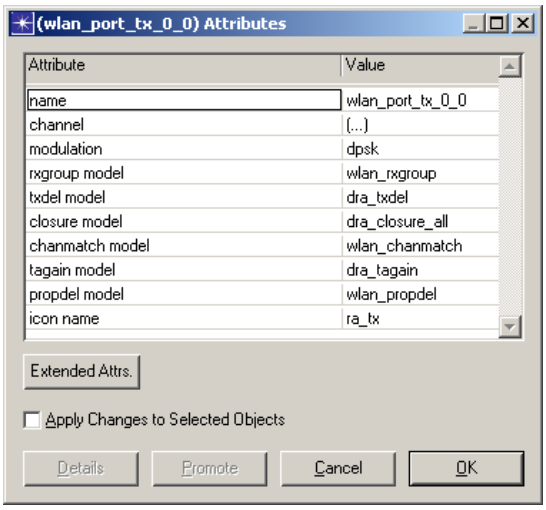

Figure 11. Radio Transmitter Module Attributes

The radio receiver module is another built-in module. Similar to the transmitter module, the receiver module is customized via its attributes and has eight radio pipeline stages associated with it, as shown in Figure 12. These are discussed in detail in a later section. The channel also specifies bandwidth, data rate, base frequency and packet formats. All of these attributes should agree with those of the transmitter to make communication possible. In addition, receiver channel attributes include processing gain, signal lock, and spreading code. The modulation attribute is the same as those of the transmitter. The noise figure is for specifying the receiver internal noise. The error correction control (ECC) threshold specifies how many errors are correctable so that retransmission is not necessary.

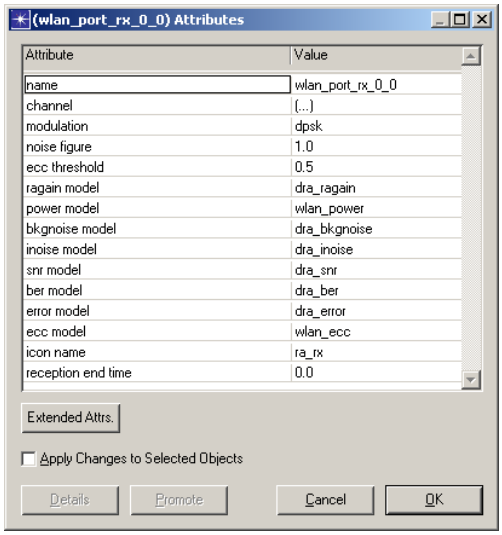

Figure 12. Radio Receiver Module Attributes

b. Radio Transceiver Pipeline

The radio transceiver pipeline is used to model the radio medium in OPNET. The radio link between a transmitter and a receiver is calculated dynamically. The radio transceiver pipeline for a WLAN model consists of fourteen stages, shown in Figure 13. As mentioned earlier and shown in Figures 11 and 12, six stages are modeled as the radio transmitter attributes while eight are modeled as the receiver attributes.

When a transmitter begins to transmit a packet, the packet will go through each of the pipeline stages. The first stage groups qualified receivers for each transmitter channel. This is not part of a transmission process but for simulation purposes only. The transmission delay (time used to transmit a packet) is calculated next. A packet will be dropped in later stages if it fails a link closure or a channel match test in the next two stages. The transmitter antenna gain, propagation delay, and receiver antenna gain are calculated respectively after that. These values together with transmitter power and propagation path loss (L_p) are used in the link budget to derive a received power in the received power stage. The propagation path loss when transmitting wavelength λ over distance D is computed as follows:

$$L_p = \frac{\lambda^2}{16\pi^2 D^2} \tag{1}$$

The next two stages calculate total noise, which is the sum of background noise and interference noise. The total noise is obtained as follows:

$$N = kTB + A_N + I_N \tag{2}$$

Where k is Boltzmann's constant (1.379×10^{-23} J/K), T is receiver system temperature, B is receiver bandwidth, A_N is ambient noise (B x 10^{-23}), and I_N is interference noise.

Based on the received power and the total noise, the signal-to-noise ratio (SNR) is derived in the *dra_snr* stage. The SNR and the processing gain are used to calculate E_b/N_0. The *dra_ber* stage derives the bit error rate (BER) from this E_b/N_0 and the modulation table. The error allocation stage then uses the BER value to compute the number of errors and then randomly allocates them to a packet. The last stage, *dra_ecc*, compares the number of errors in the packet with the error correction threshold. If the errors exceed this threshold, the packet is dropped. Otherwise, it will be set as a valid received frame and passed to the MAC layer.

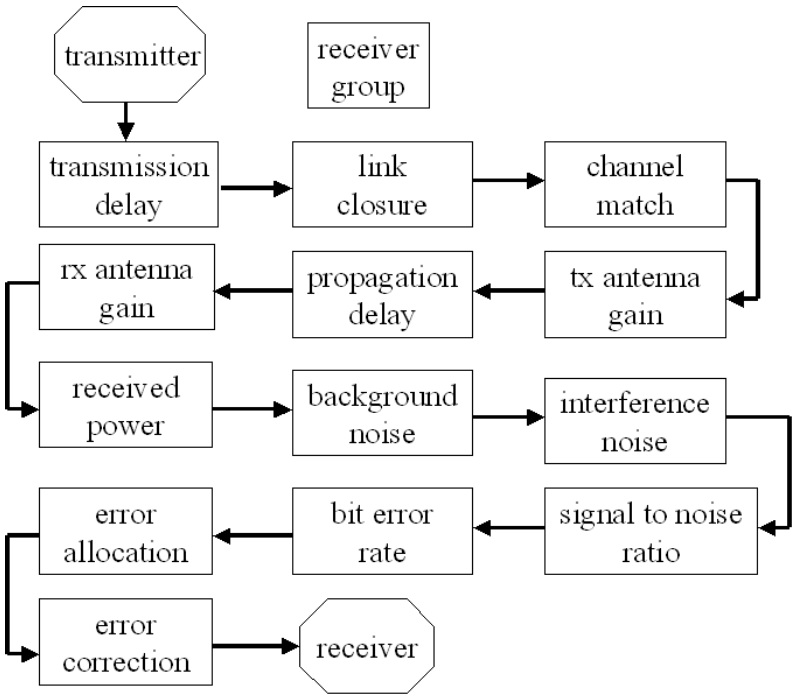

Figure 13. Radio Link Transceiver Pipelines

B. SIMULATION ENVIRONMENT

The typical network in this study consists of a number of wireless nodes within a geographical area of one square kilometer. The physical layer employed is direct sequence spread spectrum except in the jamming study, where two radio physical layers will be tested against jamming. The performance of asynchronous data transfer will be studied using the distributed coordination function of the IEEE 802.11 MAC protocol.

1. Network Application Traffic

FTP traffic is used to represent typical network traffic. Since data transfer is of interest to the study, the simulation is set up for only one FTP session. OPNET provides users with an application configuration node to set up application activities. Figure 14 shows attributes for customizing an application.

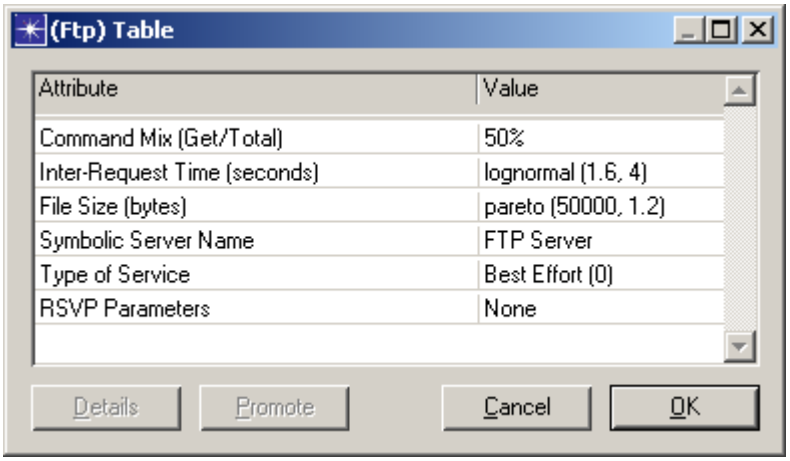

Figure 14. Application Configuration Attributes

The inter-request time attribute is the time in seconds between each file transfer within an FTP session. According to a study by Jabbari for FTP traffic, this value is typically modeled as lognormal [10]. The probability density function of this inter-request time can be expressed as

$$f_L(x) = \frac{1}{x\sqrt{2\pi\sigma^2}} \exp\left[-\frac{1}{2\sigma^2}(\ln(x)-\mu)^2\right], \quad x>0 \tag{3}$$

Jabbari further indicates that mean value $\mu = 1.6$ and standard deviation $\sigma = 2$ can approximate the empirical distributions. The file size attribute is generated randomly and can be modeled with a Pareto distribution with the probability density function

$$f(x) = \frac{ab^a}{x^{a+1}}, \quad \text{for } x \geq b \tag{4}$$

where a is the shape parameter and b is the scale parameter. According to Jabbari, the shape parameter should fall in the range $0.9 \leq a \leq 1.4$, and for all simulations a was set at 1.2. The scale parameter was set to 50,000, which gave a minimum file size of 50,000 bytes. More information on FTP traffic characteristics is included in [10]. Another important attribute is the command mix attribute. This attribute in this study was set to 50% so that 'get' and 'put' commands would be equally executed.

2. WLAN Parameters

The main objective of this study is to evaluate the performance of the IEEE 802.11 MAC protocol in the operational environment. This study also investigates which protocol features significantly affect the performance of the network. The RTS threshold and fragmentation threshold are two parameters of the protocol that will be studied in each simulation environment.

a. RTS Threshold

There are two major medium access mechanisms defined in the IEEE 802.11 standard, the basic access and the RTS/CTS access [8]. With basic access, a station may transmit a pending data frame when the medium is idle. On the other hand, when the RTS/CTS is in use, a station transmits a pending data frame after a successful RTS handshake, i.e., successfully receiving a CTS frame from the destination station.

A study by Chhaya and Gupta found that the basic access performs better with a small load, low probability of hidden nodes, and high percentage of successfully receiving a specific transmission when multiple stations transmit simultaneously (capture parameter close to 1.0) [3]. However, with a large load, the RTS/CTS method is more robust, as explained in the study, to fluctuations in parameter values and changes in the number of stations. The mechanisms can coexist by setting the threshold on the length of a data frame from the higher layer. The basic access is used if the frame size is smaller

than the threshold; otherwise, the RTS/CTS is used. These thresholds' effects on performance will be considered in each environment.

b. Fragmentation Threshold

When the medium is not suitable for receiving long frames, fragmenting a data frame from the higher layer to smaller MAC frames before transmitting increases the probability of success. A fragmentation threshold is used to indicate whether a data frame from the higher layer is fragmented. If the frame size is larger than the threshold, the frame is fragmented into smaller frames, each of which is transmitted one at a time.

c. Other Parameters

There are other parameters of the protocol. Table 1 lists some of these protocol parameters and their values used in this study. Retry limits refer to the number of attempts to transmit a frame before the frame is discarded. The long retry limit is used when a frame length is smaller than the RTS threshold; otherwise, the short retry limit is used.

Attributes	Values
Physical Characteristics	DSSS
Data Rate (bps)	2 Mbps
Short Retry Limit (time slots)	7
Long Retry Limit (time slots)	4
Slot Time (seconds)	$2x10^{-5}$
SIFS (seconds)	$1x10^{-5}$
Min contention window (time slots)	31
Max contention window (time slots)	1023

Table 1. Protocol Parameters

C. PERFORMANCE METRICS

Ideally, wireless networks should provide functionality with the same quality as wired networks do. However since the wireless medium is less reliable, the quality of services is limited. The study looks at the following performance metrics.

1. Throughput

Throughput is one of the most important performance metrics in any network. It is defined as the number of bits that are successfully transmitted within a time interval divided by the time interval itself [3], [11]. As described in [3], this time interval in a WLAN is typically between the consecutive times the medium is idle for more than a DIFS period. Throughput is commonly measured in bits per seconds. The MAC protocol implementation tries to maximize this metric.

2. Delay

The MAC layer in every station has a queue to store packets received from the higher layer. Normally, the MAC layer transmits a packet immediately after receiving a packet. However, if a packet is being received from the physical layer, previous attempts to transmit the packet have failed, or the medium is being used, it will keep the packets from the higher layer in the queue. Delay is the time a packet spends in this queue until it is successfully transmitted [3], [11]. The delay is another important performance metric and the MAC protocol will try to minimize it.

3. Fairness

Fairness is yet another important characteristic for the MAC protocol. The protocol should not favor any particular station. All stations should evenly share the medium. In this study, all stations have the same user profile. Their performance should be very similar if the protocol is fair.

D. MULTIHOP MODEL

This model is for analyzing how well the protocol performs in multihop scenarios. The multihop environment is one of the characteristics of MANET. Consequently, the

MAC protocol should perform reasonably well in this environment. The throughput and delay are measured for a two-, three-, and five-hop environment.

A wireless router for this study is implemented using two OPNET *wireless_Ethernet_routers*. Connecting the Ethernet interface of these routers by a 10-Mbps link results in a node having two wireless interfaces and effectively functions as a wireless router. When two wireless interfaces belong to the same BSS, the access point functionality on one of these interfaces needs to be disabled. In this thesis, if it does not explicitly mention otherwise, a node is also a router. Figure 15 shows a three-hop network as an example of the network configuration for studying multihop effects.

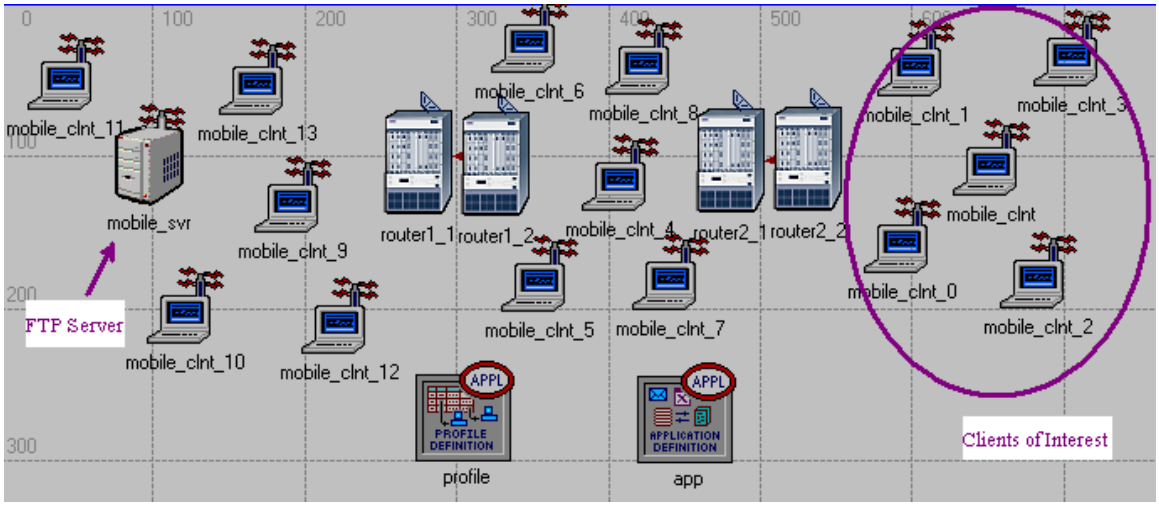

Figure 15. A Multihop Network Configuration

As shown in the figure, the server station (near the left edge) is placed so that it is far from clients of interest (near the right edge). Packets have to go through routers to get to client stations from the server. Since client stations on the far right are of interest, their performance is measured.

E. JAMMING MODEL

Jamming is a highly anticipated situation in the operational environment. JTRS considers it as a threat. Hence, examining its effects on performance of the IEEE 802.11 protocol is of interest. In this study, two radio physical layer, DSSS and FHSS, are used

to investigate effects of jamming on the MAC protocol performance. The IR physical layer, which is good for indoor LAN, is not used because its range is limited, 20 meters maximum.

The radio transceiver pipeline procedures can interact with all signals that are transmitted at the same time [9]. This consequently makes it possible for self-interference and jamming to be taken into account. Although the channel match stage distinguishes signals from noise, the received power computation of interference signals proceeds similar to that of actual data signals. Interference signals will eventually be dropped in later stages of the pipeline. This study uses a single band jamming model available in the OPNET model library. The jammer consists of a source to generate a packet and a radio transmitter to send a packet, operating at a single fixed frequency band. A packet is continuously transmitted once every second. A jamming scenario is laid out as shown in Figure 16. A jammer is placed in the transmitting range of all stations as if it were a regular station.

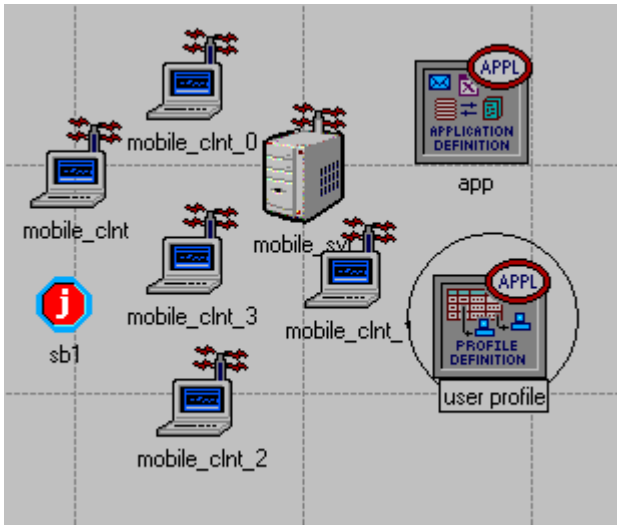

Figure 16. A Jamming Network Configuration

F. VELOCITY MODEL

Another desirable characteristic of the wireless network, especially in the operational environment is to have stations moving freely while communicating. This

model identifies the effect of mobility of a station on throughput and delay. Figure 17 shows a typical network configuration for studying the velocity effects. A station of interest moves "randomly" with the velocity of 5, 25, or 50 km/h. In this model, the motion of the node must be preprogrammed into OPNET with a specified trajectory, carrying it into and out of transmission range during the simulation. Thus the motion is not truly random. One of limitations in OPNET, the effects of Doppler are not a factor in any computation.

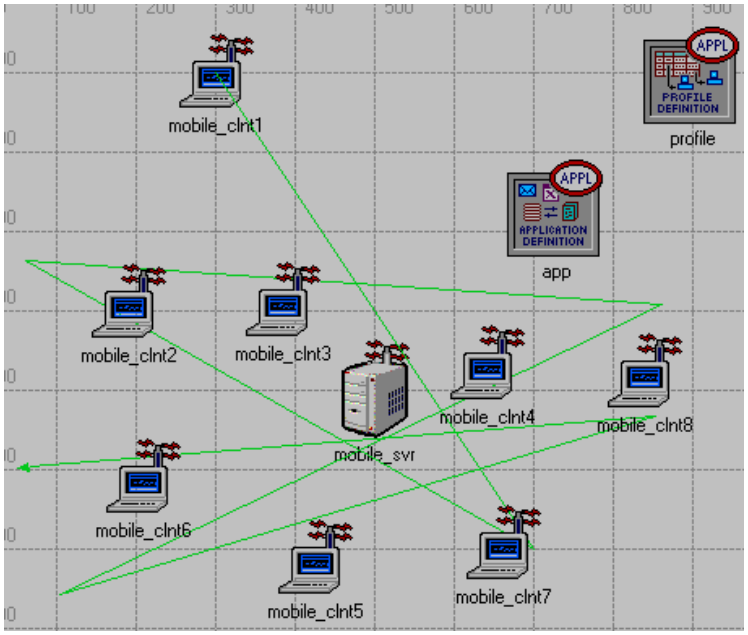

Figure 17. A Node-Velocity Network Configuration

G. SUMMARY

In this chapter, the OPNET model of the IEEE 802.11 MAC protocol is described. OPNET modeling and communication methods are explained. The chapter also includes a description of the simulation environment. The simulation results are presented and analyzed in Chapter IV.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SIMULATION RESULTS

This chapter presents and analyzes the OPNET simulation results of the three scenarios. Section A discusses the results of the effects of the multihop environment while Section B covers the results of jamming effects. Finally, Section C provides the results of the effects of node velocity.

A. MULTIHOP ENVIRONMENT RESULTS

This part of the study is to evaluate how the IEEE 802.11 MAC protocol performs in the multihop environment. Using two, three, or five hops, the average throughput and delay were measured and compared. The effects of the RTS mechanism and fragmentation in this environment were also studied.

1. Performance versus Number of Hops

This result, shown in Figure 18, was the average throughput of an FTP client station located in the last hop of three different network configurations. These three networks were configured in order that the client station of interest is two, three, and five hops away from the FTP server station. To focus on the effects of number of hops as much as possible, the RTS mechanism and fragmenation were not used. The effects of these mechanisms on the multihop environment will be discussed later.

As shown in Figure 18, the average throughput decreases when a packet must travel through other stations to get to its destination. The result shows that when comparing the two-hop with the five-hop scenario, the average throughput significantly decreased. For example, at the simulation time of 15 minutes, the throughput of two hops is approximately 102,000 bits per second (bps) and five hops is about 25 kbps. The throughput decreased by approximately 75%. The decrease in throughput was expected.

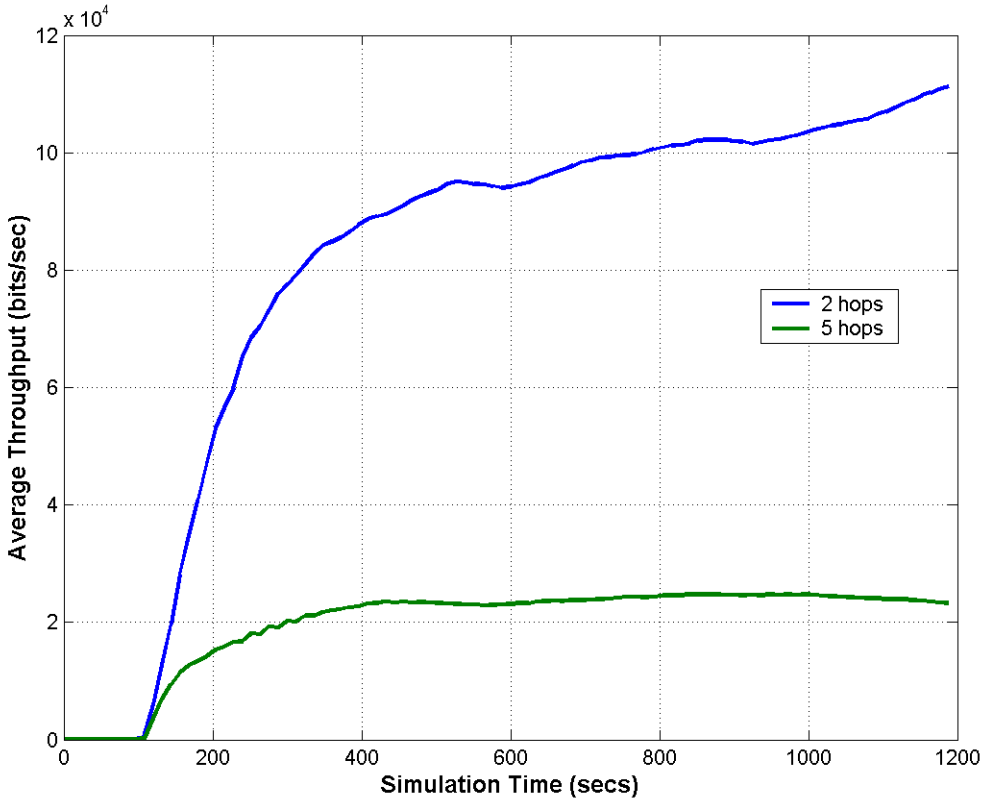

Figure 18. Average Throughput versus Number of Hops

The reason for this decrease could be explained by the following scenario. If it normally took t seconds to transfer a packet of length n bits from one wireless interface to the other, the five-hop configuration would take $10t$ seconds to send the packet and to receive another packet of the same length. In a two-hop scenario, this time would be $4t$ seconds. Therefore, the throughput deceased by 3/5. Other factors would affect the performance as well. For example, there were stations in between routers in the five-hop environment, which could have caused the throughput to drop since the routers might be busy communicating with these stations.

The average delay experienced by the same client station as above is shown in Figure 19. This plot is obtained by dividing the average end-to-end delay by the total number of packets received. The OPNET end-to-end delay computation provides some type of delay accumulation for all packets received during a specified time period (in

these simulations, 12 seconds). The delay provided by the simulation would be higher for stations that receive a greater number of packets in those 12 seconds: this means that stations with higher throughput (e.g., two hops away) would see a cumulative delay larger than a station with lower throughput (e.g., five hops), even though every additional hop would increase the end-to-end delay. This plot provides a normalized delay per packet, based on the cumulative delay provided by OPNET. The accuracy of the normalized technique may be doubtful but is presented for consistency in measuring important network performance parameters. The simulation results show that this client station experienced similar delay in these two scenarios.

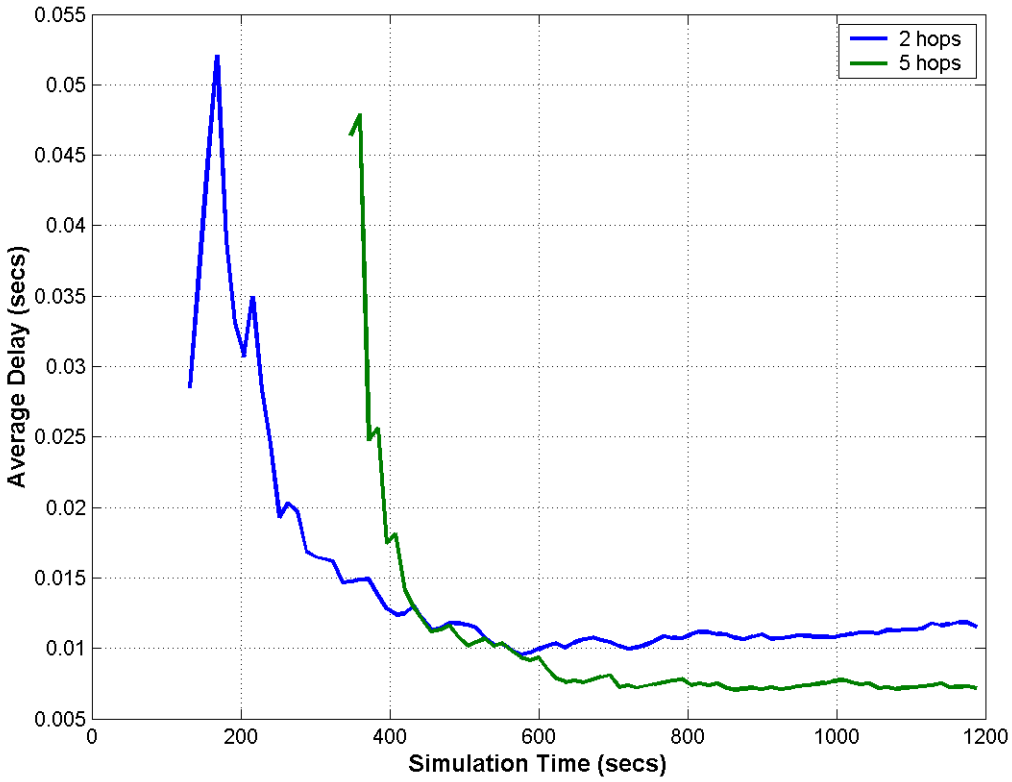

Figure 19. Average Delay versus Number of Hops

2. Fairness in Multihop Environment

Another important feature of a MAC protocol is that it distributes the medium access to all stations fairly. To investigate fairness of the IEEE 802.11 MAC protocol,

the average throughput results of client stations from different numbers of hops away are compared. These client stations were two, three, four, and five hops away from the server station. The results shown in Figure 20 were observed from the five-hop network. The throughputs of these stations were fairly close. This result demonstrates that the protocol is reasonably fair. These results are consistent with those obtained in the two-hop and three-hop scenarios: in all cases, station throughputs were roughly equal indicating the fairness of the protocol.

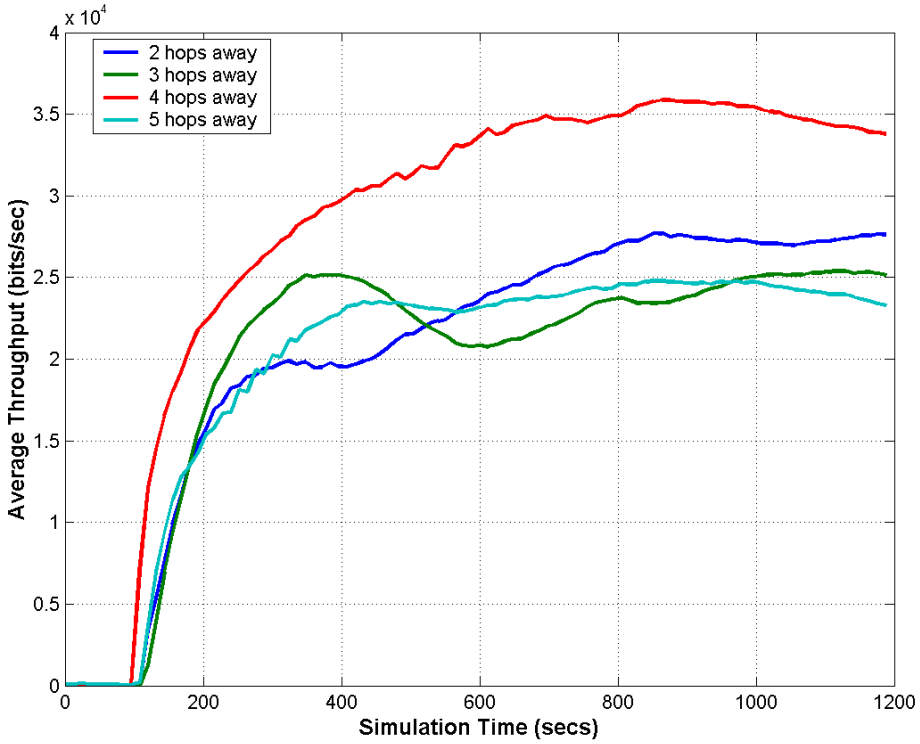

Figure 20. Average Throughput of Clients at Different Hop Locations

3. Effects of the RTS Mechanism in the Multihop Environment

This part of the study is to investigate how the RTS mechanism affects the protocol performance in the multihop environment. The mechanism assures the source that the destination is not communicating with other stations. Consequently, collisions can be avoided. The three-hop scenario experimented with three different values of RTS Threshold: 1, 500, and None. The threshold value of 1 always enables the RTS

mechanism. Regardless of the size of the MAC Protocol Data Unit (MPDU), the RTS handshake will always precede the data transfer. On the other hand, the threshold value of 'None' disables the RTS mechanism. With a threshold of 500 bytes, the handshake is used only when a packet size exceeds 500 bytes. Using a threshold value of 500 bytes is suggested by [12] to achieve reasonable performance when the mechanism is enabled.

Figures 21 and 22 show the average throughput and delay, respectively. As shown in Figure 21, when the RTS was always used, the average throughput was zero indicating that the communication was not possible. The possible cause of this might have come from the overhead of the RTS mechanism adding to the delay constraint of the FTP application. This may result in the FTP application attempting to retransmit the same frame over and over. However, when the threshold was set to 500, the average throughput was reasonable and slightly better than when the mechanism was disabled. When the RTS threshold of 500 was used or the mechanism was disabled, the average delays were also very close, as shown in Figure 22, and remain rather constant. The average delay was infinite when the mechanism was always enabled.

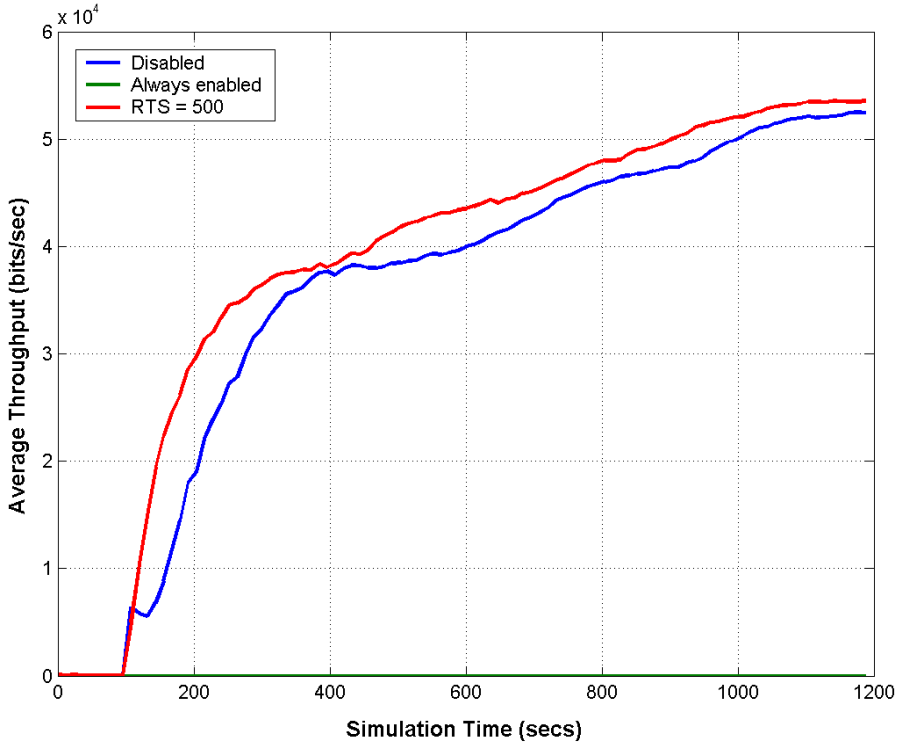

Figure 21. Average Throughput with RTS Mechanism

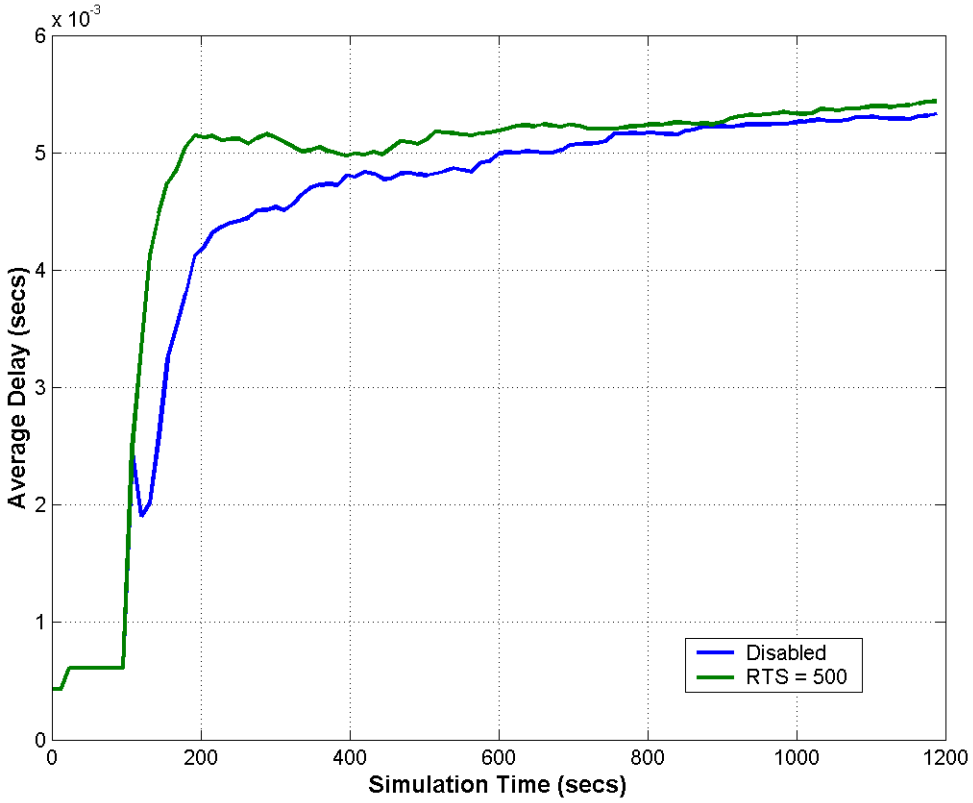

Figure 22. Average Delay with RTS Mechanism

As a result, the RTS handshake would help to improve the performance of the protocol in multihop environments if its threshold were approximately 500 bytes. A threshold of 300 bytes was also examined and found to have similar performance.

4. Effects of Fragmentation in the Multihop Environment

Using an RTS Threshold of 500, this section examines the effects of fragmentation in the multihop environment. Using an RTS threshold of 500 gave the highest average throughput among the previous study cases. The average throughput and delay are shown in Figure 23 and 24, respectively. With FTP traffic characteristics defined earlier, fragmenting and defragmenting a large packet did help to improve performance. The performance was even better with a higher fragmentation threshold. However, the improvement in throughput was approximately 10% with a threshold of 500 bytes and 20% with a threshold of 1,000 bytes. Additionally, there was a tradeoff in

using fragmentation since the network experienced greater delay. The average delay was increased by 20.75% for a threshold of 500 bytes, and increased by almost 38% with a threshold of 1,000 bytes.

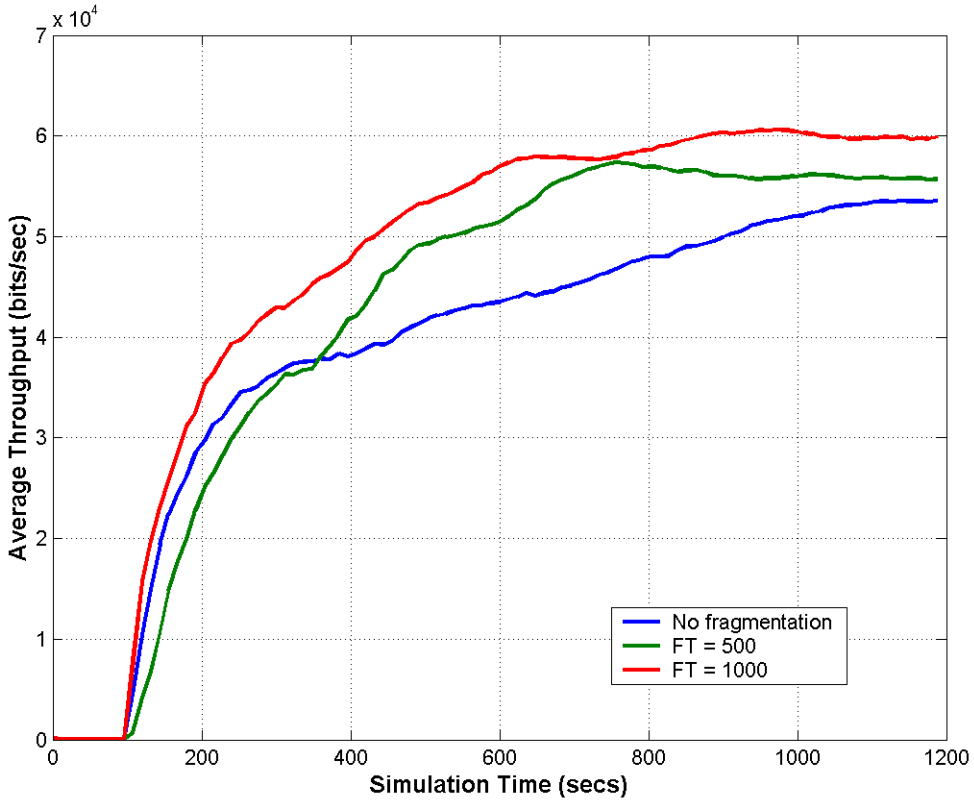

Figure 23. Average Throughput with Fragmentation

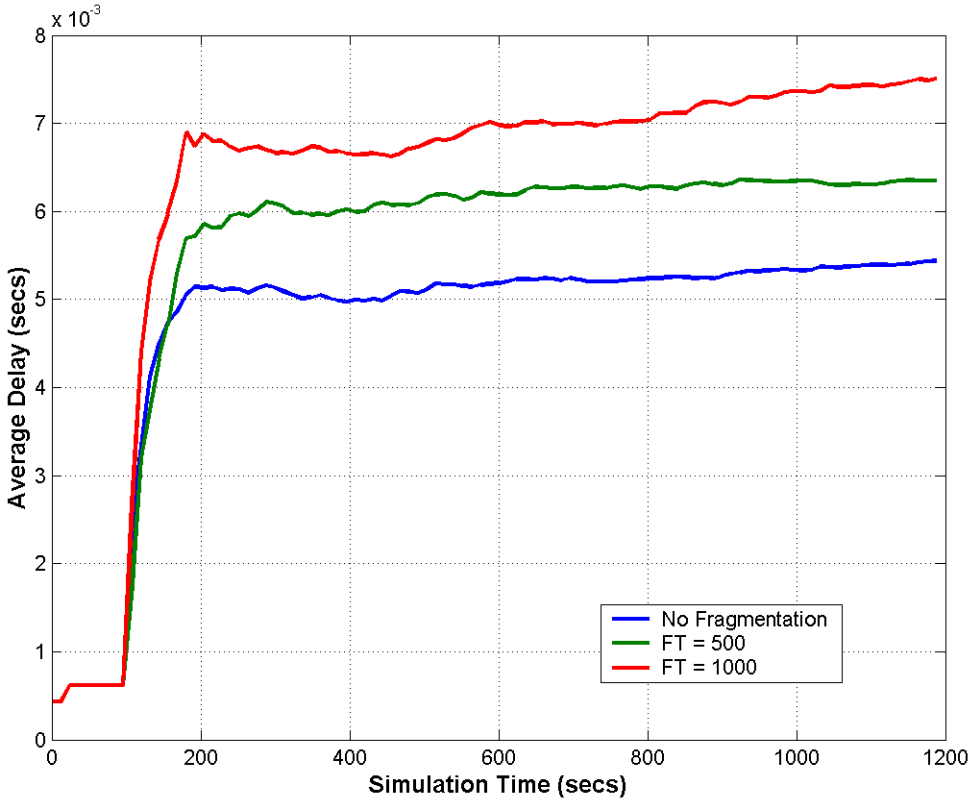

Figure 24. Average Delay with Fragmentation

B. JAMMING ENVIRONMENT RESULTS

This part of the study is to examine jamming effects on performance. Two radio physical layers specified in the standard are examined in the area of jamming. Moreover, effects of RTS and fragmentation mechanisms are also studied. The results are discussed below.

1. The Radio Physical Layers versus Jamming

Figure 25 shows the average throughput when two different radio physical layers, defined in the IEEE 802.11 standard, were used. In the presence of jamming, the results show that DSSS physical layer performed better than the FHSS physical layer. The DSSS average throughput was approximately 43% better than that of the FHSS physical layer. The figure shows that performance seemed to decrease as the simulation time elapsed. This may be partially affected by the fact that a file size decreases as the FTP

session is close to the end. As mentioned earlier this study uses one FTP session in order to focus more on data exchange. Moreover, the FHSS-based network experienced more delay than the DSSS-based networks, as is evident in Figure 26: approximately 20% more.

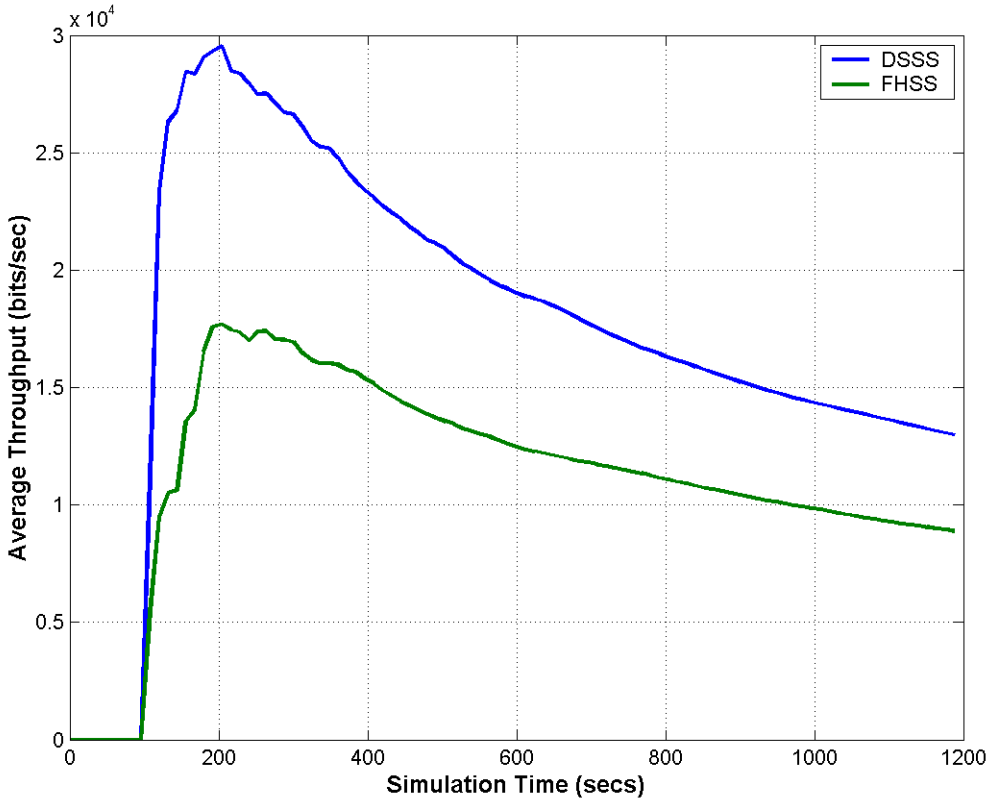

Figure 25. Average Throughput in Jamming

According to results, the DSSS is the best physical layer among the two when jamming occurs. However, since the WLAN model does not yet implement the real physical specifications in the IEEE 802.11 standard, these physical characteristics are only for specifying a slot time, SIFS, maximum and minimum contention window sizes of the corresponding physical layer. These results might not reflect the performance of the actual physical layer, specified in the standard.

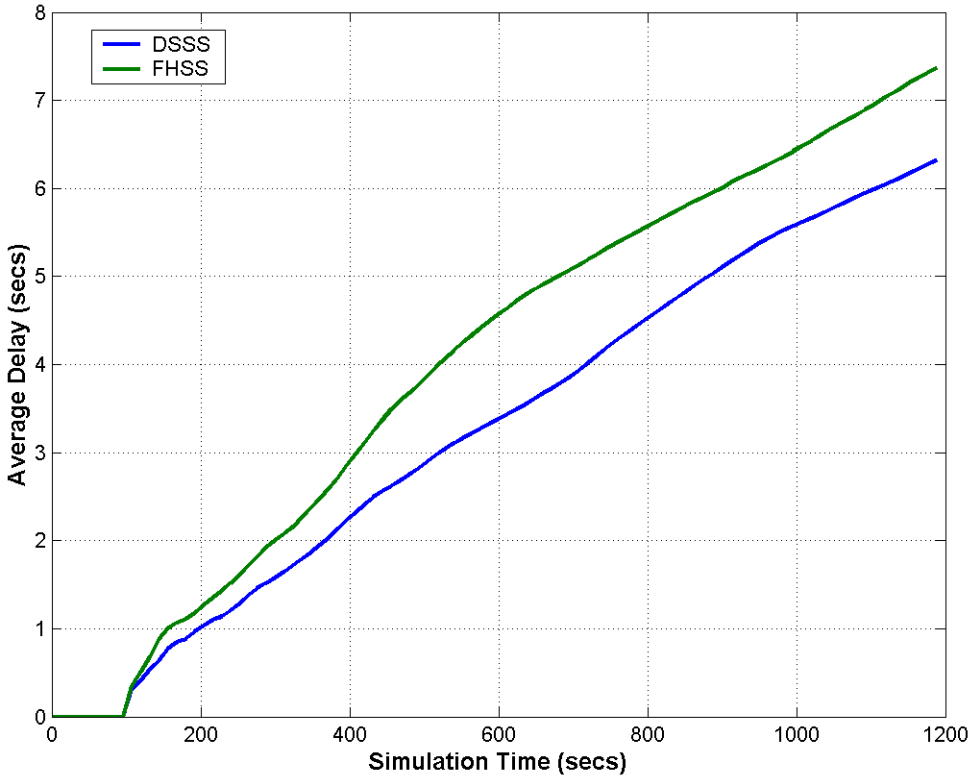

Figure 26. Average Delay in Jamming

2. Effects of the RTS Mechanism in a Jamming Environment

To investigate the effects of the RTS mechanism when jamming is present, this part of the study used a DSSS physical layer characteristics with three different values for the RTS threshold: 1 byte (mechanism always enabled), 500 bytes, and 'None' (mechanism disabled). In the presence of jamming, the RTS mechanism, to some extent, helped to improve performance when the RTS threshold was set to 500 bytes, as shown in Figure 27. This improvement was approximately 6.25%. However, when the mechanism is always enabled, the performance significantly decreases, i.e., almost 18.75% average throughput degradation, compared with when the mechanism is disabled, which is clearly shown in this figure.

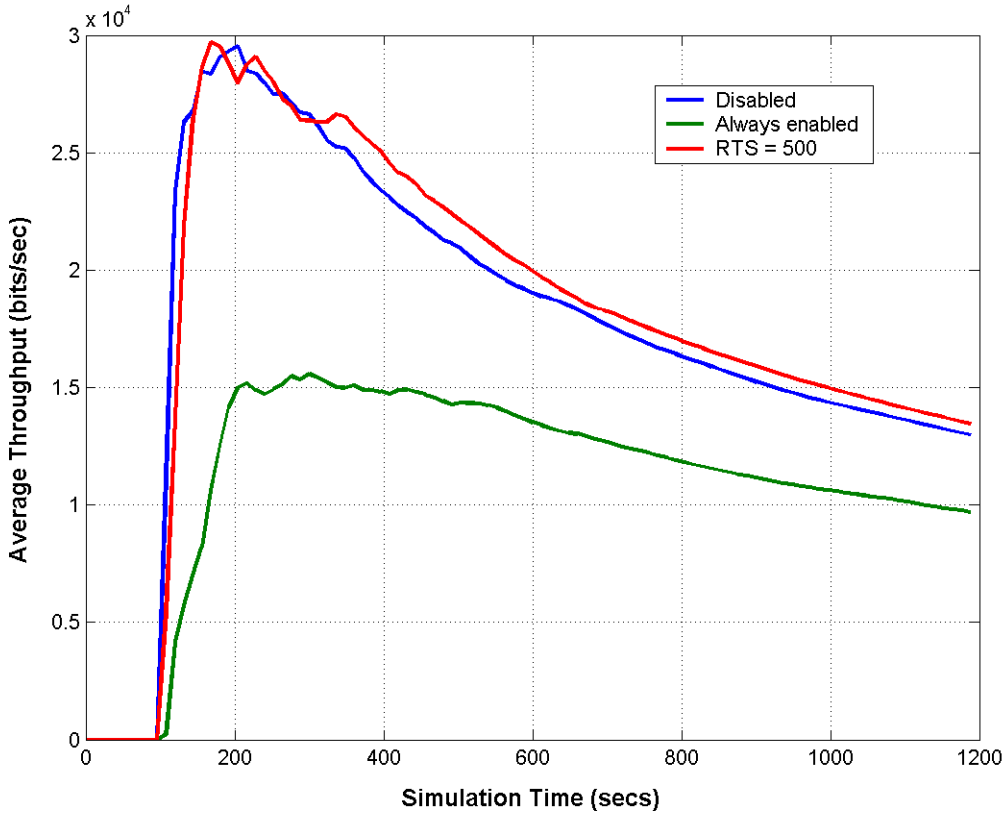

Figure 27. Average Throughput in Jamming with RTS Mechanism

The delays experienced by networks with these RTS thresholds were not significantly different. As shown in Figure 28, when the RTS mechanism was always enabled, the delay was slightly higher than when the mechanism was disabled. The client station experienced less delay when the RTS threshold was set to 500 bytes. Notice, however, that when the RTS mechanism was always enabled, the performance visibly degraded: that is, lower throughput with greater delay. Figure 27 also showed that the throughputs decreased as the simulation time elapsed. This resulted from the increase in delays in Figure 28.

As a result, the RTS mechanism would provide a marginal improvement in performance if its threshold were set to 500 bytes or more. The threshold of 300 bytes was also examined and found to have approximately similar performance.

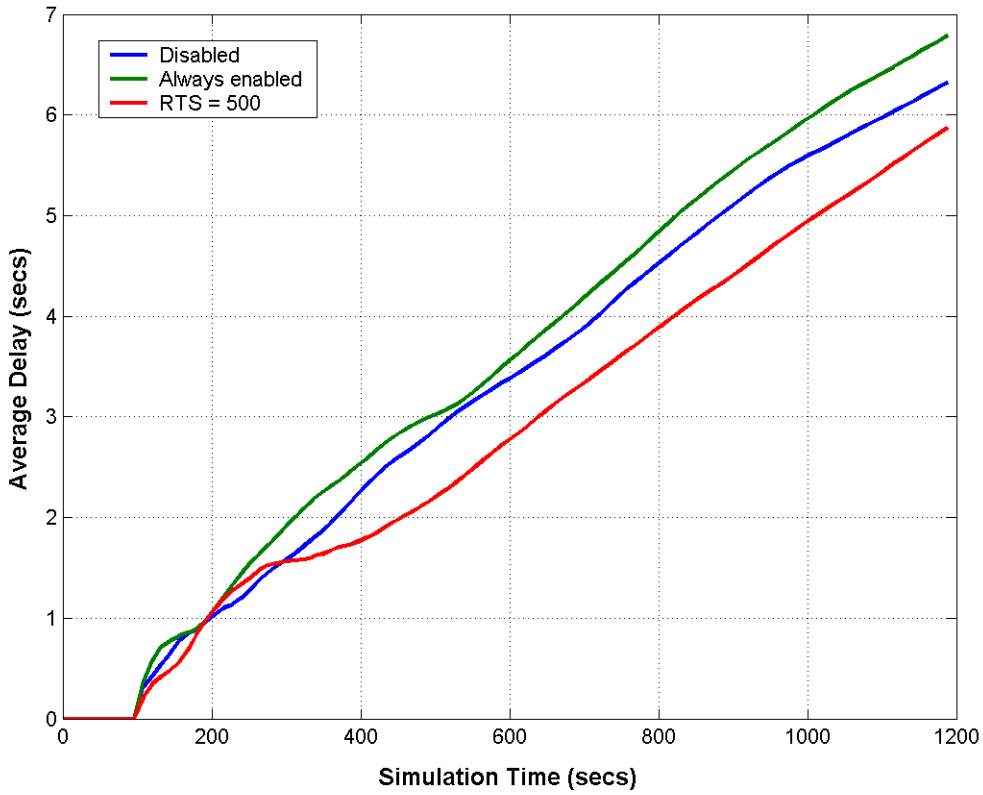

Figure 28. Average Delay in Jamming with RTS Mechanism

3. Effects of Fragmentation in a Jamming Environment

Fragmenting and defragmenting a packet may also affect performance when jamming is present. Taking fragmentation into account, this part of the study enabled fragmentation and varied its threshold: 500 and 1000 bytes. The RTS mechanism was also enabled by using an RTS threshold of 500 bytes, which gave the highest throughput in the previous setting. The average throughput shown in Figure 29 indicates that fragmentation did not improve performance at all. On the contrary, the fragmentation dramatically deceased the throughput, regardless of what the threshold value was. The decrease was approximately 50%. This might be explained as follows: since all fragments of a particular frame must be sent in one fragmentation burst, jamming might prohibit more fragmentation bursts to occur.

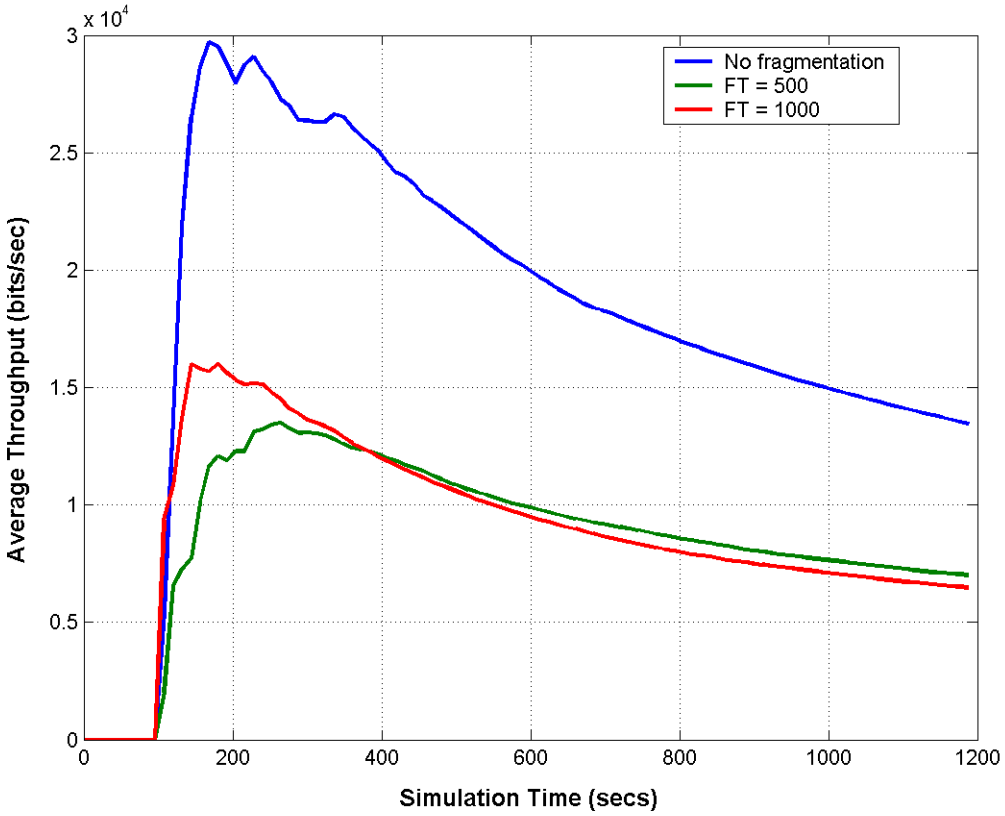

Figure 29. Average Throughput in Jamming with Fragmentation

Fragmentation also increased delay. With a higher fragmentation threshold, a node experienced even more delay, as shown in Figure 30. For example, at the simulation time of 15 minutes, the delay for an FT of 500 bytes was approximately 10.10 seconds, and 7.55 seconds for an FT of 1000. The delay when there was no fragmentation was around 2.90 seconds. Consequently, fragmentation should be disabled in jamming environment.

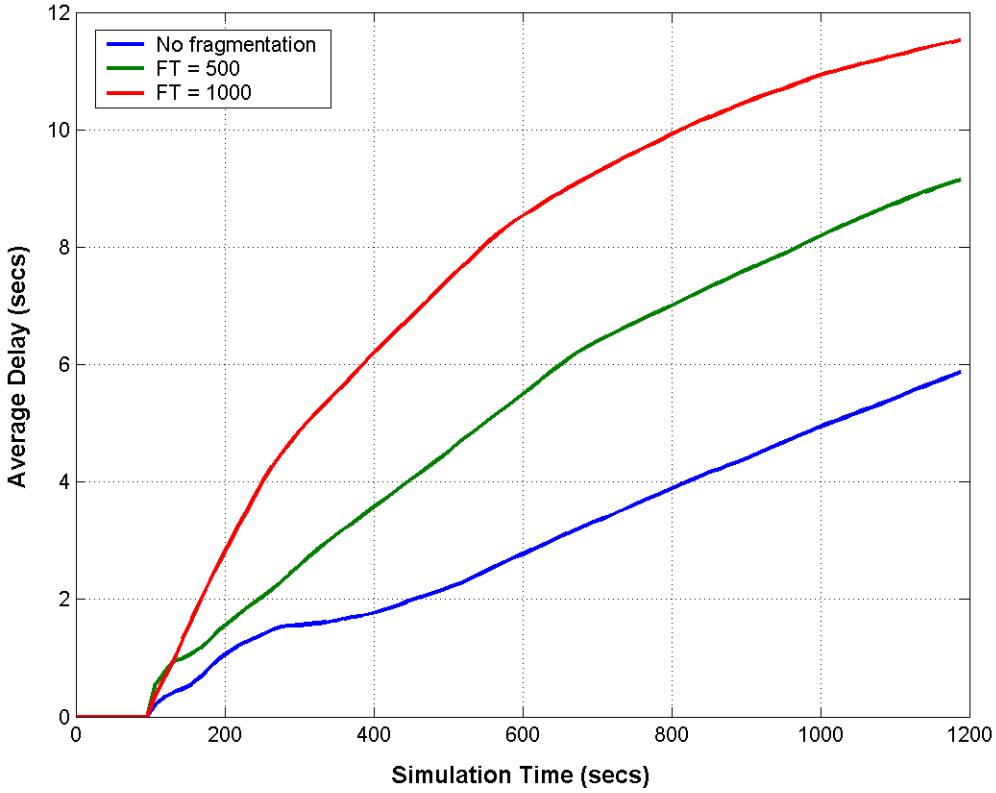

Figure 30. Average Delay in Jamming with Fragmentation

C. VELOCITY ENVIRONMENT RESULTS

This part of the study investigated the effects of node velocity on performance. These scenarios consisted of a stationary FTP server, one mobile client and several stationary clients. The mobile client station was moving in a randomly created trajectory with velocities of 5, 25, or 50 km/h, in and out of transmission range of the FTP server. These results were also compared with that of a stationary node.

Figures 31 and 32 show the average throughput and delay, respectively. As expected, the throughput decreased as the node velocity increased. Higher node velocities also experienced more delay. The throughput was considerably decreased when comparing the throughput of stationary node to that of the node with velocity of 5 km/h. The decrease was almost 52%. Furthermore, the node with velocity of 5 km/h endured twice the delay of a stationary node. On the other hand, both throughput and

delay of the station with node velocities of 25 and 50 km/h were not very different. This shows that although the performance might degrade dramatically when stations were moving, the protocol still performed reasonably well when node velocities were increased. Nonetheless, their average throughput was approximately 36% less than that of a 5 km/h station with an almost 47% increase in delay. The decrease in throughput was expected and agreed with the study in [6].

Therefore, though the node velocity substantially decreased the performance, higher velocities did not further affect it. As evidenced in Figures 31 and 32, the station with velocity of 50 km/h performed about as well as the station with velocity of 25 km/h.

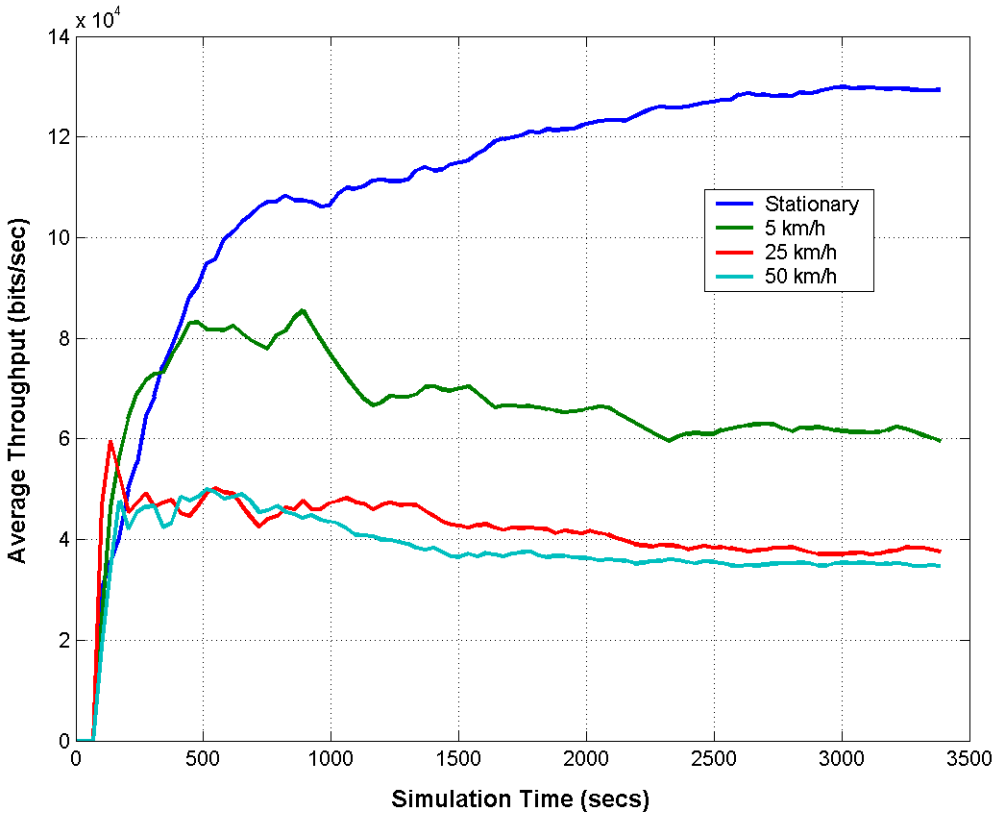

Figure 31. Average Throughput with Different Node Velocities

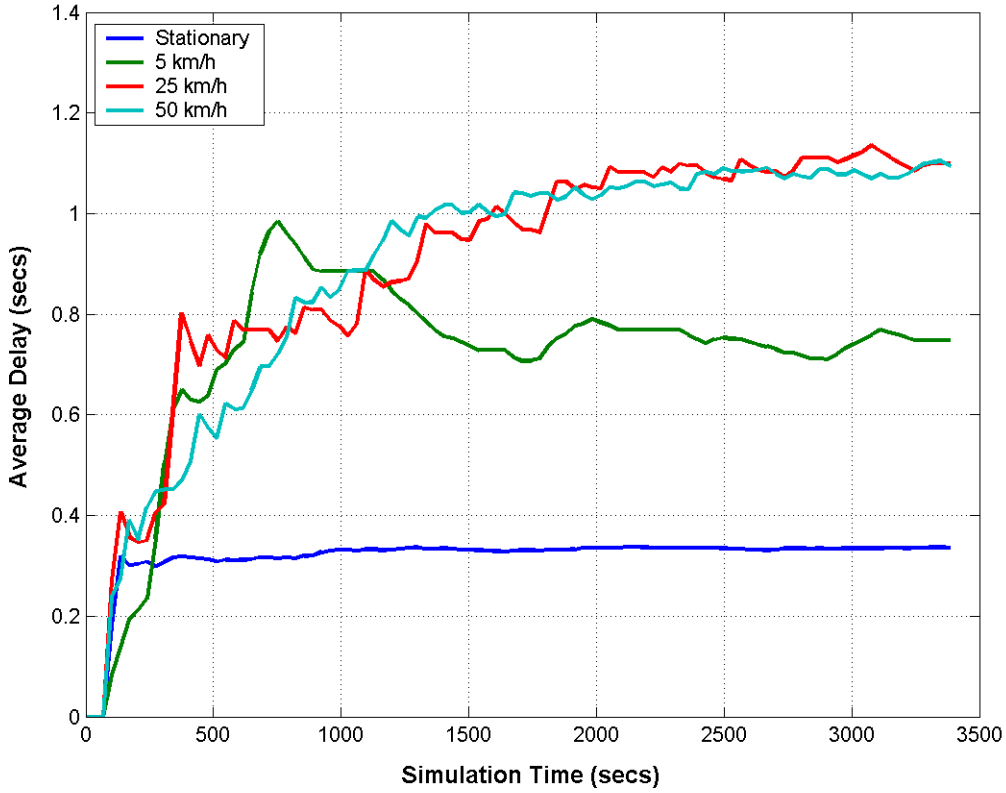

Figure 32. Average Delay with Different Node Velocities

D. SUMMARY

This chapter presented the simulation results obtained to evaluate the performance of the IEEE 802.11 MAC protocol in operational environments. Specifically, the protocol was tested by measuring throughput, delay and fairness over varying number of hops, in the presence of jamming and with varying node velocity. The use of the RTS/CTS handshake and fragmentation was evaluated in these scenarios. Chapter V summarizes the conclusions and suggests follow-on research areas.

V. CONCLUSIONS AND RECOMMENDATIONS

The objective of this thesis was to evaluate the IEEE 802.11 MAC protocol in an operational environment. To accomplish this, the OPNET simulation tool was used to create wireless networks. In OPNET, network parameters were varied and simulations run to collect data on network throughput, delay and fairness in multihop, jamming and high mobility environments.

A. CONCLUSIONS

In the multihop environments, the results showed that the performance decreased as the number of hops increased, as expected. This degradation in the performance of the three-hop from the two-hop network was more than twice the degradation of the five-hop from the three-hop network. Specifically, the average throughput went down by almost 54% when comparing the result of the three-hop to that of the two-hop networks. The average throughput of the five-hop network dropped by approximately 75% from that of the two-hop network. The protocol was found to be reasonably fair in that the average throughput of most client stations with different number of hops away from the server station were comparable. The RTS mechanism and fragmentation also increased the performance of the protocol in this environment. The RTS threshold of 500 bytes or more was found to slightly improve the performance. The fragmentation threshold between 500 and 1000 bytes could further improve the performance.

In the present of jamming, the simulation results showed that the DSSS physical layer performed noticeably better than the FHSS physical layer. Specifically, the average throughput using the DSSS physical layer was approximately 43% better. In jamming, the RTS mechanism helped improve the performance to some extent if its threshold was 500 bytes or more. On the other hand, fragmentation considerably decreased the performance in this kind of network environment.

As the node velocity increases, the performance decreases. As the simulation results revealed, the average throughput went down about 52% when the node velocity changed from stationary to 5 km/h. However, the degradation is smaller when the

velocity increases further: the results showed that the average throughputs of node velocities of 25 km/h and 50 km/h were very close.

B. RECOMMENDATIONS

This simulation study was based on the MAC protocol model available in OPNET network simulation software. The model has omitted or simplified parts of the specification [9]. Moreover, there are also some aspects of the standard in a MANET environment that should still be evaluated. Specifically, this study would suggest the following be explored.

Since OPNET WLAN model has not yet simulated the actual physical layer specifications in the IEEE 802.11 standard, it would be interesting to investigate the protocol performance in these three network environments: the DSSS, FHSS, and IR physical layers should be implemented and their specifications should be met. Although the main point is to evaluate the MAC protocol, more realistic results would be obtained if the evaluation were carried out with the actual physical layer. Furthermore, a mobile station that functions as a node and router would be desirable so that they can route packets as well. This can be achieved by implementing a station with two wireless interfaces. This research studied the effects of node velocity in a single-hop environment. A more in-depth study involving true random node motion and velocity in a multihop environment would be desirable.

To simulate an even more realistic operation environment, a combination of these environments could create some interesting network configurations. The network would consist of multihop, nodes with random motion, and a number of jammers. Node altitude and three-dimensional movement should also be taken into account. This scenario would require stations to move to different BSSs. Handoff mechanisms would be a necessary and very important feature to study as well. Moreover, effects of the RTS mechanism and fragmentation should also be further evaluated under these conditions.

LIST OF REFERENCES

1. Vaidya, Nitin H., "Mobile Ad Hoc Networks: Routing, MAC and Transport Issues", MobiComm 2001 Tutorial, Rome, IT, pp. 1-431, July 2001.

2. Operational Requirements Document (ORD) for Joint Tactical Radio System (JTRS), JTRS Joint Program Office, 23 March 1998.

3. Chhaya, H. S. and Gupta, S., "Performance modeling of asynchronous data transfer methods of IEEE 802.11 MAC protocol," *Wireless Networks*, Vol. 3, pp. 217-234, 1997.

4. O'Hara, B. and Petrick, A., *The IEEE 802.11 Handbook: A Designer's Companion*, IEEE Press, 1999.

5. Xu, S. and Saadawi, T., "Does the IEEE 802.11 MAC Protocol Work Well in Multihop Wireless Ad Hoc Networks?," *IEEE Communications Magazine*, Vol. 39, Issue 6, pp. 130-137, 2001.

6. Khuruna, S., Kahol, A., Gupta, S.K.S., and Srimani, P.K., "Performance Evaluation of Distributed Co-Ordination Function for IEEE 802.11 Wireless LAN Protocol in Presence of Mobile and Hidden Terminals," *Proc. of 7th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems*, 1999, pp. 40-47.

7. Crow, B. P., Widjaja, I., Kim, L. G., and Sakai, P. T. "IEEE 802.11 Wireless Local Area Networks," *IEEE Communications Magazine*, Vol. 35, Issue 9, pp. 116-126, 1997.

8. The Institute of Electrical and Electronics Engineers, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 20 August 1999.

9. OPNET Modeler Version 8.0 Online Documentation, OPNET Technologies, Inc.

10. Jabbari, B., Lecture notes for ECE 642 (Internet Traffic Modeling), George Mason University, http://cnl.gmu.edu/bjabbari.

11. Gummalla, A. C. V. and Limb, J. O., "Wireless medium access control protocols," *IEEE Communications Surveys*, Vol. 3, No. 2, pp. 2-15, 2000.

12. Crow, B. P., Widjaja, I., Kim, L. G., and Sakai, P. T. “IEEE 802.11 Wireless Local Area Networks,” *Proc. of INFOCOM’97 Sixteenth Annual Joint Conference of the IEEE Computer and Communication Societies*, Vol. 1, 1997, pp. 126-133.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Chairman, Code IS
   Information Science Department
   Naval Postgraduate School
   Monterey, California

3. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

4. Dr. Robert Ives, Code EC/Ir
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California 93943-5121

5. Dr. Murali Tummala, Code EC/Tm
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California 93943-5121

6. Dr. Rich C. North, Code D855
   Spawar Systems Center
   53560 Hull Street
   San Diego, CA 92152

7. Ens. Kacha Jitpanya
   Royal Thai Navy
   Ministry of Defense
   Thailand