THROUGHPUT ANALYSIS OF WIRELESS MESH NETWORK

By

NURUL SUHAIZA ZULKIFLI

FINAL REPORT

Submitted to the Electrical & Electronics Engineering Programme
in Partial Fulfillment of the Requirements
for the Degree
Bachelor of Engineering (Hons)
(Electrical & Electronics Engineering)

Universiti Teknologi Petronas
Bandar Seri Iskandar
31750 Tronoh
Perak Darul Ridzuan

CERTIFICATION OF APPROVAL

THROUGHPUT ANALYSIS OF
WIRELESS MESH NETWORK

by

Nurul Suhaiza Zulkifli

A project dissertation submitted to the
Electrical & Electronics Engineering Programme
Universiti Teknologi PETRONAS
in partial fulfilment of the requirement for the
Bachelor of Engineering (Hons)
(Electrical & Electronics Engineering)

Approved:

____

Mr. Azlan Awang
Project Supervisor

UNIVERSITI TEKNOLOGI PETRONAS
TRONOH, PERAK

June 2007

CERTIFICATION OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this project, that the original work is my own except as specified in the references and acknowledgements, and that the original work contained herein have not been undertaken or done by unspecified sources or persons.

Nurul Suhaiza Zulkifli

ABSTRACT

Wireless Mesh Network (WMN) is a combination of both wireless and ad hoc technologies, thus having the advantages of low cost, reliability and scalability. It is indeed becoming an appealing choice for the construction of community network to extend internet services. However, these potentials can not be realized without a proper study on the performance of WMN in different setups and situations. The throughput may vary from a single node pair to multiple node pairs and chain links. Thus this project aims to analyze the throughput of different WMN setups and hopefully will provide some insights to the behavior of WMN. This project is divided into two parts. The first part of the project is to understand the theory behind the WMN technology, its advantages over existing technologies and explore how some of the networking protocols operate in a working environment. The second part of the project is concentrated on simulating the network using OPNET. The results show that WMN with constant traffic has higher throughput than exponential traffic in high traffic cases, while exponential traffic causes the network throughput to decrease after a maximum acceptable traffic size. As for the multiple senders to multiple receivers case, it definitely has higher throughput than a single sender-receiver within the same area.

ACKNOWLEDGEMENTS

First of all, I would like to thank my supervisor Mr. Azlan Awang who has given me insightful guidance, valuable suggestions, and timely encouragements in completing the project. My personal thanks are also dedicated to all the technicians and lecturers of the Electrical and Electronics department, for their continuous support during the period of my research. Also, my sincere appreciation to all my friends who have always been there for me during the good times and even more, the rough times. Last but not least, I would like to express my deepest gratitude to my parents for sharing all my pain and joy, for encouraging and supporting me all the time. This project would not have carried out smoothly without their wishes and blessings. I hope that with all the effort I have put on the project will eventually bring benefits to the society in some ways.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

CTS	Clear To Send
EIRP	Effective Isotropic Radiated Power
FCC	Federal Communications Commission
IEEE	Institute of Electrical and Electronics Engineers
MAC	Media Access Control
MANET	Mobile Ad Hoc Network
RTS	Request To Send
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network

CHAPTER 1
INTRODUCTION

1.1 Background of Study

Mobile ad hoc networks (MANETs) have wide applications in many situations wherever wireless communication and networking are preferred for convenience and/or low cost, such as wireless mesh networks (WMNs) and sensor networks. MANET consists of wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary network topologies, allowing people and devices to seamlessly inter-network in areas with no preexisting communication infrastructure [1]. The salient feature of this breed of networks is that they can operate in different propagations and network operating conditions, which cannot be predicted during the network design stage. Such a self-organizing and rapidly deployable network permits a new paradigm of wireless wearable devices that would immediately and easily enable instantaneous person-to-person, person-to-machine, or machine-to-person communications.

Such perceived versatility elicited immediate interest in the early days among military, police, and rescue agencies. Soldiers equipped with multimode mobile communicators can now communicate in an ad hoc manner, without the need for fixed wireless base stations. In addition, small vehicular devices equipped with audio sensors and cameras can be deployed at targeted regions to collect important location and environmental information that will be communicated back to a processing node via ad hoc mobile communications. Moreover, ad hoc mobile communication is particularly useful in relaying information (status, situation awareness, and the like) via data, video and/or voice from one rescue team member to another over a small handheld or wearable wireless device.

Recently, home or small office networking and collaborative computing with laptop computers in a small area have emerged as alternative areas of application. People in a meeting or a conference can freely use their laptops, or PDAs, to have instant network formation in addition to file and information sharing without the presence of fixed base stations and system administrators. For this reason, WMNs are becoming a popular alternative in extending WLANs. The mesh structure represents a multidrop system in which nodes assist other nodes in transmitting packets through the network. Each node functions as a router, relaying packets for its neighbors. Through the relay process, a packet will be forwarded through intermediate nodes to its destination.

Interestingly, the field of ad hoc mobile networks is rapidly growing and changing, and while there are still many challenges that need to be met, it is likely that such networks will see widespread use in the near future.

1.2 Problem Statement

Wireless Mesh Network is a combination of both wireless and ad hoc technologies, thus having the advantages of low cost, reliability and scalability. It is indeed becoming an appealing choice for the construction of community network to extend internet services. However, these potentials can not be realized without a proper study on the performance of WMN in different setups and situations. The throughput may vary from a single node pair to multiple node pairs and chain links. Thus this project aims to analyze the throughput of different WMN setups and hopefully will provide some insights to the behavior of WMNs.

1.3 Objectives and Scope of Study

1.3.1 Objectives

The objective of this project is to study the performance of WMN in terms of throughput. Various setups of WMN will produce different values of throughput. From the analysis, the different characteristics of the setups can be revealed.

1.3.2 Scope of Work

The scope of this project:

- Study on wireless technology generally, and WMN specifically.
- Simulations of WMN in different setups.
  - One sender to one receiver
  - Multiple senders to multiple senders
  - Nodes in chain
- Analysis of results gained from the simulations.

1.3.3 Feasibility of Project within the Scope and Timeframe

The project is conducted within the timeframe of two semesters, which is about one year. The first part of the project is focused on the research of Wireless Mesh Network, its fundamental concept and related issues . The second part of the project will be dedicated to creating the network simulation using a network simulation tool called OPNET.

CHAPTER 2
LITERATURE REVIEW / THEORY

2.1 Wireless Mesh Networks (WMNs)

A WMN is a self-configuring network of nodes interconnected (possibly using multiple radio technologies/interfaces [2]) using wireless links. WMNs represent the logical extension of WLANs, providing high-speed seamless connectivity to nomadic and mobile users. On the other hand, mesh networks inherit some features from the ad hoc networks field. In particular, WMNs use multi-hopping to transmit packets from the end user to the Internet gateway and vice versa, and are characterized by self-organization and self-healing capabilities, a key factor for enabling a rapid, effective and low-cost deployment. WMNs differ from ad hoc networks for both the goal (WMNs are mostly intended as access networks to Internet gateways) and the devices heterogeneity.

Nodes in a WMN can play two different logical roles, i.e., mesh clients and mesh routers [3]. Mesh clients can be the source/destination of connections, while mesh routers are in charge of forwarding packets to and from the Internet. A single node can play both roles at the same time, as in standard ad hoc networking paradigms [4]. Multi-tier architectures can be envisaged [2], with mesh routers providing multi-hop backhaul connectivity to the Internet, while the clients act just as sources/destinations of Internet connections. Actually, these architectures provide more flexibility to system designers, in that powerful dedicated devices with specific features (e.g., multi-radio interfaces) can be used to perform packet forwarding, thus enhancing network performance. Mesh architectures can therefore be thought as a generalization of standard WLANs, where hotspots are wirelessly interconnected and multi-hop routing is exploited in order to extended both network coverage and reliability. The latter option applies usually to metropolitan-scale area networks, but we can also think of WMNs as extensions of standard indoor WLANs, where extended coverage can be obtained by allowing multi-hop communications by store-and-forward operations.

WMN architectures can be classified into three types:

- Infrastructure WMNs
- Client WMNs
- Hybrid WMNs

2.1.1 Infrastructure WMNs

In infrastructure WMNs, wireless routers act as a self-configuring and self-healing mesh backbone, providing the clients with the opportunity to connect to a remote Internet gateway. Examples of such architecture include the MIT's Roofnet [5] and the commercial LocustWorld [6] deployments.

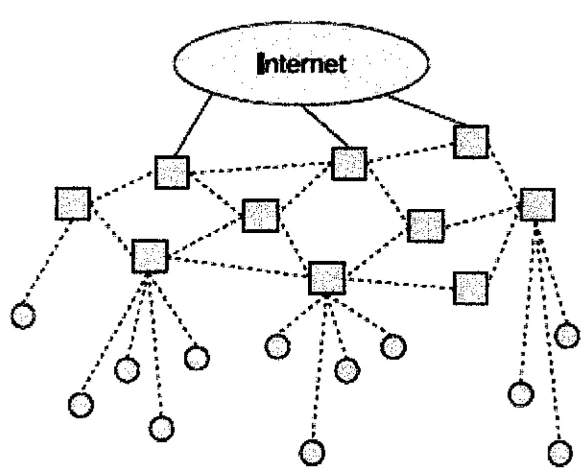

Figure 1 Infrastructure WMNs

2.1.2 Client WMNs

In client WMNs, client nodes organize themselves into a flat architecture for providing Internet access by means of store-and-forward operations. This solution adapts well to extensions of indoor WLANs. On the other hand, it is not suitable for metropolitan-level networks due to the obvious scalability problems. The Microsoft's

Mesh Connectivity Layer [7] falls into this category.

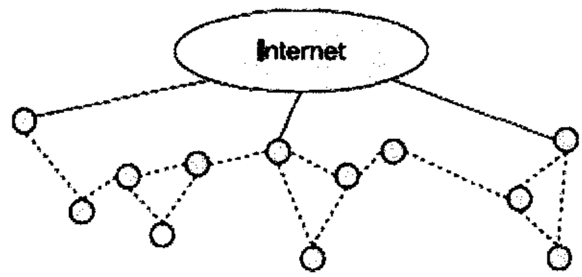

Figure 2 Client WMNs

2.1.3 Hybrid WMNs

Hybrid WMNs represent the combination of the two afore-mentioned solutions, as can be seen in Figure 3. In this scenario, a hierarchy with dedicated mesh routers, is present, but at the same time client-to-client communications are enabled in order to extend the coverage and robustness of the single "cells".

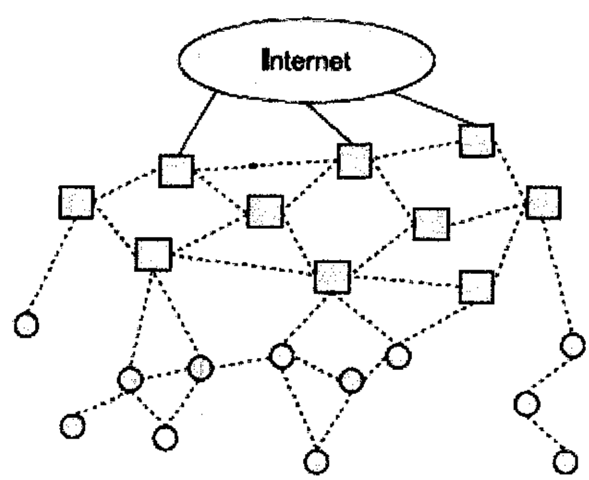

Figure 3 Hybrid WMNs

2.2 Advantages of WMNs

There are many reasons to consider the use of a WMN. Table 1 below summarizes the most common advantages as well as disadvantages associated with the use of a WMN.

Table 1 Advantages and disadvantages of a WMN

Advantages	Disadvantages
Reliability	Lack of standards
Self-Configuration	Security
Self-Healing	Overhead
Scalability	
Economics	

2.2.1 Reliability

In a WMN, each node functions as a relay to move packets toward their ultimate destination. Because nodes can enter and leave the mesh, each node must be capable of dynamically changing its forwarding pattern based upon its neighboring nodes. Thus, the mesh topology enhances reliability because the failure of one link due to RF interference, or the movement of a node between source and destination, will result in packets being forwarded via an alternative link toward their destination.

2.2.2 Self-Configuration

There is no need to configure each node in a mesh network since nodes learn their neighbors and paths to other nodes. Thus, the self-configuration capability of nodes can considerably reduce the need for network administration.

2.2.3 Self-Healing

Nodes in a wireless mesh network dynamically learn their neighbors as well as links to other nodes. Therefore, there is automatic compensation for the failure or removal of a node. Whenever a transmission impairment happens, which affects the use of a link or the failure of a node, other nodes establish alternate paths. The establishment of alternative path results in a self-healing capability.

2.2.4 Scalability

As mentioned before, nodes can enter and exit a mesh network as long as they operate software compatible with other nodes in the network. This means that we can extend the area of coverage of a WMN by simply placing new nodes at appropriate locations where they can communicate with existing network nodes. Thus, a WMN is scalable.

2.2.5 Economics

Since a WMN does not require centralized administration nor do nodes require manual configuration, such networks are less expensive to set up and operate than conventional networks. Similarly, the ability of wireless mesh networks to automatically resolve link and node outage problem via their self-healing capability eliminates the necessity for manual intervention when things go wrong.

2.3 Disadvantages of WMNs

As can be seen in Table 1, there are a few disadvantages associated with WMNs.

2.3.1 Lack of standards

Currently, organizations are in the process of developing wireless mesh networking standards. This has caused the lack of interoperability between different vendors because there are no existing standards with which vendors can tailor their products to comply.

2.3.2 Security

Because nodes within a WMN function as routers relaying packets to other nodes, security is an important issue. Thus a method of authentication of nodes is required in addition to securing the flow of data through nodes.

2.3.3 Overhead

As nodes must learn their neighbors as well as paths to other nodes, they must create and maintain routing tables. As network traffic and the number of nodes in the network increases, so will the amount of processing devoted to routing packets. Thus, the efficiency of routing mechanism as well as the number of nodes and level of network traffic results in processor overhead that can adversely affect the performance of the node to perform other tasks.

CHAPTER 3
METHODOLOGY / PROJECT WORK

3.1 Procedure Identification

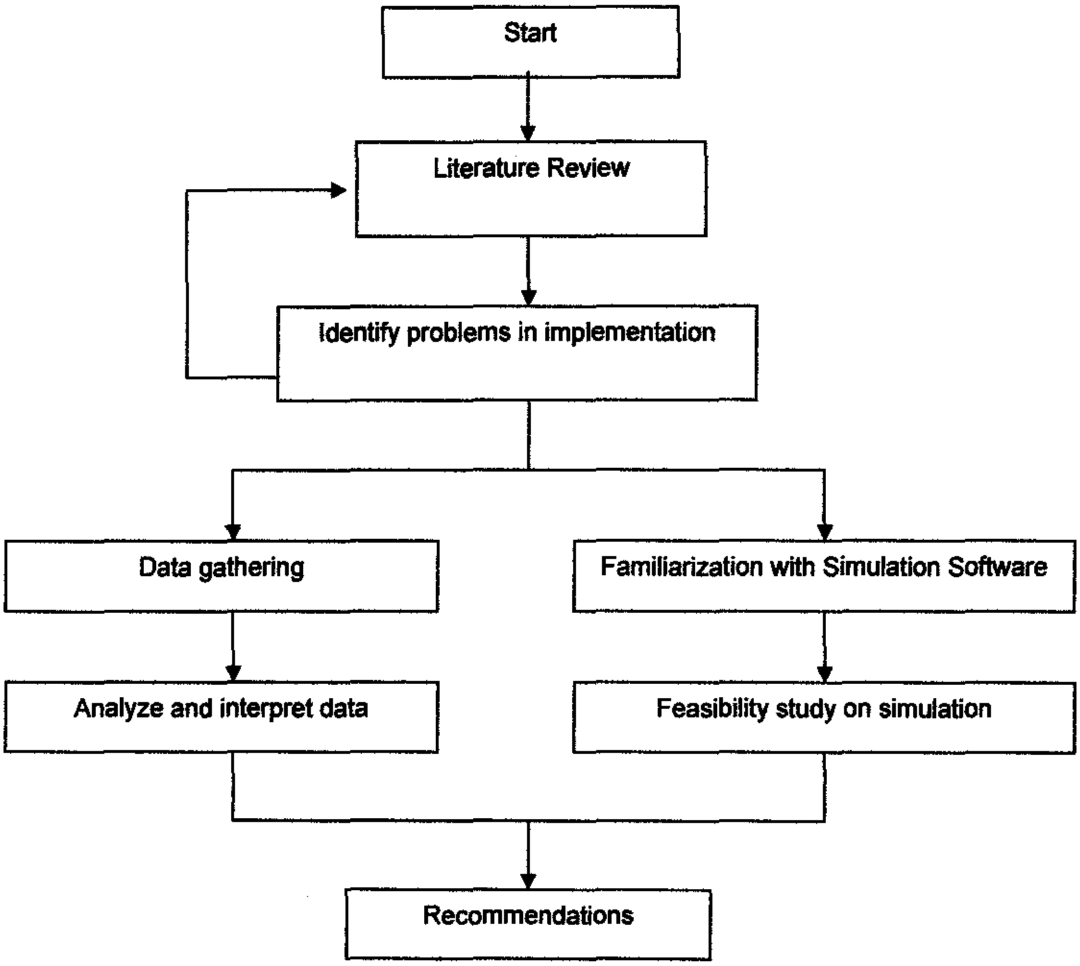

Figure 4 Design Methodology

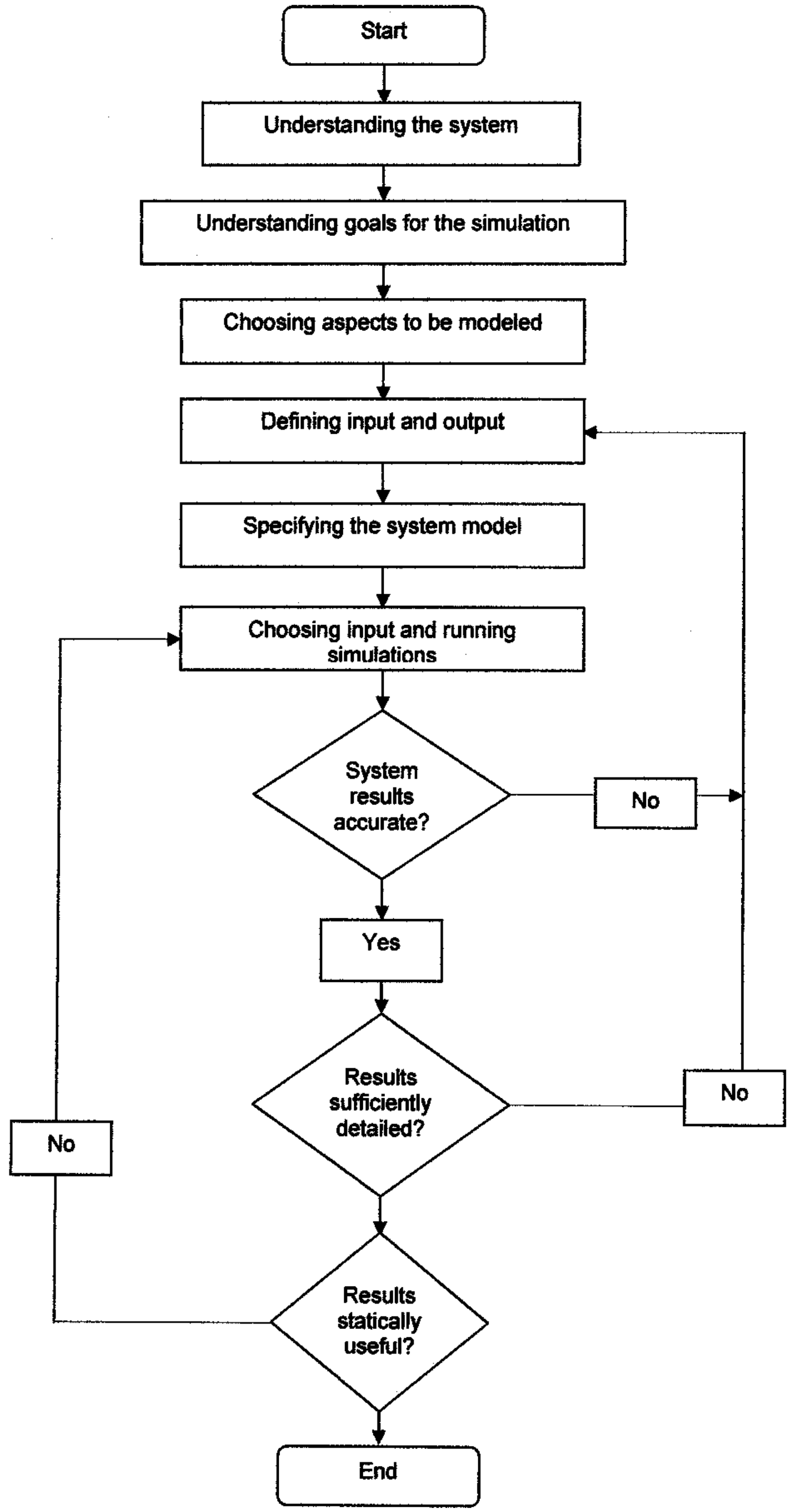

Figure 5 OPNET design workflow

- Study on Wireless Mesh Network
  - Key functionality required to implement a robust WMN
  - The underlying technologies (switching, wireless communications, security, management, routing, etc.)
- Study on the software and peripherals for the implementation
- Design the WMN simulation based on calculations and theories
- Analyze results from simulation and troubleshoot

3.2 Tools

In completing the project, various tools will be used to assist in developing the wireless mesh network. The tools can be categorized into hardware and software.

3.2.1 Software

- OPNET Modeler (v11.5) – A network modeling and simulation tool which allows us to design and study communication networks, devices, protocols and applications.

3.2.2 Hardware

- PCs or laptops

CHAPTER 4
RESULTS AND DISCUSSION

4.1 Parameters Calculation and Simulation Configuration

4.1.1 OPNET Models

There are a few different WLAN models available in OPNET including the Mobile Ad-hoc Network (MANET) node. The MANET node model represents a raw packet generator transmitting packets over IP and WLAN. Protocols supported include IP and IEEE 802.11. One of its special attributes that is useful in realizing the simulation is the MANET Traffic Generation Parameters, which can be used to specify the rate at which raw unformatted packets are generated. Figure 6 shows the process model of a MANET node in OPNET.

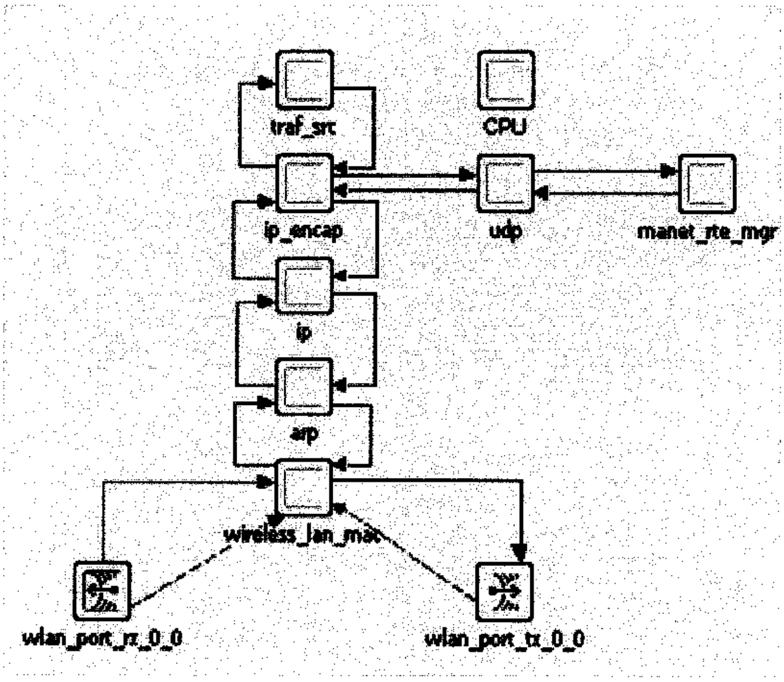

Figure 6 MANET Station Model

The lower layers of WLAN are modeled as RX and TX ports as the physical layer, while the *wireless_lan_mac* process as the MAC layer.

There are four important measurements observed from the simulations:

- **Load:** Total number of bits received from the higher layer to the MAC layer. Packets arriving from the higher layer are stored in the higher layer queue.
- **Throughput:** Total number of bits sent to the higher layer from the MAC layer. The data packets received at the physical layer are sent to the higher layer if they are destined for this station, and they will arrive to the IP layer I they are rerouted to other station.
- **Dropped data packets:** They are not part of the load as they are dropped due to the overflow of higher-layer buffer.
- **Traffic:** The upper layers packets forwarded downstream to the network.

4.1.2 OPNET MANET Node Configuration

Below is the configuration applied to MANET nodes in the simulation. It is used in all experiments, however with different values of transmission power, depending on the experiments. All other attributes not mentioned here are configured with the default settings in OPNET.

Table 2 MANET Node Configuration

Attributes	**Value**
Transmission power	0.001 W
RTS threshold	256 bytes
Data rate	11 Mbps
Physical Characteristics	Direct Sequence
Packet Reception-Power Threshold	-90 dBm
Buffer Size	256000 bits

- Transmission power - Specifies the transmit power of the STA in Watts. In the United States, when using omni-directional antennas having less than 6 dB gain in mobile WLAN scenarios, the FCC rules require EIRP to be 1 watt (1,000 milliwatts) or less. The EIRP limitations for fixed, point-to-point systems that use directive antennas with at least 6 dB gain is 4 watts.

- RTS threshold – Specifies the threshold for performing RTS/CTS frame exchange proceeding the transmission of the data frame. For the data packets whose size exceeds the threshold, completion of a successful RTS/CTS frame exchange is required before the transmission of the actual packet over the radio channel.

- Data rate - Specifies the data rate that will be used by the MAC for the transmission of the data frames via physical layer. The set of supported data rates are specified in IEEE's 802.11 and 802.11b standards.

- Physical characteristics - Based on the value of this attribute, which determines the physical layer technology in use, the WLAN MAC will configure the values of the following protocols parameters as indicated in the IEEE 802.11 WLAN standard. All WLAN MACs that belong to the same BSS should have the same physical characteristics configuration; otherwise the simulation will terminate with an error message.

- Packet Reception-Power Threshold - Defines the received power threshold value in Watts at the radio receiver for arriving WLAN packets. Packets with a power less than threshold considered as noise packets and they don't change the status of the receiver to "busy" from MAC's point of view, and don't turn on the signal lock at the receiver. These packets serve as interference source against the valid packets. The value of Packet Reception-Power Threshold can be converted to watts using:

$$\textit{Packet Reception-Power Threshold (watts)} = \frac{10^{PTdBm/10}}{1000} \qquad \text{(Eq.1)}$$

where

PT_{dBm} = Packet Reception-Power Threshold (dBm)

4.1.3 Path Loss

Receiver power in a wireless transmission can be calculated using path loss [1]. Path loss is the reduction in power density (attenuation) of an electromagnetic wave as it propagates through space. Below is the equation for path loss.

$$\textit{Path loss, } L_p = \frac{16\pi^2 d^i}{\lambda^2} \qquad \text{(Eq.2) [1]}$$

Where

L_p = path loss

d = distance between transmitter and receiver

i = path loss exponent

(2 for free space environment, 3 or 4 for normal environment)

λ = wavelength

Wavelength λ can be calculated with the following equation

$$\lambda \textit{ (meter)} = \frac{C(meter/\sec)}{F(Hz)} \qquad \text{(Eq.3) [1]}$$

Where

C = Speed of light = $3x10^8$ m/s

F = Frequency = 2.4 GHz = $2.4x10^9$ Hz

For the experiment, frequency of 2.401 GHz is used, which is the IEEE 802.11b frequency. Thus the value of wavelength λ is:

$$\lambda \textit{ (meter)} = \frac{3x10^8}{2.4x10^9} = 0.1249479 \text{ m}$$

Using this value of λ, path loss L_p for a distance 300m in free space environment can now be calculated.

$$L_p = \frac{16\pi^2(300)^2}{(0.1249479)^2} = 910.3408904\text{x}10^6$$

4.1.4 Receive Power

The expected receive power P_{rx} is calculated from the transmitted power P_{tx} and path loss L_p using this formula:

$$P_{rx} = \frac{P_{tx}}{L_p} \qquad \text{(Eq.4) [1]}$$

$$P_{rx} = \frac{0.001w}{910.3408904\text{x}10^6} = 1.09849\text{x}10^{-12}\,\text{watt}$$

From the configuration in Table 2, the power threshold is -90 dBm or $1\text{x}10^{-12}$ watt, which means that the receive power is just higher than the threshold. This justifies the reason for using transmit power of 0.001 watt.

4.1.5 Transmit Power

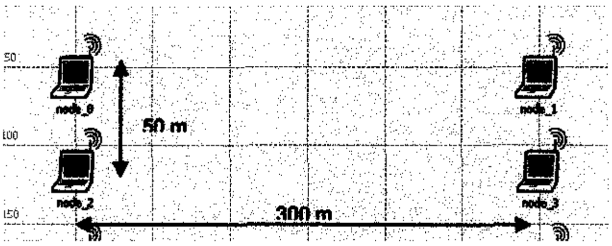

Figure 7 Transmit power for different distances

To calculate the values of transmit power for difference distance, below equation is used.

$$\textit{Transmit power, } P_{tx}\ \text{(distance } d_{ref}) = \left(\frac{d_{ref}^{\ 2}}{d^2}\right) P_{tx} \qquad \text{(Eq.5) [1]}$$

Table 3 below depicts the different values of P_{tx} for different values of reference distances.

Table 3 Path loss and transmit power for different reference distance

d_{ref} (meter)	Path loss	P_{tx} (watt)
50	3.95456 x10^{-8}	2.77778 x10^{-5}
60	2.74622 x10^{-8}	4.00000 x10^{-5}
70	2.01763 x10^{-8}	5.44444 x10^{-5}
80	1.54475 x10^{-8}	7.11111 x10^{-5}
90	1.22054 x10^{-8}	9.00000 x10^{-5}
100	9.88640 x10^{-8}	1.11111 x10^{-4}
150	4.39396 x10^{-8}	2.50000 x10^{-4}
200	2.47160 x10^{-8}	4.44444 x10^{-4}
250	1.58182 x10^{-8}	6.94444 x10^{-4}
300	1.09849 x10^{-8}	1.00000 x10^{-4}

4.1.6 Traffic Generation

In the experiments, the traffic packets are exponentially distributed in size with a mean of 10000 bits, and the inter-arrival time between packets is exponentially distributed with a mean of 1 second. To generate more traffic in a second, the number of packets generate is changed by adding more packets. For example, for a traffic size of 1Mbps, 100 packets are needed with 10000 bits each.

4.2 802.11 Experiments

4.2.1 One sender and one receiver (exponential traffic)

The nodes are configured to operate at 11Mbps bandwidth, and is 300m apart from each other. Traffic is generated at **node_0** (sender) and is sent to **node_1** (receiver), with the packets exponentially distributed with a mean of 10000 bits. Load is measured at **node_0** while throughput is obtained at **node_1**.

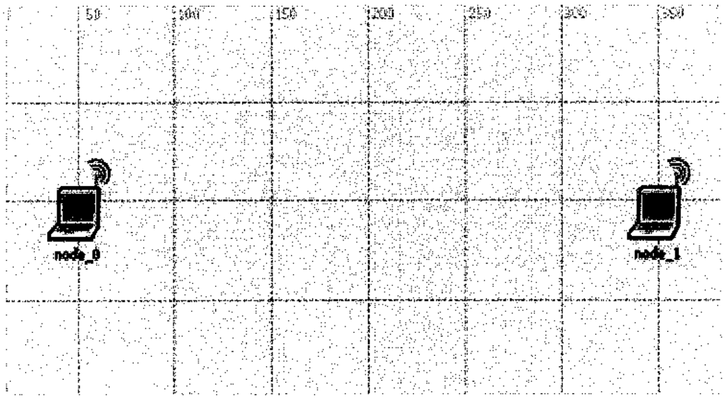

Figure 8 Setup for one sender and one receiver

The graphical results for the load, throughput and drop for each traffic can be seen in Appendix A. Below is the summary of all the results.

Table 4 Results (one sender and one receiver, exponential traffic)

Traffic (Mbps)	Load (bps)	Throughput (bps)	Drop (bps)
1	983,360	983,251	0
2	1,978,701	1,966,345	0
3	2,999,579	2,454,412	0
4	4,042,897	2,607,351	2,925,379
5	5,006,304	2,588,621	4,743,633
6	6,040,179	2,581,394	3,280,012
7	6,999,138	2,579,365	4,318,723

From the results in Table 4, we can see that there is no drop for low traffic sizes, i.e. those less than 4 Mbps. The reason is, all traffic is forwarded down to the network and the load is of the traffic size. Meanwhile, the values of throughput at **node_1** are quite close to the load values.

However, when traffic is bigger than 4 Mbps, drop begins to happen as can be seen from the decreasing values of load and throughput. Therefore it is safe to say that when traffic size is larger, the load and throughput will decrease.

As mentioned earlier, the MAC buffer size is set to 256000 bits. This means that the buffer is almost full all the time when the traffic is exponentially distributed. Whenever there is a small space in the buffer, and a big frame arrives, it will be dropped directly. The higher traffic, the more probability of having frames bigger than the space in buffer, thus producing lower throughputs. This can be illustrated in the figure below.

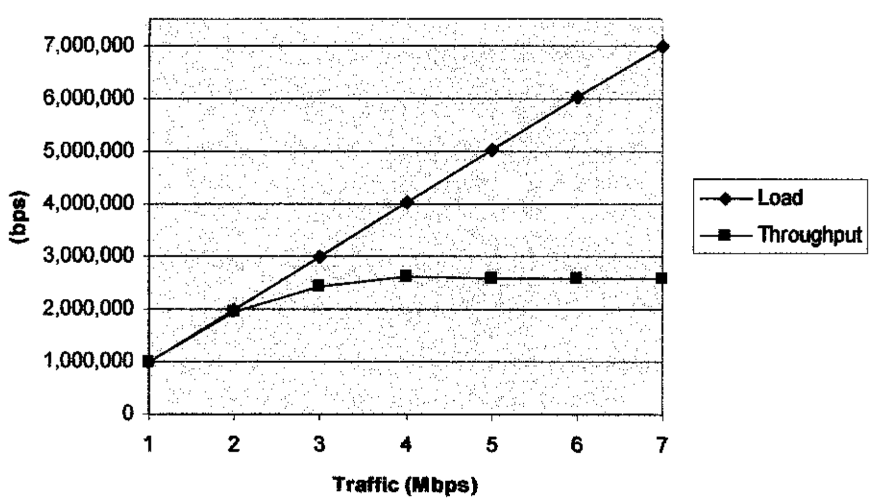

Figure 9 Load and throughput for one sender to one receiver (exponential traffic)

4.2.2 One sender and one receiver (constant traffic)

The same experiment as above is repeated, but using constant packets of 10000 bits each. The graphical results for the load, throughput and drop for each traffic can be seen in Appendix B. The results show higher throughputs compared to exponentially distributed packets in the earlier experiment. It also shows stable values after the highest throughput is achieved, because when having constant size packets, the probability of drop is less since larger packets have higher probability of dropping.

Table 5 Results (one sender and one receiver, constant traffic)

Traffic (Mbps)	Load (bps)	Throughput (bps)
1	1,019,653	1,019,651
2	2,019,577	1,997,944
3	3,001,858	2,647,492
4	4,042,897	2,818,384
5	5,030,543	2,579,366
6	5,981,918	2,601,049
7	6,822,071	2,587,317

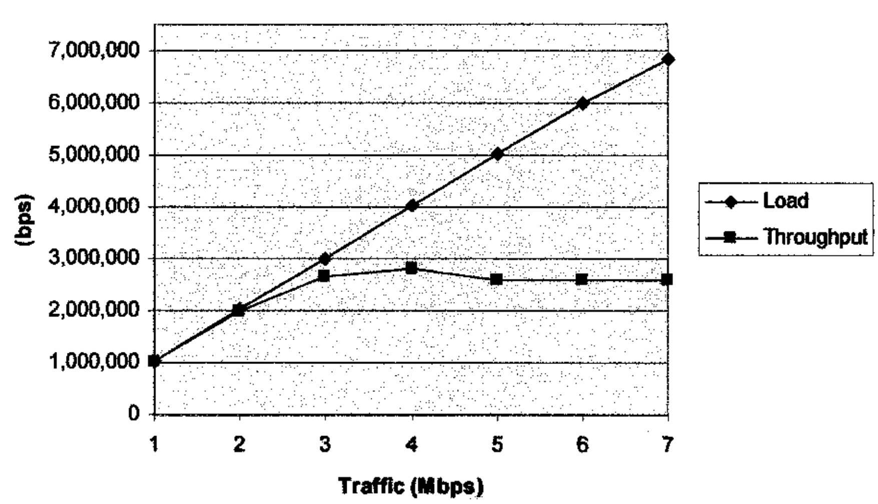

Figure 10 Load and throughput for one sender to one receiver (constant traffic)

4.2.3 Six senders and six receivers (exponential traffic)

For this experiment, six senders are configured to send data to six receivers within the same distance (300 meters). This means there are six one-to-one transmissions. In Figure 11, the distance between the senders are 60 meters and the total distance from the **node_0** to **node_10** is still 300 meters, and vice versa for the receivers. Therefore, all senders and receivers are within the transmission range.

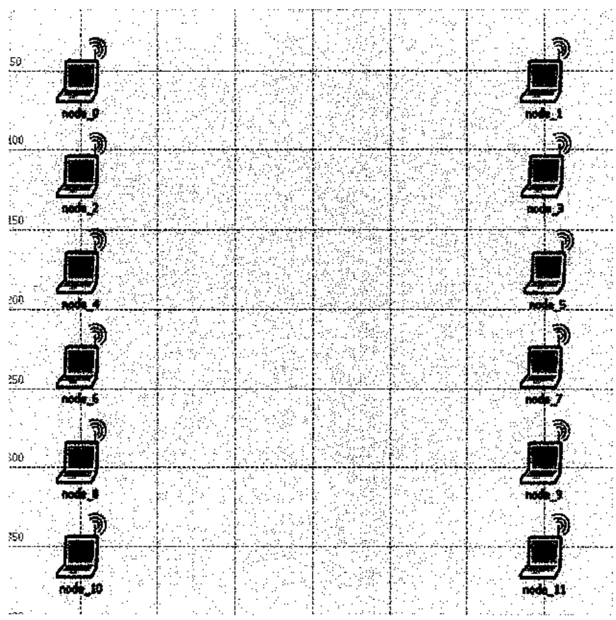

Figure 11 Setup for six senders and six receivers.

The results are as in Table 6. The maximum throughput is about 3.6 Mbps, and then the value seems to decrease after the traffic exceeds 4.5 Mbps. Here, the traffic is exponentially distributed in size, and the MAC layer buffer is limited. Therefore, the arriving packets may be dropped if the remaining space in the buffer is smaller than the packet size. Thus, the number of large packets increase if the traffic size increase, and causing more dropping and less throughput.

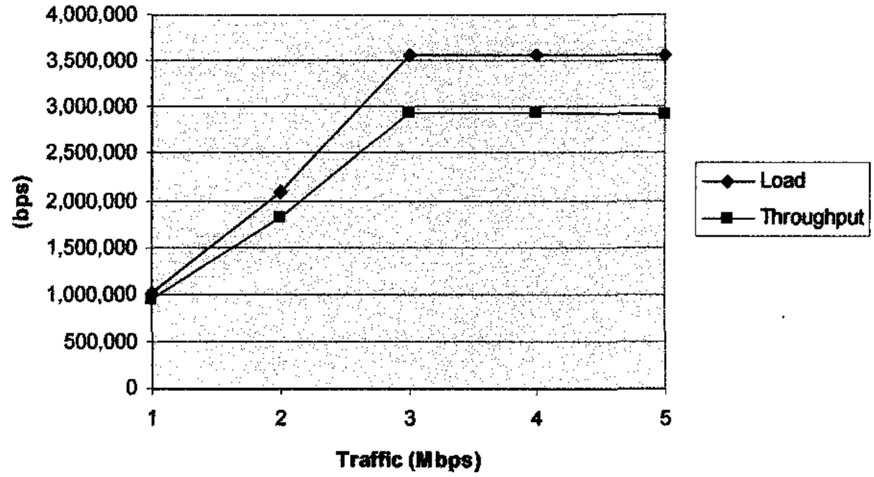

Figure 13 Load and throughput for six senders to six receivers (constant traffic)

Table 7 Results (six senders and six receivers, constant traffic)

Traffic (Mbps)	Load (bps)	Throughput (bps)
1	1,013,938	958,752
2	2,083,441	1,832,736
3	3,560,074	2,936,464
4	3,569,768	2,941,674
5	3,559,337	2,915,526

4.3 Chain of four nodes

In this experiment, traffic is generated at the source node, **node_0** and destined to the destination node, **node_3**. However, the data cannot be transmitted directly due the power used is only sufficient to reach the next neighbor. The distance between the nodes is 100 meters, and the data will be passed to each intermediate nodes until it arrives to the destination node.

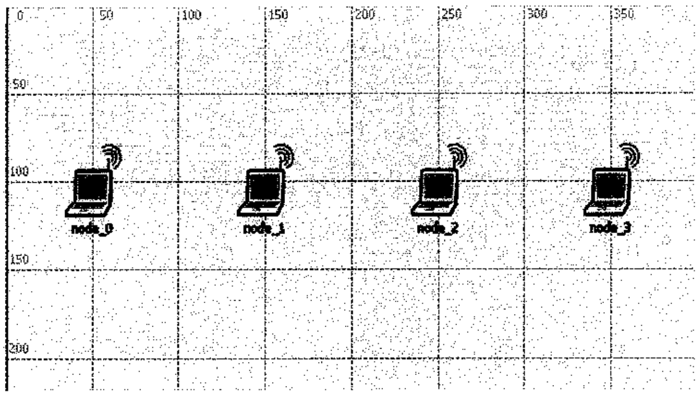

Figure 14 Setup for chain of four nodes

There will be only one active transmission at a time as the RTS and CTS packets will cause the nodes that are not part of the transmission to wait. Thus the total throughput in all nodes is divided by the number of hops. The load was measured at the source node and the throughput at the destination node.

As seen in the results below, the maximum throughput for the destination node is about 1.5 Mbps which is less than half of the maximum throughput in a single hop.

Table 8 Results (Chain of four nodes)

Traffic (mbps)	Load (bps)	Throughput (bps)
0.5	499,935	499,925
1.0	990,755	990,684
1.5	1,508,718	1,508,579
2	1,991,473	1,164,279

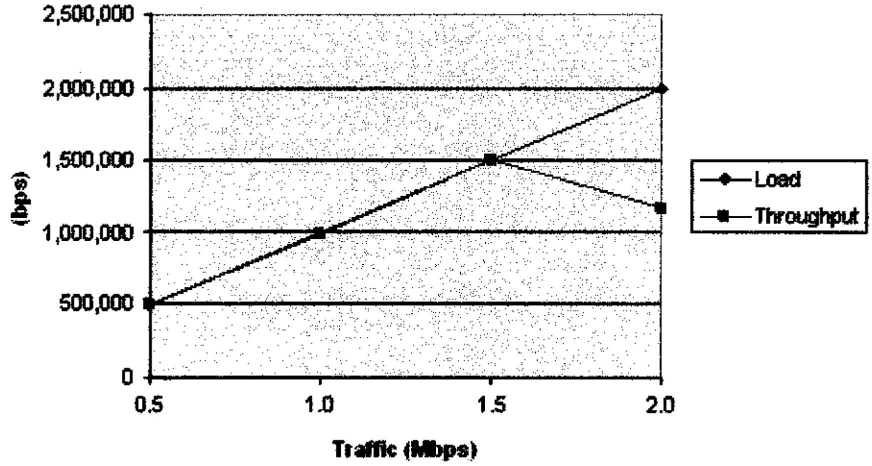

Figure 15 Load and throughput for a chain of four nodes

CHAPTER 5
CONCLUSION

At the end of this project, the implementation of Wireless Mesh Network through the OPNET simulation has indeed reflected the network performance in real life.

The results show that constant traffic has higher throughput than exponential traffic in high traffic cases, while exponential traffic causes the network throughput to decrease after a maximum acceptable traffic size, which happens because the buffer size limit cannot manage the large packets. For a constant traffic, the throughput stays at the maximum values if the traffic size increases because the packets have the same size, and packets have equal probability of dropping.

As for the multiple senders to multiple receivers case, it definitely has higher throughput than a single sender-receiver within the same area. One sender have to wait more between packets, but the waiting time is less when having multiple senders because least waiting time is used.

This project is still very much at its basic level, thus a lot of work has to be done to gain more meaningful findings on WMN. Below are a few suggested future works:

- Implement more experiments in different setups and configurations for additional performance measurements.
- Mobility modeling as in real life, nodes can be both mobile and stationery.
- WMN need extra security consideration, since wireless connection are open links. Therefore security is important for a confidential data exchange.

REFERENCES

1. P. Mohana Shankar, "Introduction to Wireless System", John Wiley & Sons Inc, 2002.
2. R Draves, J Padhye, and B. Zill, "Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks", 2004.
3. I. Akyildiz, X. Wang, and W.Wang, "Wireless Mesh Networks: A Survey", 2005.
4. I Chlamtac, M. Conti, and J. Liu, "Mobile Ad Hoc Networking: Imperatives and Challenges", 2003.
5. "MIT Roofnet", http://pdos.csail.mit.edu/roofnet, retrieved on 21/08/2006.
6. "LocustWorld", http://www.locustworld.com, retrieved on 21/08/2006
7. "Self-Organizing Neighborhood Wireless Mesh Network", http://research.microsoft.com/mesh/, retrieved on 21/08/2006.
8. Jochen H. Shiller, "Mobile Communication", Addison Wesley Inc., 2003.
9. Gilbert Held, "Wireless Mesh Networks", Auerbach Publications, 2005.
10. Sumit Roy, Hui Ma, Rajiv Vijayakumar, Jing Zhu, "Optimizing 802.11 Wireless Mesh Network Performance Using Physical Carrier Sensing", April 2006.

APPENDIX A

RESULTS

One sender and one receiver (exponential traffic)

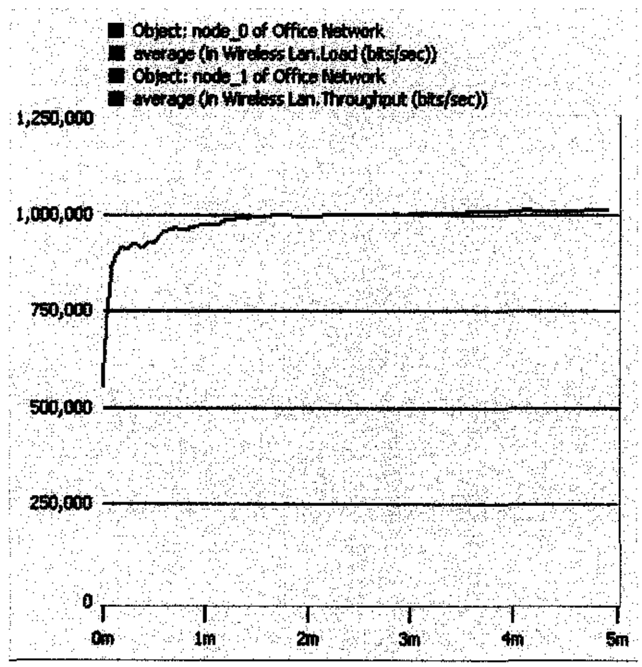

Figure 16 1 Mbps traffic

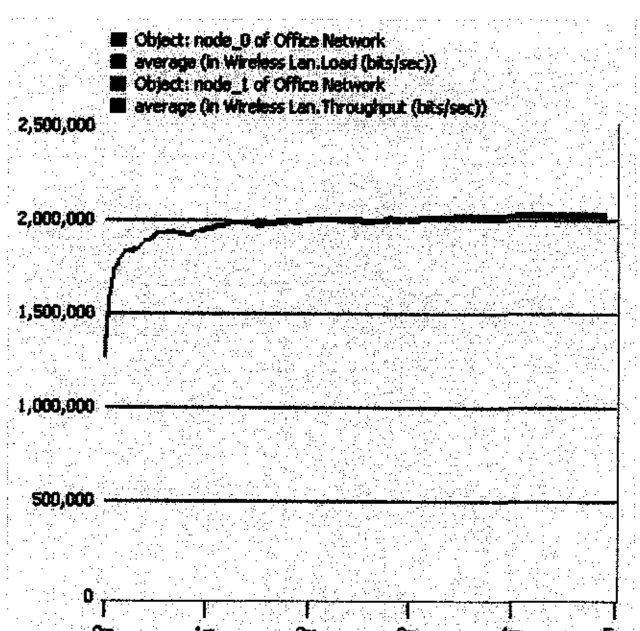

Figure 17 2 Mbps traffic

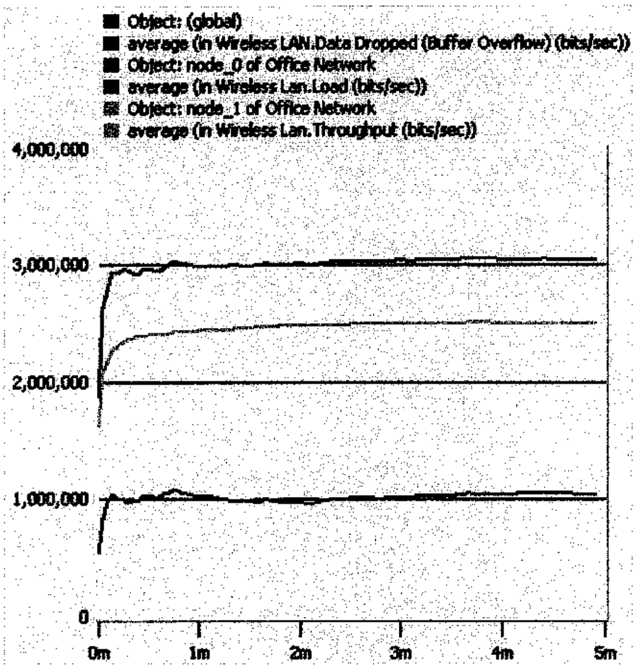

Figure 18 3 Mbps traffic

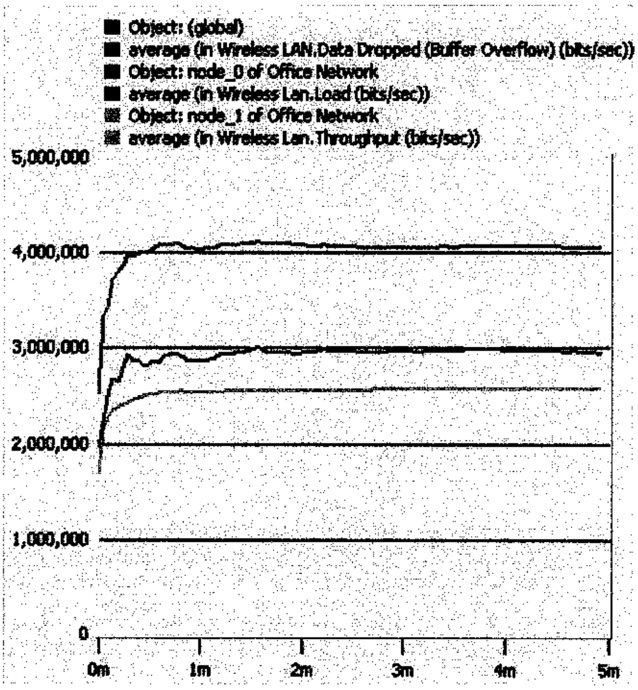

Figure 19 4 Mbps traffic

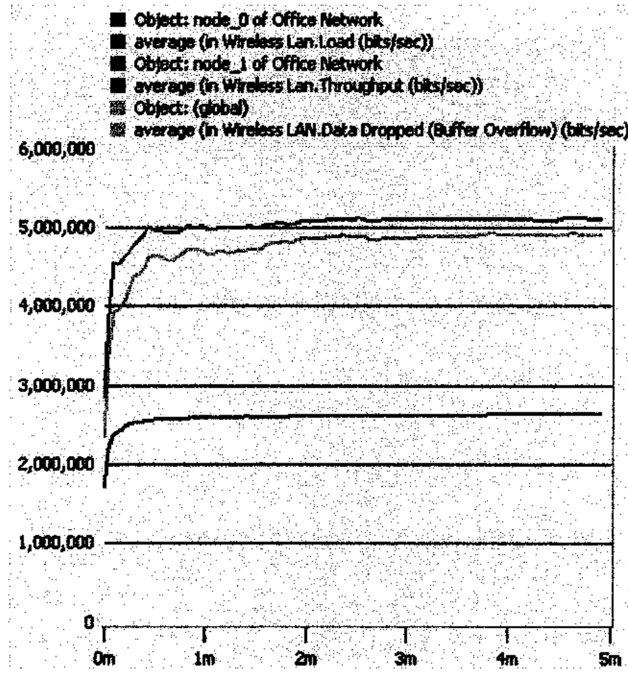

Figure 20 5 Mbps traffic

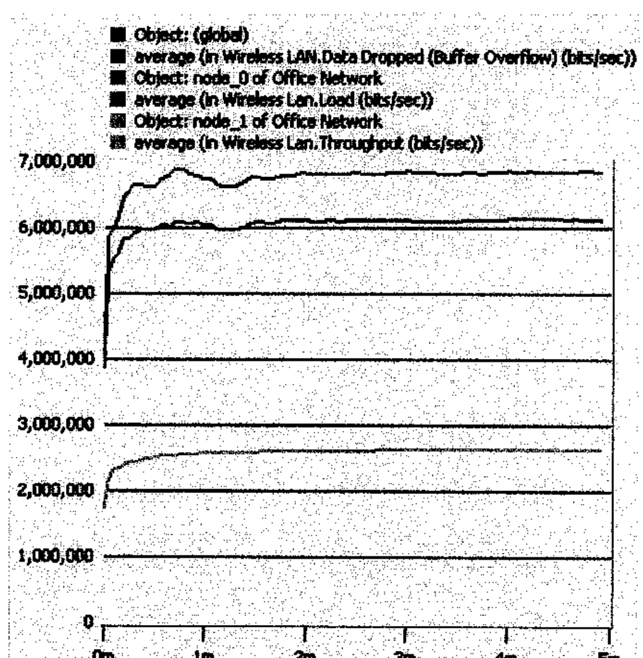

Figure 21 6 Mbps traffic

APPENDIX B

RESULTS

One sender and one receiver (constant traffic)

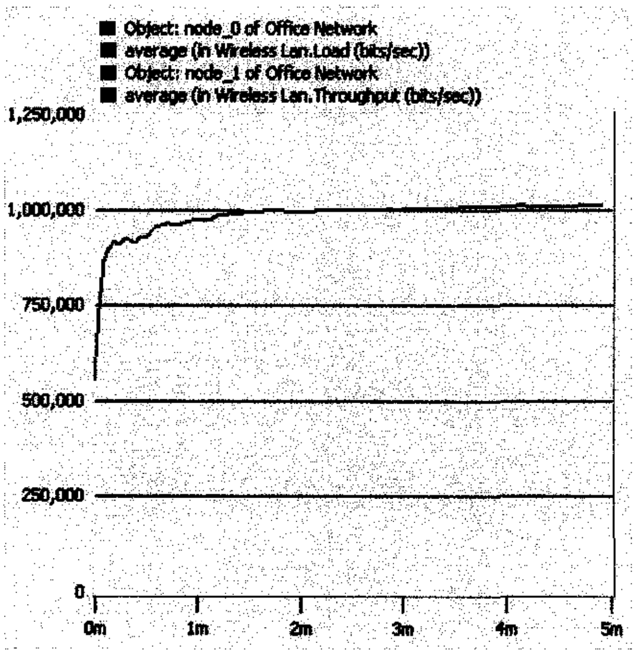

Figure 22 1 Mbps traffic

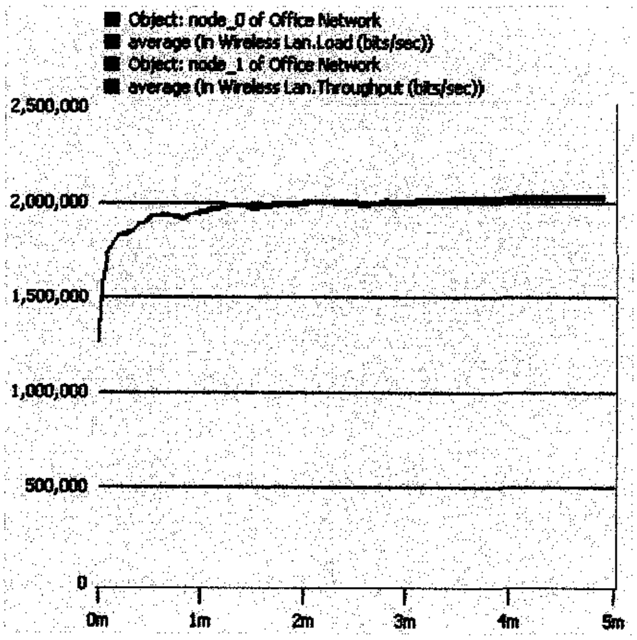

Figure 23 2 Mbps traffic

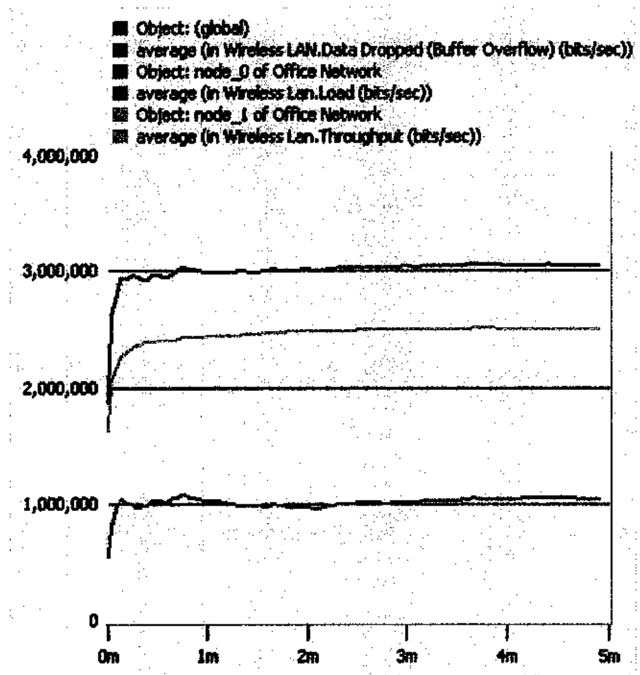

Figure 24 3 Mbps Traffic

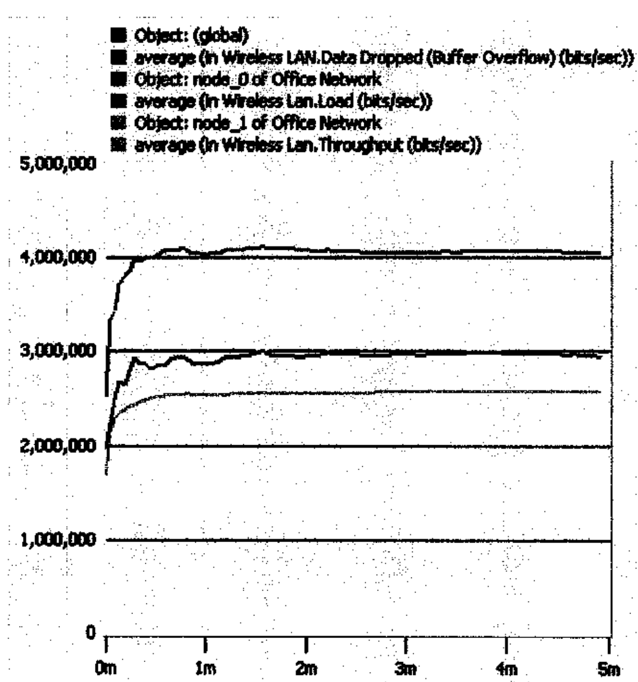

Figure 25 4 Mbps traffic

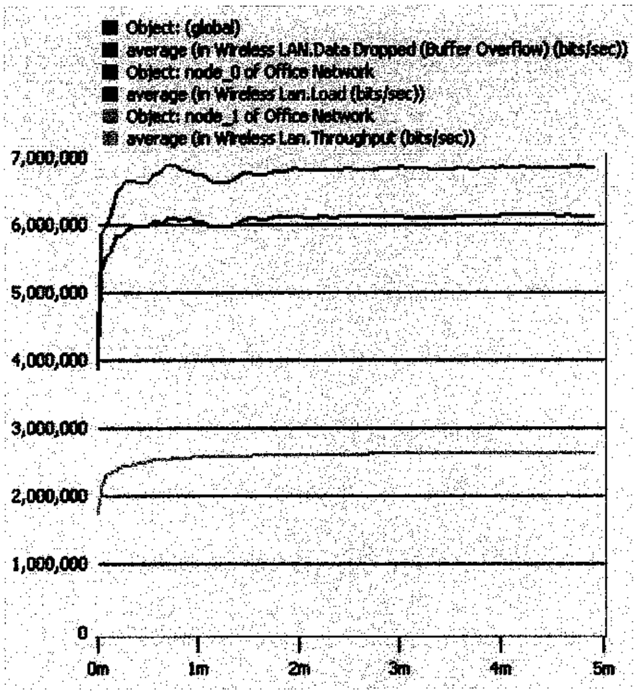

Figure 26 6 Mbps traffic