THE EFFECT OF EAVESDROPPING AND WORMHOLE ATTACKS ON MOBILE AD HOC NETWORK

A Thesis submitted to
College of Arts and Sciences (Applied Sciences)
In Partial fulfillment of the requirements for the degree
Master of Science (Information Technology)
University Utara Malaysia

By

Nadher Mohammed Ahmed Al-Safwani

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

NADHER MOHAMMED AHMED AL-SAFWANI
(800321)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

THE EFFECT OF EAVESDROPPING AND WORMHOLE ATTACKS ON MOBILE AD HOC NETWORK

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **ASSOC.PROF. HATIM MOHAMAD TAHIR**

Tandatangan
(Signature) : _____

Tarikh
(Date) : 8/11/09

Assoc. Prof. HATIM MOHAMAD TAHIR
College Of Arts & Sciences
Univesiti Utara Malaysia
06010 UUM Sintok, Kedah, Malaysia
Tel: +604-928 4659 Fax: +604-928 4753
H/P: 019-454 9603 e-mail: hatim@uum.edu.my
Website: stafweb.uum.edu.my/hatim

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a Master of Science in Information Technology (MSc. IT) from University Utara Malaysia, I agree that the University library may make it freely available for inspection. I further agree that permission for copying of this project in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or in their absence, by the Dean of College of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to University Utara Malaysia for any scholarly use which may be made of any material from my project.

Request for permission to copy or make other use of materials in this thesis, in whole or in part, should be addressed to:

Dean of Research and Graduate Studies

Colleges of Arts and Sciences

University Utara Malaysia

06010 UUM Sintok

Kedah Darul Aman

Malaysia

ABSTRACT

Security has become the main concern to grant protected communication between mobile nodes in an unfriendly environment. Wireless Ad Hoc network might be unprotected against attacks by malicious nodes. This project evaluates the impact of some adversary attacks on mobile Ad Hoc network system (MANET's) which have be tested using QualNet simulator. Moreover, it investigates the active and passive attack on mobile Ad Hoc network. At the same time, it measures the performance of MANET with and without these attacks. The simulation is done on data link layer and network layer of mobile nodes in wireless Ad Hoc network. The results of this evaluation are very important to estimate the deployment of the Mobile Ad Hoc nodes for security. Moreover, this study have been analyzed the performance of MANET and perform "what-if" analyses to optimize them.

ACKNOWLEDGEMENT

All praise is due to Allah, Most Gracious, and Most Merciful. Without whose help and mercy, I would not have reached this far.

It would not have been possible for me to complete the course of my master without encourage and support of my family. My first expression of gratitude goes to my parents, wife, brothers, and sisters whose give me the strength to complete this course.

I would like to express my gratitude to my supervisor, Associate Professor Hatim Mohammed Tahir for expertise, gentle guidance, encouragement, critical remarks and advices which ensured that, progress, was continuously maintained. Our discussions since the last three months have contributed to the completion of this work.

I also would like to express my thanks to the University Utara Malaysia, colleagues, and friends to many moments of insight, inspiration, laughter, and for the given support.

Sincere Grateful

Nadher Mohammed A. Al -Safwani

DEDICATION

==========

I would like to dedicate this thesis to my father and mother,

wife, brothers, and sisters who lovely encouraged

and support me through all my study

The motivation for all I do.

==========

TABLE OF CONTENT

PERMISSION TO USE..... i

ABSTRACT ii

ACKNOWLEDGEMENT..... iii

DEDICATION..... iv

TABLE OF CONTENT..... v

LIST OF FIGURES..... viii

LIST OF TABLES..... x

LIST OF ABBREVIATIONS..... xi

CHAPTER 1: INTRODUCTION

1.1 Background 1

1.2 Problem Statement..... 5

1.3 Project Questions 6

1.4 Project Objectives 6

1.5 Scope and Limitations 7

1.6 Project Significance 7

1.7 Thesis Organization..... 8

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction 9

2.1 Ad Hoc Networking 10

2.3 Mobile Ad Hoc Network Challenges 14

2.4 Mobility Ad Hoc Security..... 17

2.4.1 Threats 18

2.4.2 Vulnerabilities 19

2.4.3 Attacks 21

2.4.3.1 Passive Attacks 23

2.4.3.1 Active Attacks 25

2.4.4 Security Goals 29

2.5 QulaNet Simulation 31

2.5.1 QualNet Architecture 33

2.6 Related Work 34

2.7 Summary 37

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Research Methodology 38

3.1.1 Problem definition 39

3.1.2 Construction and Simulation Model 40

3.1.3 Testing and Validating the Model 43

3.1.4 Design of the Experiment 43

3.1.5 Conducting the Experiments 45

3.1.6 Evaluation the Results 46

3.2 Conclusion 46

CHAPTER 4: FINDINGS AND ANALYSIS OF DATA

4.1 Introduction 47

4.2 Application to Research Questions 48

4.3 Eavesdropping Test 49

4.3.1 Eavesdropping Results 49

4.4 Wormhole Attack Test..... 52

4.4.1Wormhole Attack Results 53

4.5 Conclusion..... 57

CHAPTER 5: CONCLUSION AND FUTURE WORK

5.1 Introduction..... 58

5.2 Conclusion..... 58

5.3 Future Work..... 60

REFERENCES

APPENDIX A: AN INSTALLITION OF QUALNET 4.5..... ... 65

APPENDIX B: EAVESDROPPING RESULTS..... 69

APPENDIX C: WORMHOLE ATTACK RESULTS..... 75

LIST OF FIGURES

Figure 1.1: Ad Hoc Network..... 2

Figure 1.2: Information Security 4

Figure 2.1: (a) Ad Hoc (b) Cellular networking 10

Figure 2.2: Conceptual representation of mobile Ad Hoc Network 11

Figure 2.3: Passive Attacks 23

Figure 2.4: Active Attacks 25

Figure 2.5: Wormhole Attack 28

Figure 2.6: QualNet Architecture 33

Figure 3.1: Simulation Model 39

Figure 3.2: Test Bed Setup for Eavesdropping 41

Figure 3.3: Test Bed Setup for Wormhole 42

Figure 4.1: Total Bytes received with and without Wormhole 54

Figure 4.2: Total Packets received with and without Wormhole 55

Figure 4.3: Throughput with and without Wormhole 55

Figure 4.4: Average End-To-End delay with and without Wormhole 56

Figure 4.5: Average Jitter with and Without Wormhole 57

Figure A.1: QualNet 4.5.1 GUI Simulation 68

Figure C.1: Run 2 Wormhole Frames Intercepted all..... 75

Figure C.2: Run 2 Wormhole Frames Tunneled 75

Figure C.3: Run 2 Wormhole Frames Replayed 76

Figure C.4: Run 2 (802.11) Signals Transmitted 76

Figure C.5: Run 2 Broadcast Packets Received 77

Figure C.6: Run 4 Wormhole Frames Intercepted All.....77

Figure C.7: Run 4 Frames Dropped by Wormhole 78

Figure C.8: Run 4 Wormhole Frames Tunneled 78

Figure C.9: Run 4 Wormhole Frames Replayed 79

Figure C.10: Run 4 (802.11) Signals Transmitted.....79

Figure C.11: Run 4 Broadcast Packets Received Clearly..... 80

Figure C.12: Run 6 Wormhole Frames Intercepted All 80

Figure C.13: Run 6 Frames Dropped by Wormhole 81

Figure C.14: Run 6 Frames Tunneled 81

Figure C.15: Run 6 (802.11) Signals Transmitted 82

Figure C.16: Run 6 Broadcast Packets received clearly..... 82

LIST OF TABLES

Table 2.1: Ad Hoc and Cellular Networking..... 12

Table 2.2: Security Classification 22

Table 2.3: Security Attacks on Protocol Stack 29

Table 3.1: Minimum Requirements to install QulaNet for windows 40

Table 3.2: Experimental Design for First Scenario 44

Table 3.3: Experimental Design for Second Scenario 45

Table 4.1: Eavesdrop output format 50

Table 4.2: Description of IP Header Eavesdrop output 51

Table 4.3: Description of IP flags Eavesdrop output 51

Table A.1: C++ Compiler 67

Table B.1: Results of Eavesdropping Experiential design 69

LIST OF ABBREVIATIONS

AODV	Ad Hoc on demand Distance Vector
CBR	Constant Bit Rate
DoS	Denial of Service
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
MAC	Medium Access control
MANET	Mobile Ad Hoc Network
NS	Network Simulation
SNT	Scalable Network Technologies
SYN	Synchronize
TCP	Transmission Control Protocol
UDP	User Data Protocol
WLAN	Wide Local Area Network

CHAPTER ONE

INTRODUCATION

1.1 Background

The wireless arena has been growing exponentially in past few decades. We have seen a great advances in network infrastructures as growing availability of wireless applications and the emergence of universal wireless devices like laptops ,PDA ,and cell phone (Papaleo, 2007). Nowadays, mobile users can rely on cellular phone to check emails and browse the internet. For example ,travelers with laptop can use the internet anytime and anywhere (Basagni, Conti, & Giordano, 2004). In the next generation of wireless communication systems, there will be a need for the fast deployment of independent mobile users. Important examples include establishing survivable, efficient, dynamic communication for emergency operations, disaster recovery, and military networks. Such network scenarios cannot rely on centralized and organized connectivity.

There are currently two kinds of mobile wireless networks. The first type is known as infrastructured networks with fixed and wired gateways. Typical applications of this type of "one-hop" wireless network include wireless local area networks (WLANs). The second type of mobile wireless network is infrastructureless mobile network commonly known as the Ad Hoc network or wireless Ad Hoc network (Jin & Jin, 2008).

Ad Hoc network systems are independent systems which consist of a collection of mobile nodes that use wireless transmission for communication .They are self – organized, self-configured ,and self –controlled infrastructureless networks (Sarkar, Basavaraju, & Puttamadappa, 2008). In Ad Hoc network, the devices themselves are the network, and this allows seamless communication at low cost, self organizing and free deployment as shown in figure 1.1.

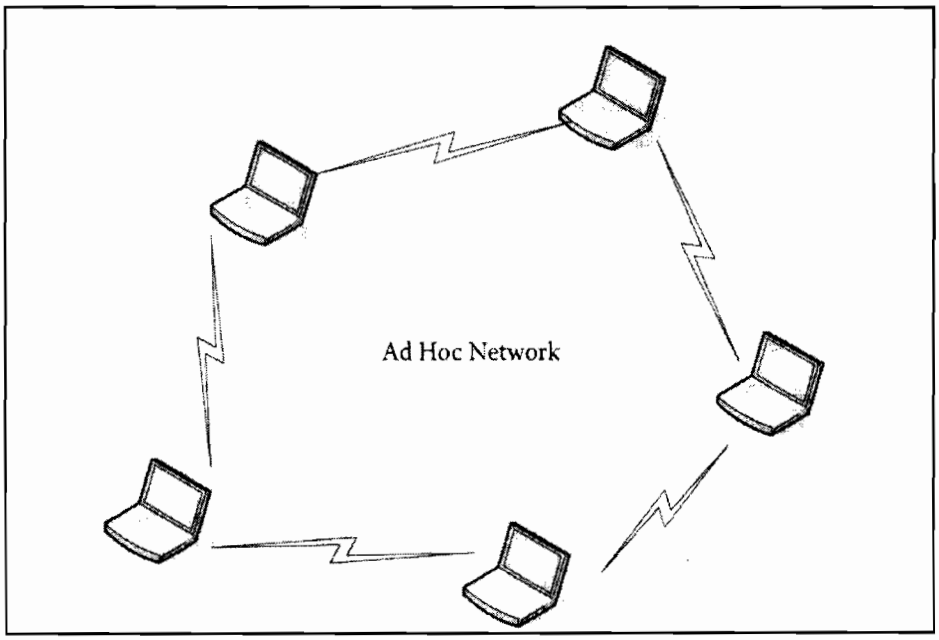


Figure 1.1 : Ad Hoc Network (Sarkar *et al.*, 2008)

Hence, mobile Ad Hoc (MANET) is different from other network solutions. For the first time users can create their own network which can be deploy and configure easily and cheaply. On the other hand, the radio transmission range is small, therefore, communication partners are not often within direct radio range; so

connections should be setup over multiple nodes and these nodes maybe will change depending on node mobility.

These change frequent route break and force source to maintain connections to their distant communication partner. For all of these reasons mobile Ad Hoc network is one of the more modern and challenging area of network security (Basagni *et al.*, 2004).The nodes in MANET consider as routers. The routers are free to move randomly ,and organize themselves at random ;so the network wireless topology may change rapidly and changeably. Mobility and large network size combined with devices heterogeneity, security, bandwidth, and battery power constraints make the design of sufficient routing protocols as a major challenge .This project is studying the performance of some of these challenges features on mobile Ad Hoc network.

Security in MANET system is one of the main concern to provide protected communication between mobile nodes in strange environment .Unlike the wired line networks ,the unique characteristics of mobile Ad Hoc networks create a number of nontrivial challenges to security design like open peer-to peer network architecture ,shared wireless medium, inflexible resources constraints and highly dynamic network topology . (Sarkar *et al.*, 2008)

If we see around us any protected system have weaknesses or vulnerabilities .Those may be targeted by an attacker .Hence ,one approach to design security mechanisms for any system is to look at the threats that face the system and the attacks possible given the vulnerabilities .This approach should ensure the system secure with these

threats, attacks, and vulnerabilities. Those vulnerabilities in MANET those in wireless links are vulnerable to several types of attacks due to natural type of the nodes. Even within the available mechanisms such as encryption and authentication can't perfectly prevent the attacks on the air-link (Anjum & Mouchtaris, 2007).

In order to implement security in MANET, environment needs to be secured against attacks. A security attack is an attempt to compromise the security of information owned by others .Security services in MANET's are needed to protect against these attacks ,and to ensure the security of the information . These services can be categorized into tow type, namely communications security and computer security as shown in Figure 1.2. Communication security protect against passive and active attacks through communication links or accidental emanations. This ensure that communication services continue with the required level of quality ,and their information couldn't capture or derived by unauthorized node (Çayırcı & Rong, 2009).

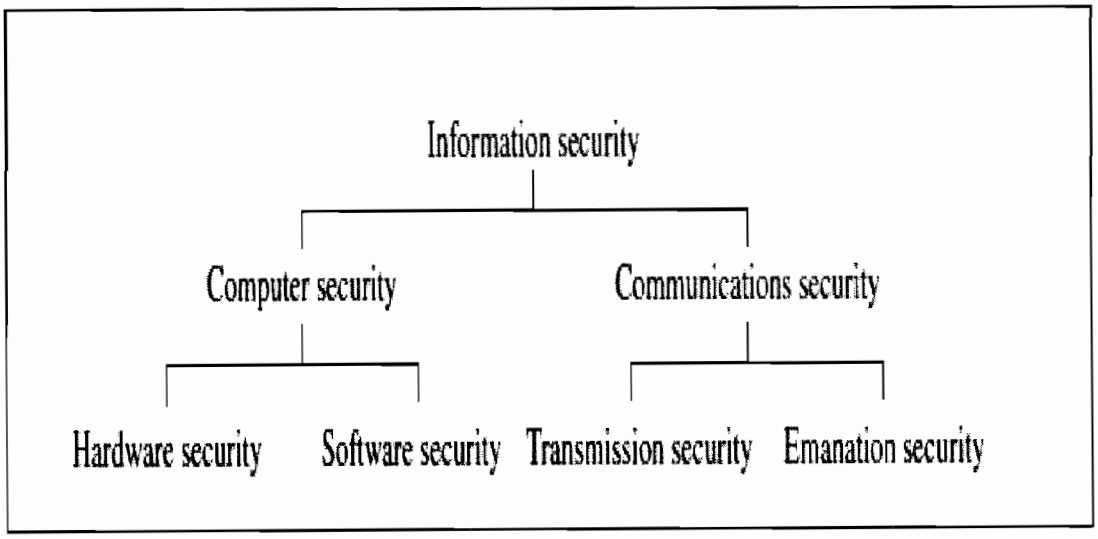


Figure 1.2: Information Security (Çayırcı & Rong, 2009)

This project was investigated on the development of communication security, and how these services in MANET were attacked by passive and active attacks. Moreover; it was evaluated the performances of the entire framework of the network after these attacks happen.

1.2 Problem Statement

The nature of mobile compute environment makes it very vulnerable to an adversary's malicious attacks. First of all, the use of wireless links render the network susceptible to attacks range from passive eavesdropping to active nosy attacks such as wormhole attack, rushing attack, black hole attack, neighbor attack, and jellyfish attack. Unlike wired networks where an adversary must gain physical access to the network wires, or pass through several lines of defense gateways such firewall, attacks on a wireless network can come from all directions and target at any node. Damages can include explore secret information and node impersonation. All of these mean that a wireless network does not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly (Papaleo, 2007) .

There is no well defined place where we deploy to protect a single security solution. Moreover, laptops and Mobiles are compromises to the attackers. Attackers may creep into the network through these subverted nodes which pose the weakest link and incur a domino effect of security breaches in the system.

The deployment of mobile Ad Hoc network is growing in the world. This leads to new challenges as large amount of data which may hold malicious content such as

worms, viruses, or Trojans to move over these networks. There is a need to detect active and passive attacks, and let the network service providers (NSPs) to offer improved security features to the customers as a value adding feature into the frame work of the network. In addition, network security administrators need to understand the vulnerabilities and the attacks in their environments with their effect on MANET before applying their deployment in the real environment to detect the threats and find efficiency solutions of the MANET framework. Moreover, there are plenty of features existing in real life networks, but new standards and attack signatures are changing continuously at a rapid rate. So network must upgrade and protect our mobile Ad Hoc network environment up-to–date.

1.3 Project Questions

This project aims to answer the following research questions:

i) How to determine likelihood of such an attack such as eavesdropping and wormhole attacks in mobile Ad Hoc network (MANET)?

ii) How to evaluate the performance in MANET framework with and without eavesdropping and wormhole attacks using QualNet Simulator?

1.4 Project Objectives

The main objectives of this project are:-

i) To determine likelihood of such an attack such as eavesdropping and wormhole attacks in Mobile Ad Hoc network (MANET).

ii) To evaluate the performance in MANET framework with and without eavesdropping and wormhole attacks using QualNet Simulator.

1.5 Scope And Limitations

This project is running with Simulation tool to study the effect of Eavesdropping and wormhole on mobile Ad Hoc. The scope of this project is limited by:

i) We used QualNet 4.5.1 GUI simulator because it provides a comprehensive environment for designing network protocols, creating and visualizing network scenarios under user-specified condition and analyzing the performance.

ii) Performing the experiment on Windows XP sp 2 operating system using QualNet GUI will give us ease design and good maintain for multiple nodes.

iii) Measuring the network performance by using some metrics such as throughput, average Jitter, and average end -to end –delay.

1.6 Project Significance

The major contributions of this project are:

i) This project have been analyzed the performance of the wireless Ad Hoc network before and after the attack.

ii) Measurements and statistics of the project will help wireless Ad Hoc security vendors to update their equipments with latest results of attacks.

iii) The project helps to evaluate the vulnerabilities and the threats in mobile Ad Hoc system (MANET's).

iv) Detecting active and positive attacks reduced the challenge and the issues of mobile Ad Hoc Framework.

v) The results from the study will allow security experts and network administrator to write their own detection unit plug-ins and test them.

vi) By keeping the simulation tool QualNet update up-to-date with latest trends in network technology, we can consider it as host based intrusion detection system that is consider as a second depth of defense for MANET framework.

vii) This study provided a starting point for other future studies that measured and evaluate the issues and the challenges of wireless Ad Hoc security attacks to evaluate the rest of attacks and to implement a security design.

1.7 Thesis Organization

Chapter tow is going to talk about the wireless Ad Hoc and their issues and challenges of security. Moreover, we are talking about the latest researchers in MANET security .On the other hand, chapter three is considered as a descriptive part illustrating the simulation methodology that we use it in our project. Purposely, chapter four is the representation of the outcomes and the analysis of the experiments results that have examined. Chapter five introduces the concluded words and highlights certain suggestions for future works

CHAPTER TWO

LETERATURE REVIEW

2.1 Introduction

Wireless networks have become increasingly popular in the past few decades, particularly within the 1990's when they are being adapted to enable mobility and wireless devices became popular (Jin & Jin, 2008) .We have seen great advances in network infrastructure ,grown fields of wireless applications and devices like mobile ,laptop and PDA's. There are many reasons of the current popularity of wireless technologies. We can list them as below:

i. The cost of wireless devices has dropped a lot that allowing wireless vendor to reduce the price of wireless services and make them much more reasonable to end users.

ii. The cost of installing wireless networks in rising markets has reduced well than the cost of installing wired networks.

iii. The services of wireless themselves have improved greatly, making it possible to offer and support both voice and data services over such network. The resulting attractive the user to use them anytime and anywhere.

These devices are now playing an important role in our live. Not only mobile users are getting smaller, cheaper more convenient and more powerful, but also run more

application and network services. Market reports show that the worldwide number of cellular has been doubling every 1 ½ years with the total number growing from 23 million in 1992 to 860 million in June 2002. They assume that one day user using wireless internet will be more than people use fix line internet. Then there is a need to a free infrastructure solution to this issue we call it mobile Ad Hoc (Anjum & Mouchtaris, 2007; Basagni et al., 2004).

2.2 Ad Hoc Networking

Wireless networking paradigms can be categorized generally into two classes: wireless Ad Hoc and cellular networking. The existence of a fixed infrastructure is the main difference between these two classes as shown in figure 2.1.

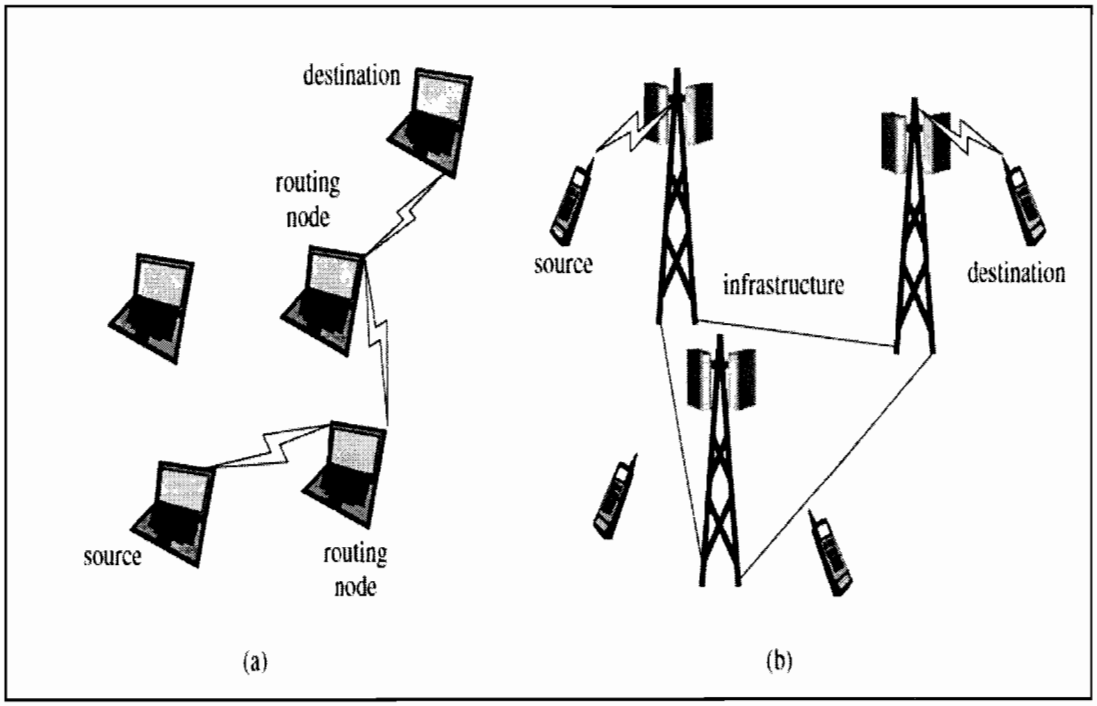


Figure 2.1: (a) Ad Hoc (b) cellular networking(Çayırcı & Rong, 2009)

Usual wireless networks require fixed network infrastructure with centralized monitoring for their transactions, but wireless mobile Ad Hoc network consists of collection of dynamic nodes. An Ad Hoc network is usually a self-organizing and self-configuring multi-hop network which does not require any fixed infrastructure. Ad Hoc networks are suited for use in situations where infrastructure is either not available, not trusted, or should not be relied on in times of emergency. Since no fixed infrastructure without base station, they can be used anytime and anywhere. In addition, since all nodes are allowed to be mobile, so the changes in the network need time varying. Add and delete node could occur only by connections with other nodes .That mean no other agency is involved. We can see that in disorganized or hostile environments including isolated scenes of natural disaster and armed conflicted as examples as shown in figure 2.2 for conceptual representation .(Çayırcı & Rong, 2009; Jin & Jin, 2008; Mishra, 2008).

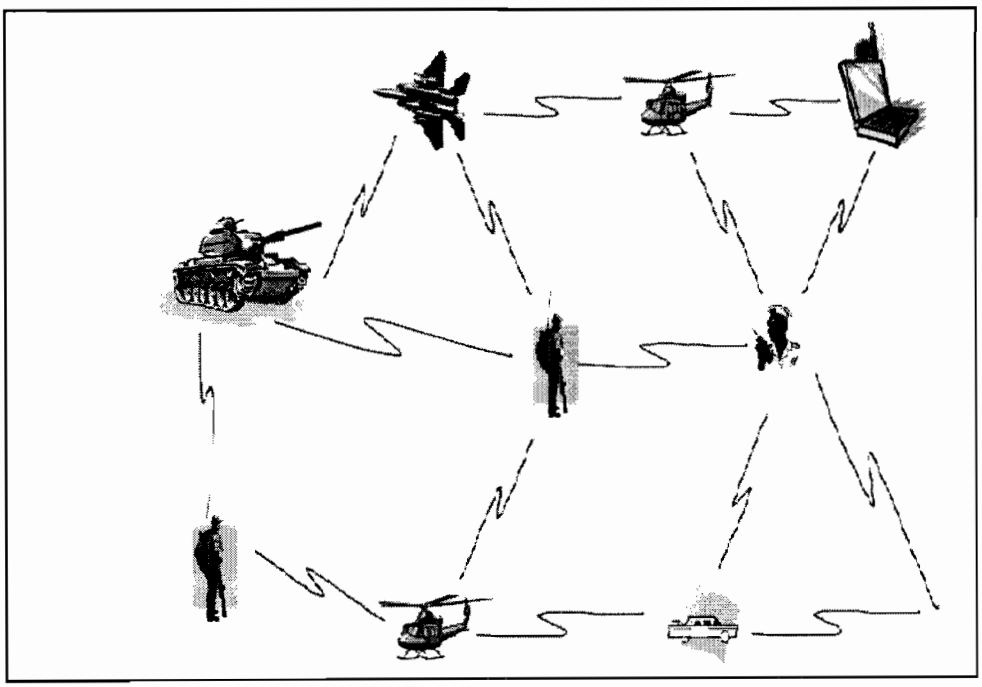


Figure 2.2:Conceptual representation of mobile Ad Hoc network(Mishra, 2008)

Nowadays, home or small office networks and shared computing with laptop Computers in a small area (such as conference or classroom, single building, meeting center, etc) have showed as other areas of MANET application. These include commercial applications based on more and more developing standards such as Bluetooth, Piconet, HomeRF, and Shared wireless Access Protocol, etc.

People have recognized that mobile Ad Hoc network has the good choose use in all the traditional areas of interest of mobile framework; so Ad Hoc network is different from cellular network. The basic characteristics of Ad Hoc and cellular networks are compared in table 2.1

Table 2.1:Ad Hoc and cellular network (Çayırcı & Rong, 2009; Sarkar *et al.*, 2008)

	Ad Hoc Network	Cellular network
Infrastructure	There is no infrastructure.	There is a fixed infrastructure.
Topology	The backbone nodes may be mobile. Topology may change, often due to mobility and/or node failures.	The nodes in the infrastructure are fixed. Terminals can be mobile. However, the topology of the infrastructure seldom changes.
Nodes	The terminal nodes used by the users can also relay the traffic of other nodes.	The nodes in the infrastructure convey data between the source and destination. Their usage as terminal stations or host computers is

	Ad Hoc Network	Cellular network
		not ordinary. The terminal nodes do not relay traffic from others.
Links	The links are mostly wireless. An end-to-end connection can be made through multiple wireless links, i.e. hops.	The terminal nodes access the Infrastructure via a wireless link. The links in the infrastructure can be wireless Or non wireless.

One example of Ad Hoc is an architecture using 802.11 cards. In these architecture 802.11 nodes reach other nodes they need to communicate with using their neighbors. Nodes that are close to each other discover their neighbor's nodes .When nodes need to communicate with other nodes it sends the traffic to its neighbors and these neighbors pass it along towards their neighbors and so on. This repeats until the destination of the traffic is reached. Such architecture requires that every node in the network play the role of a router by being able to determine the paths that packets need to take in order to reach their destinations. Networks that support the Ad Hoc architecture are typically called wireless Ad Hoc networks or mobile Ad Hoc networks (MANET).(Çayırcı & Rong, 2009; Mishra, 2008)

2.3 Mobile Ad Hoc Network Challenges

In 1996, The Internet Engineering Task Force (IETF) set down a MANET workgroup, and their goal is to standardize IP routing protocol functionality suitable for wireless routing applications within both static and dynamic topologies. A mobile Ad Hoc network (MANET) group has been formed within IETF. The main focus of this group is to support MANET with hundreds of routers and solve challenges in this kind of network. In Ad Hoc network, nodes are dynamic and random movement. It must deal with limitations such as high power consumption, low bandwidth, high error rates and arbitrary movements of nodes, because an Ad Hoc network hasn't any fixed infrastructure. When two mobile nodes are within the cover range of communicating each other, they can communicate directly (Jin & Jin, 2008; Thales, 2007).

Refereeing to (Çayırcı & Rong, 2009) there are many more application areas for Ad Hoc networks. These applications can be realized by noticing challenges specific to wireless Ad Hoc networking. Some of these challenges are briefly explained below:

I. The Wireless Medium

In Ad Hoc networks at least some of the communication links are established through the wireless medium. The wireless medium is differentiated from other media mainly by the following:

a) The wireless medium is more error prone; for example, the bit error rates (BERs) in the wireless medium can be 107 times higher than fiber optic.

b) The capacity of the wireless medium is limited. When a guided medium is used, it is possible to increase the capacity by laying new lines but in the wireless medium, the range is limited and cannot be extended.

II. Interference, Hidden Terminals and Exposed Terminals

Free transmission in broadcast media may lead to the time overlap of two or more packet receptions called collision or interference. However, in wireless medium the hidden terminal prevent the collision. For example, transmissions of a node can be interfered with another terminal that can't be detected and prevent the collision, but it will be a destination to other terminals.

Another event that has an impact on the efficiency of Ad Hoc protocols especially for medium access control is called the exposed terminal .That mean source (A) may not start its transmission to destination (C) because avoiding the collision of source (B) to destination (D). Here in this example source (A) is an exposed terminal.

III. Mobility , Node failures , Self-forming ,Self-configuration, Topology Maintenance, Routing and self-healing

The challenges starting by wireless medium are increased by the mobility of nodes which act as both terminals and routers. In Ad Hoc node can be both a

terminal and router. Therefore, when nodes change their location or fail the topology of MANET may change.

Refereeing to (CCapkun, Hubaux, & Buttya´n, 2006; djenouri, khelladi, & Badache, 2005; Ghaffari, 2006; Mishra, 2008) most Ad Hoc networks are self-forming, self-healing, which means they can autonomously form a network and adapt to the changes in the network. The efficiency in these self-forming and self-healing close and related to an availability .There is an exchange between the topology maintenance cost and the efficiency of self-forming and self-healing algorithms. As the resolution and the accuracy of the topology data increase, more efficient self-forming and self-healing algorithms can be developed.

However, this also indicates an increase in the topology maintenance cost. For example the number of data packets transferred for topology maintenance, which is also dependent on the frequency of topology changes. The topology maintenance process can be classified according to the following criteria:

a) Traffic generated for monitoring purposes: active or passive.
b) Monitoring frequency: on demand (event-driven) or continuous (time-driven).
c) Replication of information: centralized or distributed.

IV. Node Localization and Time Synchronization

In a network where there is no fixed infrastructure, node localization and time synchronization become more challenging.

V. End-to-end Reliability and Congestion Control

Topology changes are always coming up in Ad Hoc networks and the wireless medium is error prone .Hence, the end-to-end connection oriented transmission control protocol (TCP) which is based on the approach that the packet losses during transfer are mostly due to congestion .So that will not fit well with Ad Hoc networks.

2.4 Mobile Ad Hoc Security

Referring to (Sarkar *et al.*, 2008) Security has become a main concern to provide protected communication between mobile nodes in a hostile or an unfriendly environment. Unlike the wired line networks, the unique characteristics of mobile Ad Hoc networks pose a number of non small challenges to security design, such as open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. These challenges clearly make a case for building multi fence security solutions that achieve both broad protection and desirable network performance.

Any system that has to be protected might have weaknesses or vulnerabilities, some or all of which may be targeted by an attacker. Hence, one approach to designing security mechanisms for systems is to look at the threats that the system faces and the attacks possible given the vulnerabilities. The designed security mechanisms should then ensure that the system is secure in the beam of these threats, attacks, and vulnerabilities.(Anjum & Mouchtaris, 2007; YianHuang & Lee, 2003)

2.4.1 Threats

Referring to (Anjum & Mouchtaris, 2007) threats are the means through which the ability or goal of an agent to adversely affect an automated system, facility or operation can be clear . All methods or things used to exploit a weakness in a system, operation, or facility form threat agents. Examples of threats include hackers, unhappy employees, industrial spying, national intelligence services, and criminal organizations. We consider three main categories of threats:

I. Amateur Adversary

Amateur adversaries can launch simple attacks such as wireless sniffing or denial of service. Some examples of amateur adversaries are script kiddies or hobbyist hackers.

II. Professional Adversary

A professional adversary can launch more complicated attacks such as layer 2 hijacking, man-in-the-middle attack, or Sybil attack. Crime syndicates or terrorist organizations can be considered as professional adversaries

III. Well-funded Adversary

A well-funded adversary does not have any interest on money. Such an adversary can launch very complicated attacks such as rushing attacks, wormhole attacks, as well as capture devices that are part of the network. Foreign intelligence services can be considered as an example of a well-funded adversary.

2.4.2 Vulnerabilities

Vulnerabilities are any hardware, firmware, or software flaw that leaves an information system open for potential exploitation. The exploitation can be of various types, such as gaining unauthorized access to information or disrupting critical processing.

Referring to (Anjum & Mouchtaris, 2007; Johston & Walker, 2004; Mishra, 2008; Sarkar et al., 2008; Wang, Wang, & Han, 2009) the wireless Ad Hoc nature of MANET brings new security challenges to the network design .Wireless networks are generally more vulnerability to information and physical security threats than fixed wired networks .Vulnerability of channels and nodes absence of infrastructure and dynamically changing topology make Ad Hoc networks security difficult task. Transferring messages via wireless channels allow message eavesdropping and injection.

Referring to (Anjum & Mouchtaris, 2007; Çayırcı & Rong, 2009; Johston & Walker, 2004) mobile wireless environment has introduced new types of computational and communication activities that rarely appear in wired environments such as illustrated below:

a) Users trying to be stingy about communication because of slower links, limited bandwidth, higher cost and battery power limit. So the mechanisms like disconnect operation depend on location appear.
b) Application and services in a mobile wireless network can be week.
c) In mobile Ad Hoc are often proxies and software agents running in intermediate nodes to achieve performance.
d) In MANET is difficult to obtain enough audit data.
e) Mobile networks do not communicate as frequently as their wired counter parts .This is can be a problem for intrusion detection systems attempting to define normality for anomaly detection.
f) Use of wireless links makes these networks very vulnerable to attacks ranging from passive eavesdropping to active interfering. An attacker just needs to be within radio range of a node in order to intercept network traffic.
g) Constraints existing in Ad Hoc networks also add to vulnerabilities. For example networks have limited computational ability, as low processor and small memory size. The limitations on power usage are another major constraint .That can let attacker to lunch denial of service (DoS) Attacks on battery of legitimate node.

h) The node in MANET are vulnerable to being physically captured which may result in the cryptographic keys being exposed.

i) Another problem with wireless Ad Hoc environments that could not distinguish between malicious behavior and acceptable behavior. For example. Important levels of packet dropping may be result of the physical characteristics of the wireless links .These packets drops may be not necessary to contain attacks .Nodes may appear and disappear from the network not because they are being attacked but because of mobility and power constraints.

j) In addition, Ad Hoc networks suffer from vulnerabilities current in wired network such as passive eavesdropping, spoofing, replay, or denial of service .Due to the topology of Ad Hoc network is defined by geographical position, they don't have a clearly defined physical boundary defense.

2.4.3 Attacks

Referring to (Anjum & Mouchtaris, 2007; Wu, Chen, Wu, & Cardei, 2006) attacks against the network may come from malicious nodes that are not part of the network and are trying to join the network without authorization. Such nodes are typically called outsiders. Networks are typically protected from malicious outsiders through the use of cryptographic techniques. Such techniques allow nodes to securely verify the identity of other nodes and can therefore try to prevent any harm being caused by the malicious outsiders. We also consider attacks from nodes that are authorized to be part of the network and are typically called insiders. Insider nodes may launch attacks because they have been

compromised by an unauthorized user (e.g. hacker) through some form of remote penetration, or have been physically captured by a malicious user.

Ad Hoc attacks can be classified into active and passive attacks. A passive attack does not inject any message, but it listen to the channel. A passive attack tries to discover valuable information and does not produce any new traffic in the network. An active attack message directly inserted into the networks such attacks make actions such as replication, modification, and deletion of exchanged data. In Ad Hoc networks, active attacks are impersonation, Denial of Services (DOS), and disclosure attack. Adversaries attempt to change the behavior of the operational mechanisms in active attacks while they are subtle in their activities in passive attacks. (Sarkar *et al.*, 2008; Wu *et al.*, 2006)

The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks, according to the attack means see table 2.2

Table 2.2: Security Attacks classification (Wu *et al.*, 2006)

Passive Attacks	Eavesdropping, traffic analysis, monitoring
Active Attacks	Jamming, spoofing, modification, replaying, DoS

2.4.3.1 Passive Attacks

A passive attack obtains data exchanged in the network without disrupting the operation of the communications. In passive attacks attackers are typically secret, i.e. hidden, and tap the communication lines to collect data. Passive attacks can be grouped into eavesdropping and traffic analysis types as illustrated in figure 2.3

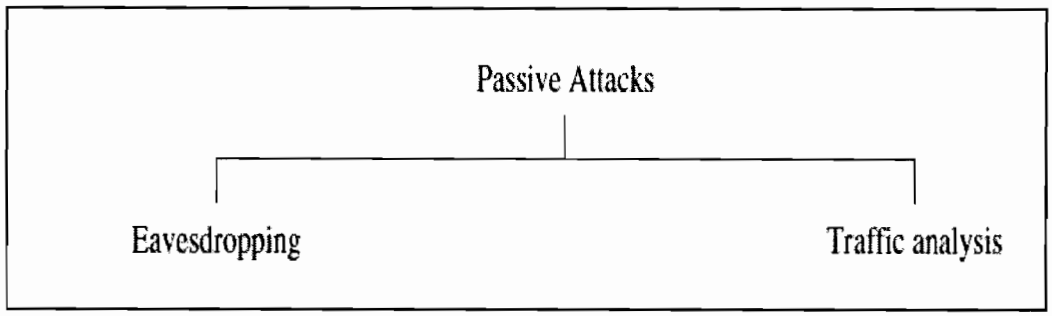


Figure 2.3 :Passive Attacks(Çayırcı & Rong, 2009)

I. Eavesdropping

Classified data can be eavesdropped by tapping communication lines, and wireless links are easier to tap. Therefore, wireless networks are more susceptible to passive attacks. In particular when known standards are used and plain data, for example not encrypted, are sent wirelessly. An adversary can easily receive and read the data and listen to or watch audio–visual transmissions. Eavesdropping is a very easy passive attack in the radio environment. When one sends a message over the wireless medium, everyone prepared with a suitable transceiver in the range of the transmission can potentially decode the message and obtain sensitive information. The sender or the intended receiver has no means of detecting if the

transmission has been eavesdropped. However, this attack can be prevented by using an encryption scheme at the link level to protect the transmitted data. Of course, this requires efficient key distribution strategies; so that keys for encrypting the transmitted traffic can be transmitted to all nodes. Attacks against privacy may start with attacks against anonymity. Adversary attackers first need to know which node serves which individual and for what purpose. Similarly, the adversary needs to know which data packet is coming from which node. After this is achieved, the collected data may become more important.(Çayırcı & Rong, 2009; djenouri et al., 2005; Mishra, 2008; Vinayakray, 2002)

II. Traffic Analysis

As well as the content of data packets, the traffic pattern may also be very valuable for adversaries. For example, important information about the networking topology can be derived by analyzing traffic patterns. In Ad Hoc networks, especially in sensor networks, the nodes closer to the base station, for example the sink, make more transmissions than the other nodes because they relay more packets than the nodes farther from the base station. Traffic analysis can also be used to organize attacks against anonymity. Detecting the source nodes for certain data packets may also be a target for adversaries. This information helps to detect the location of events, weaknesses, capabilities and the functions or the owners of the nodes.

One of the following techniques may be used for traffic analysis:

a) Traffic analysis at the physical layer.

b) Traffic analysis in MAC and higher layers.

c) Traffic analysis by event correlation.

d) Active traffic analysis.

2.4.3.2 Active Attacks

Referring to (Çayırcı & Rong, 2009; Wu *et al.*, 2006; YianHuang & Lee, 2003) in active attacks, an adversary actually affects the operations in the attacked network. This effect may be the objective of the attack and can be detected. For example, attacks make actions such as replication, modification, and deletion of exchanged data. Sometimes the adversary tries to stay undetected, aiming to gain unauthorized access to the system resources or threatening confidentiality and or integrity of the content of the network. We group active attacks into four classes, as shown in Figure 2.4.

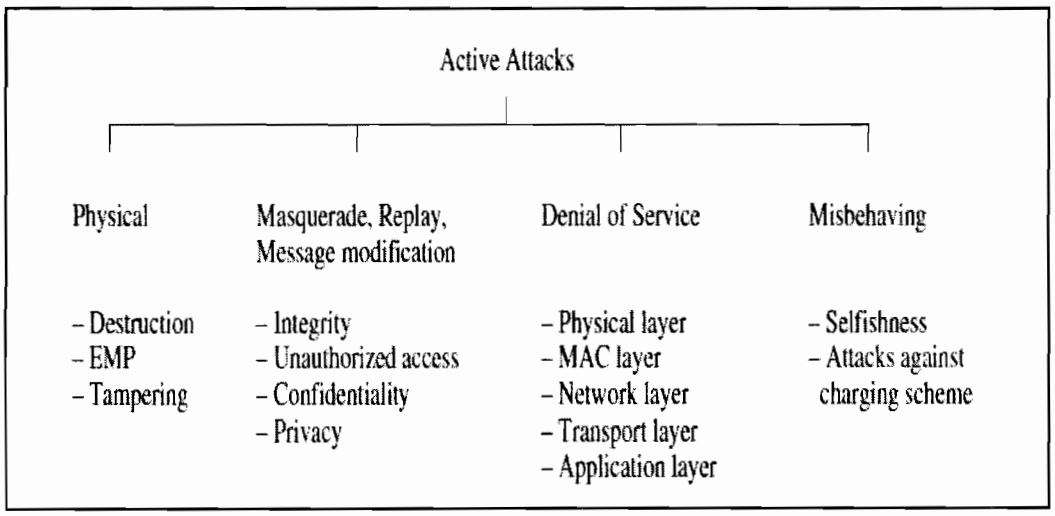


Figure 2.4: Active Attacks(Çayırcı & Rong, 2009)

I. Physical Attack

An adversary may physically damage hardware to terminate the nodes. This is a security attack that can also be considered to fall in the domain of fault tolerance, which is the ability to provide networking functionalities without any interruption due to node failures.

II. Masquerade, Replay and Message Modification

A masquerading node acts as if it is another node. Messages can be captured and replayed by masquerading nodes. Finally, the content of the captured messages can be modified before being replayed. Various scenarios and threats can be developed based on these approaches.

III. Denial-of-Service Attacks

A denial-of-service (DoS) attack mainly targets the availability of network services. A DoS is defined as any event that reduce a network's capacity to perform its expected function correctly or in a timely manner. We will review the main important scenario in DoS such as DoS against Routing Schemes .In this attack DoS will attack network layer for Ad Hoc network protocols. These attacks generally fall into one of two categories routing disruption attacks or resource consumption attacks. Routing disruption attacks aim to make the routing scheme dysfunction, making it unable to provide the required networking services. The goal of resource consumption attacks is to consume network resources such as bandwidth, memory, computational power and energy. Both are denial-of-service attacks and examples of them are listed below:

a) **Spoofed, altered or replayed routing information:**

Routing information exchanged among nodes can be altered by malicious nodes to have a detrimental effect on the routing scheme.

b) **Hello flood attack**

A malicious node may broadcast routing or other information with high enough transmission power to convince every node in the network that it is their neighbor. When the other nodes send their packets to the malicious node, those packets are not received by any node.

c) **Wormhole attack**

Refereeing to (Kargl & Schoch, 2007)a malicious node can eavesdrop or receive data packets at a point and transfer them to another malicious node, which is at another part of the network, through an out-of-band channel. The second malicious node then replays the packets. This makes all the nodes that can hear the transmissions by the second malicious node believe that the node that sent the packets to the first malicious node is their single-hop neighbor and they are receiving the packets directly from it. For example, the packets sent by node A as shown in Figure 2.5 are also received by node w1, which is a malicious node. Then node w1 forwards these packets to node w2 through a channel which is out of band for all the nodes in the network except for the adversaries. Node w2 replays the packets and node f receives them as if it was receiving them directly from node a. The packets that follow the normal route, i.e. a-b-c-d-e-f, reach node f later than those conveyed through the wormhole and are therefore dropped because they do more hops – wormholes are

typically established through faster channels. Wormholes are very difficult to detect and can impact on the performance of many network services such as time synchronization, localization and data fusion.

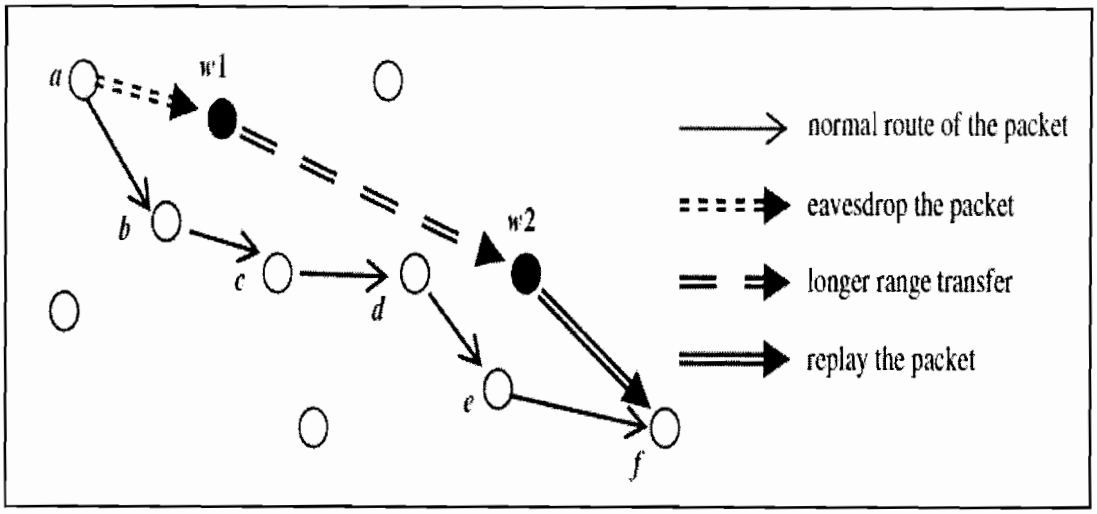


Figure 2.5: Wormhole Attack(Çayırcı & Rong, 2009)

d) Black hole attack

A malicious node may drop all the packets that it receives for forwarding. This attack is especially effective when the black hole node is also a sink hole. Such an attack combination may stop all the data traffic around the black hole.

e) Sybil attack

A single node presents multiple identities to the other nodes in the network. This reduces the effectiveness of fault-tolerance schemes and poses a significant threat to geographic routing protocols. Apart from these services it may also affect the performance of other schemes such as misbehavior

detection, voting-based algorithms, data aggregation and fusion and distributed storage.

f) Rushing attack

An attacker disseminates route request and reply messages quickly throughout the network. This suppresses any later legitimate route request messages, i.e. nodes drop them, because nodes suppress the other copies of a route request that they have already processed.

Referring to (Wu *et al.*, 2006) attacks can also be classified according to network protocol stacks. Table 2.3 shows an example of a classification of security attacks based on protocol stack; some attacks could be launched at multiple layers.

Table 2.3: Security Attacks on Protocol Stack (Wu *et al.*, 2006)

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

2.4.4 Security Goals

Referring to (Çayırcı & Rong, 2009; Wang *et al.*, 2009; YianHuang & Lee, 2003; Yu, Zhang, Song, & Chen, 2005) (Papaleo, 2007) in short, the goal of security is

to provide security services to defend against all the kinds of threats. The Security services include the following:

a) **Authentication:** Ensures that the other end of a connection or the creator of a packet is the node that is claimed.

b) **Access control:** prevents unauthorized access to a resource.

c) **Confidentiality**: protects overall content or a field in a message. Confidentiality can also be required to prevent an adversary from undertaking traffic analysis.

d) **Privacy**: prevents adversaries from get information that may have private content .The private information may be obtained through the analysis of traffic patterns, i.e. frequency, source node, routes, etc.

e) **Integrity**: ensures that a packet is not modified during transmission.

f) **Authorization**: authorizes another node to update information (import authorization) or to receive information (export authorization). Typically, other services such as authentication and integrity are used for authorization.

g) **Anonymity**: hides the source of a packet or frame. It is a service that can help with data confidentiality and privacy.

h) **Non repudiation**: proves the source of a packet. In authentication the source proves its identity. Non repudiation prevents the source from denying that it sent a packet.

i) **Freshness**: ensures that a malicious node does not resend previously captured packets.

j) **Availability**: mainly targets DoS attacks and is the ability to sustain the networking functionalities without any interruption due to security threats.

I. **Resilience to attacks**: required to provide the network functionalities when a portion of nodes is compromised or destroyed.

2.5 QualNet Simulation

Refereeing to (Hogie, 2007; Mishra, Nadkarni, Patcha, & Tech, 2004; Otrok, Paquet, Debbabi, & Bhattacharya, 2007) in their survey about the best simulation are using in testing MANET security attacks , they recommend QualNet as the best commercial simulation for test intrusion with Ad Hoc wireless environments. QualNet simulation is a commercial Ad Hoc network simulator based on the GloMoSim core. It extends the GloMoSim offer by bringing support, a decent documentation, and a complete set of user-friendly tools for building scenarios and analyzing simulation output. QualNet also extends the set of mobility models and protocols supported by the initial GloMoSim distribution. As it is built on top of GloMoSim, QualNet is written in Parsec. QualNet Developer is a tool created by Scalable Network Technologies (SNT) to improve the design, operation, and management of networks. QualNet Developer is a full suite of tools for modeling large wired and wireless networks. It uses simulation and emulation to guess the behavior and performance of networks with thousands of nodes.

Moreover QualNet Developer enables users to:

a) Design new protocol models.

b) Optimize new and existing models.

c) Design large wired and wireless networks using SNT-provided or user-designed models.

d) Analyze the performance of networks and perform "what-if" analyses to optimize them.

e) Perform cross-layer optimization of wireless network stacks.

The key features of QualNet Developer that enable the creation a virtual network environment (VNE) are:

I. Speed

QualNet Developer can support real-time speed to enable software-in-the-loop, network emulation, and hardware-in-the-loop modeling. Faster speed enables model developers and network designers to run multiple "what-if" analyses by varying model, network, and traffic parameters in a short time.

II. Scalability

QualNet Developer supports thousands of nodes by taking advantage of the latest software, hardware and parallel computing techniques. The base QualNet Developer product can run two threads simultaneously to benefit from the latest dual-core processors from Intel and AMD. Advanced versions of QualNet Developer can run on cluster, multi-core, and multi-processor systems to model large networks with high fidelity.

III. Model loyalty

QualNet Developer uses highly detailed standards-based implementation of protocol models. It also includes advanced models for the wireless environment to enable more accurate modeling of real-world networks.

IV. Portability

QualNet Developer and its library of models run on a vast array of platforms, including Linux, Solaris, Windows XP, and Mac OS X operating systems, distributed and cluster parallel architectures, and both 32- and 64-bit computing platforms. Users can develop a protocol model or design a network in QualNet Developer on their desktop or laptop computer and then transfer and run it on a powerful multi-processor Linux server to perform capacity, performance, and scalability analyses.

V. Extensibility

QualNet Developer can connect to other hardware and software applications, such as real networks, and third party visualization software.

2.5.1 QualNet Architecture

Figure 2.6 illustrates the QualNet Developer architecture. A high-level description of the various components is provided below:

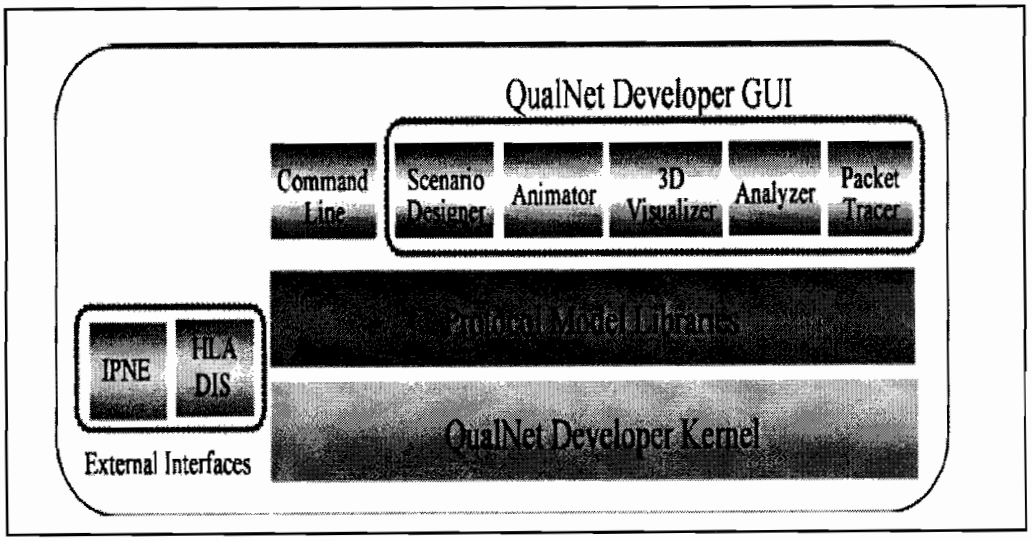


Figure 2.6: QualNet Architecture source from: http://www.scalable-networks.com

2.6 Related Work

Referring to (Erciyes, Dagdeviren, & Cokuslu, 2006; Otrok *et al.*, 2007; Schoch, Feiri, & Frank Kargl, 2008) different simulations used with testing intrusions in mobile Ad Hoc system like NS-2 , OPNET and GloMoSim ,but using QualNet support some features that consider very important to test MANET security . 6.3% of the researchers use QualNet network simulator software, which has been developed by Scalable Network Technologies (SNT). QualNet modifications, with respect to other network simulators are in terms of scalability, accuracy, and speed. Thus, researchers can model large networks using QualNet, getting better vision into how the network behaves as it scales from 10 to 10,000 devices. Moreover, its results are near to real live network. Finally, QualNet has successfully simulated real-time simulation of mobile communication networks with over 2000 wireless radios with amazing accuracy.

Using different simulation provide us a good comparative result between them. Some researchers used NS-2 and OPNET in their experiments to analysis the security performance in wireless Ad Hoc environment.

It is stated by (Garrido, Malumbres, & Calafate, 2007) they make experiment on MANETs network to make the evaluation of 802.11e model using NS-2 and OPNET simulation tools. They focus on performance evaluation of IEEE 802.11e on MANETs in both stationary and mobile scenarios. They describe the tested experiment in details and the differences between the two simulation tools NS-2 and OPNET. With comparing OPNET with NS -2 there are results could be used to

evaluate the performance of IEEE 802.11g/e .The results show that the modification are important to express critical differences and obtain similar results .The summary based on simulation results for the different MANET scenarios are that trend of all the metrics in both simulators were reliable, also in other experiment are different.

Referring to (Garrido, Malumbres, & Calafate, 2008) they make experiment on MANET environment using OPNET and compare theses results with another study using NS-2. Their study is a comparative study between two common network simulation tools, namely, NS-2 and OPNET Modeler; they have been carried out, involving several standing and mobile MANET system scenarios using IEEE 802.11g/e. Some important differences between them have reported, and the corresponding modifications to deal with each of them are presented. Results showed that the referred modifications are necessary in order to address such critical differences similar results. The conclusions based on the simulation results for the different MANET scenarios. From the results they could conclude that more comparisons between network simulators in general, and between Ns-2 and OPNET Modeler in particular, could be done. Finally, it will be interesting to develop a topology generator tool that is able to build scenarios for MANETs, and then could be able to export the topology to several network simulators (including NS-2 and OPNET Modeler). Alternatively, building another tool that allows importing the scenarios created for NS-2 to OPNET would also be useful.

Refereeing to (Sharma & Gupta, 2009) they simulated Black hole attacks in wireless Ad Hoc using QualNet Simulator and evaluated their effects on the network performance that measured the packet loss in the network and compare network performance with and without a black hole attack. The simulation is done on AODV (Ad Hoc on Demand Distance Vector) Routing Protocol. They chose AODV protocol because it is widely used and it is vulnerable to these attacks because of the mechanisms it employs. They had implemented Black hole attack in a QualNet simulator. For their simulations, they used CBR (Constant Bit Rate) application, UDP/IP, IEEE 802.11b MAC and physical channel based on statistical propagation model. The simulated network consists of 40 randomly allocated wireless nodes in a 1500 by 1500 square meter flat space. The node transmission range is 250 m power range. Random waypoint model is used for scenarios with node mobility. The selected pause time is 30 second.

In the result of their experiment with development in computing environments, the services based on Ad Hoc networks have been increased. Wireless ad hoc networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes. In their paper the effect of Packet Delivery Ratio, Throughput, End-to-End Delay and Jitter has been detected with respect to the variable node mobility. There is reduction in Packet Delivery Ratio, Throughput, E-E Delay, and Jitter. Moreover, in black hole attack all network traffics are redirected to a specific node or from the malicious node causing serious damage to networks and

nodes .The detection of black holes in Ad Hoc networks is still considered to be a challenging task.

2.7 Summary

In the above section, we have explained the concept of mobile Ad Hoc environments and their architecture. Issues and challenges in wireless Ad Hoc are huge and need to implement new policies to handle them. There are there natural approaches to network security protection through filtering, protection through assessment, and protection through detection. In this chapter we identify most the threats and vulnerabilities in MANET. In a brief discussion we discussed the varies type of attacks and the experiments those run on wireless Ad Hoc network to make a good assessment to protect our network . Moreover, we describe the reasons that we choose the simulator QualNet and its features with mobile Ad Hoc. In next chapter we are going to discuss the research methodology in this project.

CAHPTER THREE

RESEARCH METHODOLOGY

3.1 Research Methodology

This chapter is describing the methodology that was applied in the project based on our understanding. There are several methodologies in Information technology that can be applied .We can Use different methodologies for different kind of problems .In Our Experiment on mobile Ad Hoc security the element of testing and simulation are involved ,the methodology that we are choosing should be able to simulate our test bed. We are using Simulation model by Turban and Aronsson (1998) because we want to run the simulation for testing the values of the model and evaluate the results(Turban,1998) .

The experiment that will be setting up used the simulation model which consists of steps as shown in figure 3.1. Simulation involves setting up a model of area system and conducting repetitive experiments on it.

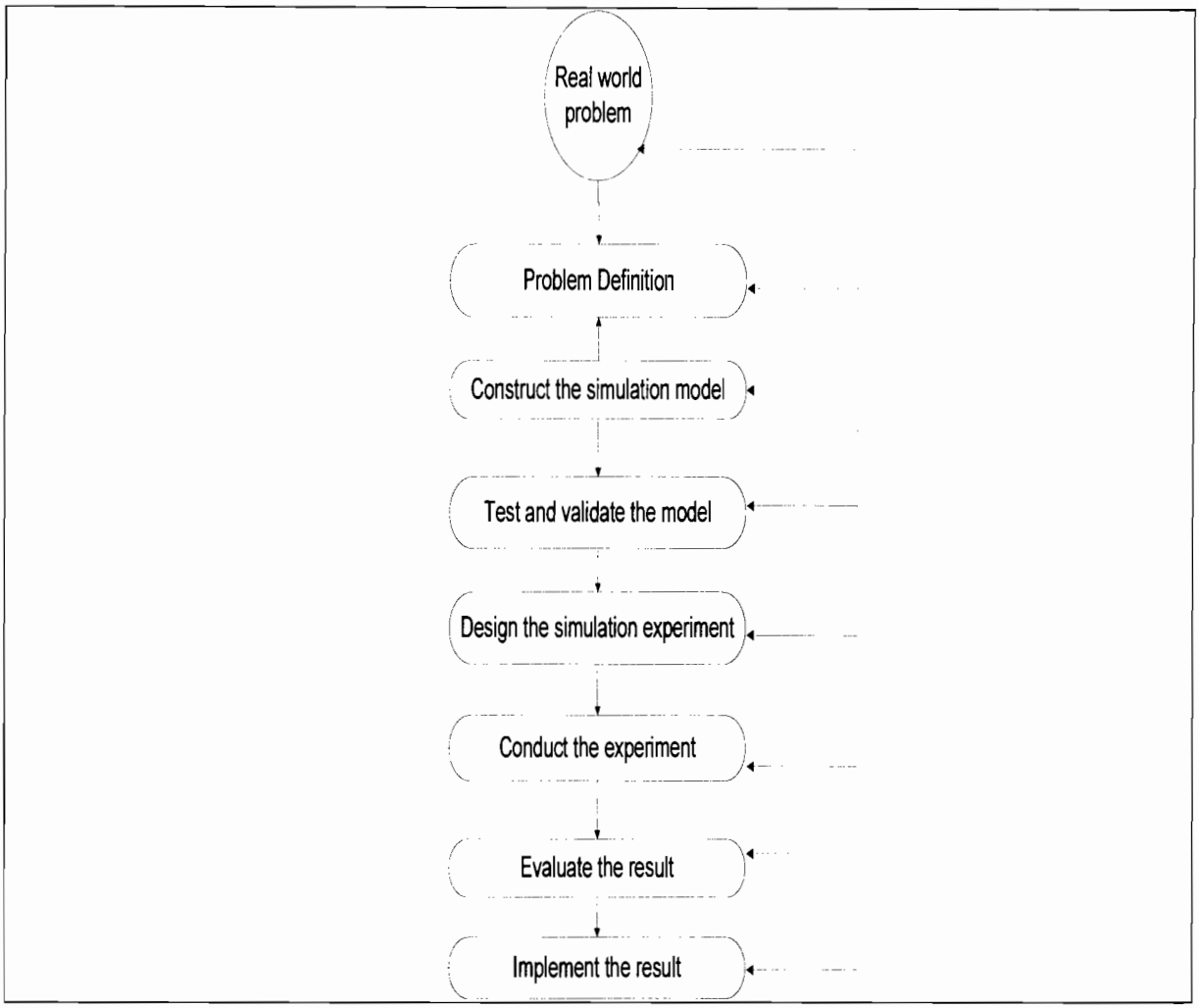


Figure 3.1 : Simulation Model (Turban, 1998)

3.1.1 Problem Definition

There are many issues and challenges in Mobile ad hoc security .One of the main vulnerabilities of MANETs comes from their open peer-to-peer structure .unlike wired networks which have committed routers; each node in MANET may function as a router and forward packets to other nodes. Malicious attackers can expose this gap and can access to wireless channel and attack the nodes .There is no clear line of

defense in MANETs from the security design .There is no well-defined infrastructure where we may deploy a single security (Sarkar *et al.*, 2008) . So we used QualNet Simulation as detection simulation to detect intrusions such eavesdropping and wormhole attacks ,and evaluate these attacks and the performance of the network within these attacks.

3.1.2 Construction the simulation model

In construction of the model testing, it is required to prepare a test bed and determining the setup for the various component .In addition to that ,we have to declare the relationship between all the variables in the design. For evaluating the attacks in mobile Ad Hoc network, we install QualNet 4.5 simulation in test pc running windows XP as operating system.

There are some requirements for QualNet 4.5 to run on PC, the table 3.1 shows the minimum requirements to install QualNet 4.5 for windows.

Table 3.1: Minimum requirements to install QualNet 4.5 for Windows

Item	**Requirements**
CPU	x86 compatible (including Intel Core Duo, Pentium, Xeon, and AMD Athlon). Or AMD64 compatible (including AMD Opteron, Athlon 64, Intel Core 2 Duo, and Pentium/Xeon EM64T).
Memory	• 512 MB for simulations of networks with up to 100 nodes.

Item	Requirements
	• 768 MB for simulations of networks with up to 250 nodes. • 1 GB for simulations of networks with up to 1000 nodes.
Disk	500 MB free disk space.
Java	Sun Java™ 2 SDK, Standard Edition, version 1.4.2 or higher
C++ compiler	Microsoft Visual C++ .NET 2002 or higher

In our experiment we run two kinds of scenarios to test the attacks:

I. First Scenario :

The scenario is testing eavesdropping within mobile Ad Hoc network. In the first scenario our construction consist of 6 nodes and then change and build new construction consist of 25 and 40 nodes . The environment on figure 3.2 shows the test bed setup for first scenario.

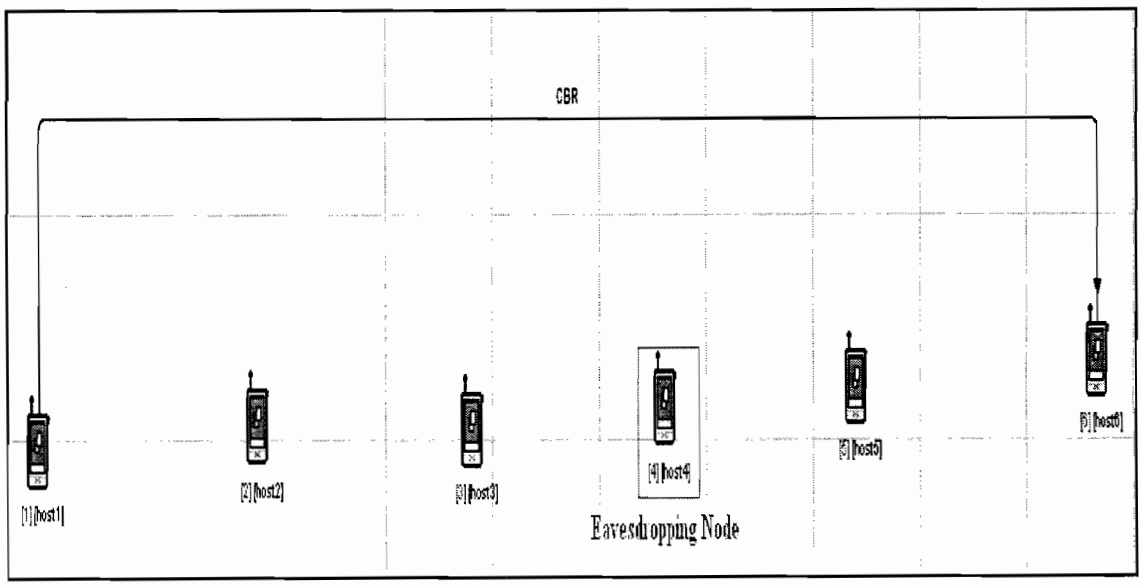


Figure 3.2: Test Bed Setup for Eavesdropping

II. Second scenario :

In this scenario test bed setup was build for wormhole attack on mobile Ad Hoc network .Our setup test MANET with and without the attacks. Referring to (Anjum & Mouchtaris, 2007) a wormhole attack typically requires the presence of at least two colluding nodes in an Ad Hoc network .The malicious nodes need to be geographically separated to allow that attack to be effective. In this attack, a malicious node captures packets from one location and "tunnels" these packets to the other malicious node, which is assumed to be located at some distance. So we need to isolate two nodes or more to test this attack .The figure 3.3 show test bed for second scenario.

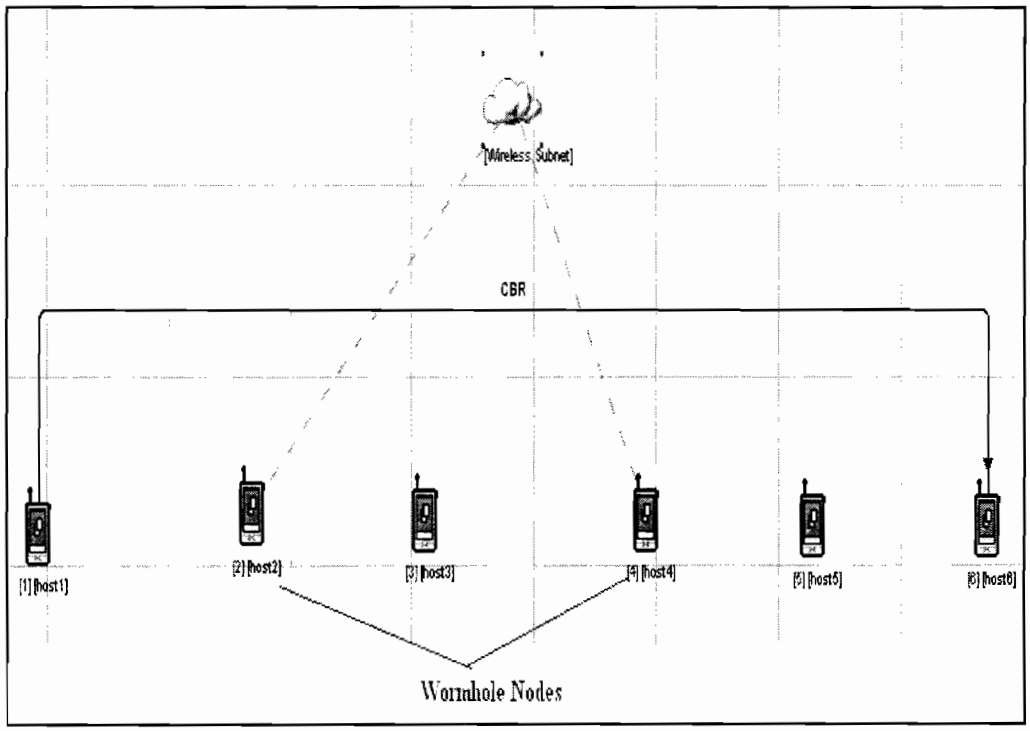


Figure 3.3: Test Bed Setup for Wormhole

In this figure we run this scenario on 6 nodes after that we increase the number of the nodes to 25 and 40. This scenario runs frequently on three different topologies. The experiment design will describe more in details in design section of the experiment.

3.1.3 Testing and validating the model

In this section ,we are describing the structural testing that use in this experiment to test the simulation study .In this section we are looking to the relationship and their correct configuration parameters of the simulation .The structural system testing techniques provide the facility for determining the implemented configuration and its relationship of parts function; so that they can perform the intended tasks .In this section we review the model design depending on our documentation manuals to see the configuration of the variables and the errors .QualNet 4.5 is simulation has been configured to be detection tool against passive and active attack by change some parameters of the nodes in the experiment. We use this simulator to assessment the attacks and conduct results to protect the network .The goal is to test both the first and second scenario of this experiment, and test their implementation.

3.1.4 Design of the experiment

We have implemented eavesdropping and wormhole attack in a QualNet 4.5 simulator. In first scenario we used FTP (File Transfer Protocol) application, CBR (Constant Bit Rate) application and TELNET application .We also used IEEE 802.11b MAC and physical channel based on statistical propagation model. The simulated network consists of 6, 25, and 40 randomly allocated wireless nodes in a

1500 by 1500 square meter flat space. The node transmission range is 250 m power range. Mobility mode is used for this scenario. The selected pause time is 30 s. The size of data payload is 512 bytes. In this scenario we take 6, 25, and 40 nodes in which of these topologies that we will change some nodes of them to be eavesdropping. Mobility of nodes configured and changed randomly from 10mps to 30 mps.

Table 3.2 as shown below illustrated the experimental design for the simulation phase one.

Table 3.2: Experimental design for first scenario

Run	No. Nodes	FTP	CBR	TELNET	No. Eavesdropping
1	6	X	0	0	1
2	6	0	X	0	1
3	6	0	0	X	1
4	25	X	0	0	1
5	25	0	X	0	1
6	25	0	0	X	1
7	40	X	0	0	1
8	40	0	X	0	1
9	40	0	0	X	1

In second scenario, we used IEEE 802.11b MAC and physical channel based on statistical propagation model. In addition we used CBR (Constant Bit Rate) application to communicate between some of the nodes. The simulated network consists of 6, 10, and 25 randomly allocated wireless nodes in a 1500 by 1500 square meter flat space. The node transmission range is 250 m power range. Mobility mode is used for this scenario too. The selected pause time is 30 s. The size of data payload is 512 bytes. In this scenario we take 6, 25, and 40 nodes in which of these topologies we will change some nodes of them to be as malicious wormhole nodes. Table 3.3 as shown below illustrated the experimental design for the simulation phase two.

Table 3.3: Experimental design for second scenario

Run	No of nodes	No of wormhole nodes
1	6	0
2	6	2
3	25	0
4	25	3
5	40	0
6	40	4

3.1.5 Conducting the experiments

In this section we run the experiments and collected the output of it. First of all, these experiments run the first scenario depending on the table 3.2. Second experiments run the second scenario depending on table 3.3. In next chapter we will explain in details all the outputs that conduct from these experiments. Moreover we will present the experiment specification and graphics statistics.

3.1.6 Evaluation the Results

In this section we used QualNet 4.5 Analyzer to analyze the results that have been conducted from the previous section. QualNet analyzer shows us graphical results for all the experiments that run on the simulation model. The results have been generated from the experiments will be analyzed to see the analysis and performance testing in details in chapter four.

3.2 Conclusion

We have discussed the simulation model that was used in our project that was suggested by (Turban, 1998).The six steps in the simulation model are :

i. Problem definition.
ii. Construction of the simulation model.
iii. Testing and validation of the model
iv. Designing the experiment.
v. Conducting the experiment.
vi. Evaluating the model.

The objectives of the experiments are conducting and will be explained in details in chapter four.

CHAPTER FOUR

FINDING AND ANALYSIS OF DATA

4.1 Introduction

An Ad Hoc network is a collection of nodes that do not rely on a fixed and predefine infrastructure to keep the network connected. So the functioning of Ad Hoc networks is dependent on the trust and co-operation between nodes. Wireless Ad Hoc networks are usually vulnerable to different security threats attacks such as eavesdropping and wormhole. We made our simulations using QualNet Simulator 4.5 and determine theses attacks using the output of this simulator and evaluate the results of the experiments to compare the network performance with and without these attacks in the network.

Simulators are considered as the main tool in MANET for testing intrusion. Simulators help researchers to study the performance and the reliability of their algorithms and detections of attacks without using real mobile nodes. It potentially allows studying a large number of possible system configurations controlling the amount of complexity and realism included in the simulation model. It will give researchers a vision of how will work in reality and under different circumstances (Caro, 2003).

Refereeing to (Otrok *et al.*, 2007) 6.3% uses QualNet network simulator software, which has been developed by Scalable Network Technologies (SNT). QualNet modifications, with respect to other network simulators, are in terms of scalability,

accuracy, and speed. Thus, researchers can model large networks using QualNet, getting better vision into how the network behaves as it scales from 10 to 10,000 devices. Moreover, its results are near to real live network. Finally, QualNet has successfully simulated real-time simulation of mobile communication networks with over 2000 wireless radios with astonishing accuracy.

QulaNet simulation is the best choose for this project because of many facilities that contains .According to (Caro, 2003) QualNet appears as the best compromise in terms of number of pre-built components, modularity, scalability, and modifiability . He sees QualNet as an effective simulation framework on top of which we can build the complete simulation architecture for mobile ad hoc networks. Installation of QualNet 4.5.1 in windows is shown in appendix A in this project. Today, QualNet provides a readily-available simulation and emulation tool that can assess any network security protocols and evaluate their performance in experimental scenarios. A QualNet assessment can save a great deal of cost, and in many cases unrecoverable casualty loss, by reducing deployment expenses and fixing flaws or failures in proposed network security plans

4.2 Application to Research Questions

This study and the conduct output results answer the two research questions by implement the test bed scenario in QualNet 4.5 simulation. Question 1 asks how to determine likelihood of such an attack such as eavesdropping and wormhole in MANET. Question 2 asks how to evaluate the performance in MANET framework with and without some types of passive and active attacks using QualNet Simulator.

4.3 Eavesdropping Test

This scenario determine eavesdropping in MANET and analyze the output of the experiment .Refereeing to table 3.2 in chapter three in design section, the experiments were run by changing some compensations and modification of some nodes .In the first scenario to detect the eavesdropping in MANET , the experiment was conduct by using FTP (File Transfer Protocol) application, CBR (Constant Bit Rate) application and TELNET application .We used also IEEE 802.11b MAC and physical channel based on statistical propagation model. The simulated network consists of 6, 10, and 25 randomly allocated wireless nodes in a 1500 by 1500 square meter flat space. The node transmission range is 250 m power range. Mobility mode is used for this scenario. The selected pause time is 30 s. The size of data payload is 512 bytes. The experiment was run 13 times with different topologies using QualNet 4.5 GUI simulation .The results and the outputs was gathered and summarized in appendix B.

4.3.1 Eavesdropping Results

Referring to table B.1 in appendix section we can notify valuable information were extracting from the packets that were transmitted in the simulation network. Everyone equipped with a suitable transceiver in the range of the transmission can potentially decode the message and obtain sensitive information. In this section we are explained the output description of eavesdropping. The eavesdropped packets are output to a file, the format of which is described blew in Table 4.1. Moreover, as we noticed that in the project, the performance of the transfer packets remain the same within eavesdropping nodes or without eavesdropping nodes .The main concern in

eavesdropping attack is to expose the integrity of the environment and attack the privacy of the data .Eavesdropping might give an adversary access to secret information, violating confidentiality.

Table 4.1: Eavesdrop output format

Output Field	Description
Time	
ip_v	IP Version 4
ip_hl	IP Header
ip_tos	IP type of services
ip_len	Total length of the IP header
ip_id	IP identification
Flags	
ip_reserved	To distinguish SDR control packets
ip_dont_fragment	To handle fragmentation/offset whenever needed
ip_more_fragments	To handle fragmentation/offset whenever needed
ip_fragment_offset	To handle fragmentation/offset whenever needed
ip_ttl	IP time to live
ip_p	Transport protocol
ip_sum	Checksum
ip_src	Source IP
ip_dst	Destination IP

These formats help us to identify the transmissions packet between nodes in MANET .As we can see from table B.1 in Appendix B every run explore some delivery packets in same range . The experiments from treatment run 1 to treatment run 9 show secret information such as IP version, IP header, IP type of services, total length of the IP header, and IP identification as explained in table 4.2.

Table 4.2: Description of IP Header Eavesdrop output

Time:	ip_v	ip_hl	ip_tos	ip_len	ip_id
<simtime>1.003435170	<ipv4>4	5	0	540	3
<simtime>2.293415633	<ipv4>4	5	0	40	11

Those will help the attacker to know your network architecture .In the same table we can see that the rest of obtained output illustrate the architecture of the network flags in IP layer such as IP reserved , IP don't fragment ,IP more fragment , IP fragment offset , IP time to live , IP transport protocol , IP sum ,IP Source ,IP destination as explained in table 4.3.

Table 4.3: Description of IP flags Eavesdrop output

ip_fragment_offset	ip_ttl	ip_p	ip_sum	ip_src	ip_dst
0	63	6	0	192.0.0.11	192.0.0.17
0	62	6	0	192.0.0.11	192.0.0.17
0	61	17	0	192.0.0.1	192.0.0.8
0	64	17	0	192.0.6	192.0.0.1
0	63	17	0	192.0.0.6	192.0.0.1

As we noticed from table B.1 IP transport protocol can be very important to the attacker. Protocols types in the table can be (TCP /UDP /ICMP) or any kind of protocols. The intruder could lunch DOS and TCP SYN attack. So each eavesdropper has an IP protocol stack. If needed, it can be an internal adversary or compromised node to participate in network functions. Some of experiments conduct empty output and that refer to insufficient eavesdrop nodes.

4.4 Wormhole Attack Test

We used IEEE 802.11b MAC and physical channel based on statistical propagation model. In addition we use CBR (Constant Bit Rate) application to communicate between some of the nodes. The simulated network consists of 6, 25, and 40 randomly allocated wireless nodes in a 1500 by 1500 square meter flat space. The node transmission range is 250 m power range. Mobility mode is used for this scenario too. The selected pause time is 30 s. The size of data payload is 512 bytes. In this scenario were taking 6, 25, and 40 nodes in which of these topologies .we change some nodes of them to be as malicious wormhole nodes. In this attack adversaries can collude to transport routing and other packets out of band (using different channels). This will interfere with the operation of the routing protocols. So we add wireless subnet in the simulation to link between wormhole nodes and configure to be different channel. Referring to table 4.1 in chapter three in design section we run 6 experiments in QualNet 4.5 GUI simulation with and without wormhole .We can see all the graphic figures that conduct from the simulation in appendix C.

4.4.1 Wormhole Attack Results

Referring to table 3.3 in chapter 3 in run 2 experiment, we can see simple scenario where nodes 2 and 4 are connected to a wireless subnet enabled as wormhole subnet. One CBR application is configured from node 1 to node 6. 100 packets are sent from node 1 to node 6. We used wormhole all pass parameter in the wireless subnet. Figure C.1 show the Number of frames intercepted by the wormhole node. Figure C.2 show the Number of frames tunneled by the wormhole node. (Frames intercepted multiple times due to repetitive replay will not be tunneled.). Figure C.3 show Number of frames replayed by the wormhole node. In Figure C.4 we can see signals transmitted and those wormhole nodes have more signals transmitted than others, because the term "wormhole" refers to adversary carrying information and traveling faster than anyone else. Figure C.5 show that the broadcast packets received clearly in data link layer. We can see all the data with wormhole has unclear received packets.

We run the experiment using table 3.3 as a reference .We simulated MANET under many topologies and all the topologies show the same results as simple scenario as we can see in the figures from C.6 to C.16 with different combinations. In figure C.7 and C.13, we can notice there are some new results when changed the parameter wormhole (drop all packet). Figure C.7 and C.13 describe Number of frames dropped by the wormhole link (since the frames are classified as data packets, for example, with packet size greater than a threshold).

Moreover, in these experiments, the project evaluates the performance between the MANET environment with and without wormhole attacks. We used some metric vectors to compare the performance and the progress of the simulation test bed. The metrics used to evaluate the performance are given below:

i. Total byte received.

ii. Total packet received.

iii. Throughput (bit/s).

iv. Average end to end delivery

v. Average jitter.

We took all the results from previous results and compare them to obtain the differences and the similarities between them, and how these affect the network. The total receives bytes with and without wormhole will illustrate in Figure 4.1.

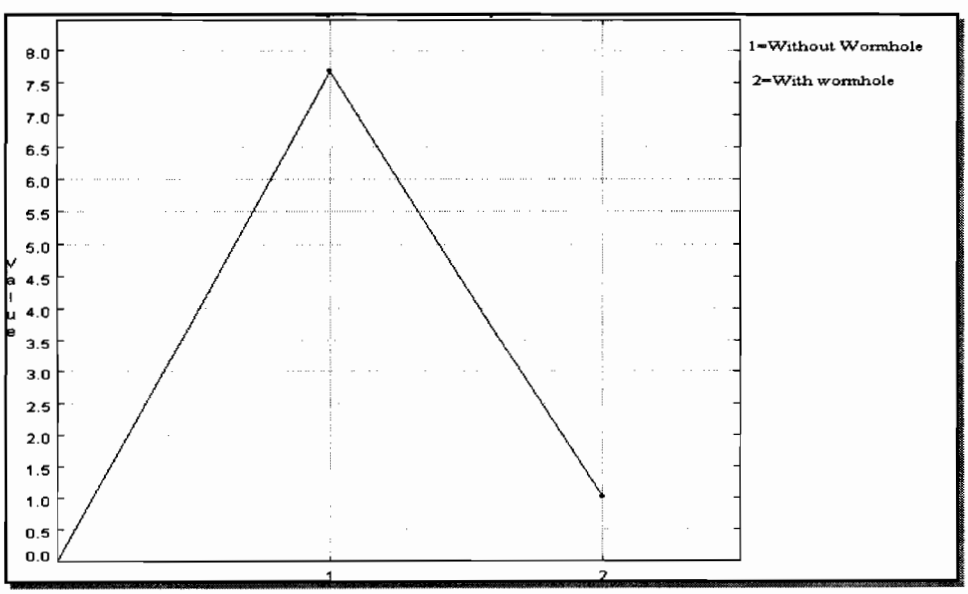


Figure 4.1: Total receive bytes with and without Wormhole

We can see that without wormhole many bytes receive by nodes within the experiments. Figure 4.2 will show the total receive but by packets.

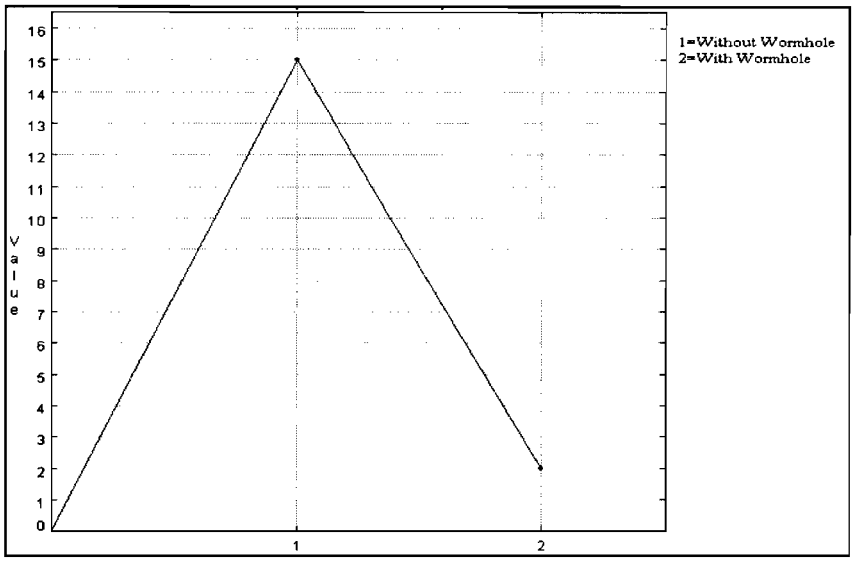


Figure 4.2: Total Packets Received with and without Wormhole

From the above figure we can see that value was 80% with wormhole but it decrease to reach 10%.Throughput is the average rate of successful message delivery over a communication channel as we can show in figure 4.3.

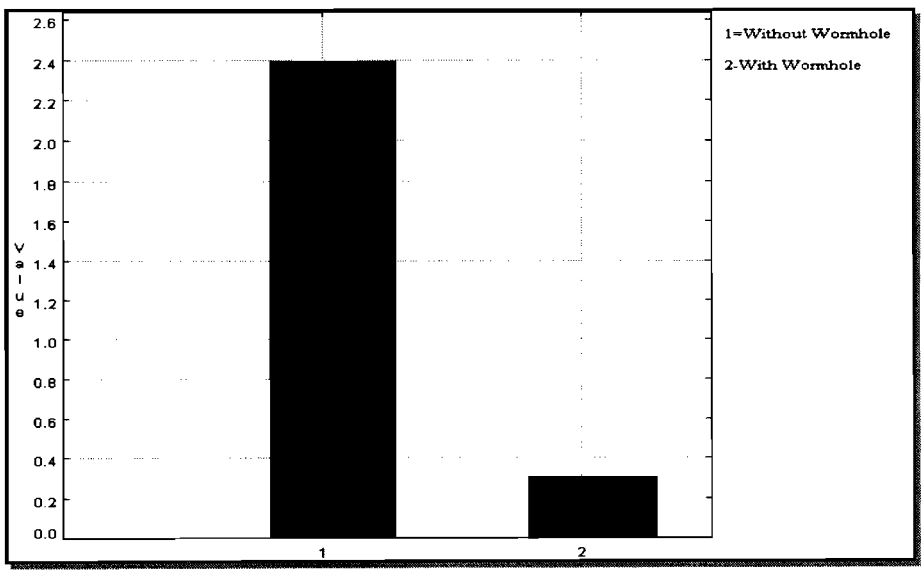


Figure 4.3: Throughput (bits/sec) with and without wormhole

Figure 4.3 shows the impact of the wormhole to the networks throughput. The throughput of the network also decreases due to wormhole effect as compared to that without the effect of wormhole attack. It can be observed from Figure 4.4 that, there is an increase in the average end-to-end delay without the effect of wormhole, as compared to the effect of wormhole attack. This is due to the immediate reply from the malicious node, for example the nature of malicious node here as it would not check its routing table.

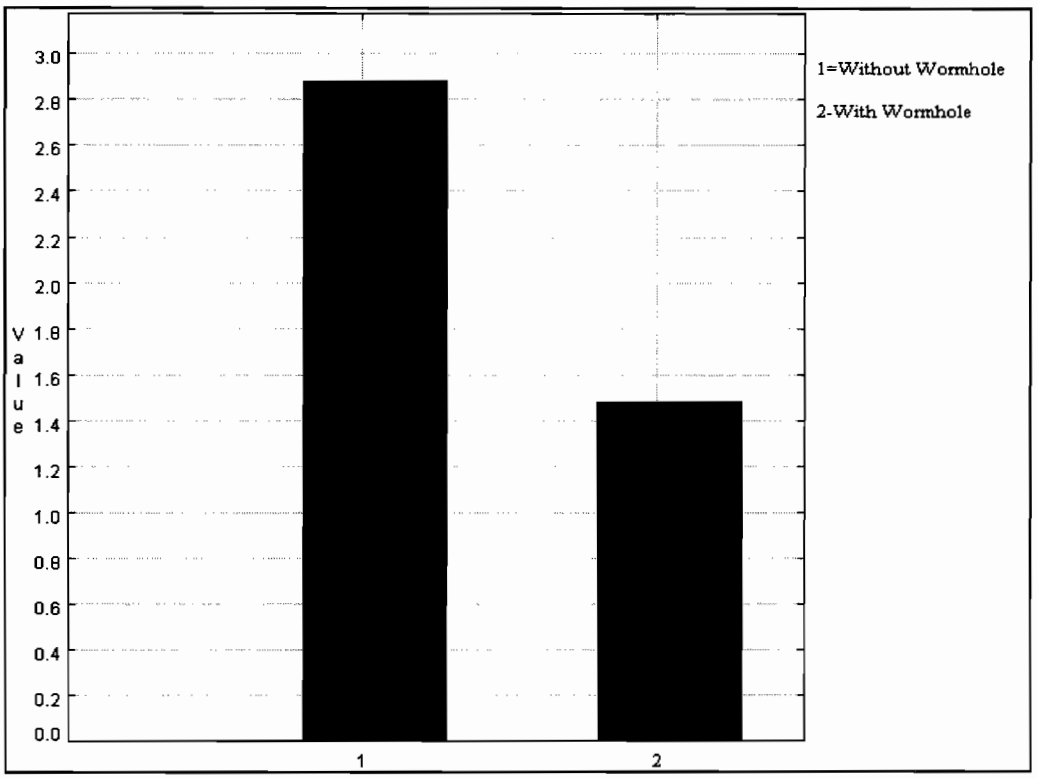


Figure 4.4: Average end-to-end delay with and without wormhole

The last metric element is that average jitter that shown in figure 4.5. Average jitter between the nodes is more without the wormhole attack, as compared to the average jitter between the nodes with the effect of wormhole attack. This is due to the

malicious nodes provides the path with fewer number of nodes, or smaller path. Thus average jitter between the nodes is reduced.

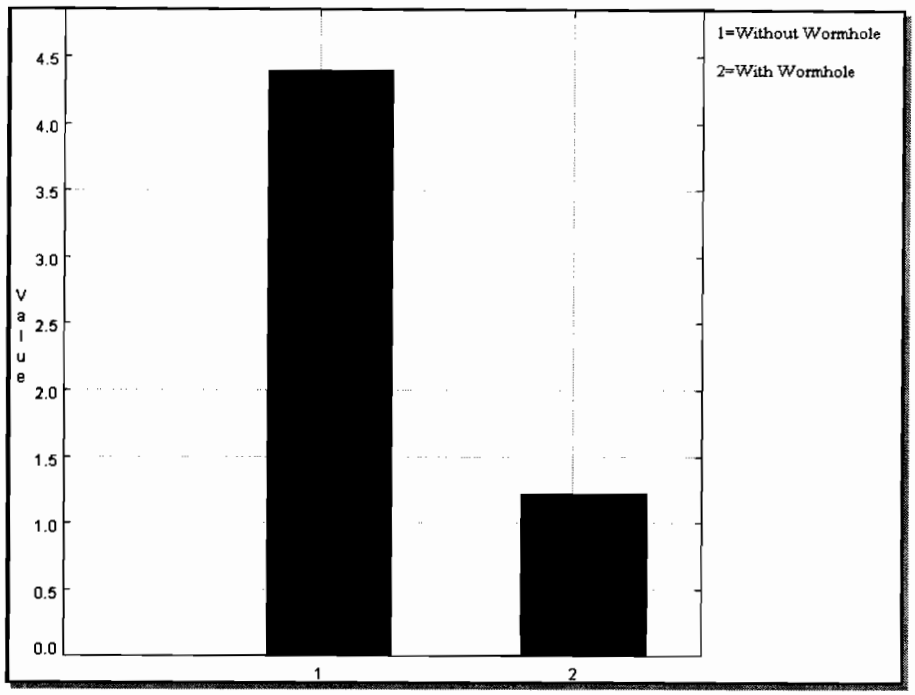


Figure 4.5: Average Jitter with and without wormhole attack

Moreover as comparison of figures 4.3, 4.4, and 4.5, we can notice that throughput values are more than average end-to-end delay and average jitter. That illustrated the main affect value belong to successful messages in MANET.

4.5 Conclusion

This chapter contains the results of our experiments that run on Mobile Ad Hoc network using QualNet simulator. The results of first scenario show the output file in MANET and how that refers to eavesdropping nodes. The output file show some leaking voluble information to illegal intruder user. The other results of the second scenario that refer to wormhole attack in MANET. These results explained the effect of the wormhole on MANET by assessment some factors and metrics such as throughput, average end to end delivery ,and average jitter.

CHAPTER FIVE

CONCLUSIONS AND FUTURE WORK

5.1 Introduction

With development in computing environments, the services based on Ad Hoc networks have been increased. Mobile Ad hoc networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes. A MANET is referred to as an infrastructureless network because the mobile nodes in the network dynamically set up paths among themselves to transmit. Many researchers and studies involve in studying the security architecture of Mobile Ad Hoc Network .Some surveys conduct the different several of MANET challenges and issues. This project study some of fames attacks in wireless Ad Hoc network and assessment the effect of them on the entire frame work using some metrics.

5.2 Conclusions

Attacks in wireless Ad Hoc are one of the mandatory issues and challenges in the network. There are a wide variety of attacks that target the weakness of MANET. The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks.

This project has been assessment the MANET attacks such as eavesdropping and wormhole in entire network. This study answers the research questions and concludes a new result which is very important to security experts. Determine the eavesdropping

and wormhole attacks and evaluate the performance of the network are the main objectives in this project.

Using QualNet 4.5 simulation was helpful in this project to obtain a good output results about the attacks and their impact in the framework. The project consists of two scenarios. First scenario about determine eavesdropping attacks and evaluate the performance in the network. Second scenario was to detect the active wormhole attack and evaluate the performance with and without it.

In the first scenario, the experiment conducted the output and evaluated the results. Referring to the results that notice by monitor some of output files, we can know the eavesdropping nodes and determine the valuable information that could be stolen as we can see them in appendix B. Network performance didn't change regarding to eavesdropping passive attack . Reading the messages can be very dangerous because this may be attack the privacy and integrity layer. By implementing cryptography and encryption mechanisms could be reduce these attacks.

In second scenario in this project the effect, Throughput, End-to-End Delay and Jitter have been detected with respect to attend and absences of wormhole. There is reduction in Throughput, E-E Delay, and Jitter as shown in Chapter four. As we can see the figures in appendix C, the effect on network performance is reduced with wormhole attack.

In addition, comparing these metrics together within wormhole attack illustrated that throughput factor is the most effecter within mobile Ad Hoc network with wormhole nodes. These results show that wormhole attack effect and reduce the successful messages between MANET nodes channels. Using these metrics is helping us with strategy to detect the wormhole attack in MANET.

5.3 Future Work

The detection of attacks in Ad Hoc networks is still considered to be a challenging task. This study conducts some statistics about mobile Ad Hoc attacks and how we can detect these attacks by analyzes these metrics. As a part of Future work we can plan to run these experiments with different simulations to measure the performance for those simulations such as NS-2 or OPNET. Different results could be compared to insure the actual behave for active and passive attacks. Another part of future work is implementing these measures with intrusion detection system (IDS) in MANET system. We need to deploy IDS and adapt these techniques in Wireless Ad Hoc network. Applying these measurements in MANET Architecture can help to build new second line defense against Adversary attacks.

REFERENCES

Anguswamy, R., Thiagarajan, M., & H.Dagli, C. (2008). Systems Methodology and Framework for problem definition in Mobile ad hoc networks.

Anjum, F., & Mouchtaris, P. (2007). security for Wireless Ad Hoc security

Basagni, S., Conti, M., & Giordano, S. (2004). Mobile Ad Hoc Networking.

Bianchi, A., & Pizzutilo, S. (2008). A Tool for Modeling and Simulating Mobile Ad-hoc Networks.

Bye, R., Schmidt, s., Luther, k., & Albayrak, s. (2008). Application-Level simulation for network security

Caballero, E. J. (2006). Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks - The routing problem.

Caro, G. A. D. (2003). Analysis of simulation environments for mobile ad hoc networks.

Carrillo, L., Marzo, J. L., VILÀ, P., & VILÀ, P. (2004). MAntS-Hoc: A Multi-agent Ant-based System for Routing in Mobile Ad Hoc Networks.

Çayırcı, E., & Rong, C. (2009). Security in Wireless Ad Hoc and Sensor Networks.

CCapkun, S., Hubaux, J. P., & Buttya´n, L. (2006). Mobility Helps Peer-to-Peer Security.

Chan, H., & Perrig, A. (2003). Security and Privacy in Sensor Networks.

Choi, S., Kim, D.-y., Lee, D.-h., & Jung, J.-i. (2008). WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks.

Demetrios, Z.-Y. (2001). A Glance at Quality of Services in Mobile Ad-Hoc Networks.

djenouri, D., khelladi, L., & Badache, N. (2005). A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks.

Erciyes, K., Dagdeviren, O., & Cokuslu, D. (2006). Modeling and Simulation of Wireles sensor and Mobike Ad Hoc Networks

Garrido, P. P., Malumbres, M. P., & Calafate, C. T. (2007). EVALUATION OF 802.11E MODELS UNDER NS-2 AND OPNET MODELER SIMULATION TOOLS IN MANET NETWORKS

Garrido, P. P., Malumbres, M. P., & Calafate, C. T. (2008). ns-2 vs. OPNET: a comparative study of the IEEE 802.11e technology on MANET environments.

Ghaffari, A. (2006). Vulnerability and Security of Mobile Ad hoc Networks.

Hogie, L. (2007). Mobile Ad Hoc Networks: Modelling, Simulation and Broadcast-based Applications.

Hu, Y., Perrig, A., & Johnson, D. B. (2002). Ariadne: A Secure OnDemand Routing Protocol for Ad Hoc Networks.

Jin, C., & Jin, S.-W. (2008). Invulnerability Assessment for Mobile Ad Hoc Networks.

Johston, D., & Walker, J. (2004). Overview of IEEE 802.16 security.

Kargl, F., & Schoch, E. (2007). Simulation of MANETs: A Qualitative Comparison between JiST/SWANS and ns-2.

Karlof, C., & Wagner, D. (2003). Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures.

Kurkowski, S., Camp, T., & Colagrosso, M. (2005). MANET Simulation Studies: The Incredibles.

Lin, X.-H., Kwok, Y.-K., & Lau, V. K. N. (2003). Power Control for IEEE 802.11 Ad Hoc Networks:Issues and A New Algorithm.

Liu, J., Fu, F., Xiao, J., & Lu, Y. (2007). Secure Routing for Mobile Ad Hoc Networks.

Michiardi, P., & Molva, R. (2002). Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks.

Mishra, A. (2008). Security and Quality of service in Ad hoc wireless Netoworks.

Mishra, A., Nadkarni, K., Patcha, A., & Tech, V. (2004). Intrusion Detection in Wireless Ad Hoc Networks.

Ning, P., & Sun, K. (2003). How to Misuse AODV: A Case Study of Insider Attacks against Mobile Ad-Hoc Routing Protocols.

Otrok, H., Paquet, J., Debbabi, M., & Bhattacharya, P. (2007). Testing Intrusion Detection Systems in MANET: A Comprehensive Study.

Papaleo, G. (2007). Wireless Network Intrusion Detection System: implementation and architectural issues.

Ravi, S., Raghunathan, A., & Chakradhar, S. (2003). Embedding Security in Wireless Embedded Systems.

Sabir, A., Murphy, S., & Yang, Y. (2006). Generic Threats to Routing Protocols.

Sarkar, S. K., Basavaraju, T. G., & Puttamadappa, C. (2008). ad hoc mobile wireless networks : principles, protocols, and applications.

Schoch, E., Feiri, M., & Frank Kargl, M. W. (2008). Simulation of Ad Hoc Networks: ns-2 compared to JiST/SWANS.

Schoch, E., Feiri, M., Kargl, F., & Weber, M. (2008). Simulation of Ad Hoc Networks: ns-2 compared to JiST/SWANS.

Sharma, S., & Gupta, R. (2009). Simulation Study of Blackhole Attack in the Mobile Ad Hoc Networks.

Stajano, F., & Anderson, R. (2004). The Resurrecting Duckling:Security Issues for Ad-hoc Wireless Networks.

Thales. (2007). Implementing Mobile Ad Hoc Networking (MANET) over Legacy Tactical Radio Links.

Turban, E. a. A., J.E (1998). decision support systems and intelligent systems.

Scalable Network Technologies (SNT) . QualNet. http://www.qualnet.com/.

Vinayakray, P. (2002). Security within Ad hoc Networks.

Wang, H., Wang, Y., & Han, J. (2009). A Security Architecture for Tactical Mobile Ad hoc Networks.

Wu, B., Chen, J., Wu, J., & Cardei, M. (2006). A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks.

YianHuang, & Lee, W. (2003). A Cooperative Intrusion Detection System for Ad Hoc Networks.

Yu, S., Zhang, Y., Song, C., & Chen, K. (2005). A security architecture for Mobile Ad Hoc Networks.

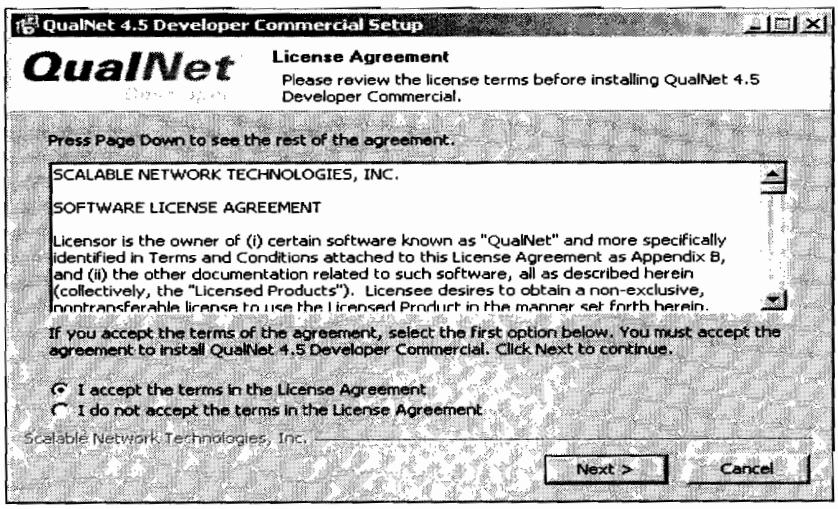
Yun, J., Sohn, K., & Yoon, H. (2007). Dynamic Simulation on Network Security Simulator using SSFNET.

Zhang, Y., Huang, Y.-a., & Lee, W. (2005). An Extensible Environment for Evaluating Secure MANET.

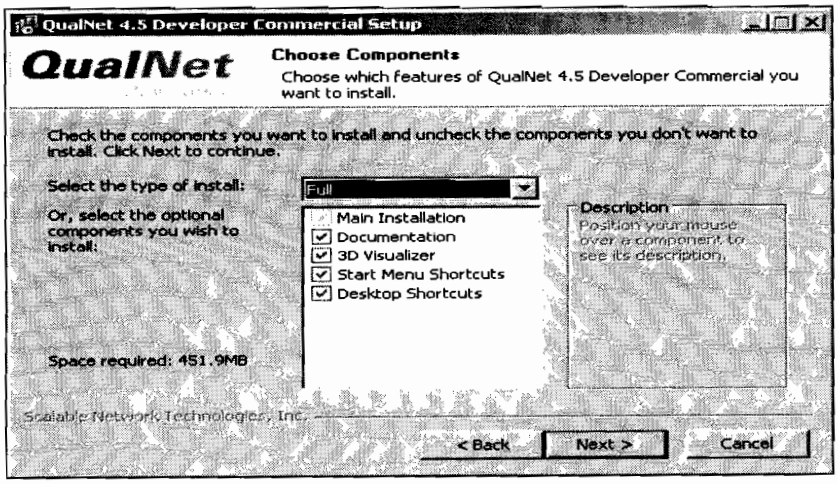
Zhou, L., & Haas, Z. J. (1999). Securing Ad Hoc Networks. Cornell University Ithaca, NY 14853.

To install QualNet 4.5.1 see table 3.1 for Minimum requirements to install for Windows XP. We have to follow these steps to install them

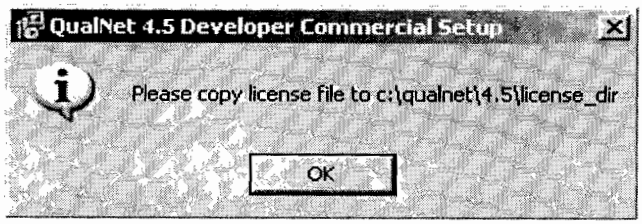
- Download the installation package (file qualnet-4.5-commercial-installer.exe) from the QualNet download page or load it from the installation CD.
- Double click on the file qualnet-4.5-commercial-installer.exe



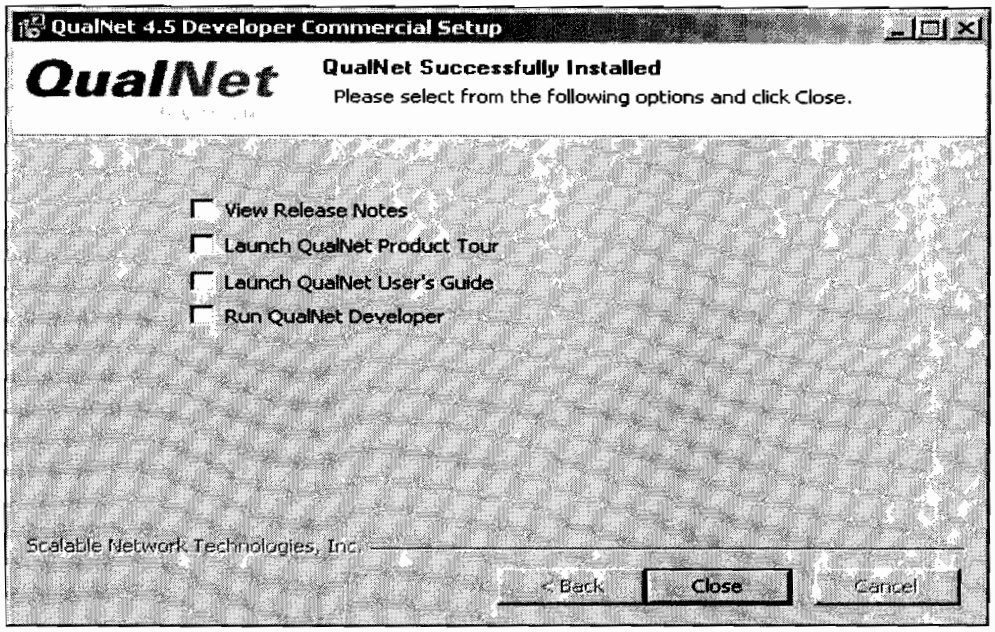
- Select the components to install in the Choose Components dialog box. The default type of install is full.



- Follow the default installation and when prompted, copy the license file to the license directory. (the license provide by QualNet package)

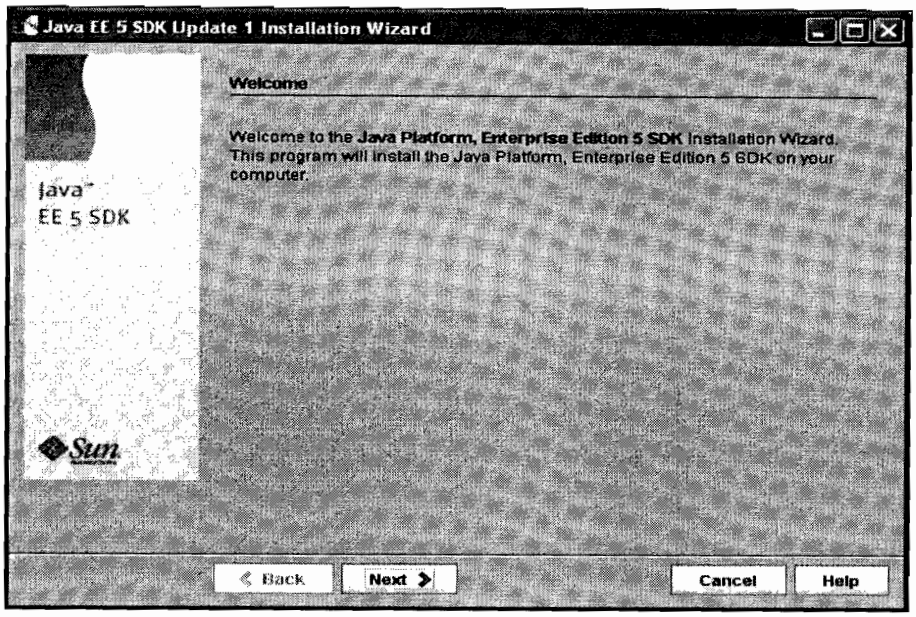


- After install the license in license directory in the default path in c drive , the screen below with the confirmation of the installation .



- Then we install third software programs such as Java support and C++ compiler. Java support is required to run the QualNet GUI. A C++ compiler is required to recompile the source code when models are added or modified.
- I run Sun Java 2 SDK, Standard Edition, version 1.4.2 or higher, that is required to run the QualNet graphical tools. Go to the following URL for

information on downloading Java: http://www.scalable-networks.com/products/sysreq.php



- After that to compile QualNet source code or custom addons, one of the C++ compilers listed in table A.1.I use Microsoft Visual Studio 2005 to compile source code

Table A.1: C++ compilers

C++ Compiler	Abbreviation
Microsoft Visual C++ .NET 2002	VC7
Microsoft Visual C++ .NET 2003	VC7
Microsoft Visual Studio 2003	VC7
Microsoft Visual Studio 2005	VC8
Microsoft Visual C++ 2005 Express Edition	VC8 Express

- I made compile QualNet4.5 by open the program from this path :
  Start > All Programs > Microsoft Visual Studio 2005 > Visual Studio Tools >Visual Studio 2005 Command Prompt .

- Then run these commands :

  copy Makefile-windows-vc8 Makefile

  nmake clean

  nmake

  - After all of those steps we can run QualNet 4.5.1 GUI I by double-clicking on the shortcut icon on the desktop

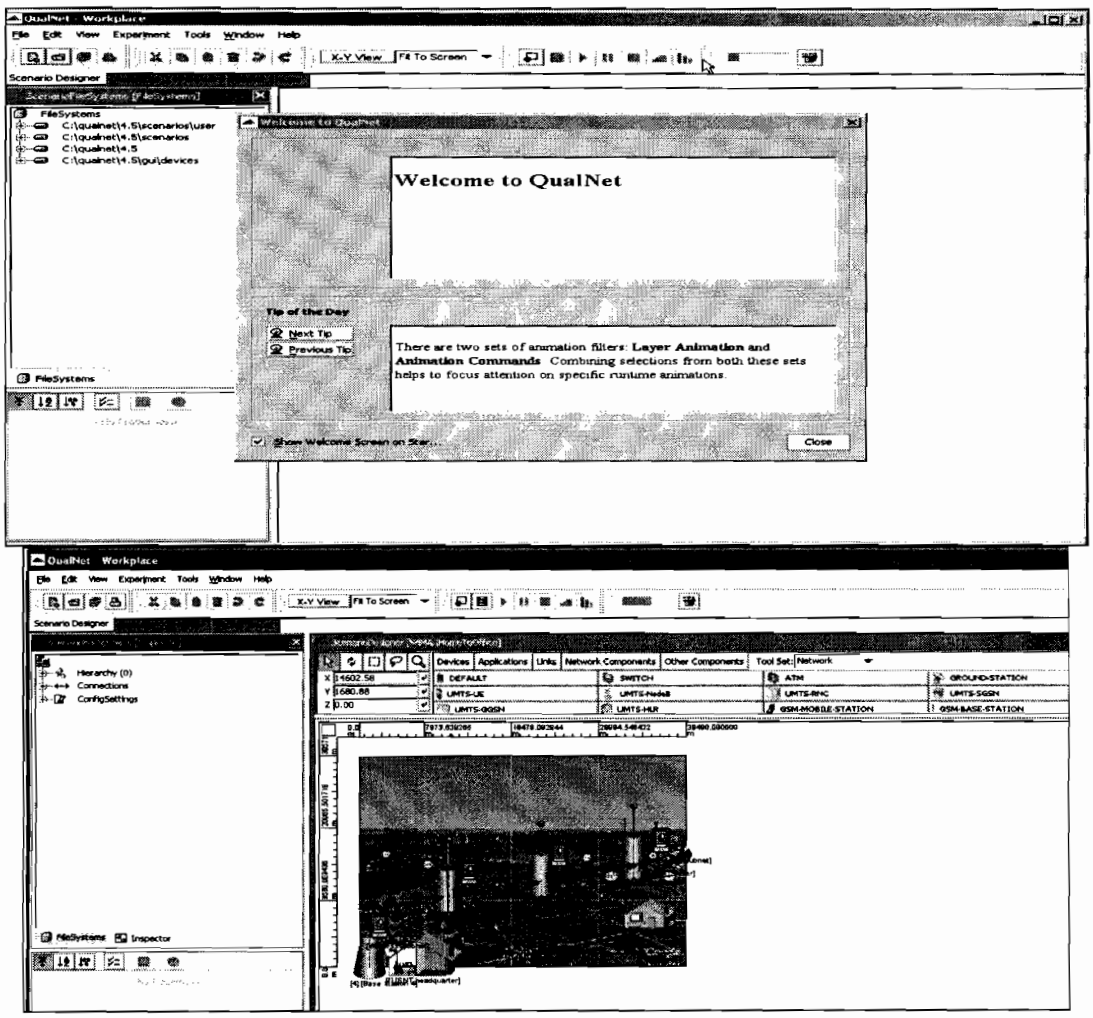


Figure A.1: QualNet 4.5.1 GUI Simulation

APPENDIX B: EAVESDROPPING RESULTS

Table B-1: Results of eavesdropping experiential design

Treatment Run	Log Output
Run 1	<simtime>26.272078475</simtime><ipv4>4 5 0 40 668 <flags>0 0 0</flags> 0 61 6 0 192.0.0.6 192.0.0.1</ipv4> <simtime>26.294323673</simtime><ipv4>4 5 0 552 1216 <flags>0 0 0</flags> 0 63 6 0 192.0.0.1 192.0.0.6</ipv4> <simtime>26.298206233</simtime><ipv4>4 5 0 552 1216 <flags>0 0 0</flags> 0 62 6 0 192.0.0.1 192.0.0.6</ipv4> <simtime>26.307372705</simtime><ipv4>4 5 0 40 669 <flags>0 0 0</flags> 0 62 6 0 192.0.0.6 192.0.0.1</ipv4> <simtime>26.308947327</simtime><ipv4>4 5 0 40 669 <flags>0 0 0</flags> 0 61 6 0 192.0.0.6 192.0.0.1</ipv4> <simtime>26.315730809</simtime><ipv4>4 5 0 552 1217 <flags>0 0 0</flags> 0 64 6 0 192.0.0.1 192.0.0.6</ipv4>
Run 2	<simtime>1.572373120</simtime><ipv4>4 5 0 40 9 <flags>0 0 0</flags> 0 63 6 0 192.0.0.6 192.0.0.1</ipv4> <simtime>1.573967557</simtime><ipv4>4 5 0 40 9 <flags>0 0 0</flags> 0 62 6 0 192.0.0.6 192.0.0.1</ipv4> <simtime>1.577010523</simtime><ipv4>4 5 0 41 10 <flags>0 0 0</flags> 0 63 6 0 192.0.0.6 192.0.0.1</ipv4> <simtime>1.578408960</simtime><ipv4>4 5 0 41 10 <flags>0 0 0</flags> 0 62 6 0 192.0.0.6 192.0.0.1</ipv4> <simtime>1.582775841</simtime><ipv4>4 5 0 40 11 <flags>0 0 0</flags> 0 63 6 0 192.0.0.1 192.0.0.6</ipv4> <simtime>1.584530206</simtime><ipv4>4 5 0 40 11 <flags>0 0 0</flags> 0 62 6 0 192.0.0.1 192.0.0.6</ipv4> <simtime>1.585985001</simtime><ipv4>4 5 0 40 11 <flags>0 0 0</flags> 0 61 6 0 192.0.0.1 192.0.0.6</ipv4>

APPENDIX B: EAVESDROPPING RESULTS

Table B-1: Results of eavesdropping experiential design

Treatment Run	Log Output
Run 3	<simtime>1.572373120</simtime><ipv4>4 5 0 40 9 <flags>0 0 0</flags> 0 63 6 0 192.0.0.6 192.0.0.1</ipv4> <simtime>1.573967557</simtime><ipv4>4 5 0 40 9 <flags>0 0 0</flags> 0 62 6 0 192.0.0.6 192.0.0.1</ipv4> <simtime>1.577010523</simtime><ipv4>4 5 0 41 10 <flags>0 0 0</flags> 0 63 6 0 192.0.0.6 192.0.0.1</ipv4> <simtime>1.578408960</simtime><ipv4>4 5 0 41 10 <flags>0 0 0</flags> 0 62 6 0 192.0.0.6 192.0.0.1</ipv4> <simtime>1.582775841</simtime><ipv4>4 5 0 40 11 <flags>0 0 0</flags> 0 63 6 0 192.0.0.1 192.0.0.6</ipv4> <simtime>1.584530206</simtime><ipv4>4 5 0 40 11 <flags>0 0 0</flags> 0 62 6 0 192.0.0.1 192.0.0.6</ipv4> <simtime>1.585985001</simtime><ipv4>4 5 0 40 11 <flags>0 0 0</flags> 0 61 6 0 192.0.0.1 192.0.0.6</ipv4>
Run 4	<simtime>1.004077231</simtime><ipv4>4 5 0 44 4 <flags>0 0 0</flags> 0 64 6 0 192.0.0.17 192.0.0.11</ipv4> <simtime>1.005787352</simtime><ipv4>4 5 0 44 4 <flags>0 0 0</flags> 0 63 6 0 192.0.0.17 192.0.0.11</ipv4> <simtime>1.010367946</simtime><ipv4>4 5 0 44 4 <flags>0 0 0</flags> 0 62 6 0 192.0.0.17 192.0.0.11</ipv4>
Run 5	<simtime>1.003617151</simtime><ipv4>4 5 0 540 6 <flags>0 0 0</flags> 0 64 17 0 192.0.0.11 192.0.0.17</ipv4> <simtime>1.007312276</simtime><ipv4>4 5 0 540 6 <flags>0 0 0</flags> 0 63 17 0

APPENDIX B: EAVESDROPPING RESULTS

Table B-1: Results of eavesdropping experiential design

Treatment Run	Log Output
	192.0.0.11 192.0.0.17</ipv4> <simtime>2.003437151</simtime><ipv4>4 5 0 540 7 <flags>0 0 0</flags> 0 64 17 0 192.0.0.11 192.0.0.17</ipv4> <simtime>2.006892276</simtime><ipv4>4 5 0 540 7 <flags>0 0 0</flags> 0 63 17 0 192.0.0.11 192.0.0.17</ipv4> <simtime>3.003497151</simtime><ipv4>4 5 0 540 8 <flags>0 0 0</flags> 0 64 17 0 192.0.0.11 192.0.0.17</ipv4> <simtime>3.007292276</simtime><ipv4>4 5 0 540 8 <flags>0 0 0</flags> 0 63 17 0 192.0.0.11 192.0.0.17</ipv4>
Run 6	<simtime>2.291821954</simtime><ipv4>4 5 0 40 11 <flags>0 0 0</flags> 0 63 6 0 192.0.0.11 192.0.0.17</ipv4> <simtime>2.293415633</simtime><ipv4>4 5 0 40 11 <flags>0 0 0</flags> 0 62 6 0 192.0.0.11 192.0.0.17</ipv4> <simtime>2.487770595</simtime><ipv4>4 5 0 41 12 <flags>0 0 0</flags> 0 63 6 0 192.0.0.11 192.0.0.17</ipv4> <simtime>2.489188274</simtime><ipv4>4 5 0 41 12 <flags>0 0 0</flags> 0 62 6 0 192.0.0.11 192.0.0.17</ipv4> <simtime>2.493653200</simtime><ipv4>4 5 0 40 9 <flags>0 0 0</flags> 0 62 6 0 192.0.0.17 192.0.0.11</ipv4> <simtime>2.504763307</simtime><ipv4>4 5 0 40 9 <flags>0 0 0</flags> 0 62 6 0 192.0.0.17 192.0.0.11</ipv4> <simtime>2.508387491</simtime><ipv4>4 5 0 552 10 <flags>0 0 0</flags> 0 62 6 0 192.0.0.17 192.0.0.11</ipv4> <simtime>2.510231675</simtime><ipv4>4 5 0 57 11 <flags>0 0 0</flags> 0 62 6 0 192.0.0.17 192.0.0.11</ipv4>
Run 7	<simtime>22.916856151</simtime><ipv4>4 5 0 40 168 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>22.953012121</simtime><ipv4>4 5 0 40 169 <flags>0 0 0</flags> 0 62 6 0

APPENDIX B: EAVESDROPPING RESULTS

Table B-1: Results of eavesdropping experiential design

Treatment Run	Log Output
	192.0.0.9 192.0.0.33</ipv4> <simtime>22.956022535</simtime><ipv4>4 5 0 40 170 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>23.093679601</simtime><ipv4>4 5 0 40 171 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>23.114831792</simtime><ipv4>4 5 0 40 172 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>23.118503205</simtime><ipv4>4 5 0 40 172 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>23.121677582</simtime><ipv4>4 5 0 40 172 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>24.372050054</simtime><ipv4>4 5 0 40 173 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4>
Run 8	<simtime>1.011419628</simtime><ipv4>4 5 0 44 9 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>1.147432047</simtime><ipv4>4 5 0 40 10 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>1.150346461</simtime><ipv4>4 5 0 41 11 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>2.003594064</simtime><ipv4>4 5 0 40 12 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>2.007652407</simtime><ipv4>4 5 0 41 13 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>2.180936062</simtime><ipv4>4 5 0 40 14 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>2.185354405</simtime><ipv4>4 5 0 41 15 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4>

APPENDIX B: EAVESDROPPING RESULTS

Table B-1: Results of eavesdropping experiential design

Treatment Run	Log Output
	<simtime>2.714797063</simtime><ipv4>4 5 0 40 16 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>2.719435406</simtime><ipv4>4 5 0 41 17 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>2.741184147</simtime><ipv4>4 5 0 40 18 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>2.746322561</simtime><ipv4>4 5 0 552 19 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>2.938158032</simtime><ipv4>4 5 0 60 20 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>6.553279062</simtime><ipv4>4 5 0 40 21 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>6.558597406</simtime><ipv4>4 5 0 41 22 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4
Run 9	simtime>29.286100819</simtime><ipv4>4 5 0 40 70 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>29.294151964</simtime><ipv4>4 5 0 92 71 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>29.439114639</simtime><ipv4>4 5 0 40 72 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>29.454520615</simtime><ipv4>4 5 0 41 73 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>29.765079027</simtime><ipv4>4 5 0 40 74 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>29.767947779</simtime><ipv4>4 5 0 283 75 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>29.797451228</simtime><ipv4>4 5 0 40 76 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4>

APPENDIX B: EAVESDROPPING RESULTS

Table B-1: Results of eavesdropping experiential design

Treatment Run	Log Output
	<simtime>29.800285642</simtime><ipv4>4 5 0 41 77 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>29.959107048</simtime><ipv4>4 5 0 40 78 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4> <simtime>29.960539800</simtime><ipv4>4 5 0 49 79 <flags>0 0 0</flags> 0 62 6 0 192.0.0.9 192.0.0.33</ipv4>

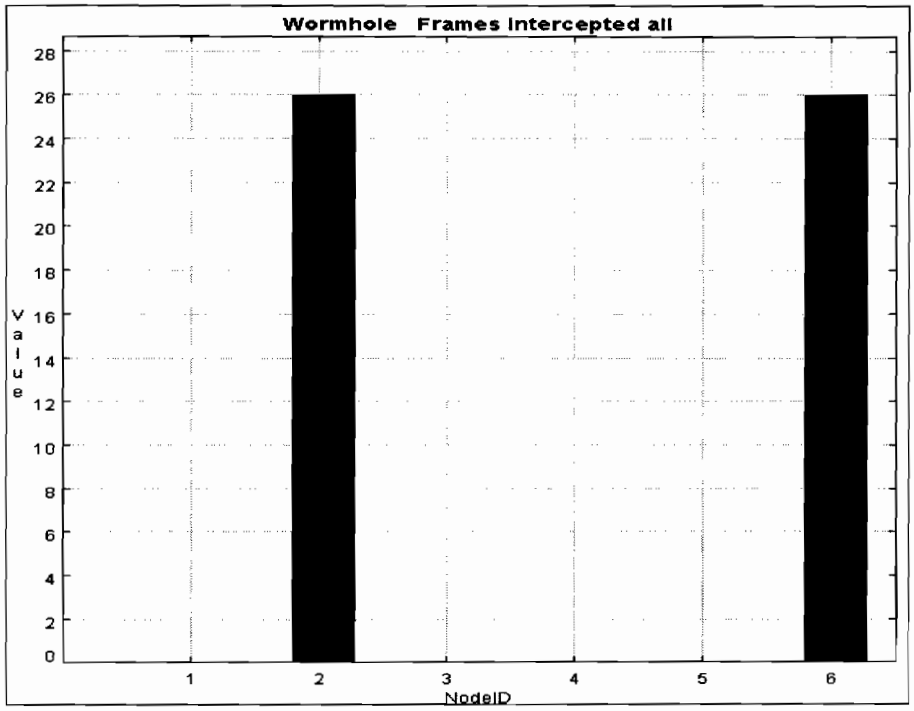


Figure C.1: Run 2 Wormhole Frames Intercepted All.

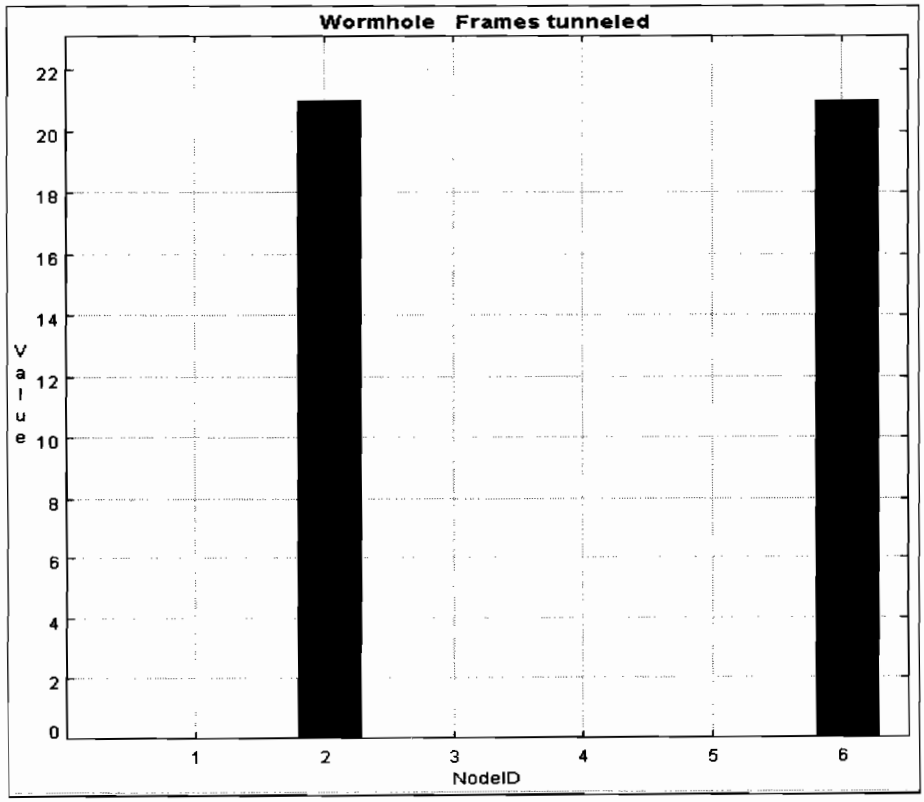


Figure C.2: Run 2 Wormhole Frames Tunneled

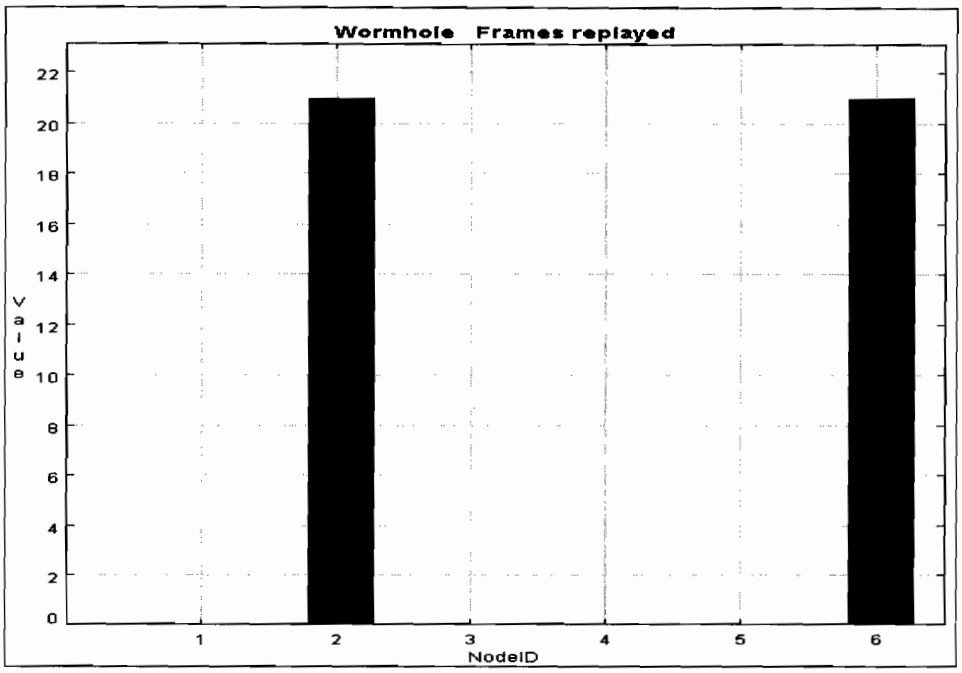


Figure C.3: Run 2Wormhole Frames Replayed

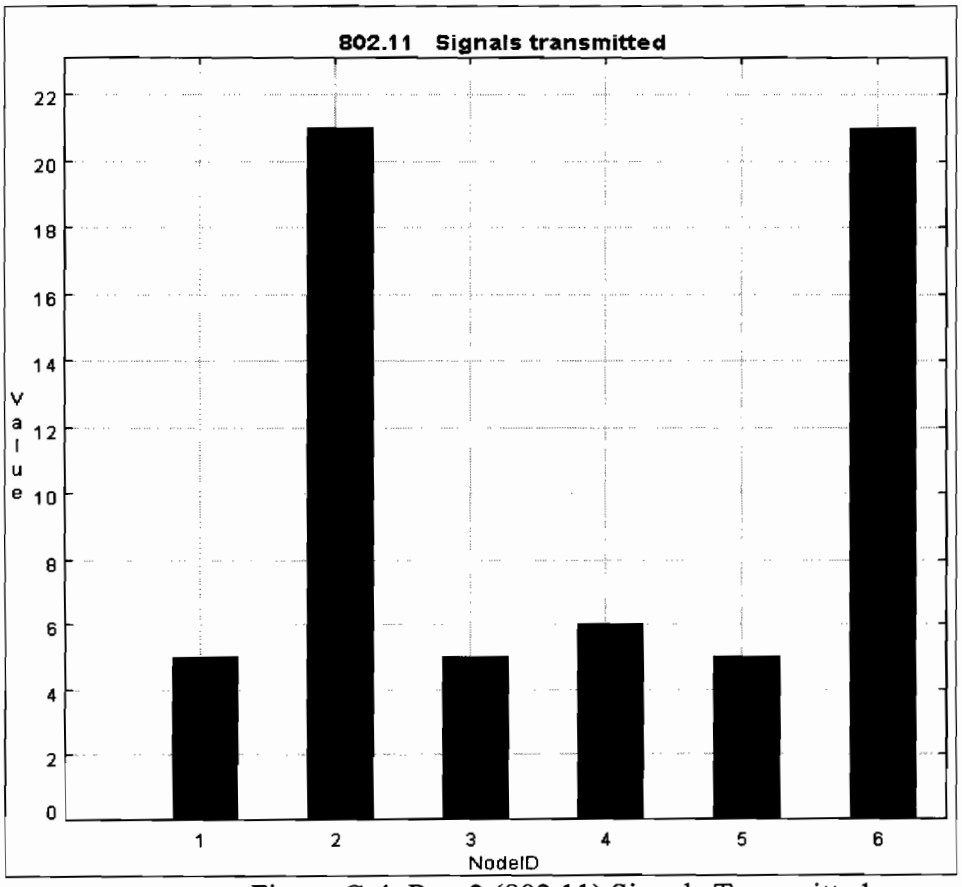


Figure C-4: Run 2 (802.11) Signals Transmitted

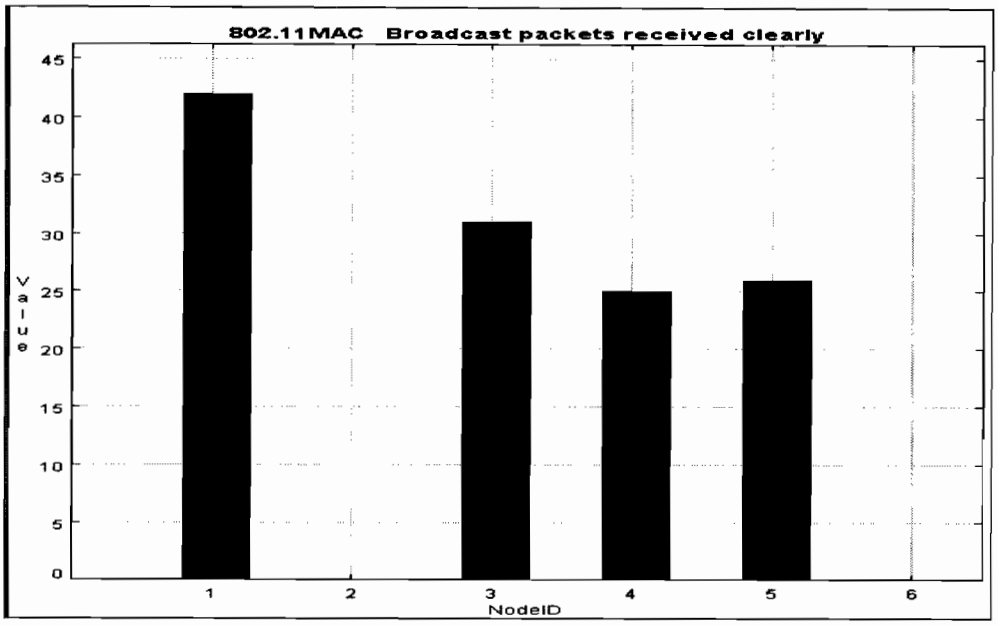


Figure C.5:Run2 Broadcast Packets Received Clearly

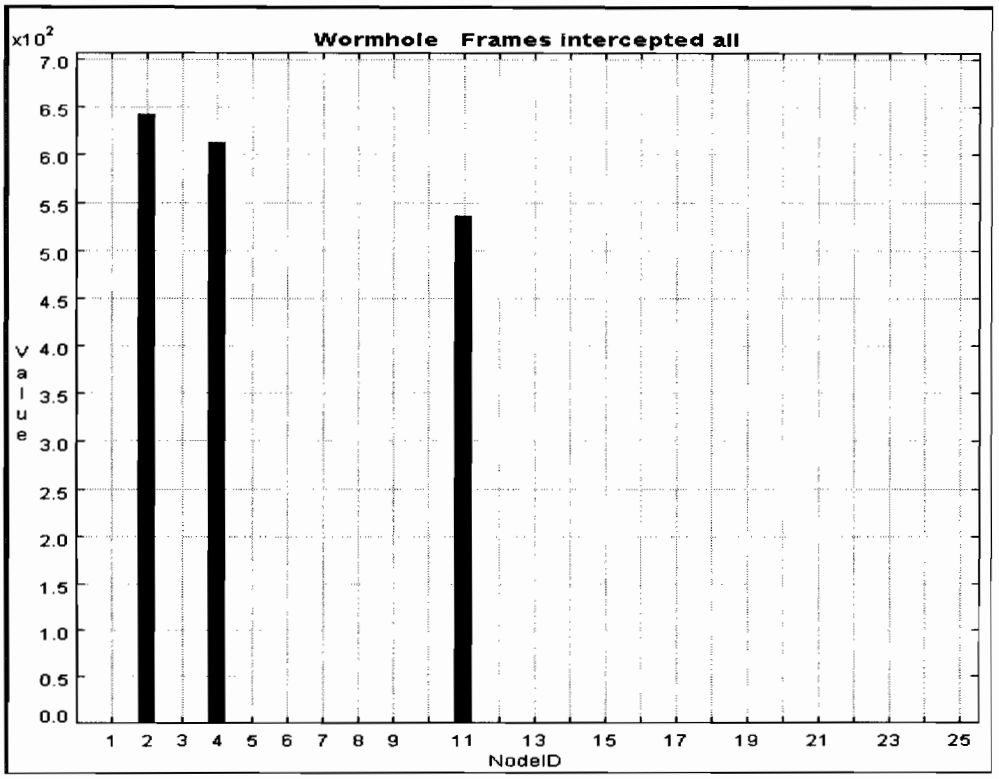


Figure C.6: Run 4 Wormhole Frames Intercepted All

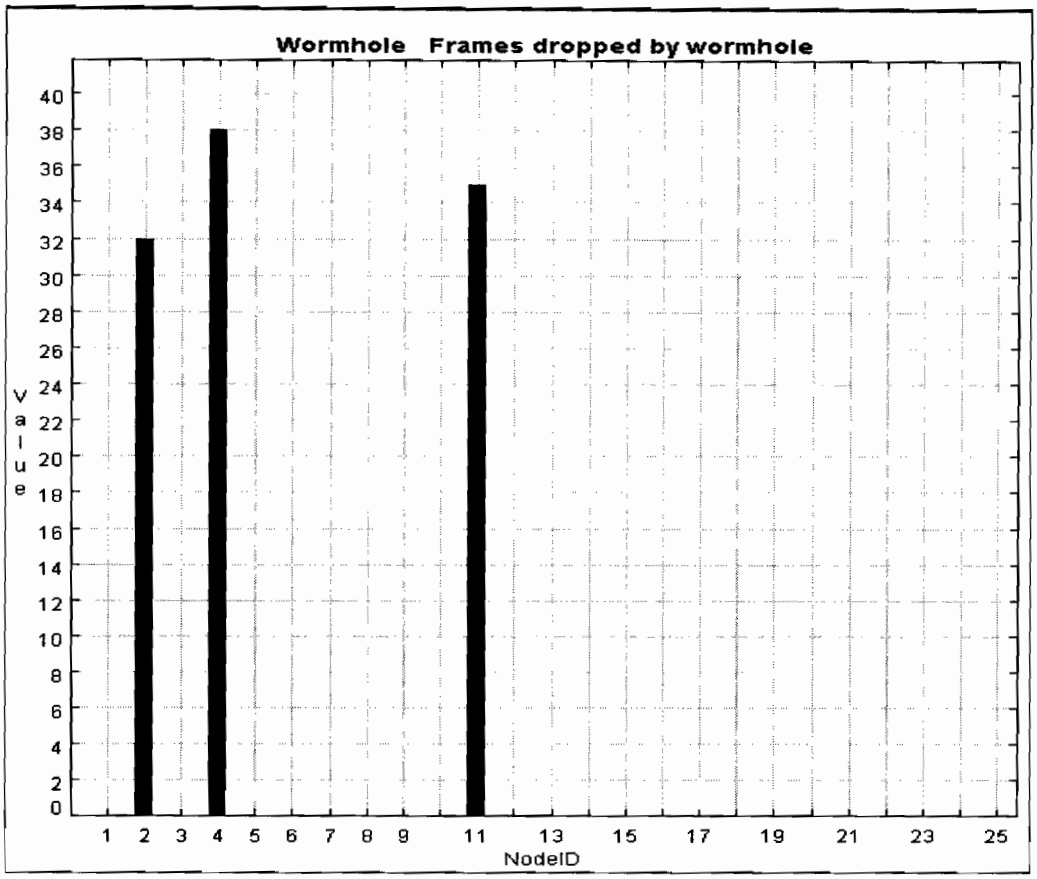


Figure C-7: Run 4 Frames Dropped by Wormhole

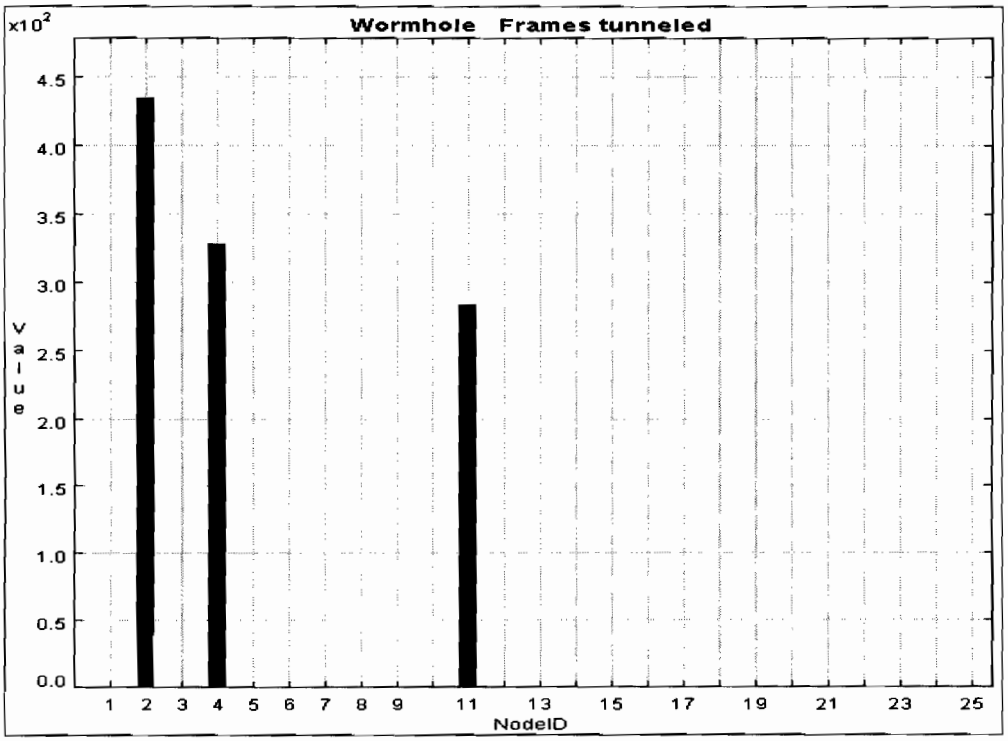


Figure C.8: Run 4 Wormhole Frames Tunneled

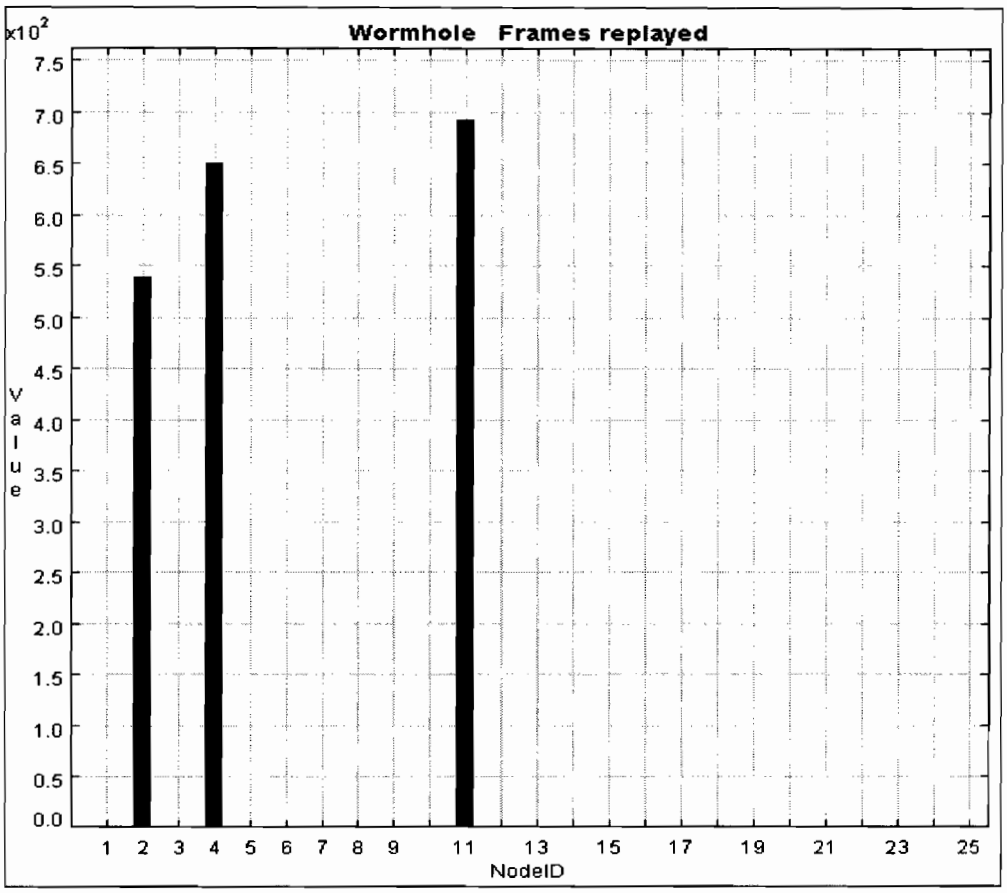


Figure C.9: Run 4 Wormhole Frames Replayed

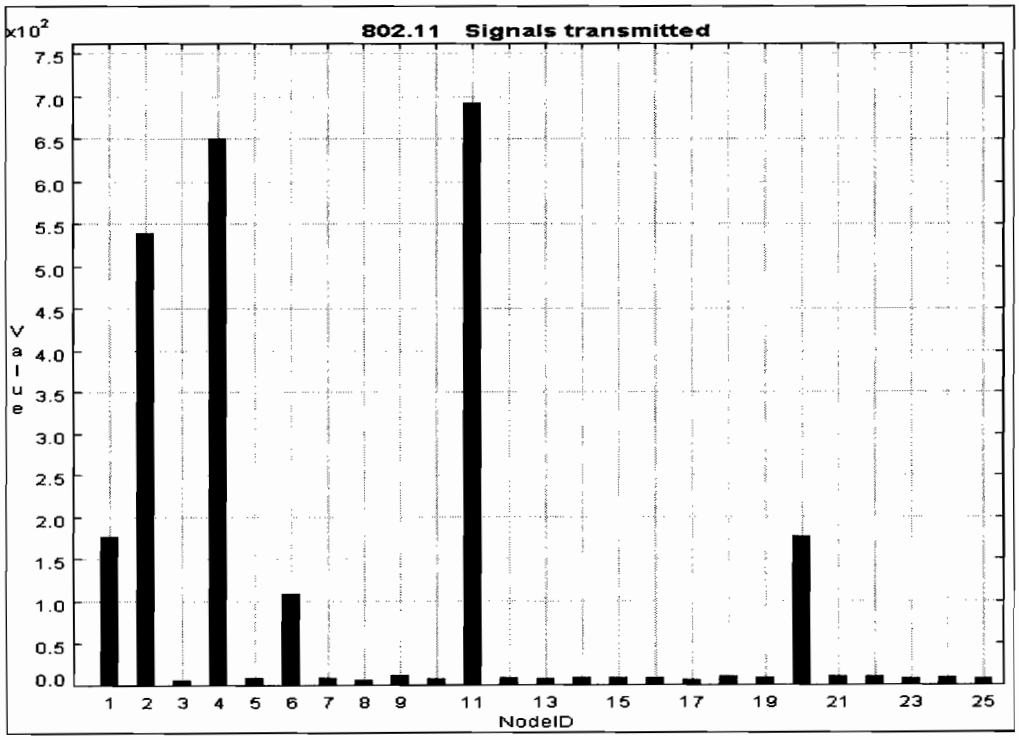


Figure C.10: Run 4 (802.11) Signals Transmitted

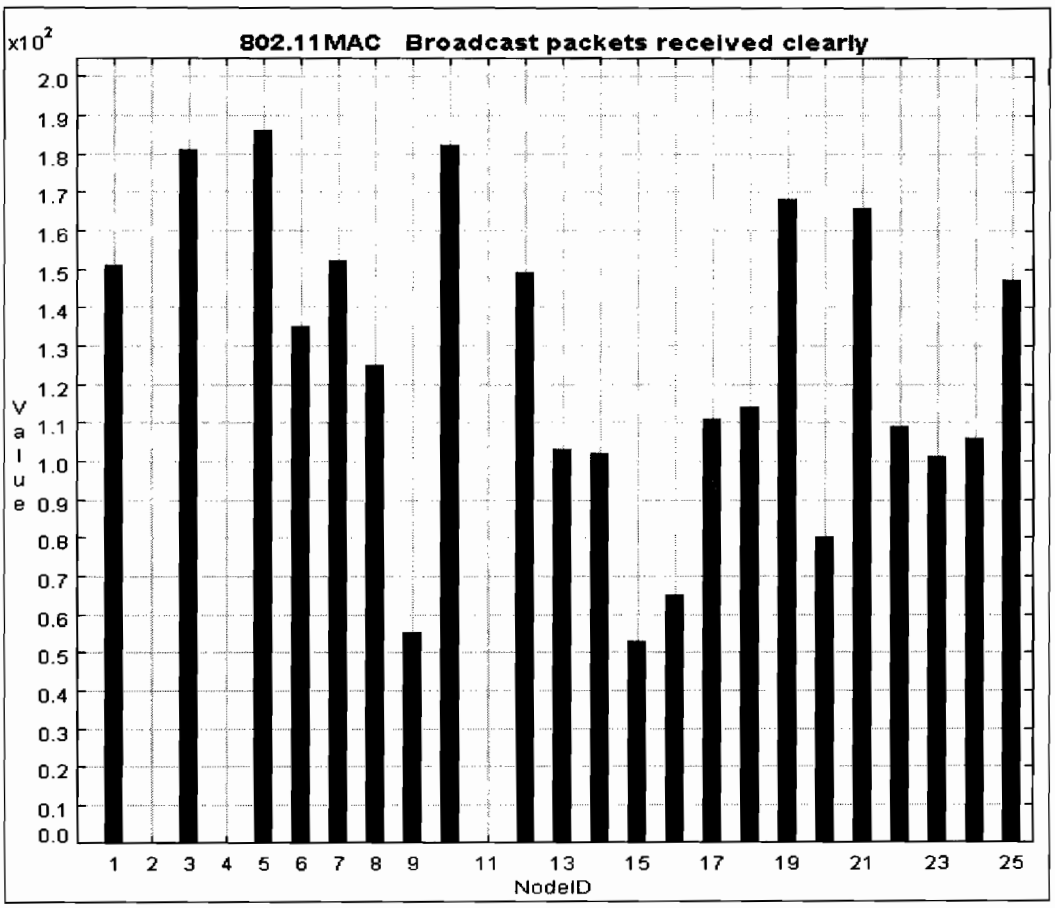


Figure C.11: Run 4 Broadcast Packets Received

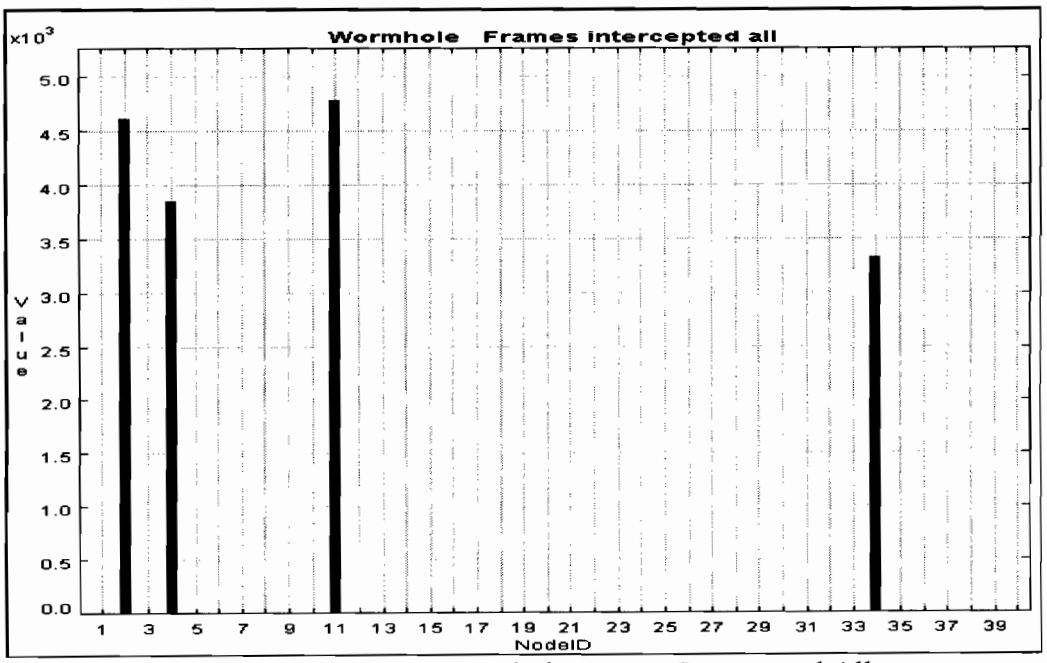


Figure C.12: Run 6 Wormhole Frames Intercepted All

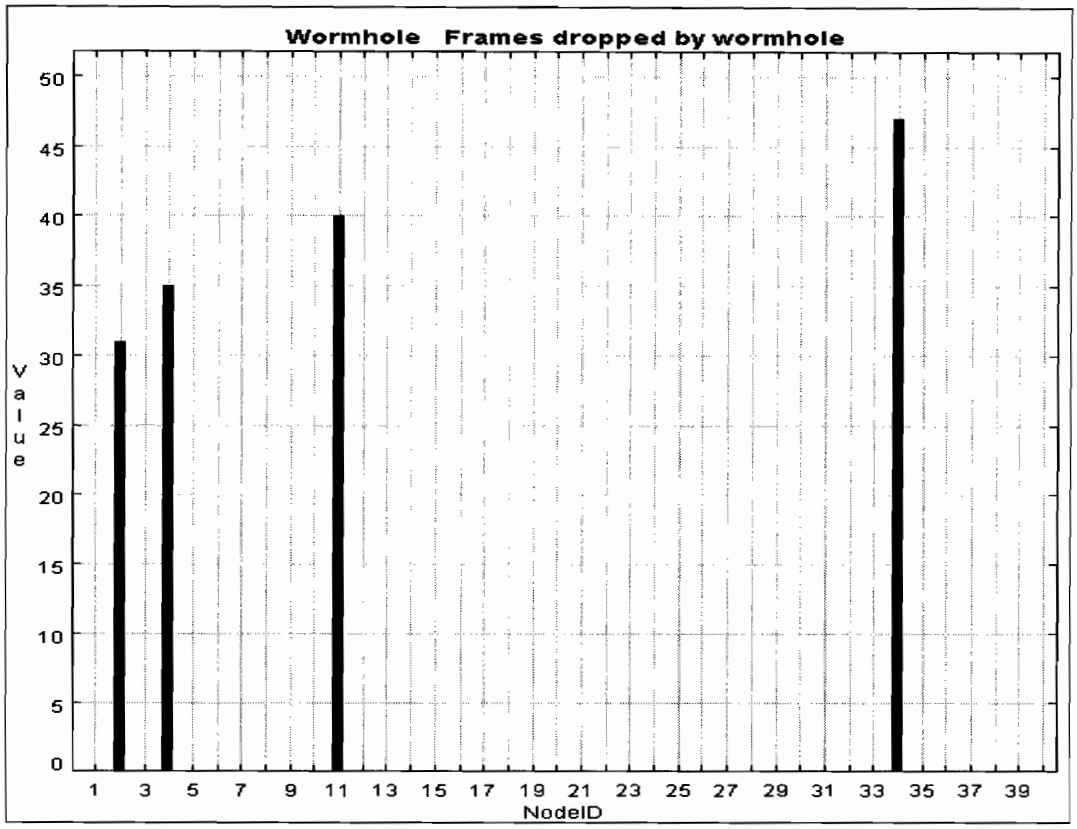


Figure C.13: Run 6 Frames Dropped by Wormhole

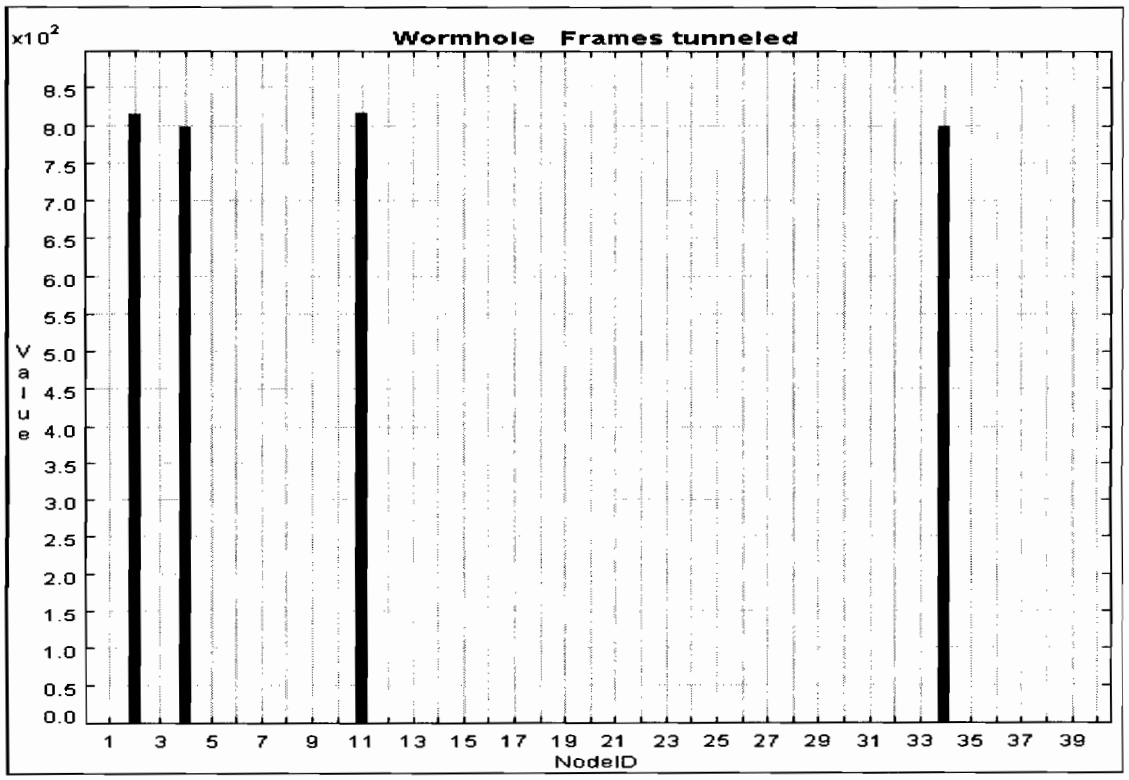


Figure C.14: Run 6 Frames Tunneled

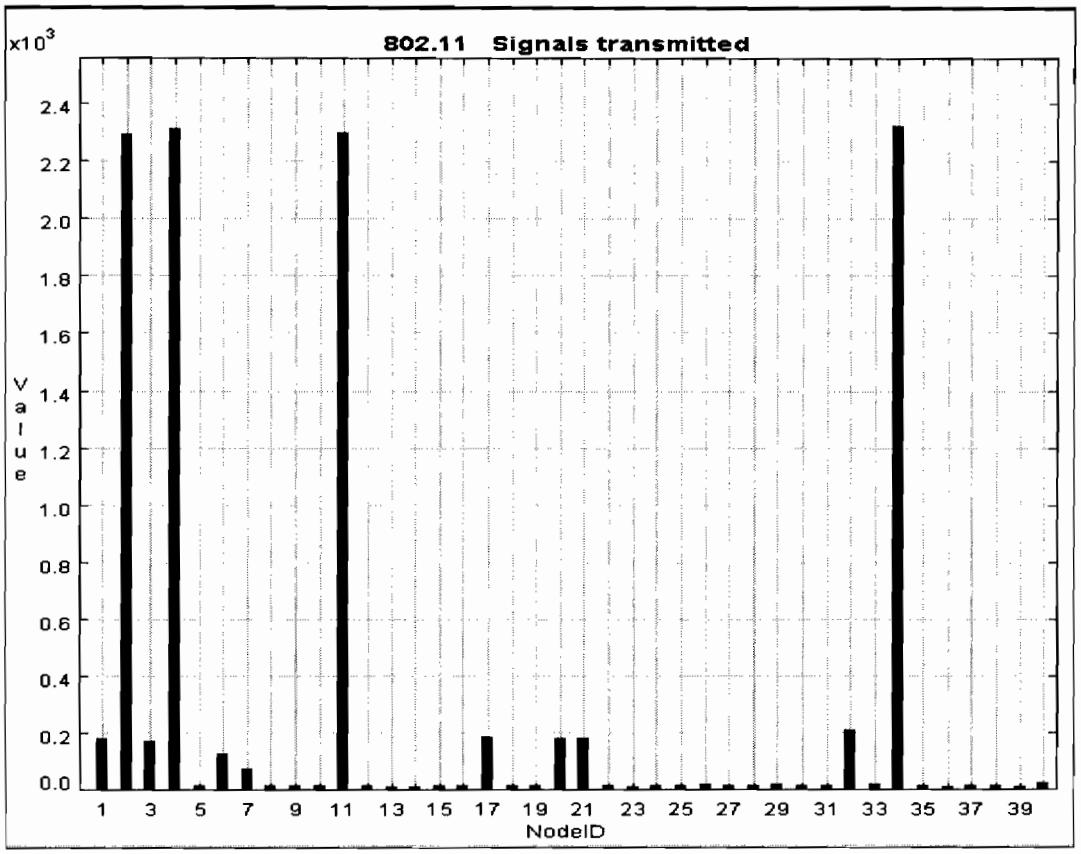


Figure C.15: Run 6 Signals Transmitted

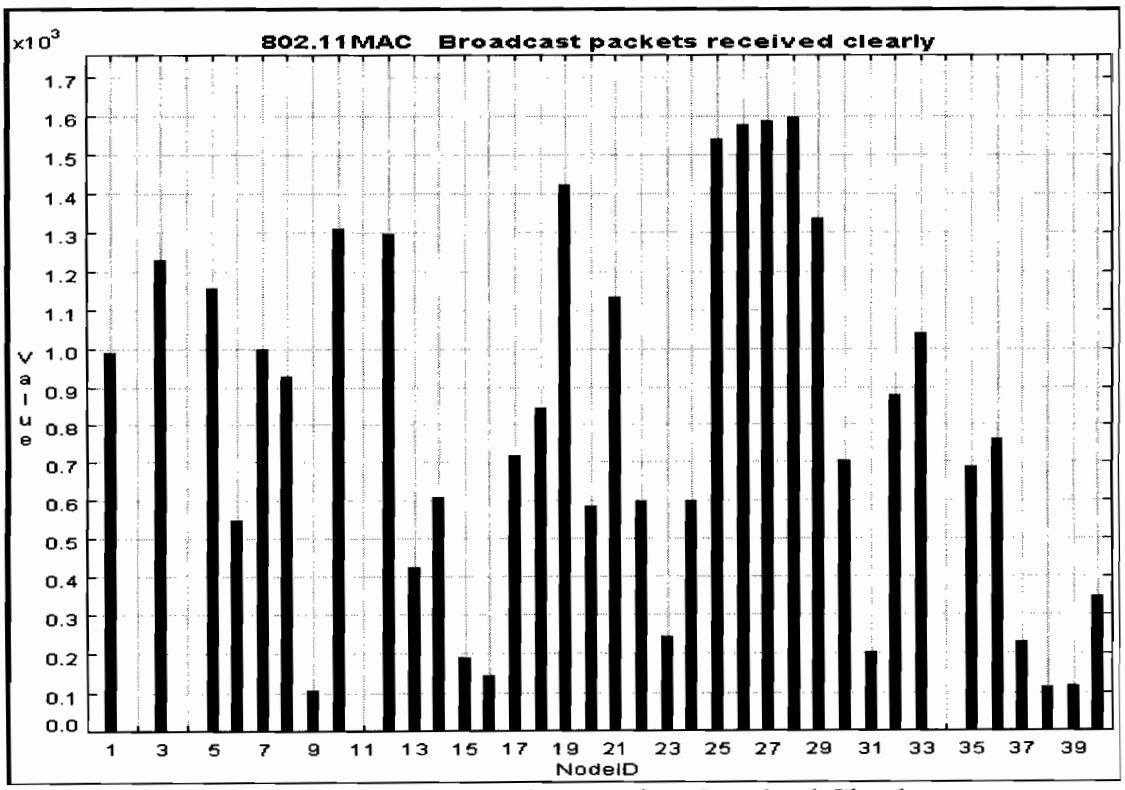


Figure C.16: Run 6 Broadcast Packets Received Clearly