Investigate Performance of 802.11b and 802.11g Standards with DSR Protocol using OPNET

Mohammed Dalshad Khorsheed

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirements for the Degree of

Master of Science
in
Computer Engineering

Eastern Mediterranean University
June 2013
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Prof. Dr. Elvan Yılmaz
Director

I certify that this thesis satisfies the requirements as a thesis for the degree of Master of Science in Computer Engineering.

Assoc. Prof. Dr. Muhammed Salamah
Chair, Department of Computer Engineering

We certify that we have read this thesis and that in our opinion it is fully adequate in scope and quality as a thesis for the degree of Master of Science in Computer Engineering.

Asst. Prof. Dr. Gürcü Öz
Supervisor

Examining Committee

1. Assoc. Prof. Dr. Muhammed Salamah

2. Asst. Prof. Dr. Gürcü Öz

3. Asst. Prof. Dr. Önsen Toygar

ABSTRACT

MANETs stands for mobile ad-hoc networks. They are a collection of mobile devices that do not require any infrastructure or centralized control. Additionally, they do not contain any central coordinator like a router or an access point. This network has a lot of features that are different from other networks such as ease of movement between networks and the ability of mobile devices to leave the network. Because, there is no router in this network, the routing process is done by the nodes themselves.

There are more than one routing protocols proposed for this network, each working under different strategies. A routing protocol is used to discover routes between stations. It plays an important role for the overall performance of MANETs. MANET routing protocols include Optimized Link State Routing protocol (OLSR), Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Temporary Ordered Routing algorithm (TORA). A good understanding of the effect of each of these routing protocols on a typical IEEE 802.11 network will cater for an efficient design and deployment of an appropriate MANETs.

In this thesis, we used an FTP application to investigate and analyze the performance of wireless standards 802.11b and 802.11g with the different data rates. The routing protocol that is used is a dynamic source routing protocol. The performance metrics used are number of hops per route, media access delay, retransmission attempts, download response time, upload response time and throughput. OPNET version 17.1 is used as a simulation tool to model and simulate ad-hoc network.

The simulation results conclude that the average media access delay of 802.11g is decreased when the data rate is increasing. The throughput of 802.11g standard is increasing when the data rate is increased. Additionally, the throughput of 802.11g is greater compared with 802.11b when they are used with the same data rate. Data traffic ratio of 802.11g standard is increased with increasing data rate.

Keywords: Mobile ad-hoc Network, Wireless Standards, DSR, FTP, OPNET Simulator

ÖZ

MANET (Mobile Ad-hoc Networks) mobil özel amaca yönelik (ad-hoc) ağların kısaltılmışıdır. Herhangi bir altyapı veya merkezi kontrol gerektirmeyen bir grup mobil cihazın birleşmesinden oluşur. Buna ek olarak yönlendirici ve giriş (Access Point) gibi merkezi bir dönemi içermez. Bu ağlar diğer ağlardan farklı olarak mobil cihazların bir ağdan diğer ağa hareket edebilmelerini ve ağdan ayrılmaları gibi farklı özellikler içerirler. Bu ağlarda yönlendirici olmadığından, yönlendirme işlemi ağı oluşturan düğümler tarafından yapılır.

Bu ağlar için, her biri farklı stratejilerde çalışan, yönlendirme protokolleri vardır. Bir yönlendirme protokolü istasyonlar arasında yön bulma maksadıyla kullanılır ve MANET'lerin genel performanslarında önemli rol oynar. MANET yönlendirme protokollerine örnek olarak Optimized Link State Routing (OLSR), Ad-hoc On demand Distance Vector (AODV), Dynamic Source Routing (DSR) ve Temporary Ordered Routing Algorithm (TORA) verilebilir.

Bu yönlendirme protokollerinin tipik IEEE 802.11 ağlarına olan etkisini en iyi şekilde anlamak MANET'lerin etkili tasarımlarını ve kullanımlarını sağlayacaktır.

Bu tezde FTP protokolü ile gerçekleştirilen veri transferinde 802.11b ve 802.11g standartlarının farklı veri hızlarında performansları incelenmiştir. DSR protokolü yönlendirme protokolü olarak kullanılmıştır. Performans ölçmek için yön boyunca sekme sayısı (number of hops per route) ortam giriş gecikmesi (Media Access Delay),

geri gönderim girişimi (Retranmission Attempts), indirme yanıt zamanı (Download Response Time), yükleme yanıt zamanı (Upload Response Time) ve çıkan iş oranı (Throughput) ölçüt birimleri kullanılmıştır. Ad- hoc ağların modellenmesi ve simülasyonu için OPNET'in 17.1 versiyonu benzetim aleti olarak kullanılmıştır.

Simülasyon sonuçları şöyle özetlenebilir: 802.11g'de ortalama ortam giriş gecikmesi veri hızı arttıkça azalmaktadır. Aynı zamanda bu çıkan iş oranı standartta veri hızı arttıkça da artmaktadır.

Buna ek olarak, aynı veri boyutlarında 802.11g'de ölçülen iş oranı 802.11b'den daha yüksektir. 802.11g'de veri trafik oranı veri hızı arttığı zaman artmaktadır.

Anahtar Kelimeler: MANETS Mobil Ad-hoc Ağ, Kablosuz Standartlar (802.11), DSR, FTP, OPNET Simulator

ACKNOWLEDGMENTS

At first I want to thank God after he gave me enough effort and success to work on this thesis. I would like to thank our supervisor Dr. Gurgu. Oz for her excellent support, kind commitment, encouragement, guidance, comments and making OPNET available for simulations to be carried out during this research process. Without her contributions this research would not have been possible. I am also grateful to all of my friends those who give me suggestions, discussions and comments led to a viable contribution to the simulation experiment and dissertation write-up. Thank you for your support.

To the loving memory of my father (Dlshad K.Othman), the first to teach me

To my beloved Mother (Dlkhwaz H.Musrafa), for her prayers to me

To my uncle (Gaffar K.Othman) for his support to me

To my brothers (Dashti and Ahmad) and sisters (Zheen, Wan and Rozh), for care and support all the time

To all my friends

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

OPNET	Optimized Network Engineering Tool
MANET	Mobile Ad Hoc Network
PRNET	Packet Radio Network
FTP	File Transfer Protocol
HTTP	Hybrid Text Transfer Protocol
DSR	Dynamic Source Routing
AODV	ad-Hoc On demand Distance Vector
ZRP	Zone Routing Protocol
OLSR	Optimized Link State Routing
DARPA	Defence Advanced Research Project Agency
ALOHA	Areal Location of Hazardous Atmospheres
CSMA	Carrier Sense Multiple Access
SURAN	Survivable Adaptive Radio Network
DOD	Department of Defence
GloMo	Globe Mobile Information System
NTDR	Near Term Digital Radio
DSDV	Destination Sequenced Distance Vector
RREQ	Route Request
RREP	Route Reply
WLANs	Wireless Local Area Networks
CM	Control Module

SANET	Static Ad-Hoc network
VANET	Vehicular Ad-Hoc Networks
In VANET	Intelligent Vehicular Ad-Hoc Networks
I MANET	Internet Based Mobile Ad-Hoc Networks
QOS	Quality of service
TCP	Transmission Control Protocol
TTL	Time To Live
Wi-Fi	Wireless Fidelity

Chapter 1

INTRODUCTION

1.1 Introduction

MANET is a network made up of two or more of the so-called node and can be used in wireless networking capabilities. These nodes, such as laptop computers, mobile phones and PDAs have a set of specific capabilities for direct transmission which can be directly used to communicate between the two devices in the same range, otherwise intermediate nodes will be used. Thus, a multi-hop scenario will happen in which numerous intermediate will be used before they reach the end destination. Each node works as a router. Communication success depends on the cooperation of other node. Intermediate nodes are used to transfer many of the routing protocols [1] that have been proposed to the network from intruders. Many of them assume that other nodes are trustable so they do not study attack and security subjects. The lack of infrastructure and rapid deployment practices makes them more susceptible to a wide range of security attacks. Any nodes that can move randomly and freely in any direction will order themselves automatically in the network. Topology of the network changes frequently, unpredictably and rapidly, thus changing the situation of trust between nodes. Many solutions exist to solve such attacks [2], [3], [4] but they cannot stop the attacks like a wormhole attack. One of the interesting research areas is a routing protocol. Many routing protocols have been developed from MANET such as DSR, AODV, and OLSR etc.

The MANET simulation modeling tool will make you able to understand the process in networks. In recent years, the ad-hoc routing protocols developed multiple networks, in order to find the easiest way between the source and destination. To be a potential transfer data between two nodes, due to the limited transfer of node, multi hops are required. Because of the mobility of the nodes, the condition becomes even more complex. Routing protocols can be classified in three different parts called "proactive", "reactive" and "hybrid protocols". Proactive routing protocols are usually schedule-driven, for instance Destination Sequenced Distance Vector (DSDV). Reactive routing protocol does not orderly update the routing knowledge. Update of information happens when some data needs to be transferred. Some examples of reactive routing protocols are Ad-hoc On demand Distance Vector (AODV) and Dynamic Source Routing (DSR). Hybrid protocols are a mix of both approaches reactive and proactive, for instance zone routing protocol (ZRP).

Dynamic Source Routing (DSR) protocol's protocol is an on-demand routing protocol. Hence and beacon less does not require periodic hello packets, that's the main difference between DSR and the other on demand routing protocols. Gaze a source node that does not have a route to the destination. When the source node has sent a data packet to the destination, then it starts a route request packet. This route request is overflowed throughout the network. The DSR's key features are source routing, the data packet sender knows the all path route to the destination. Route cache it stored all routes. The source node when sent data packets it loads the entire route in the packet header. Intermediate nodes whose purpose is to forward the packet depend on the route in their header.

In this thesis, I used mobile ad-hoc network with reactive protocol dynamic source routing protocol DSR is explained. File Transfer Protocol (FTP) application is considered for three cases: one server to one client, one server to twelve clients, one server to twenty four clients. The scalability of network topology is considered 25 nodes with two type of wireless standards 802.11g and 802.11b that have different data rates. All nodes are used in this network are not in the same coverage area of each other. The intermediate nodes help server and client to reach each other. Furthermore, the performance metrics were chosen for comparison between wireless standards that are important for application and protocol. These standards which are number of hops, media access delay, retransmission attempts, routing traffic ratio, throughput, download response time and upload response time. In addition, I used OPNET 17.1 simulator to calculate and reach the results.

The organization this thesis comprises six chapters. Chapter 1 contains introduction description and survey. Chapter 2 gives details about MANET and wireless network. Chapter 3 contains overview and important properties of the DSR protocol and deals with file transfer protocol (FTP). Chapter 4 explains OPNET 17.1 and simulation setup. Chapter 5 contains simulation results and discussion. Chapter 6 provides the conclusion and references.

1.2 Survey and Related Work

A mobile ad-hoc network, as it is the called proposes "MOBILE”. Free to move around autonomously free to move around independently means that mobile nodes are free to agree with each other over limited bandwidth wireless links without centralized base station. It is one of the primary reason for having multi-hop features or several hops to guarantee transmission of the data packets between nodes. Other factors are the incomplete radio range and the constant movement of the mobile nodes which is why the mobile nodes have to double as routes in order to link between nodes. The MANETs have another cognition advantage of being dynamic in nature as the nodes are independent and free. Therefore, due to the presence of the dynamic nature of the MANET routing protocols, you should be able to cope with environmental changes and still retain the tracks despite the changing nature network connection. MANETs support different routing protocol that can be classified into proactive protocol, reactive protocol and hybrid routing protocol.

The spotlight of this thesis shifts across the reactive protocols particularly DSR.

The main aim in using Dynamic Source Routing (DSR) is that it keeps on bandwidth utilization by managing the packets by control restriction and doesn’t need the periodic schedule to update as in schedule driven approaches. The DSR’s primary function is to easily start a path creation only when the source node or server nodes desire to broadcast; after the s node has requested to transmit it will set up a path with flooding the route request (RREQ) message packets purpose for the destination node. In this case if the request "RREQ" message packet obtains delivered to the destination node nodule, then only it will be able to send the source node the route reply (RREP) message with the "RREQ" received message to pass through the formerly defined route.

Wireless technology comes through the IEEE 802.11 standards families who show an additional role in the global infrastructure of the Internet. This wireless fidelity (Wi-Fi) is the another famous name in this technology which provides low cost wireless Internet facility for the last users, with up to 54 Mbps data transmission rate at the physical layer. IEEE 802.11b the data rate up to 11Mbps and IEEE 802.1g the data rate up to 54 Mbps standards are two of the most popular technologies on the wireless LAN market.

File transfer protocol is a procedure of transferring data files from the source node to the destination node over a network. The FTP has the simple way of sending file and receiving file over internet. File transfer protocol divides files into segments and assigns a reference number to each.

In [5] the author evaluates the performance and compares the two reactive routing protocols AODV and DSR on FTP application. In this paper, it's concluded that the performance of AODV and DSR is dependent on various variables and environmental conditions like topology, node mobility, node density, type of traffic etc. For route discovery, AODV sends many small routing control packets, while DSR sends fewer but bigger control packets during transmission of data packets. All this results into making DSR more useful in smaller networks with less mobility and

AODV more appropriate in ad hoc networks with a higher mobility and higher data transfer rate. In [6] the author evaluates and analyzes the performance of reactive (AODV, DSR) routing protocols based on traffic generators like FTP application. In this paper, it's concluded that the delivery ratio for reactive protocols, namely AODV and DSR, is approximately 100%. Both protocols have almost the same delivery ratio at all pause times hence these show the independence of delivery ratio on pause time. In [7] the author evaluates the performance of reactive (DSR) routing protocols under different applications like FTP, video conference and HTTP applications based on delay, throughput using OPNET14.5.in this paper, it's concluded that DSR routing protocol is made under different traffic load like HTTP, FTP, Email, video conference at fix mobility 10m/sec. The average end to end delay is highest in video conference while lowest in FTP and HTTP. Throughput is also highest in video conference and lowest in FTP and HTTP. In [8] the author analyzed performance evaluation of three reactive routing protocols Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Temporally Ordered Routing Algorithm (TORA) for the three different Physical Characteristics namely Direct Sequence. In this paper, it is concluded that AODV performs best in case of wireless LAN delay, retransmission attempts and in media access delay due to frequent broadcasting of RREQ and route re-initialization messages to find an optimal fresh path. In contrast, TORA performs best in case of throughput as it does not engage in the route discovery again and again as it already have a DAG of all the nodes in the network. DSR has higher delay as DSR maintains a large route information table to store transmission data and consume time during updating periodically with frequent changes occurring due to high mobility. In [9] the author analyzes performance modeling of IEEE 802.11 WLAN using OPNET. In this thesis it is concluded delay increases with larger number of nodes. The models built using OPNET simulator were validated using propagation measurements from wireless laptops And access points for an IEEE 802.11b/g WLAN. In [10] the author evaluates the performance analysis of AODV, OLSR, GRP routing protocol by considering IEEE 802.11standard on FTP application. In this paper, it is concluded that media access delay of 802.11g performs better than 802.11a and 802.11b. And also throughput of 802.11g is better than 802.11b. Based on the results in Table 1.1 we can come up with the following conclusion: In our study we considered different number of clients, using different standards (with different data rates) and evaluated additional performance metrics on the network using OPNET 17.1 which not done before.

Table1.1: Summarv of related work

Ref. No.	Simulation Setup							
	Simulator	**Application Type**	**Routing protocols**	**Number of nodes**	**Mobility**	**Area of Simulation**	**IEEE 802.11**	**Performance metrics**
[5]	OPNET9.1	FTP	DSR AODV	15	Mobile node Speed 5 m/s	3000m x 3000m	802.11(b) 11Mb	Throughput Retransmission Routing traffic received
[6]	OPNET9.1	FTP	DSR, AODV and WRP	50	Mobile node	1000m x 1000m	802.11 (b) 11Mb	Throughput Packet Delivery Ratio FTP Traffic
[7]	OPNET14.5	Http, FTP, E-mail	DSR	35	Mobile node	800m x 800m	802.11(b)	delay Throughput
[8]	OPNET 11.1	FTP	DSR, AODV and TORA	7	Mobile node	1500 m x 1500 m	802.11(b) 2Mb	Retransmission attempts Media access delay Throughput
[9]	OPNET 14.5	FTP	DSR	2,10,15 25,30	Mobile node	1000m x 1000m	802.11(b) 11Mb 802.11(g) 54Mb	Throughput
[10]	OPNET 9.1	FTP	DSR, AODV, GRP, OLSR	80, 100	Mobile node	1500 m x 1500 m	802.11(b)11m 802.11(g)11m 802.11(a) 11m	Retransmission attempts Media access delay Throughput

Chapter 2

WIRELESS TECHNOLOGY AND MOBILE AD HOC NETWORKS

2.1 Introduction

Today wireless networks are gaining peak popularity, as the user wants wireless connectivity without having to think about their geographic position. Users can communicate and transfer data between each other without any wired medium between them. One of the biggest reasons of the popularity of these networks is broadly penetration of wireless devices. Wireless "applications" and "devices" mainly confirm on wireless local area networks (WLANs). This type has mainly two modes of operations, i.e. in the existence of Control Module (CM) also recognized as base stations, and ad-hoc connectivity where there is no Control Module. MANET does not depend on fixed infrastructure in order to carry out their operations. The operation mode of such network is can that it stands alone, or may be linked with one or multiple points to provide internet and connectivity to cellular networks.

These networks have the same conventional problems of wireless communications i.e. bandwidth limitations"," enhancement of transmission quality "," battery power" and "coverage problems".

Before describing wireless networks, it is significant to understand what a network is and what different kinds of networks are available today.

A network is any set of devices/all computers connected with each other by intermediary of communication channels that help the users to share resources and communicate with other users. There are two major types of the i.e. "wired network" and" wireless network".

Wired network are those networks in which computer devices are attached to each with the help of wire. The wire is used as a medium of communication for transmitting data from one point of the network to the anther point of the network.

Wireless network means that any computer can communicate with each other and transfer data without a wire. Also the communication medium between the computers device is wireless. If a computer device needs to communicate with another device, the destination device must be put within the radio frequency range of each other. The users of wireless networks transmit and receive data using electromagnetic waves. Recently wireless networks are more popular day by day because of their mobility, simplicity and very affordable and cost saving installation.

2.2 IEEE Standard for Wireless Networks

Institute of Electrical and Electronics Engineers (IEEE) define the standards for related technologies [1]. IEEE defined three major operational standards for wireless LAN, i.e. IEEE" 802.11a", "802.11b" and" 802.11g". The completely three standards belong to IEEE 802.11 protocol family. In 1999 802.11a standard was confirmed by

IEEE. The "802.11a" has range data rate of 54Mbps. The 802.11b is the most established and frequently deployed wireless network standard. Most of the public wireless like “hotspots” use 802.11b standard. It operates in 2.4 GHz spectrum and the nominal data transfer is 11 Mbps. In 2002 and 2003, WLAN products supporting a newer standard called 802.11g emerged on the market. 802.11g attempts to combine the best of both 802.11a and 802.11b. 802.11g supports bandwidth up to 54 Mbps, and uses the 2.4 GHz frequency for greater range. We chose two of wireless standards 802.11b and 802.11g to enable me to compare between wireless standard 802.11g with different data rate and compare between wireless standards 802.11g and 802.11b with same data rates. Wireless standard 802.11g is backwards compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

2.3 Wireless Networks

Ad-hoc networks have no infrastructure, nodes are free to join and leave the network. All nodes in this kind of network can connect with each other through a wireless link. A node can work as a router to forward the data to the neighbor's node. Therefore this kind of network is also recognized as infrastructure less networks. Ad-hoc networks have no centralized administration, although, ad-hoc networks have the ability to handle any malfunctioning in the nodes or any changes that it is experiencing due to topology changes. Whenever a node wants to down or leave the network it causes the link between other nodes to be broken. The influenced nodes in the network simply request for new routes and new links are established.

Ad-hoc networks can be divided in Static Ad-hoc Network "SANET" and Mobile Ad-hoc Network "MANET". In the static network there is no mobility in the nodes of the network, that is why they are known as static ad-hoc networks. The geographic locations of the nodes or the stations are fixed. Mobile ad-hoc network is an autonomous system, where connection is made between nodes/station through wireless links. To join or leave the network there is no restriction on the nodes. Therefore the nodes join or leave freely. Mobile ad-hoc network topology is dynamic and can change quickly because it can organize itself randomly and the nodes move freely. This property of the nodes makes the mobile ad-Hoc networks unpredictable from the point of view of topology and scalability. See Figure 2.1

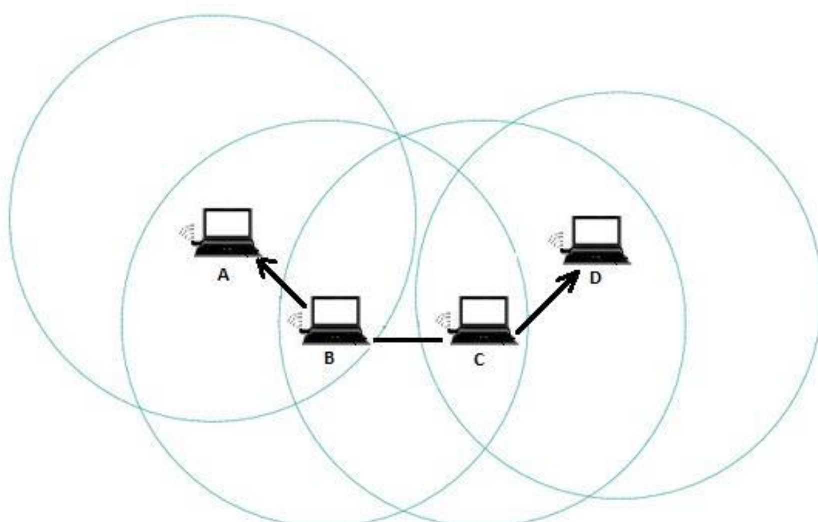

Figure 2.1: Mobile Ad-Hoc Network [11]

2.4 Characteristics of Mobile Ad-Hoc Network

When a node wants to communicate with another node, the destination node must be located within the radio range of the source node wanting the communication. The intermediate nodes in the network support in routing the packets for the source node to the destination node. These networks are entirely self-organized, at the same time nodes are autonomous and play the role of router and host. MANET is self-controlling, i.e there is no centralized control and the communication is carried out with blind mutual trust amongst the nodes. The network can be set up anywhere; there is no geographical restriction. The limited energy resource of the nodes is one of the limitations of MANET.

Three Types of Mobile Ad-Hoc Network:

Vehicular Ad-Hoc Networks ("VANETs")

Intelligent Vehicular Ad-Hoc Networks ("In VANETs")

Internet Based Mobile Ad-Hoc Networks ("I MANETs")

2.4.1 Vehicular Ad-Hoc Networks ("VANET's")

VANET is a type of Mobile Ad-Hoc network where vehicles are equipped with wireless and form a network without help of any infrastructure. The equipment is placed inside vehicles as well as on the road for providing access to other vehicles in order to form a network and communicate.

2.4.2 Intelligent Vehicular Ad-Hoc Networks ("In VANET's")

Vehicles that form Mobile Ad-Hoc Network for communication using WiMax IEEE 802.16 and WiFi 802.11. The main aim of designing InVANET's is to avoid vehicle collision so as to keep passengers as safe as possible. This also help drivers to keep secure distance between the vehicles as well as assist them at how much speed other vehicles are approaching. InVANET's applications are also employed for military purposes to communicate with each other.

2.4.3 Internet Based Mobile Ad-Hoc Networks (I MANET's)

These are used for linking up the mobile nodes and fixed internet gateways. In these networks the normal routing algorithms do not apply [12].

2.5 Routing in MANETs

Mobile ad-hoc network is the rapid growing technology from the past 20 years. The gain in their popularity is because of the ease of deployment, infrastructure less and their dynamic nature. MANETs generate a new set of demands to be implemented and provide capable better end-to-end communication. MANETs uses TCP/IP structure to provide the means of communication between communicating work stations. Work stations are mobile and have limited resources**,** therefore the traditional TCP/IP model necessarily needs to be renewal or modified, in order to recompense the MANETs mobility provide effective functionality. In addition, routing in any network is a key research area for researchers. Routing protocols in MANETs are challenging and attractive tasks; researchers are giving immense amount of attention to this key area [13].

2.6 Classification of MANETs Routing Protocols

Routing protocols in MANETs are classified into three different classes according to their employment:

1. Reactive protocols

2. Proactive protocols

3. Hybrid protocols

The hierarchy of routing protocol in MANET is shown below in Figure 2.2.

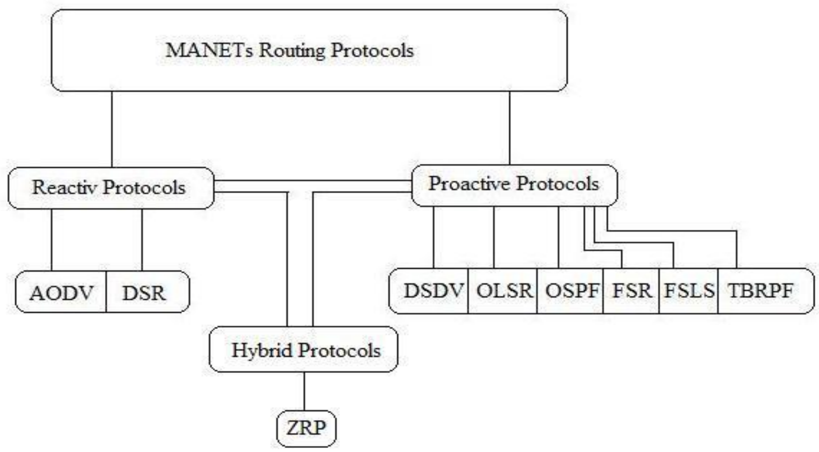

Figure 2.2: MANET Routing Protocols [11]

2.6.1 Reactive Protocols

Reactive protocols are also recognized as on demand driven reactive protocols. The main reason they are known as reactive protocols is that they do not begin route discovery by themselves, only when they are sent request [9], when a source node requests to find a route. When one node wants to communicate with another node in the network, and the source node does not have a route to the node it wants to communicate with, reactive routing protocols will generate a route for the source to the destination node. Reactive protocols normally:

- When tries to find the destination ("on demand"), using flooding technique to deploy the queuery.

- Don not find any route until demanded.
- Do not consume bandwidth to sending information.
- Only consume bandwidth, when the source node starts transmitting the data to the destination.
- Reactive protocols like (AODV and DSR).

2.6.2 Proactive Protocols

Proactive routing protocols work as the other way around as compared to reactive routing protocols. These protocols always maintain the updated topology of the network. Every node in the network knows about each other in advance, in other words the complete network is known to all the nodes making that network. All the routing information is usually kept in tables [13]. There is no change in the network topology; these schedules are updated according to the change. The nodes exchange topology information with each other; they can have route information any time when they needed [13]. Proactive protocols like (DSDV, OLSR, OSPF, FSR, FSLS and TBRPF).

2.6.3 Hybrid Protocol

Hybrid protocols exploit the strengths of both reactive protocol and proactive protocol, and integrate them together to get good results [9]. The area of network is divided into zones, and use different protocols in the two different network zones i.e. one of the protocols is used within the zone, and the other one is used between them. An example of hybrid routing protocol is zone routing protocol (ZRP). ZRP protocol uses the proactive mechanism for route establishment within the nodes neighborhood and for communication between the neighborhoods it the reactive protocols.

Chapter 3

DSR PROTOCOL AND FTP APPLICATION

3.1 Overview of the Dynamic Source Routing (DSR) Protocol

Dynamic source routing protocol is one of the most reactive protocols in ad-hoc network. It is composed of two basic mechanisms for its operation namely; "Route Discovery" and "Route Maintenance" of source routes in the ad-hoc network.

Route discovery is the mechanism containing the route request "RREQ" message and route reply "RRER" message. In the discovery part, when a node wants to send a message to a destination node at first they send broadcast route request "RREQ" message to the all neighbor nodes with unique ids. After that only the destination node sends route reply "RRER" to the source node. It is only sent when the "RREQ" packets reach the proposed destination node. The destination node uses the cached routing knowledge to traverse the "RREQ" packet to the source node. If the cache knowledge in the "RREQ" route request packet is not enough, the destination node must use the information in the route reply "RRER" packet header. The DSR protocol chooses the shortest path between source node and destination node, see Figure (3.1).

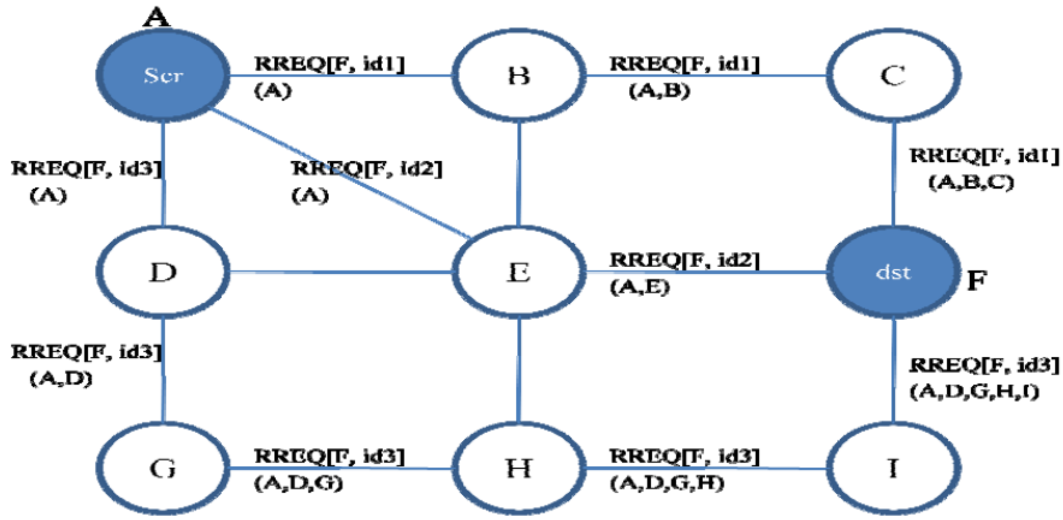

Figure 3.1: Route Discovery Process in DSR protocol [14]

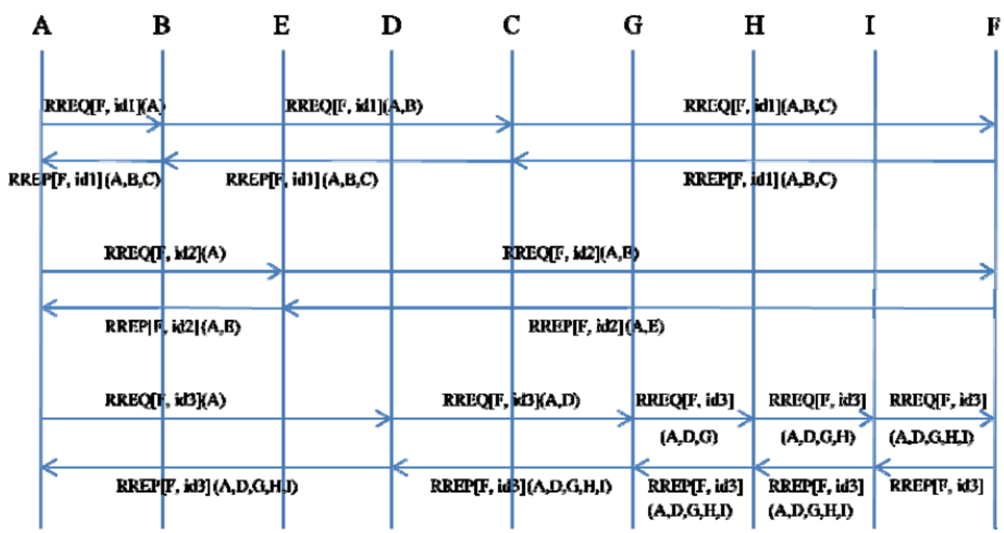

Figure 3.2: Route Discovery Sequence in DSR protocol [14]

Route maintenance starts to work when the transmission packet between source node and destination node is lost. The node causing the lost transmission is removed from the rout knowledge cached by the node in the area network, after that route discovery starts again to establish the new reliable route to reach the destination node.

The absence of periodic table update messages in DSR makes its bandwidth efficient. DSR does not use periodic HELLO messages. Instead when establishing a route it floods the network with RREQ packets. When a destination node receives the RREQ packet it responds with a RREP packet. Which carries the same information as the RREQ packet about the route it traversed. When an intermediate node receives a RREQ packet, as long as it is not a duplicate RREQ packet and its TTL counter is not exceeded, the intermediate node rebroadcasts the RREQ packet to all its neighbors. And the sequence number in the RREQ packet helps to avoid packets from looping. All duplicate RREQ packets are dropped [13].

3.2 Optimization of Dynamic Source Route (DSR) Protocol

The DSR was revised since 1994 in simulation and analyzing optimization. In this thesis the required rules are investigated for correct protocol as in safe node reply to a route request for another node and improvements to a route discovery and route maintenance [15,16] with optimization to the protocol including.

- Several different route cache data structures and algorithm, and the rules that govern how the route cache can be used to limit the re propagation of route discoveries.
- Allowing source route to be less expensive if nodes are closer together.
- Slaving packets that are sent with an incorrect source route, so that route maintenance has time to react without dropping packet.
- Improving the speed of data removed from the node caches.
- The use of control message piggybacking to support asymmetric routes.

- The two phase structure of route discovery.
- Techniques for avoiding route replay storms.

3.3 The Dynamic Source Route (DSR) Protocol Performance

The DSR performances are significantly better than the three other ad-hoc network routing protocols. When measured in three key metrics and a forth routing protocol runs 50 nodes simulation study [17]. They are objected to identical workloads packets with identical node movement. This makes it possible to compare the performance of the protocols, since they were compared in identical environment.

3.4 Caching Strategies of Dynamic Source Routing Protocol (DSR)

The Dynamic Source Routing (DSR) protocol is the protocol of option in our thesis. It is a simple but very efficient routing protocol for ad-hoc network. In this part we propose to take a closer look at some of the exotic features of DSR protocol with regards to it caching mechanism.

3.4.1 Cache Organization of the DSR

One of the major advantages of the dynamic source routing is the availability of a caching mechanism. A cache of the DSR protocol is basically a buffer especially for storing routes. The caching mechanism in DSR ensures the avoidance of extravagant route discoveries, in that way reducing control overheads and at the same time saving massive bandwidth and energy. When routes are discovered, they are directly stored in the nodes routes caches so that subsequent transmission of data packets along the same routes can take place without re-initiating a fresh route discovery process.

One of the basic design choices to be made in developing a caching strategy for DSR protocol is to determine how the cache is to be ordered or structured, i.e., locating the type of data structure to be used to represent the cache. In DSR protocols two types of cache organization are used, namely: "path cache " and " link cache". in path cache a node caches a complete path from route discovery process where as in link cache, caches in node each link separately. A path cache is not very complicated in this situation to implement and it can be easily ensured that all paths are loop-free, since each individual route from an "RREP" route request is loop-free. To locate a route in a path cache, the source node can simply search its cache for any ready path that leads to the destination node. Contrariwise, to locate a route in link cache, a node must use a much more intricate search algorithm to locate the current best path through the graph to the destination node. Implementing such a search algorithm is very tricky and needs much CPU processing.

3.4.2 Cache Timeout of the DSR protocol

Cache timeout is a strategy designed to transact with the route staleness in DSR caching mechanism. It is the amount of time that a route would save in a nodes route cache before it would be removed. Cache timeout predicts the lifetime of an individual route. Cache timeout strategies, similar to cache capacity, also inform of some design choices to be considered while implementing the Dynamic Source Routing (DSR) protocol. Although path cache have a mechanism for deleting route entries by a capacity limit, for link cache the timeout can be "adaptive" or " static". In adaptive timeout, each link is deleted from the cache after a certain amount of time has elapsed after the link was added to the cache. Otherwise, in adaptive timeout, a node decides a convenient time out after which an added link will be removed from the cache. The adaptive timeout value should be founded on the properties of the link or the nodes constituting the last points in the link.

3.4.3 Cache Capacity of the DSR protocol

Cache capacity is the amount of routes that can be saved in the cache of any private node. Cache capacity is an important choice to be considered while designing a DSR protocol. About a" link cache", the obvious design choice is to allow the cache to save any links that are discovered, since there is a fixed maximum number of N2 links could exist in a mobile ad hoc network of N nodes. However, for a "path cache", the maximum storage area that could be needed is much larger than that of link cache, since each path is cached separately and there is no sharing in the data structure even when two paths share a number of common routes.

3.5 File Transfer Protocol (FTP)

Is a method to transfer files between server node and client node on the network. FTP is a simple network protocol based on network protocol. File transfer protocol and uses two types of modes to transferring data.

FTP is a file transfer protocol used by FTP applications to implement vast data transfer from server to users. Main aims of FTP include file sharing promotion between computers, usage of remote systems through some applications, use of remote systems through some applications. Data transfer of FTP is very efficient and reliable. FTPs are designed individually for application programs for utilization. To understand how the FTP service functions the model is explained in Figure (3.3).

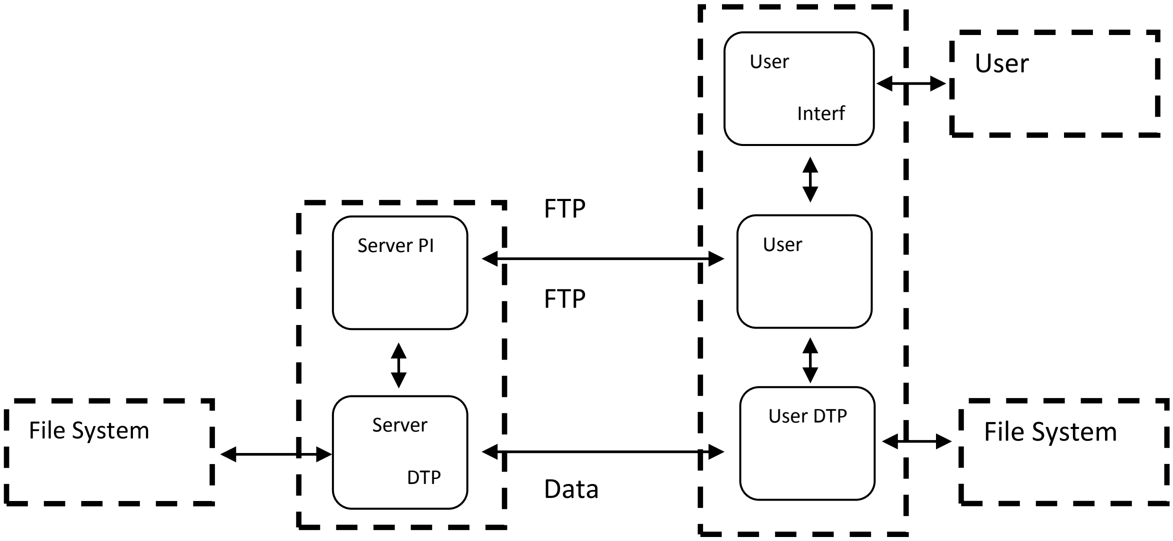

Figure 3.3: FTP Model [18]

There are many modules in Figure (3.3) which participate in the enforcement of FTP service by the application programs. Generally, in a FTP connection setup, a control connection is started by user protocol interpreter ("PI") to utilize user-PI for generating an FTP command towards server-PI when the user wants to begin the connection. Similarly, an FTP reply is acquired from server-PI to user-PI. Through control connection performed whole process. FTP command contains some parameters for "data connection" such as data port, transfer mode, data representation type and structure by these parameters. File transfer protocol command also holds the information about the operation of the file by the operating system (OS), e.g, delete, retrieve, store, append. User data transfer process (DTP) requires listening to the server start data connection in defined data port to establish and transfer data according to the defined parameters.

Chapter 4

OPNET SIMULATION ENVIROMENTS AND SIMULATION SETUP

This chapter details the architecture of OPNET 17.1 simulator. The second section details how to use the MANET model in OPNET to simulate DSR networks.

4.1 OPNET Architecture

OPNET provides a comprehensive development environment for modeling, performance evaluation of communication networks and distributed systems [19]. The package consists of a number of tools, each one focusing on particular aspects of the modeling task. These tools fall into three major categories that correspond to the three phases of modeling and simulation projects: Specification, data collection, simulation and analysis. It is important that these phases are important performed in sequence. They generally form a cycle, with a return to specification following analysis. Specification is actually divided into two phases: initial specification and re-specification, with only the latter belonging to the cycle, as illustrated in the following Figure (4.1).

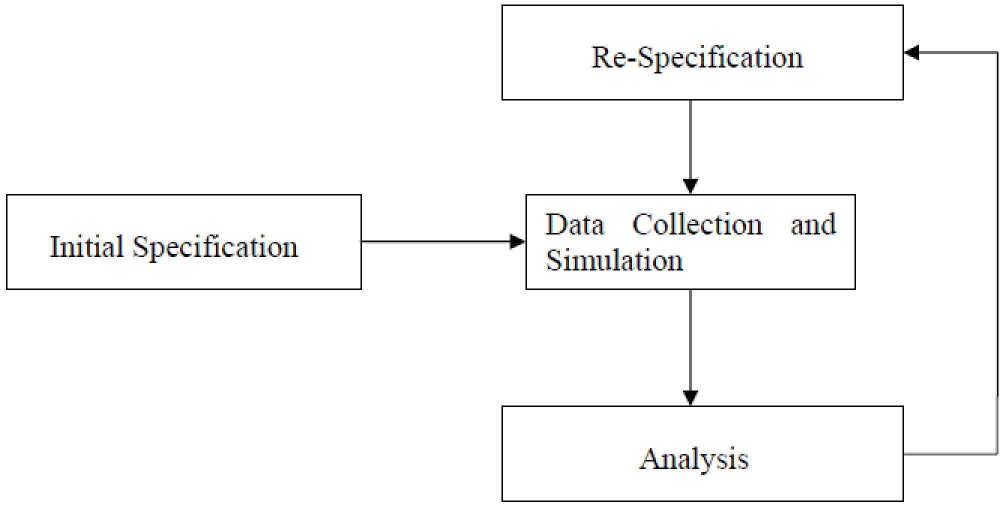

Figure 4.1: OPNET Structures [20]

4.2 Profile Configuration

Profiles describe the activity patterns of a user or group of users in terms of the applications used over a period of time. You can have more than one different profiles running on a given LAN or workstation. These profiles can represent different user groups, e.g. An Engineering profile, a sales profile and an administration profile to depict typical applications used for each employee group.

Profiles can execute repeatedly on the same node. OPNET enables you to configure profile repetitions to run concurrently (at the same time) or serially (one after the other).

4.3 Application Configuration

A profile is constructed using different application definitions; for each application definition you can specify usage parameters such as start time, duration and repeatability [21]. You may have two identical applications with different usage parameters; you can use different names to identify these as two distinct application definitions. For example, the engineer may browse the web frequently in the morning but occasionally in the afternoon. Hence, you can create two different application definitions for web browsing, such as web_browsing_morning and web_browsing_noon, with two different usage patterns. You can also create application definitions based on different workgroups. For example, you may have an engineering email and a sales email where the former may send 3 emails/sec while the latter may send 10 emails/sec.

4.4 Mobility of nodes

The speed of a node in MANET plays an important role towards the performance of routing protocols [22]. Mobility of nodes has a direct impact on pause time; it is a time for which a data packet stays in a node waiting for a destination, before moving to that destination.

4.5 Simulation setup

Table 4.1. OPNET Simulation Configuration

General parameter	Value
Area	1000m x1000m
Simulator	OPNET 17.1
Network Size	25 nodes
Mobility Model	Random way point
Traffic Type	FTP
Physical Characteristics	802.11g and 802.11b
Data Rates	11Mb - 24Mb - 54Mb
Routing Protocol	DSR
Simulation Time	300 Sec
Address Mode	IPv4

4.6 Simulation steps

This chapter explains the steps for our simulation by using OPNET modeler 17.1, and each step is detailed in pictures. We have 12 scenarios and the aim of this thesis is to show the difference between wireless standards 802.11g and 802.11b over File Transfer Protocol (FTP) application.

Step 1: Go to start menu, double click on the Visual Machine, as shown in Figure 4.2.

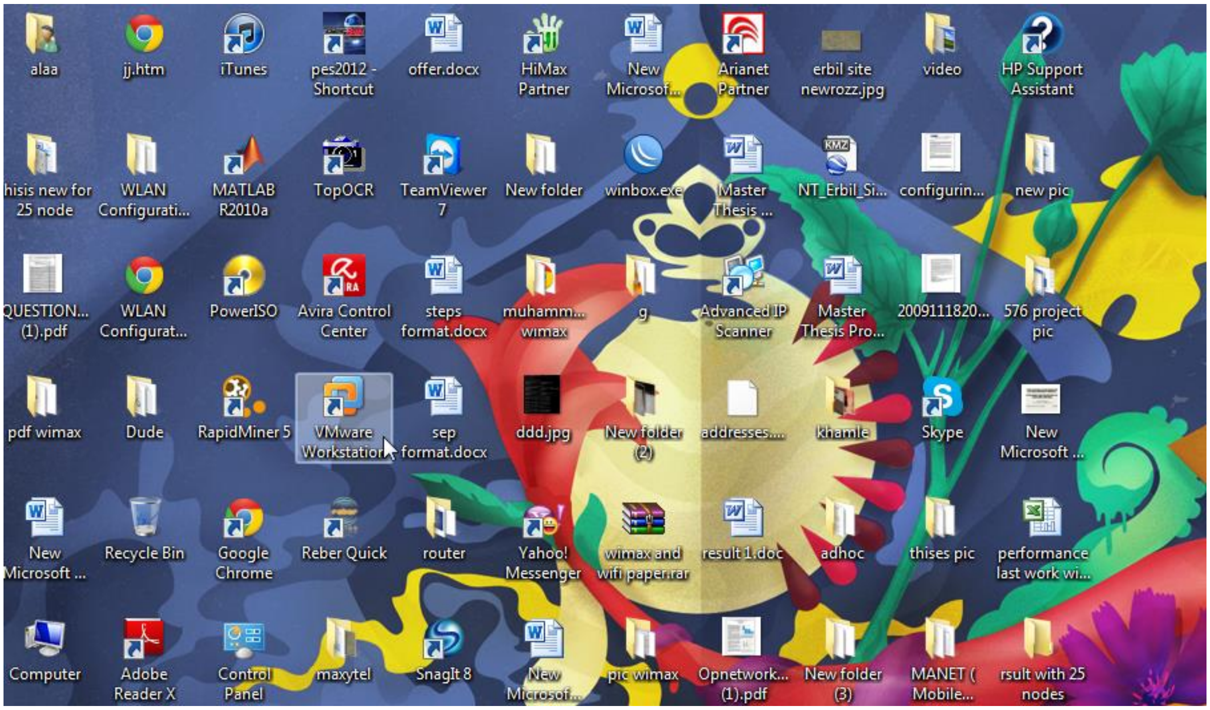

Figure 4.2: VMware Workstation

Step 2: After opening the new screen you should copy path from file (Shortcut to bin) as in Figures 4.3 and 4.4 to Visual Studio Command Prompt (2010) as in Figure 4.5.

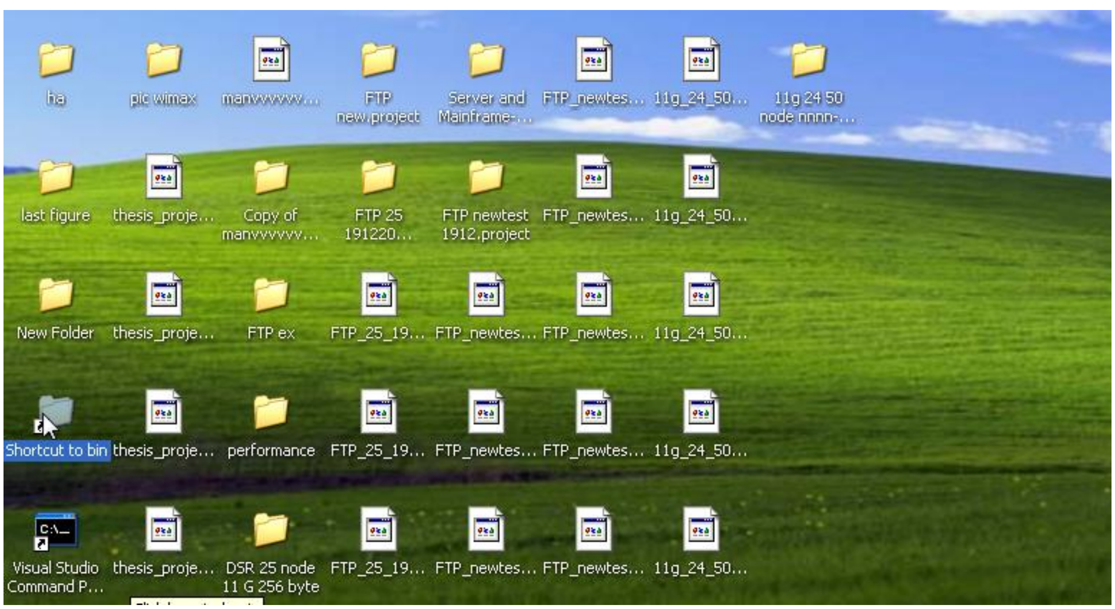

Figure 4.3: Path of OPNET 17.1

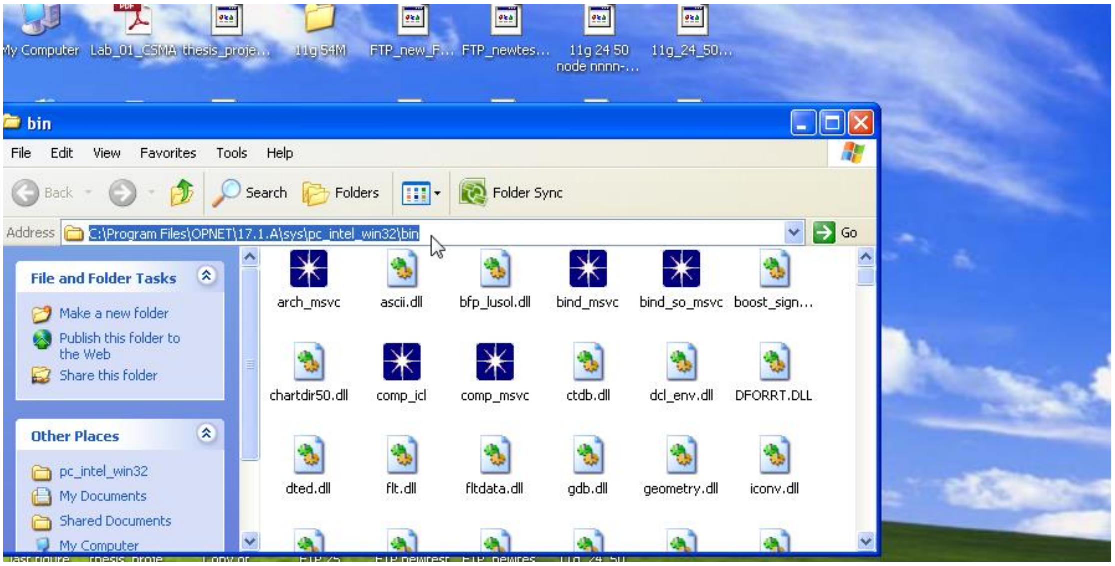

Figure 4.4: Binary Window for OPNET 17.1

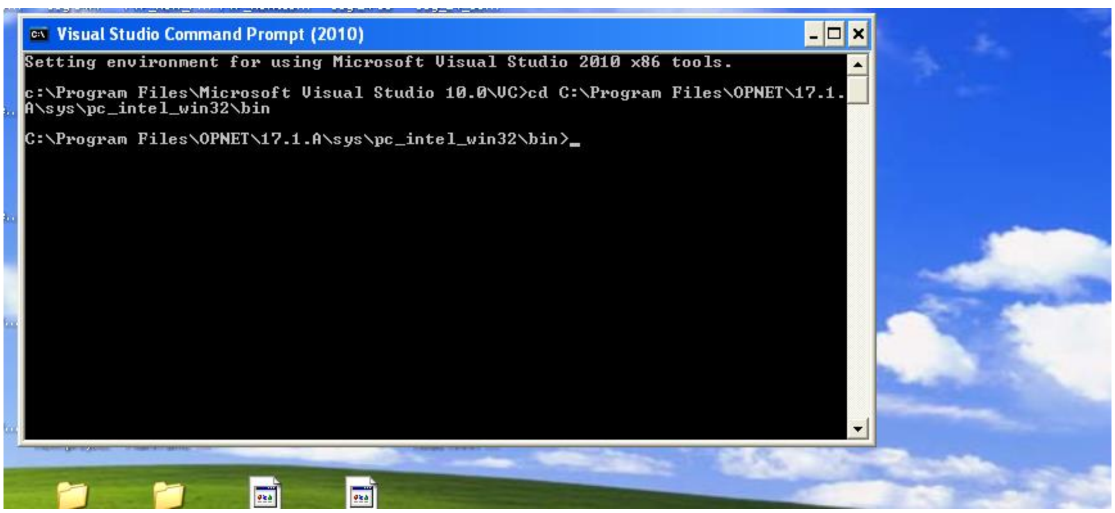

Figure 4.5: Visual Studio Command Prompt 2010

Step 3: Write on a black screen (Visual Studio Command Prompt (2010)) (CD) after that paste the path (C:\Program Files\OPNET\17.1.A\sys\pc_intel_win32\bin) as a Figure 4.6.

Step 4: write on a black screen (Visual Studio Command Prompt (2010)) (modeler) and click ENTER, you should wait 10 second as a Figure 4.6.

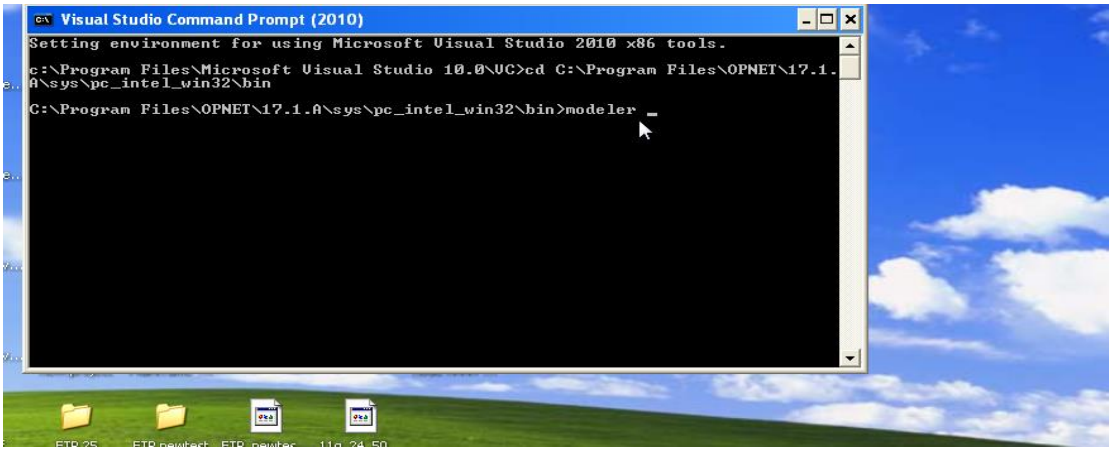

Figure 4.6: Visual Studio Command Prompt 2010

Step 5: After reading agreement it will be open OPNET Modeler shown as in Figure 4.7.

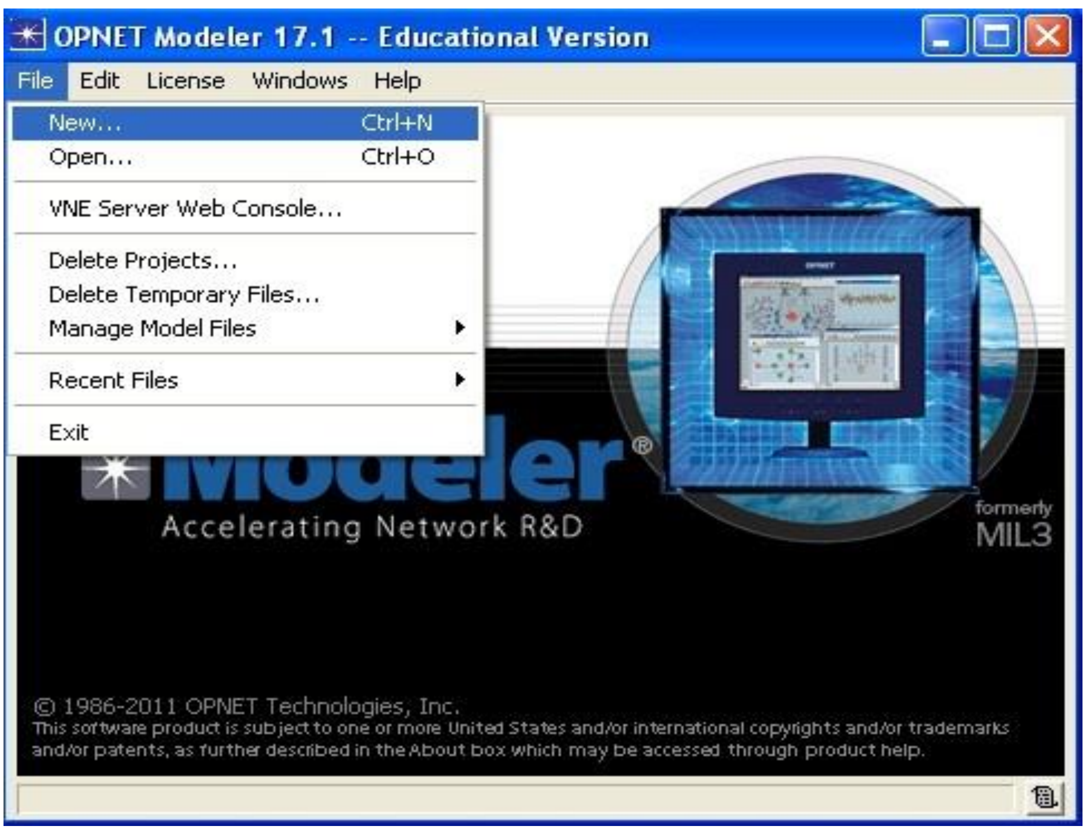

Figure 4.7: Windows OPNET Modeler 17.1

Step 6: For open new scenario click on File and select New and click OK, as in Figures 4.8 and 4.9.

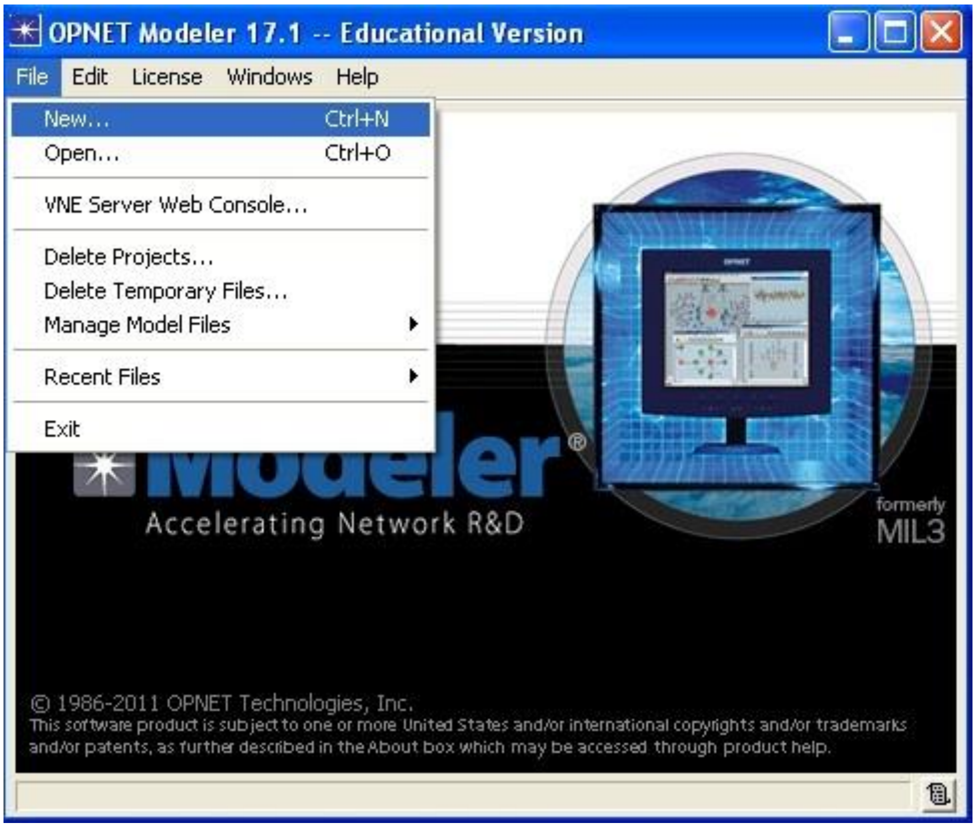

Figure 4.8: OPNET Modeler 17.1

Figure 4.9: Create New Project

Step 7: In this step we should write the name of our project, as in Figure 4.10.

Figure 4.10: Enter Name of Project

Step 8: Choose the Create Empty Scenario from initial topology list windows and click Next, as in Figure 4.11.

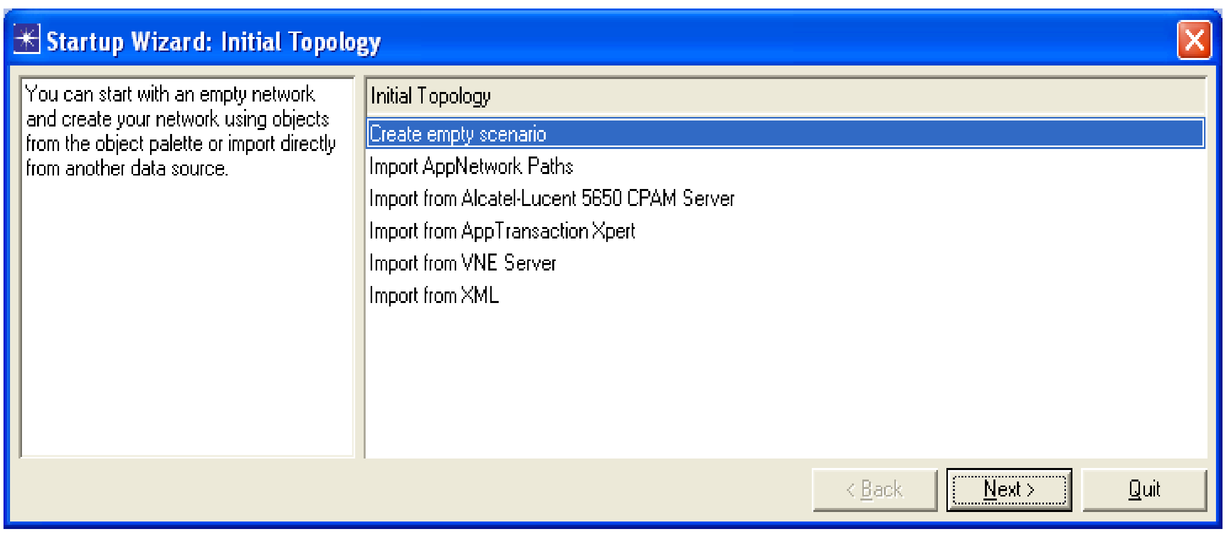

Figure 4.11: Initial Topology

Step 9: In our Simulation we select the campus as network scale like in Figure 4.12 and select Next. The size of it as shown in Figure 5.13 and select Next; The area 1000 *1000 square meters.

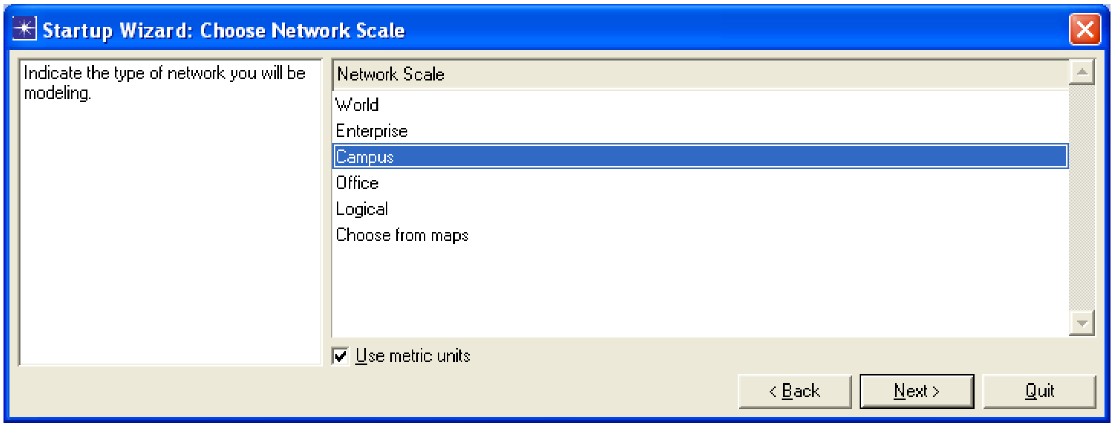

Figure 4.12: Choose Network Scale

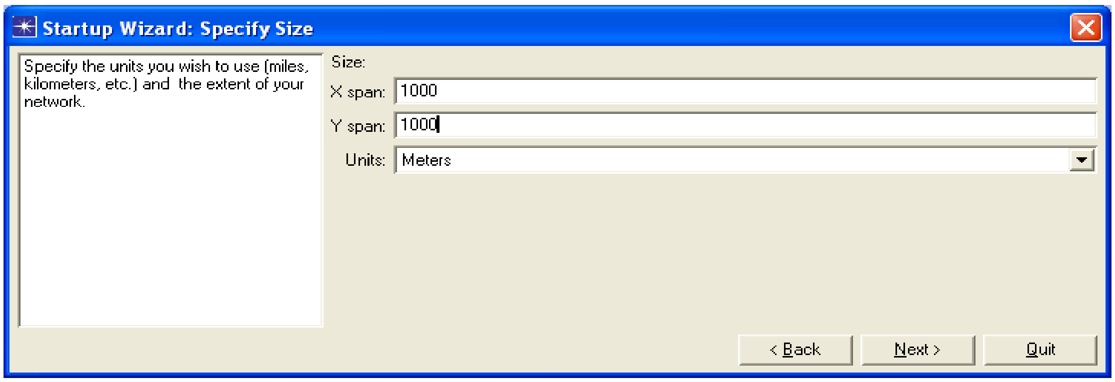

Figure 4.13: Specify Size

Step 10: In the technology list we choose my work (MANET) and click Next , as in Figure 4.14.

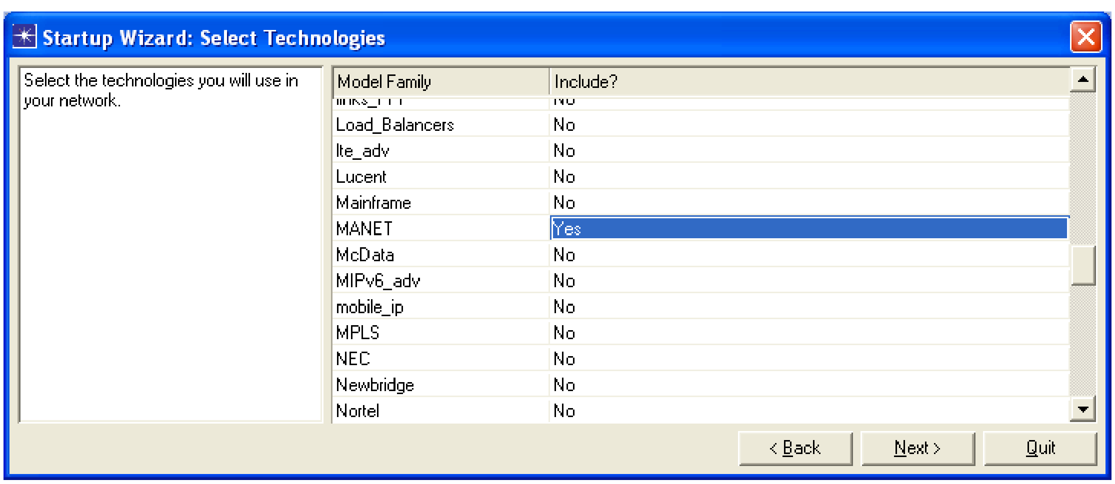

Figure 4.14: Select Technologies

Step 11: To start our simulation work click on Finish, as in Figure 5.15.

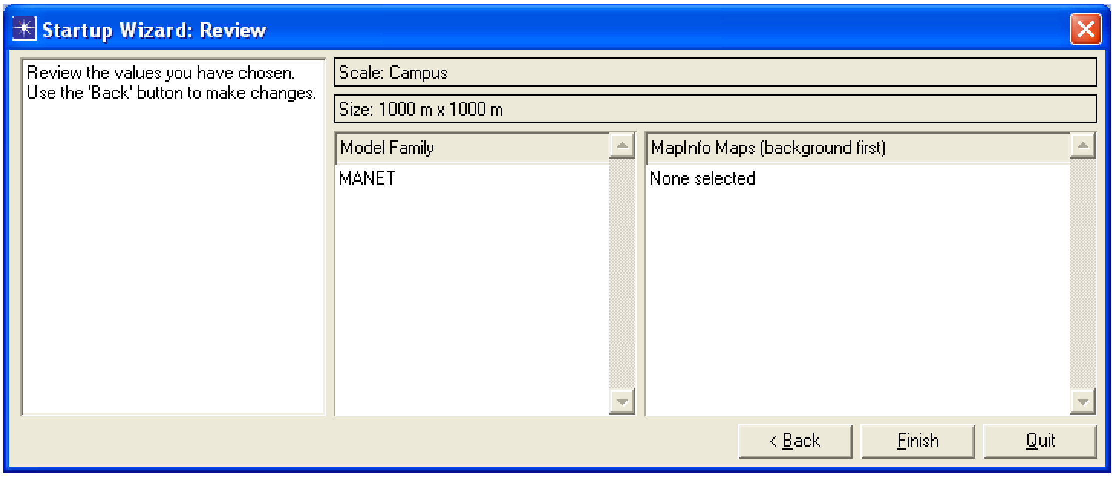

Figure 4.15: Review Window

after step 11 we select object palette tree to choose procedures used to build network topology, as in Figure 4.16.

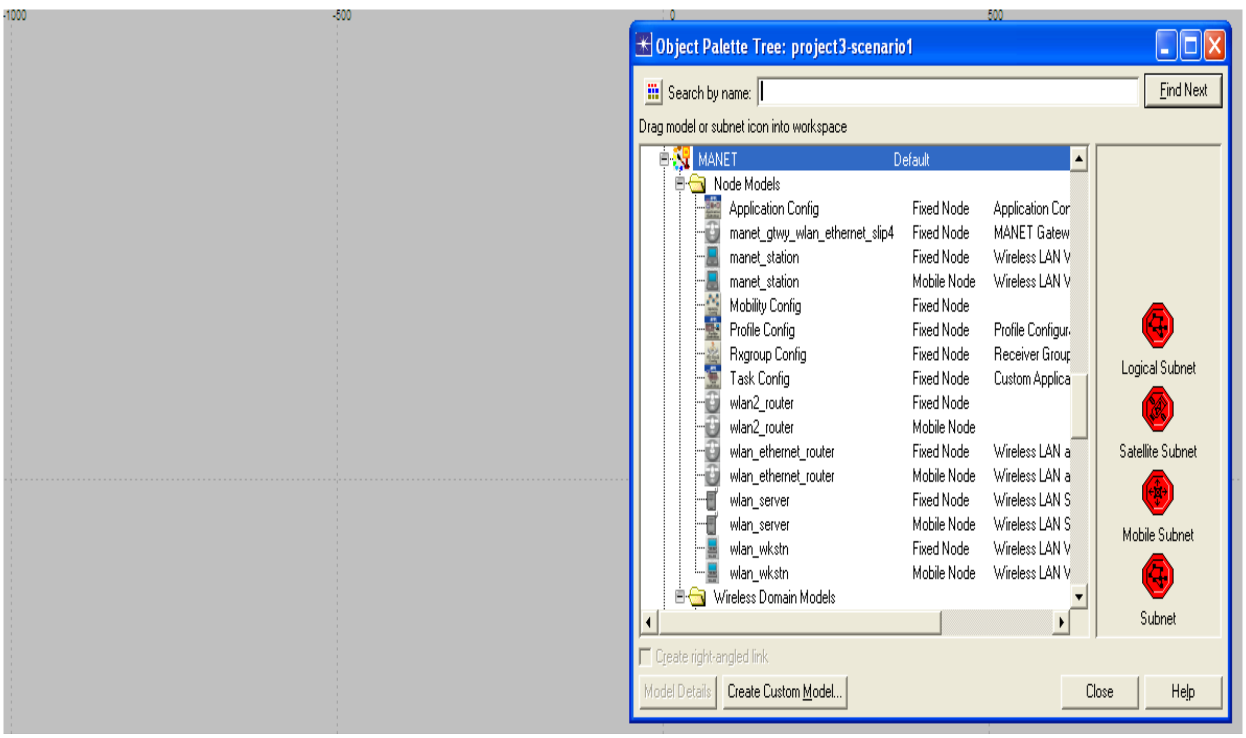

Figure 4.16: Object Palette Tree of MANET in OPNET

Step 12: In Figure 4.17 (object palette tree) choose application configuration node. After FTP is selected we have some procedure inside it like size that is equal to (CONSTANT= 256). Shown as a Figure 4.18 and 4.19.

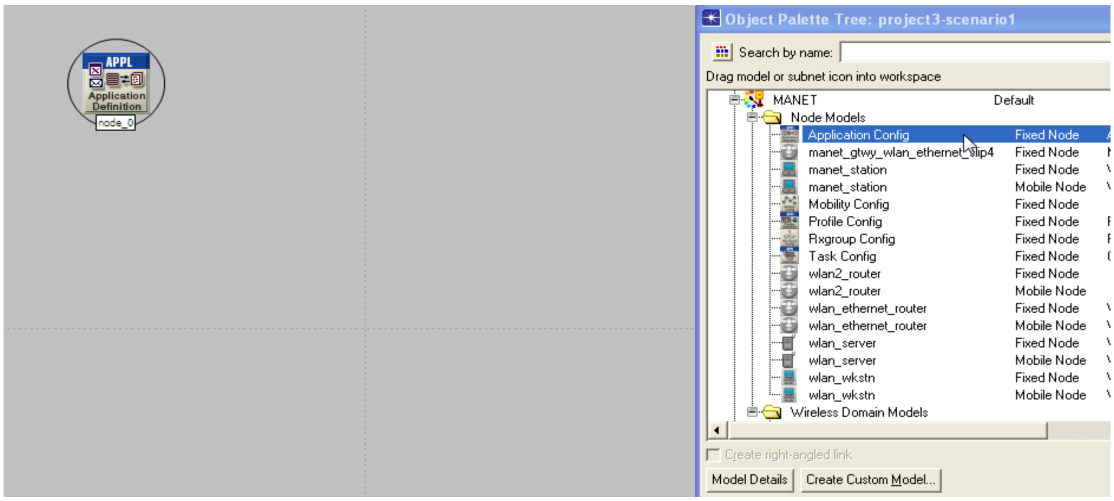

Figure 4.17: Object Palette Tree of MANET in OPNET

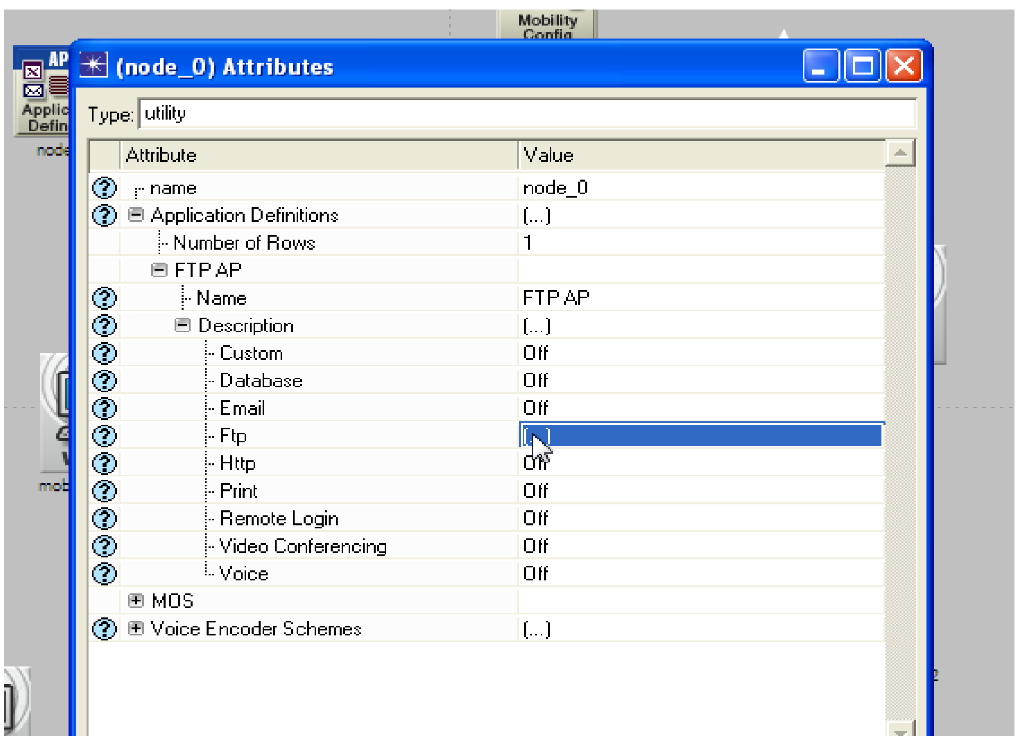

Figure 4.18: FTP Application Configuration Attributes

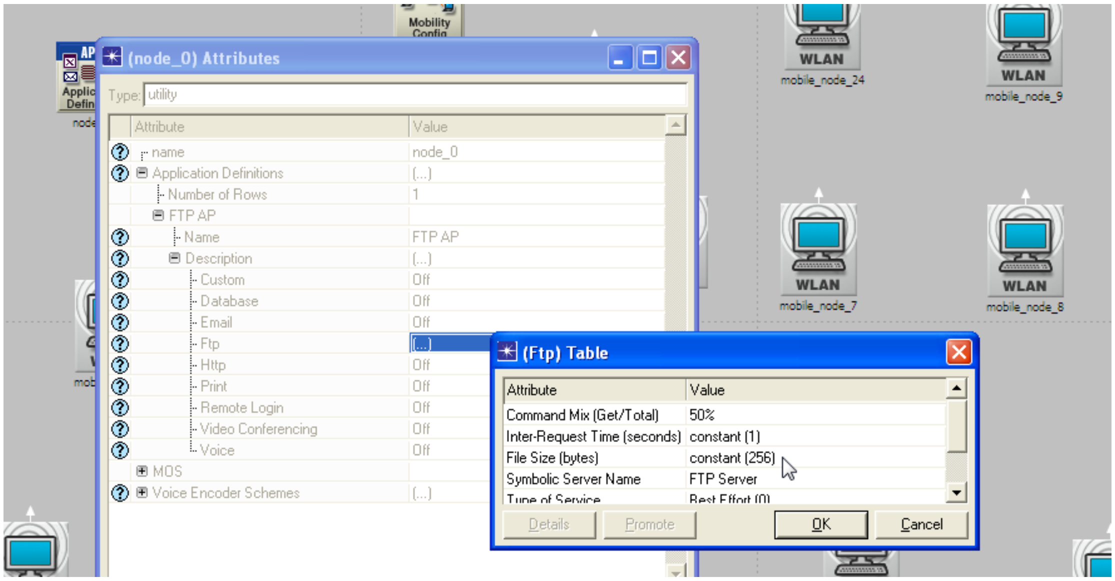

Figure 4.19: FTP Table

Step 13: In this step we choose profile configuration in object palette tree as in Figure 4.20.

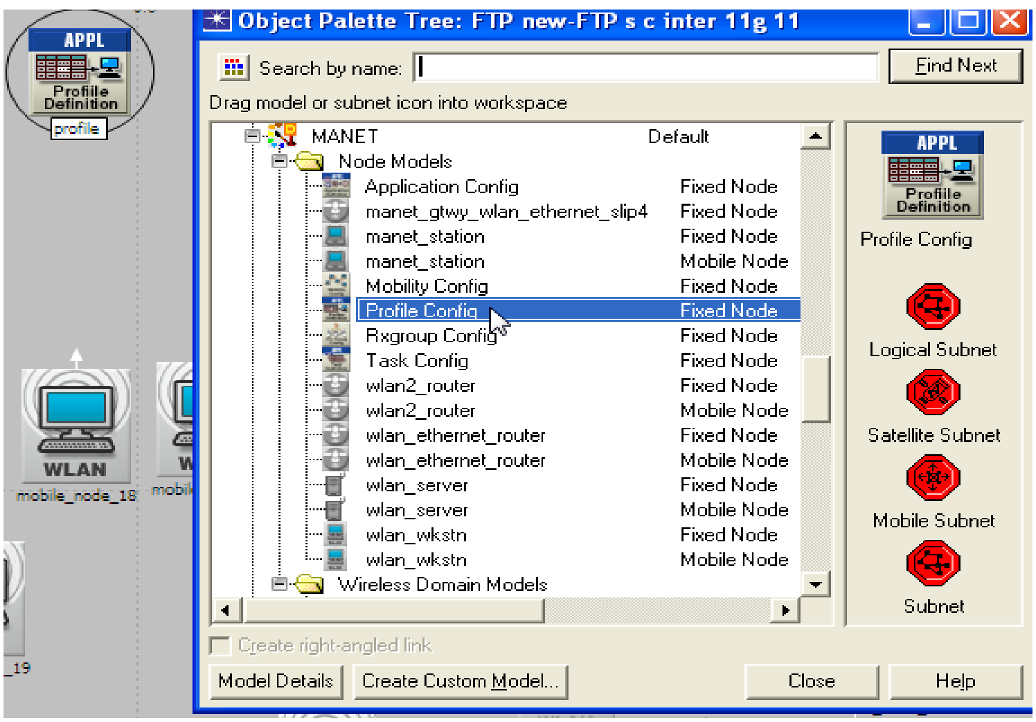

Figure 4.20: Object Palette Tree

After adding profile configuration for my scenario select right click on profile configuration (as in Figure 4.21) and we do our configuration by some steps:

Step 13.1: Write name of profile that is chosen (profile) as in Figure 4.22.

Step 13.2: Write name of application and profile configuration change to 1 (because we have one profile) as in Figures 4.23 and 4.24.

Step 13.3: Select application procedure to choose number of applications her we have only one application FTP, so I choose number 1 as in Figure 4.25.

For (step 3) must be do some configuration like (start time of application, duration of application, inter-repetition time of application, number of repetition, and repetition pattern, all inside the profile .

Some definitions of those parameters above are:

Start Time offset (second): It means the time of the start of the application inside the profile as in Figure 4.26.

Duration (second): It means the duration of time of the application when it finishes as in Figure 4.26.

Inter-repetition Time (second): It means when the first application inside of profile finishes until the next application starts (distance time between applications inside of profile) as in Figure 4.26.

Number of Repetition: It means how many repetition applications are done inside of profile) as in Figure 4.26.

Repetition pattern: How applications work like serial or parallel as Figure 4.26.

Step 13.4: Start time (seconds) time start of profile during simulation here we want to start my profile after 10 seconds of the simulation start as in Figure 4.26.

Step 13.5: Duration of profile here we choose end of simulation it means after start of profile inside of simulation profile it will be finished at the end of simulation Figure 4.26.

Step 13.6: Inter-repetition time (seconds) distance between repetitions of profile inside of simulation here we choose 0 because I have one profile and one execution of profile as in Figure 4.28.

Step 13.7: Repetition we choose 0 because we need one execution of profile during simulation as in Figure 4.28.

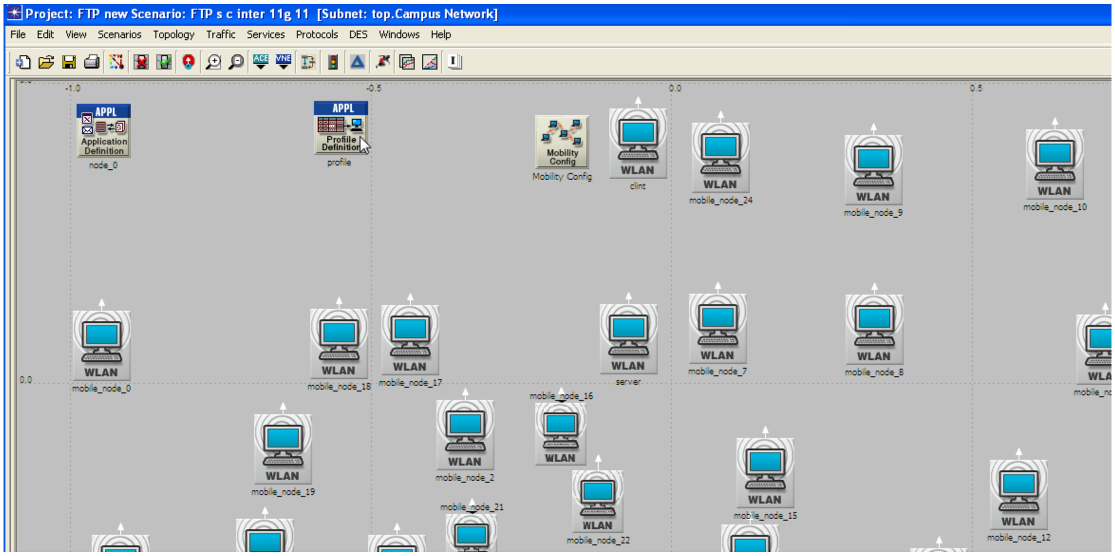

Figure 4.21: Simulation Structure with 25 nodes

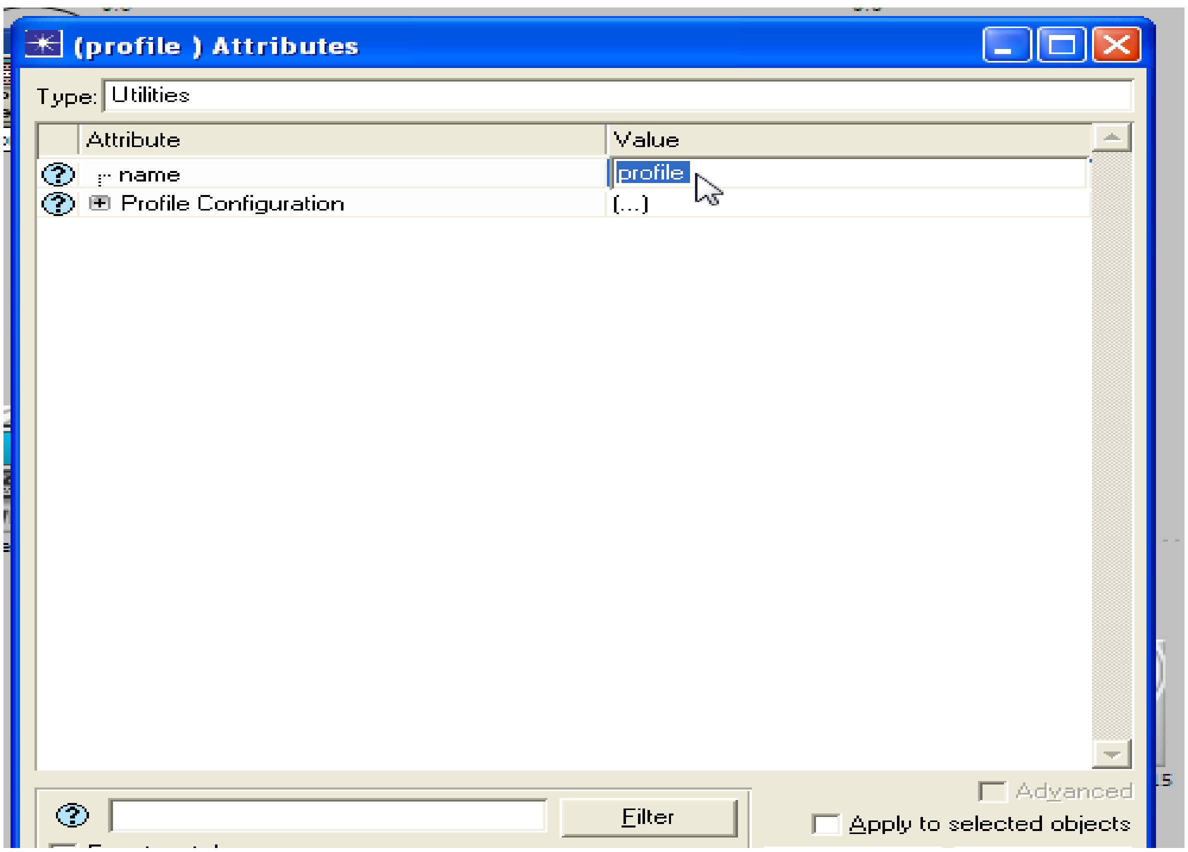

Figure 4.22: Profile Definition Attributes

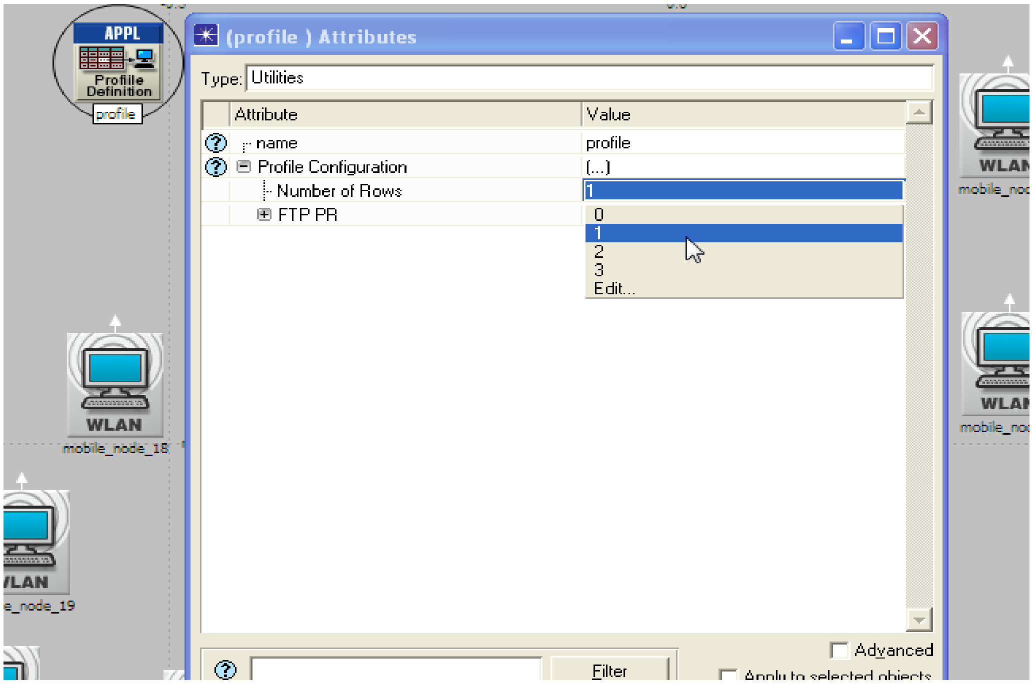

Figure 4.23: Profile Definition Attributes

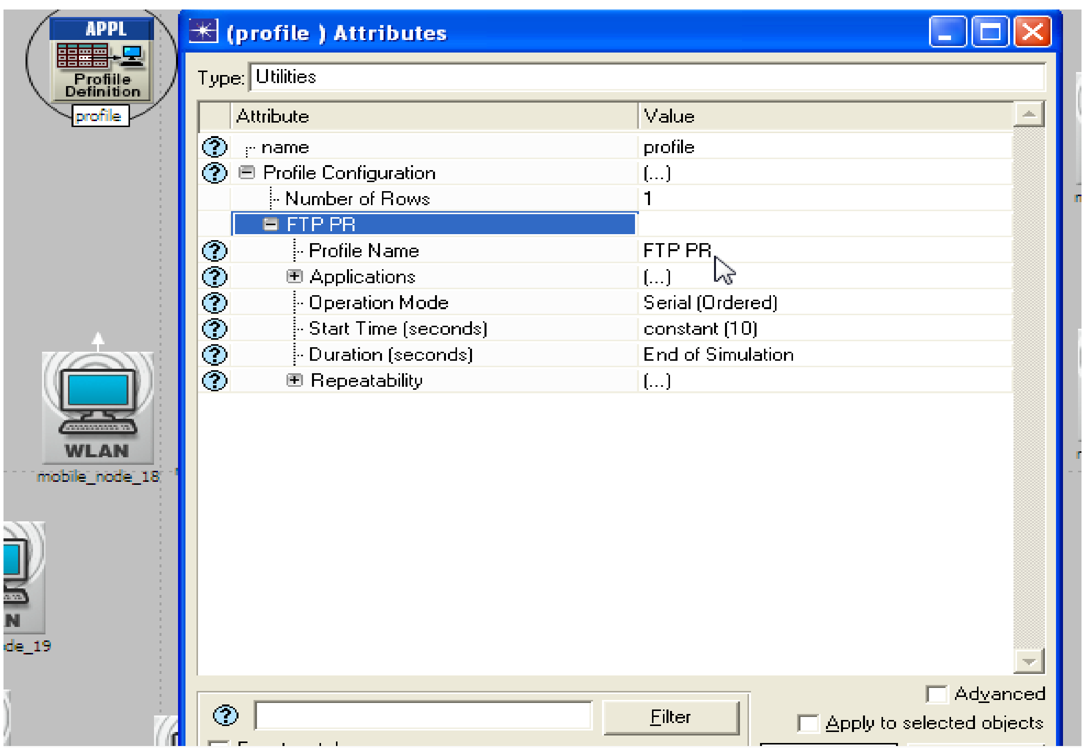

Figure 4.24: Profile Definition Attributes

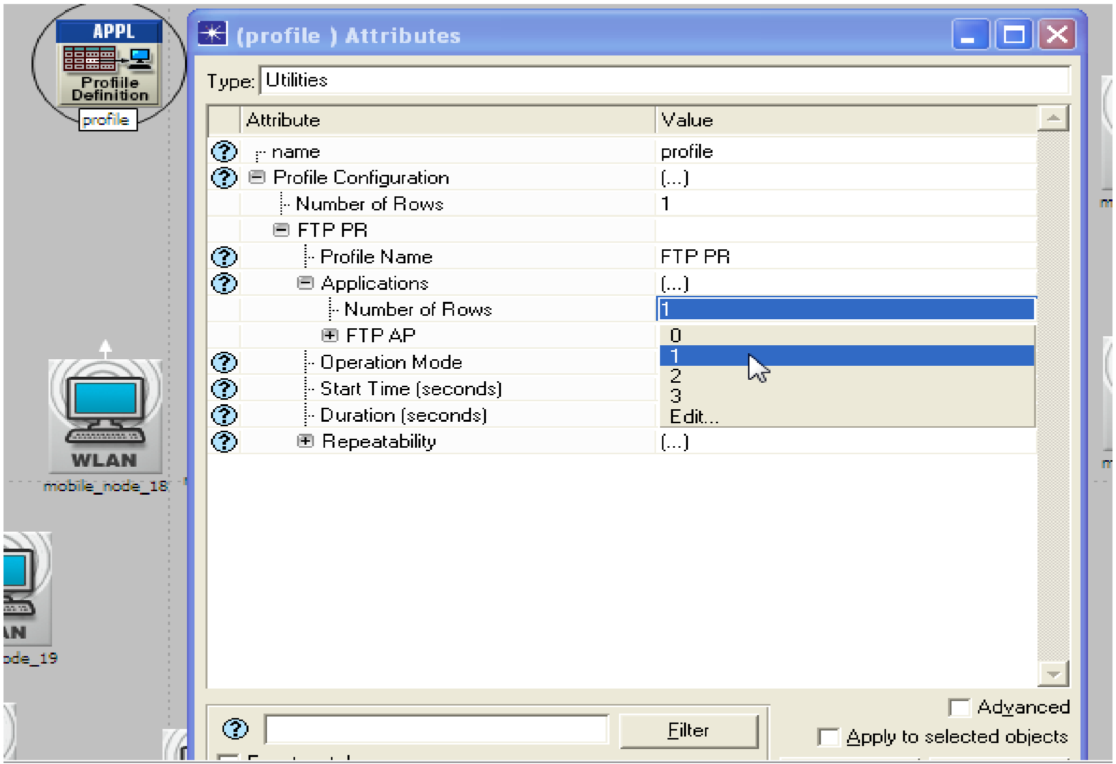

Figure 4.25: Profile Definition Attributes

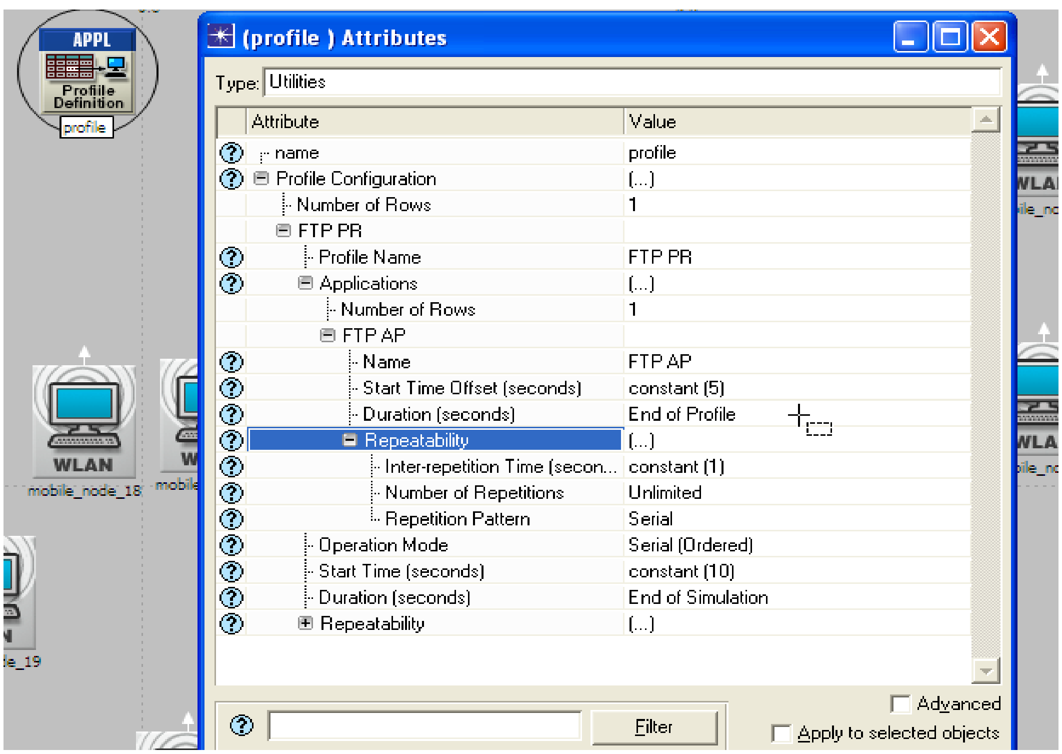

Figure 4.26: Profile Definition Attributes

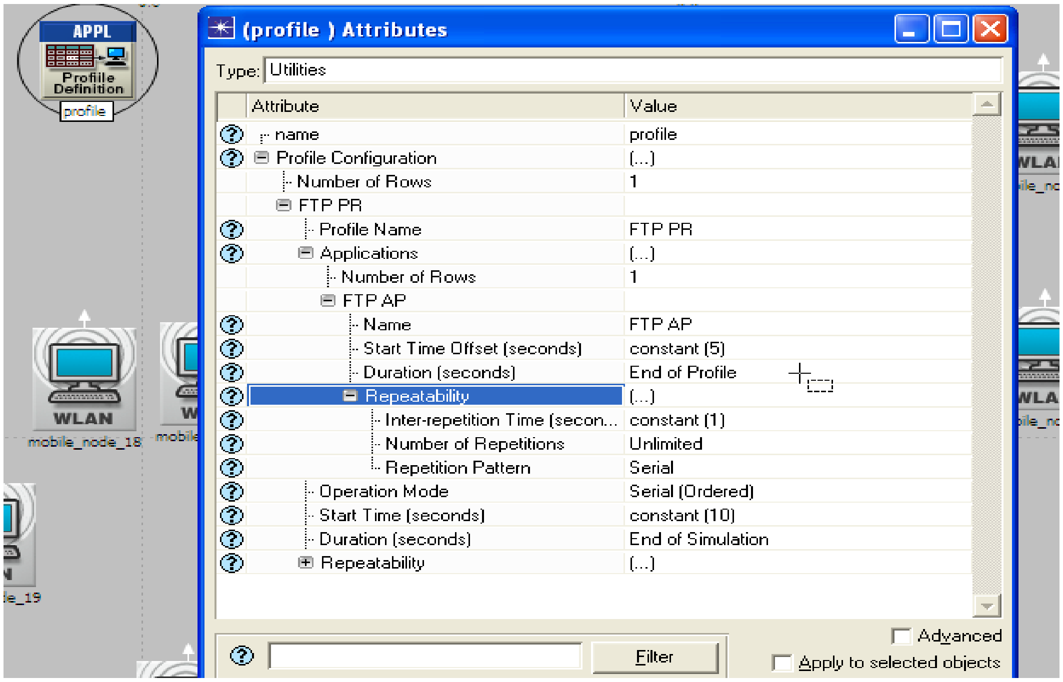

Figure 4.27: Profile Definition Attributes

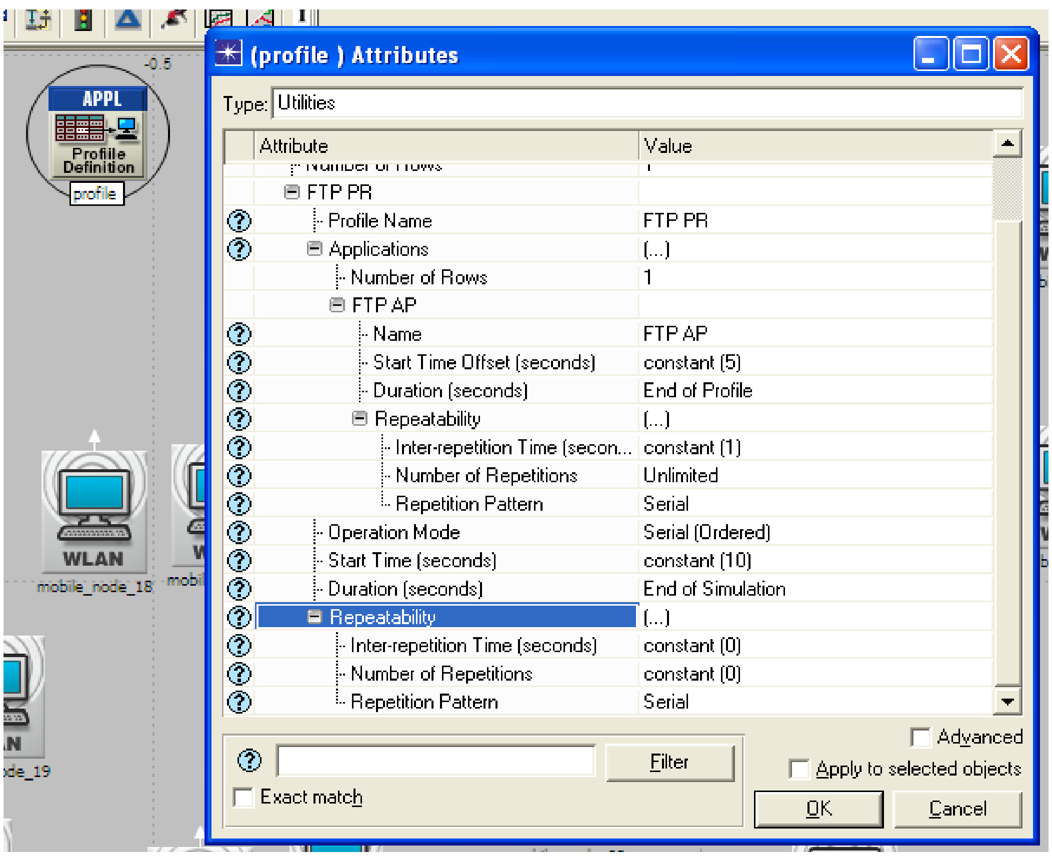

Figure 4.28: Profile Definition Attributes

Step 14: In this step nodes are added to the scenario. Select right click on one node and after that choose (select similar node) as in Figures 4.29 and 4.30.

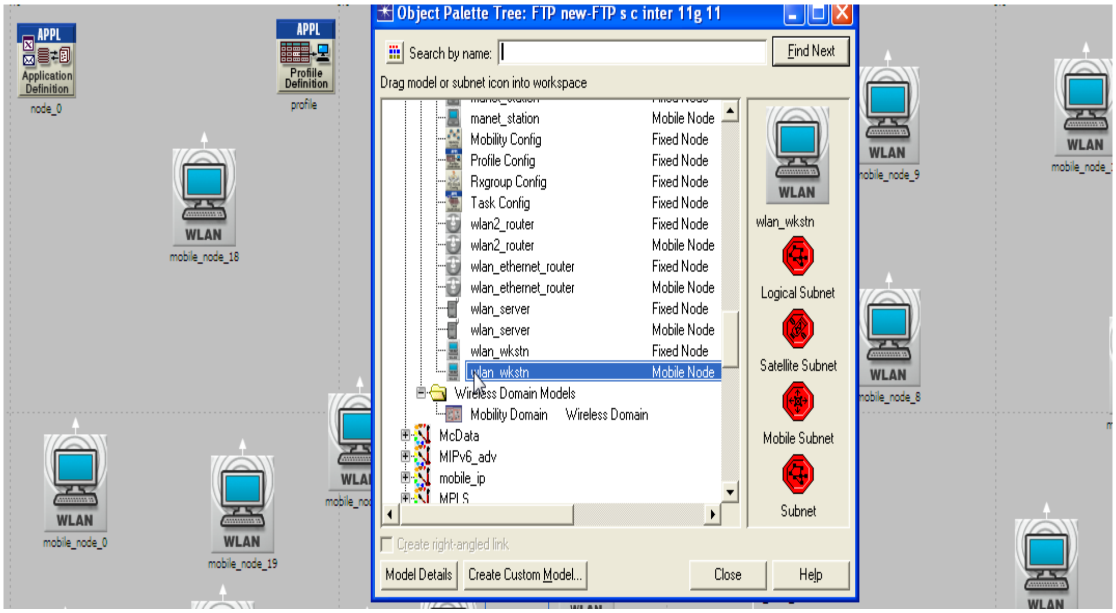

Figure 4.29: Object Palette Tree (WLAN WKSTN)

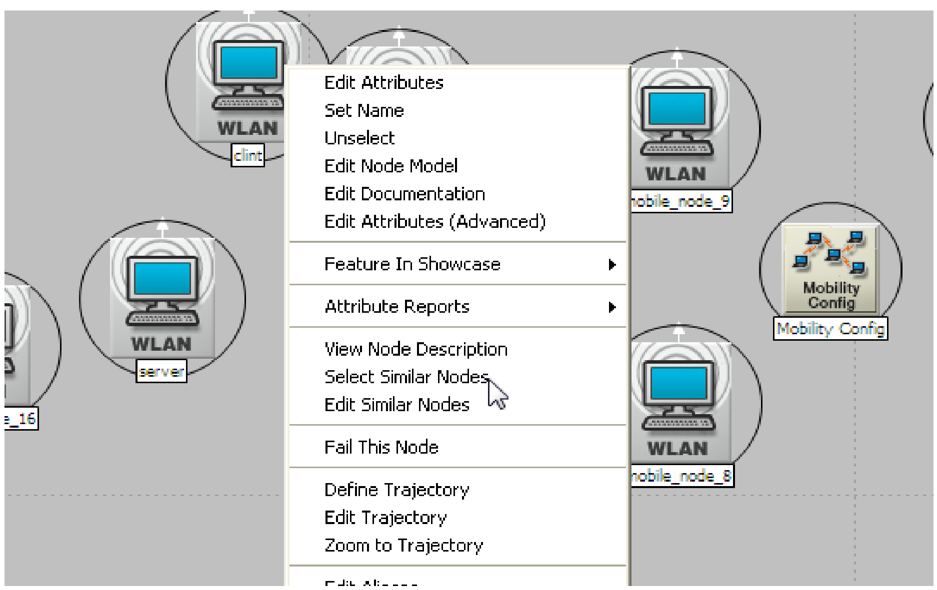

Figure 4.30: Node Attributes

After selecting same nodes do configuration of node by selecting edit attributes as in Figure 4.31.

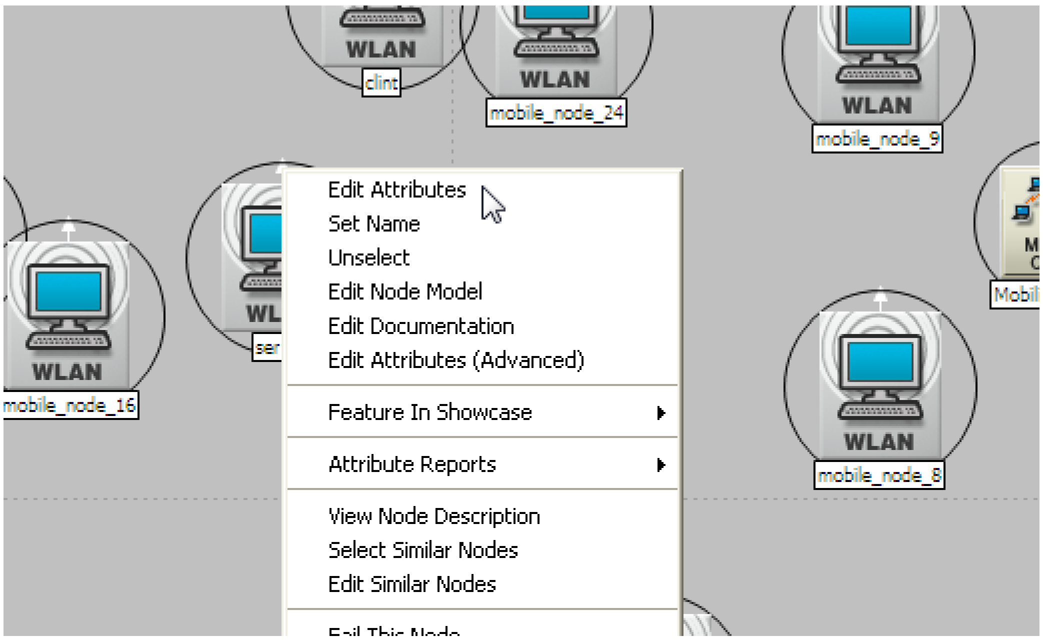

Figure 4.31: Node Attributes

Step 15: Here we choose the protocol used in our scenario, the physical characteristic used and which data rate show those configurations as in Figures 4.32 and 4.33.

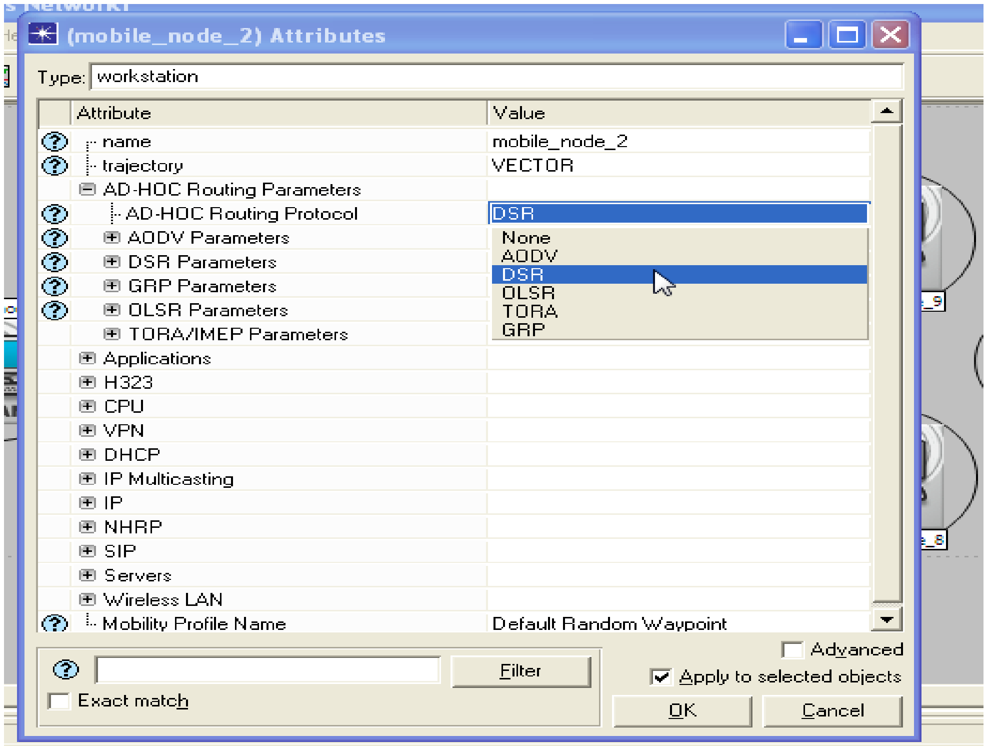

Figure 4.32: Mobile Node Attributes

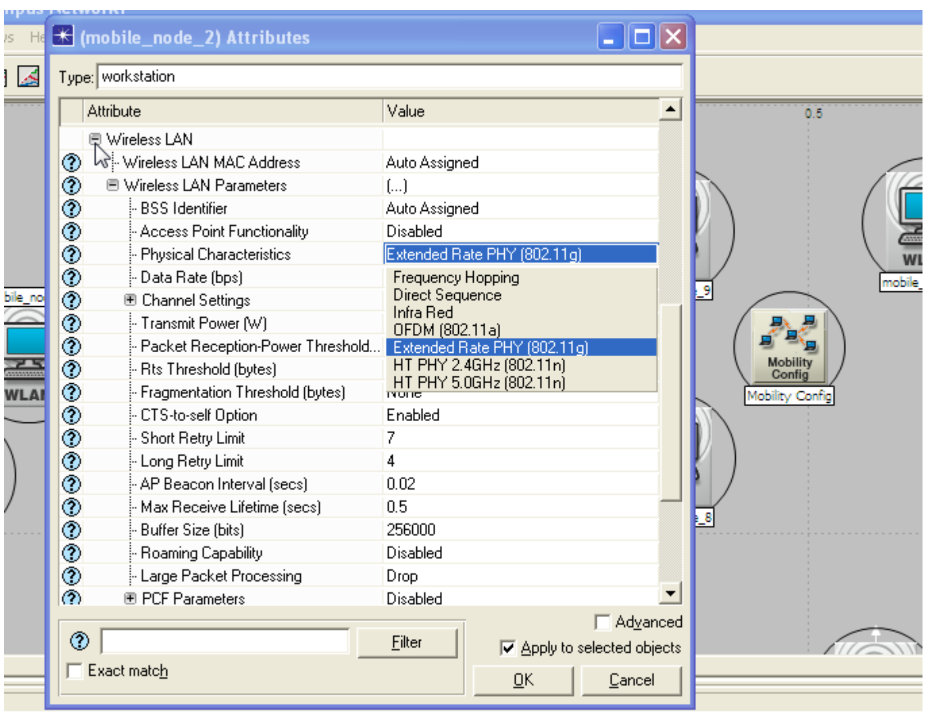

Figure 4.33: Mobile Node Attributes

Step 16: In this step we select physical characteristics and we need to select standard of wireless as in Figure 4.34.

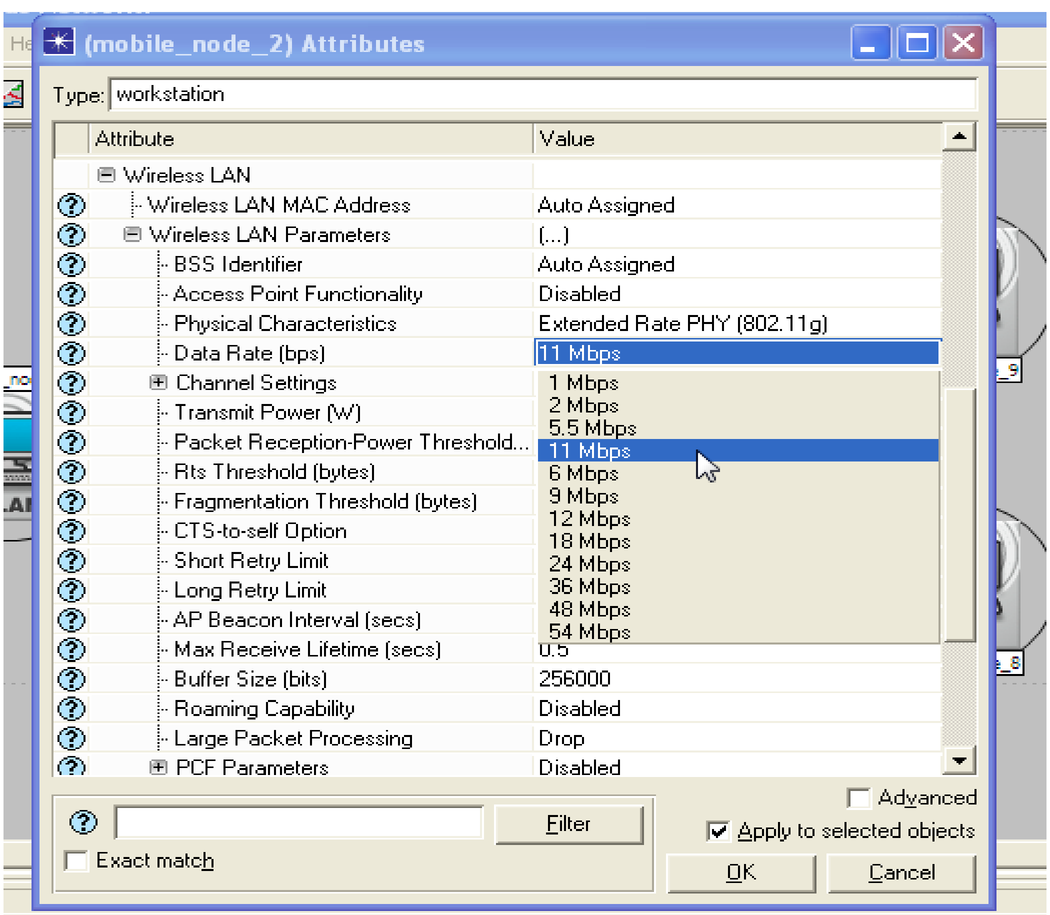

Figure 4.34: Mobile Node Attributes

Step 17: In this step select topology, shown as in Figure 4.35.

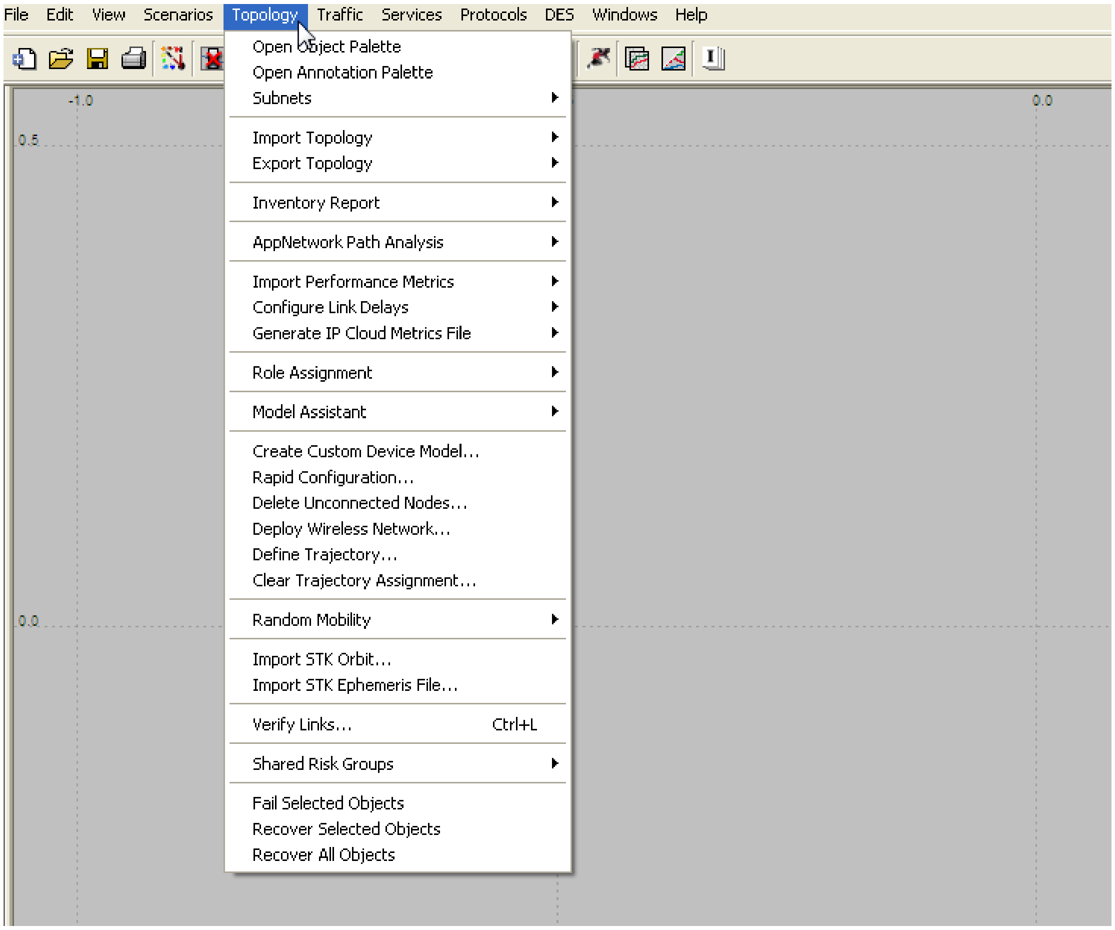

Figure 4.35: Network Topology

Step 18: Select (Random Mobility) to move nodes randomly shown as in Figure 4.36.

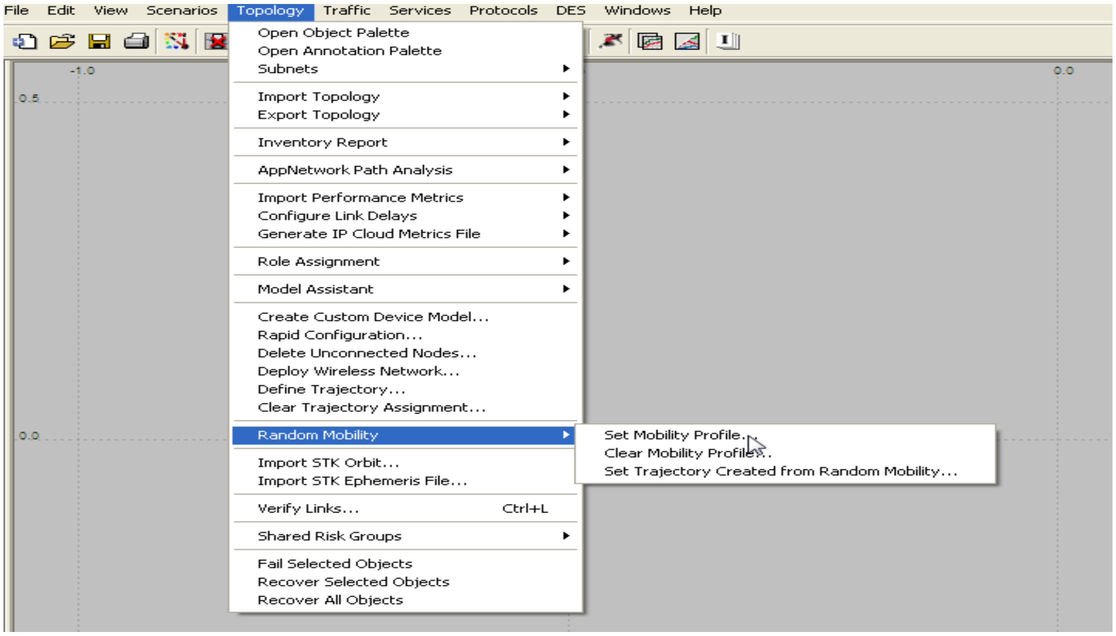

Figure 4.36: Random Mobility of Network Topology

Step 19: In this step we have to configure (Mobility Profile) for the mobility profile configuring parts such as:

- Mobility Model: In this parameter (Random Waypoint) is chosen: this parameter is used for moving nodes in area randomly.
- X-max (meter) and Y-Max (meter): here using the same area as we chose before in (step 9).
- Speed (meters/second): Here we choose the case of semi-real, a parameter used for moving each node by seconds. we selected between (1m and 1.5m).

All entire configurations are shown in the Figure 4.37.

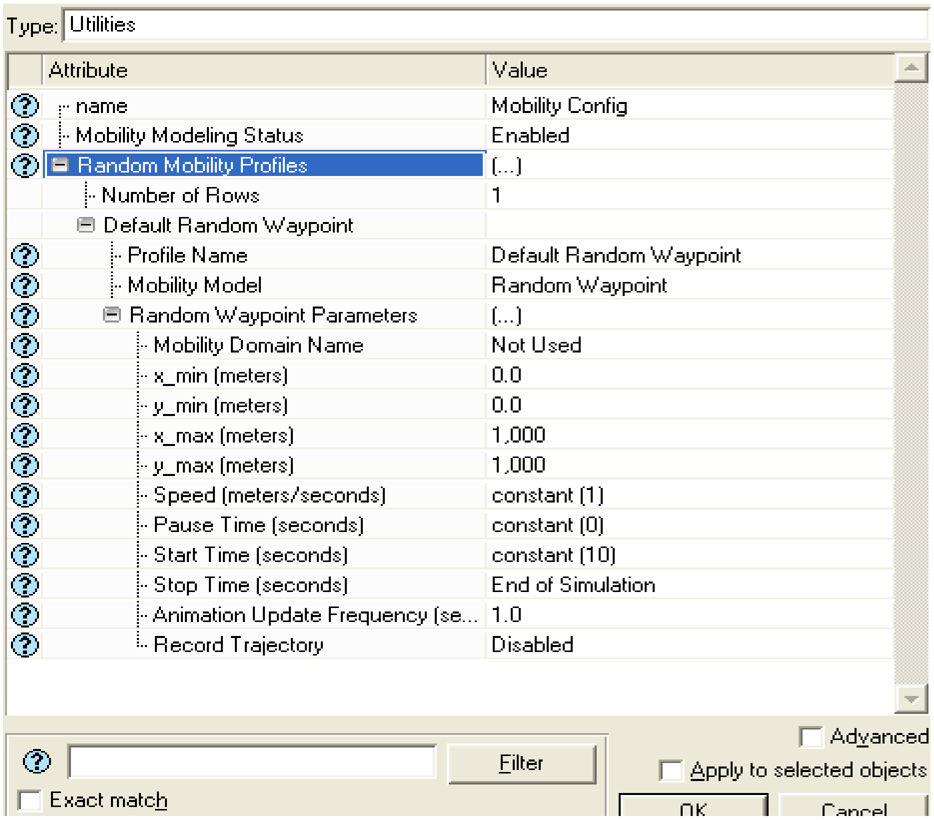

Figure 4.37: Mobility Attributes

Step 20: In this step select (Protocol) and select (IP) to give all nodes IP but in the beginning we have to select (similar node) procedure by right click on any node.

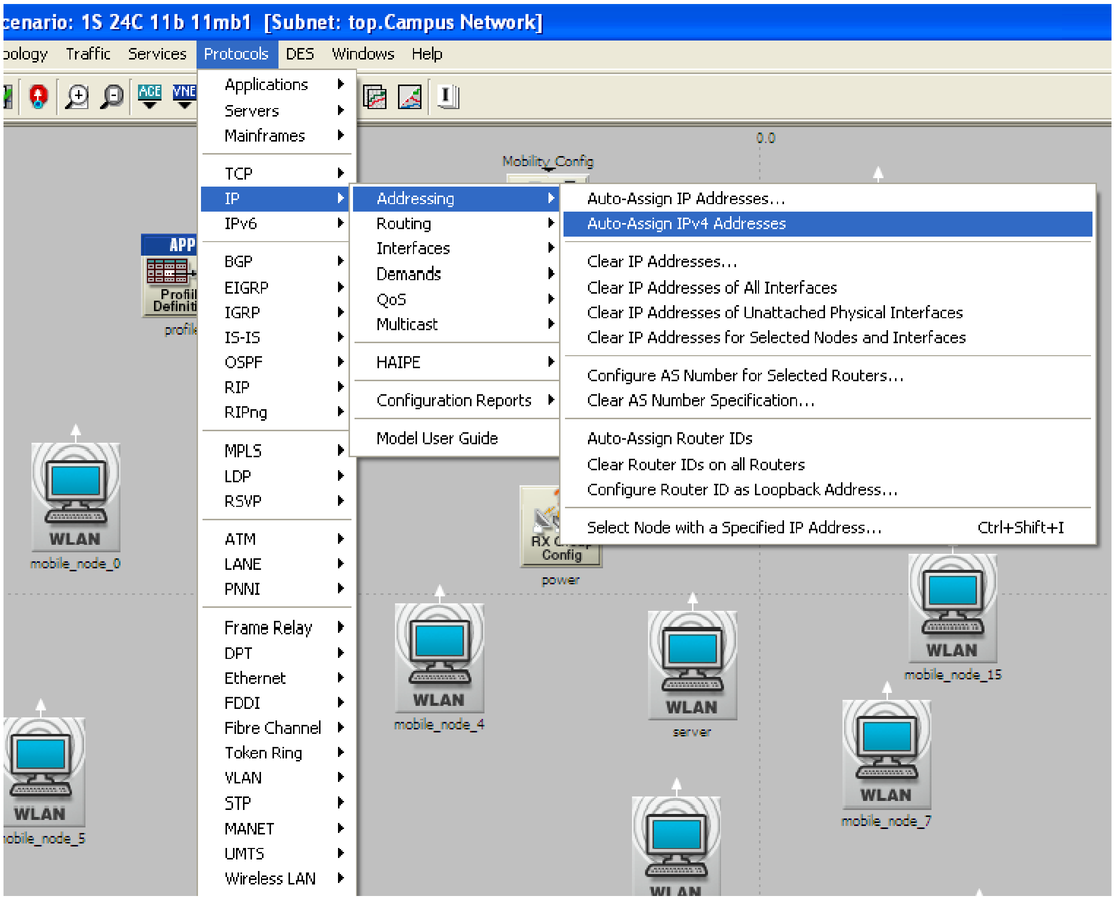

Figure 4.38: Protocol IPv4 Addresses

Step21: To choose the number of servers and the number of client select, as shown in Figures 4.39 and 4.40.

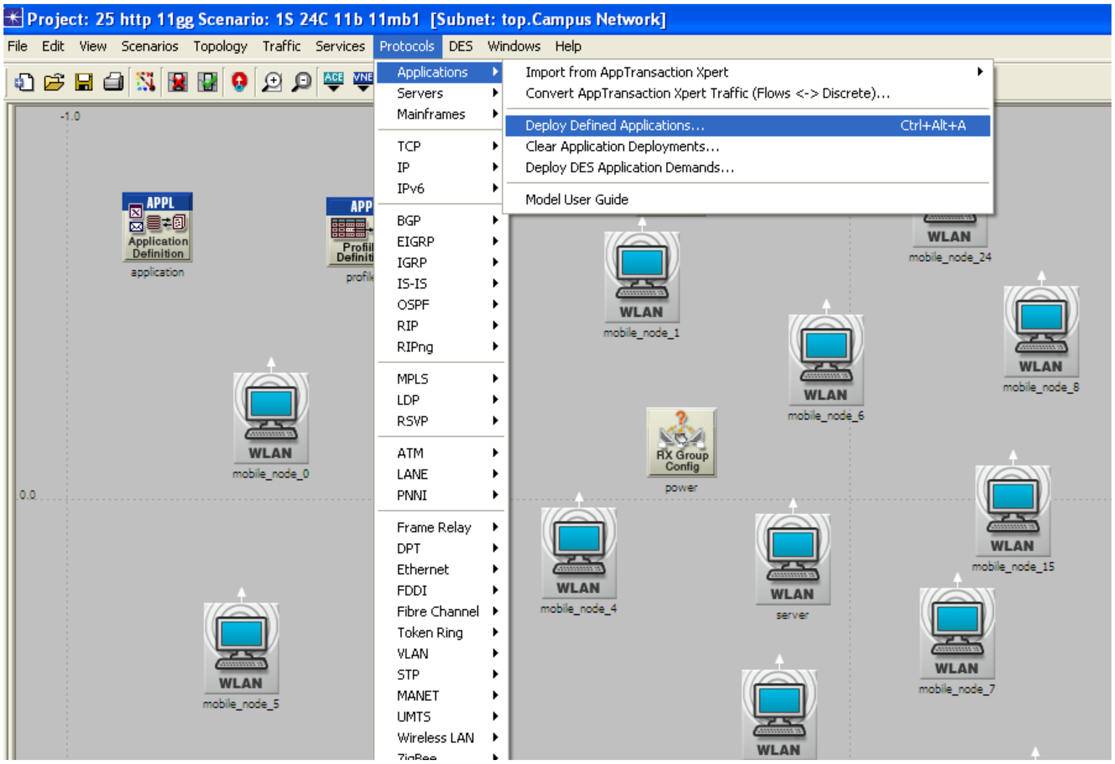

Figure 4.39: Protocol Deploy Defined Application

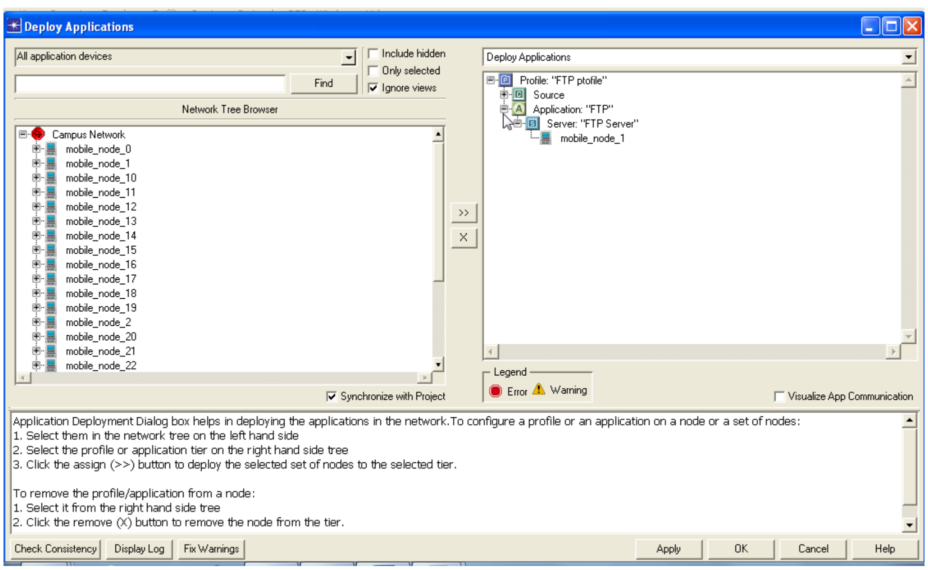

Figure 4.40: Deploy Application

Step22: In this step we used RX GROUP, shown as in Figure 4.41

Distance threshold (meter): This option will limit the receivers outside of the specified distance threshold value from the receiver group."Line of Sight" option when selected will use simple Earth LOS computation used in dra_closure pipeline stage model (Transmission rage power).

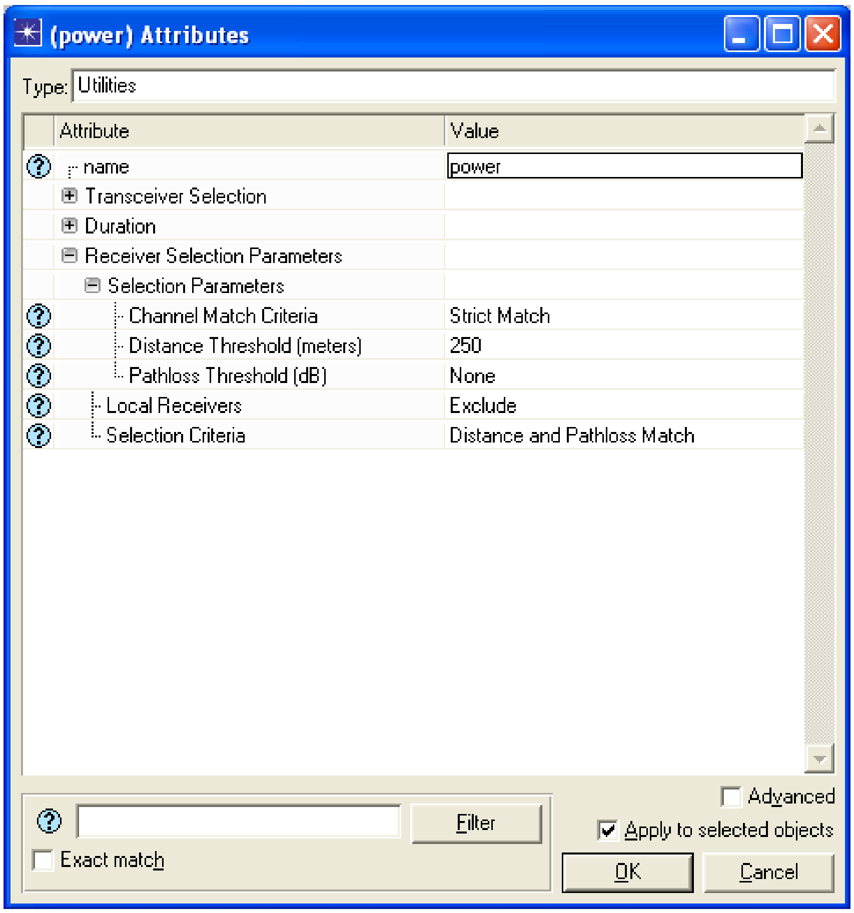

Figure 4.41: RX Group

Step 23: After finishing all steps above, parameters should be selected the to show results. The steps for selecting are shown as in Figures 4.43 and 4.44.

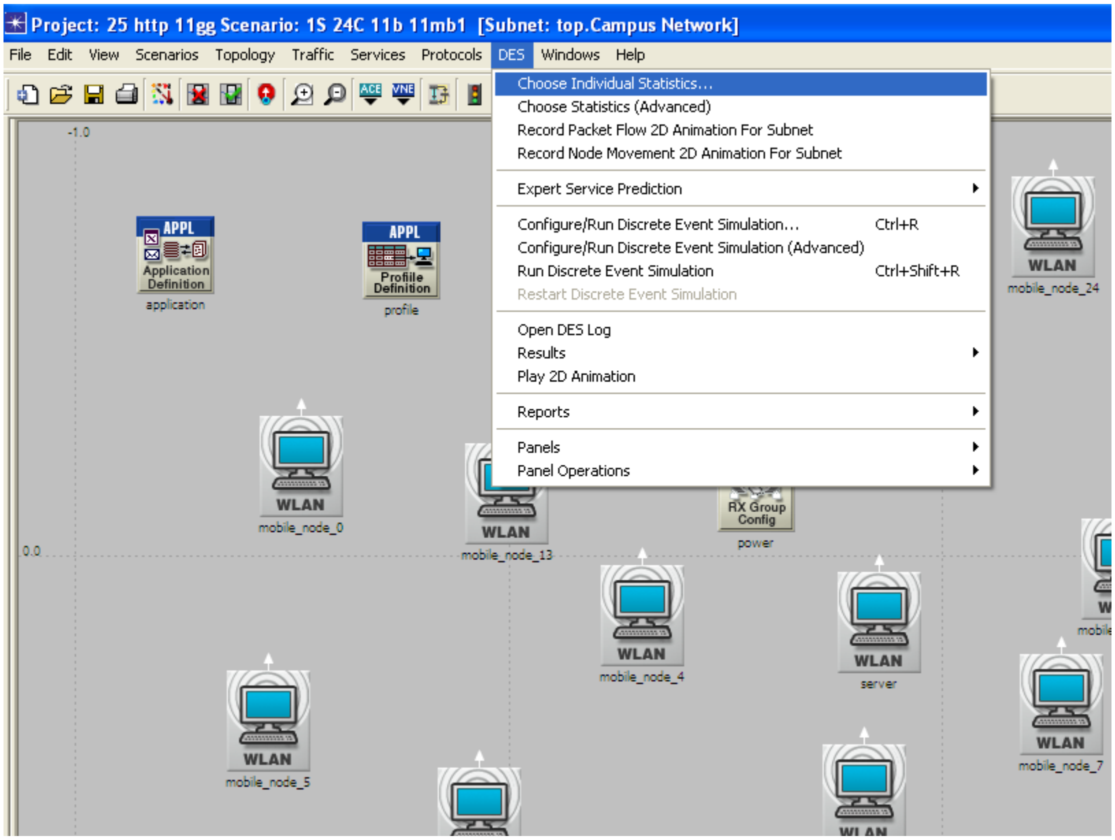

Figure 4.42: View Results DES

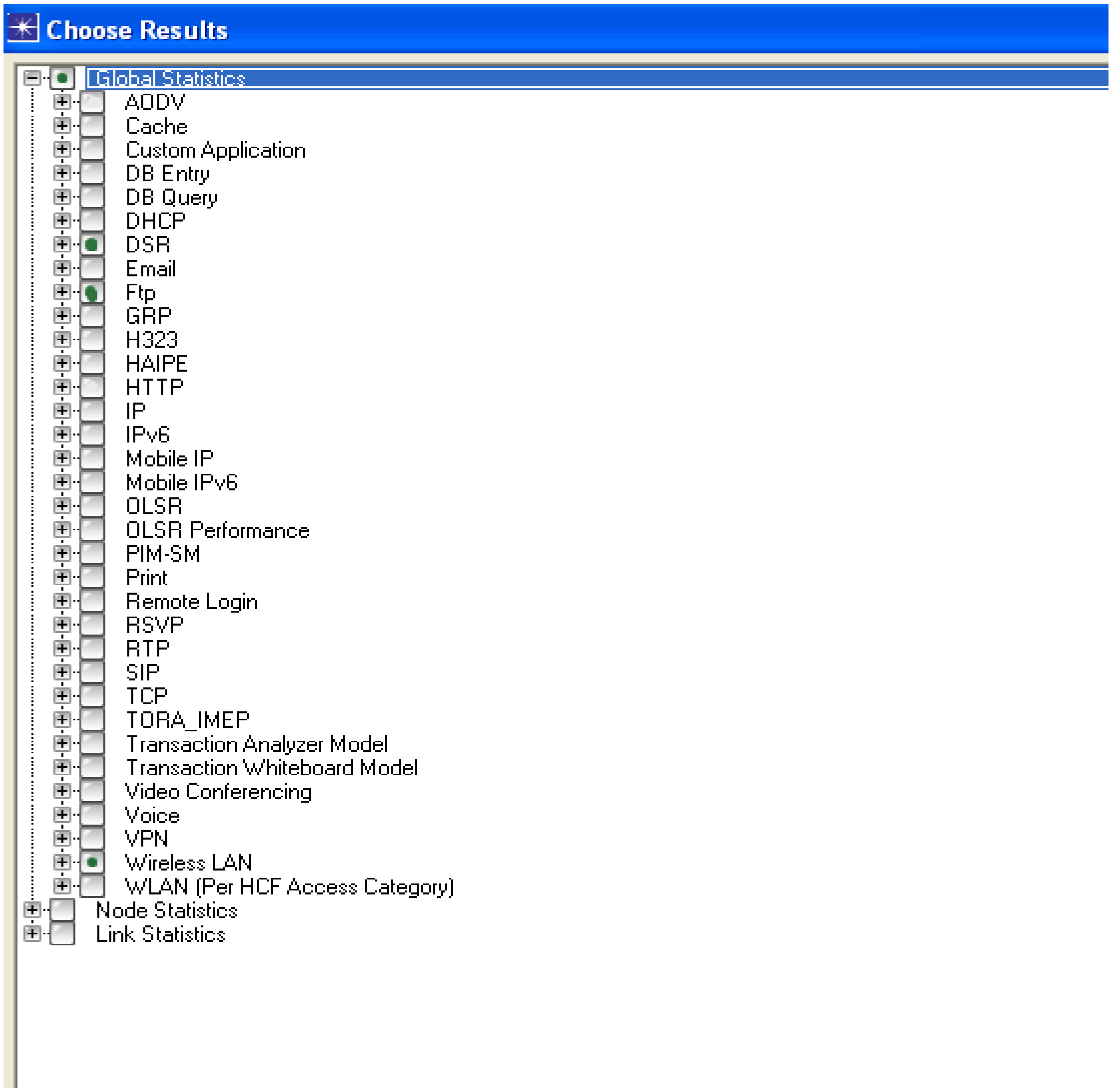

Figure 4.43: Choose Results window

Step 24: In this step select the run that is used to start simulation and duration time for every run and number for runs in same simulation all this setting shown in Figure 4.44.

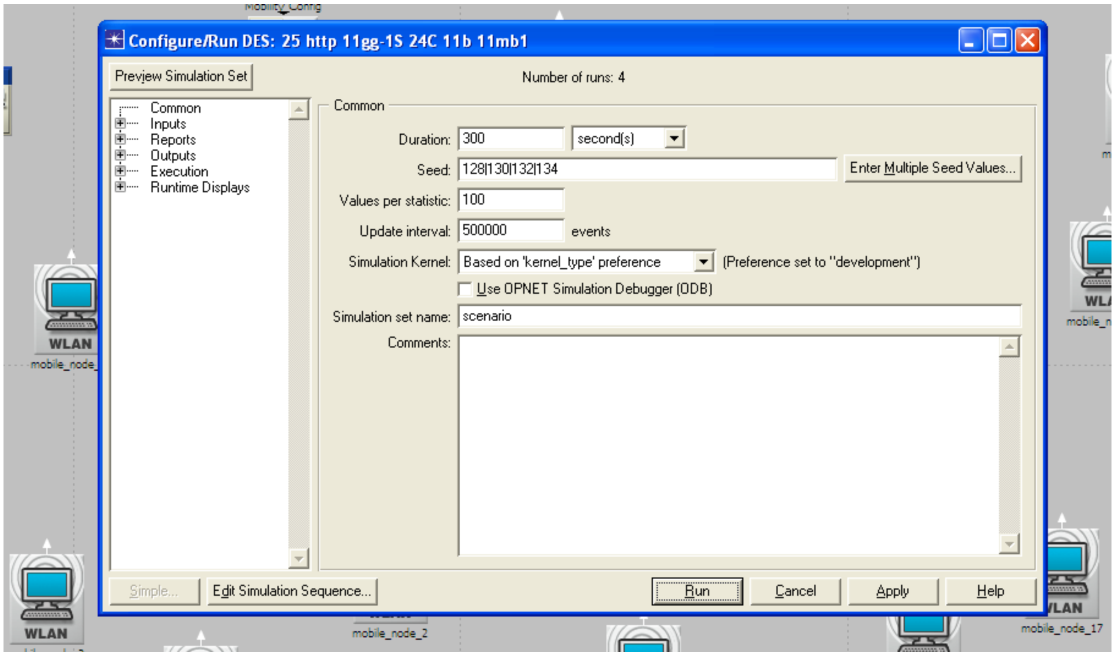

Figure 4.44: Configuration Run DES

4.7 Run Simulations

After applying the statistics to mobile nodes and other modules, simulation is run for 300 seconds for each scenario. There are 12 scenarios for FTP application. Each scenario is repeated 4 times.

Chapter 5

SIMULATION RESULTS AND DISCUSSION

5.1 Performance Metrics

Number of hopes: In computer networking, a hop represents one portion of the path between source and destination. When communicating over the Internet, for example, data passes through a number of intermediate devices (like routers) rather than flowing directly over a single wire. Each such device causes data to "hop" between one point-to-point network connection and another.

Route Discover (RD) time: Representing ad-hoc routing protocols that are source-initiated on-demand-based and initiating a route discovery (RD) whenever a route desired by the source is not immediately available in the route cache. The RD process is invoked by the source node sending a BQ control packet that is broadcast in search of valid route(s) to the destination. After some delay, if the network is not partitioned, the BQ control packet will ultimately reach the destination node. The destination node uncovers the route path information contained inside the BQ control packet. A REPLY control packet is then sent back via the reverse path, so that ultimately the source is informed about the discovered route.

Routing Traffic ratio: This matric calculate the number of routing traffic received packets over routing traffic send by all nodes in the network.

Media access delay: Is the time a node takes to access media (link) to start its transmission. Media access delay includes queuing delays and the delays due to contentions and back offs.

Retransmission Attempts: Representing the number of times data has to be retransmitted by the Source node.

Throughput: Will test the amount of data that reaches the receiver from the source to the time taken by the receiver to receive the last packet.

$$Throughput = \frac{received\_bytes}{Time\_of\_simulation}$$

FTP Traffic: Describes the concept of the FTP traffic of the whole network (Global Statistics). The statistics for the FTP traffic of the network include the FTP download response time (sec), the FTP upload response time (sec), the FTP traffic sent(bytes/sec) and the FTP traffic received (bytes/sec).

First of all, the FTP download response time (sec) describes the time elapsed between sending a request and receiving the response packet. Measured from the time a client application sends a request to the server to the time it receives a response packet.

Every response packet sent from a server to an FTP application is included in this statistic. In addition, the FTP uploads response time (sec) represents the time elapsed between sending a file and receiving the response. The response time for responses sent from any server to an FTP application is included in this statistic.

Note:

1/1: It means that one server and one client.

1/12: It means that one server and twelve clients.

1/24: It means that one server and twenty four clients.

5.2 Results and Discussions

Category 1:

In the first category, I used wireless standard 802.11g with different data rate (11Mbps, 24Mbps, and 54Mbps). In this category also we have one server with different number of clients (1 Server / 1Client with 23 Intermediate nodes, 1 Server / 12 Clients with 12 Intermediate nodes, 1 Server / 24Clients). We used DSR protocol to evaluate the performance metrics over FTP application in the area 1000m * 1000m and the network size being 25 nodes. In addition to we used OPNET modeler 17.1 to simulate our work.

Table 5.1: Simulation Results of Average Number of Hops for Wireless Standard 802.11g with Different Data Rates for DSR Protocol.

802.11g data rate Mb/s	Number of Hops per route		
	1\1	1\12	1\24
11	1.697	2.202	2.581
24	1.806	2.313	2.939
54	2.373	2.672	3.512

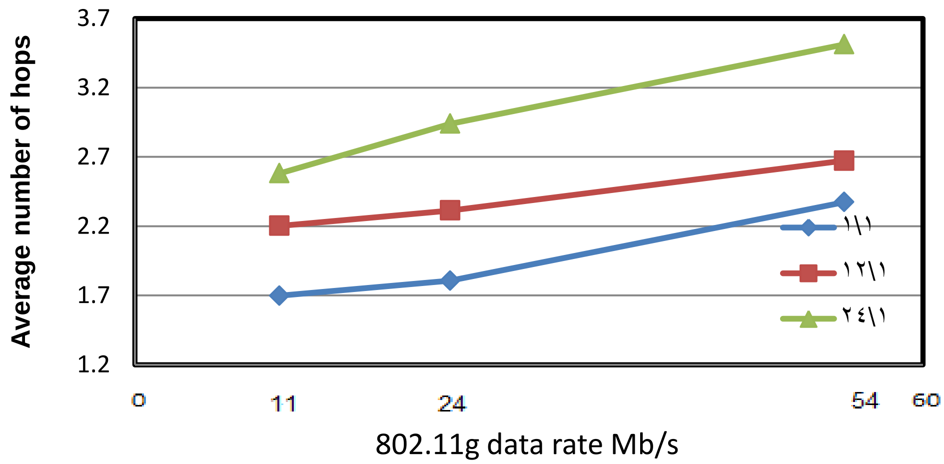

Figure 5.1: Average Number of Hops Versus Wireless Standard 802.11g With Different Data Rates for DSR Protocol with 25 Nodes.

In Figure 5.1 above it can observe that the number of hops of 1/24 clients with the data rate 11Mbps is the highest number of hops in that the server sent 24 requests "RREQ" to 24 clients. Some of the clients can receive packets from server directly without any intermediate nodes. The main factor that affects the number of hops is the distance between the nodes and the transmitting power of wireless nodes in MANET.

Table 5.2: Simulation Results of Route Discovery Time for Wireless Standard 802.11g with Different Data Rates for DSR Protocol.

802.11g data rate Mb/s	Route Discovery Time		
	1\1	1\12	1\24
11	0.008	0.050	0.076
24	0.006	0.044	0.070
54	0.010	0.054	0.096

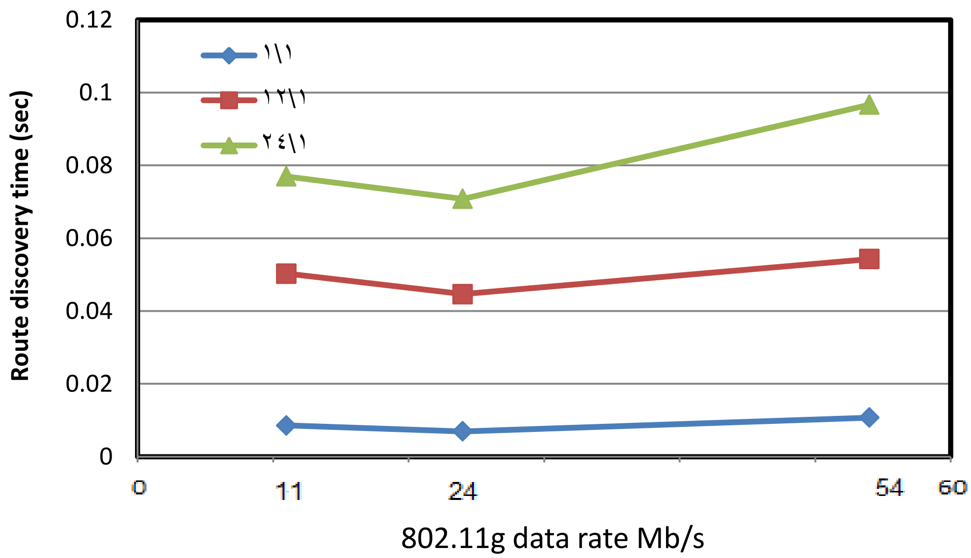

Figure 5.2: Route Discovery Time Versus Wireless Standard 802.11g with Different Data Rates for DSR Protocol with 25 Nodes.

In the Figure above it is seen that the route discovery time for one server with 24 clients has the highest level in the different data rates. Therefore, when we have the large number of requests form the clients need a very long time to know the path between source and destination. So when we have one server with one client we have only one request form client, so RD time needs to find one shortest path between source and destination since in this case does not need more time.

Table 5.3: Simulation Results of Routing Traffic Ratio for Wireless Standard 802.11g with Different Data Rates for DSR Protocol.

802.11g data rate Mb/s	Routing Traffic Ratio		
	1\1	1\12	1\24
11	0.415	0.392	0.368
24	0.415	0.626	0.708
54	0.340	0.880	0.893

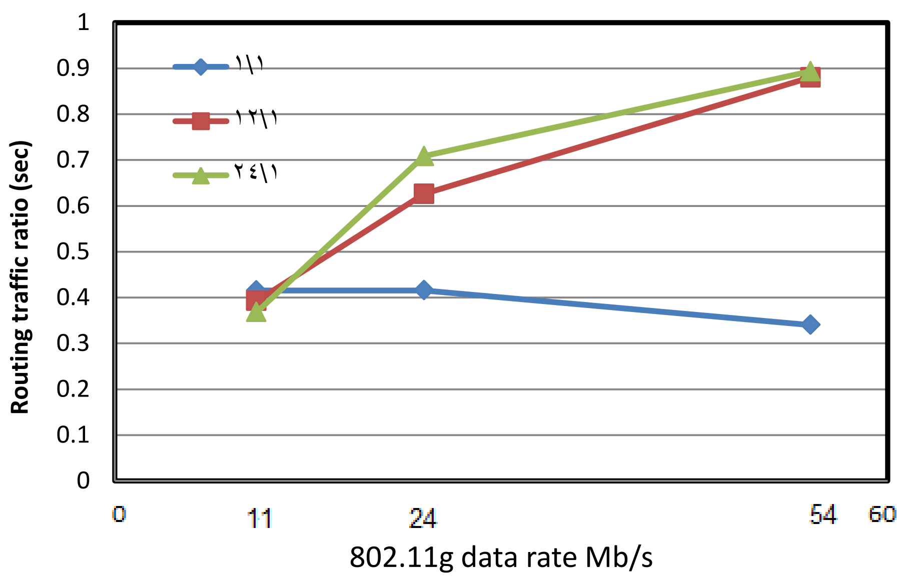

Figure 5.3: Routing Traffic Ratio Versus Wireless Standard 802.11g with Different Data Rates for DSR Protocol with 25 Nodes.

In the Figure above we can observe the routing traffic ratio of wireless standard 802.11g compared with different data rates. When the network is 1/12 and 1/24 we have highest routing traffic ratio as compared to 1/1 that has the lowest routing traffic ratio. This is because when number of clients in network that are communicating with server increased the amount of routing traffic wills increase in the network.

Table 5.4: Simulation Results of Media Access Delay for Wireless Standard 802.11g with Different Data Rates for DSR Protocol.

802.11g data rate Mb/s	Media Access Delay		
	1\1	1\12	1\24
11	0.0006	0.009	0.021
24	0.0004	0.006	0.012
54	0.0004	0.005	0.011

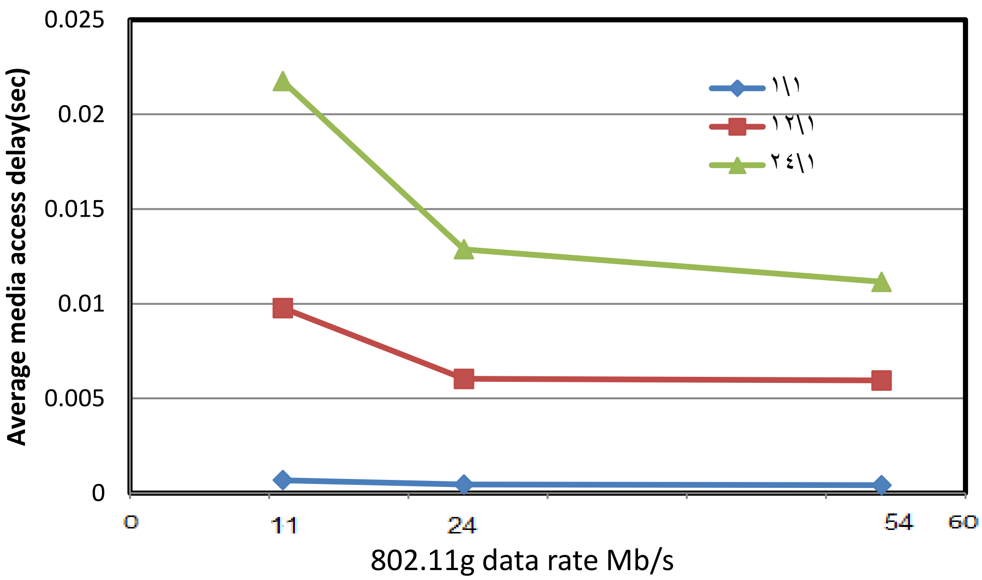

Figure 5.4: Average Media Access Delay Versus Wireless Standard 802.11g with Different Data Rates for DSR Protocol with 25 Nodes.

For Figure 5.4 it can be observed that the media access delay for all three cases will decrease and 1/24 that has the highest value compared to other cases. It means that the nodes need too much time to transmit packets from one node to another. So whenever the number of hops increases, media access delay increases. Additionally when data rate increases, the media access delay decreases.

Table 5.5: Simulation Results of Average Retransmission Attempts for Wireless Standard 802.11g with Different Data rates for DSR Protocol.

802.11g data rate Mb/s	Average Retransmission Attempts		
	1\1	1\12	1\24
11	0.172	0.297	0.365
24	0.156	0.263	0.330
54	0.145	0.252	0.317

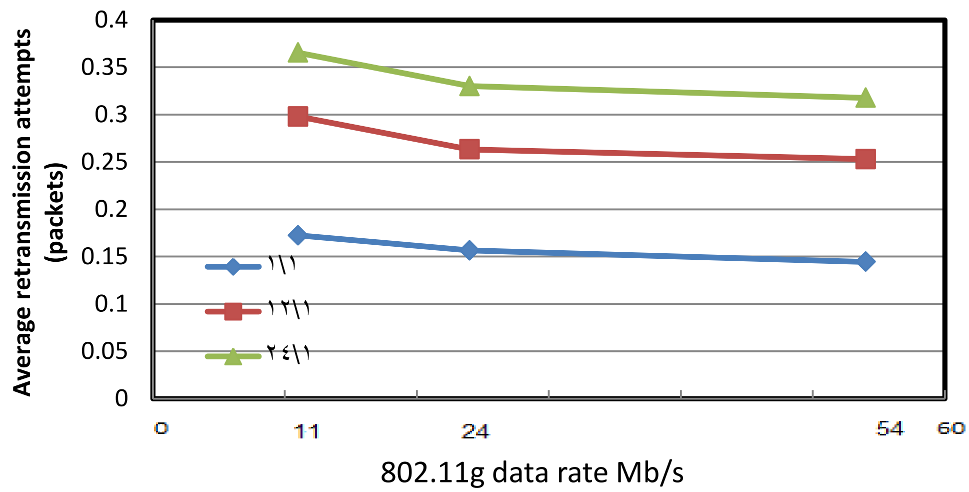

Figure 5.5: Average Retransmission Attempts Versus Wireless Standard 802.11g with Different Data Rates for DSR Protocol with 25 Nodes.

In Figure 5.5 above, it can be observed that retransmission packet in 1/24 has a high value of retransmission packets between a source node and destination node. In three cases above, when the data rate increases, so the number of retransmission of packets decreases. Because in one server and twenty-four clients there is loss in packet for this reason the retransmission will decrease.

Table 5.6: Simulation Results of Average Throughput for Wireless Standard 802.11g with Different Data Rates for DSR Protocol.

802.11g data rate Mb/s	Throughput		
	1\1	1\12	1\24
11	10384.667	127803.36	249234.08
24	10472.987	218820.693	368185.92
54	10523.813	316883.573	571878.32

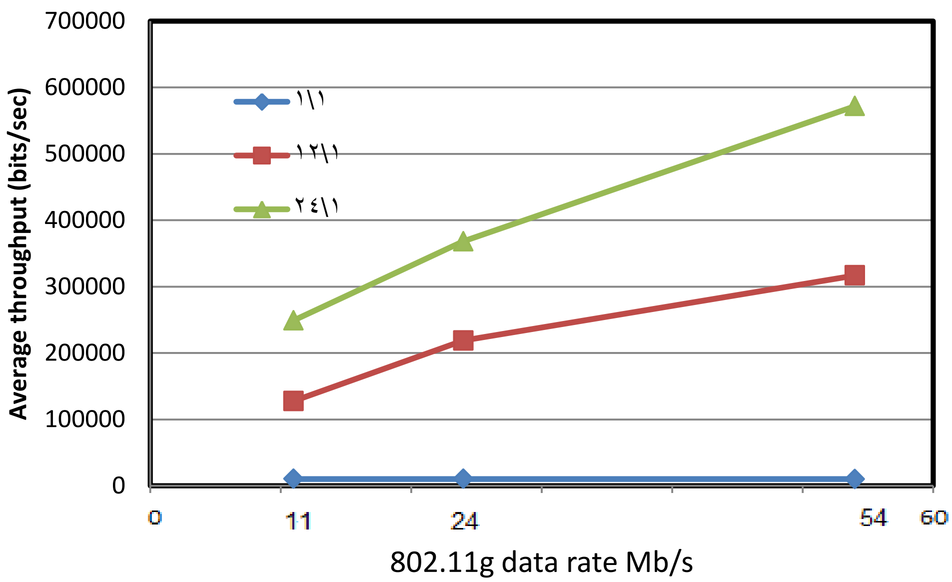

Figure 5.6: Average Throughput Versus Wireless Standard 802.11g with Different Data Rates for DSR Protocol with 25 Nodes.

In Figure 5.6 above it can be observed that 1/24 has the highest value and 1/1 has the lowest value of throughput when they have data rate 11Mbps. It means that 1/24 has the large number packets successfully transmitted from source node to destination node. It appears that when data rate increases, the throughput also increases.

Table 5.7: Simulation Results of Average Download Response Time for Wireless Standard 802.11g with Different Data Rates for DSR Protocol.

802.11g data rate Mb/s	Download Response Time		
	1\1	1\12	1\24
11	0.005	0.080	0.158
24	0.006	0.172	0.311
54	0.008	0.479	0.616

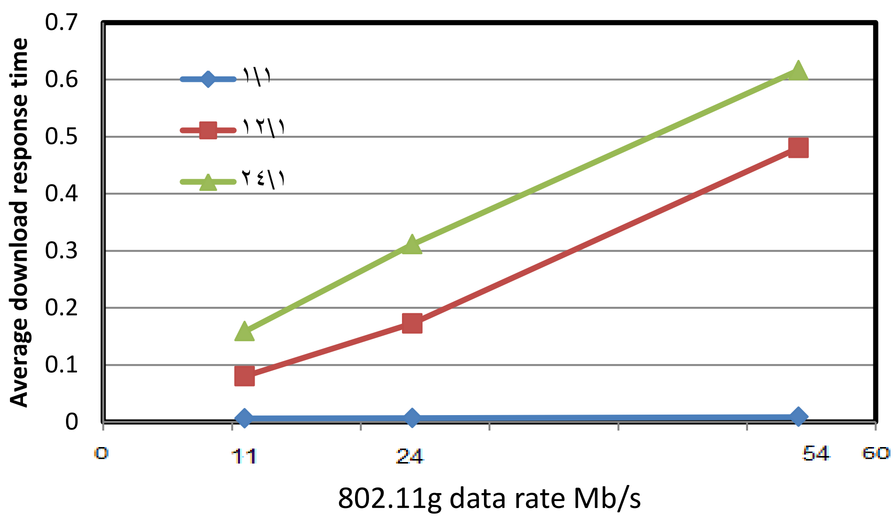

Figure 5.7: Average Download Response Time Versus Wireless Standard 802.11g with Different Data Rates for DSR Protocol with 25 Nodes.

In the Figure above we can observe that server 1/24 clients have the highest value and 1/1 has the lowest value of download response time. In three cases above the value increases when the data rate increases. It means that the time elapsed between sending a request and receiving the response packet increases.

Table 5.8: Simulation Results of Average Upload Response for Wireless Standard 802.11g with Different Data Rates for DSR Protocol.

802.11g data rate Mb/s	Upload Response Time		
	1\1	1\12	1\24
11	0.003	0.077	0.158
24	0.004	0.132	0.269
54	0.005	0.330	0.599

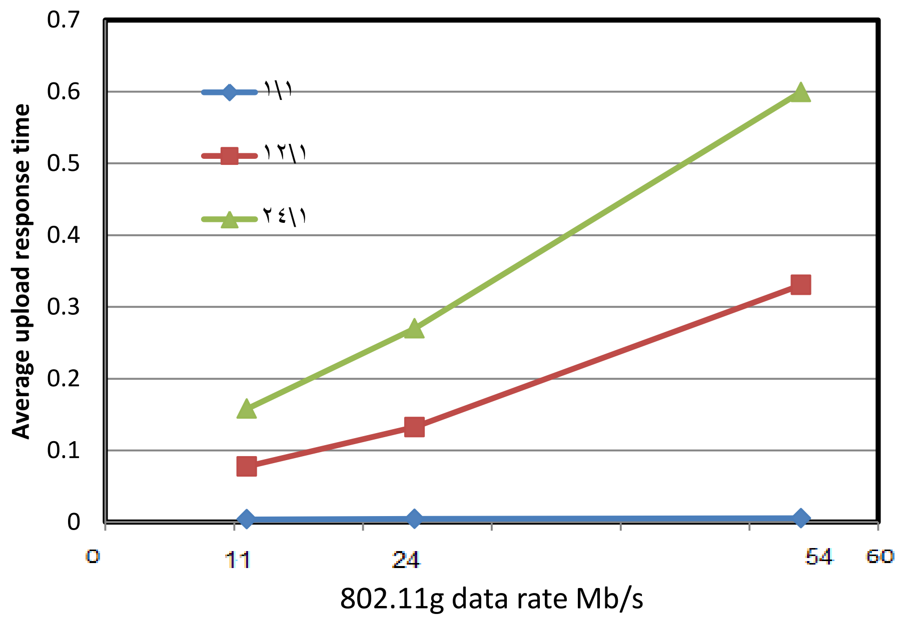

Figure 5.8: Average Upload Response Time Versus Wireless Standard 802.11g with Different Data Rates for DSR Protocol with 25 Nodes.

In Figure 5.8 above it can be observed that the FTP upload response time has the highest value in 1/24 with data rate 54Mbps and this rate is decreased in other cases when the data rates are decreased. It means that average FTP upload time depends on the data rates and needs time elapse to send a file and receive a response.

Category 2:

In the second category we used wireless standards 802.11g and 802.11b with data rate (11Mbps). In this category, we have also the one server with different number of client (1 Server / 1Client with 23 intermediate nodes, 1 Server / 12 Clients with 12 intermediate nodes, 1 Server / 24Clients). We used DSR protocol to evaluate the performance metrics over FTP application in the area 1000 * 1000 meter and the network size is 25 nodes. In addition we used OPNET modeler 17.1 to simulate our work.

Table 5.9: Simulation Results of Average Number of Hops for 802.11g and 802.11b Wireless Standards with DSR Protocol.

802.11g data rate Mb/s	Number of Hops per route		
	1\1	1\12	1\24
802.11g(11)	1.697	2.202	2.581
802.11b(11)	1.817	2.312	2.716

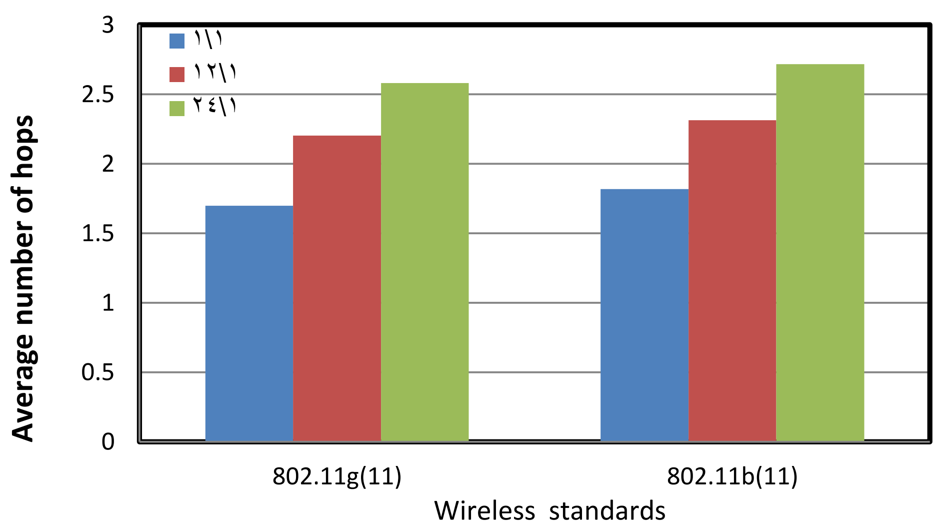

Figure 5.9: Average Number of Hops Versus Different Wireless Standards 802.11g and 802.11b for DSR Protocol with 25 Nodes.

In Figure 5.9 above it can be observed that the average number of hops that compared with wireless standards 802.11b and 802.11g with same data rate (11Mbps). In wireless standard 802.11b network topology 1/24 has the maximum number of hops. It therefore seem that when the wireless standard 802.11b has a large number of clients they need more hops to transmit packets between source node and destination node as compared to wireless standard 802.11g.

Table 5.10: Simulation Results of Routing Discovery Time for 802.11g and 802.11b Wireless Standards with DSR Protocol.

802.11 data rate Mb/s	Routing Discovery Time		
	1\1	1\12	1\24
802.11g(11)	0.008	0.050	0.076
802.11b(11)	0.010	0.072	0.128

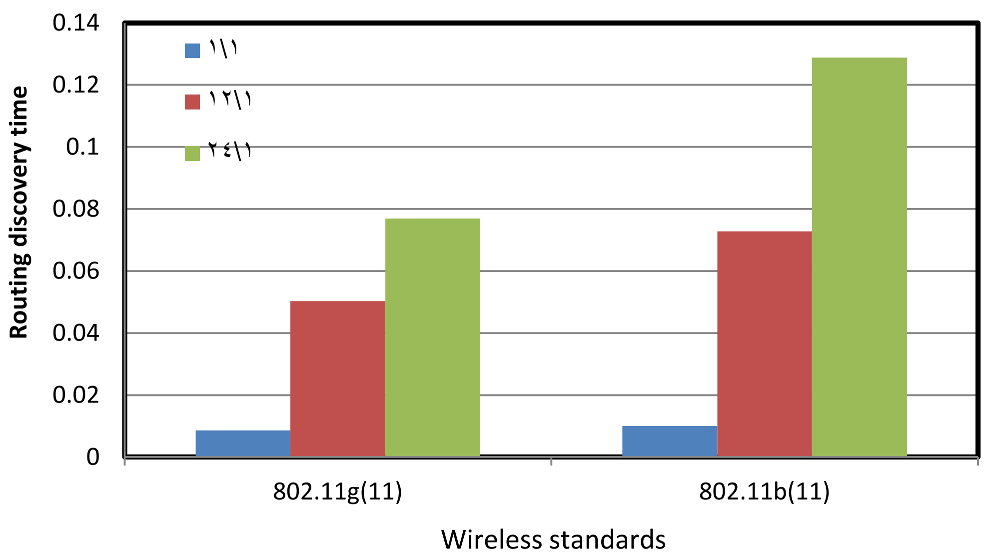

Figure 5.10: Routing Discovery Time Versus Different Wireless Standards 802.11g and 802.11b for DSR Protocol with 25 Nodes.

In Figure 5.10 above it can be observed that the Route Discovery time for 1/24 has the highest value in the same data rates. This means that when we have a large number of requests form the clients, it need too much time to know the path between source and destination. Consequently, when we have one server with one client we have only one request from the client, so RD time needs to find one shortest path between source and destination in this case it does not need more time. For this reason above it appears to us that the wireless standard 802.11b needs more time that 802.11g to know the path between a source node and destination node.

Table 5.11: Simulation Results of Average Routing Traffic Ratio Time for 802.11g and 802.11b Wireless Standards with DSR Protocol.

802.11 data rate Mb/s	Routing Traffic Ratio		
	1\1	1\12	1\24
802.11g (11)	0.415	0.392	0.368
802.11b (11)	0.409	0.473	0.419

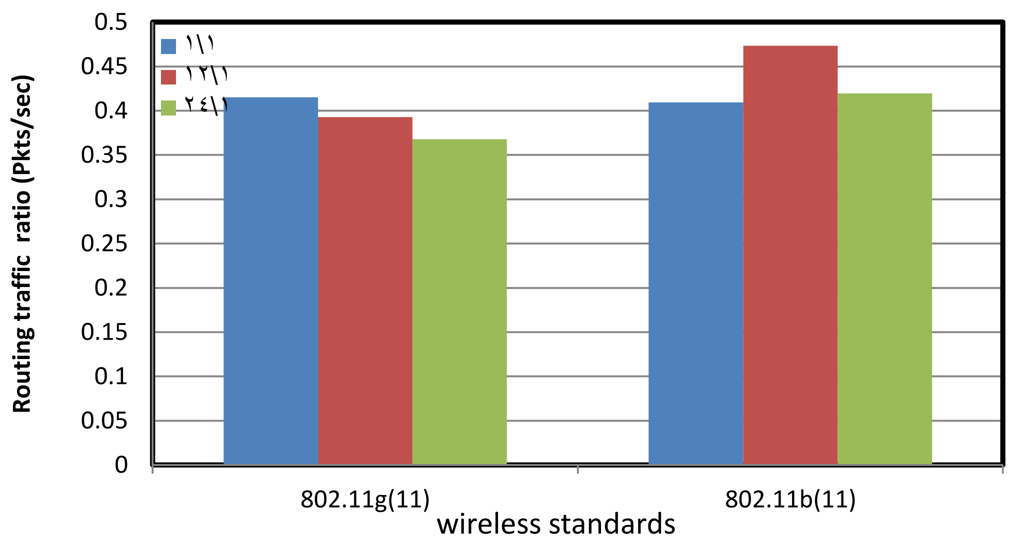

Figure 5.11: Average Routing Traffic Ratio Versus Different Wireless Standards 802.11g and 802.11b for DSR Protocol with 25 Nodes.

In Figure 5.11 above it can be observed that the routing traffic ratio of wireless standards 802.11g and 802.11b with data rates11 Mbps. When the network is 1/12 and 1/24 we have the highest routing traffic ratio as compared to 1/1 that has the lowest routing traffic ratio in wireless standard 802.11b. So it appears to us that the wireless standard 802.11b has more risks than 802.11g to lose packets. When number of clients increases the number of lose packets increases.

Table 5.12: Simulation Results of Average Media Access Delay for 802.11g and 802.11b Wireless Standards with DSR Protocol.

802.11 data rate Mb/s	Media Access Delay		
	1\1	1\12	1\24
802.11g(11)	0.0006	0.009	0.021
802.11b(11)	0.0014	0.017	0.037

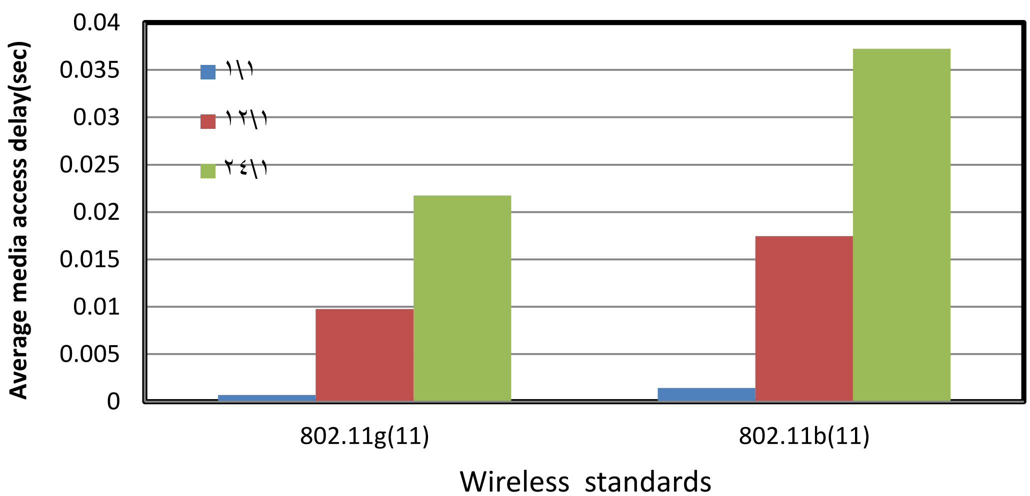

Figure 5.12: Average Media Access Delay Versus Different Wireless Standards 802.11g and 802.11b for DSR Protocol with 25 Nodes.

In Figure 5.12 above it can be observed that the media access delay for wireless standard 802.11b has the highest media access delay as compared to 802.11g. 1/24 has the highest value when we use wireless standard 802.11b. It means that the nodes need too much time to transmit packets from one node to another. So whenever the number of hops increases the media access delay increases. It appears to us that the wireless standard 802.11b needs more time than wireless standard 802.11g to transmit packets between nodes.

Table 5.13: Simulation Results of Average Retransmission Attempts for 802.11g and 802.11b Wireless Standards with DSR Protocol.

802.11g data rate Mb/s	Retransmission Attempts		
	1\1	1\12	1\24
802.11g(11)	0.172	0.297	0.365
802.11b(11)	0.051	0.200	0.220

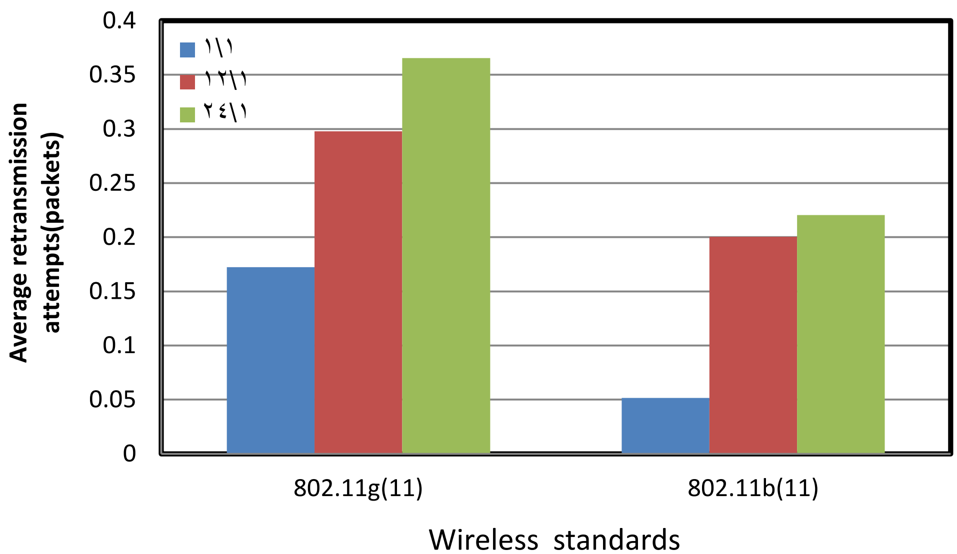

Figure 5.13: Average Retransmission Attempts Versus Different Wireless Standards 802.11g and for DSR Protocol with 25 Nodes.

In Figure 5.13 above it can be observed that retransmission packets of wireless standard 802.11g in 1/24 and 1/12 have a high value of retransmission packets between source node and destination node. It appears to us that the when we use the wireless standard 8020.11g needs more retransmission than wireless standard 802.11b. So with wireless standard 802.11g we have Opportunity more than wireless standard 802.11b to lose packets in the way.

Table 5.14: Simulation Results of Average Throughput Versus for 802.11g and 802.11b Wireless Standards with DSR Protocol.

802.11g data rate Mb/s	Throughput		
	1\1	1\12	1\24
802.11g(11)	10384.666	127803.36	249234.08
802.11b(11)	10261.2	117112.96	232077.52

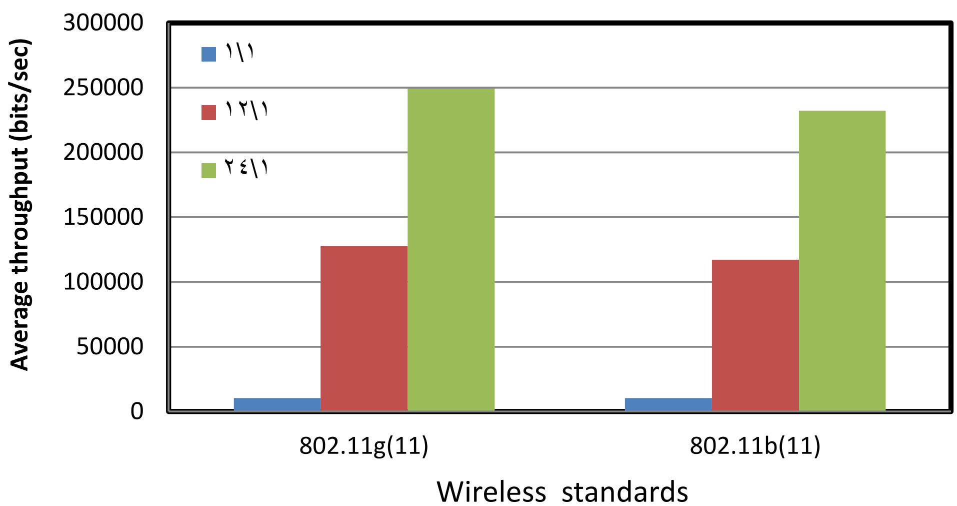

Figure 5.14: Average Throughput Versus Different Wireless Standards 802.11g and 802.11b for DSR Protocol with 25 Nodes.

In Figure 5.14 above it can be observed that the wireless standard 802.11g has higher value than 802.11b. It appears to us that the number of bits transmitted successfully by 802.11g is higher than the number of bits transmitted by 802.11b. When we use wireless 802.11g (11Mbps) they are able to transmit data successfully more than 802.11b (11Mbps).

Table 5.15: Simulation Results of Average Download Response Time for 802.11g and 802.11b Wireless Standards with DSR Protocol.

802.11g data rate Mb/s	Download Response Time		
	1\1	1\12	1\24
802.11g(11)	0.005	0.080	0.158
802.11b(11)	0.011	0.134	0.268

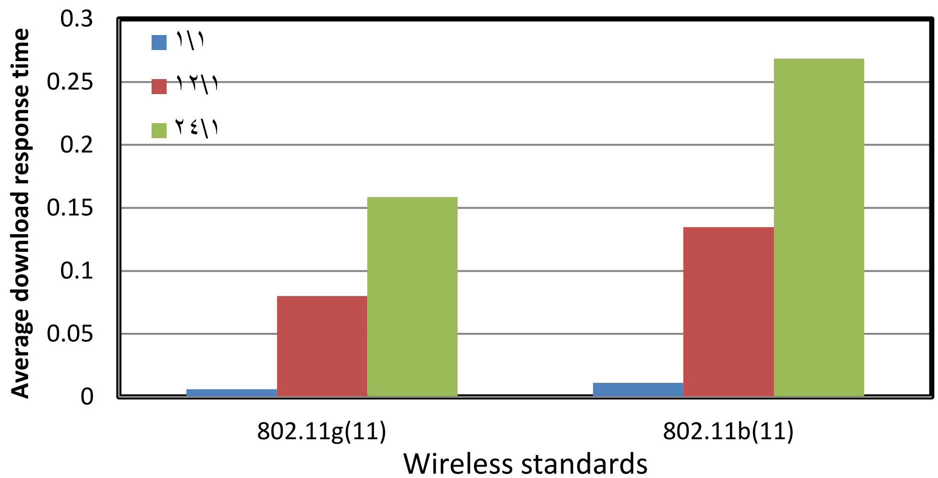

Figure 5.15: Average Download Response Time Versus Different Wireless Standards 802.11g and 802.11b for DSR Protocol with 25 Nodes.

In Figure 5.15 above it can be observed that the FTP download response time with wireless standard 802.11b has a high value in 1/24 as compared with wireless standard 802.11g in the same data rate. It means that the wireless standard 802.1b with 11 Mbps need more time than wireless standard 802.11g to send a request and receive the response packet.

Table 5.16: Simulation Results of Average Upload Response Time for 802.11g and 802.11b Wireless Standards with DSR Protocol.

802.11g data rate Mb/s	Upload Response Time		
	1\1	1\12	1\24
802.11g(11)	0.003	0.077	0.158
802.11b(11)	0.011	0.134	0.266

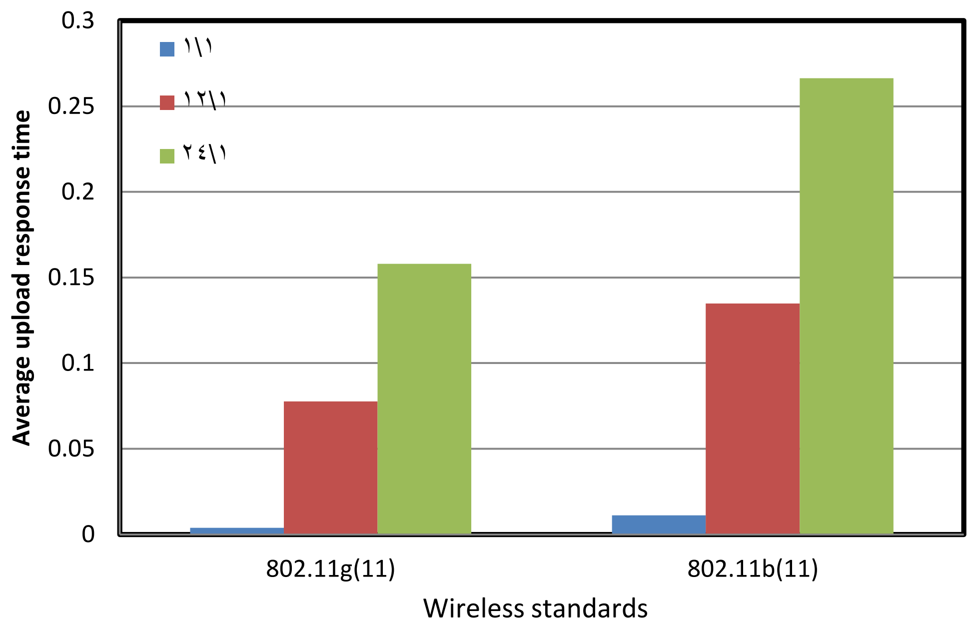

Figure 5.16: Average Upload Response Time Different Versus Wireless Standards 802.11g and 802.11b for DSR Protocol with 25 Nodes.

In Figure 5.16 above it can be observed that FTP upload response time in wireless standard 802.11b is higher than 802.11g when they use 1/24. It appears to us that the wireless standard 802.11b needs more time than wireless standard 802.11g for send file and receives a response.

Table 5.17: Comparison parameters with [23]

Parameter	**Our work**	**[23]**
Application type	FTP	HTTP
Message size	256 bytes	1000 bytes
Routing protocol	DSR	AODV
Application start time	Constant 5 (sec)	Constant 10 (sec)
Profile start time	Constant 10 (sec)	Constant 5 (sec)

Table 5.17 shows usage of the parameters between our work and [23], were in [23] HTTP application is used with AODV routing protocol.

Table 5.18: Comparison between our work and [23] when there is 1 server and 1 client (1/1) in the network

Performance metric	**Our work**				**[23]**			
	Standards				**Standards**			
	802.11g 11Mbps	802.11g 24Mbps	802.11g 54Mbps	802.11b 11Mbps	802.11g 11Mbps	802.11g 24Mbps	802.11g 54Mbps	802.11b 11Mbps
Number of hops per route	1.697	1.806	2.373	1.817	1.741	1.796	1.836	1.901
Route discovery time (sec)	0.008	0.006	0.010	0.010	0.098	0.095	0.287	0.144
Media access delay (sec)	0.000 6	0.0004	0.0004	0.0014	0.001	0.0007	0.0007	0.002
Retransmis sion attempts (Packets)	0.172	0.156	0.145	0.051	0.331	0.251	0.229	0.301
Throughpu t (bit/sec)	10384	10472	10523	10261	539409	577180	617577	537768

Table 5.18 shows the comparison of the results between our work and ref [23], were in [23] the HTTP application is used with AODV routing protocol. The table shows the results of network while there is, 1 server and 1 client, were the used metrics are number of hops, route discovery time, media access delay, retransmission attempts ad

throughput with wireless standard 802.11b with 11Mbps and wireless standard 802.11g with different data rates (11Mbps, 24Mbps and 54Mbps). In this study the number of hops in 802.11g with data rate (24Mb and 54Mb) has higher value as a comparison with ref [23] in wireless standard 802.11g with data rates (24Mb and 54Mb). Route discovery time in our work is compared with all cases have the lower values as a comparison with ref [23]. Also, media access delay in my work with four cases has the lower value as a comparison with ref [23]. A retransmission attempt in ref [23] with four cases has the higher value as a comparison with our work. Throughput in our work with four cases has the lower value as a comparison with ref [23].

Table 5.19: Comparison between our work and [23] when there is 1 server and 12 clients (1/12) in the network

Performance metric	**Our work**				**[23]**			
	Standards				**Standards**			
	802.11g 11Mbps	802.11g 24Mbps	802.11g 54Mbps	802.11b 11Mbps	802.11g 11Mbps	802.11g 24Mbps	802.11g 54Mbps	802.11b 11Mbps
Number of hops per route	2.202	2.313	2.672	2.312	2.417	2.584	2.677	2.420
Route discovery time (sec)	0.50	0.44	0.54	0.072	0.613	0.479	0.430	0.753
Media access delay (sec)	0.009	0.006	0.005	0.017	0.003	0.002	0.001	0.005
Retransmission attempts (Packets)	0.297	0.263	0.252	0.200	0.385	0.302	0.238	0.373
Throughput (bit/sec)	127803	218820	316883	117112	1691439	2171878	2335747	1489968

Table 5.19 shows the comparison of results between our work and ref [23], were in [23] HTTP application is used with AODV routing protocol. The table shows the results of network while there is1 server and 12 clients, were the used metrics are number of hops, route discovery time, media access delay, retransmission attempts ad throughput with wireless standard 802.11b with 11Mbps and wireless standard 802.11g with different data rates (11Mbps, 24Mbps and 54Mbps). In our work, the number of hops in four cases has a lower value as a comparison with ref [23] in. Route discovery time in our work in all four cases has the lower values as a comparison with ref [23]. Also media access delay in all cases has the lower value as a comparison with ref [23]. A retransmission attempt in ref [23] with four cases has the higher value as a comparison with my work. Furthermore, throughputs in our work in all four cases have the lower value as a comparison with ref [23].

Table 5.20: Comparison between our work and [23] when there is 1 server and 24 clients (1/24) in the network

Performance metric	**Our work**				**[23]**			
	Standards				**Standards**			
	802.11g 11Mbps	802.11g 24Mbps	802.11g 54Mbps	802.11b 11Mbps	802.11g 11Mbps	802.11g 24Mbps	802.11g 54Mbps	802.11b 11Mbps
Number of hops per route	2.581	2.939	3.512	2.716	3.503	3.631	3.685	3.358
Route discovery time (sec)	0.076	0.070	0.096	0.0128	0.695	0.445	0.353	0.799
Media access delay (sec)	0.021	0.012	0.011	0.037	0.006	0.003	0.002	0.12
Retransmission attempts (Packets)	0.365	0.330	0.317	0.220	0.418	0.318	0.301	0.403
Throughput (bit/sec)	249234	368185	571878	232077	2343734	3529255	3651725	1859979

Table 5.20 shows the comparison of the results between our work and ref [23], were in [23] the HTTP application is used with AODV routing protocol. The table shows the results of network while there is 1 server and 24 clients, were the used metrics are number of hops, route discovery time, media access delay, retransmission attempts ad throughput with wireless standard 802.11b with 11Mbps and wireless standard 802.11g with different data rates (11Mbps, 24Mbps and 54Mbps). In our work, the numbers of hops in all four cases has lower value as a comparison with ref [23] in. Route discovery time in my work with all cases has the lower values as a comparison with ref [23]. Media access delay in our work with all cases has the lower value as a comparison with ref [23]. A retransmission attempt in ref [23] in all four cases has the higher value as a comparison with our work. Also throughput in all four cases has the lower value as a comparison with ref [23].

5.3 Confidence Interval Calculation

Average values and confidence intervals of the investigated performance metrics of the experiments are provided. In table 5.18-5.21 the performance metrics that were used in these experiments are number of hops per route, route discovery time, download response time and upload response time.

Table 5.21: Average values and 95% confidence intervals of the performance metrics for DSR with message number of nodes size 256 bytes for 25 mobile nodes with wireless standard 802.11g (11Mbps).

Metric	Wireless standard 802.11g (11Mbps) With different number of client and intermediate		
	1server/1client	1server/12client	1server /24client
Number of hops per route	1.497181 ± 0.018311	2.202352 ± 0.289319	2.381695 ± 0.302946
Route discovery time	0.008595 ± 0.008457	0.050262 ± 0.012069	0.076965 ± 0.01009
Download response time	0.005957 ± 0.000225	0.08002 ± 0.014825	0.158683 ± 0.006975
Upload Response Time	0.005936 ± 0.000224	0.077745 ± 0.012206	0.158019 ± 0.00569

Table 5.22: Average values and 95% confidence intervals of the performance metrics for DSR with message size 256 bytes for 25 mobile nodes with wireless standard 802.11g (24Mbps).

Metric	Wireless standard 802.11g (24Mbps) With different number of client and intermediate		
	1server/1client	1server/12client	1server /24client
Number of hops per route	1.806221 ± 0.078884	2.013042 ± 0.497151	1.839278 ± 0.74855
Route discovery time	0.006967 ± 0.004546	0.044656 ± 0.044432	0.070808 ± 0.040301
Download response time	0.003658 ± 0.00014	0.172534 ± 0.188216	0.311064 ± 0.198648
Upload Response Time	0.003587 ± 0.00012	0.132028 ± 0.107507	0.269978 ± 0.176739

Table 5.23: Average values and 95% confidence intervals of the performance metrics for DSR with message size 256 bytes for 25 mobile nodes with wireless standard 802.11g (54Mbps).

Metric	Wireless standard 802.11g (54Mbps) With different number of client and intermediate		
	1server/1client	1server/12client	1server /24client
Number of hops per route	2.373285 ± 0.259926	2.272182 ± 0.19933	2.212401 ± 0.396263
Route discovery time	0.010751 ± 0.005445	0.054285 ± 0.093839	0.096687 ± 0.089777
Download response time	0.008568 ± 0.016663	0.579945 ± 0.743032	0.616203 ± 0.57674
Upload Response Time	0.003432 ± 0.000227	0.618696 ± 0.900182	0.599318 ± 0.659488

Table 5.24: Average values and 95% confidence intervals of the performance metrics for DSR with message size 256 bytes for 25 mobile nodes with wireless standard 802.11b (11Mbps).

Metric	Wireless standard 802.11b (11Mbps) With different number of client and intermediate		
	1server/1client	1server/12client	1server /24client
Number of hops per route	1.494586 ± 0.019908	2.253243 ± 0.196072	2.482147 ± 0.223787
Route discovery time	0.010046 ± 0.0103	0.072742 ± 0.02148	0.12882 ± 0.032655
Download response time	0.011208 ± 0.000709	0.134615 ± 0.017463	0.268381 ± 0.014515
Upload Response Time	0.011072 ± 0.000298	0.134533 ± 0.015787	0.266438 ± 0.015512

Chapter 6

CONCLUSION

In this study, we investigate the wireless standards 802.11b and 802.11g using same data rate (11 Mbps). Additionally 802.11g is used with different data rates 11 Mbps, 24 Mbps and 54 Mbps. FTP application is used to make data traffic on network with DSR protocol. Different network types were used, with 1 server /1 client, 1 server / 12 clients and 1 server/ 24 clients. Different performance metrics were used as number of hopes, delay, throughput, retransmission attempts, download response time and upload response time.

The simulation results conclude the following: The number of hops per route of 802.11g is increased by increasing data rate (11Mbps, 24 Mbps and 54Mbps). The additionally by comparing 802.11b with 802.11g in number of hops per route, 802.11b uses more number of hops per route. The average media access delay of 802.11g is decreased by increasing data rate (11Mbps, 24 Mbps and 54Mbps). The throughput of 802.11g standard is increasing when data rate is increased. Additionally, the throughput of 802.11g is greater compared with 802.11b when they are used with same data rate. The average download response time and average upload response time of FTP application is increased by increasing data rates using 802.11g. Also, average upload response time and average download response time of

802.11b is more than by 802.11g. Data traffic ratio of 802.g standard is increased by increasing data rate.

REFERENCES

[1] Perkins.C.E. “*Ad hoc Networking*", Boston, Addison Wesley (2001).

[2] Tamilselvan L. and Sankaranarayanan D. V. “*Prevention of impersonation attack in wireless mobile ad hoc Networks*", International Journal of Computer Science and Network Security (IJCSNS), Vol. 7, No. 3, p.118–123 (2007).

[3] Papadimitratos P. and Haas Z. J. “*Secure routing for mobile ad hoc networks*", In Proceedings of CS Communication Networks and Distributed Systems Modeling and Simulation Conference (2002).

[4] Hu Y. C, Johnson D. B. and Perrig A. SEAD: “*Secure efficient distance vector routing for mobile wireless ad hoc networks*", In IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), p.3–13 (2002).

[5] Ramanuj. N. P. And Diwanji. H. M. “*Behavior Analysis of TCP Traffic in Mobile Ad Hoc Network using Reactive Routing Protocols*”. IP Multimedia Communications, p.89-93 (2008).

[6] Sharma. M. L., Rizvi. N. F., Sharma. N., Malhan. A., Sharma. S. "*Performance Evaluation of MANET Routing Protocols under CBR and FTP traffic classes*". Int. J. Comp. Tech. Appl., Vol. 2(3), p.392-400 (2011).

[7] Singh. P, Barkhodia. E, Walia. G. K. "*Evaluation of various Traffic loads in MANET with DSR routing protocol through use of OPNET Simulator*". International Journal of Distributed and Parallel Systems (IJDPS), Vol.3, No.3, p.75-83 (2012).

[8] Puneet, Sawhney. R. S., Vohra. R. "*Physical Characteristics based MANET Routing Protocols for Campus Network*". International Journal of Computer Applications (0975 – 8887), Vol.48, No.3, p.32-38 (2012).

[9] Nuri. I. "Performance Modeling of IEEE802.11 WLAN using OPNET". AUT University, New Zealand, (2009).

[10] Anjali, Maninder. S "Simulation and Performance Analysis of AODV, OLSR, GRP Routing Protocol by considering IEEE 802.11Standard" International Journal of Computer Applications (0975 – 8887), Vol.2, No.3, p.171-178 (2012).

[11] Ullah. I. "*Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols.*" M.A. thesis, Blekinge Institute of Technology, Sweden, 2010.

[12] http://en.wikipedia.org/wiki/Mobile_ad_hoc_network, last visited 12, Apr, 2010.

[13] Abolhasan. M, T. Wysocki. T, Dutkiewicz. E, "*A Review of Routing Protocols for Mobile Ad-Hoc Networks*", Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.

[14] Nyirenda. B and Mwanza. J. "*Performance Evaluation of Routing Protocols in Mobile Ad hoc Networks (MANETs)*". M.A. thesis, Blekinge Institute of Technology, Sweden, 2009.

[15] David A. M, Josh B, Jorjeta J, and David B. J. *"The Effects of On-Demand Behavior in Routing Protocols for Ad Hoc Networks*". IEEE Journal on Selected Areas in Communications", 17(8):1439–1453, August 1999.

[16] David B. Johnson and David A. Maltz. *"Dynamic Source Routing in Ad Hoc Wireless Networks". In Mobile Computing*, edited by Tomasz Imielinski and Hank Korth, chapter 5, p. 153–181.Kluwer Academic Publishers, (1996).

[17] Broch. J., Maltz. D. A., Johnson. D. B., Yih-chun Hu, and Jetcheva. J. "*A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols*." In Proceedings of the Fourth Annual ACM/IEEE International

Conference on Mobile Computing and Networking (MobiCom'98), p.85–97, Dallax, TX, October 1998.

[18] "Routing Protocols for ad-hoc Mobile Wireless Networks", http://www.cse.wustl.edu/~jain/cis788-99/ftp/adhoc_routing/index.html, Accessed October 24, 2010.

[19] "Introduction to using OPNET Modeler". Retrieved July 22, 2003. WebSite:http://www.sce.carleton.ca/faculty/lambadaris/courses/5001/opent_tutorial.pdf.

[20] Suresh. A. "*Performance Analysis of Ad hoc On-demand Distance Vector routing (AODV) using OPNET Simulator*" M.A. thesis, University of Bremen, Germany, April 2005.

[21] *"OPNET Network Modeler"*. Retrieved July 24, 2003.
Web Site: http://www.eos.ncsu.edu/software/opnet/.

[22] Taposh D. R. *"Simulation of a Wireless LAN using OPNET"*. Retrieved 24 July, 2003.
Web Site: http://www.ece.iit.edu/~tdutta/Website/WirelessLan.pdfl

[23] Araz. J. Q "Performance evaluation of wireless IEEE 802.11g and 802.11b on HTTP Application over AODV using OPNET" M.A. thesis, University of Eastern Mediterranean University Gazimağusa, North Cyprus, June 2013.