Performance Evaluation of Wireless Standards 802.11g and 802.11b on HTTP Application over AODV Protocol using OPNET

Araz Jameel Qasim

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

Mobile ad hoc network (MANET) is a wireless network that does not contain an infrastructure. Nodes in this network are mobile and can join or leave out from the network in time. This feature can be used in many applications like collecting data. In addition to this mobile devices associated with stations are subject to change and continuity, which has led to many changes in the network topology. However, the problem with this network is that it is easily penetrated by hackers trying to break in, and therefore it should increase its efficiency using routing protocols. It is used to find the path between stations or update existing ones. Routing protocols are classified, as a proactive protocols (e.g., OLSR), reactive protocols (e.g., AODV and DSR), and hybrid protocol (e.g., TORA). The IEEE 802.11 wireless LAN, also known as Wi-Fi, has been classified into several standards including 802.11a, 802.11b and 802.11g.

In this thesis, we used HTTP application to compare between IEEE 802.11b and 802.11g with different data rates. The routing protocol is used ad hoc on demand distance vector (AODV) protocol in this simulation. Performance of these routing protocols is analyzedby metrics; number of hops per route, HTTP page response time, HTTP object response time, route discovery time, media access delay, retransmission attempts(packet) and throughput.OPNET Modeler version 17.1 is used for modeling and simulatingad hoc network.

It is demonstrated from the simulation results that; the media access delay of 802.11b with 11Mbps is greater than 802.11g in all used network cases of clients number. Average retransmission attempts of 802.11g is decreased by increasing the data rates

(11Mbps, 24Mbps, and 54Mbps) of network, additionally, the peak value of retransmission attempts is where 24 clients are communicating with server for both standards 802.11b and 802.11g. Throughput of the network for 802.11g is greater than 802.11b for 11Mbps data rate. Additionally, throughput of both standards are increased by increasing the number of nodes that are communicating with the server.

Keyword: MANET, AODV, HTTP, IEEE 802.11, OPNET

ÖZ

Mobil özel amaca yönelik (ad hoc) ağ (MANET) altyapısı olmayan kablosuz bir ağdır. Bu ağdaki düğümler mobil olup zaman içerisinde ağa katılıp ağdan ayrılabilirler. Bu özellik veri toplama gibi birçok uygulamada kullanabilirler. Mobil cihazların hareketliliğinden dolayı zaman içerisinde ağın topolojisinde de değişikliler olmaktadır. Bu ağlardaki başlıca problem ağı yıkmak için dış saldırılara açık olması ve verimliliği artırmak için etkili yönlendirme protokollerine gerek duyulmasıdır. Yönlendirme protokolleri, istasyonlar arasında yolu bulmak ve var olanı güncellenmek için kullanılırlar. Yönlendirme protokolleri proaktif(ör. OLSR), reaktif (ör. AODV) ve karma (ör. TORA) olmak üzere sınıflara ayrılırlar. IEEE 802.11 veya WI-FI olarak da bilinen kablosuz LAN standardının 802.11a, 802.11b ve 802.11 gibi farklı varyasyonlar vardır. Bu tezde, HTTP Protokolü'nün kullandığı web uygulaması kullanılarak 802.11b ve 802.11g standartları farklı veri oranlarında karşılaştırılmıştır. Simülasyonlarda kullanılan yönlendirme protokolü Ad hoc on- demand Distance Vector (AODV) Protokolü'dür. Sistemin performansı, her yönde seçilen sekme sayısı (number of hopsperroute), HTTP sayfa yanıt zamanı (HTTP page response time), HTTP nesne yanıt zamanı (HTTP objectresponse time), ortam giriş gecikmesi (media Access delay), paketlerin yeniden gönderim girişi (retransmission attempts) (packet) ve üretilmiştir (throughput) ölçütleri kullanılarak analiz edilmiştir. OPNET simülatör versiyon 17.1 ad hoc ağlarının modellenmesi ve simülasyonu için kullanılmıştır.

Simülasyon sonuçlarından elde edilen sonuçlar ortama giriş gecikmez sistemde olan bütün kullanım saflarında 802.11b'de 802.11g'den daha fazladır. 802.11g'de veri hızı arttırıldığı zaman yeniden gönderim girişimi azalıyor. Ağda üretilen iş arası 11Mbps veri hızında 802.11g'de 802,11b'den daha fazladır. Buna ek olarak her iki standartta da üretilen iş oranı sunucuyla iletişime geçen düğüm sayısı arttıkça artıyor.

Anahtar Kelimeler: MANET, AODV, HTTP, IEEE 802.11, OPNET

Many hands make light work

I dedicate this thesis to my parents, my family and my friends.

ACKNOWLEDGMENTS

First of all, I would like to thank Almighty Allah for blessing me with the ability, patience and necessary strength to complete this thesis.I would like to extend my profound thanks and gratitude to my supervisor Assist. Prof. Dr.Gürcü Özfor her useful comments, remarks and encouragement. I am sure that this dissertation would not have been possible without the guidance of others in particular my supervisor who in one way and another contributed valuable assistance in preparation and completion of this thesis. Apart from the effort I made, the success of any project depends largely on the encouragement and guidance of others. I would like to seize this opportunity to express my gratitude to those who encourage and assisted me in successful completion of this project. Once more I would like to show my greatest appreciation to my supervisor Assist. Prof. Dr. Gürcü Özfor guidance, constant support and help.

Finally, I would like to thank my parents and family for their support overseas. Without their help, I could not complete the dissertation on time.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREIATIONS

MANET	Mobile Ad hoc Network
HTTP	Hybrid Text Transfer Protocol
AODV	Ad hoc On-demand Distance Vector
DSR	Dynamic Source Routing
IP Address	Internet Protocol Address
IETF	Internet Engineering Task Force
OPNET	Optimized Network Engineering Tool
OLSR	Optimized Link State Routing
RFC	Request For Comments
RREQ	Route Request
RREP	Route Reply
RERR	Route Error
RIP	Routing Information Protocol
RQPD	Random Query Processing Delay
TCP	Transmission Control Protocol
TTL	Time To Live
Wi-Fi	Wireless Fidelity
WG	Working Group
WRP	Wireless Routing Protocol
WLAN	Wireless Local Area Network

Chapter 1

INTRODUCTION

1.1 Introduction

Presently Mobile ad hoc network (MANET) is the most well known wireless network.It consists of a number of independent wireless nodes having no centralized access point, infrastructure and any centralized administration. The use of wireless technology has become an omnipresent method to access the internet because it is easily and inexpensively deployed and has the possibility of adding new devices to the network at low or no cost at all.MANETs can be applied to different applications such as emergency relief scenarios, law enforcement, public meetings and even to battlefield communications. In MANET each node can communicate with nodes in its range and with those beyond its range using the concept of multihop communication in which other nodes relay the packets [1]. The idea of mobile ad hoc networking is sometimes understood as infrastructure less networking as it does not need any servers, routers, access points or cables.

MANET routing protocol noticed experimental Request For Comments (RFC) since 2003. Proper addressing of deployment and implementation of the protocol are not done by (RCFs), while the proposed routing protocol was pointed out as trail technology with the expectation of finalizing it into a standard. MANET working group (WG) of internet engineering task force (ISTF) [2], undertook much research to develop and standardize the different routing protocols such as dynamic source routing (DSR), optimization link state routing (OLSR), temporally ordered routing algorithm (TORA) and ad hoc on demand distance vector (AODV). MANET stepwise exploited wireless communication at the global level as the vital and common means of human communication. Hot spots in universities, Offices, Hotels and Airports are configured with WI-FI cards, standing as a major source of human communications in our contemporary world. As a result this motivated the researchers to focus their attention on the deployment of MANET. With no doubt, in this type of advanced communication network, routing plays a significant role to route the data in the network. Finally, the exploration of wireless devices is paving the road to focus our studies on large networks and consequently more advanced human communications.

MANET protocols calculated and implemented at the network layer is able to severely affect the applications running at the application layer, causing unacceptable results for the users in critical situations. So the users decisions resulting in unfinished, slow and non accepting received information can bear higher losses. We want to create different scenarios to improve understanding of the MANET performance based on the applications running of the devices**.** A number of researchers intensively worked on analyzing the performance of MANET routing protocols, Transmission Control Protocol (TCP) traffic. But since MANET is one of the most efficient and reliable network for communication with distinct applications in offices, universities, hotels and airports, etc. HTTP performance is necessary in order to enable the web based applications. So it is necessary to studythe performance of selected MANET routing protocol such as AODV over HTTP traffic heavy browsing since these playa key role in MANET applications.

Routing protocols for different types of wireless networks have been proposed by a number of researchers. Researchers traditionally classify these protocols as proactive protocols, reactive protocols, or a hybrid of the two, based on the way they find new routes or update existing ones. Proactive routing protocols keep routes continuously updated, while reactive routing protocols react on demand. Routing protocols can also be classified as link state protocols or distance-vector protocols [27].

In this thesis, we used Ad hocon demand vector (AODV) protocol which was explained in the simulation design. The performance of the reactive routing protocol AODV according to the design simulation model was studied. HTTP applications are put into four categories, namely, heavy browsing, light browsing, image browsing and searching, but in our simulation we used HTTP heavy browsing. Network scalability is considered with 25 nodes with the mobility of mobile nodes. Network simulation is classified into three categories; one server and one client, one server and twelve clients, and one server and twentyfour clients.Finally, the performance metrics were chosen to compare wireless standards 802.11g with 802.11b with different data rates. Important factors for HTTP applications and AODV protocol are : number of hops per route, HTTP object response time, HTTP page response time, media access delay, retransmission attempts(packet) and throughput.

This thesis is divided into seven chapters. Chapter 1deals with the introduction, problem definition and related work.Chapter 2details the overview of mobile ad hoc network. Chapter 3 details the wireless LAN standards IEEE 802.11 and the overview of thead hoc on demand vector (AODV) protocol. Chapter 4details the hybrid text transfer protocol(HTTP) and transport control protocol TCP. Chapter 5 explains simulation work and how OPNET works. Chapter 6 details the results and the discussion of results. Chapter 7 details the conclusion followed by the references.

1.2 Survey and Related Work

MANEThasexpeditious features,it is decentralized and easily deployable.It does not need any infrastructure to achieve fast growth of its application. Mobile ad hoc network routing plays a critical role. This feature encouraged researchers to evaluate the routing protocols indifferent network conditions and to establish their impact over MANET performance. Routing protocols used to find out the path of a set of rules that have the capacity to connect devices with each other. The propagation range of the MANET is limitedfor this reason ad hoc route networks are using the multihop feature between nodes. The nodes involved in traversing the packets over MANET are not aware of this network topology,but they have the ability to cross the packets in MANET networks are not aware of the network topology. Routing protocols have a characteristic detection network topology and receive messages from adjacent nodes. The Hypertext Transfer Protocol (HTTP) is one of the main communication protocols for web traffic,HTTPis the client-server network protocol that has been in use by the World-Wide Web since 1990. When you surf the web, your browser will be sending HTTP request messages for HTML pages, style sheets, scripts and images. Web servers handle these requests by returning response messages including the requested resource. The ad hocon demand distance vector (AODV) is a reactive routing protocol that supports two routing mechanisms, unicast and multicast. AODV used to discover the route between source and destination.AODV protocol has three types of messages : route error (RERR), route request (RREQ) and route replay (RREP).The traditional routing table AODV usesone entry per destination. Not including source routing, AODV depends on routing table entries to transmit an RREP back to source. AODV protocol prevents routing loops and maintain on each side to determine the freshness of routing information through the sequencenumbers. These sequence numbers are carried by routing packets. An important feature of an AODV is the timer maintenance based states in every node, regarding operation of individual routing table entries[7].The IEEE 802.11 technology is mostly deployed for WLAN application. The IEEE 802.11 is also called as Wi-Fi that have three standards :

802.11b with data rate between (1-11)Mbps, 802.11gwith data rate between (1-54)Mbps and 802.11a with data rate between (6 -54)Mbps. The IEEE 802.11b and 802.11g using 2.4 GHz. In this thesis we compare 802.11g and 802.11b with different data rates[10].

In [3] the authorsevaluatethe performance of AODV protocol over HTTP application. In this paper it is concluded that AODV has high delay and high throughput when number of nodes increases. In [4] the authors evaluate the performance of AODV, OLSR and DSR ad hoc routing protocols using HTTP and FTP application by OPNET modeler. In this paper, it is concluded that the delay by using DSR protocol is the highest and by using OLSR the lowest. In the case of throughput, the throughput of OLSR is least but the AODV has comparative good throughput. In the case of HTTP traffic the delay and throughput are both less as compared with FTP traffic. In [5] the authorscompare the performance of AODV,DSR,OLSR and GRP on VoIP and HTTP over different IEEE 802.11 standards. In this paper it is concluded that OLSR protocol has a better performance in terms of throughput and delay, particularly for large networks. For the smaller networks the performance of AODV and OLSR is the same. In[6] the authorspresent an evaluation performance for wireless ad hoc network over HTTP application. In this paper, it is concluded that wireless LAN 802.11b supports up to 100 clients and web browsing in both infrastructure and ad hoc modes. In[7] the authors compare the performance of AODV, TORA and OLSR with reference to variable network size. In this paper, it is concluded when the number of nodes increased the network average end to end delay also increased for all three routing protocols.AODV performed decently in terms of throughput when increased the number of nodes. In[8] the authorsevaluate the performance analysis of MANET using different routing protocols on HTTP application. In this paper, we analyzed the performance of various protocols such as OLSR, AODV, GRP and DSR. The simulation results shows that OLSR protocol has better performance in terms of throughput and delay, particularly for large networks. For smaller networks the performance of AODV and OLSR are the same.With respect to the results in Table 1.1,the followings are discovered: In thisthesis we have considered the different number of clients, using different standards (with different data rates) and evaluatedmore performance metrics on the network using OPNET 17.1 which is the new work in this field.

Table 1.1: Summary of related works

Ref. No.	**Simulation Setup**							
	Simulator	**Application Type**	**Routing protocols**	**Number of nodes**	**Mobility**	**Area of Simulation**	**IEEE 802.11**	**Performance metrics**
[3]	OPNET	HTTP heavy browsing	AODV	40 nodes	Mobile nodes Speed 10 m/s	1000 ×1000 meter	802.11	Throughput (bit/sec)
[4]	OPNET	HTTP	AODV DSR	40 nodes	Speed 10 m/s	600 × 600 meter	802.11	Throughput (bit/sec)
[5]	OPNET	HTTP	AODV DSR	5 nodes 20 nodes 50 nodes 100 nodes	Mobile node	500 × 500 meter	802.11 (b) 11Mbps	Throughput (bit/sec) Route discovery time
[6]	OPNET	HTTP	AODV DSR OLSR	20 nodes	Mobile node Speed 5m/s	--	802.11 (g) 54Mbps	Throughput (bit/sec)
[7]	OPNET	HTTP	TORA, AODV, OLSR	25 nodes 50 nodes	Speed 5m/s	900 × 900 meter	802.11b 11 Mbps	Throughput (bit/sec)
[8]	OPNET	HTTP	AODV, DSR, GRP,	20 nodes	Speed 5m/s	--	802.11 (g) 54Mbps	Throughput (bit/sec)

Chapter 2

MOBILE AD HOC NETWORKS (MANETs)

2.1 Introduction

Two terms are used for MANET: either mobile ad hoc network or mobile mesh network. One must understand the basic concepts underlying the main scenarios like mesh network and mobile network before discussing MANET.If each node works independentlyof other nodes,regardless if it is connected to another network or not, it is called a mesh network, or one can say they can connect themselves to expand their network [11], as in Figure 2.1.Therefore the mobile network is the same as mesh network.

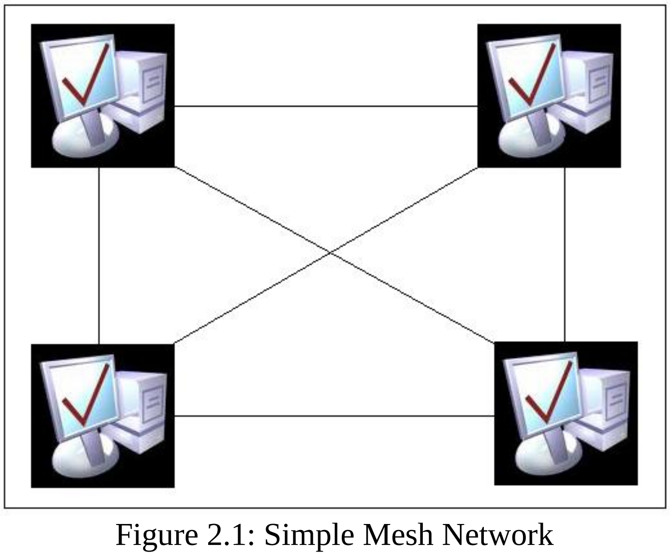


Figure 2.1: Simple Mesh Network

MANET developed in self configuration by mobile devices with wireless connected links. The nodes or devices of MANET are free to move independently in any direction without any restrictions.They frequently change their links to other devices making new link or new networks. For this reason MANET is dynamically increasing and decreasing in size.Nodes act as a router playing a retail role between communication channels.MANET has a property of routing traffic of their spreading network, contracting and changing dynamically. Alsoit makes communication between nodes difficult such the network increasesquickly for wide network connection like internet,The basic diagram is shown below in Figure 2.2.

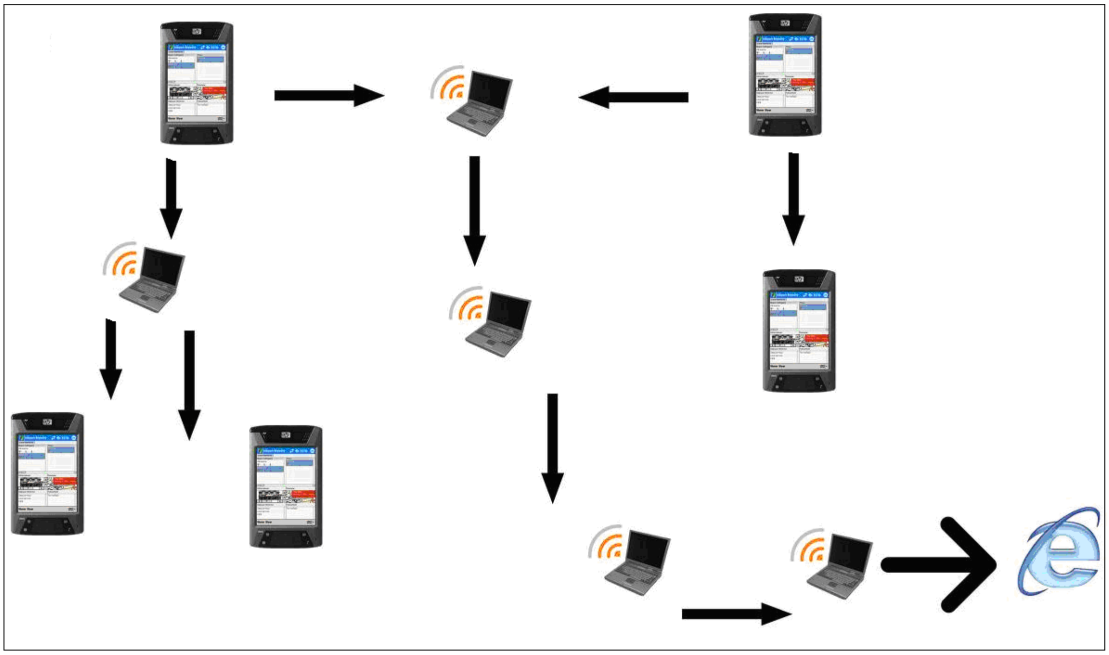


Figure 2.2: Simple Mobile Ad hoc Network [12]

Ad hoc work on top of the link layer for one kind of wireless due to router ability, if the mesh networks are not Ad hoc but it can be one kind of the mesh network, since it depended upon the type of the network environment.Figure 2.1 showed one kind of mesh network, but there are many types.It is clear that MANETs became popular and opened the door for researchers to work in the protocol domain .

The following are required criterias for a MANET network [13] :

- The routing mechanism are of multiple hops.
- There should be address assignment procedure in the mobile Ad hoc network itself configuring network in order to be able to connect each other with new network or mobile devices.
- A procedure should be followed like merging into the networks for detecting or participating in the existing network.
- A standard security protocol or mechanism is required between devices.

For the mobile Ad hoc network there should be some important routing protocol rules such as :

- Each device should be able to self start and to be selforganized to function.
- There will be no loops with multiple hop environment among devices to route protocol mechanism.
- There should be a maintenance procedure among the dynamic devices expansion the mobile Ad hoc networking is usually dynamically spreading .
- Among the devices a rapid convergence is required .
- Larger networks are also possible to deal with.

2.2 MANET Routing Protocols

The purpose of the mobile Ad hoc networks IETF in the networking group [14] is to repair mobile Ad hoc networks in IP routing standard, for which there are three basic protocols in MANET, while the a fourth one functions experimentally. These protocols can be divided into three categories: reactive, proactive and hybrid protocols.

2.2.1 The Reactive Routing Protocols

Two main thing in this protocol have to be noted [15]: firstly, it never takes the initiative to order taking in routes for network, and secondly, whenever routes are created the reactive routing protocol will be developed on demand by flooding mechanism. Such a kind of routing protocol has advantages and disadvantages as stated below :

- Bandwidth is used when there is a need to find the route, otherwise not.
- The flooding procedure due to overhead as shown in Figure 3.3 below.
- A delay in the network is there at the start .

The three steps to explain the procedure of the reactive routing protocols are :

Step1 : Here, two nodes exist to communicate at position A and B.

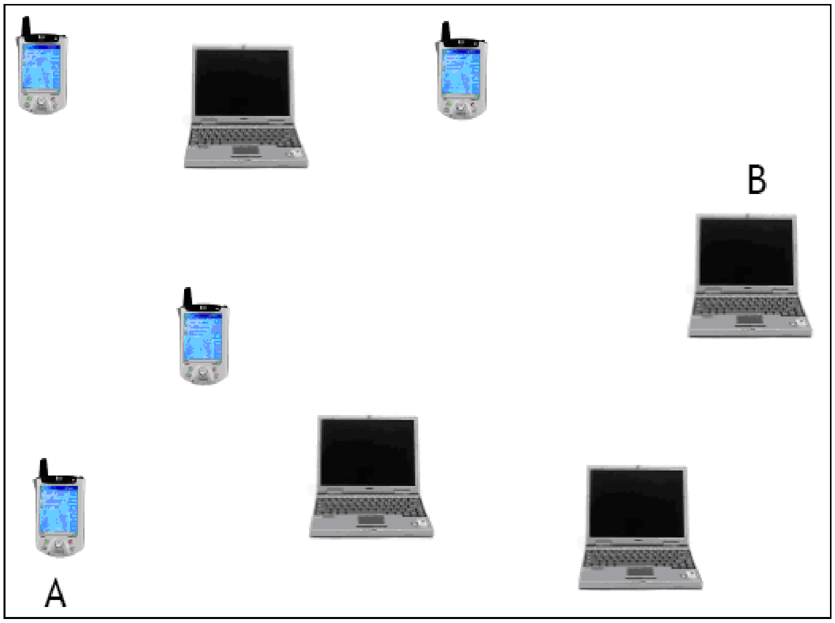


Figure 2.3: Reactive routing procedure [13]

Step2: To communicate with B, A must flood the routes towards B, as in Figure 2.4.

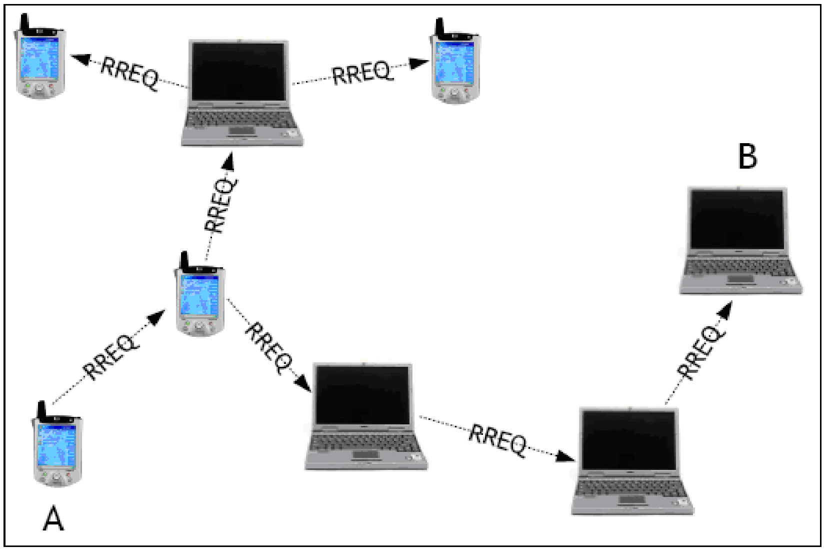


Figure 2.4: Reactive Routing Procedure[12]

Step3 : To let A and B communicate a unicast-ed feedback will be received, as in Figure 2.5.

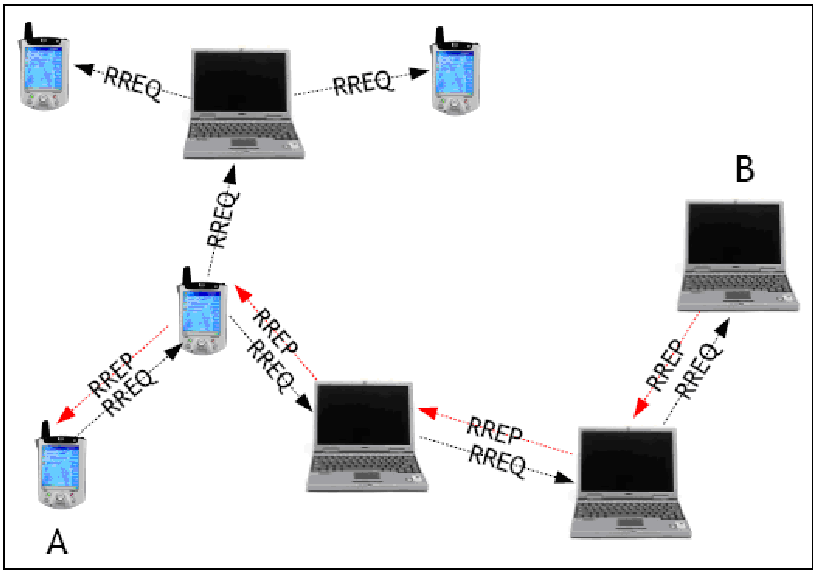


Figure 2.5: Reactive Routing Procedure[12]

2.2.2 The Proactive Routing Protocols

The mechanism of proactive routing protocols is completely different from the reactive routing protocols since it depend on the continuous traffic control. All routing information is maintained at all times since the network is dynamic. Two things should be kept in mind: firstly, because of the network drawbacks due to the continuous control traffic mechanism there is a lot of overhead on the network. Secondly, the route will be available all the time to maximize communication between the devices.There is a three steps algorithm in this protocol:

Link and Neighbor Sensing: In this sensor mechanism neighbors and links develop a relationship between each other by sending Hello packets to each other causing a connection between the devices [14]. In mobile Ad hoc networks all nodes or devices send Hello packets among each other,and thus relationships between links and neighbors are created. Figure2.6 shows the basic scenarios between neighbors.

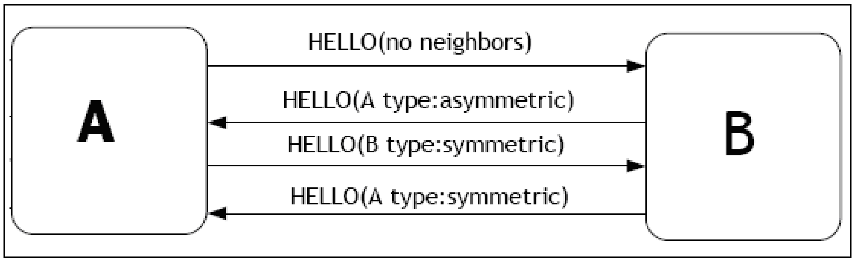


Figure 2.6: Link and Neighbor Sensing Mechanism

- Neighbor / link sensing
- Multipoint Relaying
- Link - state messaging and route calculation

Multipoint Relaying: Whenever the devices send Hello packets to each other or every node sends broadcast Hello packet to every node except itself [15], a lot of duplicate packets will be created.To overcome such duplicationa multipoint relaying process is used to reduce the number of duplicate packets.In addition this mechanism will also restrict other nodes. Or devices when it is required to send the broadcast packet to know connectivity between neighbor and link.Every node in this network for this selection has been developed or maintain its own multiple relaying procedure to run the protocol. The basic rule if there are two neighbor nodes, is thatthere should be M and N existing nodes surrounding them, as in Fgure 2.7.

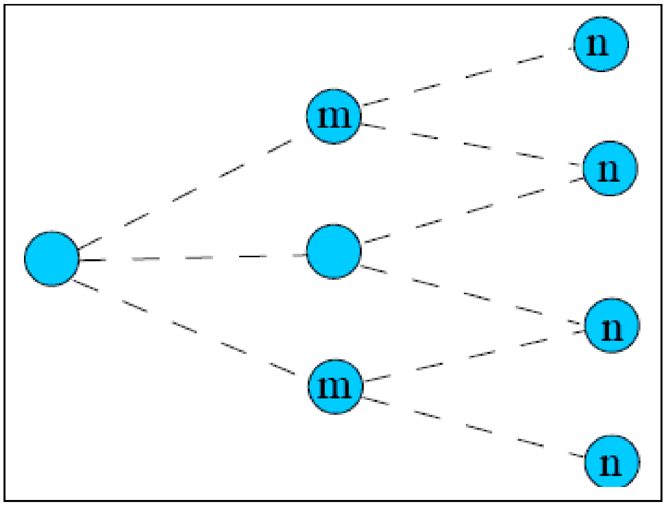


Figure 2.7: Multipoint Relay Selection Mechanism[12]

When sending traffic (step) all nodes from the network must be established.Or maintain every node these own multipoint relaying selectors. Whenever the proactive routing protocol is followed there is one basic rule for forwarding traffic:all the packet from the routing **(n)** is received by the multipoint relaying selector, then the packet is forwarded whenever its TTL value is greater than 0;the packet will reach its destination accordingly, as in Figure 2.8.

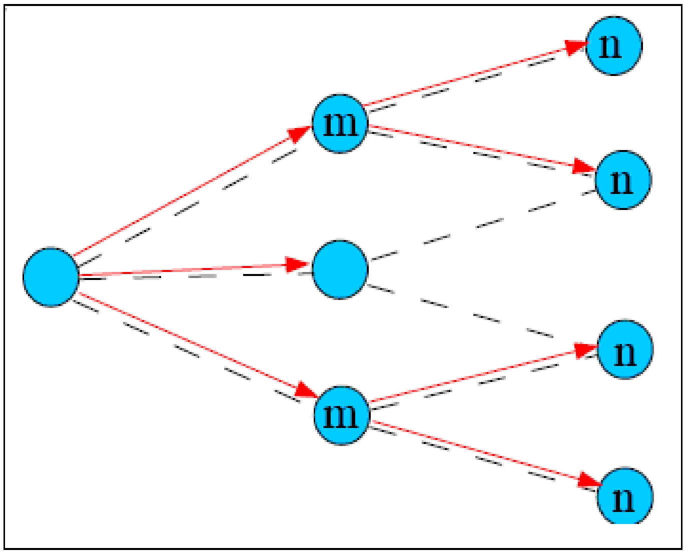


Figure 2.8: Forwarding of Traffic[12]

Link State Function: All devices in the network will flood out or broadcast link state information among devices, or a node is the main function of link state in order to keep nodes updated.

Multipoint relaying selectors used for forwarding routes will be better used for forwarding link state information.This is the reason explained why multipoint relaying selectors are used to send link messages making the decrease in size useful in link state messages.There will be a selection for multipoint relaying procedure before forwarding routes. So the nodes or devices are chosen as a multipoint relaying making them responsible for ending the link state message.The selected nodes in the link state procedure send link state messagesto the network called topology control message (TC). It can be used to develop a network since a relationship is developed between the nodes.The link state message and multipoint relaying example is shown in Figure2.14.

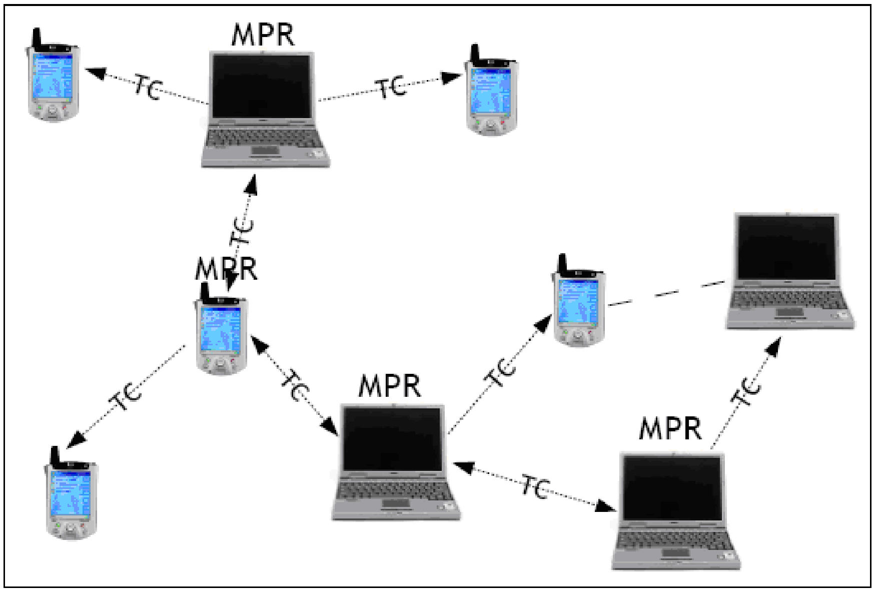


Figure 2.9: Link State Mechanism

2.3 The MANET Qualitative Properties

The MANET has the following properties [16] :

- Operation is distributed
- Freedom from loop
- Demand based operation
- Protective operation
- Security
- Sleep period operation
- Unidirectional link support

Distributed Operation: The advantage of this property is that it has distributed operation but despite of this fact it is working effectively in the network, and then there will be no overhead on the network.

Loop Freedom: It is very important in performance prospective to have loops free network because it is well known that when the network spread dynamically the nodes or devices can communicate with each other with no loop mechanism. This is to avoid redundancy in the network, and the mobile Ad hoc network can deal with this problem using the TTL mechanism value and bind the loops in oreder to avoid them in the network.

Demand Based Operation: Two types of operation in the network exist: fire is uniform based operation and the other oneis the demand based operation. In case of MANET the concern will be the second one only in order to control routing traffic in large networks. Also, demand based operation provides better resource utilization, improved efficiency and it can deal with delays in the network.

Proactive Operation: Due to the case when demand based operation scenarios are not effective, the proative operation is used. Whenever such a situation occurs the demand based operation is very useful and most effective for small rise networks.The protective shows the best results and more effective in the network.

Security: In the beginning of MANET there was no problem of security no user now has new technology and having different techniques to overcome network so security issues become necessary keeping in mind to control the network risk and reliability but the following problems in some security exist they are :

- Network traffic snooping
- Replay attacks
- Changing packets leader
- Routing redirection procedure

MANET has ability to control these security problems, therefore it provides appropriate security.

Sleep Period Operation: In wireless personal area network in MANET or devices there is a sleep mode for a certain time. Devices connected in master and slave concept with each other, so in order to proceed further there are a number of device connection limitation for energy conservation put are sleep period before connecting more devices. In order to overcome sleep period operation mechanism MANET increase their characteristics and functions in the wireless and mobile domain network.

Unidirectional Link Support: The bidirectional links in routing algorithm are established among the devices for proper function of the devices but MANET support unidirectional links in order to deal with broader networks. A situation of using both the unidirectional and bidirectional links may exist.

2.4 MANET Applications

MANET is gaining a lot of success in use and importance compared with other networks due to the need of massive communication . Different types of application in the field of industry are now in use. The advantages of MANET is that it does not need any new infrastructure for the implementation of any application since it works in different scenarios of wireless communication networks [16]. MANET has the ability to add or delete or remove devices or nodes from networks without any changes regarding the configuration of the networks. There are different MANET applications used in different fields of communications like large scale network infrastructure, mobile small networks and static infrastructure.Different types of MANET are used in fieldssuch as military battle field, commercial sectorand personal area network PAN.

Chapter 3

WIRELESS STANDARDS AND AODV ROUTING PROTOCOL

3.1 Wireless Standards IEEE 802.11

IEEE 802.11 technology is generally deployed for WLAN application. The IEEE 80.11 wireless LAN, also known as Wi-Fi[5], has been classified into several standards including 802.11a, 802.11b and 802.11g. The 802.11g and 802.11b are working in the 2.4 GHz Industrial Scientific Medical (ISM) band. The 802.11a is working in the 5GHz National information infrastructure band. All three wireless standards use the same media access protocol CSMA/CA. The three standards use link adaption strategy to improve the system throughput by adapting the transmission rate for longer distances. All three versions that have capability of operating in both ad hoc mode and infrastructure[26].

3.1.1 IEEE 802.11b and 802.11gStandards

This section begins with a discussion of the coexistence of wireless standards 802.11b and 802.11g in a WLAN. It will make a distinction between the challenges posted in hybrid 802.11b /802.11g mode. Making this important distinctionwill allow us to better identify and master the key concepts in throughput of 802.11g network. Since the 802.11b is very prevalent, the backward compatibility is known as one of the most important characteristics of these new standards. The 802.11g has higher data transmission than 802.11b and is comparable with 802.11a in its main characteristics.

The 802.11b devices implement two different specifications; the original, slow direct sequence (DSSS), from the initial 802.11 standard, and the high rate complementary code keying (CCK) PHY. Wireless standards 802.11g and 802.11b must be able to hear not only the older station but also the other 802.11g stations. In this thesis we used 802.11g and 802.11b and compared them[25].

3.2 Problems In Wireless LAN

Hidden Station Problem:

Let us take the four stations A,B,C,D as shown in Figure 3.2. The A and B stations are located within each other's radius range. Therefore there is a possibility of potential interference with one another. C can also potentially interfere with B and D, but not with A.*Overview to ad hoc on-demand Distance vector routing (AODV).*

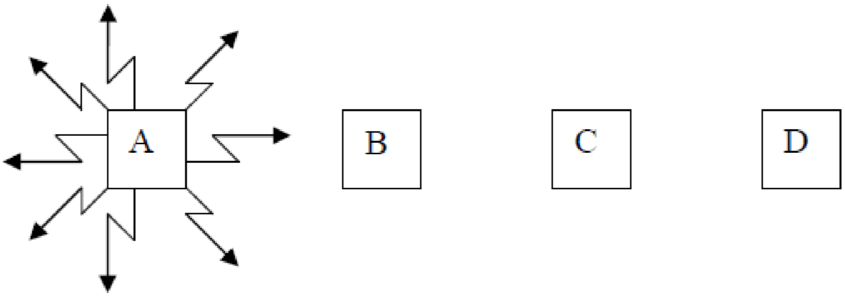


Figure 3.1: A Wireless LAN with station A transmitting (Hidden Station Problem)[22]

In Figure 3.1 a wireless LAN with station A is transmitting [Hidden S.P].Let us imagine what happens when A is transmitting to B as stated in Figure 3.1, if C senses the medium it will not hear A as A is out of range of C, hence to conclude that it can transmit is false. If C commenced transmitting, it will definitely interfere with B, wiping out the frame from A. Therefore the stations are not able to detect a potential competitor for the medium as the competitor distant away is named "Hidden Station problem".

Exposed Station Problem: Let us look at Figure 3.3. Consider B is transmitting to A. If C senses the medium,it will hear ongoing transmission and wrongly understand that it may not send to D, thus such a transmission ends in bad reception, but only in the zone between B &C irrespective of the location of the intended receivers. This situation is called "Exposed Station Problem"

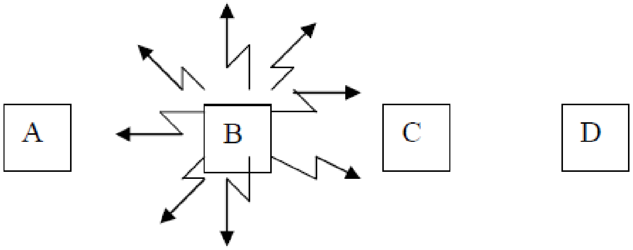


Figure 3.2: Wireless LAN with Station B Transmitting (Exposed Station Problem)[22]

Basic Access Method: CSMA/CA

CSMA/CA [Carrier Sense Multiple/Collision Avoidance] is the basic access mechanism used in WLAN, together with the distributed coordination function (DCF). To reduce the possibility of collisions caused by the hidden station problem [20], DCF uses RTS (Request to send) and CTS (Clear to Send) signals. The exposed station problem is avoided when a node is selected to wait at random back off time between two connective new packet transmission time.

3.3 Overview of Ad hocon Demand Distance Vector (AODV) Protocol

Ad hoc on-demand Distance vector Routing (AODV) is a novel algorithm for the operation of ad hoc networks. Routes are obtained when needed through each mobile node's operation as it acts as a specialized router,i.e. on request with very little or no dependence on periodic advertisement. The new routing algorithm is quite fit for dynamic self-starting network as demanded by users who like to utilize ad hoc networks. Loop free routes are provided by AODV even during repair of broken links,as the protocol does not need global periodic routing advertisement. The demand on the overall bandwidth available to the nodes is appreciably lower than in a protocol that requires such advertisement. AODV can be considered as a pure on-demand acquisition system, in that nodes do not locate on active paths neither participate in any periodic routing table exchanges or any routing information. Unless a node needs to communicate with another node it does not have to discover and maintain a route to another node. The concept of destination sequence numbering is used to maintain the most recent routing information between nodes. To supersede stale cached routes each Ad hoc node has to maintain its monotonically sequence number counter.

3.3.1 Basic Operation of AODV

Path Discovery: This section describes each individual process needed in an AODV [19] network to create, delete and maintain routes.

In case a source node needs to communicate with another and no routing information in its table exists, the path discovery starts to initiate. Every node maintains two separate counters which are a node sequence number and a broadcast number. The path discovery is initiated by a source node through broadcasting a route request [RREQ] including the following fields:

- Source sequence number
- Source address
- Broadcast ID
- Destination address
- Destination sequence number
- Hop count

The pair source address and Broadcast ID uniquely identifies a RREQ. When the source issues a new RREQ the Broadcast ID is incremented. Individual neighbor either to re-broadcast the RREQ to its own neighbor after increasing its the hop count, or satisfies the RREQ by sending a route reply [RREQ] back to the source. It is possible for a node to receive multiple copies of the same route broadcast packet from different neighbors. Re broadcasting is not possible when an immediate node receives a RREQ if it has already received a RREQ with the same broadcast ID and source address.

Reverse Path Setup : RREQ has two sequence numbers:the source sequence number and the destination sequence number. The source sequence number is needed to maintain freshness information about the reverse route to the source while the destination sequence number specifies how fresh a route to the destination should be prior to it being accepted by the source.Reference to be made to figure 3.4 When the source node S determines it needs a route to the destination node D and does not have the route available, RREQ [Route Request] broadcastsan immediate message to its neighboring nodes in quest of a route to the destination. Let us take node 1 and 4 being neighbors to the node S which receives a RREQ message, while nodes 1 and 4 create a reverse link to the source from which they received the RREQ. As nodes 1 and 4 are not aware of the link to the node D, consequently they rebroadcast this RREQ to their neighboring nodes 2 and 5. When RREQ moves from a source to different destinations, automatic reverse path is set up from all nodes back to the source as shown in Figure 3.3.This reverse route will be needed if the node receives a RREQ back to the node that originated the RREQ. Prior to broadcasting the RREQ, the originating node buffers the RREQ ID and the originator IP address. Thus reprocessing and re-forwarding of the packet is not made by the node when it receive it from its neighbors.

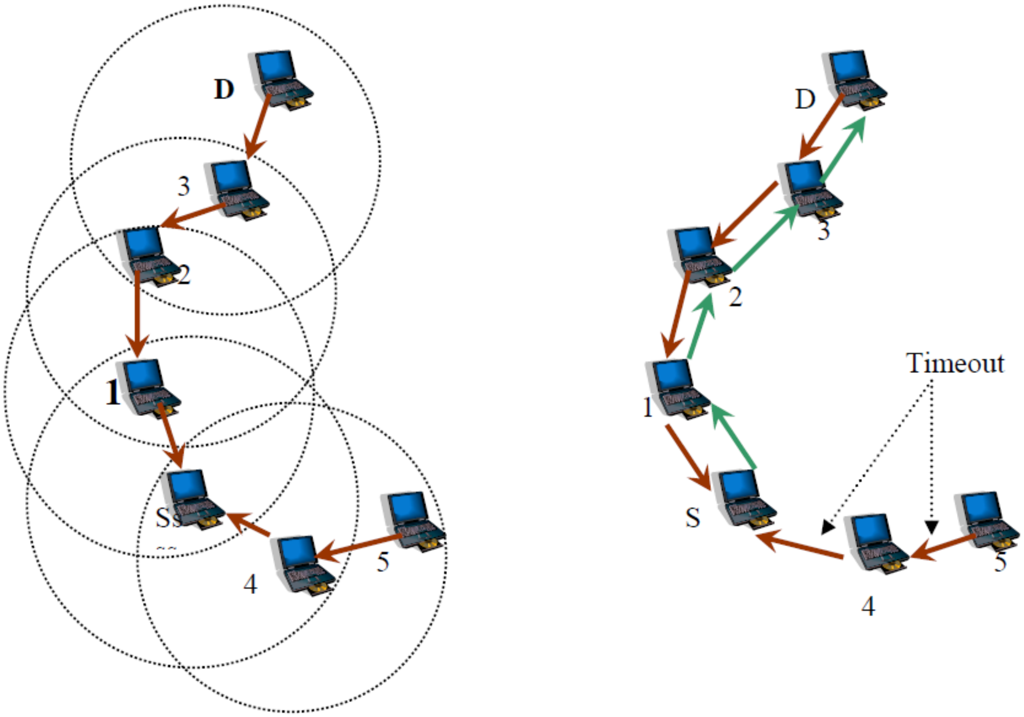


Figure 3.3: Reverse path setting[22] and forwardpath setting [22]

Forwarding path setup, finally a RREQ will reach a node that has a current route either towards the destination or to the destination itself. The receiving node will first check that the RREQ is received over a bidirectional link. If an intermediate node has a route entry for the desired destination, it determines whether the route is current by comparing the destination sequence number in its own route entry to the destination sequence number in the RREQ. If the RREQ sequence number for the destination is greater than recorded by the intermediate node, the intermediate node must not use its recorded route to respond to the RREQ. Instead the intermediate node broadcasts the RREQ. Therefore the intermediate replies only when it processes a route with a sequence number greater than, or equal to that included in the RREQ. If the RREQ has not been processed previously, while it had a current route to the destination, the node that unicast a route reply packet sends the RREQ back to the neighbor from which it received the RREQ.

A RREQ contains the following information

- Source address
- Destination address
- Destination sequence number
- Hop count
- Life time

A reverse path is established to the source of the RREQ when a broadcast packet arrives at a node that can supply a route to the destination. As the RREQ moves back to the source each node along the path set up a forward pointer from which the RREP came. For route entries to the source and destination it updates its timeout information and record the latest destination sequence number for the request destination.

Figure 3.1 expresses the forwarded path setup as the RREP moves through the nodes 3,2,1 from the destination D to the source node S. As node 4 and 5 are not along the path determined by the RREP, they will timeout after active route timeout, therefore they will delete the reverse pointers from the nodes.For a given source node towards the source RREP is first propagated by anode receiving a RREP. In case it receives another RREP it will update it routing information and propagates the RREP but only if the RREP contains either a greater destination sequence number than the previous RREP. or the same destination sequence number but with a smaller hop count.As soon as the first RREP is received, the node S can begin data transmission and finally can update its routing information provided it learns a better route.

3.3.2 Route Table Management

It is understood that the "route request expiration timer" is that which is associated with reverse path routing entries. The nodes that do not lie on the path from the source to the destination are erased by the timer. The expiration timer depends on the size of the ad hoc network. The "route caching timeout" is also another important parameter associated with routing entries, the time after which the route is considered invalid. Each routing table entry maintains the addresses of active neighbors through which packets for a given destination are received. Therefore such a neighbor is considered active for that destination,if it originates or relays at least one packet for that destination within the most recent "active time period". Through maintaining this information all active node can be notified when a link along a path to the destination breaks.If a route entry is in use by an active neighbor, it is considered active.

An Individual route table entry contains the following information .

- Destination
- Next hop
- Number of hops
- sequence number for destination
- Active neighbors for this route
- Expiration time for the route table

Whenever a route entry is used to transmit data from a source toward a destination, the timeout for the entry resets to the current time plus "active route timeout" if a mobile node is provided with a new route. The mobile node compares the destination sequence number with the current route one. The chosen route is that with the greater number. In case the source sequence number is the same, then the new route is selected only if it possesses a smaller metric to the destination.

3.3.3 Link Breakage

When link breakage takes place, the existing route in the routing table entry is definitely invalidated by the mobile node. The affected destination are listed by the node, further more it finds out which neighbors are affected by this breakage. Eventually the node has to send the route error [RERR] message to the corresponding neighbor. The RERR message can be broadcast provided there are many neighbors who need the information, or unicasted in case there is only one neighbor who needs it. If broadcast is no more possible,then the host can also iteratively unicast the message.

Path Maintenance: The routing to the path's destination is not affected by the movement of the node provided that the nodes are not lying along an active path. The movement of the source node during an active session can initiate the route discovery procedure resulting in a new route to the destination. When either the destination or some intermediate node moves,a special RREP to the affected source node is sent as a result of either destination or some intermediate node's movement. Aperiodic Hello message can be used to insure symmetric links, as well as the detection of link failures. Consequently, and with far less effort latency could be detected by using link-layer acknowledgment [LLACKS]. If attempts to forward a packet to the next hop failed ,this is an indication of link failure. If it happened that the next hop is unreachable, the node upstream of the break propagates an unsolicited RREP together with a fresh sequence number and hop count of infinite to all upstream active neighbors. Consequently those nodes relay the message to their active neighbors, and so on. This type of process goes on until all active source nodes are notified. When notification of a broken link is received and the source node stills require a route to the destination,they can start the discovery process for that purpose. To find out a whether route is still needed, a node may check whether the route has been recently used,as well as inspect if the upper level protocol is blocked or to see whether connections are open using the indicated destination. To rebuild the route to the destination, the source node has to decide to send out an RREQ with a destination sequence number of one greater than the previously known destination sequence number. This is to make sure that anew route is built and no nodes reply while the previous route is valid[22].

3.3.4 Local Connectivity Management

Besides the fact that AODV is a reactive protocol, it uses Hello message periodically to notify its neighbors that the link to the host isalive. Messages are not forwarded further because Hello messages are broadcasted with a TTL equal to 1. However, upon the host receiving the Hello message it will start updating the lifetime of the host information in the routing table. In case the host does not obtain information from the host 's neighbors about " allowed Hello loss","hello intervals" the amount of time as a result of the routing information in the routing table is marked as lost. This action initiates the RRER to send a message to notify other hosts of link breakage. Benefit can be had from the local connectivity management with Hello messages, using it to make sure that only nodes with bidirectional connectivity are regarded as neighbors. Therefore each Hello sent by a node lists the nodes from which it has heard. Each node through certain checking ensures that it is using only routes to the neighbors that have heard Hello message. To save local bandwidth checking is needed.Such checking should only be done if explicitly configured in to the nodes.

Local Repair: The host can try to repair the broken link provided so that the destination is no more than the specified amount of hops. If link repair is decided, the host increases the destination sequence number and broadcast the RREQ message to the host. The TTL for the IP leader must be calculated to avoid local repair process spread through backing the network. The host waits for the RREP message to its RREQ message for specialized amount of time. Let say that the RREP message is not received.Then the system will convert the routing table status for the entry to invalid. The hop count metric is compared when the host receives the RREP message. The RREP with the N field setup is broadcast if the hop metric from the message is greater than the previous one. When the host locally repairs the link, it will be indicated by N field in the RRER message, thus the entry in the table should not be deleted.

Chapter 4

TCP and HTTP

4.1 Transmission Control Protocol

Transmission control protocol (TCP) represents the transport layer of the OSI reference model. Data transmission is the responsibility of the transport layer. Moreover the transport layer performs the flow control, error control and division of chunks of application data into segments appropriate to the layer below. TCP utilizes a virtual connection, in other words a logical connection is established prior to transmitting data. Application of TCP cover HTTP,FTP, streaming media and E-mail. Requests for lost packet are moved by data transmission. In the mean while re arranging the out of order packets and minimizing the network congestion,as a result TCP becomes more efficient in a current packet delivery and sometimes end with long delays usually in second using request for lost packet[22] .

4.2 Web Traffic (HTTP)

Hyper Text Transfer Protocol plays a major role in communication of web browsers with web servers ensuring secure communication through avoiding eavesdroppers and counterfeits. Exchange information does not configure HTTP standards. It really has the capability of storing and exchanging all kinds of information. A set of rules for creation of web pages is provided by Hyper text makeup language (HTML). HTTP is skilled in transferring remote printing instructions, multimedia objects and program files,......,etc.

Moreover, HTTP is responsible for establishing a base foundation for all network based computing with extensive use of Web browsers due to the omnipresence of internet and its flexibility[17] .

HTTP is considered an application protocol that lies in the application layer. Reference to be made to Figure 4.1 shows the layers involved in a communication.

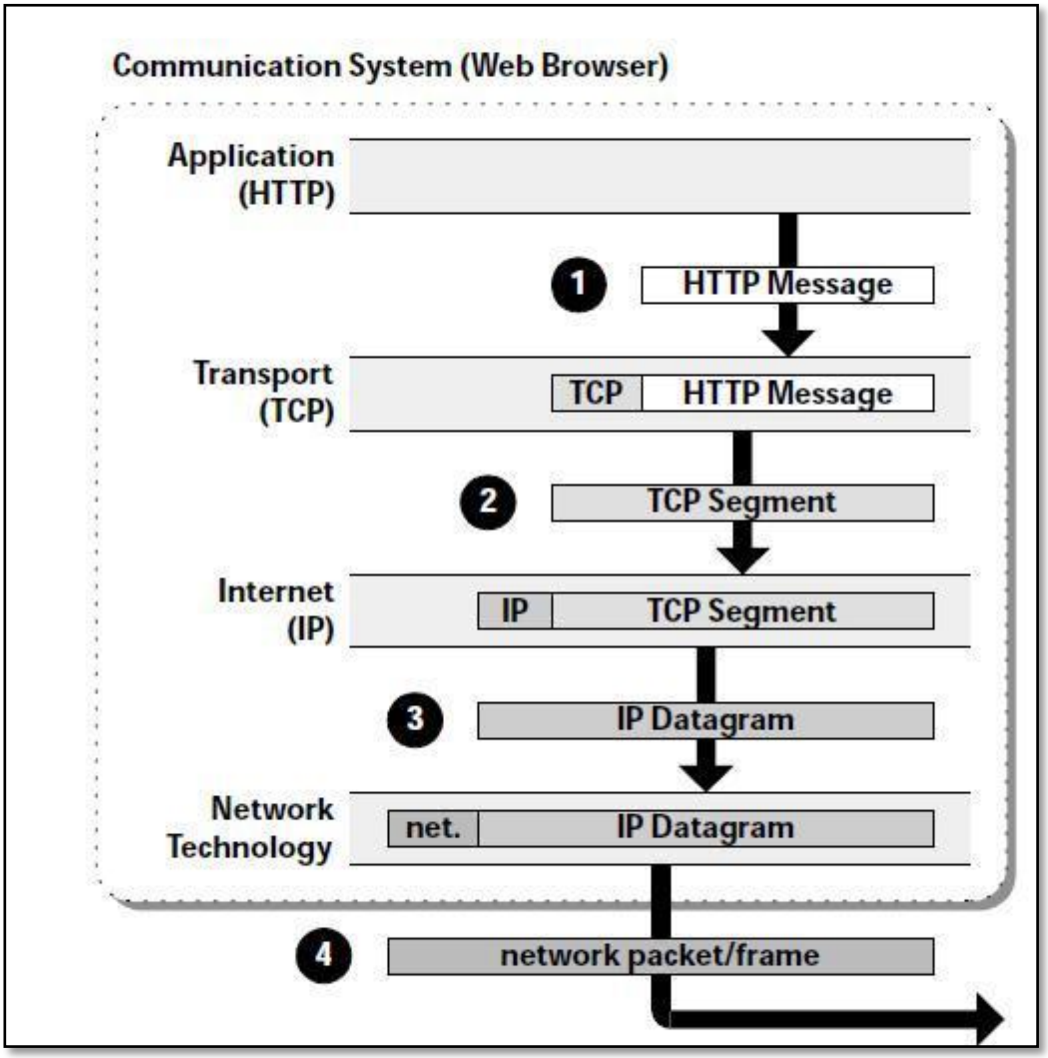


Figure 4.1: Four protocol layer used in HTTP exchange by Web Browser[18]

HTTP follows the process in figure 4.1 for communicating data and it is a two system communication. Figure 4.1 shows the first communication system which is the Web Browser, while the second communication system is the web server which is shown in Figure 4.2. Let us imagine the application layer if a HTTP needs to transmit a message.It will pass it to the lower layer protocols Transport protocol (TCP), Internet protocol (IP) and network technology consecutively as shown in Figure 4.1, until it departs from the system. The message is constructed by HTTP for transmission and then it will pass over to TCP.The message is processed by certain information resulting in the creation of the TCP segment. A TCP segment functions as an envelope making sure that the mail is transmiting and finally the TCP segment is forwarded to the IP layer. Here, IP is adding up to the current TCP segment. This process creates another envelope which is called the IP datagram. This IP datagram will be transferred for the purpose of the protocol implementation controlling the system technology. Some additional information is added and finally the message leaves the system in the shape of packets/ frames, then this HTTP message will arrive at the application layer of web server. In summary, the message coming from the lower layer passing over the protocol stalk and finally reaching the application layer where all the concerned respective information in the HTTP is removed in respective protocol layers. Then the network packet will be transferred as IP datagram and then to TCP segments. Finally,the HTTP message reaches at the destination HTTP application layer.

Reference to be made to Figure 4.2 where pictorial representation of web server communication system is illustrated [18].

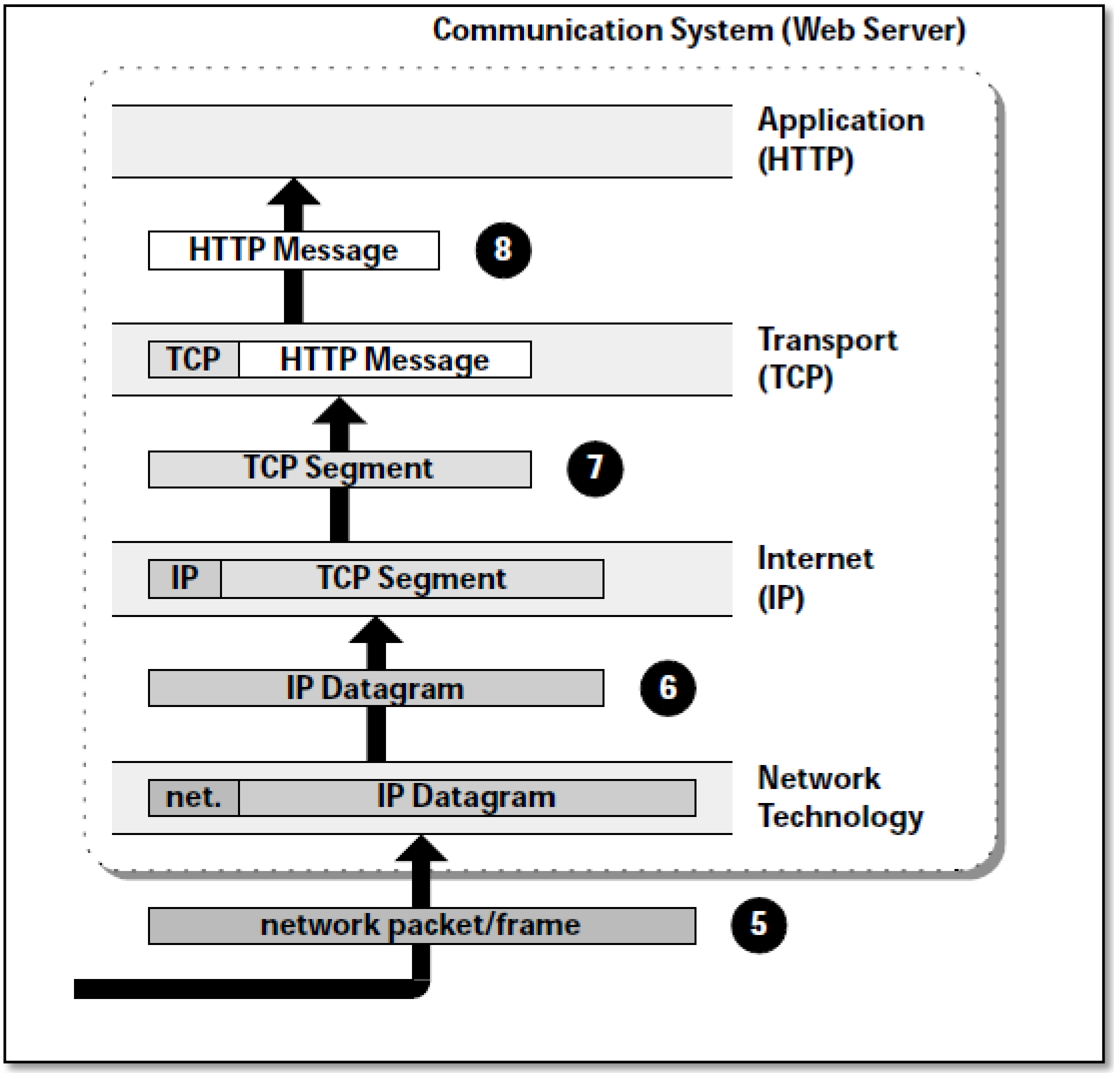


Figure 4.2:Four Protocol Layer Used in HTTP Exchange By Web Server [18]

Chapter 5

OPNET SIMULATOR AND SIMULATION STEPS

5.1 Simulation Design and Implementation

An efficient network design is of great significance in this world through its important role,it is considered an essential part for checking the performance of the designed network, and is regarded as a difficult task in a real time application. The most reputed network simulators so far designed are OPNET [Optimized Network Engineering Tool]. OPNET Modeler is not an open source product. OPNET needs license to access, it provides a GUI and comprisesa predefined model, protocols and algorithms. It is supported by very much documentation, in particular when used for commercial purposes.

OPNET Modeler Features :

- Shows flexibility and easy graphical interface to observe the results.
- Easy access to evaluation of designs of new network model and architecture.
- The network behavior is easily understood in various scenarios.
- The network model and design are already defined and available for users education and development purposes.
- Helpful for performance study of existing systems based on user condition.
- OPNET provides a virtual real time environment with GUI.
- OPNET is reliable and efficient.

5.2 Model Design of OPNET

The working of OPNET comprises FOUR parts:Model design, applying statistics, run the simulation and the viewing of obtained results and its analysis. In case the results are not correct or satisfactory, remodeling has to be done and the statistics adapted. The flow chart below represents the basic working of OPNET[23].

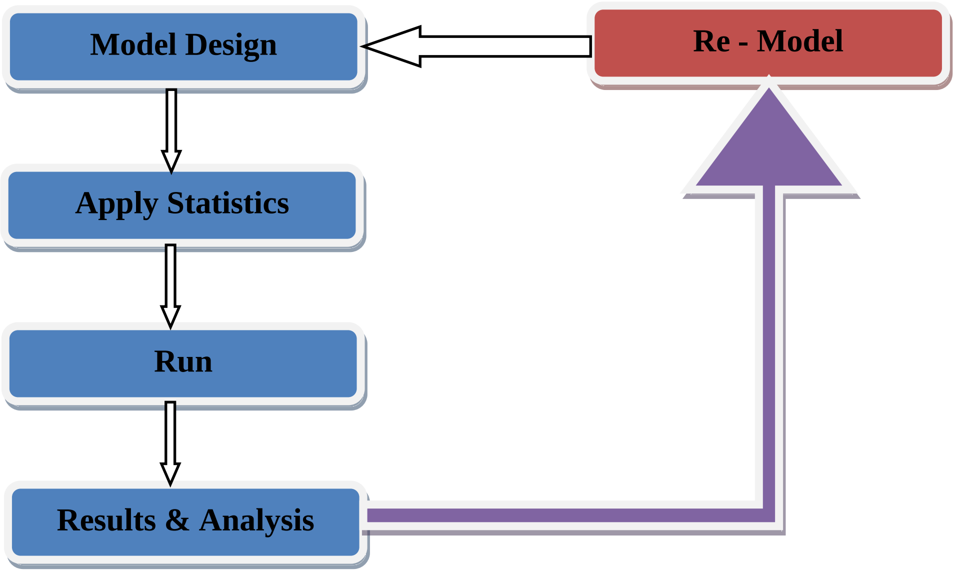


Figure 5.1. Work flow of OPNET[23]

To initiate the model design, we have to run OPNET modeler, a blank scenario is created, and soon the workspace will be seen but only after the startup wizard. Within the work space our network will be designed by using the required network entities. The network entities are: application configuration, profile configuration, mobility configuration, server and nodes. Their entities from the object palette to our project workspace. The example of network model designed over work space can be seen in Figure 5.2[24] .

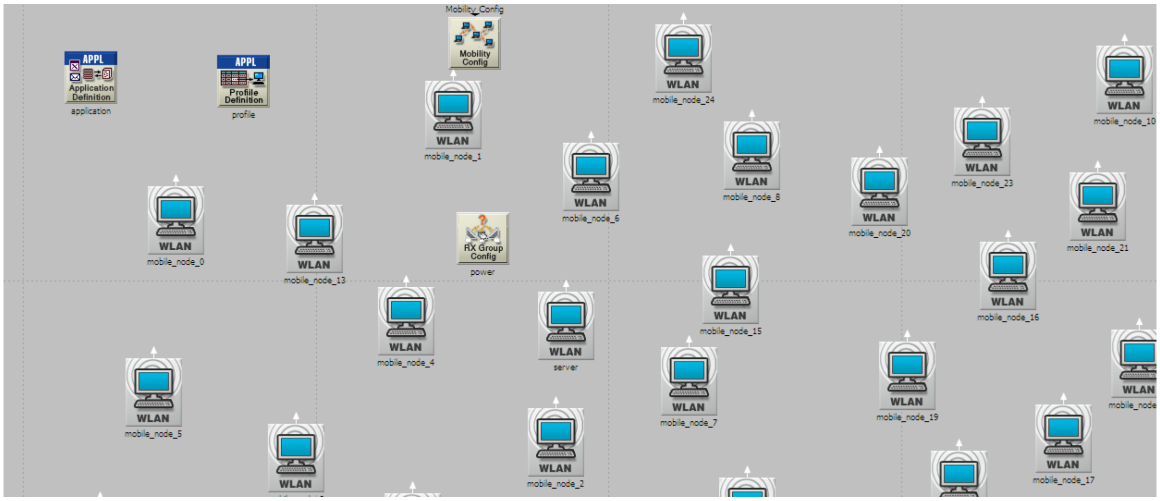


Figure 5.2: An example of network model design.

Application Configuration

The application configuration is used to specify/select required application, This is already a reliable application among a number of applications such as FTP, HTTP, E-MAIL, DATA BASE , ...etc. As the selection is optional we can nominate our choice and give the suitable description in creating a new application. For the purpose of this thesis we are depending on HTTP performance heavy browsing .

Profile Configuration

Profile configuration will be used to create user profiles.These profiles can be specified by different nodes in a network designed to make the application traffic. As configuring profiles, applications defined in the application configuration are used. In this thesis we have created two profiles HTTP Heavy browses based on the applications we have chosen in application configuration.With this profile we can restrict the nodes to an assigned profile based on user design requirement[23].

Mobility Configuration :

To specify the mobility model of the nodes in the network mobility configuration is used. The mobility configuration provides parameters to control the movement of the node speed , start time, stop time,.... ,etc. For the purpose of this thesis we have speed 1 M/Swhich is based on simulation scenario requirement.

5.3 Steps of Simulation Setup

This part of the thesis specifies the simulation steps by using OPNET modeler version 17.1, as well as specifying how to configure HTTP application, profile configuration, Mobility configuration and node configuration. The structure of this simulation consists of 25 nodes,one application node and one profile node in addition to RX Group node . We comparedthe physical characteristics with different data rate and we have many cases in nodes that contain :

- One server and 24 Clients
- One server, 12 Clients , 12 Intermediates
- One server, 1 Clients , 23 Intermediates
- In above we compare three cases together useing physical characteristics that use different data rates
- 802.11g (11Mbps - 24Mbps - 54Mbps)
- 802.11b (11Mbps)

Table 5.1: Simulation Setup Table

General parameter	Value
Simulator	OPNET 17.1
Area	1000m x1000m
Network Size	25 nodes
Mobility Model	Random way point
Traffic type	HTTP (heavy browsing)
Physical characteristics	802.11g and 802.11b
Data Rates	11Mb - 24Mb - 54Mb
Simulation Time	300 Sec
Address mode	IPv4
Routing protocol	AODV

In the following steps all the setting are described in detail:

To start with, open OPNET modeler and create a new project there are some procedure :

Step1:Go to start menu and click on the visual studio 2008, as shown in Figure 5.3.

Step2:Copy the path from the unit directory, as shown in Figure 5.4.

Step3:After opening visual studio write the directive "CD", paste the unit directory path, as shown in Figure 5.5.

Step4: After Enter it write the "modeler".

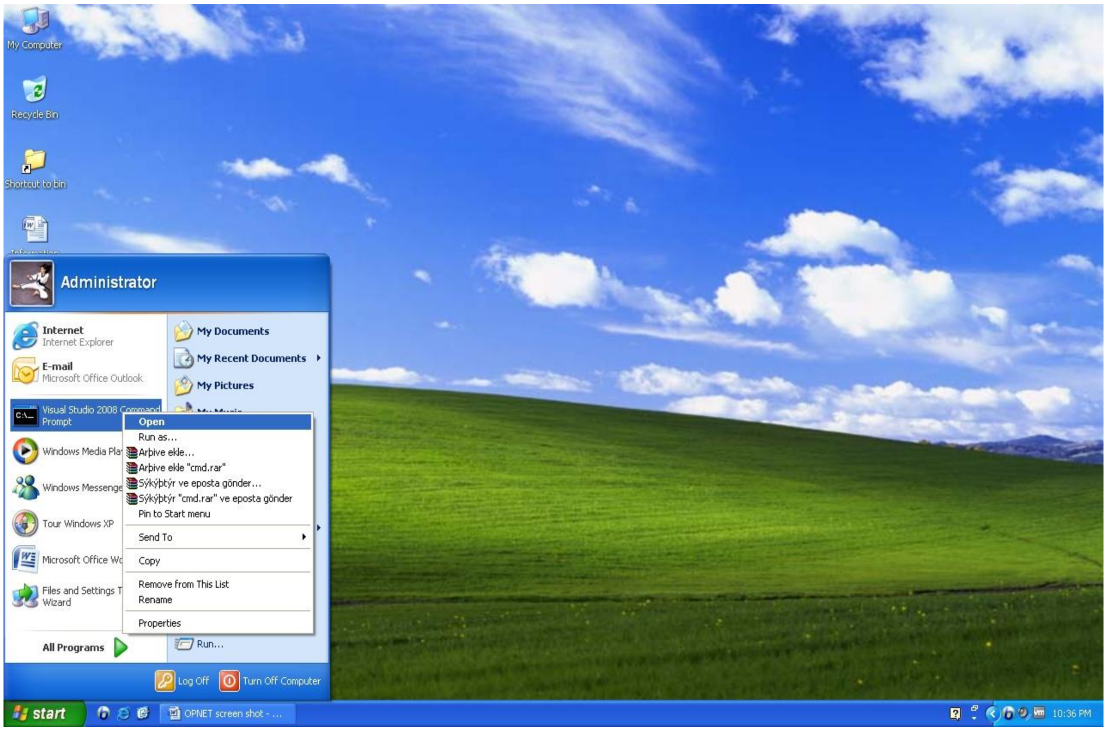


Figure 5.3: VMware Workstation

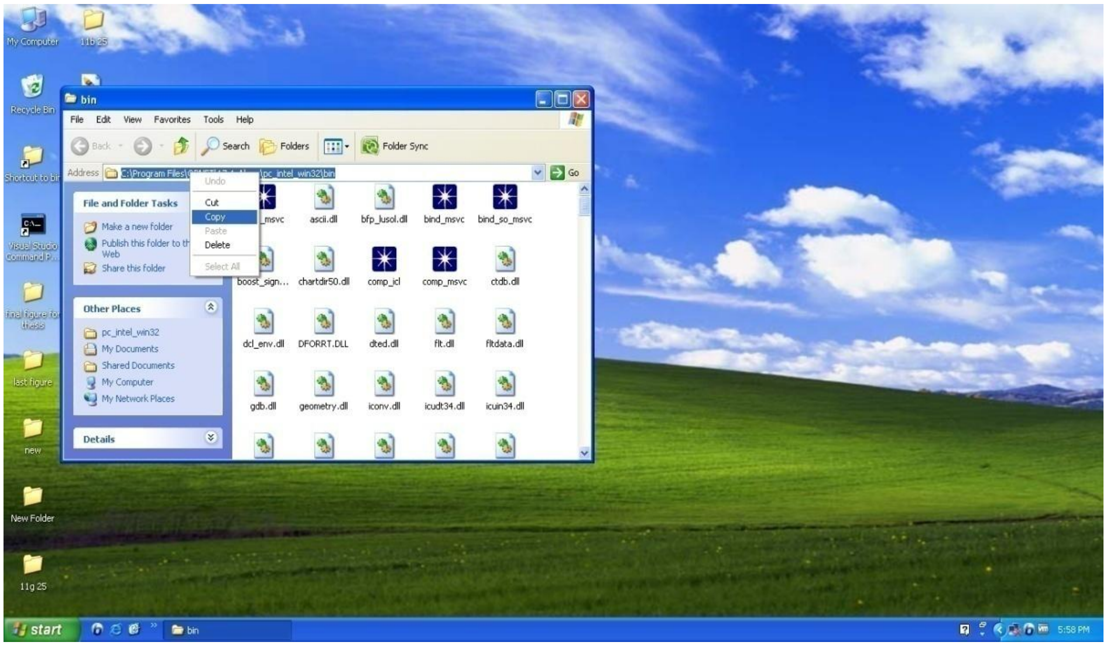
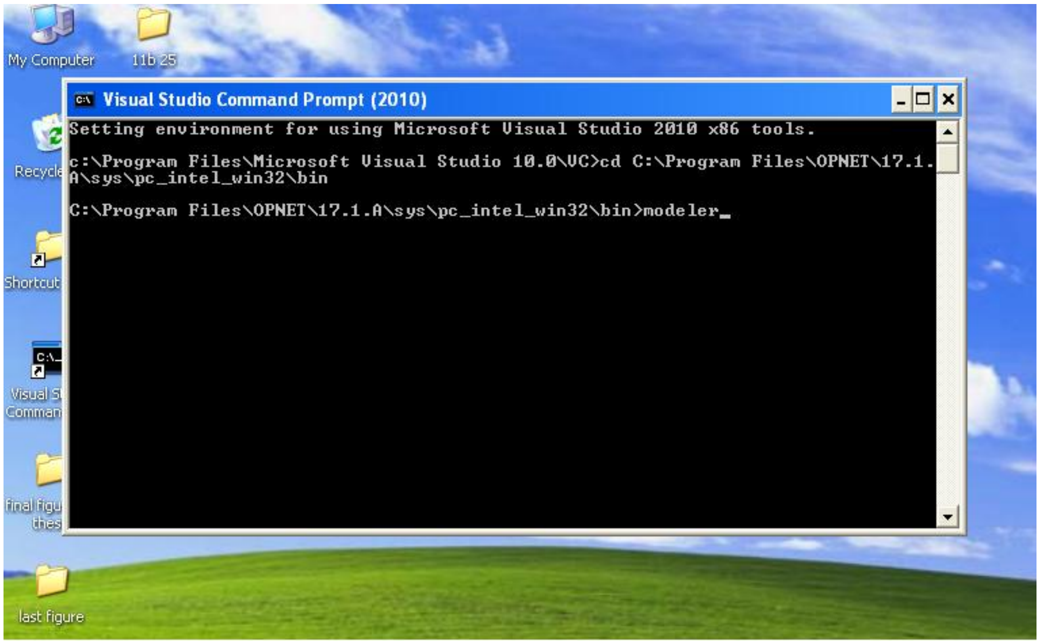


Figure 5.4: Copy OPNET path



```
Setting environment for using Microsoft Visual Studio 2010 x86 tools.

c:\Program Files\Microsoft Visual Studio 10.0\VC>cd C:\Program Files\OPNET\17.1.
A\sys\pc_intel_win32\bin

C:\Program Files\OPNET\17.1.A\sys\pc_intel_win32\bin>modeler_
```

Figure 5.5: Visual Studio

Step 5:This figure shows OPNET modeler version 17.1.

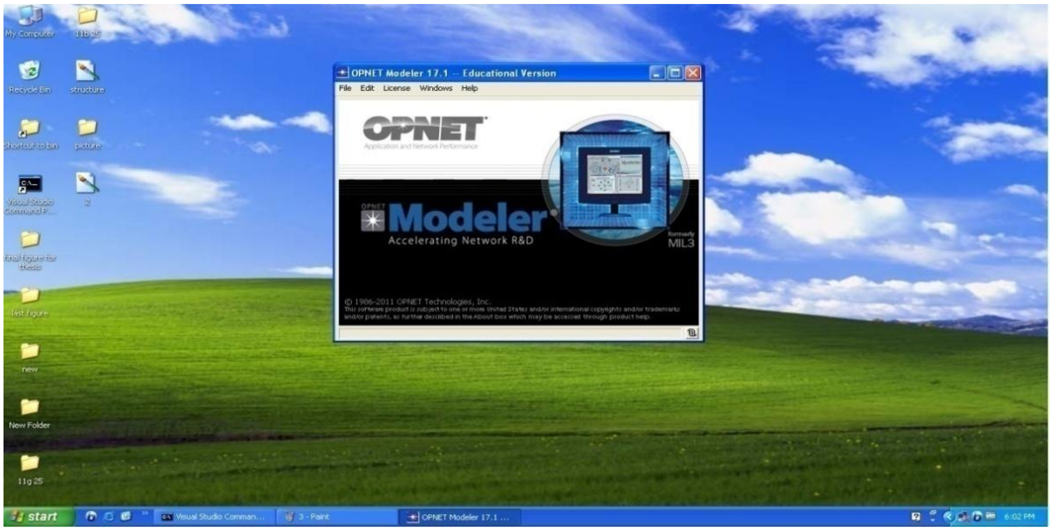
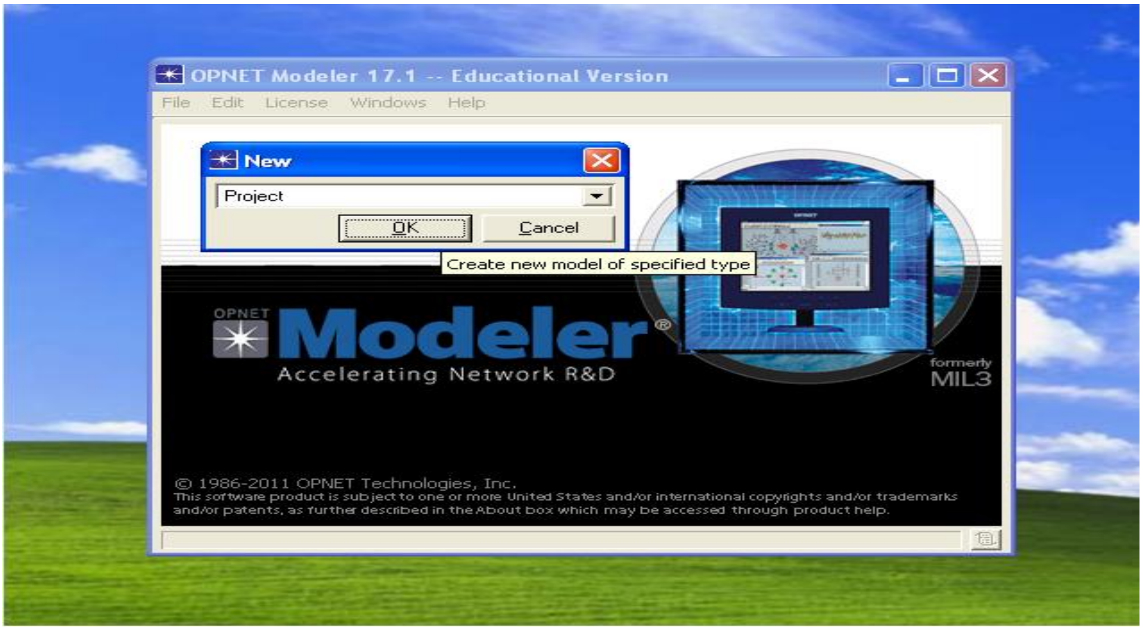

OPNET Modeler 17.1 -- Educational Version
File
Edit
License
Windows
Help
OPNET
Application and Network Performance
OPNET
Modeler
Accelerating Network R&D
formerly
MIL3
© 1986-2011 OPNET Technologies, Inc.
This software product is subject to one or more United States and/or international copyrights and/or trademarks and/or patents, as further described in the About box which may be accessed through product help.
My Computer
11b 25
Recycle Bin
structure
picture
New Folder
start
Visual Studio Comman...
OPNET Modeler 17.1 ...
6:02 PM

Figure 5.6:OPNET Modeler

Step 6:To create a new project: click on the file and select new from the file list, as shown in Figure 5.7.



Project

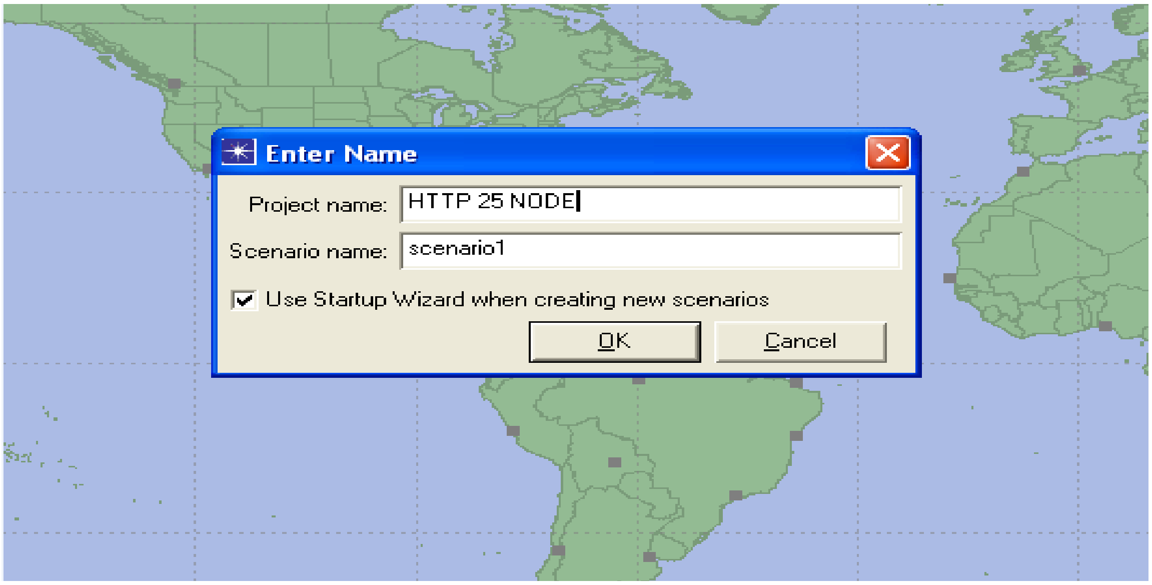
Create new model of specified type

Accelerating Network R&D

© 1986-2011 OPNET Technologies, Inc.
This software product is subject to one or more United States and/or international copyrights and/or trademarks and/or patents, as further described in the About box which may be accessed through product help.

Figure 5.7: Create New Project

Step7:This procedure can be used to write the name of the procedure and the name of a scenario as in Figure 5.8.



Project name: HTTP 25 NODE

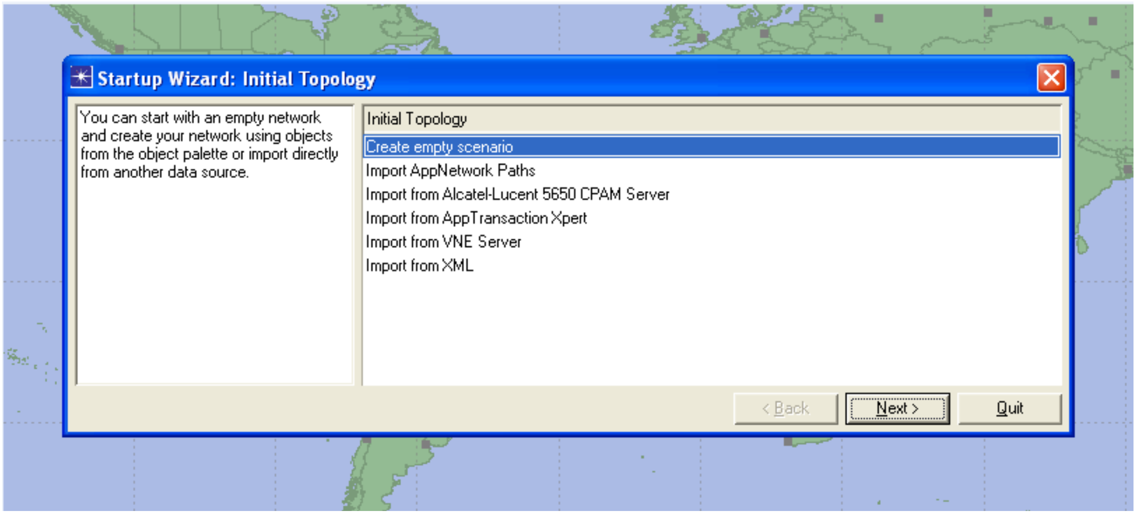
Scenario name: scenario1

☑ Use Startup Wizard when creating new scenarios

Figure 5.8: Enter the Name of Project

Step8: To create new scenarios :

- In the startup wizard: Select (create empty scenario) from the initial Topology as shown in Figure 5.9.
- Click on the "Next".

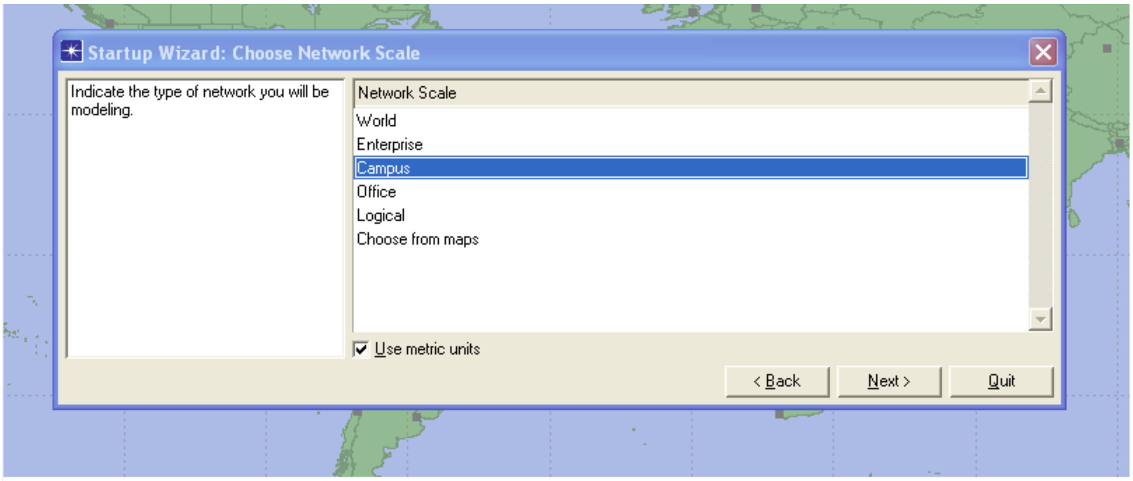

Startup Wizard: Initial Topology

You can start with an empty network and create your network using objects from the object palette or import directly from another data source.

Initial Topology: Create empty scenario

Figure 5.9: Initial Topology : Startup Wizard

Step9: Choose Network scale: Select the (Campus) from the Network scale list that contains many choices and after that click next, as shown in Fgure 5.10.


Startup Wizard: Choose Network Scale

Indicate the type of network you will be modeling.

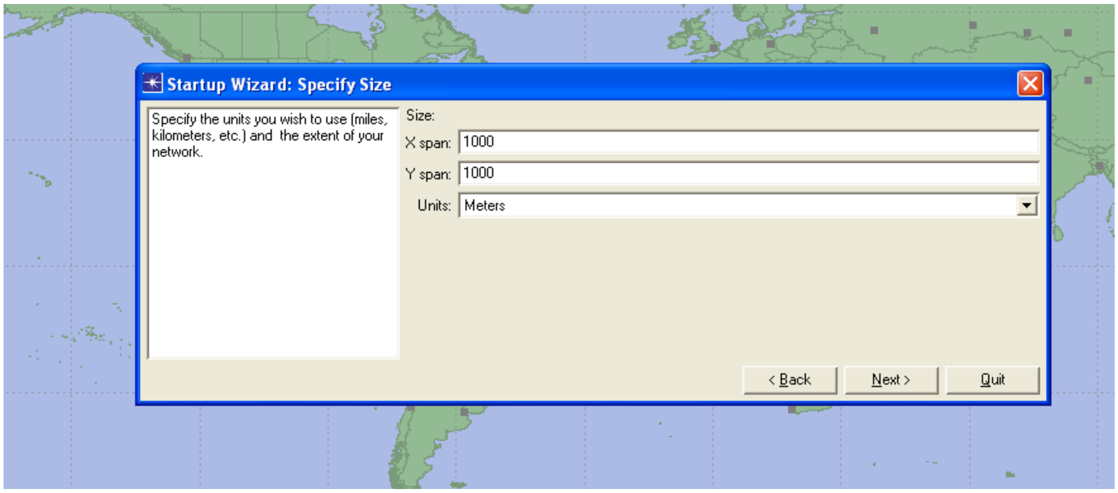
Network Scale: Campus

☑ Use metric units

Figure 5.10: Choose Network Scale

Step10: specify the size, as shown in Figure 5.11 :

- We have two fields, X-span and Y-span that select the area of our simulation.
- In Unit field: we select the (meters).



Startup Wizard: Specify Size

Specify the units you wish to use (miles, kilometers, etc.) and the extent of your network.

Size:

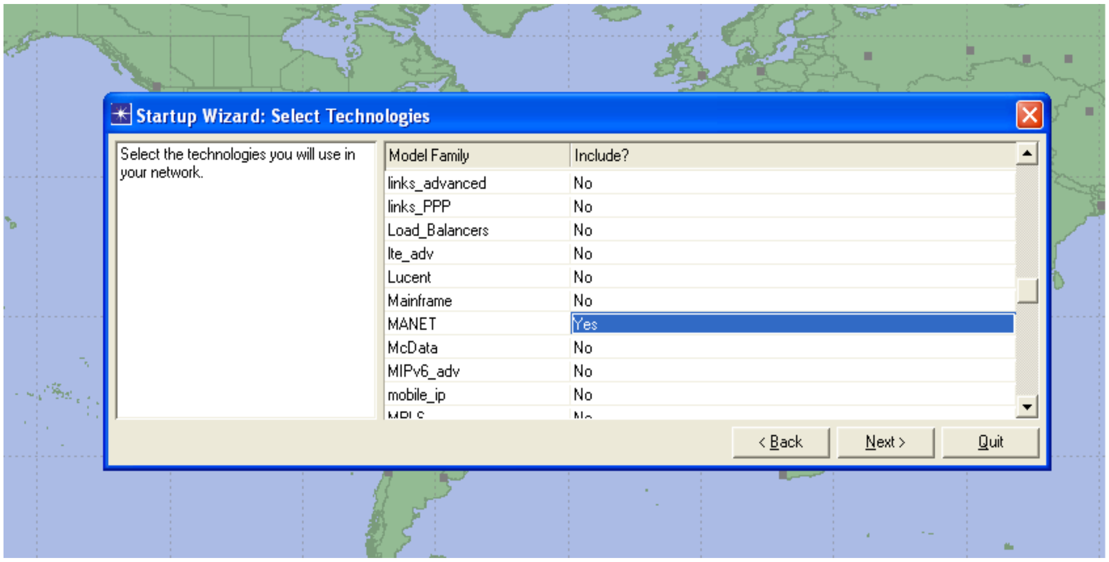
X span: 1000

Y span: 1000

Units: Meters

Figure 5.11: Startup Wizard: Specify Size

Step11:To select the Technology for this simulation click on the (MANET) because in this simulation I use Ad hoc wireless Network and click Next, as shown in Figure 5.12 .



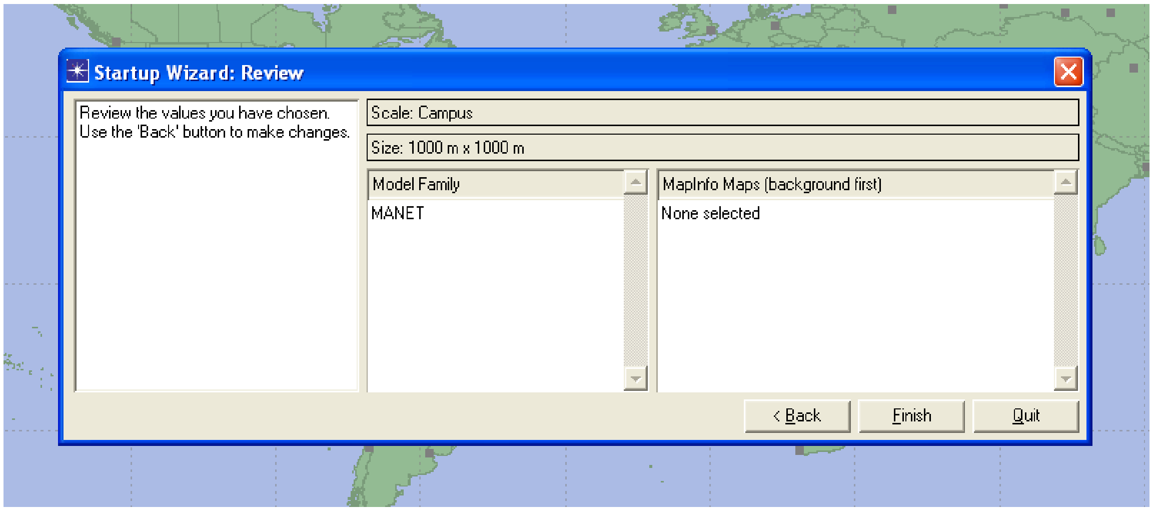
Startup Wizard: Select Technologies

Select the technologies you will use in your network.

Model Family	Include?
links_advanced	No
links_PPP	No
Load_Balancers	No
lte_adv	No
Lucent	No
Mainframe	No
MANET	Yes
McData	No
MIPv6_adv	No
mobile_ip	No

Figure 5.12: Startup Wizard: Select Technologies

Step12:After selecting the technology click (Finish) so that network simulation is built, as shown in Figure 5.13.



Review the values you have chosen.
Use the 'Back' button to make changes.

Scale: Campus

Size: 1000 m x 1000 m

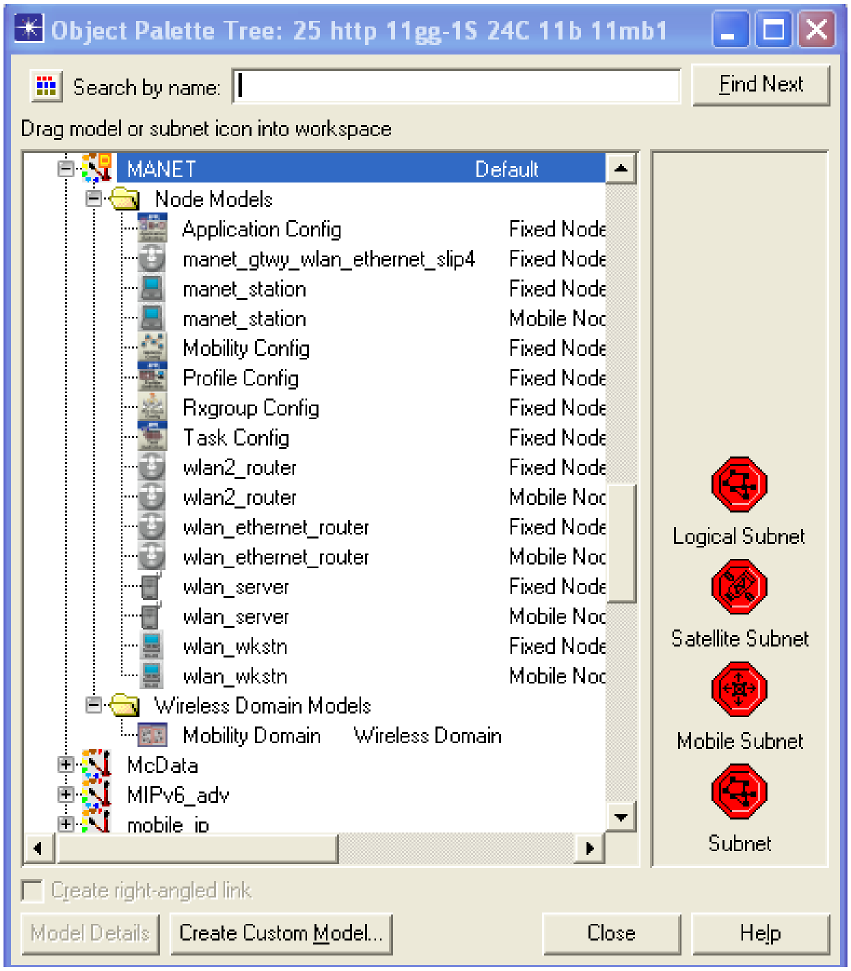
Model Family
MANET

MapInfo Maps (background first)
None selected

Figure 5.13: Startup Wizard: Review

Step13: To create the structure of simulation as shown in Figure 5.14 :

- Open the (Object palette tree) that contains Node model related to the simulation as shown in Figure 5.14.
- Select Application Node and put it in the network area.
- Select Profile Node and put it in the network area.
- Select WLAN_WKSTN(Mobile Node) and put it in the network area.



Drag model or subnet icon into workspace

MANET	Default
Node Models	
Application Config	Fixed Node
manet_gtwy_wlan_ethernet_slip4	Fixed Node
manet_station	Fixed Node
manet_station	Mobile Noc
Mobility Config	Fixed Node
Profile Config	Fixed Node
Rxgroup Config	Fixed Node
Task Config	Fixed Node
wlan2_router	Fixed Node
wlan2_router	Mobile Noc
wlan_ethernet_router	Fixed Node
wlan_ethernet_router	Mobile Noc
wlan_server	Fixed Node
wlan_server	Mobile Noc
wlan_wkstn	Fixed Node
wlan_wkstn	Mobile Noc
Wireless Domain Models	
Mobility Domain	Wireless Domain
McData	
MIPv6_adv	
mobile_ip	

Figure 5.14: Object Palette Tree

As shown in Figure5.18 in our simulation we have 25 WLAN_WKSTN(Mobile node) and application node, profile node, and the mobile node in addition to Rx group node.

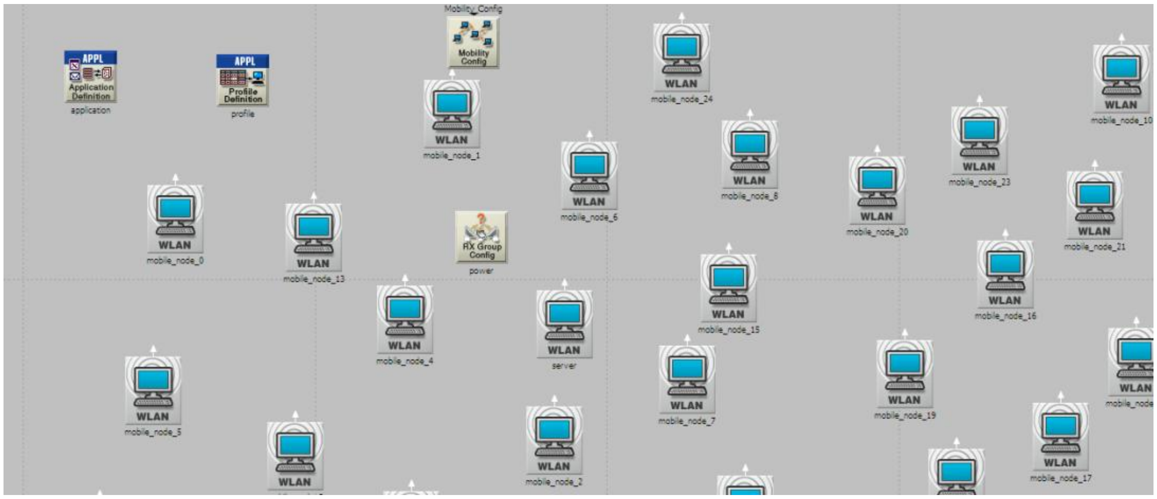
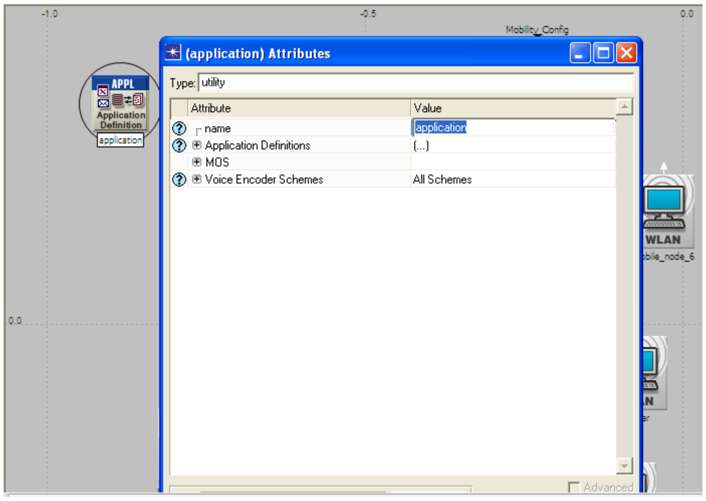


Figure 5.15: Simulation Structure

Step14: After selecting all nodes right click on application node and change the name of the application in the value field as shown in Figure 5.16 .



(application) Attributes

Type: utility

Attribute	Value
name	application
⊞ Application Definitions	(...)
⊞ MOS	
⊞ Voice Encoder Schemes	All Schemes

Figure 5.16: Application List

Step15: By mouse right click on node_15 select (select similar nodes) from the list to select all nodes as shown in Figure 5.17 and 5.18.

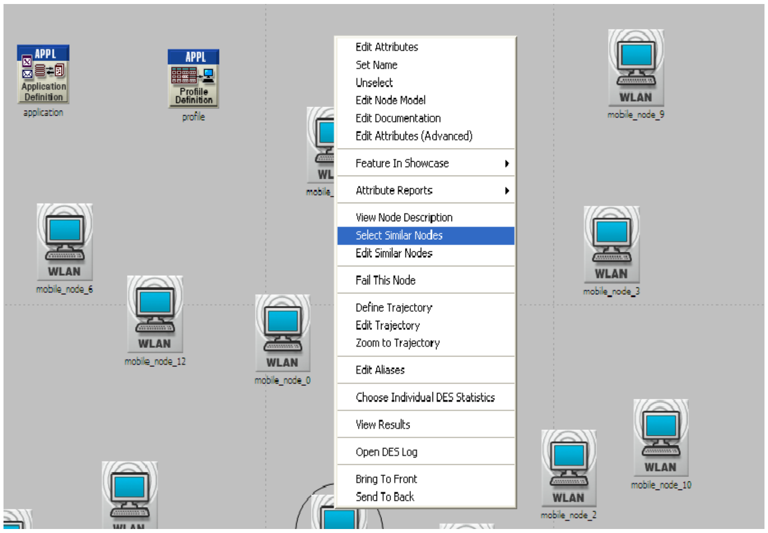


Figure 5.17:Select Similar Nodes

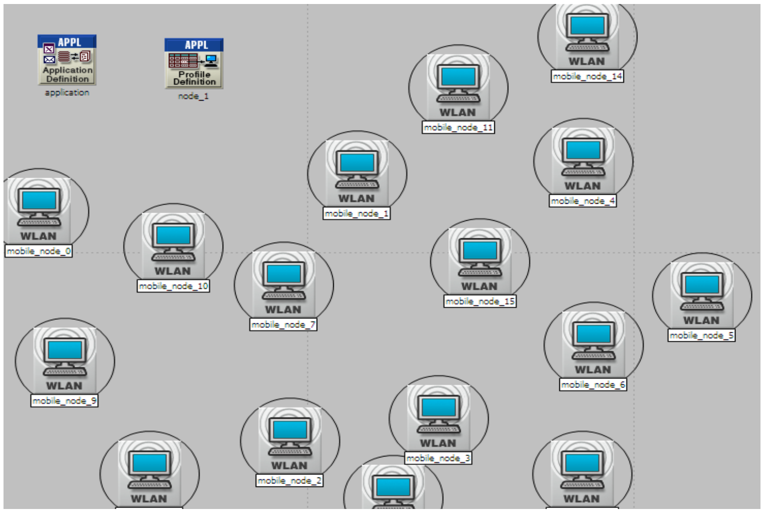


Figure 5.18: All nodes selected

Step16**:** Select Topology from pull down menu, after that select Random Mobility,then set mobility profile, as shown in Figure 5.19.

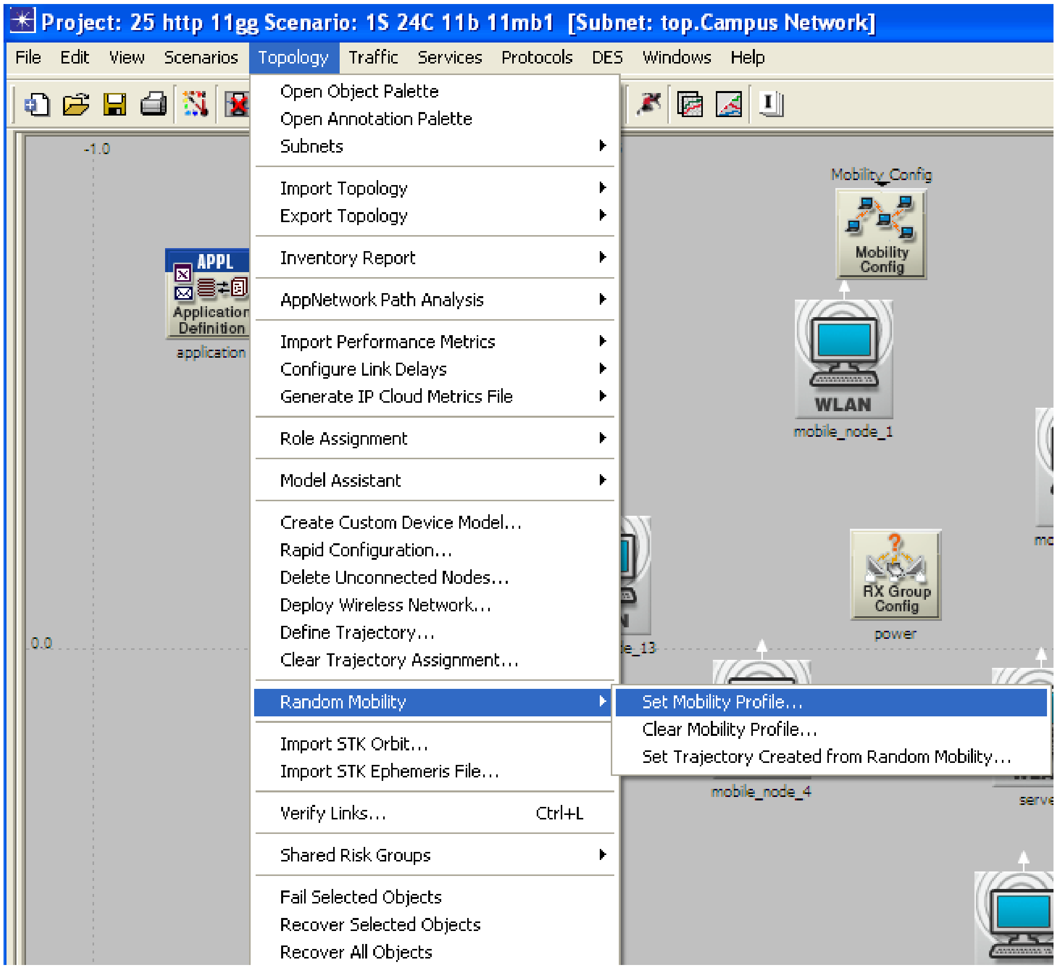


Figure 5.19: Random Mobility

Step17**:** Right click on any WLAN_WKSTN node and select (similar node) from the list so that all WLAN_WKSTN nodes are selected as shown in Figure 5.20 .

Step18:Select protocol from the main menu and select IP, Addressing then Auto-Assign IPv4. Address this procedure performs that all nodes have IPv4 as show in Figure 5.21 .

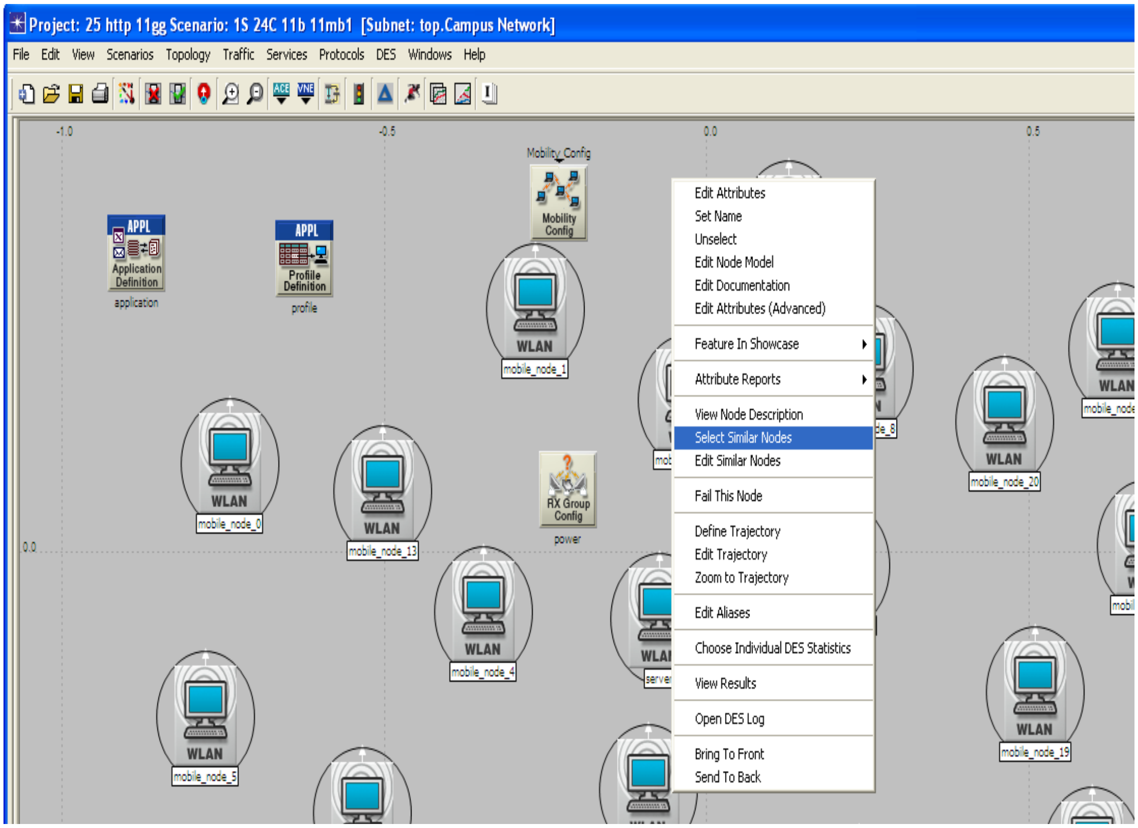


Figure 5.20: Select Similar Nodes.

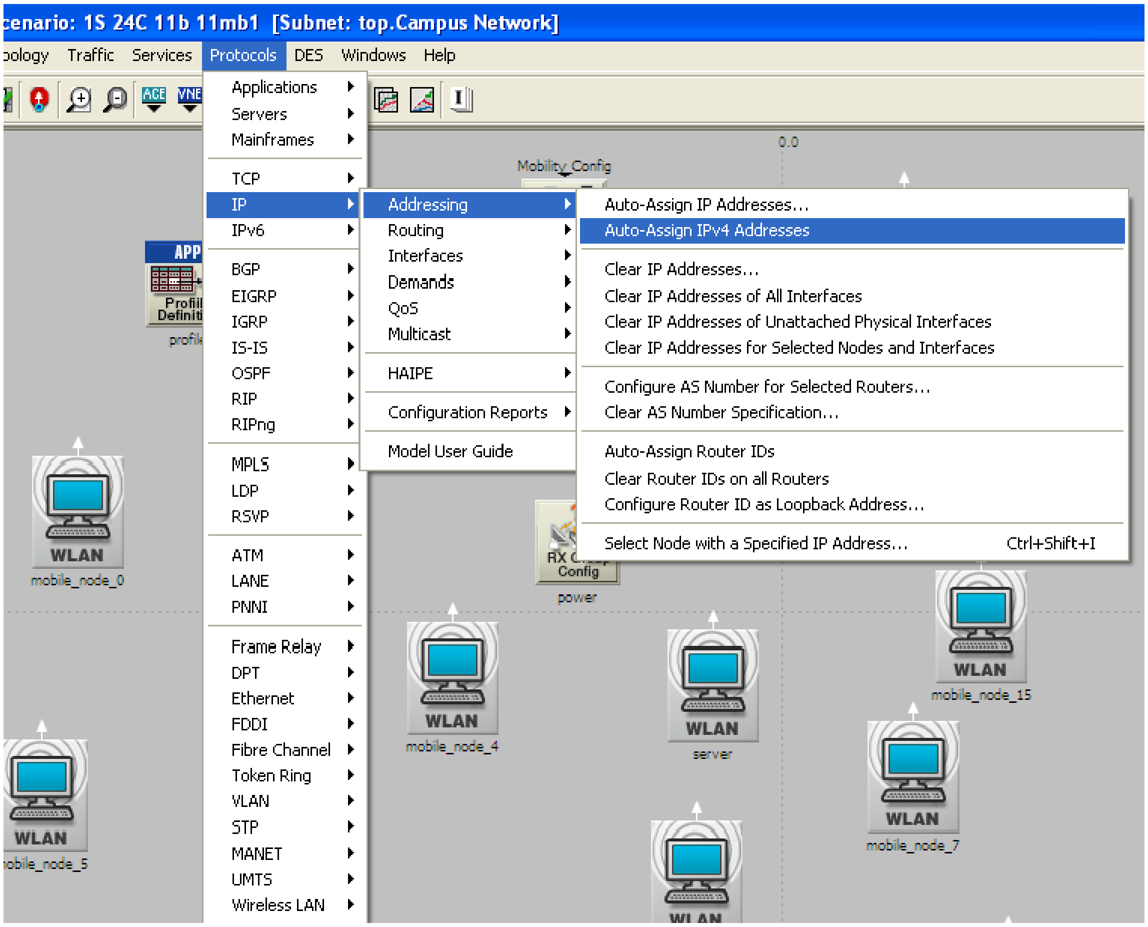

cenario: 1S 24C 11b 11mb1 [Subnet: top.Campus Network]
pology Traffic Services Protocols DES Windows Help
Applications
Servers
Mainframes
TCP
IP
IPv6
BGP
EIGRP
IGRP
IS-IS
OSPF
RIP
RIPng
MPLS
LDP
RSVP
ATM
LANE
PNNI
Frame Relay
DPT
Ethernet
FDDI
Fibre Channel
Token Ring
VLAN
STP
MANET
UMTS
Wireless LAN
Addressing
Routing
Interfaces
Demands
QoS
Multicast
HAIPE
Configuration Reports
Model User Guide
Auto-Assign IP Addresses...
Auto-Assign IPv4 Addresses
Clear IP Addresses...
Clear IP Addresses of All Interfaces
Clear IP Addresses of Unattached Physical Interfaces
Clear IP Addresses for Selected Nodes and Interfaces
Configure AS Number for Selected Routers...
Clear AS Number Specification...
Auto-Assign Router IDs
Clear Router IDs on all Routers
Configure Router ID as Loopback Address...
Select Node with a Specified IP Address... Ctrl+Shift+I
Mobility Config
0.0
APP
Profil Definiti
profile
RX Config
power
WLAN
mobile_node_0
mobile_node_4
server
mobile_node_15
mobile_node_7
obile_node_5

Figure 5.21: Auto Assign IPv4 address

Step19:Select all nodes by right click on any WLAN_WKSTN node and choose select similar nodes as shown in Figure 5.20.

Step20:Right click on any WLAN_WKSTN node and choose (Edit attribute) from the list as shown in Figure 5.22.

Step21:Choose (AODV) from ad hoc routing protocol after ad hoc Routing parameter was selected as shown in Figure 5.23.

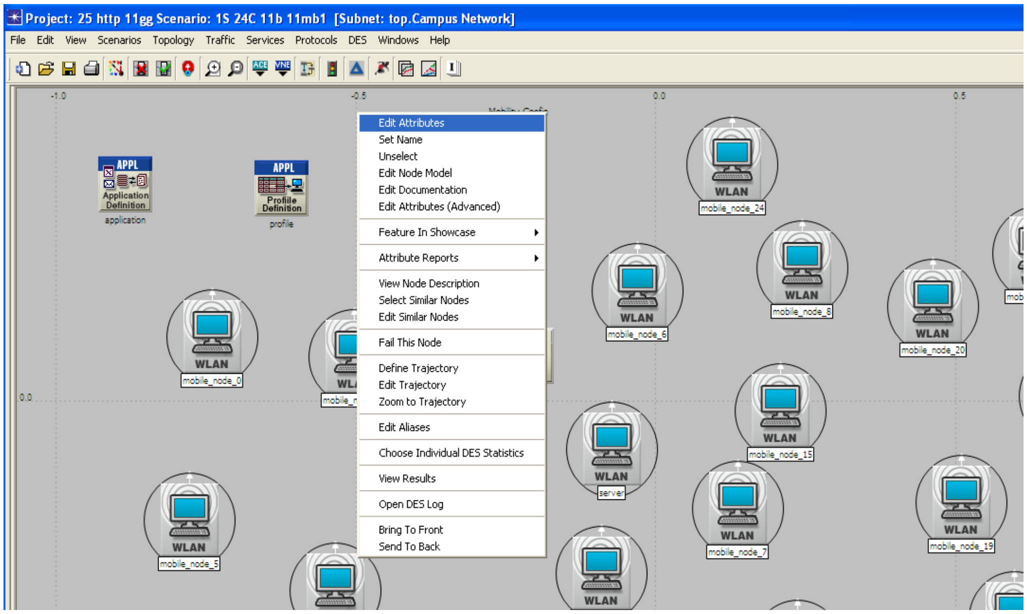
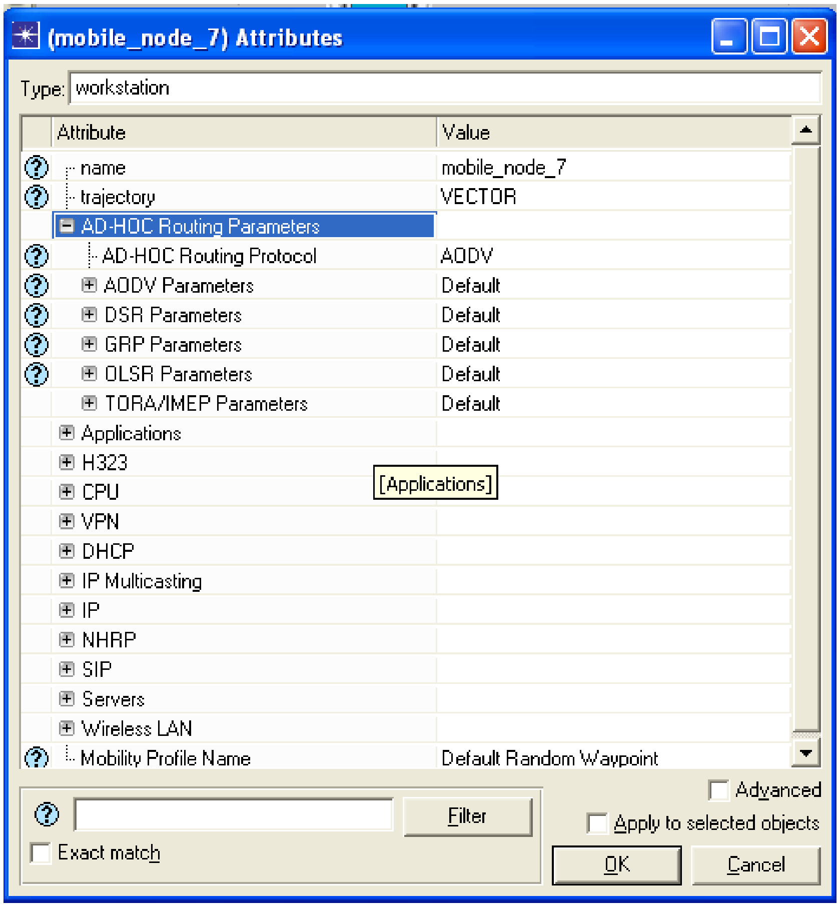


Figure 5.22: Edit Attributes



Type: workstation

Attribute	Value
name	mobile_node_7
trajectory	VECTOR
⊟ AD-HOC Routing Parameters	
AD-HOC Routing Protocol	AODV
⊞ AODV Parameters	Default
⊞ DSR Parameters	Default
⊞ GRP Parameters	Default
⊞ OLSR Parameters	Default
⊞ TORA/IMEP Parameters	Default
⊞ Applications	
⊞ H323	
⊞ CPU	
⊞ VPN	
⊞ DHCP	
⊞ IP Multicasting	
⊞ IP	
⊞ NHRP	
⊞ SIP	
⊞ Servers	
⊞ Wireless LAN	
Mobility Profile Name	Default Random Waypoint

Figure 5.23: Mobile Node : Choose AODV.

Step22. Application Configuration:

The steps of application configuration are :

- Right click on application node and select edit attributes, as shown in Figure 5.24
- Change the name of Attribute to Application as show in Figure 5.25
- Select Application definition and let the number of Row to one (We have one application HTTP)
- To specify the number of application select Enter application name and select 1 as shown in Figure 5.26
- Change the name of application to HTTP
- Click on Description procedure and select HTTP
- Choose Heavy browsing,then click on HTTP options as shown in Figure 5.27
- In page interarrival time change the distribution name to (constant) and mean outcomes to 1 as shown in Figure 5.28 by double click on heavy browsing

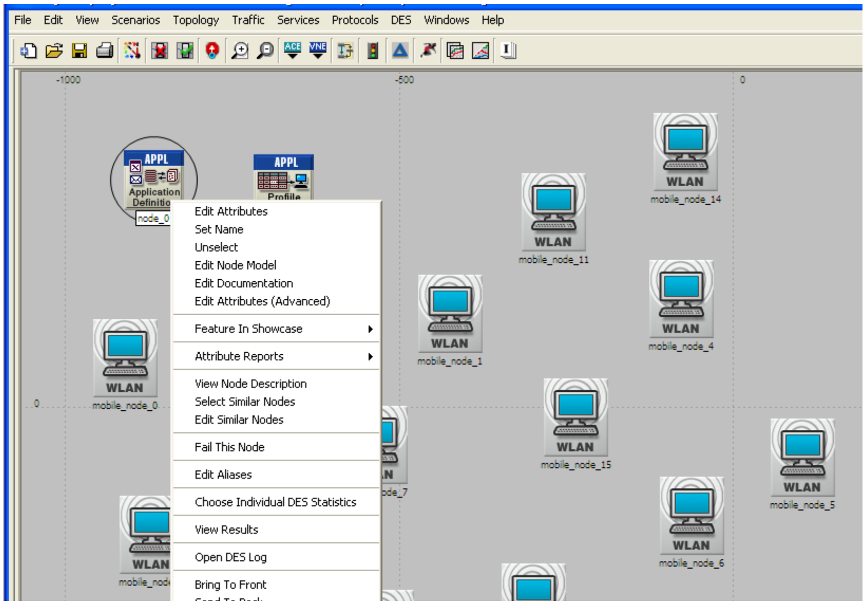
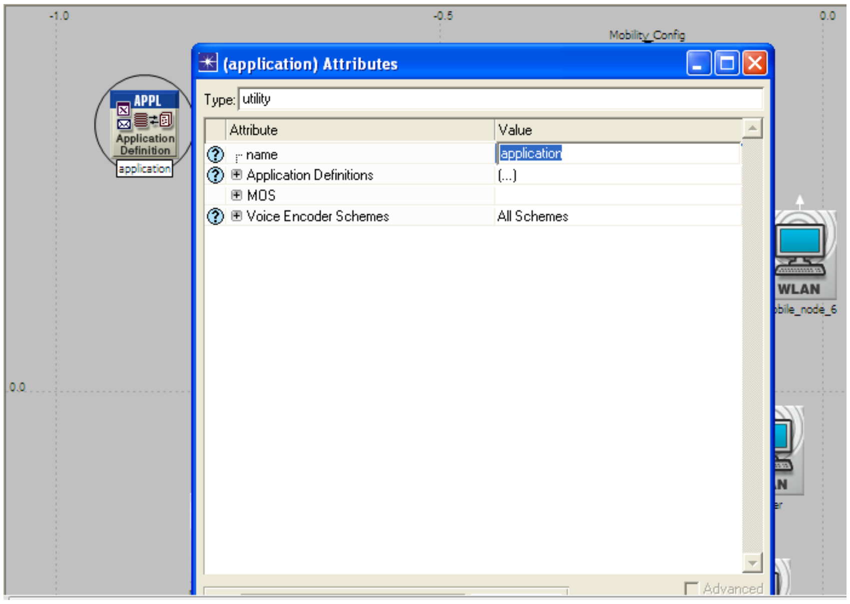


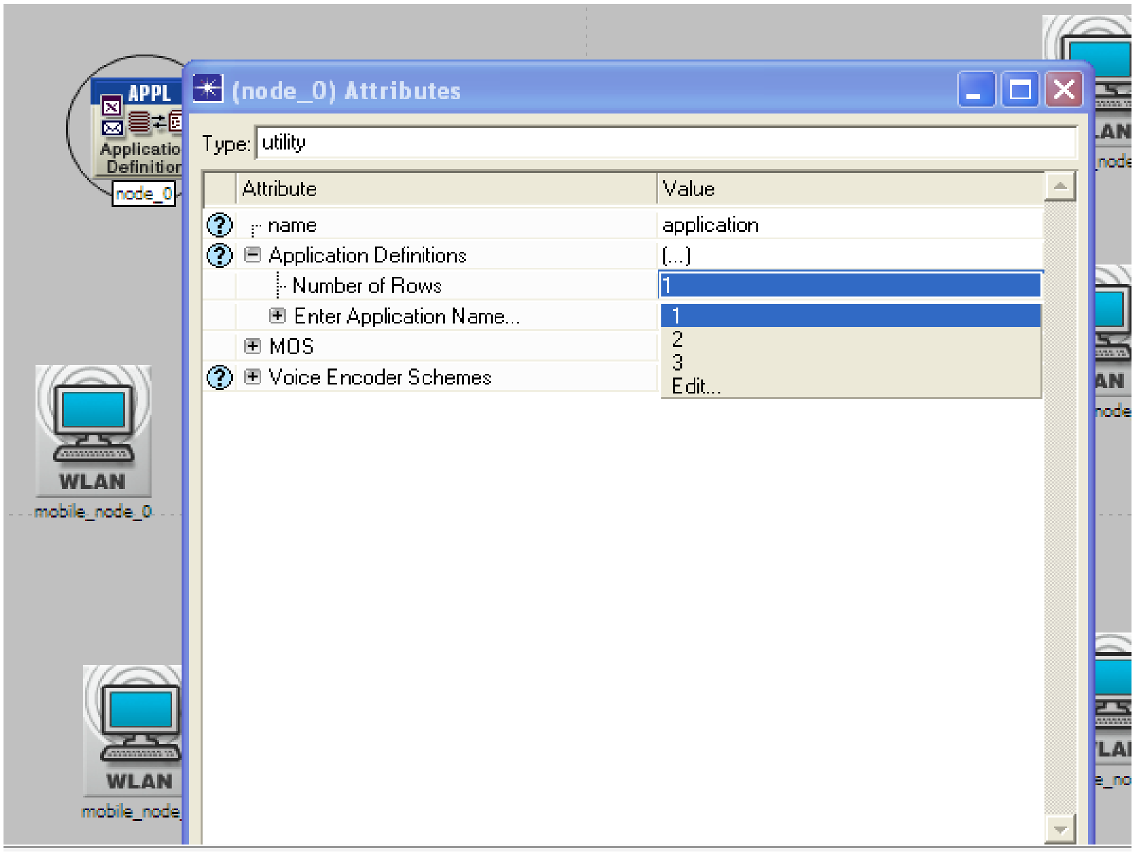
Figure 5.24: Select Application Node



Type: utility

Attribute	Value
name	application
⊞ Application Definitions	(...)
⊞ MOS	
⊞ Voice Encoder Schemes	All Schemes

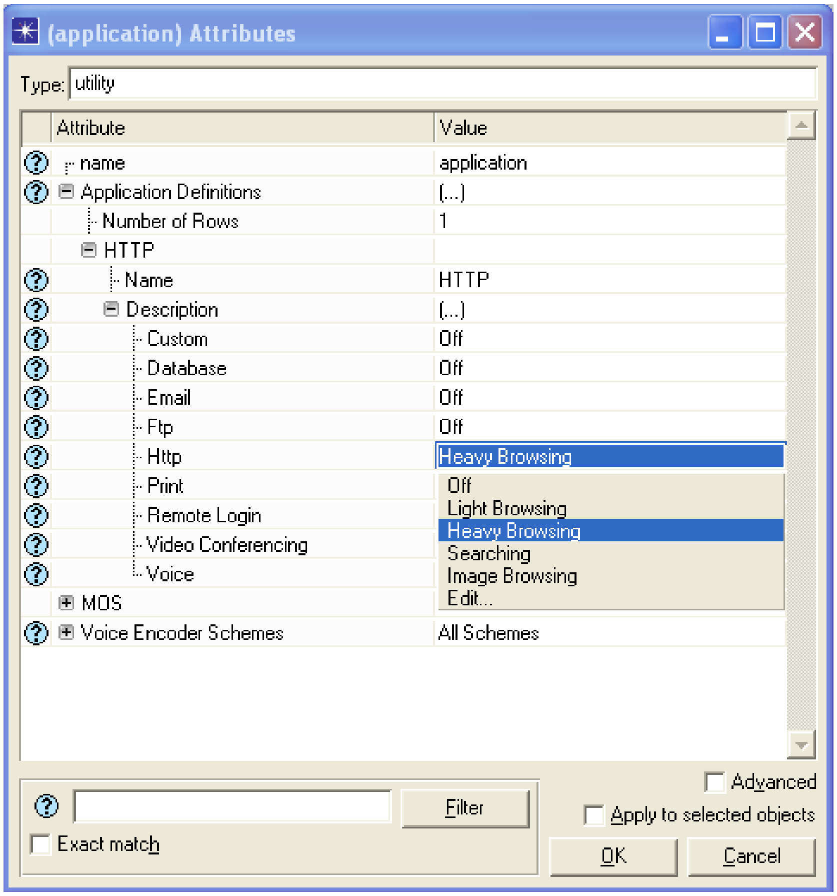
Figure 5.25: Enter The Name of Application



Type: utility

Attribute	Value
name	application
Application Definitions	(...)
Number of Rows	1
Enter Application Name...	
MOS	
Voice Encoder Schemes	

Figure 5.26: Application Definitions : Enter The Number of Row

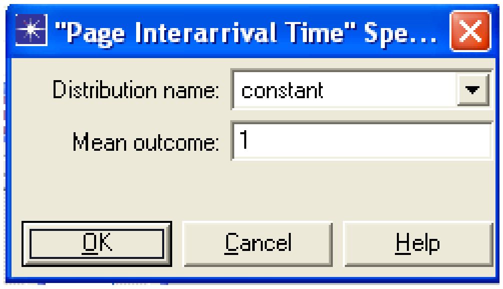


(application) Attributes

Type: utility

Attribute	Value
name	application
Application Definitions	(...)
Number of Rows	1
HTTP	
Name	HTTP
Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	Off
Http	Heavy Browsing
Print	
Remote Login	
Video Conferencing	
Voice	
MOS	
Voice Encoder Schemes	All Schemes

Figure 5.27: HTTP Heavy Browsing



"Page Interarrival Time" Spe...

Distribution name: constant

Mean outcome: 1

Figure 5.28: Page Interarrival Time

Step23: Profile configuration :

The profile contains different activities of a user or a group of users that have application list and executes the different activities on the same node by changing the parameter inside the profile node. In profile configuration we can set the number of rows, each row representing the number of profiles. In another procedure we have the number of applications that was selected in application node, but we must also change these parameters (start time offsets (second)- Duration time(second) - Repeatability). In profile procedure we have the same parameters (Operation mode- start time offset (second) -Duration time(second) - Repeatability).

- The steps for changing a parameter in profile node :

- Right click on Profile node and select (edit attributes) from the list as shown in Figure 5.29.
- Change the name of profile by changing the value to profile as shown in Figure 5.30.
- In profile configuration let the number of rows equal to one.
- In profile we can select the application that was selected in application node.
- In application procedure let the number of rows equal to one because we have one application (HTTP) as shown in Figure 5.31.
- Change the parameter of HTTP application such as: name, start time, duration and repeatability as shown in figure 5.32 , Figure 5.33 .
- Change the parameter of profile such as: operation mode, name, start time, duration and repeatability as shown in Figure 5.34, 5.35, 5.36 .
- Click OK after the necessary parameters have been changed it.

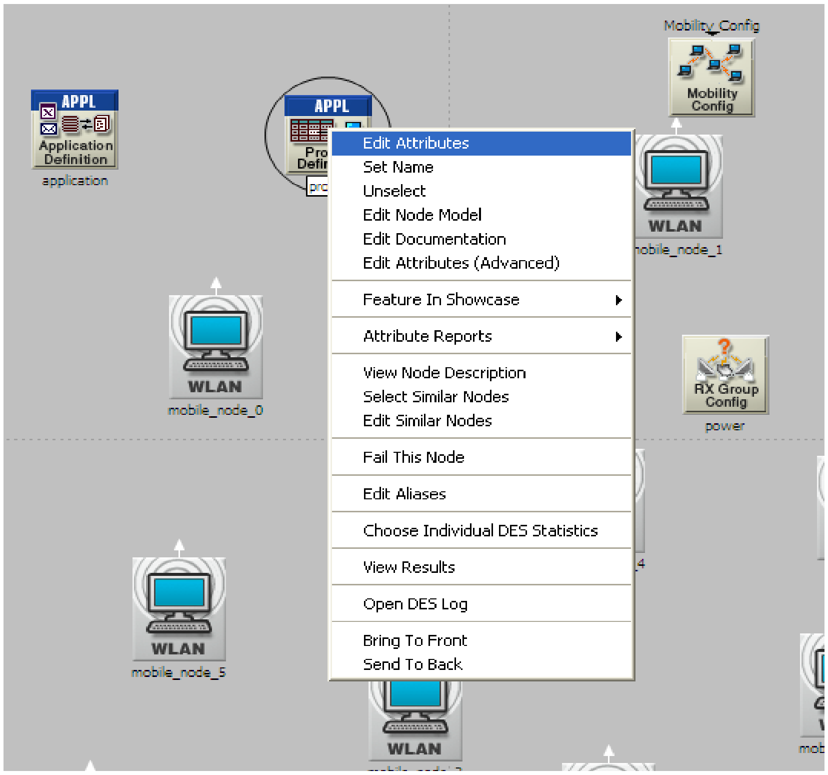
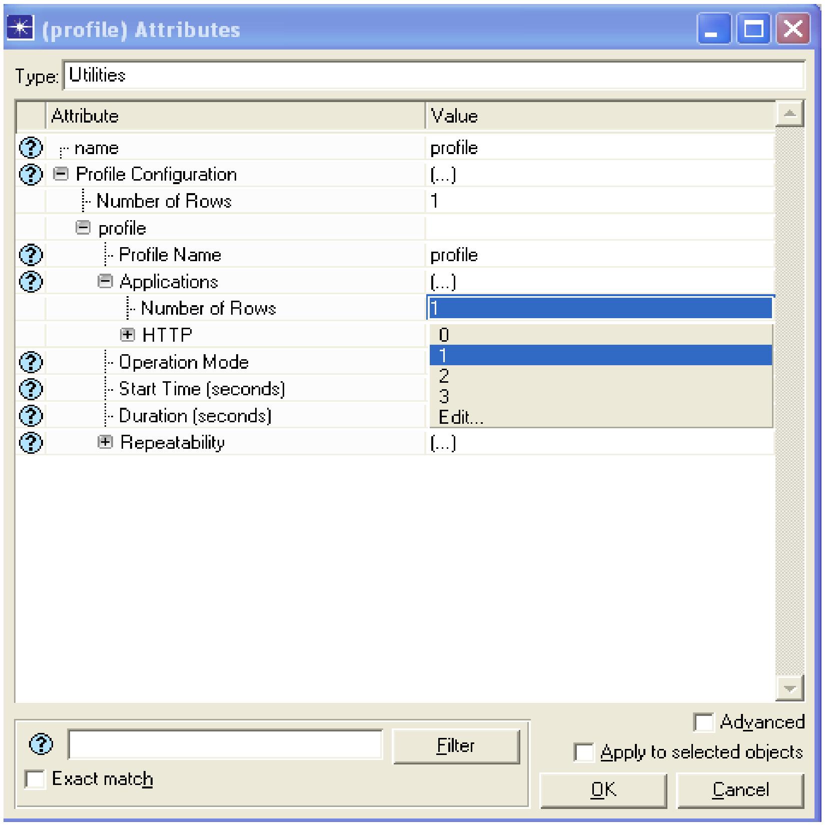


Figure 5.29: Edit Attributes

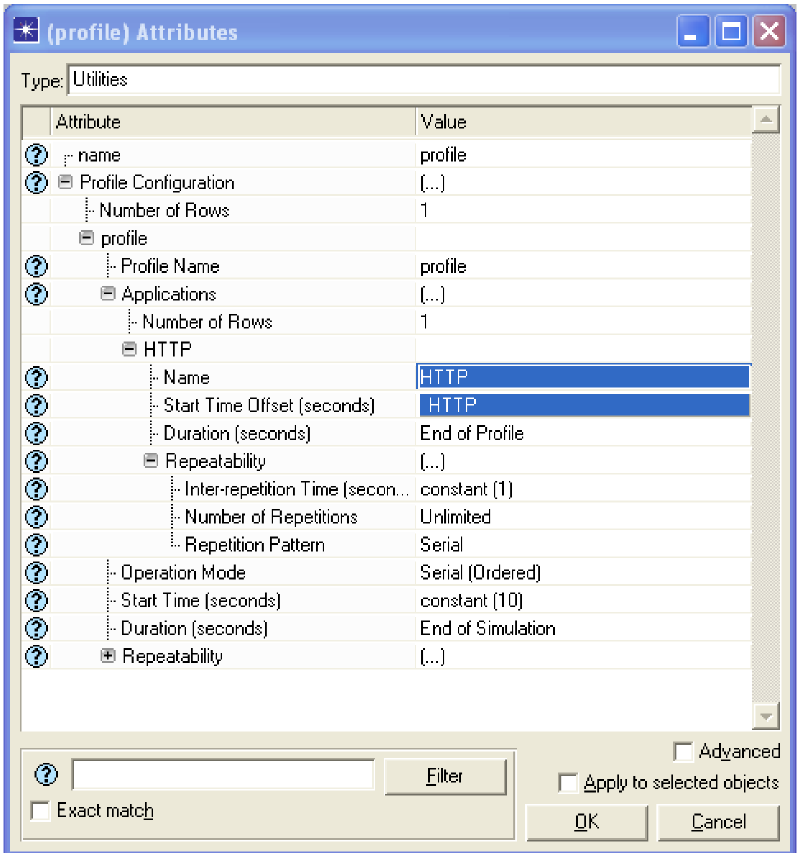


Type: Utilities

Attribute	Value
name	profile
⊟ Profile Configuration	(...)
Number of Rows	1
⊟ profile	
Profile Name	profile
⊟ Applications	(...)
Number of Rows	1
⊞ HTTP	
Operation Mode	
Start Time (seconds)	
Duration (seconds)	
⊞ Repeatability	(...)

Figure 5.30: Profile Attributes

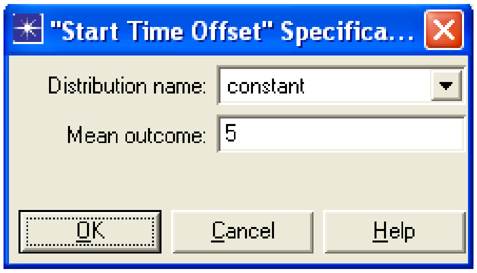
-These parameters are related to the application configuration



Type: Utilities

Attribute	Value
name	profile
Profile Configuration	(...)
Number of Rows	1
profile	
Profile Name	profile
Applications	(...)
Number of Rows	1
HTTP	
Name	HTTP
Start Time Offset (seconds)	HTTP
Duration (seconds)	End of Profile
Repeatability	(...)
Inter-repetition Time (secon...	constant (1)
Number of Repetitions	Unlimited
Repetition Pattern	Serial
Operation Mode	Serial (Ordered)
Start Time (seconds)	constant (10)
Duration (seconds)	End of Simulation
Repeatability	(...)

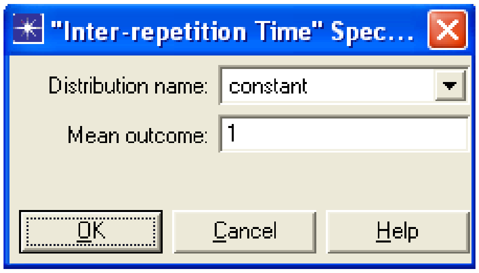
Figure 5.31: Change The Setting Of Profile



Distribution name: constant

Mean outcome: 5

Figure 5.32: Start Time Offset

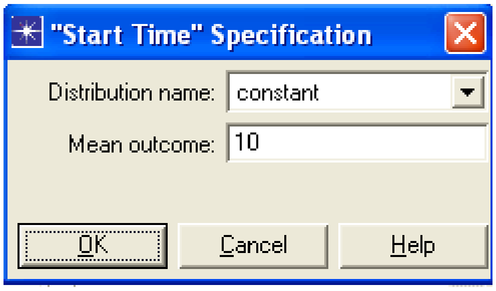


Distribution name: constant

Mean outcome: 1

Figure 5.33: Inter-repetition Time

- These parameters are related to profile configuration :

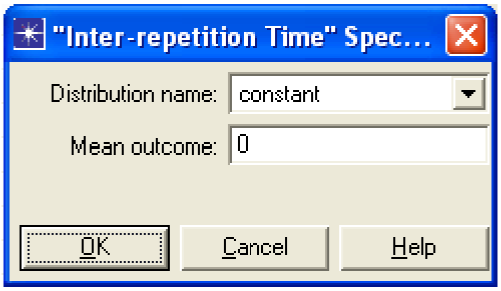


"Start Time" Specification

Distribution name: constant

Mean outcome: 10

Figure 5.34: Start Time

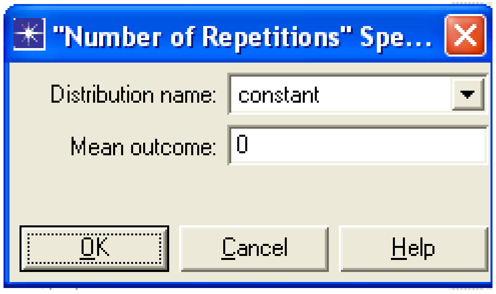


"Inter-repetition Time" Spec...

Distribution name: constant

Mean outcome: 0

Figure 5.35: Inter-repetition Time



"Number of Repetitions" Spe...

Distribution name: constant

Mean outcome: 0

Figure 5.36: Number Of Repetitions

Step24**:**Mobility model configuration :

- Right click on any mobility configuration and choose (Edit attributes) from the list as shown in Figure 5.37.
- Change the name to the mobility configuration as shown in Figure 5.38.
- Select (Random mobility profile) and let the number of rows are equal to 1 (because we have one profile) as shown in Figure 5.39.

- To specify the area of our simulation select (Random way point parameters) and change the value of Y-max (meter) and X-max (meter) to 1000 as shown in Figure 5.39.
- Select (speed meter/second) and change the value to (constant=1) as shown in Figure 5.40.
- Select (pause time /second) and change the value to (constant=0) as shown in Figure 5.41.
- Select (start time /second) and change the value to (constant=10) as shown in Figure 5.42.
- Select (stop time/second) and change the value to (End of simulation) as shown in Figure 5.43.

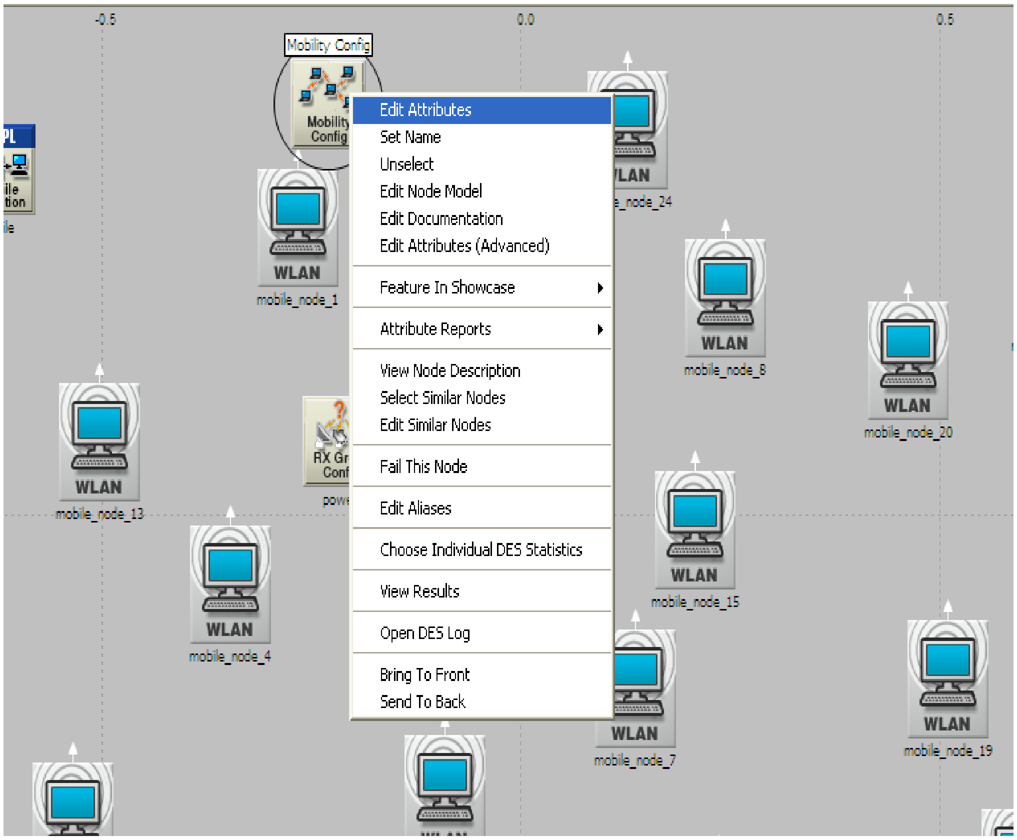
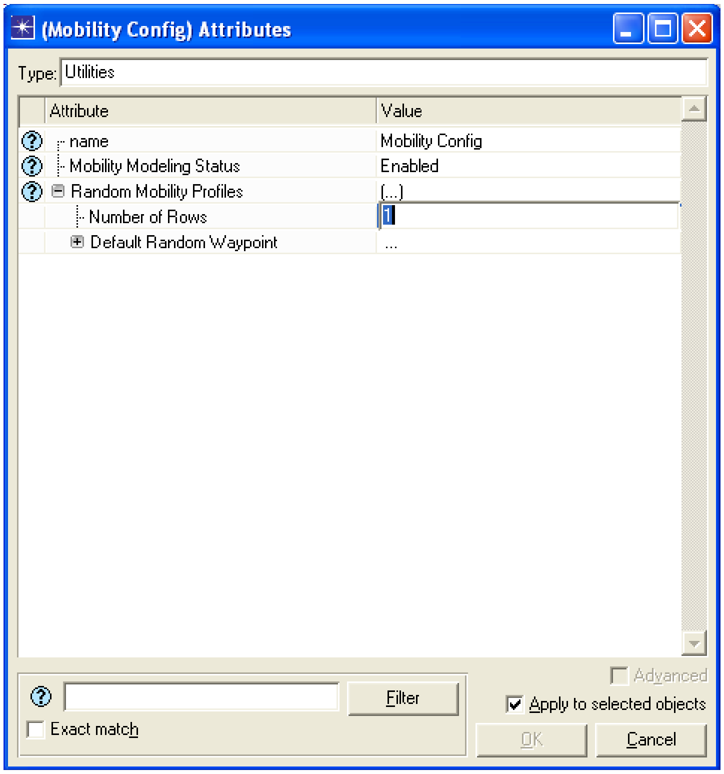


Figure 5.37: Mobility Configuration Setting



(Mobility Config) Attributes

Type: Utilities

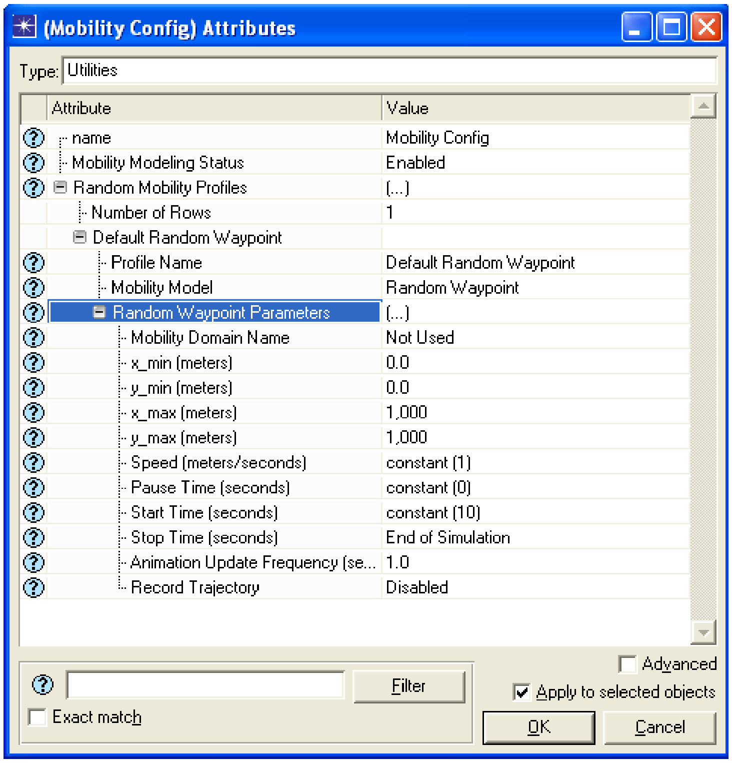
Attribute	Value
name	Mobility Config
Mobility Modeling Status	Enabled
⊟ Random Mobility Profiles	(...)
Number of Rows	1
⊞ Default Random Waypoint	...

□ Advanced

☑ Apply to selected objects

□ Exact match

Figure 5.38: Mobility Configuration List



(Mobility Config) Attributes

Type: Utilities

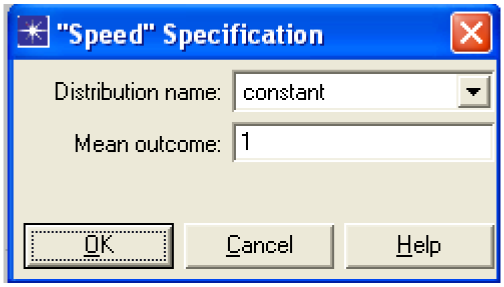
Attribute	Value
name	Mobility Config
Mobility Modeling Status	Enabled
⊟ Random Mobility Profiles	(...)
Number of Rows	1
⊟ Default Random Waypoint	
Profile Name	Default Random Waypoint
Mobility Model	Random Waypoint
⊟ Random Waypoint Parameters	(...)
Mobility Domain Name	Not Used
x_min (meters)	0.0
y_min (meters)	0.0
x_max (meters)	1,000
y_max (meters)	1,000
Speed (meters/seconds)	constant (1)
Pause Time (seconds)	constant (0)
Start Time (seconds)	constant (10)
Stop Time (seconds)	End of Simulation
Animation Update Frequency (se...	1.0
Record Trajectory	Disabled

□ Advanced

☑ Apply to selected objects

□ Exact match

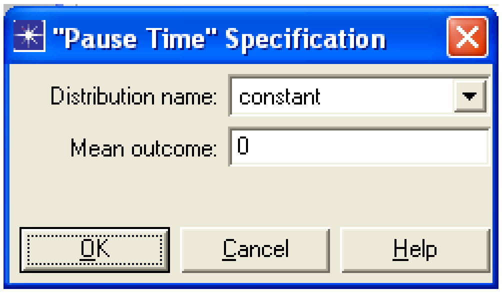
Figure 5.39:Mobility Configuration Setting


"Speed" Specification

Distribution name: constant

Mean outcome: 1

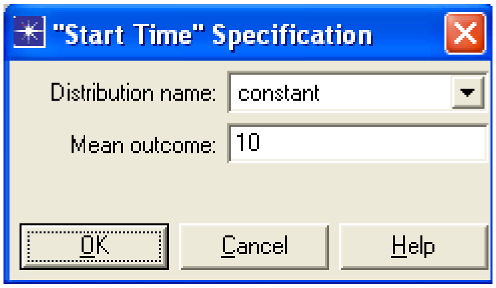
Figure 5.40: Speed Of Nodes


"Pause Time" Specification

Distribution name: constant

Mean outcome: 0

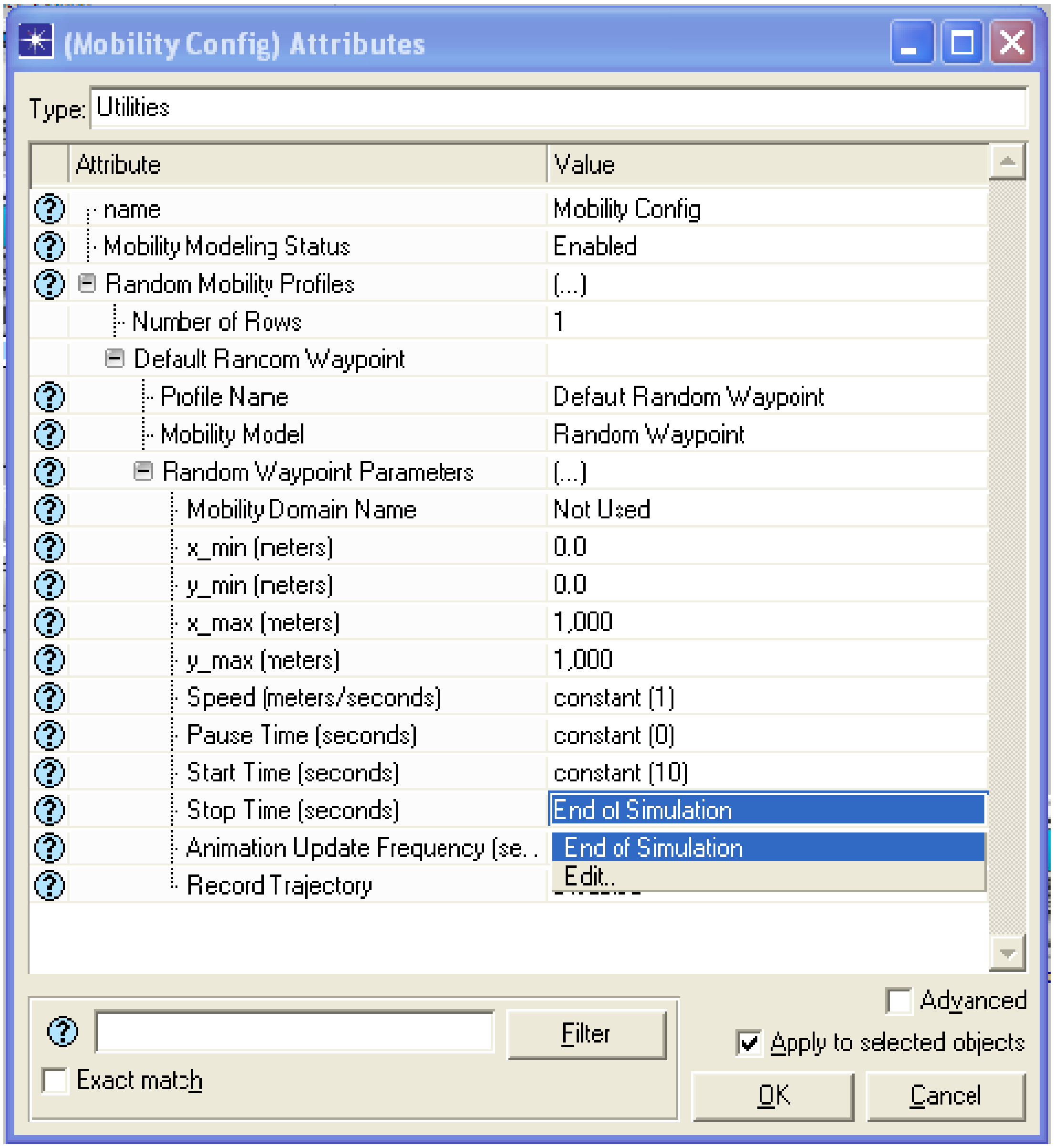
Figure 5.41: Pause Time


"Start Time" Specification

Distribution name: constant

Mean outcome: 10

Figure 5.42: Start Time



Type: Utilities

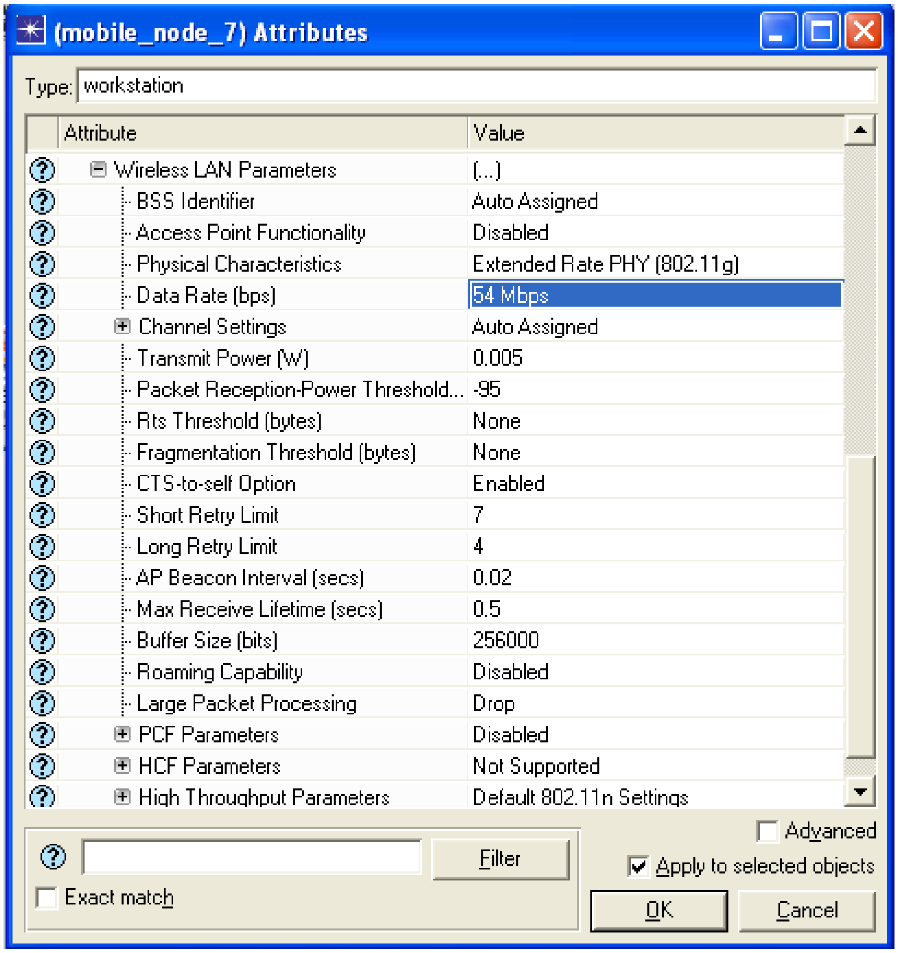
Attribute	Value
name	Mobility Config
Mobility Modeling Status	Enabled
⊟ Random Mobility Profiles	(...)
Number of Rows	1
⊟ Default Rancom Waypoint	
Profile Nane	Defaut Random Waypoint
Mobility Model	Random Waypoint
⊟ Random Waypoint Parameters	(...)
Mobility Domain Name	Not Used
x_min (neters)	0.0
y_min (neters)	0.0
x_max (neters)	1,000
y_max (neters)	1,000
Speed (meters/seconds)	constant (1)
Pause Time (seconds)	constant (0)
Start Time (seconds)	constant (10)
Stop Time (seconds)	End ol Simulation
Animation Update Frequency (se..	
Record Trajectory	

Figure 5.43: Mobility Configuration Setting

Step25:To choose physical characteristics that have data rate we must select all WLAN_WKSTNnodes by right click on any WLAN_WKSTNnode and select (Select Similar Node) from the list.

Step26:Right click on any WLAN_WKSTNnode and choose (edit attributes), then Wireless LAN parameters that contain two procedures :

- Physical Characteristics (802.11g - 802.11b)
- Data Rate as shown in Figure 5.44-5.47.



(mobile_node_7) Attributes

Type: workstation

Attribute	Value
⊟ Wireless LAN Parameters	(...)
BSS Identifier	Auto Assigned
Access Point Functionality	Disabled
Physical Characteristics	Extended Rate PHY (802.11g)
Data Rate (bps)	54 Mbps
⊞ Channel Settings	Auto Assigned
Transmit Power (W)	0.005
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000
Roaming Capability	Disabled
Large Packet Processing	Drop
⊞ PCF Parameters	Disabled
⊞ HCF Parameters	Not Supported
⊞ High Throughput Parameters	Default 802.11n Settings

□ Advanced

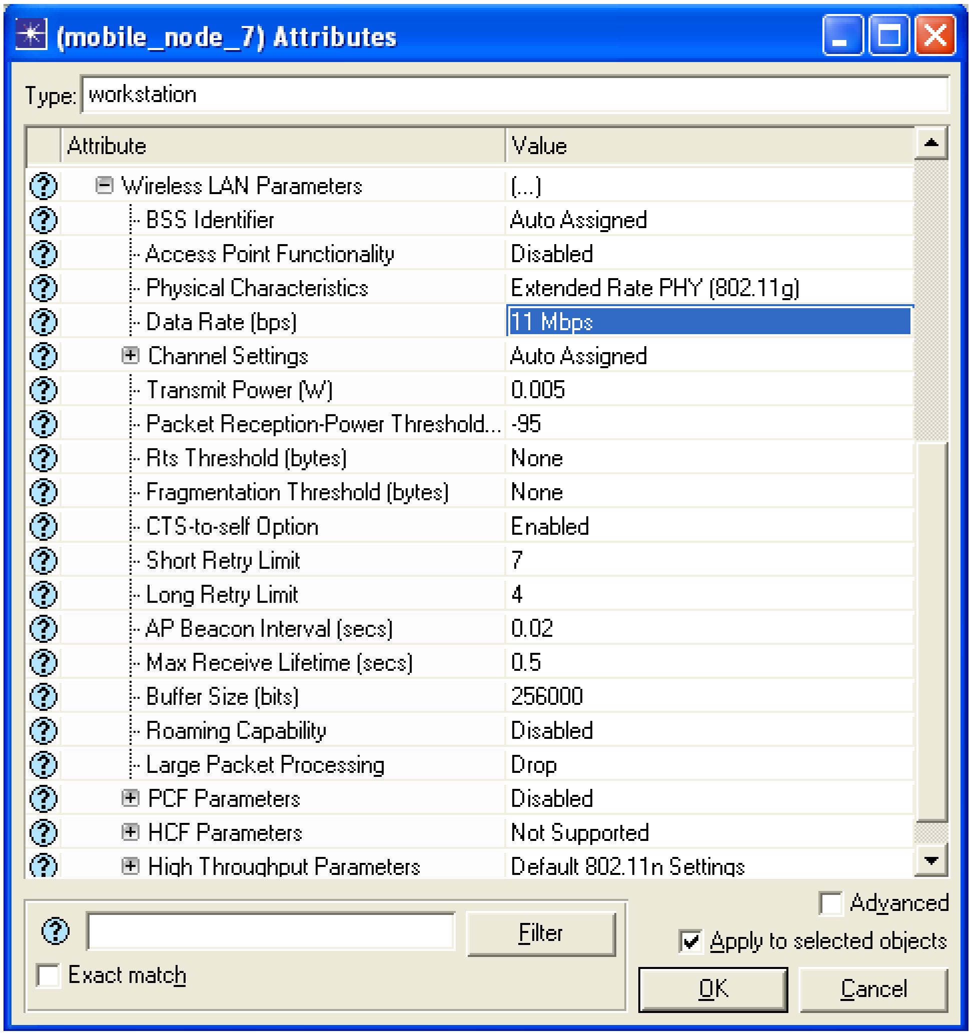
☑ Apply to selected objects

□ Exact match

Figure 5.44: Mobile Node Attribute

Physical Characteristics : 802.11g.

Data Rate (bps) : 11Mb.



(mobile_node_7) Attributes

Type: workstation

Attribute	Value
⊟ Wireless LAN Parameters	(...)
BSS Identifier	Auto Assigned
Access Point Functionality	Disabled
Physical Characteristics	Extended Rate PHY (802.11g)
Data Rate (bps)	11 Mbps
⊞ Channel Settings	Auto Assigned
Transmit Power (W)	0.005
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000
Roaming Capability	Disabled
Large Packet Processing	Drop
⊞ PCF Parameters	Disabled
⊞ HCF Parameters	Not Supported
⊞ High Throughput Parameters	Default 802.11n Settings

□ Advanced

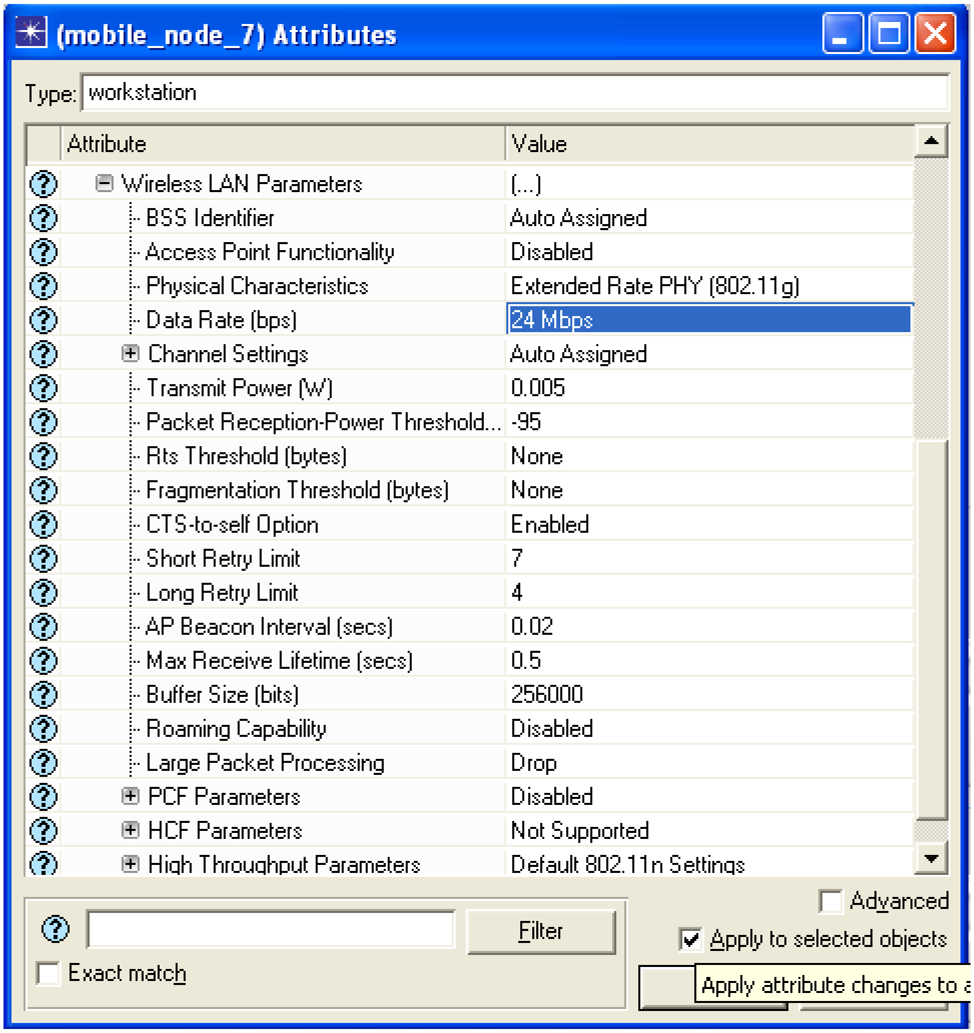
☑ Apply to selected objects

□ Exact match

Figure 5.45: Mobile Node Attribute

Physical Characteristics = 802.11g

Data Rate (bps) = 24 Mbps.



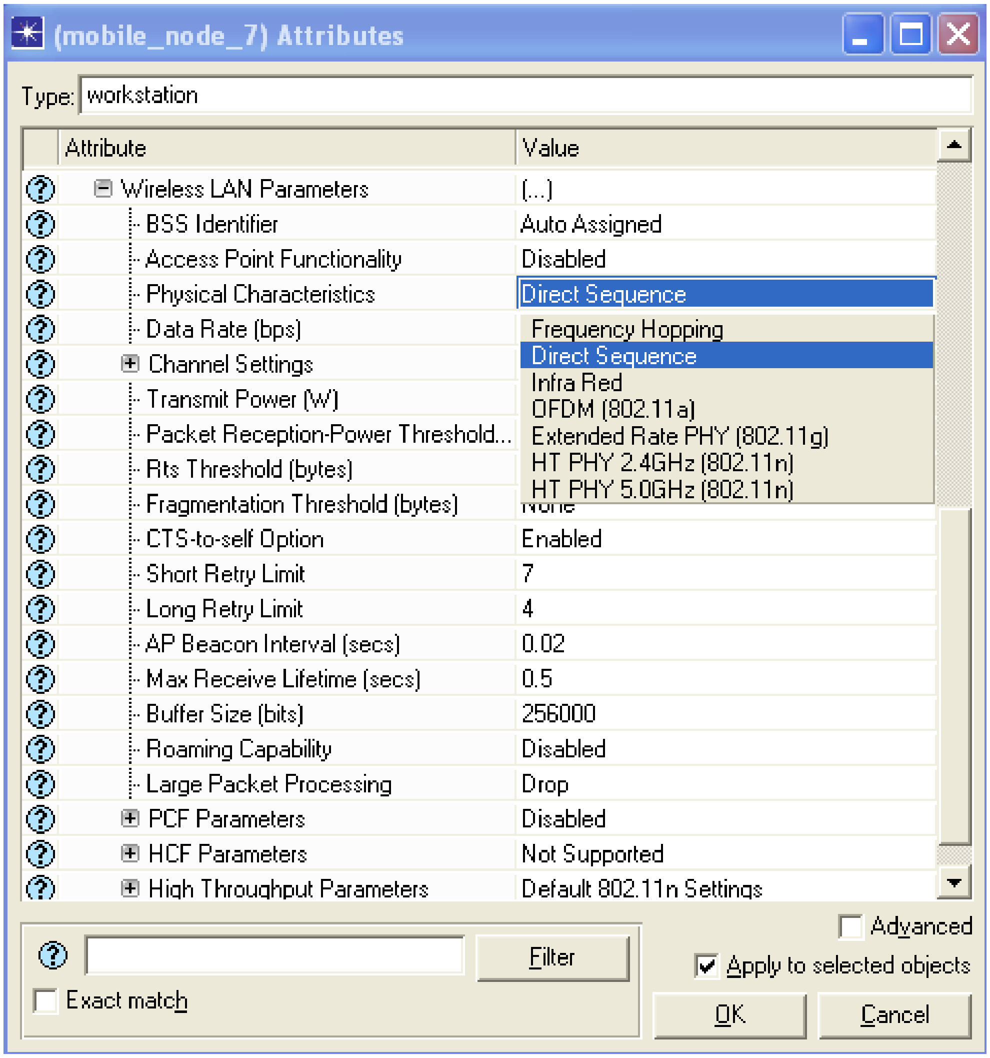
Type: workstation

Attribute	Value
⊟ Wireless LAN Parameters	(...)
BSS Identifier	Auto Assigned
Access Point Functionality	Disabled
Physical Characteristics	Extended Rate PHY (802.11g)
Data Rate (bps)	24 Mbps
⊞ Channel Settings	Auto Assigned
Transmit Power (W)	0.005
Packet Reception-Power Threshold...	-95
Rts Threshold (bytes)	None
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000
Roaming Capability	Disabled
Large Packet Processing	Drop
⊞ PCF Parameters	Disabled
⊞ HCF Parameters	Not Supported
⊞ High Throughput Parameters	Default 802.11n Settings

Figure 5.46: Mobile Node Attribute

Physical Characteristics = 802.11b.

Data Rate (bps) = 11 Mbps.



(mobile_node_7) Attributes

Type: workstation

Attribute	Value
⊟ Wireless LAN Parameters	(...)
BSS Identifier	Auto Assigned
Access Point Functionality	Disabled
Physical Characteristics	Direct Sequence
Data Rate (bps)	
⊞ Channel Settings	
Transmit Power (W)	
Packet Reception-Power Threshold...	
Rts Threshold (bytes)	
Fragmentation Threshold (bytes)	None
CTS-to-self Option	Enabled
Short Retry Limit	7
Long Retry Limit	4
AP Beacon Interval (secs)	0.02
Max Receive Lifetime (secs)	0.5
Buffer Size (bits)	256000
Roaming Capability	Disabled
Large Packet Processing	Drop
⊞ PCF Parameters	Disabled
⊞ HCF Parameters	Not Supported
⊞ High Throughput Parameters	Default 802.11n Settings

Frequency Hopping
Direct Sequence
Infra Red
OFDM (802.11a)
Extended Rate PHY (802.11g)
HT PHY 2.4GHz (802.11n)
HT PHY 5.0GHz (802.11n)

Figure 5.47: Mobile Node Attribute

Step27: As mentioned earlier we have 12 scenarios that use physical characteristics 802.11g and 802.11b with different data rates. In this simulation each scenario depends on the number of server, number of clients and the number of intermediate nodes. To specify the server and client we have a technology in OPNET modeler called deploy application, as shown in Fgure 5.48, 5.49.

Step28:Deploy application :

- Click on the protocol from the main menu and select application then select deploy defined application .
- In the network tree select nodes on the left hand side.
- On the right hand side tree select application or profile.
- To Deploy the select set of nodes click on the assign (>>) button.

- To remove profile or application :

1- Select all nodes from the right hand side.

2- Click on (x) button to remove the selected nodes.

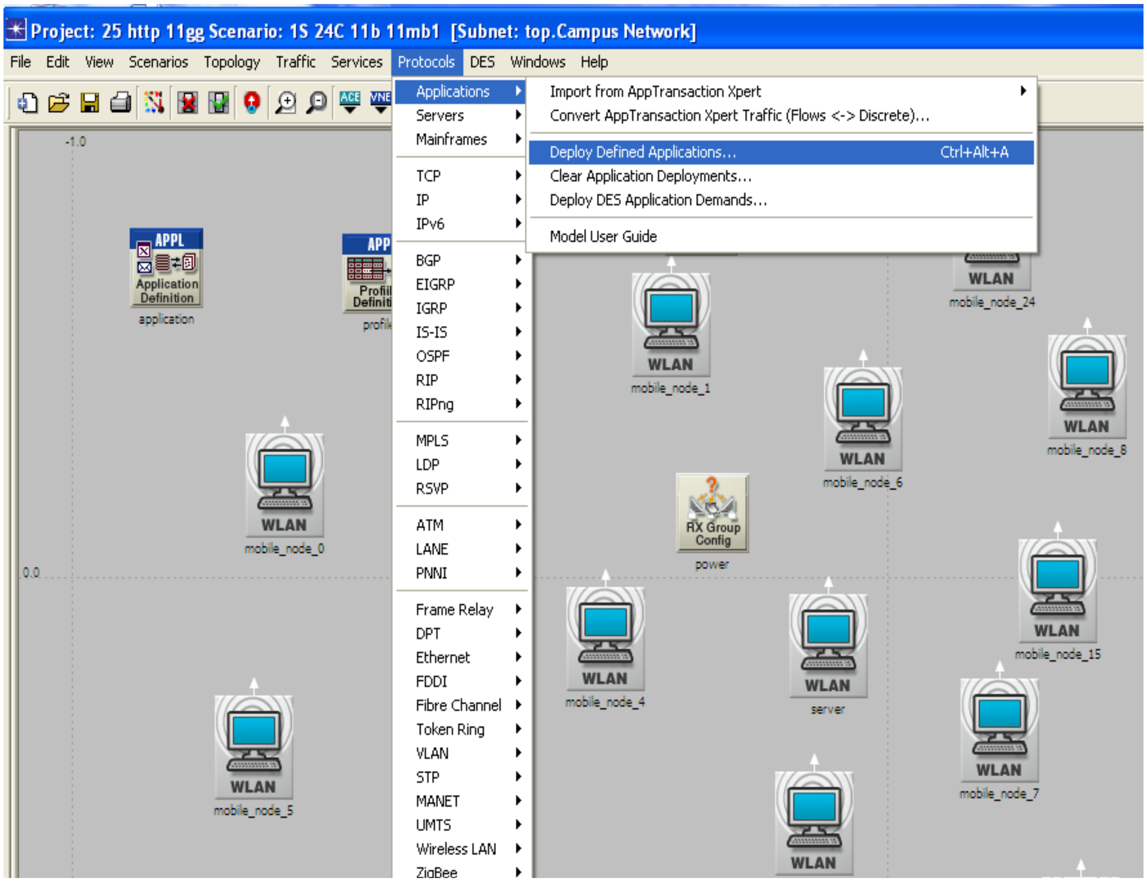
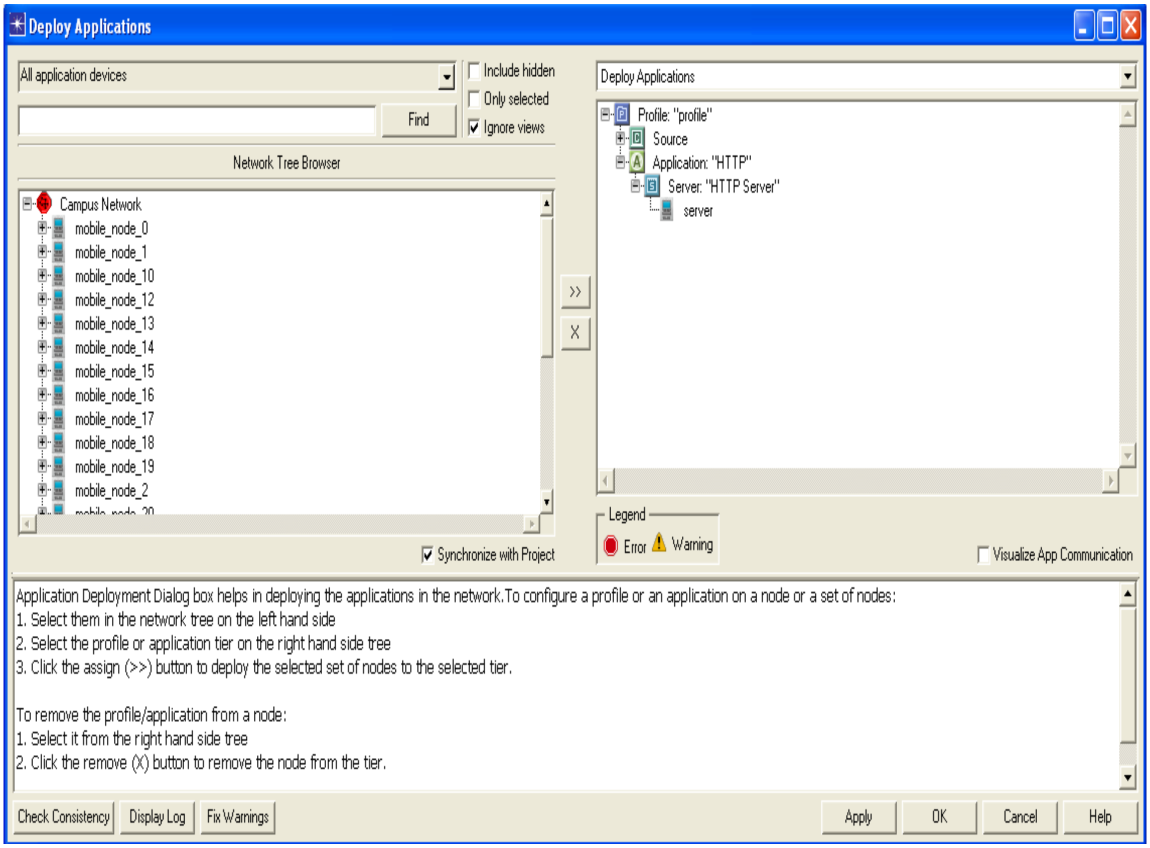

Project: 25 http 11gg Scenario: 1S 24C 11b 11mb1 [Subnet: top.Campus Network]
File Edit View Scenarios Topology Traffic Services Protocols DES Windows Help
Applications
Servers
Mainframes
TCP
IP
IPv6
BGP
EIGRP
IGRP
IS-IS
OSPF
RIP
RIPng
MPLS
LDP
RSVP
ATM
LANE
PNNI
Frame Relay
DPT
Ethernet
FDDI
Fibre Channel
Token Ring
VLAN
STP
MANET
UMTS
Wireless LAN
ZigBee
Import from AppTransaction Xpert
Convert AppTransaction Xpert Traffic (Flows <-> Discrete)...
Deploy Defined Applications... Ctrl+Alt+A
Clear Application Deployments...
Deploy DES Application Demands...
Model User Guide
APPL Application Definition
application
Profile Definition
profile
RX Group Config
power
WLAN
mobile_node_0
mobile_node_1
mobile_node_4
mobile_node_5
mobile_node_6
mobile_node_7
mobile_node_8
mobile_node_15
mobile_node_24
server

Figure 5.48: Deploy Defined Application



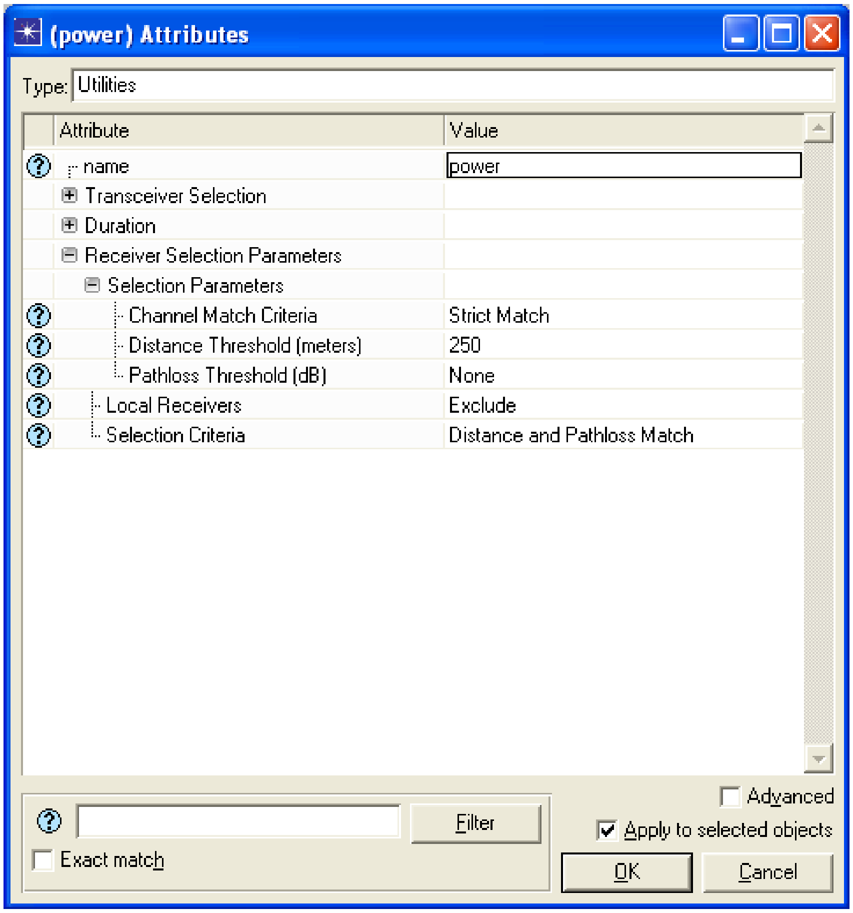
Application Deployment Dialog box helps in deploying the applications in the network.To configure a profile or an application on a node or a set of nodes:
1. Select them in the network tree on the left hand side
2. Select the profile or application tier on the right hand side tree
3. Click the assign (>>) button to deploy the selected set of nodes to the selected tier.

To remove the profile/application from a node:
1. Select it from the right hand side tree
2. Click the remove (X) button to remove the node from the tier.

Figure 5.49: Deploy Applications

Step29: We used RX Group configuration by right click on the RX Group node and changed the parameter of Distance threshold(meter) to 250 as shown in Figure 5.50.

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)



Type: Utilities

Attribute	Value
name	power
⊞ Transceiver Selection	
⊞ Duration	
⊟ Receiver Selection Parameters	
⊟ Selection Parameters	
Channel Match Criteria	Strict Match
Distance Threshold (meters)	250
Pathloss Threshold (dB)	None
Local Receivers	Exclude
Selection Criteria	Distance and Pathloss Match

□ Advanced

☑ Apply to selected objects

□ Exact match

Figure 5.50: RX Group

Step30: To Copy another scenario : select (scenario) from main menu list then (Duplicate scenario) and after selecting it,enter the name of new scenarios, as shown in Figure 5.51, 5.52.

Step30:To show the results in simulation : right click anywhere and select (view result) as shown in Figure 5.53.

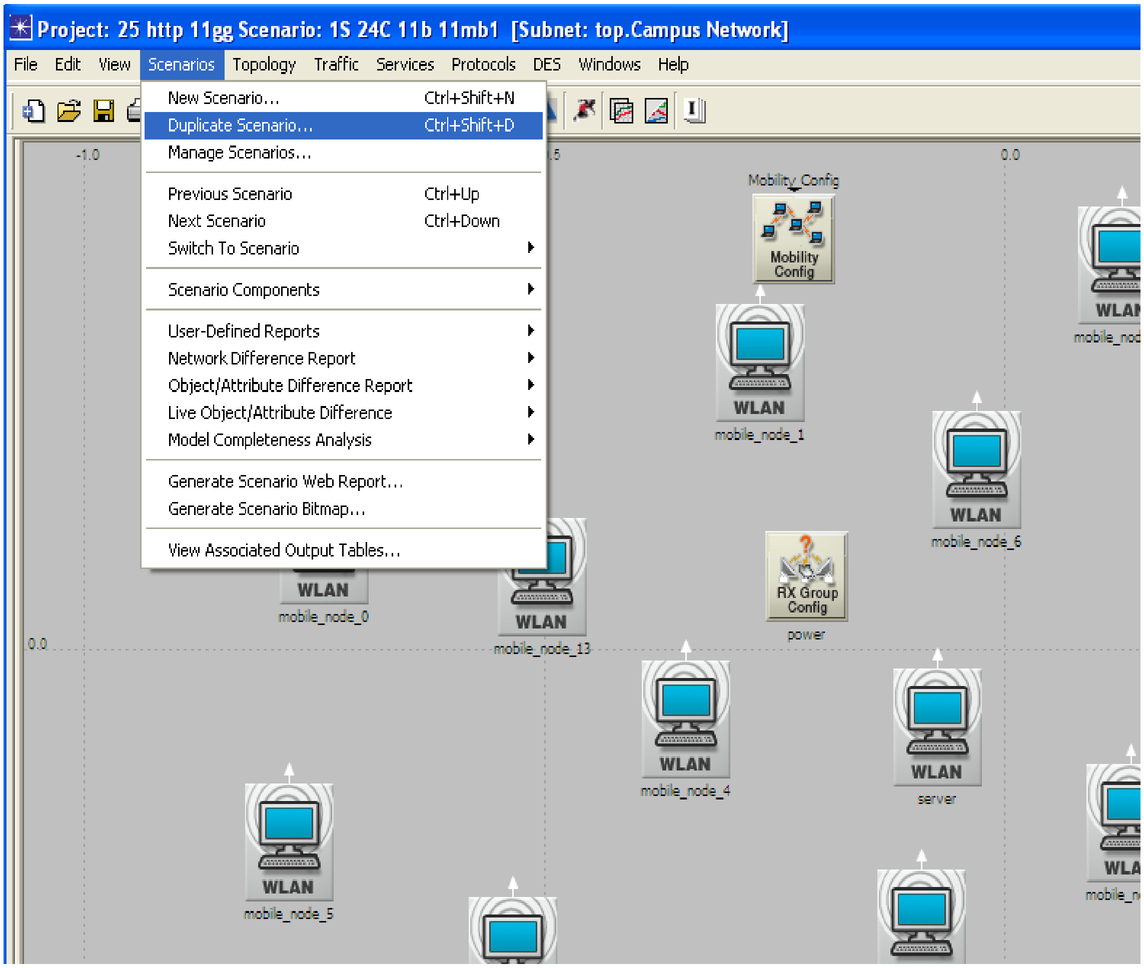
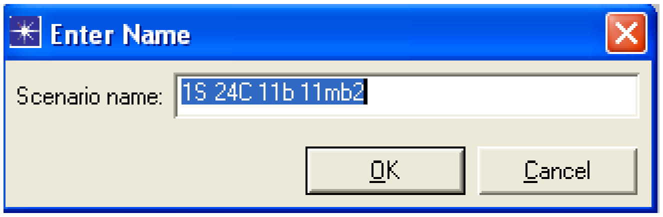

Project: 25 http 11gg Scenario: 1S 24C 11b 11mb1 [Subnet: top.Campus Network]
File
Edit
View
Scenarios
Topology
Traffic
Services
Protocols
DES
Windows
Help
New Scenario... Ctrl+Shift+N
Duplicate Scenario... Ctrl+Shift+D
Manage Scenarios...
Previous Scenario Ctrl+Up
Next Scenario Ctrl+Down
Switch To Scenario
Scenario Components
User-Defined Reports
Network Difference Report
Object/Attribute Difference Report
Live Object/Attribute Difference
Model Completeness Analysis
Generate Scenario Web Report...
Generate Scenario Bitmap...
View Associated Output Tables...
Mobility Config
mobile_node_1
mobile_node_6
RX Group Config
power
mobile_node_0
mobile_node_13
mobile_node_4
server
mobile_node_5
WLAN

Figure 5.51: Scenario List



Scenario name: 1S 24C 11b 11mb2

Figure 5.52: Scenario Name

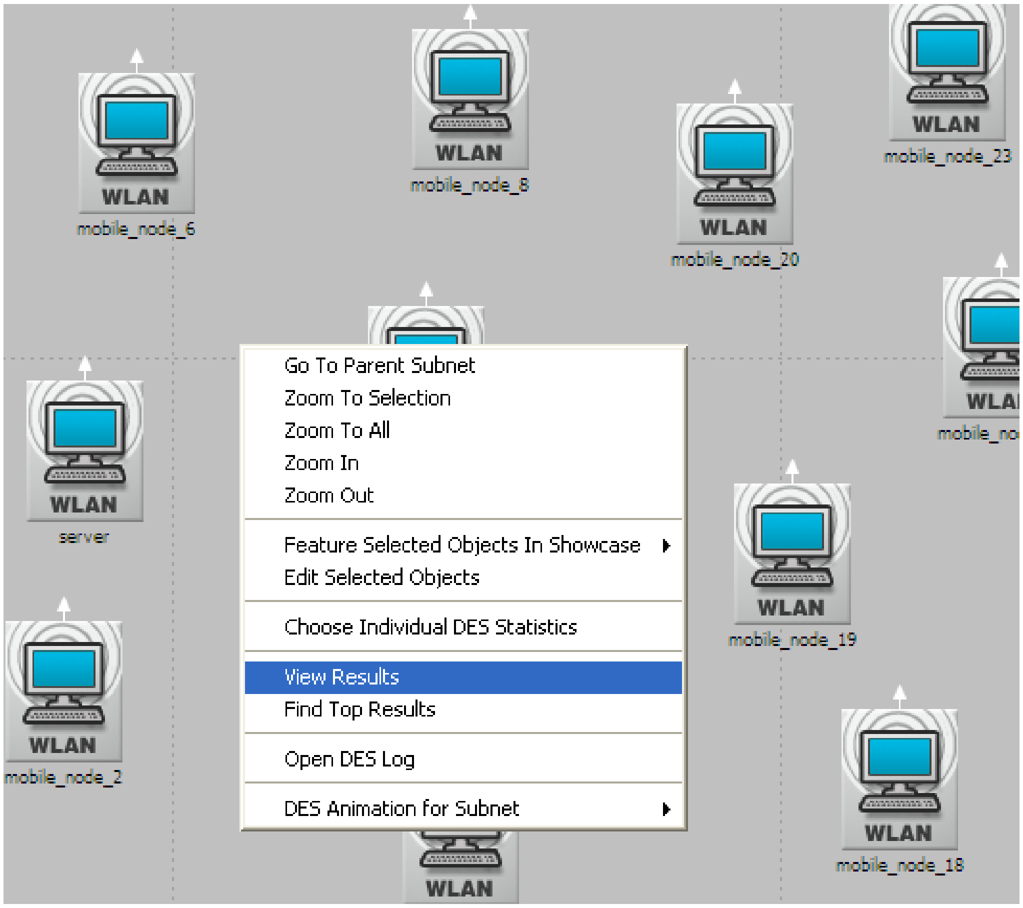


Figure 5.53:View Results

Step32:To specify the performance metrics : click on the (DES) from the main menu then (choose individual statistics).

Step33:In performance metrics we have (HTTP - AODV - WLAN).

Step34: Finally, click on the (DES), then (configure/Run discrete event simulation).

Chapter 6

RESULTS AND DISCUSSION

6.1 Performance metrics

In OPNET simulator, a number of performance metrics are present for MANET environment in order to study the overall network performance. In this thesis, we used number of hops per route, Route discovery time, HTTP object response time, HTTP page response time, Media access delay, Retransmission attempts and Throughput.

Number of hops per route: This statistic represents the number of hops in each route to every destination in the route table of all nodes in the network.

Route discovery time: The time to discover a route to a specific destination is the time when a route request was sent out to discover a route to that destination until the time a route reply is received with a route to that destination. This statistic represents the time to discover a route to a specific destination by all nodes in the network This statistic is collected in a bucket mode with sample mean within that bucket by default.

HTTP Object response time: Specifies response time for each inline object from the HTML page .

HTTP Page response time: Specifies time required to retrieve the entire page with all the contained inline objects.

Media Access Delay: Represents the global statistic for the total of queuing and contention delays of the data, management, delayed Block-ACK and Block-ACK Request frames transmitted by all WLAN MACs in the network. For each frame, this delay is calculated as the duration from the time when it is inserted into the transmission queue, which is arrival time for higher layer data packets and creation time for all other frames types, until the time when the frame is sent to the physical layer for the first time. Hence, it also includes the period for the successful RTS/CTS exchange, if this exchange is used prior to the transmission of that frame.

Retransmission: Total number of retransmission attempts by all WLAN MACs in the network until either packet is successfully transmitted or it is discarded as a result of reaching short or long retry limit.

Throughput: The average rate at which the data packet is delivered successfully from one node to another over a communication network is known as throughput. The throughput is usually measured in bits per second (bits/sec). A throughput with a higher value is more often an absolute choice in every network. Mathematically, throughput can be defined by the following formula.Throughput=(number of delivered packet * packet size) / total duration of simulation.

Category 1:

In category 1, a network model is designed with mobile nodes in OPNET 17.1 modeler for AODV routing protocol. Also, a comparison is made between 802.11g and 802.11b but with data rates 11Mb/s,and we have to study the contact of these mobile nodes on MANET routing protocols performance using HTTP heavy browsing. All scenarios contain 25 nodes with the speed of 1m/s for AODV routing protocol in the Campus having the area of 1000 x 1000 meters. The attributes of nodes and server Ad hoc routing parameters are set with respect to the required protocol. Simulation results of routing protocols are analyzed according to number of hops, route discovery time, HTTP object response time, media access delay, retransmission attempts and throughput. For the design networks the simulation time is 300 seconds.

1\1 : It means there is one server and one client.

1\12 : It means there is one server and twelve clients.

1\24 : It means there is one server and twenty four clients.

Table 6.1: Simulation Results of Average Number of Hops for 802.11g and 802.11b Standards with AODV Protocol.

802.11g data rate Mb/s	Number of Hops per route		
	1\1	1\12	1\24
802.11g 11Mb	1.741452719	2.417895783	3.503497897
802.11b 11Mb	1.901193783	2.420501148	3.358061977

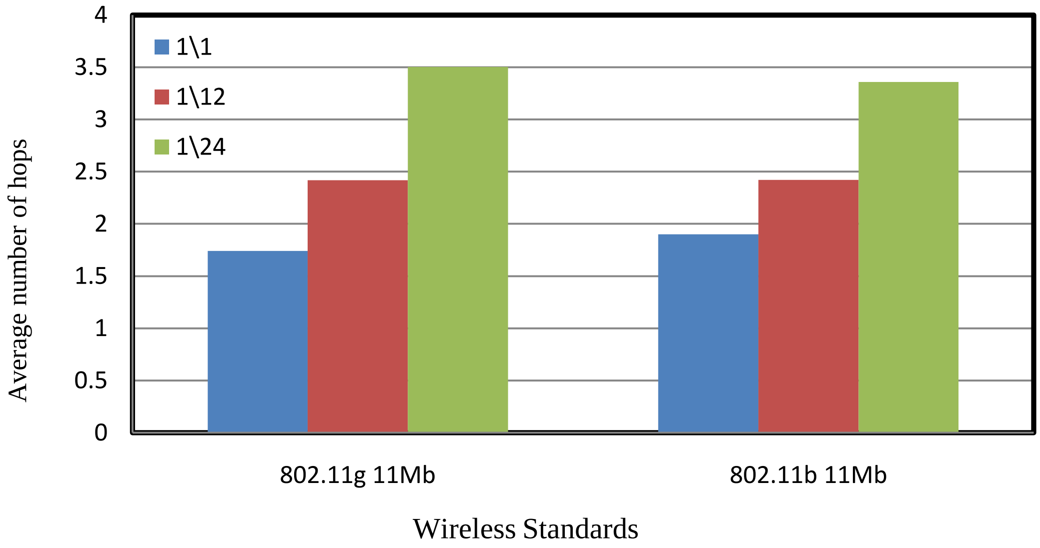


Figure 6.1:Average Number of Hops Versus Different Wireless Standard 802.11g and 802.11b for AODV Protocol.

In Figure 6.1 we can see the average number of hops compared with wireless standards 802.11g and 802.11b when the data rates is 11Mbps. Network topology 1/24 has the maximum number of hops when the wireless standards is 802.11g (11Mbps). So the number of hops depends on the number of clients. For this reason 1/24 has the highest value as compared to other cases with the lowest value.

Table 6.2: Simulation Results of Average HTTP Page Response Time for 802.11g and 802.11b Standards with AODV Protocol.

802.11g data rate Mb/s	HTTP Page Response Time		
	1\1	1\12	1\24
802.11g 11Mb	0.096	0.247	0.339
802.11b 11Mb	0.130	0.249	0.344

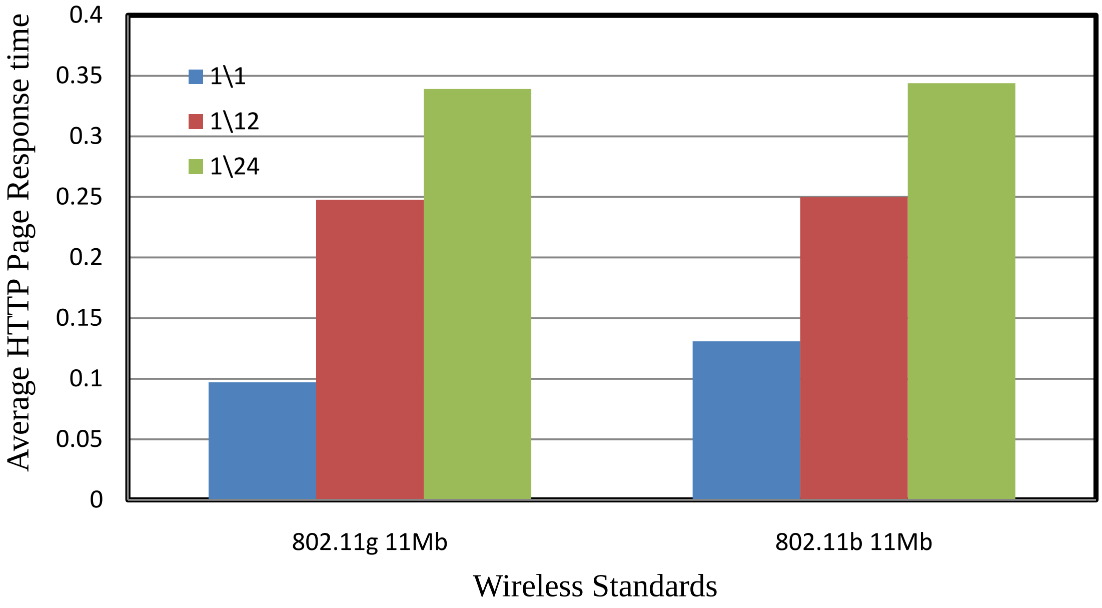


Figure 6.2:Average HTTP Page Response Time Versus Different Wireless Standard 802.11g and 802.11b for AODV Protocol

In Figure 6.2 we can observe the average HTTP page response time that is analyzed and comparedwith 802.11g and 802.11b when the data rate is 11 Mbps . When the wireless standards is 802.11b (11Mbps), network topology 1/24 has a higher value because it needsvery much time for browsing. These values are decreased gradually, especially in 1/1, the reason being that when we have only one server and one client not much time is needed for browsing.

Table 6.3:Simulation Results of Average Route Discovery Time for 802.11g and 802.11b Standards with AODV Protocol.

802.11g data rate Mb/s	Route Discovery Time		
	1\1	1\12	1\24
802.11g 11Mb	0.098	0.613	0.695
802.11b 11Mb	0.144	0.753	0.799

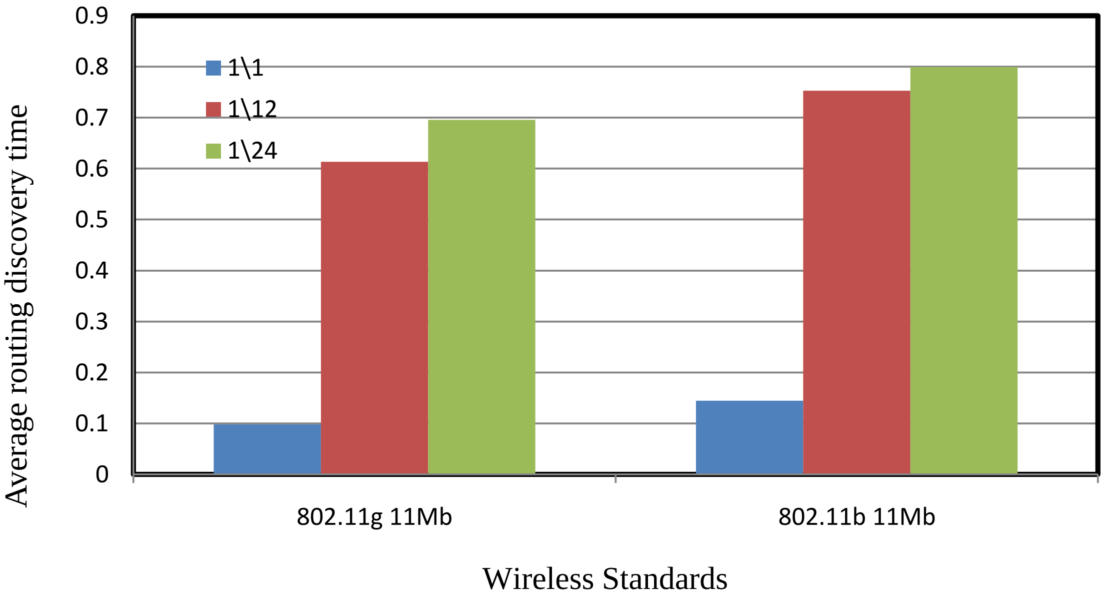


Figure 6.3: Average Routing Discovery TimeVersus Different Wireless Standard 802.11g and 802.11b for AODV Protocol.

In Figure 6.3we can see the average routing discovery time compared with 802.11g and 802.11b when the data rate is 11 Mbps. We observe that the values in 1/24,1/12 behave the same even with the increasing number of nodes. It means that route discovery time needs too much time to find the path between source node and destination node, For this reason 1/24 has the highest route discovery time as compared to 1/1 that has the least value in route discovery time. It means that the destination node does not need more time to find the route because in this case we have one server and one client.

Table 6.4:Simulation Results of Average HTTP Object Response Time for 802.11g and 802.11b Standards with AODV Protocol.

802.11g data rate Mb/s	HTTP Object Response Time		
	1\1	1\12	1\24
802.11g 11Mb	0.050	0.182	0.465
802.11b 11Mb	0.071	0.311	0.959

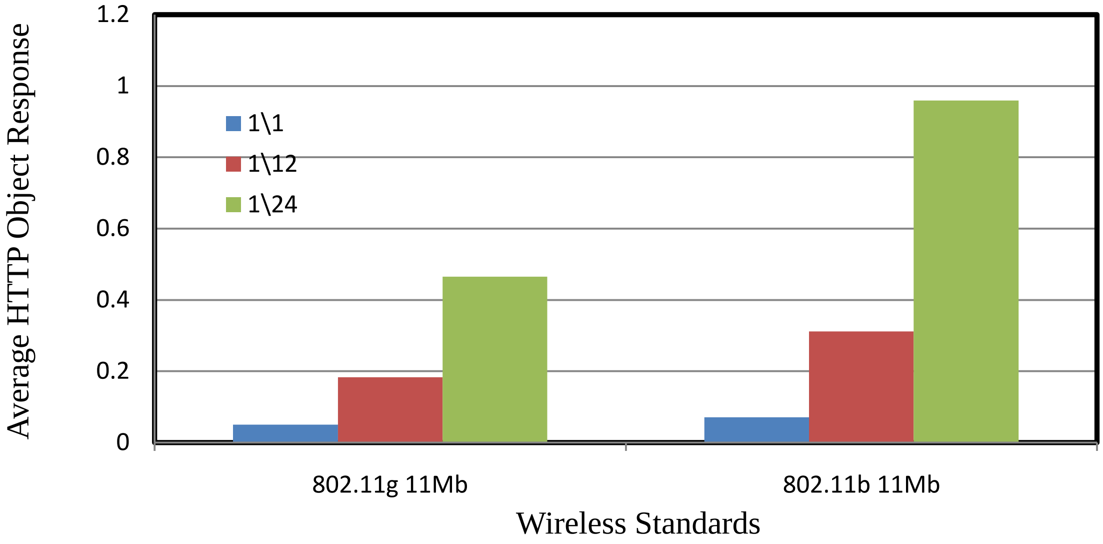


Figure 6.4:Average HTTP Object Response Versus Different Wireless Standard 802.11g and 802.11b for AODV Protocol

In Figure 6.4 we can see the average HTTP object response analyzed and compared with 802.11g and 802.11b when the data rate is 11Mbps. We observe that when the wireless standards is 802.11b (11Mbps), network topology 1/24 has the highest value of the HTTP object response while the 1/1 has the least value. It means that HTTP object response time depends on the bandwidth and enough time for browsing. It appearsthatin 1/24 where we have 24 clients in network topology we have alot of HTTP object, so it needs time for browsing.

Table 6.5:Simulation Results of Average Media Access Delay for 802.11g and 802.11b Standards with AODV Protocol.

802.11g data rate Mb/s	Media Access Delay		
	1\1	1\12	1\24
802.11g 11Mb	0.001	0.003	0.006
802.11b 11Mb	0.002	0.005	0.012

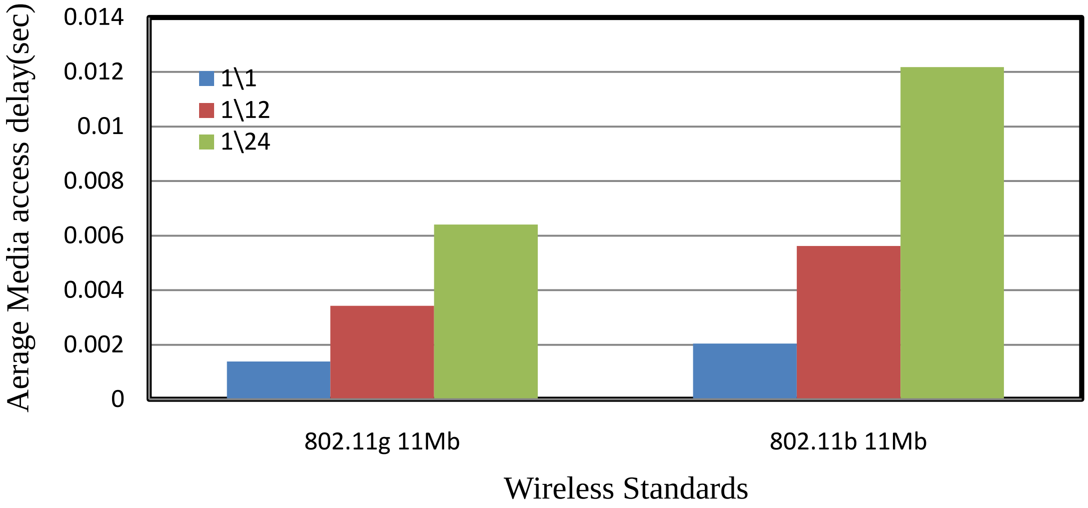


Figure 6.5:Average Media Access Delay Versus Different Wireless Standard 802.11g and 802.11b for AODV Protocol

In Figure 6.5 we can see the average media access delay analyzed and compared with 802.11g and 802.11b when the data rate is 11 Mbps. We observe that when the wireless standards is 802.11b(11Mbps), network topology 1/24 has the higher media access delay as compared to 1/1 that has the lower value. It means that the nodes need too much time to transmit packets from one node to another.So that when you increase the number of hops it may lead to an increase in media access delay.

Table 6.6:Simulation Results of Average Retransmission Attempts (Packets) for 802.11g and 802.11b Standards with AODV Protocol.

802.11g data rate Mb/s	Retransmission Attempts		
	1\1	1\12	1\24
802.11g 11Mb	0.331	0.385	0.418
802.11b 11Mb	0.301	0.373	0.403

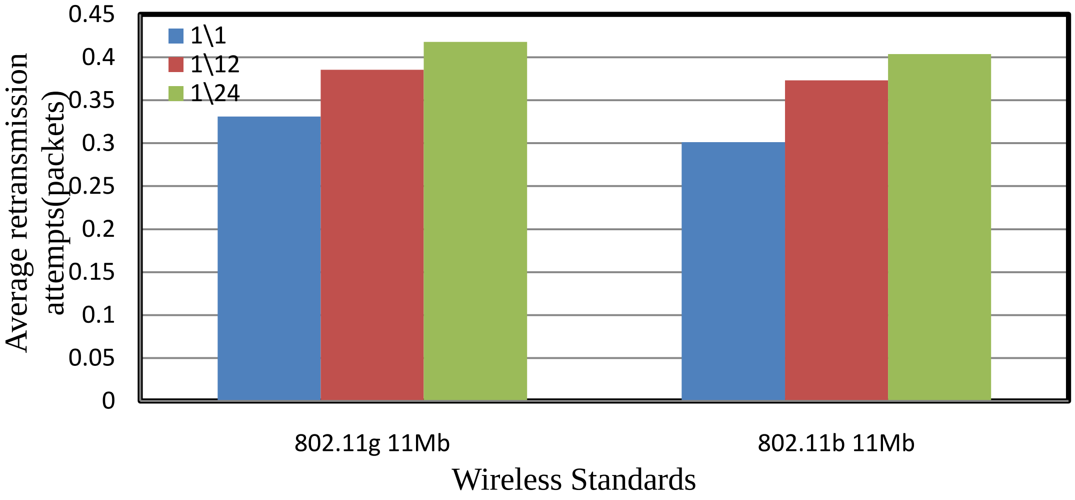


Figure 6.6: Average Retransmission Attempts (Packets)Versus Different Wireless Standard 802.11g and 802.11b for AODV protocol

In Figure 6.6 we can see the average retransmission attempts analyzed and compared with 802.11g and 802.11b with data rates 11Mbps. When the wireless standards is 802.11g (11Mbps), network topology 1/24 has the highest value compared with 1/1 havingthe lowest value, because 1/24 has a loss in packet while 1/1has no loss in packet, so the 1/24 has the higher retranmission because we have 24 clients works in the netwok.

Table 6.7:Simulation Results ofAverage Throughput for 802.11g and 802.11b Standards with AODV Protocol.

802.11g data rate Mb/s	Throughput		
	1\1	1\12	1\24
802.11g 11Mb	539409.626	1691439.073	2343734.533
802.11b 11Mb	537768	1489968.153	1859979.42

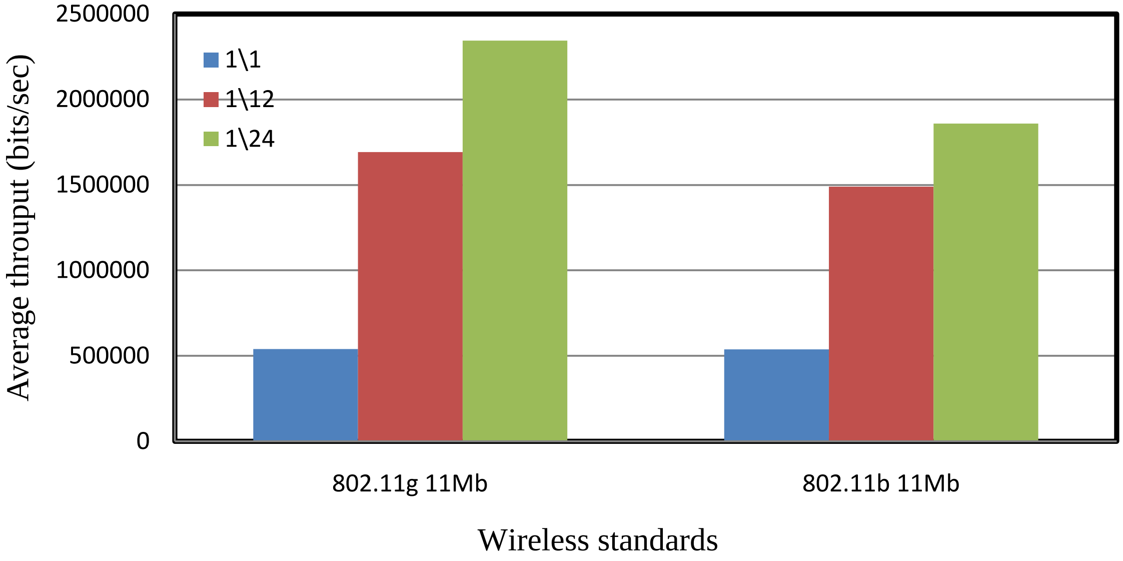


Figure 6.7: Average ThroughputVersus Different Wireless Standard 802.11g and 802.11b for AODV Protocol

In Figure 6.7 we can see the average throughput analyzed and compared with 802.11g and 802.11b with data rates 11Mbps. Network topology 1/24 has higher throughput than 802.11g. It means that this case is better than another case because the average number of packet are successfully received by the receiver from the sender and there is no loss of packets between source and destination. Also, 802.11g has a good bandwidth as compared to 802.11b.

Category2

In category2, a network model is designed with mobile nodes in OPNET 17.1 modeler for AODV routing protocol.Also, a comparison is made between 802.11g with different data rates (11, 24, 54) MB/s. We have to study the contact of these mobile nodes on MANET routing protocol performance using HTTP heavy browsing. All scenarios contain 25 nodes with the speed of 1m/s for AODV routing protocol in the Campus having the area of 1000 x 1000 meters. The attributes of nodes and server Ad hoc routing parameters are set with respect to required protocol. The simulation results of routing protocols are analyzed according to the number of hops, route discovery time, HTTP object response time, media access delay, retransmission attempts and throughput. For the design networks the simulation time is 300 seconds.

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.

Table 6.8:Simulation Results of Average Number of Hops for 802.11g Standards with AODV Protocol.

802.11g data rate Mb/s	Number of Hops per route		
	1\1	1\12	1\24
11	1.741	2.417	3.503
24	1.796	2.584	3.631
54	1.836	2.677	3.685

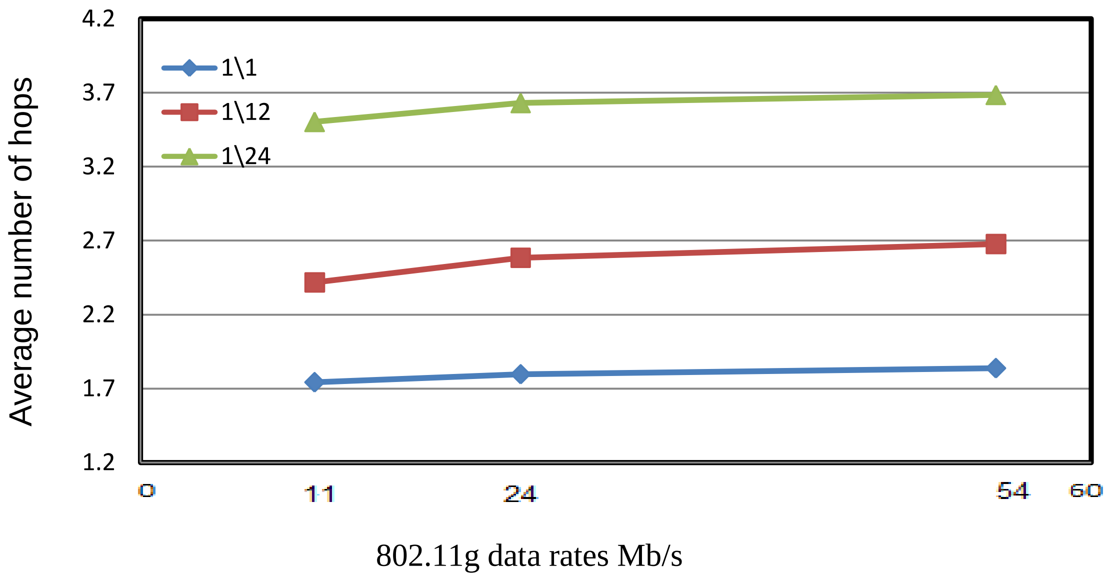


Figure 6.8: Average Number of Hops Versus Wireless Standard 802.11g with Different Data Rates for AODV Protocol

In Figure 6.8 we can see the average number of hops analyzed and compared with 802.11g that has different data rates. 1/24 has the highest number of hops when the data rate is 24 Mbps because the server sent 24 request to 24 client, For this reason 1/24 has the maximum number of hops and the traffic between node increase. Also in other cases 802.11g (11Mb) and 802.11g (54Mb) have the highest number of hops when the network is 1/24 with this rate is decreased gradually especially in 1/12. So the number of hops depends on the number of clients

Table 6.9:Simulation Results of Average Route Discovery Time for 802.11g Standards with AODV Protocol.

802.11g data rate Mb/s	Route Discovery Time		
	1\1	1\12	1\24
11	0.098	0.613	0.695
24	0.095	0.479	0.445
54	0.287	0.430	0.353

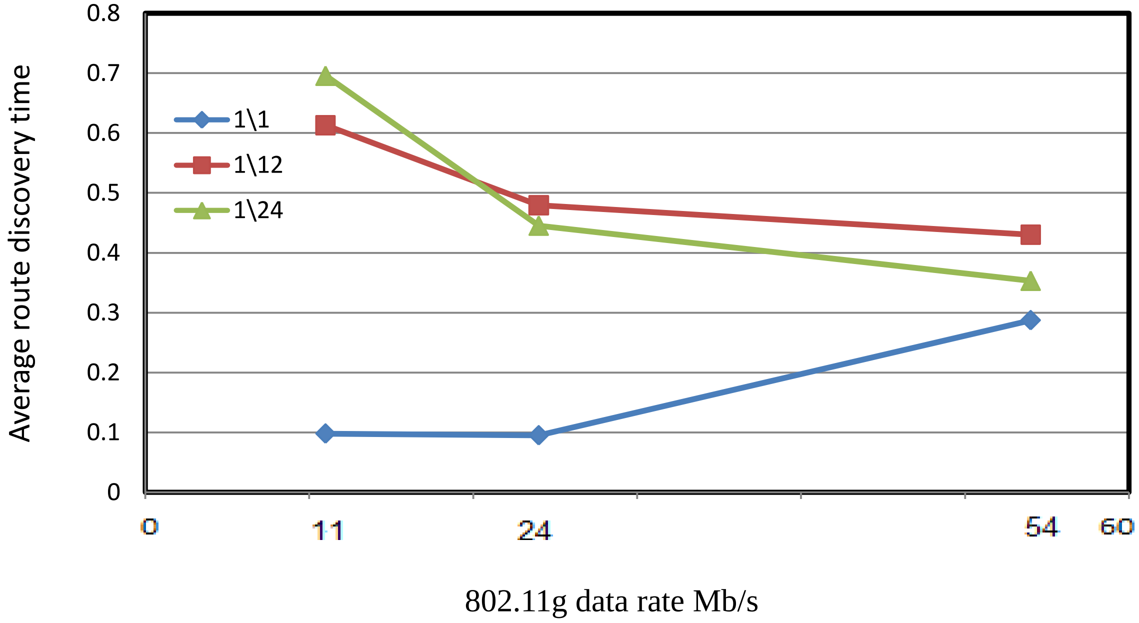


Figure 6.9:Average Route Discovery Time Versus Wireless Standard 802.11g with Different Data Rates for AODV Protocol

In Figure 6.9 we can see the average route discovery time analyzed with 802.11g in different data rates. 1/24 has the highest route discovery timewith a data rate of (11Mbps). It means that route discovery time needs much time to find the path between source node and destination. 1/1has least route discovery time when the data rate (11Mb), whichmeans that the destination node does not need more time to find the route because in this case we have one server and one client.

Table 6.10:Simulation Results of Average HTTP Object Response Time for 802.11g Standards with AODV Protocol.

802.11g data rate MB/s	HTTP Object Response Time		
	1\1	1\12	1\24
11	0.050463031	0.182939216	0.465625307
24	0.025123434	0.074801812	0.112662805
54	0.018716506	0.048504298	0.081052557

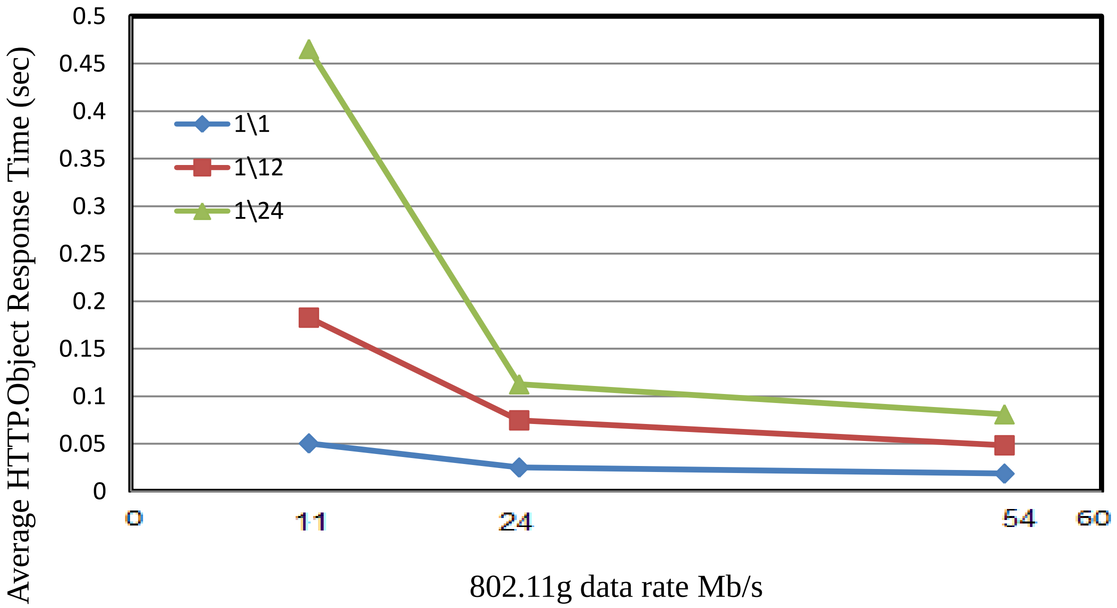


Figure 6.10: Average HTTP Object Response Time Versus Wireless Standard 802.11g with Different Data Rates for AODV Protocol

In Figure 6.10 we can see the average HTTP object response time analyzed with 802.11g in different data rates. 1/24 has a higher value when the data rate is (11Mb) as compared to other cases that have low valuesin near proximity of each other. The reason for thisis thatwhen the data rates increase the HTTP object response time, will decrease depending on the bandwidth and given enough time for browsing.

Table 6.11: Simulation Results of Average HTTP Page Response Time for 802.11g Standards with AODV Protocol.

802.11g data rate MB/s	HTTP Page Response Time		
	1\1	1\12	1\24
11	0.050	0.247	0.339
24	0.025	0.224	0.301
54	0.018	0.176	0.227

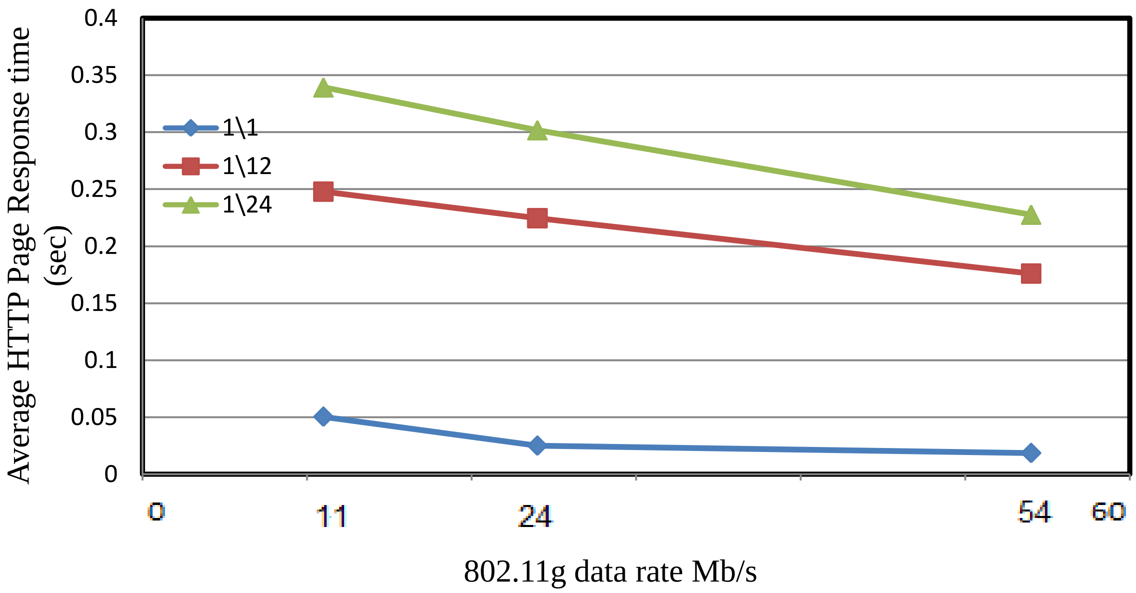


Figure 6.11:HTTP Page Response Time Versus Wireless Standard 802.11g with Different Data Rates for AODV Protocol.

In Figure 6.11 we can observe the average HTTP page response time analyzed with 802.11g in different data rates. 1/24 has a higher value when the data rate is (11Mb) because it needs too much time for browsing. Also,these values are decreased gradually, especially in 1/1,the reason being that when we have one server and one client does not need to time. So that, when the data rate increase the average HTTP page response time decrease and the bandwidth will decrease.

Table 6.12:Simulation results of average Media access delay for 802.11g standards with AODV protocol.

802.11g data rate MB/s	Media access delay		
	1\1	1\12	1\24
11	0.001	0.003	0.006
24	0.0007	0.002	0.003
54	0.000703	0.001	0.003

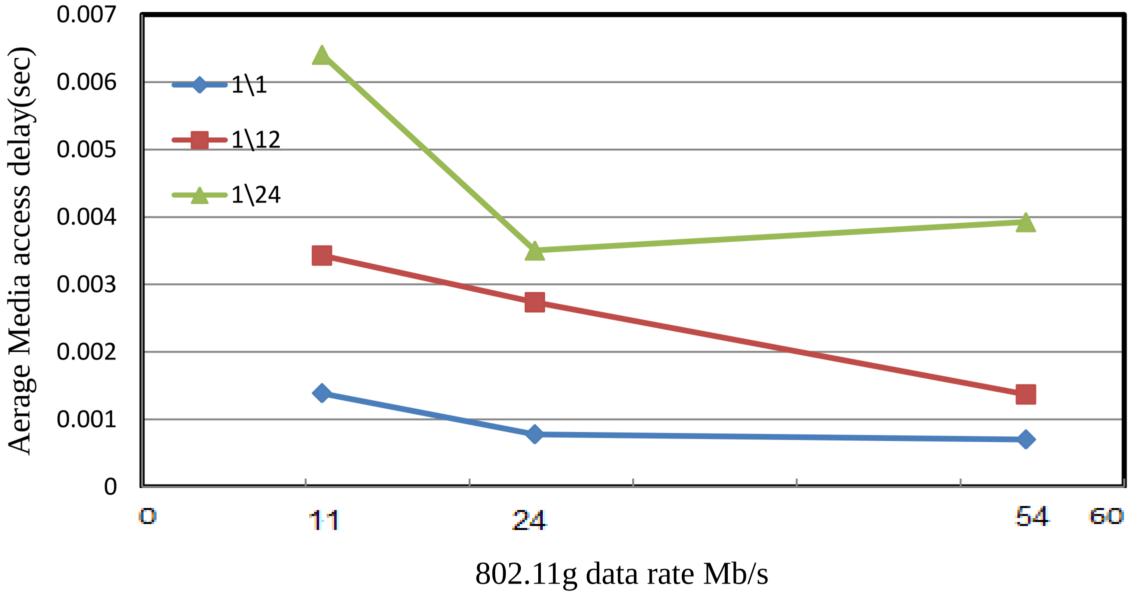


Figure 6.12:Average Media access delay versus wireless standard 802.11g with different data rates for AODV protocol

In Figure 6.12 we can see the average media access delay analyzed and compared with 802.11g in different data rates.We observe thatwhen the data rate is (11Mbps), network topology 1/24 has the higher media access delay as compared to 1/1, that has the lower value. It means thatthe nodes need too much time to transmit packets from one node to another, so any increase in the data rate is due to adecreasein media access delay.

Table 6.13:Simulation results of average Retransmission attempts (packets) for 802.11g standards with AODV protocol.

802.11g data rate MB/s	Retransmission attempts		
	1\1	1\12	1\24
11	0.331	0.385	0.418
24	0.251	0.302	0.318
54	0.229	0.238	0.301

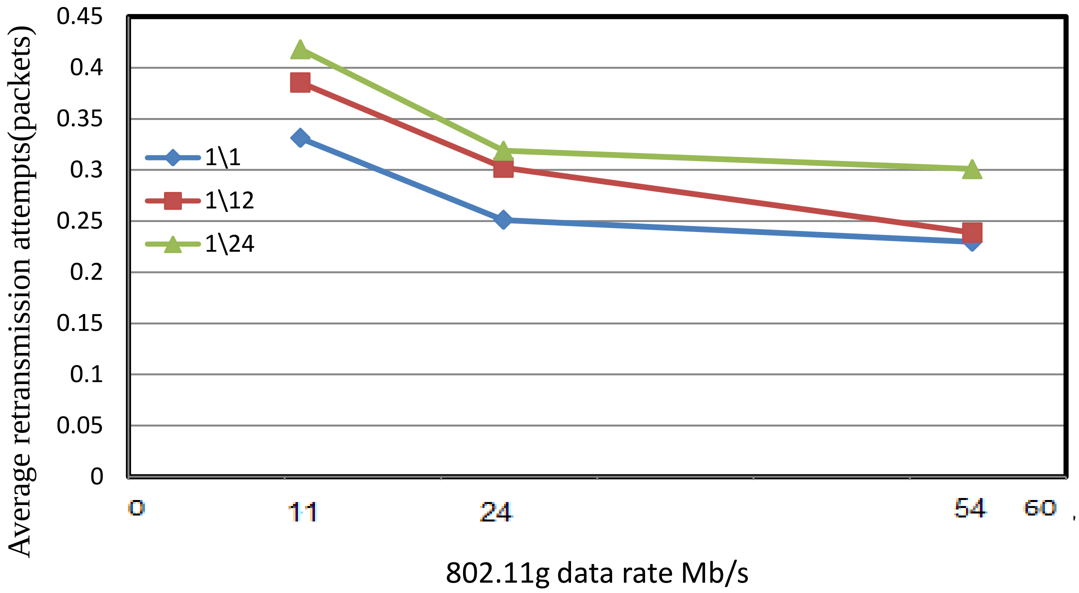


Figure 6.13:Average Retransmission attempts (packets) versus wireless standard 802.11g with different data rates for AODV protocol

In Figure 6.13 we can see the average retransmission attempts analyzed with 802.11g in different data rates. When the data rates is (11Mb), the network topology1/24,has the highest value as compared to 1/1 that has the lowest value.In three cases above the retransmission packet decreased when the data rate increased. So the number of retransmission packets depends on the data rates. 1/1 has the lowest value because in this case there is no loss in packet as compared to 1/24 that has higher retransmission because that has loss in packet.

Table 6.14:Simulation results of average Throughput for 802.11g standards with AODV protocol.

802.11g data rate Mb/s	Throughput		
	1\1	1\12	1\24
11	539409.626	1691439.073	2343734.533
24	577180.04	2171878.567	3529255.553
54	617577.64	2335747.193	3651725.653

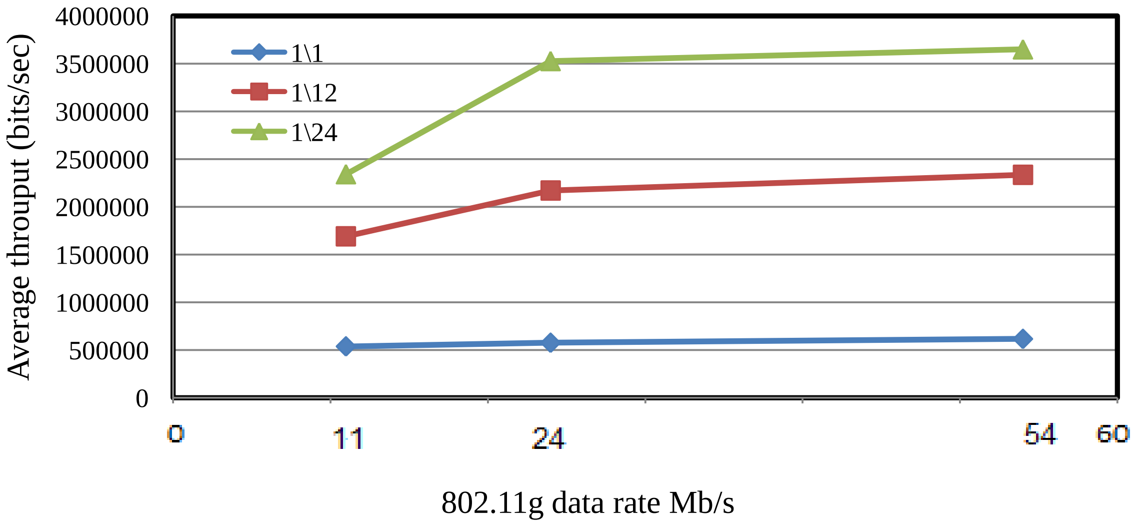


Figure 6.14:Average Throughput versus wireless standard 802.11g with different data rates for AODV protocol

In Figure 6.14 we can see the average throughput analyzed with and compared with 802.11g in different data rates. 1/24 has the higher throughput when the data rate is (54Mbps). It means that this case is better than other cases because the average number of packet are successfully received by the receiver from the sender and there is no loss in packetbetween source and destination. So that, when the data rates increase the average throughput will increase.

Table 6.15: Comparison of Parameter with [28]

Parameter	**Our work**	**[28]**
Application type	HTTP	FTP
Message size	1000 bytes	256 bytes
Routing protocol	AODV	DSR
Application Start time	Constant 10 (sec)	Constant 5 (sec)
Profile start time	Constant 5 (sec)	Constant 10 (sec)

Table 6.16 : Comparison between our work and [28] when there is one server and one client in the network

Performance metric	**Our work**				**[28]**			
	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	1.741	1.796	1.836	1.901	1.697	1.806	2.373	1.817
Route discovery time (sec)	0.098	0.095	0.287	0.144	0.008	0.006	0.010	0.010
Media access delay (sec)	0.001	0.0007	0.0007	0.002	0.0006	0.0004	0.0004	0.0014
Retransmission attempts (Packets)	0.331	0.251	0.229	0.301	0.172	0.156	0.145	0.051
Throughput (bit/sec)	539409	577180	617577	537768	10384	10472	10523	10261

Table 6.16, shows a comparison of our results with [28], when there is 1 server and 1 client in the network according to the performance metrics: number of hops per route, route discovery time, media access delay, retransmission attempts and throughput. Also, we have analyzed 802.11b and 802.11gwithdifferent data rates (11,24,54)Mbps. In [28],FTP application is used with DSR routing protocol. In our work and [28], we can see the average number of hops that have higher values in [28] as compared to our work that has lower values.[28] has the lower values of route discovery time with compared to our work that has higher values because it needs much time to discover the path between source and destination. [28] has the higher values of media access delay as

compared to our work that has lower values because of [28] that needs much time to prepare nodes before sent packets to the link. In this study,we can see the average retransmission attempts that has the higher valuesas compared to [28], it means when the data rates increase the retransmission will decrease. Also, throughput for our work in all cases has the higher values than [28], it appears for us the maximum number of packets that are successfully received by the receiver from sender.

Table 6.17:Comparison between our work and [28] when there is 1 server and 12 clients in the network

Performance metric	**Our work**				**Ref[28]**			
	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	2.417	2.584	2.677	2.420	2.202	2.313	2.672	2.312
Route discovery time (sec)	0.613	0.479	0.430	0.753	0.50	0.44	0.54	0.072
Media access delay (sec)	0.003	0.002	0.001	0.005	0.009	0.006	0.005	0.017
Retransmission attempts (Packets)	0.385	0.302	0.238	0.373	0.297	0.263	0.252	0.200
Throughput (bit/sec)	1691439	2171878	2335747	1489968	127803	218820	316883	117112

In the Table 6.17, we have comparedour work with [28], when there is 1 server and 12 clients in the network according to the performance metrics: number of hops per route, route discovery time, media access delay, retransmission attempts and throughput. Also, we analyzed 802.11b and 802.11gwithdifferent data rates (11,24, 54)Mbps. In [28],FTP application is used with DSR routing protocol. In [28] where the application is FTP that is used with DSR routing protocol. In a comparison of this study and [28], we can see the average number of hops that has higher values in our work as compared to [28] that has lower values. [28] has the lower values of route discovery time with compared to our work that hashigher values because it needs much time to discover the routes between stations. [28] has the higher values of media access delay as compared to our work that have lower values because in [28] need much time to prepare nodes before sent packets to the link. We can see the average retransmission attempts that have the higher valuesin ourworkas compared to [28] that have lower values, it means in this study, retransmission will decrease by increasing data rates. Throughput for our work in all cases has higher values than [28], it appears for us the maximum number of packet that are successfully received by the receiver from sender.

Table 6.18: Comparison between our work and [28] when there is 1 server and 24 clients in the network

Performance metric	Our work				[28]			
	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	3.503	3.631	3.685	3.358	2.581	2.939	3.512	2.716
Route discovery time (sec)	0.695	0.445	0.353	0.799	0.076	0.070	0.096	0.0128
Media access delay (sec)	0.006	0.003	0.002	0.12	0.021	0.012	0.011	0.037
Retransmission attempts (Packets)	0.418	0.318	0.301	0.403	0.365	0.330	0.317	0.220
Throughput (bit/sec)	2343734	3529255	3651725	1859979	249234	368185	571878	232077

In the Table 6.18, we have comparedour work with [28],when there is 1 server and 24 clients in the network according to the performance metrics: number of hops per route, route discovery time, media access delay, retransmission attempts and throughput. We analyzed 802.11b and 802.11gwithdifferent data rates (11,24, 54)Mbps. In [28] FTP application is used with DSR routing protocol. In [28] where the application is FTP that is used with DSR routing protocol. In our work and [28], we can see the average number of hops that have higher valuesin my work as compared to [28] that have lower values. [28] has the lower values of route discovery time with compared to our work that have higher values because is need much time to discover route between stations. [28] has the higher values of media access delay as compared to our work that has lower values because in [28] it needs much time to prepare nodes before sent packets to the link. We can see the average retransmission attempts that has the higher values in ourwork as compared to [28] that has lower values, it means retransmission in our work will decrease by increasing data rates. Also, throughput for our work in all cases has the higher values than [28], it appears for us the maximum number of packet that are successfully received by the receiver from sender.

6.2 Confidence Intervals

A confidence interval gives an estimated range of values which is likely to include an unknown population parameter, the estimated range being calculated from a given set of sample data.

If independent samples are taken repeatedly from the same population, and a confidence interval calculated for each sample, then a certain percentage (confidence level) of the intervals will include the unknown population parameter. Confidence intervals are usually calculated so that this percentage is 95%, but we can produce 90%, 99%, 99.9% (or whatever) confidence intervals for the unknown parameter.

The purpose of taking a random sample from a lot or population and computing a statistic, such s the mean from the data, is to approximate the mean of the population [29].

Table 6.19: Average values and 95% confidence intervals of the performance metrics for AODV with 802.11g(11Mbps)

Metric	**Wireless standard 802.11g (11Mbps)** **With different number of Client and intermediate**		
	1s/1c	**1s/12c**	**1s/24c**
Number of hops per route	2.741 ± 0.421	3.417 ± 0.175	5.503 ± 0.263
AODV .Route Discovery Time	0.098 ± 0.061	0.613 ± 0.084	0.695 ± 0.091
HTTP .Object Response Time (sec)	0.050 ± 0.004	0.182 ± 0.074	0.465 ± 0.181
HTTP .Page Response Time (sec)	0.096 ± 0.007	0.247 ± 0.005	0.339 ± 0.015
Wireless LAN .Media Access Delay (sec)	0.001 ± 3.912	0.003 ± 0.0006	0.006 ± 0.0007
Wireless LA N .Retransmission Attempts (packets)	0.331 ± 0.015	0.385 ± 0.020	0.418 ± 0.251
Wireless LAN .Throughput (bits/sec)	539409.6 ± 224.460	1691439 ± 189590.1	2343735 ± 64487.87

Table 6.20: Average values and 95% confidence intervals of the performance metrics for AODV with 802.11g(24Mbps).

Metric	**Wireless standard 802.11g (24Mbps)** **With different number of Client and intermediate**		
	1s/1c	**1s/12c**	**1s/24c**
Number of hops per route	2.796 ± 0.132	3.584 ± 0.127	5.631 ± 0.208
AODV .Route Discovery Time	0.095 ± 0.090	0.479 ± 0.155	0.445 ± 0.042
HTTP .Object Response Time (sec)	0.025 ± 0.001	0.074 ± 0.002	0.112 ± 0.016
HTTP .Page Response Time (sec)	0.050 ± 0.006	0.224 ± 0.032	0.301 ± 0.004
Wireless LAN .Media Access Delay (sec)	0.0007 ± 5.056	0.002 ± 0.0022	0.003 ± 0.0002
Wireless LA N .Retransmission Attempts (packets)	0.251 ± 0.035	0.302 ± 0.039	0.318 ± 0.015
Wireless LAN .Throughput (bits/sec)	517180 ± 55250.45	2171879 ± 405542.1	3529256 ± 120435.1

Table 6.21: Average values and 95% confidence intervals of the performance metrics for AODV with 802.11g(54Mbps).

Metric	**Wireless standard 802.11g (54 Mbps)** **With different number of Client and intermediate**		
	1s/1c	**1s/12c**	**1s/24c**
Number of hops per route	2.436 ± 0.618	3.277 ± 0.894	5.385 ± 1.069
AODV .Route Discovery Time	0.264 ± 0.267	0.430 ± 0.247	0.353 ± 0.047
HTTP .Object Response Time (sec)	0.018 ± 0.001	0.048 ± 0.019	0.081 ± 0.022
HTTP .Page Response Time (sec)	0.043 ± 0.011	0.176 ± 0.101	0.227 ± 0.057
Wireless LAN .Media Access Delay (sec)	0.0007 ± 0.0002	0.0013 ± 0.0005	0.003 ± 0.002
Wireless LA N .Retransmission Attempts (packets)	0.229 ± 0.049	0.238 ± 0.042	0.301 ± 0.041
Wireless LAN .Throughput (bits/sec)	417577.6 ± 209682.1	2035747 ± 782175.1	3451726 ± 883290.2

Table 6.22: Average values and 95% confidence intervals of the performance metrics for AODV with Number of Nodes 25 nodes with wireless standard 802.11b (11Mbps)

Metric	**Wireless standard 802.11b (11Mbps) With different number of Client and intermediate**		
	1s/1c	**1s/12c**	**1s/24c**
Number of hops per route	2.901194 ± 0.364528	3.420501 ± 0.235471	5.358062 ± 0.191236
AODV .Route Discovery Time	0.144852 ± 0.021957	0.753034 ± 0.188825	0.799217 ± 0.060562
HTTP .Object Response Time (sec)	0.071086 ± 0.005904	0.311564 ± 0.127176	0.95941 ± 0.134719
HTTP .Page Response Time (sec)	0.130781 ± 0.010556	0.249798 ± 0.010686	0.34405 ± 0.019406
Wireless LAN .Media Access Delay (sec)	0.002036 ± 1.750105	0.005622 ± 0.001347	0.012176 ± 0.000822
Wireless LA N .Retransmission Attempts (packets)	0.301085 ± 0.016486	0.37306 ± 0.022061	0.403585 ± 0.010115
Wireless LAN .Throughput (bits/sec)	537768 ± 1449.774	1489968 ± 116695.9	1859979 ± 99058.87

Chapter 7

CONCLUSION

In this thesis, we evaluate and analyze the performance of IEEE 802.11b and 802.11g standards on MANETs network using routing protocolAODV focusing on metrics Number of hops,Route discovery time, HTTP object response time, HTTP page response time, Retransmission,Media access delay and Throughput. Different data rates were used (11 Mbps, 24 Mbps and 54 Mbps) over HTTP heavy browsing. Different types of simulation were created using OPNET simulator version 17.1.

Simulation results show that greater number of hops used when the network topology is 1/24 (1 Server / 24 Client) as compared to other cases. Also Average route discovery time has the highest value when the network is 1/24. In the case of HTTP object response time 802.11b (11Mbps) has the greater value in all network topology cases (1/1, 1/12 and 1/24) as compared to 802.11g (11Mbps). On the other hand, results of metrics HTTP page response time, Retransmission attempts, Media access delay and Throughput show that the network 1/24 has the largest value and the media access delay increased depending on the number of clients. Using standard 802.11g with different data rates (11Mbps, 24Mbps and 54Mbps), the results are different according to the used metrics. It is concluded from the simulation results that; Average retransmission attempts of 802.11g is decreased by increasing the data rates of network. Additionally, the peak value of retransmission attempts is where 24 clients are communicating with server for both standards 802.11b and 802.11g. Additionally, throughput of both standards are increased by increasing the number of nodes that are communicating with the server.

Finally, values of used metrics increase gradually when the number of clients increase. In addition, throughput is increased in 802.11g with different data rates by increasing data rates and also for other performance metrics.

REFERENCES

[1] N. Islamkhan and R. Ahmed. "Simulation Based Performance Evaluation of Routing Protocols and TCP Variants in Mobile Ad hoc Networks." M.A. thesis, Blekinge Institute of Technology, Sweden, 2010.

[2] [Online]. Available: http://datatracker.ietf.org/wg/manet/charter/[Accessed:May 10,2010]

[3] E. Barkhodia and P. Singh. “Performance Analysis of AODV using HTTP traffic under Black Hole Attack in MANET”, Computer Science & Engineering: An International Journal (CSEIJ), Vol.2, No.3, 99-108 (2012).

[4] P. Singh, E. Barkhodia, G. Walia. “Performance Study of Different Routing Protocols (OLSR,DSR, AODV) Under Different Traffic Loads and with Same Number of Nodes in MANET using OPNET”, IJECT, Vol. 3, No.1, 155-157 (2012).

[5] N. Krishnan, M. Benjula, D.Sumathy. “Performance Analysis of MANET (WLAN) Using Different Routing Protocols in Multi service Environments-An Quantitative Study”, Int. J. Advanced Networking and Applications, Vol. 3, No.2, 1076-1079 (2011).

[6] A. Ghosh, A. Lasebae, E. Ever. “Performance Evaluation of Wireless IEEE 802.11(b) used for Ad hoc Networks in an ELearning Classroom Network”, Middlesex University, London, (2008).

[7] L. Komar, “Scalability Performance of AODV, TORA and OLSR with Reference to Variable Network Size”,IJERA, Vol. 2, 087-092 (2012).

[8] R. K. Nadesh, D. Sumathy, and M. B. Benjula, "Performance Analysis of MANET (WLAN) Using Different Routing Protocols in Multiservice Environments-An Quantitative Study", Int. J. Advanced Networking and Applications, Vol. 3, No.2, 1076-1079 (2011).

[9] M.izaz, “Transmission control protocol (TCP) Performance Evaluation in MANET” Mar 2009.
[Online]. Available:
http://www.bth.se/fou/cuppsats.nsf/all/72446dc2870fc690c125757d0037c9fe/$file/Iaz_Master_Thesis%2019march.pdf [Accessed: Mar 08.2010].

[10] M. R. Akhavan. " Study the Performance Limits of IEEE 802.11 WLANs." M.A. thesis, Lulea University of Technology, Sweden, 2006.

[11] F. Akyildiz, X. Wang , W. Wang, “*Wireless MESH Networks: A survey*”, Broadband and Wireless Networking Lab, School of Electrical and Computer Engineering, Georgia,2005.

[12] S. I. H. Shah and S. H. Shaheed. " *Performance Evaluation of MANET Routing Protocols.*" M.A. thesis, Blekinge Institute of Technology, Sweden, 2011.

[13] S. Basagni, M. Conti, S. Giordana and I. Stojmenovic,*Mobile Ad Hoc Networking*. 1st ed. Wiley Publications, 2004

[14] S. K. Sarkar, T. G. Basavaraju, and C. Puttamadappa,*Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications*. 1st ed. Auerbach Publications, 2008.

[15] A. Qayyum, L. Viennot, and A. Laouiti,"Multipoint relaying: An efficient technique for flooding in mobile wireless networks", INRIA research report RR-3898, 2000, http://citeseer.ist.psu.edu.

[16] S. Liu Wu and Y. Chee Tseng, Wireless*Ad Hoc Networking*. 1st ed. Auerbach Publications, 2007.

[17] Ed. Tittel, M. Hossain, M. Heydari "*Schaum's Outline* ***Of*** *Computer Networking",* McGraw-Hill Companies,39 (2002).

[18] S.A Thomas. "HTTP Essentials Protocol for secure,Scaleable Web Sites" Newyork: robert Ispen, 1-13 (2001).

[19] C. Perkins, B. R. E., and D. S., "Ad hoc On-demand Distance Vector routing," Request For Comments (Proposed Standard) 3561, Internet Engineering Task Force http://www.ietf.org/rfc/rfc3561.txt?number=3561, July 2003.

[20] A. S. Tanenbaum "Computer Networks", Prentice Hall India (PHI),
November 1998.

[21] P. Brenner"A Technical Tutorial on IEEE 802.11 Protocol," http://www.sss-mag.com/pdf/802_11tut.pdf.

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

[23] Y. Ravikumar and S. Chittamuru. " A Case Study on MANET Routing Protocols Performance over TCP and HTTP." M.A. thesis, Blekinge Institute of Technology, Sweden, 2010.

[24] M. W. Soomro, M. A. Memon, M. I. Abro. “Performance Analyses Of Routing Protocol inMANET with static and Mobile nodes using HTTP traffic”, IJECE, Vol. 1, No.2, 23-31 (2012).

[25] M. S. Gast, 802.11 Wireless Network : The Definitive Guide, Second Edition O' Reilly, April 2005.

[26] M. R. Akhan "Study the performance limit of IEEE 802.11 WLANs" Lulea University of Technology, Sweden, 2006.

[27] S. F. Medkiff, "Mobile Ad hoc Network Routing Protocols: Methodologies and Applications", Faculty of the Virginia Polytechnic Institute, USA 2004.

[28] M. D. Khorsheed, "Investigate performance of 802.11g and 802.11b Standards with DSR protocol using OPNET", M.A. thesis, Eastern Mediterranean University, North Cyprus, 2013.

[29] [Online]. Available: http://www.stats.gla.ac.uk..