PERFORMANCE EVOLUTION OF MANET ROUTING PROTOCOLS WITH VARIABLE FTP TRAFFIC LOAD AND VOIP APPLICATION

Md Iftekhar Mahmud Mozomder
ID: 11709013
Session: 2016-17
Dept. of ICT
Comilla University

Chapter 1

Introduction

Ad hoc network [1] is a grouping of mobile nodes that does not require a centralized access point or an existing architecture. It is an algorithm that is applied to the available infrastructure or the main access point. Each host typically runs in the form of an expert router.

MANET is a wireless self-configuring network in which nodes dynamically carry out mobility tasks associated with wired networks. Since nodes are truly mobile in MANET, regardless of direction, there is no stable network topology, which makes it very difficult to route traffic from source to destination. MANET routing protocols fall into a variety of types, including proactive, reactive, flow-oriented, adaptive, hybrid, hierarchical, geographical, power-aware, multicast, and many others [2]. Different routing protocols have been designed for each category in accordance with some particular domain needs. In general, proactive and reactive protocols are very important since they assist algorithms and applications.

Due to multi-hop routing and dynamic route calculation, a Mobile Ad hoc Network (MANET) presents a demanding environment for Voice over Internet Protocol (VoIP).

Ad hoc On-Demand Distance Vector (AODV) and Optimized Link State Routing (OLSR) are two routing protocols used in MANETs. The primary distinction between these two protocols is that OLSR is proactive and calculates all viable routes whether they are necessary or not, whereas AODV is reactive and searches for new routes as needed. Routing protocols are necessary for establishing communication between nodes, and each node must function as a router. For MANET, a number of routing protocols have been created and put into use. Temporally Ordered Routing Algorithm (TORA), Ad Hoc On-Demand Distance Vector Routing (AODV) [3], Dynamic Source Routing (DSR), etc. are some examples of these algorithms.

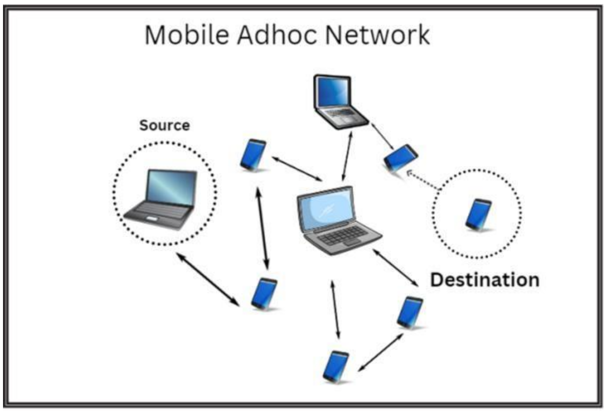


Fig 1.1: Mobile ad hoc network (MANET)

1.1 Properties of MANET

Here are a few MANET properties to consider:

Adaptive topologies: Because nodes are free to move in any direction, the network architecture is mostly made up of bidirectional linkages and is subject to change at any time. There may occasionally be a unidirectional link when the transmission powers of two nodes vary.

Connectivity with limited bandwidth and varying capacities: Infrastructure networks continue to have substantially greater capacity than wireless links.

Operating with energy restrictions: A MANET's nodes may use batteries or other non-renewable energy sources to power some or all of them. Energy conservation may be the most crucial system design optimization need for these nodes or devices.

Little physical protection: Compared to MANETs, wireless networks are often less at risk from physical security threats. The increased risk of eavesdropping, spoofing, and denial of service (DoS) attacks must be properly taken into account. In order to reduce security concerns, wireless networks frequently use a variety of link security methods currently available.

Less Human Involvement: They are dynamically independent because they require less human input to configure the network.

1.2 MANET's use cases

Particularly in industrial and commercial environments, including cooperative and mobile data sharing, ad hoc networks are used. Various military networking requirements for stable, IP-compliant data services will exist both now and in the future in mobile wireless communication networks, many of which are composed of highly dynamic independent topological segments. Global roaming, data rates appropriate for multimedia applications, and cooperation with other network designs are some of the advanced aspects of mobile ad hoc networks that are opening up new application possibilities.

Mesh wireless networks: A wireless mesh network (WMN) is a mesh network made up of nodes placed at each network user's location known as wireless access points (WAPs). Each node just needs to send as far as the next node, which decentralizes and streamlines the networking architecture. The wireless mesh network might or might not have an internet connection. The following are typical uses for wireless mesh networks, which are also known as a sort of wireless ad hoc network (WANET):

- Adding internet of things (IoT) connectivity to sensors, security systems, smart appliances, and monitoring systems.
- Use of free Wi-Fi made available by towns and municipalities.
- Setting up networks in communities in development where there is no infrastructure for internet wiring.
- Wi-Fi hotspots within the house.
- Wi-Fi and networking in mobile settings, including building sites.

Wireless Sensor Network: Sensors are useful tools that gather information on particular factors like noise, temperature, humidity, pressure, etc. To enable the collection of extensive amounts of sensor data, sensors are increasingly being wirelessly connected. We can utilize analytics processing to interpret a sizable sample of sensor data. As sensors may now be placed without fixed radio towers and create networks on the spot, wireless sensor network connectivity is built on the ideas of wireless ad hoc networks. One of the first projects at UC Berkeley was "Smart Dust," which involved connecting smart dust with tiny radios. Recently, academic research on mobile wireless sensor networks (MWSNs) has increased.

Military applications: Ad hoc/sensor networks are perfect for battlefield management because many military applications call for an instantaneous communications arrangement.

Telemedicine: When helping a vehicle accident victim in a remote location, a paramedic needs to access medical records (such X-rays) and may need the assistance of a surgeon through video conference for an emergency intervention. In fact, the paramedic might have to transport the patient's X-rays and the results of an additional diagnostic test directly from the accident site to the hospital.

Disaster management software: For instance, when a natural disaster strikes and the entire communication infrastructure is in disarray, these things can happen. As quickly as possible, communication needs to be established again.

Application for tele-geoprocessing: The combination of GPS, GIS (Geographical Information Systems), and high-capacity wireless mobile systems has allowed for the development of a new category of applications known as tele-geo processing.

Education via the internet: Due to the practical difficulty of delivering expensive last-mile wireline internet service to every user in these areas, educational possibilities are offered online or in remote locations.

Virtual Navigation: In a distant database, a large city's physical features, such as its streets, buildings, and other physical features, are graphically depicted. They might also be able to discover possible points of interest or "virtually" inspect the internal layout of a structure, including an emergency escape plan.

VANETs (vehicular area networks): For distributing emergency services and other information, this is a valuable and expanding ad hoc network application. Both urban and rural locations benefit from this. the exchange of basic and necessary data in a given situation.

1.3 Benefits of MANETs

- Because each node may function as both a router and a host, it is autonomous.
- separation from the main network management.
- Highly extensible and appropriate for future network hub additions.
- Self-configuring and self-healing nodes do not need human intervention.
- Because MANETs are decentralized networks, infrastructure is not needed.
- Decentralized networks are frequently more stable than centralized networks because information is transmitted using a multi-hop strategy. For instance, in a cellular

network, if a base station fails, coverage is lost; but, with a MANET, the possibility of a single point of failure is much reduced because data can travel over multiple path.

- Flexibility (mobile devices can be used to create an ad hoc network anywhere), scalability (you can instantly add more nodes to the network), and lower maintenance costs (you don't need to initially develop infrastructure) are further benefits of MANETs over fixed-topology networks.

1.4 The drawbacks of MANETs

- Resources are constrained due to numerous restrictions like noise, interference conditions, and other issues. There are no authorisation facilities.
- Data is sent between two sleeping nodes with a noticeable delay when there is high latency, and because there is insufficient physical security, they are more susceptible to attacks.

1.5 Objectives

- Using simulation to compare the performance of proactive, reactive and hybrid routing strategies.
- The primary goal of this thesis is to research, analyze, and contrast how various scenarios affect the performance of routing protocols such AODV, OLSR, and GRP utilizing OPNET Modeler with FTP traffic and VOIP.
- Consider performance metrics such as packet delivery ratio, end-to-end delay, throughput, network load, jitter, and Normalizing Routing Load when evaluating the effectiveness of the AODV, GRP, and OLSR routing protocols.

Chapter 2

Literature Review

The behavior of the AODV routing protocol was examined by Sharda Patel, Arunima Patel, and Ashok Verma utilizing various performance matrices with Black Hole attacks by various ranges of nodes and blackhole nodes. Their test results show that the AODV protocol performs well against black hole attacks [7].

The authors, H. Singh, H. Kaur, A. Sharma, and R. Malhotra, conducted study on a thorough analysis of a reactive technique that is frequently utilized. They employed the GRP protocol. Here, OPNET Modeler is employed. [9].

Researchers B. A. S. Roopa Devi, Dr. B. Prabhakara Rao, and T. Jagadeepak conducted AODV, DSDV, and DSR studies. Here, Network Simulator-2 is employed. Here, a variety of performance matrices are utilized. [10].

The DSDV and AODV protocols were studied by the authors, D. Kumar, A. Srivastava, and S. C. Gupta. Here, Network Simulator NS2 is employed. Here, the performance matrix for delay and throughput is assessed. For testing the effectiveness of the routing protocol, they alter the parameters packet size and time interval [13].

Proactive and reactive routing protocols were examined by the authors, Y. Bai, Y. Mai, and N. Wang. Overhead, throughput, and end-to-end delay are the performance parameters that are covered here. [14].

This section has examined a number of earlier studies on MANETs routing protocols.

In order to improve the performance of the upgraded AODV, Sherin Hijazi, Mahmoud Moshref, and Saleh Al-Sharaeh examined the blackhole attack. They conducted their study using the NS2 simulator. The results of their experiment show that it performs better than blackhole AODV [1].

A new protocol was tested by OTMANI Mohamed, EZZATI Abdellah, and FIHRI Mohammed. It functions like a black hole yet communicates like an AODV. They looked at a few situations using this new protocol to determine how blackhole attacks could cause more packet loss [3].

Blackhole attack performance has been compared by Karuna Dara. They take into account the AODV routing protocol in MANET in two separate circumstances for their research. The effectiveness of the AODV depends on both the number of malicious nodes and the location of each malicious node [4].

Different ad-hoc networks were used to model the impact of black holes on ns-2 by Y. M. Erten, Can Erkin Acar, and Semih Dokurer. Their stimulation results demonstrate that the packet loss was decreased by their improved AODV protocol [5].

In the beginning, Drs. Bipul Syam Purkayastha, Prodipto Das, and Rajib Das implemented a method that can identify and mitigate Black hole nodes in the MANET. They investigated a simulation implementation that used the effects of a black hole attack to explain network performance [6].

Table 2.1: List of Literature Reviews.

Sl. No.	Authors' Name	Used Routing Protocols	Measure of Network Performance
1	Saleh Al-Sharaeh, Mahmoud Moshref, and Sherin Hijazi.	OLSR	The rate of packet delivery, Jitter delay, end-to-end delay, and packet loss.
2	Asif Uddin Khan and others.	AODV	Packet delivery ratio and normalizing routing load.
3	Taher Delkesh and others.	AODV	PDR, packet loss rate, delay, routing load, and throughput.
4	Huaqiang Xu and others	AODV	Latency, PDR, NRL, and the ratio of rebroadcasts.
5	Ashadi Kurniawan and others.	DSDV, OLSR, and AODV	Throughput of received data, Packet Delivery Ratio, Transmitting Delay percent of lost packets.

Chapter 3

MANET Routing Protocol

3.1 MANET Protocol Category

In MANET, there are primarily three active routing protocols, which are as follows:

- Proactive
- Reactive and
- Hybrid routing protocol

3.1.1 Proactive or Table -driven Routing Protocol:

Table-driven routing protocols, commonly referred to as proactive routing methods. Every mobile node keeps a separate routing database that lists the paths to every potential destination mobile node. The mobile ad hoc network's topology is dynamic, hence these routing tables are updated periodically as and when the network topology changes. Its downside is that it has trouble with vast networks since keeping track of the routes to all potential nodes makes the routing table entries too big. The proactive routing algorithm entails the following three steps:

- Multipoint Relaying
- Link -State messages and route computation;
- Neighbor/Link Sensing

The existing table-driven or proactive protocols include Cluster-head Gateway Switch Routing Protocol (CGSR), Fish-eye State Routing Protocol (FSR), Destination-Sequenced Distance Vector (DSDV), and Optimized Link State Routing (OLSR) [9].

3.1.2 Reactive or on –demand Routing Protocol:

Also called as on-demand routing protocol, these include. In this type of routing, the path is only found when it is required. To accomplish route discovery, route request packets are disseminated over the mobile network. Its two primary components are route discovery and route maintenance.

Source routing and Hop-by-hop routing are two categories into which reactive protocols can be divided.

Each data packet in source-routed on-demand protocols carries the complete source and destination addresses. As a result, each intermediary node transmits these packets in accordance with the data stored in each packet's header [6]. This indicates that in order to transfer the packet to its destination, the intermediate nodes do not need to keep accurate routing information for each active route [6]. Additionally, nodes are not required to keep their neighbors connected by repeated beaconing messages.

The primary flaw of source routing systems is their poor performance in big networks [6]. There are two key causes for this. First, when each route has more intermediary nodes, the likelihood that the route would fail increases. Since each node can update its routing table when it receives updated topology information and transmit the data packets along newer and better routes, this technique has the benefit of being able to adapt routes to the dynamically changing environment of MANETs [6].

Reactive routing protocols come in a variety of forms, including Dynamic Source Routing (DSR), Ad-hoc On-Demand Distance Vector Routing (AODV), Temporarily Ordered Routing Algorithm (TORA), and Associativity-based Routing (ABR), among others.

3.1.3 Routing Protocol for Hybrid Networks

The benefits of reactive and proactive routing protocols are essentially combined. The source and destination mobile nodes' zones and positions are taken into account when these protocols adjust. Zone Routing Protocol (ZRP) is one of the most widely used hybrid routing protocols. After segmenting the network into several zones, the locations of the source and destination mobile nodes are tracked. Proactive routing is used to transmit the data packets between the source and destination mobile nodes if they are both located in the same zone. Additionally, reactive routing is employed to transmit the data packets between the source and destination mobile nodes if they are situated in separate zones. Zone Routing Protocol (ZRP) and Enhanced Interior Gateway Routing Protocol (EIGRP) are two examples of the various types of hybrid routing protocols.

3.2 The AODV, GRP, and OLSR Routing Protocol are described:

3.2.1 AODV (Ad-Hoc On Demand Vector Routing protocol)

It is an on-demand and reactive routing protocol. It is an expansion of the dynamic source routing protocol (DSR) and aids in eradicating some of its drawbacks. After route discovery, the source mobile node in DSR includes the whole path in the header of the data packet it delivers to the destination mobile node. As a result, as the size of the network grows, so does the length of the total path and the size of the header in each data packet, which slows down the entire network.

Ad-Hoc On Demand Vector Routing protocol was developed as a result. The primary distinction is in how the path is stored; with AODV Sourcenodes, each node does not maintain information about its previous and subsequent neighbors. Route maintenance and Route discovery are the other two phases of operation.

The AODV routing process has two stages. They are Maintenance of Route and route finding. Every node keeps a routing table that contains information about the network. Management of route tables is the focus of AODV. Reverse pointers maintain route information even for transitory paths.

Route Finding

When a source node wishes to interact with a destination node but lacks knowledge of the routing table, route discovery begins. By sending route request packets to its neighbors, the source node initiates the route discovery process. The following fields are included in the route request:

- The source address
- The source sequence number
- The broadcast id
- The final destination.
- The destination sequence number
- Hop number

Once the RREQ has reached them with a new enough path to reach them, the destination or intermediary node answers by unicasting an RREP packet back to the neighbor from whence it initially received the RREQ. As the RREP is routed back through the reverse path, nodes along the path accumulate forward route entries in their route tables that lead to the node from which the RREP originated. These forward route entries display the actual forward path. A route timer is attached to each route record, and if the timer is not used, the entry will be deleted [6]. Since the RREP is sent along the path chosen by the RREP, AODV only supports symmetric links.

Maintenance of Route

The AODV routing protocol uses an RERR packet, or the RERR from a broken communication link to the relevant routing source node, in the event of a link failure. If a node loses connectivity, the next hop node should be linked to the active use of the upstream node's damage to send unsolicited RERR packets. Next, the RERR packet is created with a new serial number and a hop count of 2. Even if it is in touch with the destination node, the source node must restart the route discovery procedure after getting the notification of broken links. In order to ensure the construction of a fresh, effective routing, it will at this point broadcast an RREQ packet for those who do not know the most recent location in the middle of the destination node to react.

Route Table Control

For each destination of interest, each mobile node in the network stores an item in its route database. There are the following details in each entry:

The following information is provided for this route:

- Destination
- Next hop
- Number of hops
- Destination sequence number
- Route table entry expiration time

When a route data is used to send information from a source node to a destination node, the time out is rebooting to the current time and an active route timeout for each instance. If a new route is located, the comparison procedure for the destination grade quantity of the new route begins with the present route. The new route is only selected in this case if it has a lower metric to the destination and if the sequence quantities are the same. If not, the route with the highest sequence number is chosen as the new route. The node that needs to communicate during a link break must invalidate the existing route in the routing table entry. That node must direct the afflicted nodes to their intended locations and ascertain which neighbors this connection breaking can have an impact on. The route error message (RERR), which can be broadcast if there are many neighbors or unicasted if there is just one, can be sent by the node to the designated neighbors as a last resort.

Both benefits and drawbacks

The AODV routing protocol can handle a variety of data traffic levels as well as low, moderate, and somewhat high mobility rates. It is intended for mobile node networks (MANETs) with populations of tens to thousands of nodes. AODV has also been designed to reduce spread of control traffic and minimize overhead on data traffic in order to improve performance and scalability. With this protocol, routes are constructed as needed, destination sequence numbers are used to identify the most recent route to the destination, and the connection setup wait is reduced.

If the source sequence number is very old and the intermediate nodes have a higher but not the most recent destination sequence number, resulting in stale entries, this protocol's disadvantage of intermediate nodes can result in inconsistent routes. Heavy control overhead can also result from sending many RREP packets in response to a single RREQ packet. Another drawback of AODV is the needless bandwidth usage caused by the periodic beaconing. However, compared to other reactive protocols like DSR, the reactive distance- vector protocol's connection setup delay is rather significant and a lot longer.

Advancements of AODV

- Routes are created on demand, and the most recent route to the destination can be found using the destination sequence number.
- Even for nodes that are constantly moving, it supports packet transmissions for both unicast and multicast.
- It facilitates connection setup with less delay.
- The Hello messages, which are in charge of route maintenance, are constrained to prevent needless network overhead.

3.2.2 Optimized Link State Routing (OLSR)

OLSR is a proactive (table-driven) routing system, exchanging topology data often with other network nodes [19]. This protocol, which was created for mobile Ad hoc networks and is also used in WiMAX Mesh, is an optimization of the conventional link status protocol. Reduced transmission requirements result in smaller control packet sizes, which are the responsibility of the OLSR. With the aid of Multipoint Relays (MPRs), the primary objective of OLSR is to organize the control traffic overhead in the network [18]. The OLSR protocol's central principle is the MPR hypothesis. In the network, the source and destination routes are calculated using the MPR approach. Furthermore, by limiting the amount of packet transmissions, the MPRs enable a mechanism for flooding the control traffic [18]. When the information about the link state is broadcast in the network, they must be engaged in a different task. The task delivers the shortest routes to every destination in MANET after providing notifications for the link-state data for respective MPR selectors [18]. It is possible to prevent the problems that arise during packet transmission over a unidirectional network by selecting the path through the multipoint relays. The MPRs are distributed from symmetric or bi-directional one-hop nearby nodes [18].

OLSR employs the HELLO message, the Topology Control (TC) message, and the Multiple Interface Declaration (MID) message as three different forms of control messages. MANETs can decrease the maximum time interval while at the same time continuously maintaining safe routes to all destinations because of the benefits of these signals that are sent out on a frequent basis [18]. The OLSR protocol is improved for dense and large networks by this feature [19]. In a larger and denser network, the OLSR protocol can achieve greater optimization than the pure link state method [21]. The goal of OLSR is to construct a full distribution method that is devoid of central entities [18].

The OLSR interfaces and mobile nodes that are featured in the MANET are explained by the basic functionality [18]. It consists of the following elements:

- Neighbor discovery,
- Packet formatting, forwarding,
- MPR selection, MPR signaling,
- Topology control message diffusion,
- Route calculation, and
- Link sensing are some of the processes covered.

Benefits of OLSR

The following can be used to describe the benefits of OLSR:

- The average end-to-end delay is lower with OLSR. It is therefore utilized for applications that require the least amount of delay [22].
- The OLSR solution is simpler to use and does not require a centralized administrative system to manage its routing process [22].

- With its quick source and destination pair changes, OLSR improves the protocol's suitability for an ad hoc network [22].

3.2.3 GRP: GEOGRAPHIC ROUTING PROTOCOL

The proactive routing protocol GRP [4] uses the hop-by-hop kind of routing and performs regular frequency changes. In the worst situation, it completely floods and offers only one route. GRP routing involves a number of the stages shown below:

- Hello Messages are periodically sent in order to maintain the information about the neighboring nodes.
- Hello messages from neighboring nodes serve as evidence of local connectivity; if a hello message is not received within a predetermined time frame (known as the "neighbor expiry time"), link loss is suspected.
- To bootstrap the MANET network, all of the nodes engage in initial flooding.
- GPS positioning or flooding mechanisms are used to determine the position of nodes, and flooding is also used to handle position updates.
- To lessen the overhead caused by the floods, a fuzzy routing criterion is implemented.
- When nodes provide messages about position updates, the network is divided into different quadrants, and information is controlled by flooding method.
- GRP transfers packets to the target with the shortest distance in mind; nodes that receive packets send them to the nearest node by taking the shortest route. Any loops in the delivery of the packet to its destination are crossed.
- When a route is blocked, a backtracking technique is used, which causes packets to return to the previous hop before a new route is formed.

3.2.4 VOIP (Protocol for Voice over Internet)

VoIP is a relatively new technology that uses packet switched networks to transmit digital voice data. On Public Switched Telephone Network (PSTN) channels designed for voice, conventional voice telephony is transmitted in full duplex mode [VSMH02].

A coder/decoder (codec) is used in VoIP to compress and transform analog speech data to a digital format. The Transmission Control Protocol (TCP)/IP stack receives this stream of binary data and decodes it into a sequence of packets for network transmission [Wal05]. The IP packets are de-headered at the receiver before being delivered as a continuous bit stream to a suitable decoder [HPG05].

Chapter 4

Methodology

4.1 Design and implementation of simulations

Designing and implementing simulations is thought to be a crucial step in evaluating the effectiveness of the intended network. It is regarded as a taxing task in its current implementation. OPNET [Optimized Network Engineering Tool] is one of the most well-known network simulators to date. This product is not open source. OPNET requires a license in order to access permeation. It gives you a GUI. It includes preset models, protocols, algorithms, and standards. It is quite well documented, especially when employed for commercial purposes.

4.1.1 Features of the OPNET Modeler

- It exhibits adaptability. Additionally, it offers a simple graphical interface for viewing the outcomes.
- It is simple to evaluate new network model and architecture designs.
- The network behavior in diverse contexts is simple to comprehend.
- The network model and design are fully defined and readily available for user education and development.
- It is highly useful for analyzing the performance of current systems based on user needs.
- Because it offers a GUI-enabled virtual real-time environment, OPNET has a significant opportunity.
- OPNET is trustworthy and effective.

Four routing protocols were simulated using OPNET Modeler 14.5. For designing, stimulating, and analyzing a network topology, various toolboxes are available. We have employed the MANET toolset in our research. For network design, this toolkit includes a variety of components, including a mobile wlan station, profile configuration, application configuration, mobility configuration, etc.

4.2 OPNET Model Design

The four different pieces that make up OPNET simulator's operating principles are as follows. The essential components are depicted in fig. 4.1. Model design comes first on the list. Statistical data is applied to a network model after it has been designed. Results are then received after the simulation procedure has begun to run. The next step is to assess these results. If the outcome is inaccurate or unacceptable, we must re-model and then follow the same steps.

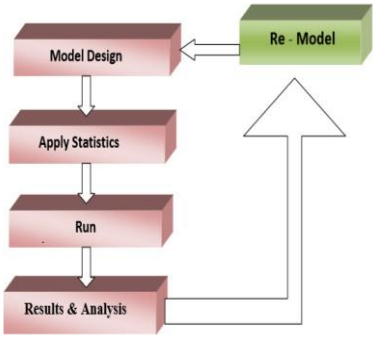
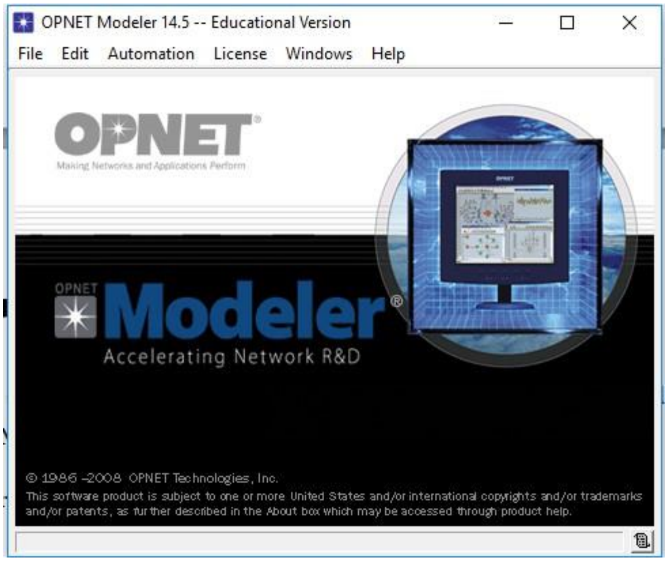


Fig 4.1: The OPNET simulator's functionality

4.3 Setup of a Mobile Ad hoc Network for a Typical Situation

To construct a basic MANET in OPNET, perform the following steps.

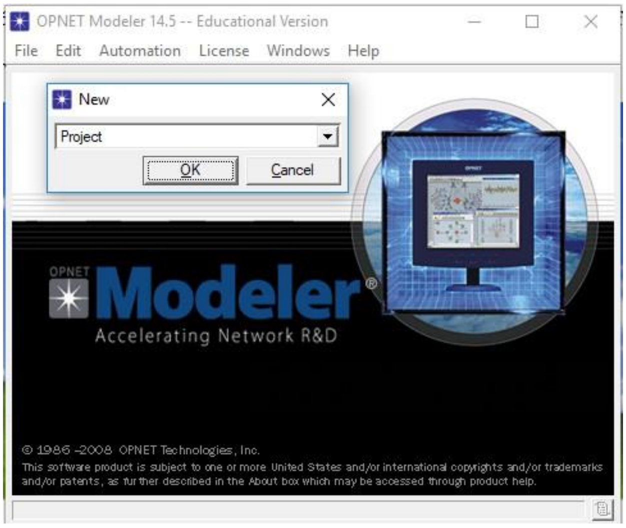
Step 1: Version 14.5 of the OPNET modeler is displayed in the image below:


OPNET Modeler 14.5 -- Educational Version
File
Edit
Automation
License
Windows
Help
OPNET
Making Networks and Applications Perform
OPNET Modeler
Accelerating Network R&D

© 1986 -2008 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.

Fig 4.2 OPNET modeler

Step 2: As shown in Figure 4.3, click on the file and then choose new from the file list to start a new project.

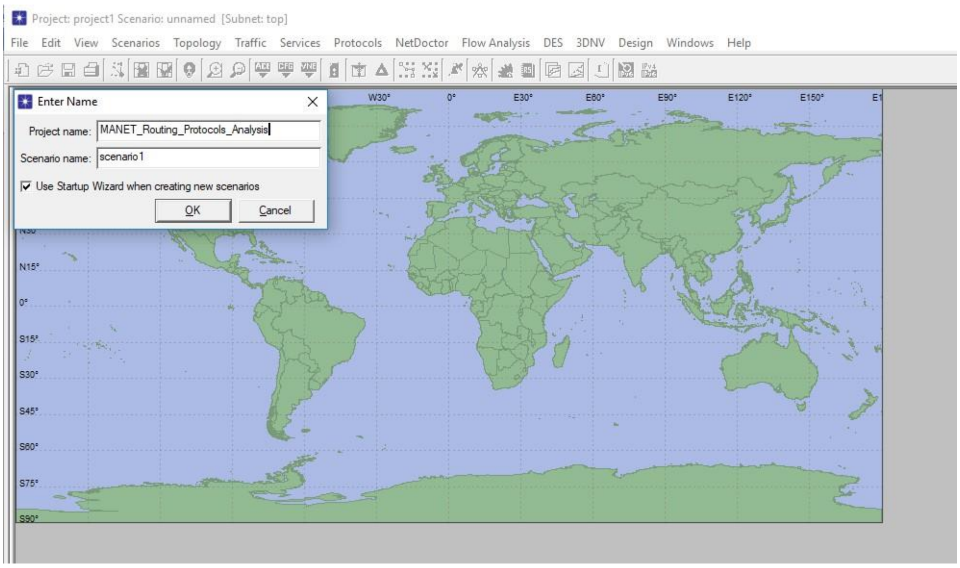


New: Project

© 1986 -2008 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.

Fig 4.3: New Project Creation

Step 3: As shown in Figure 4.4, this procedure can be used to write the name of the procedure followed by the name of a scenario.



Project name: MANET_Routing_Protocols_Analysis

Scenario name: scenario1

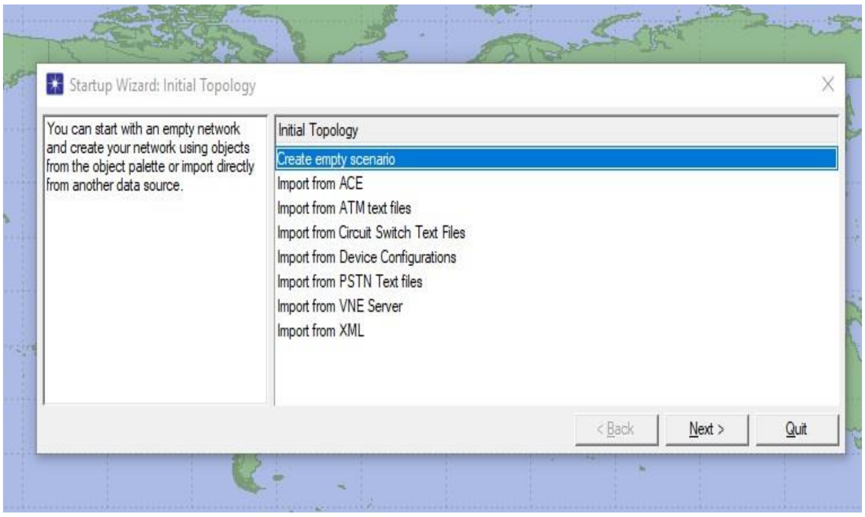
☑ Use Startup Wizard when creating new scenarios

Fig 4.4: Enter the name of project

Step 4: Construct fresh scenarios

- We must choose to construct an empty scenario from the initial Topology in the starting wizard.

- Press the "Next" button.



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

Import from ACE

Import from ATM text files

Import from Circuit Switch Text Files

Import from Device Configurations

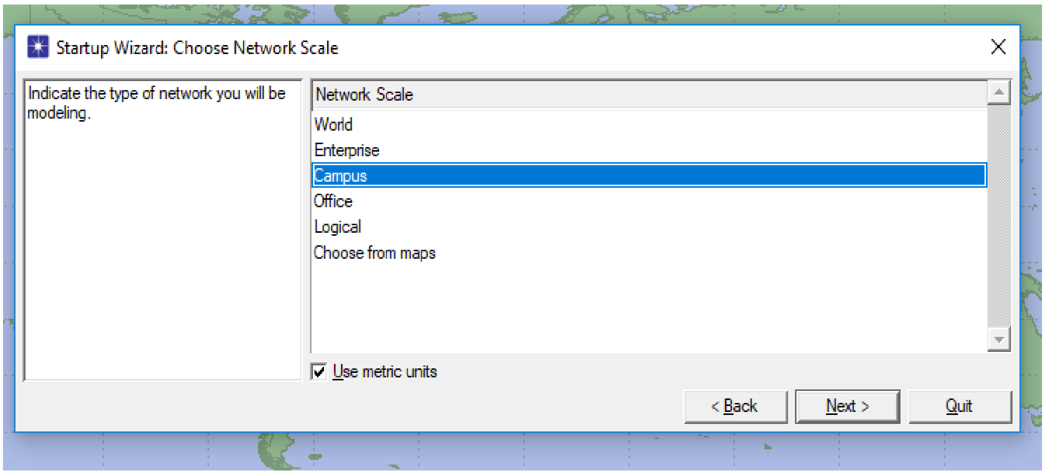
Import from PSTN Text files

Import from VNE Server

Import from XML

Fig 4.5: First topology: Startup Wizard

Step 5: Select the Network scale. Click next after selecting the Campus from the long list of options for the Network scale, as seen in figure 4.6.



Startup Wizard: Choose Network Scale

Indicate the type of network you will be modeling.

Network Scale

World

Enterprise

Campus

Office

Logical

Choose from maps

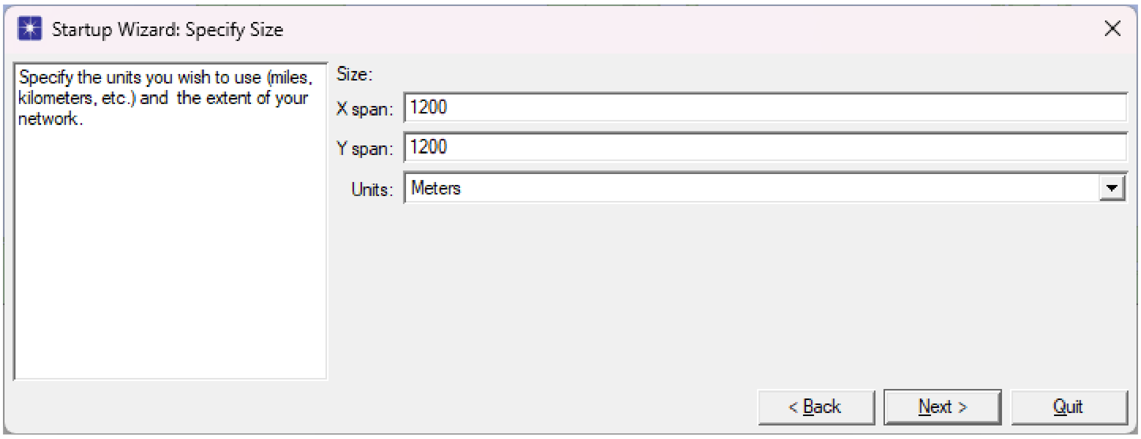
☑ Use metric units

Fig 4.6 Choose network scalability

Step 6: As seen in Figure 4.7, specify the size.

- To choose the simulation's region, we have two fields: X-span and Y-span.

- For the Unit field, we select (meters).



Startup Wizard: Specify Size

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

Size:

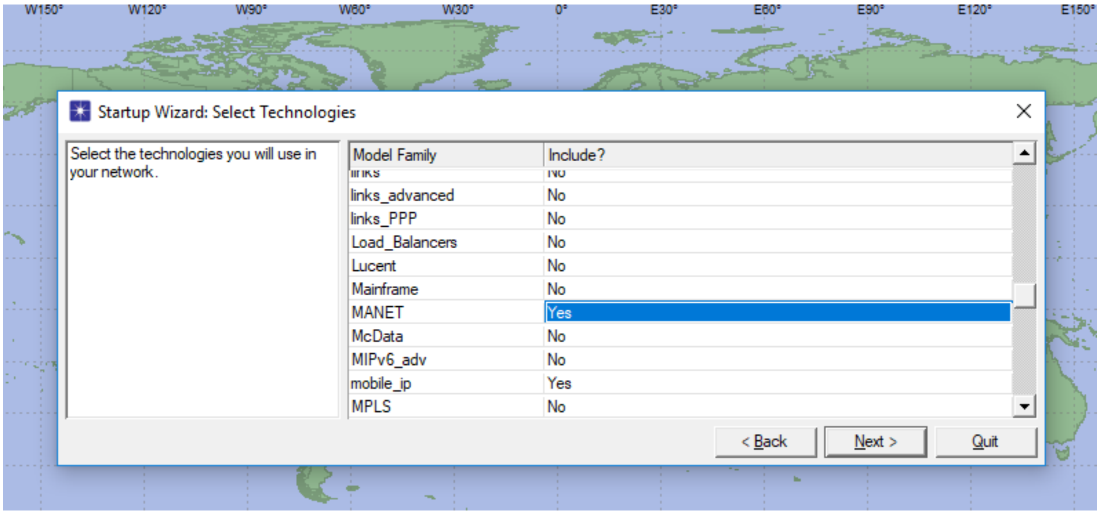
X span: 1200

Y span: 1200

Units: Meters

Fig 4.7: Startup Wizard: Choose a size

Step 7: Click on the MANET (mobile ad hoc wireless network) to choose the technology for our simulation, and then click the next button.



Startup Wizard: Select Technologies

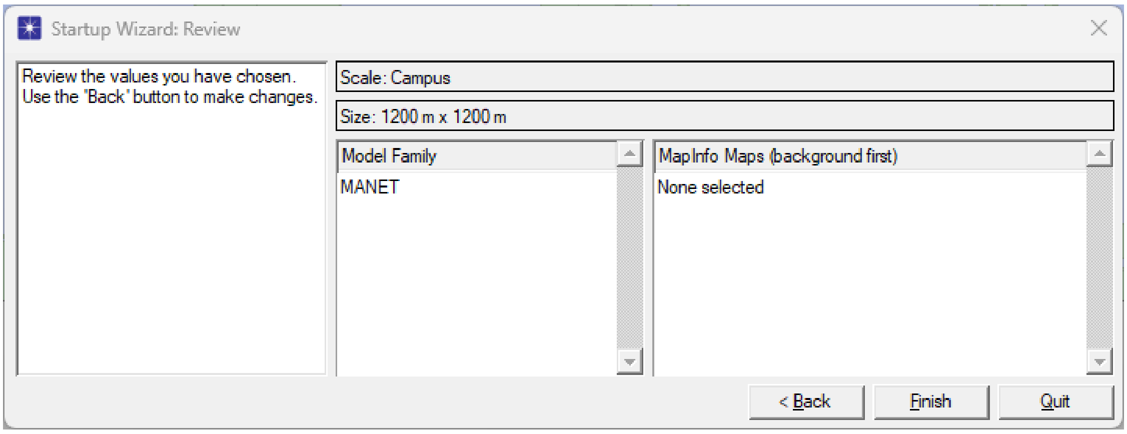
Select the technologies you will use in your network.

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

Fig 4.8: Startup Wizard: Choose Technologies

Step 8:

- Click Finish after choosing your technology.
- It will produce a simulation of a network.



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

Scale: Campus

Size: 1200 m x 1200 m

Model Family	MapInfo Maps (background first)
MANET	None selected

Fig 4.9 Startup Wizard: Examine

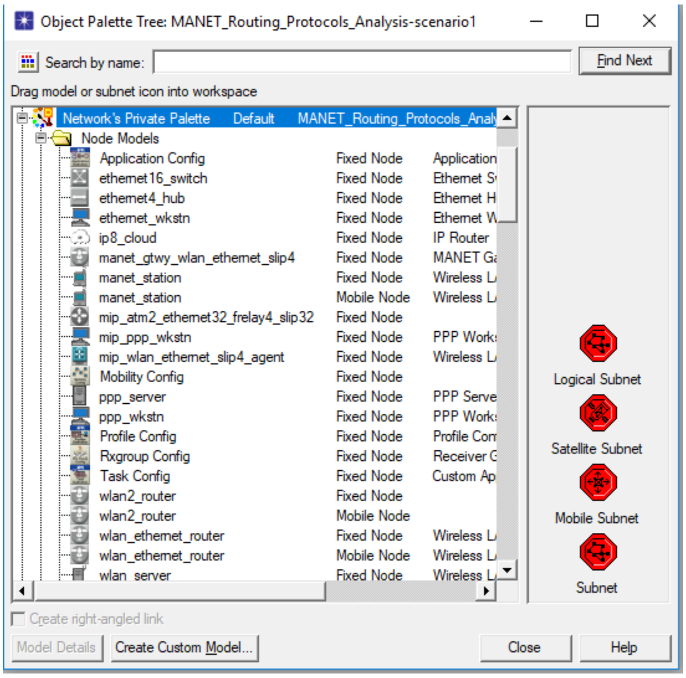
Step 9: The following actions must be taken in order to build the simulation's framework.

• Open the Object palette tree depicted in Figure 4.10, which contains the simulation-related Node model.

• Choose an application node and position it in the network zone.

• Choose a profile node and add it to the network zone.

• Choose WLAN_WKSTN (Mobile Node) and position it in the network region.



Drag model or subnet icon into workspace

□ Create right-angled link

Network's Private Palette	Default	MANET_Routing_Protocols_Analy
Node Models		
Application Config	Fixed Node	Application
ethernet16_switch	Fixed Node	Ethernet S
ethernet4_hub	Fixed Node	Ethernet H
ethernet_wkstn	Fixed Node	Ethernet W
ip8_cloud	Fixed Node	IP Router
manet_gtwy_wlan_ethernet_slip4	Fixed Node	MANET Ga
manet_station	Fixed Node	Wireless L
manet_station	Mobile Node	Wireless L
mip_atm2_ethernet32_frelay4_slip32	Fixed Node	
mip_ppp_wkstn	Fixed Node	PPP Work
mip_wlan_ethernet_slip4_agent	Fixed Node	Wireless L
Mobility Config	Fixed Node	
ppp_server	Fixed Node	PPP Serve
ppp_wkstn	Fixed Node	PPP Work
Profile Config	Fixed Node	Profile Con
Rxgroup Config	Fixed Node	Receiver G
Task Config	Fixed Node	Custom Ap
wlan2_router	Fixed Node	
wlan2_router	Mobile Node	
wlan_ethernet_router	Fixed Node	Wireless L
wlan_ethernet_router	Mobile Node	Wireless L
wlan_server	Fixed Node	Wireless L

Fig. 4.10: Table of Objects

A small number of the many objects in the MANET simulation object palette tree are used in the scenario that is provided below.

- The mobile clients that we used were wireless LAN mobile workstations. Different variations of 10 to 60 nodes are produced in our research situations. They are selected from the object palette, and we drag them to the work area.

- To set the programs that are used throughout the network, we used application configuration. We have employed FTP or FTP applications in our research.

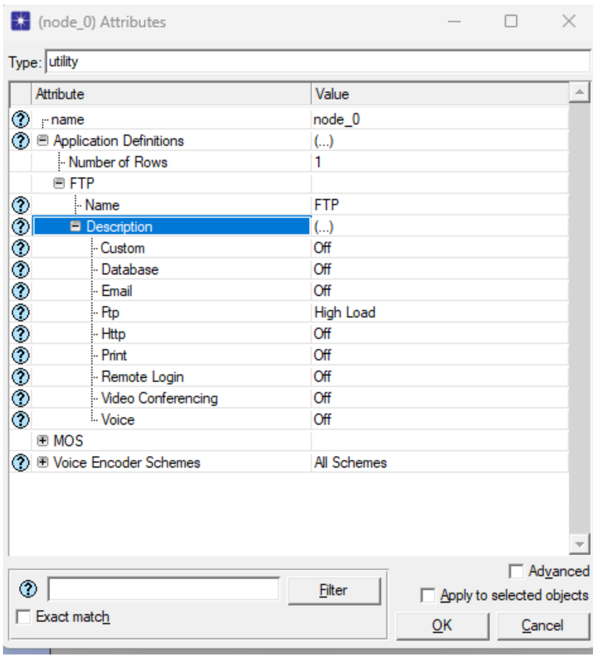
- To set the necessary profiles for the applications, we used profile configuration.

- For each of the mobile nodes, we have utilized mobility profiles.

The objects mentioned above are used to simulate the MANET. The meticulous configuration parameters are as follows:

4.3.1 Defined Application Configurations

This is used to specify the required programs that produce network traffic. There is a feature in the application configuration object that allows us to create as many applications as we like. In conducting our investigation, we employed the FTP application, whose snapshot is provided below:



(node_0) Attributes

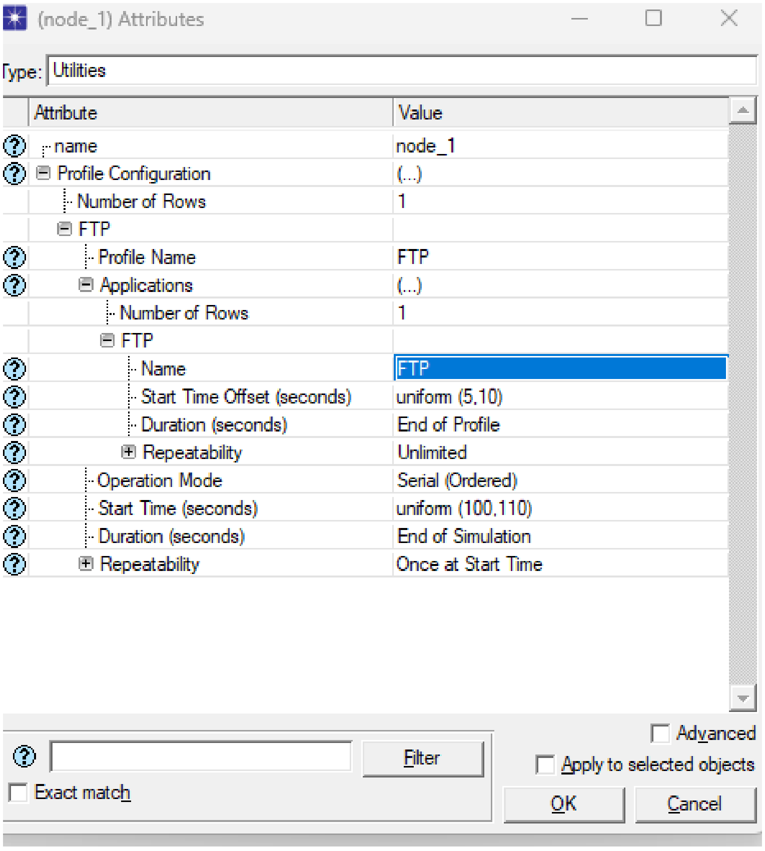
Type: utility

Attribute	Value
name	node_0
⊟ Application Definitions	(...)
Number of Rows	1
⊟ FTP	
Name	FTP
⊟ Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	High Load
Http	Off
Print	Off
Remote Login	Off
Video Conferencing	Off
Voice	Off
⊞ MOS	
⊞ Voice Encoder Schemes	All Schemes

Fig 4.11: Application configuration for FTP

4.3.2 Settings for Profile Configuration

We utilized the Profile configuration object to construct the profile, and the related screenshot is shown below:



(node_1) Attributes

Type: Utilities

Attribute	Value
name	node_1
⊟ Profile Configuration	(...)
Number of Rows	1
⊟ FTP	
Profile Name	FTP
⊟ Applications	(...)
Number of Rows	1
⊟ FTP	
Name	FTP
Start Time Offset (seconds)	uniform (5,10)
Duration (seconds)	End of Profile
⊞ Repeatability	Unlimited
Operation Mode	Serial (Ordered)
Start Time (seconds)	uniform (100,110)
Duration (seconds)	End of Simulation
⊞ Repeatability	Once at Start Time

Fig 4.12: Profile for FTP

4.3.3 Mobility Setup

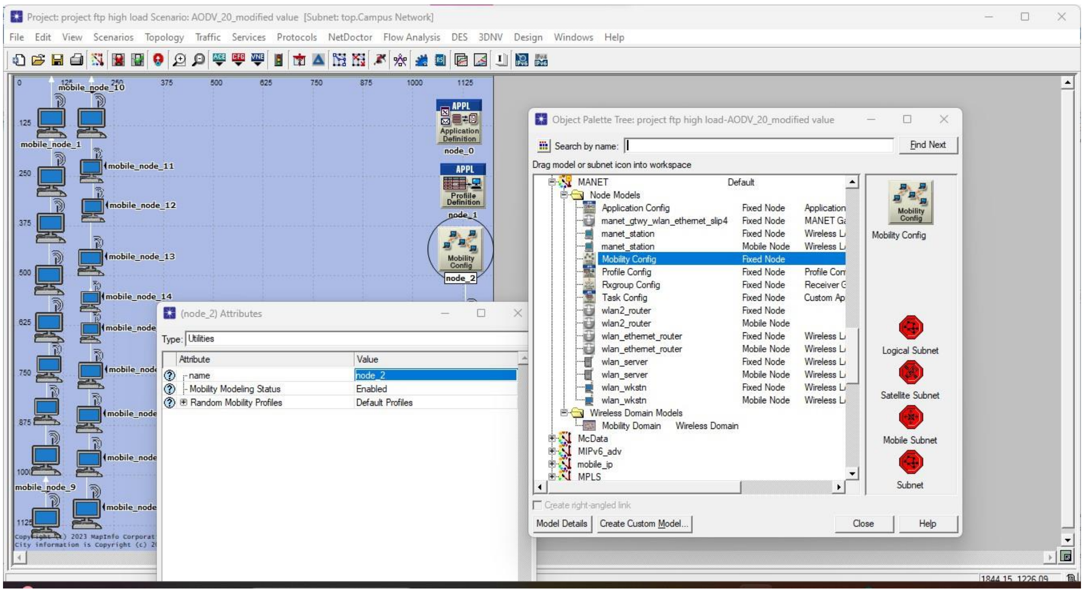
All mobile clients within the workspace have had their mobility patterns established using mobility configuration. OPNET uses a variety of mobility models for simulation. We have used default random way point mobility in our investigation.

Model for Random Waypoints

In this model, a node selects a termination at random and advances in the direction of the destination with a random velocity. It ceases after arriving at the location for a while. The 'pause time' argument specifies the length of this pausing period. It continues to select a random termination after the pause. The procedures are listed below:

- To edit attributes, use the list that appears when you right-click on any mobility setting, as shown in figure 4.13.
- Rename the configuration to "mobility," as seen in figure 4.14.

- As shown in Figure 4.15, select (Random mobility profile) and set the number of rows to 1 (because there is only one profile).
- As shown in figure 4.15, modify the values of Y-max (meter) and X-max (meter) to 1000 in order to designate the region of our simulation.
- Select (speed meter/second) then change the value to (constant=10)
- Select (pause time /second) then change the value to (constant=50)
- Select (start time /second) then change the value to (constant=100)
- Select (stop time/second) then change the value to (End of simulation)


Project: project ftp high load Scenario: AODV_20_modified value [Subnet: top.Campus Network]

(node_2) Attributes

Type: Utilities

Attribute	Value
name	node_2
Mobility Modeling Status	Enabled
⊞ Random Mobility Profiles	Default Profiles

Object Palette Tree: project ftp high load-AODV_20_modified value

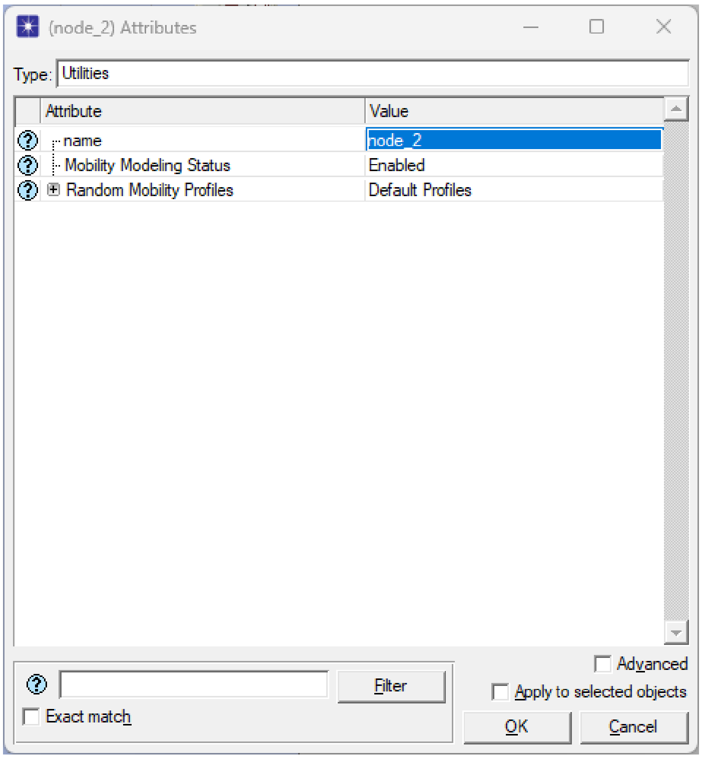
Search by name:

Drag model or subnet icon into workspace

MANET	Default	
Node Models		
Application Config	Fixed Node	Application
manet_gtwy_wlan_ethernet_slip4	Fixed Node	MANET Ga
manet_station	Fixed Node	Wireless L
manet_station	Mobile Node	Wireless L
Mobility Config	Fixed Node	
Profile Config	Fixed Node	Profile Con
Rxgroup Config	Fixed Node	Receiver G
Task Config	Fixed Node	Custom Ap
wlan2_router	Fixed Node	
wlan2_router	Mobile Node	
wlan_ethernet_router	Fixed Node	Wireless L
wlan_ethernet_router	Mobile Node	Wireless L
wlan_server	Fixed Node	Wireless L
wlan_server	Mobile Node	Wireless L
wlan_wkstn	Fixed Node	Wireless L
wlan_wkstn	Mobile Node	Wireless L
Wireless Domain Models		
Mobility Domain	Wireless Domain	
McData		
MIPv6_adv		
mobile_ip		
MPLS		

□ Create right-angled link

Fig. 4.13: Mobility configuration setting

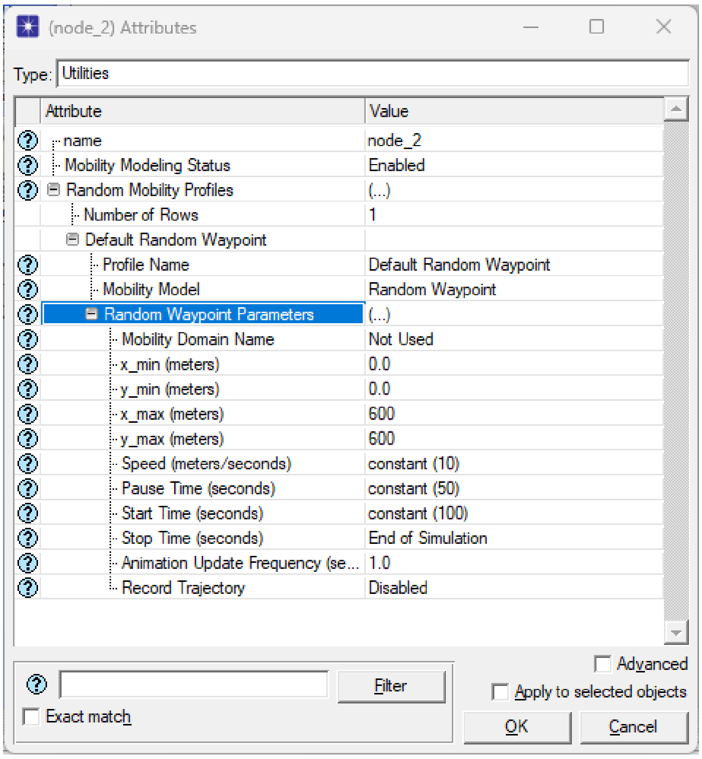


(node_2) Attributes

Type: Utilities

Attribute	Value
name	node_2
Mobility Modeling Status	Enabled
⊞ Random Mobility Profiles	Default Profiles

Fig. 4.14: Mobility configuration list



(node_2) Attributes

Type: Utilities

Attribute	Value
name	node_2
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)	600
y_max (meters)	600
Speed (meters/seconds)	constant (10)
Pause Time (seconds)	constant (50)
Start Time (seconds)	constant (100)
Stop Time (seconds)	End of Simulation
Animation Update Frequency (se...	1.0
Record Trajectory	Disabled

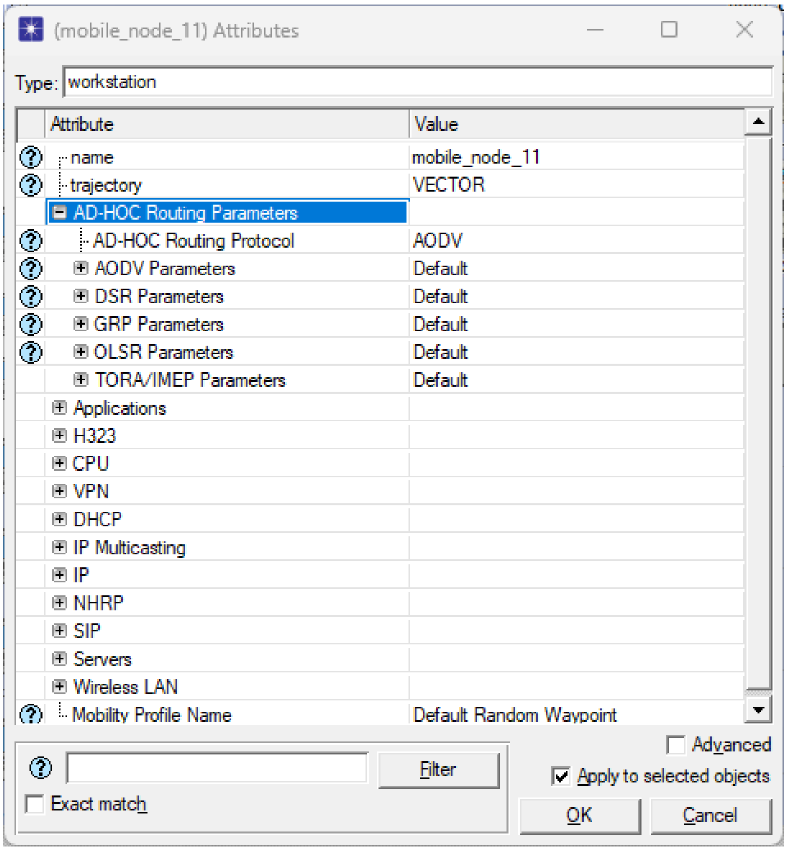
Fig. 4.15: Mobility configuration setting

By right-clicking any WLAN_WKSTN node and selecting (Select Similar Node) from the list, all WLAN_WKSTN nodes must be selected in order to choose the physical attributes that affect data rate.

4.3.4 Settings for Mobile Nodes

To communicate between these nodes, routing protocol is needed. We have used proactive and reactive routing protocols such AODV, GRP, and OLSR in our research. Different scenarios with variable numbers of mobile nodes and various routing methods have been used.

The screenshot for AODV is as follows:



(mobile_node_11) Attributes

Type: workstation

Attribute	Value
name	mobile_node_11
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

□ Advanced

☑ Apply to selected objects

□ Exact match

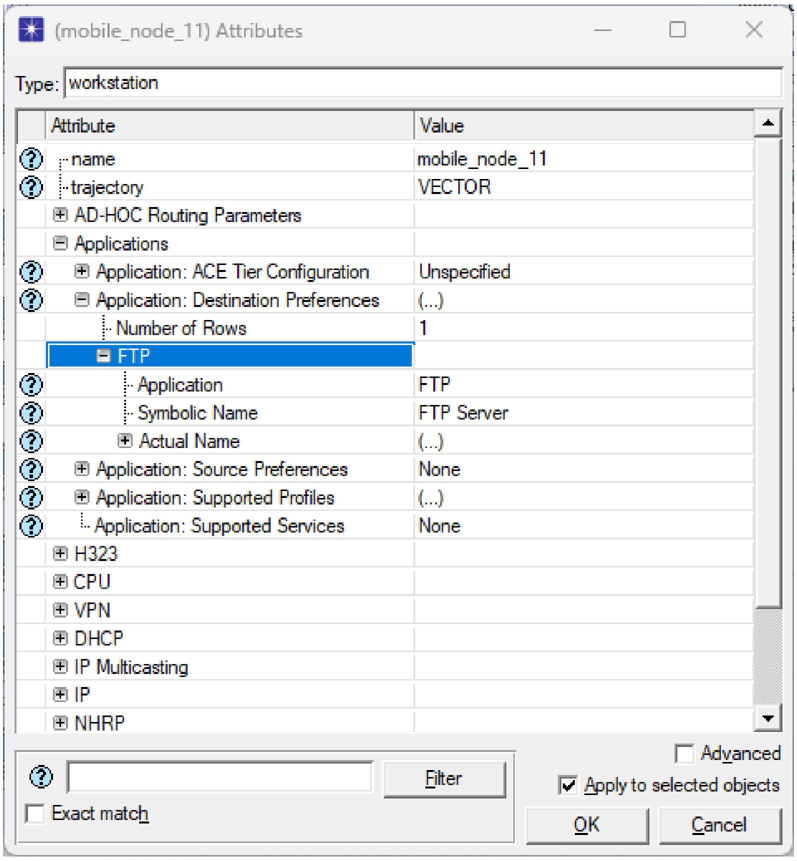
Fig 4.16: Ad Hoc routing protocol (AODV)

GRP and OLSR protocols were chosen from the Ad Hoc routing parameter in a similar manner.

4.3.5 Preferences for Destination

A random destination will be selected from the pool of nodes that currently support the application of interest if Destination Preferences is set to none.

For FTP, the following options are available for destination preference:


(mobile_node_11) Attributes

Type: workstation

Attribute	Value
name	mobile_node_11
trajectory	VECTOR
⊞ AD-HOC Routing Parameters	
⊟ Applications	
⊞ Application: ACE Tier Configuration	Unspecified
⊟ Application: Destination Preferences	(...)
Number of Rows	1
⊟ FTP	
Application	FTP
Symbolic Name	FTP Server
⊞ Actual Name	(...)
⊞ Application: Source Preferences	None
⊞ Application: Supported Profiles	(...)
Application: Supported Services	None
⊞ H323	
⊞ CPU	
⊞ VPN	
⊞ DHCP	
⊞ IP Multicasting	
⊞ IP	
⊞ NHRP	

□ Exact match

□ Advanced

☑ Apply to selected objects

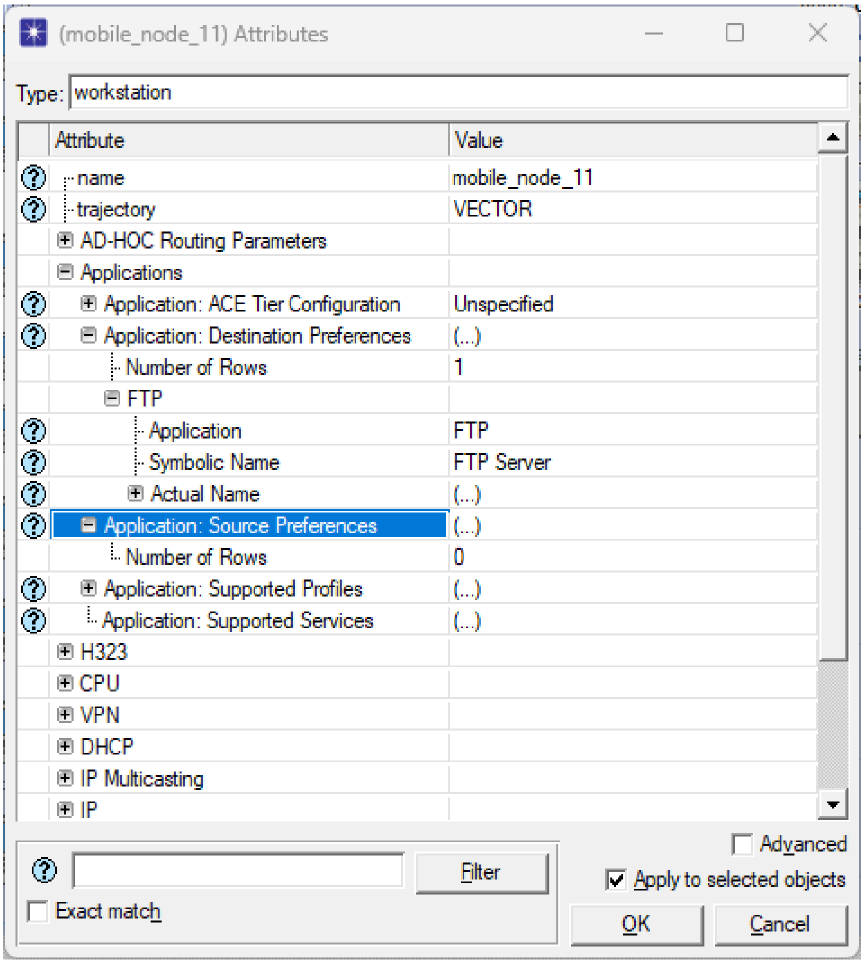
Fig. 4.17: Destination preference for FTP

4.3.6 Preference for sources

A number of clients (sources) may be selected from the list of nodes that now support the application of interest because Source Preferences is set to none. If there are n nodes in the system, we have chosen the remaining n-1 nodes as the source node in our simulations [18].

For instance, if there are 60 nodes in the system, one of them will be chosen at random to function as a server node, and the other nodes would serve as source nodes.

Source preferences can be set to none for FTP in the following ways:



(mobile_node_11) Attributes

Type: workstation

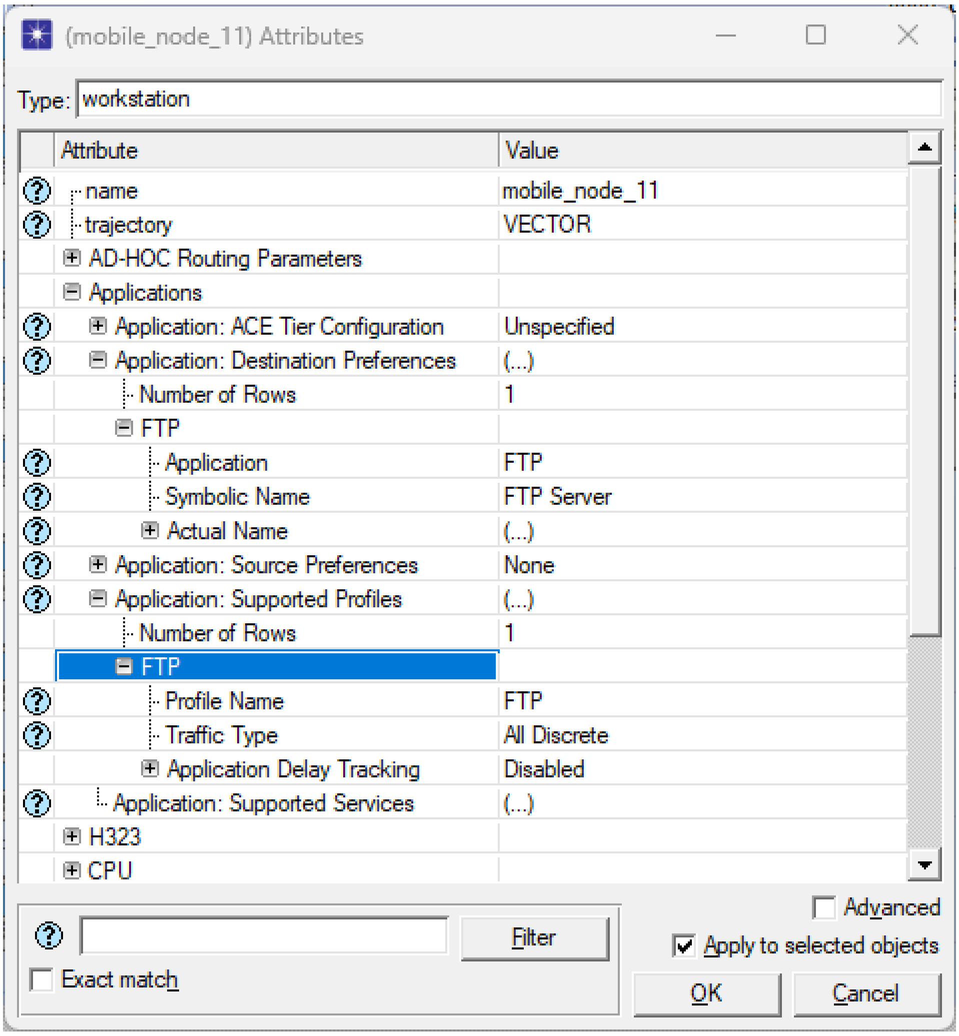
Attribute	Value
name	mobile_node_11
trajectory	VECTOR
⊞ AD-HOC Routing Parameters	
⊟ Applications	
⊞ Application: ACE Tier Configuration	Unspecified
⊟ Application: Destination Preferences	(...)
Number of Rows	1
⊟ FTP	
Application	FTP
Symbolic Name	FTP Server
⊞ Actual Name	(...)
⊟ Application: Source Preferences	(...)
Number of Rows	0
⊞ Application: Supported Profiles	(...)
Application: Supported Services	(...)
⊞ H323	
⊞ CPU	
⊞ VPN	
⊞ DHCP	
⊞ IP Multicasting	
⊞ IP	

Fig. 4.18: Source Preferences for FTP

4.3.7 Assisted or Supported Profile

It lists all of the profiles whose names are active on this node [18]. Each profile is specifically defined during profile configuration. A profile describes user behavior in terms of the programs being utilized. the volume of traffic that each application produces.

The supported profiles for FTP are defined as follows:



(mobile_node_11) Attributes

Type: workstation

Attribute	Value
name	mobile_node_11
trajectory	VECTOR
⊞ AD-HOC Routing Parameters	
⊟ Applications	
⊞ Application: ACE Tier Configuration	Unspecified
⊟ Application: Destination Preferences	(...)
Number of Rows	1
⊟ FTP	
Application	FTP
Symbolic Name	FTP Server
⊞ Actual Name	(...)
⊞ Application: Source Preferences	None
⊟ Application: Supported Profiles	(...)
Number of Rows	1
⊟ FTP	
Profile Name	FTP
Traffic Type	All Discrete
⊞ Application Delay Tracking	Disabled
Application: Supported Services	(...)
⊞ H323	
⊞ CPU	

□ Advanced

☑ Apply to selected objects

□ Exact match

Fig. 4.19: Supported profiles for FTP

4.3.8 Variety of Traffic

The traffic type that will be produced for the necessary profile is specified. If it is set to All Discrete, the program included in this profile will emit discrete data packets [18]. Using the utility "Protocols / Applications / Deploy Defined Applications..," we may change the value of this attribute. The following procedure must be followed in order to assign the mobility model to all mobile nodes from the mobile configuration object. We must choose Random Mobility from the topology before setting the mobility profile.

The mobility defined across the mobile configuration is set using the mobility profile. The comparable network is as follows once the fundamental network configuration is complete:

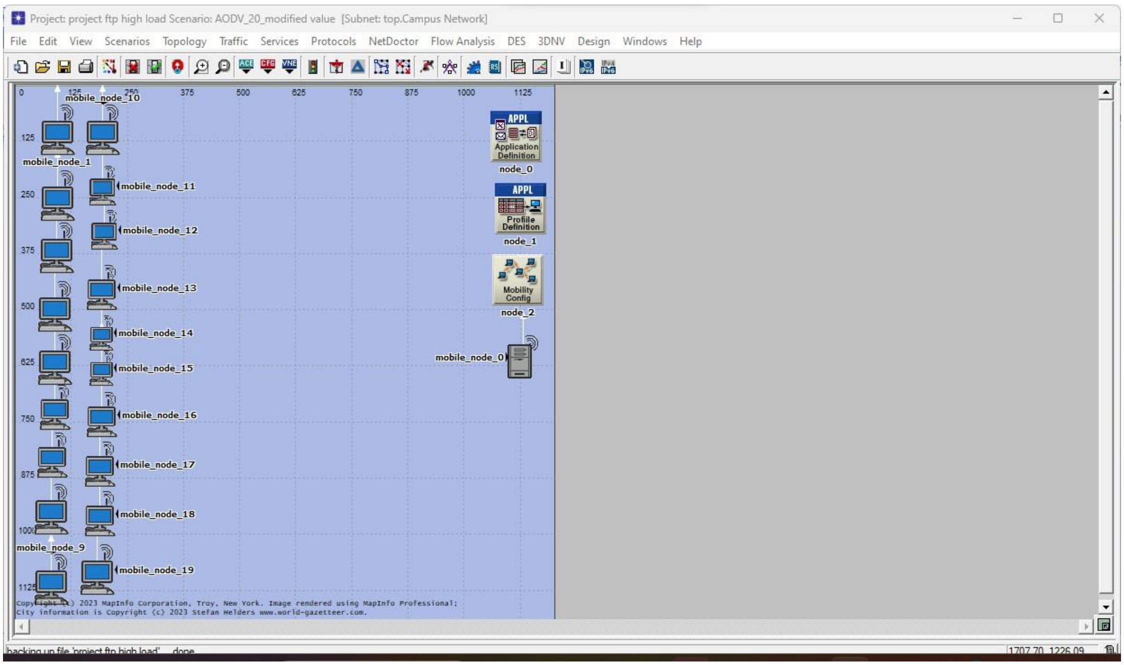

Project: project ftp high load Scenario: AODV_20_modified value [Subnet: top.Campus Network]
File Edit View Scenarios Topology Traffic Services Protocols NetDoctor Flow Analysis DES 3DNV Design Windows Help
APPL
Application Definition
node_0
APPL
Profile Definition
node_1
Mobility Config
node_2
mobile_node_0
mobile_node_1
mobile_node_9
mobile_node_10
mobile_node_11
mobile_node_12
mobile_node_13
mobile_node_14
mobile_node_15
mobile_node_16
mobile_node_17
mobile_node_18
mobile_node_19
Copyright (c) 2023 MapInfo Corporation, Troy, New York. Image rendered using MapInfo Professional;
City information is Copyright (c) 2023 Stefan Helders www.world-gazetteer.com.
backing up file 'project ftp high load' ... done
1707.70, 1226.09

Fig. 4.20: MANET scenario for 20 nodes

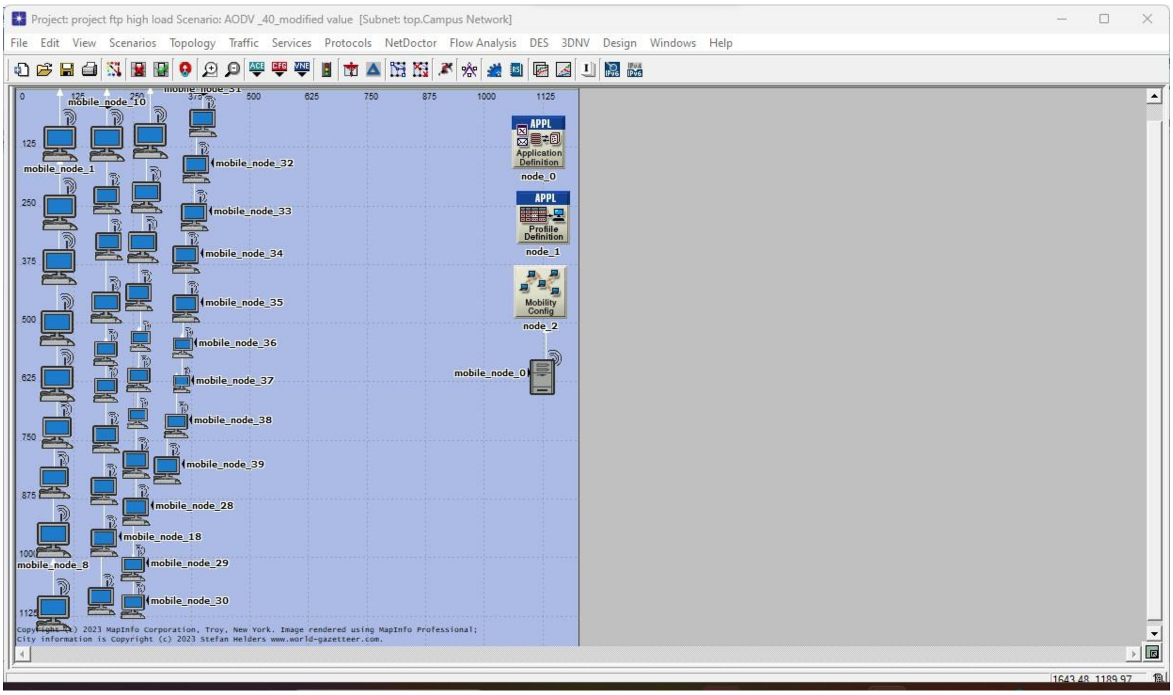

Project: project ftp high load Scenario: AODV _40_modified value [Subnet: top.Campus Network]
File Edit View Scenarios Topology Traffic Services Protocols NetDoctor Flow Analysis DES 3DNV Design Windows Help
APPL
Application Definition
node_0
APPL
Profile Definition
node_1
Mobility Config
node_2
mobile_node_0
mobile_node_1
mobile_node_8
mobile_node_10
mobile_node_31
mobile_node_32
mobile_node_33
mobile_node_34
mobile_node_35
mobile_node_36
mobile_node_37
mobile_node_38
mobile_node_39
mobile_node_28
mobile_node_18
mobile_node_29
mobile_node_30
Copyright (c) 2023 MapInfo Corporation, Troy, New York. Image rendered using MapInfo Professional;
City information is Copyright (c) 2023 Stefan Helders www.world-gazetteer.com.
1643.48, 1189.97

Fig. 4.21: MANET scenario for 40 nodes

4.3.9 Settings for Mobile Nodes

With different nodes ranging from 20 to 100, we simulated the AODV, GRP, and OLSR protocols in various circumstances. A homogenous network with identical mobile nodes was taken into account for each of the scenarios. The modeled network's nodes were each outfitted with a wireless transceiver that complied with the 802.11 (Wi-Fi) operation requirements. An omnidirectional antenna with a transmission power of 0.005W and a data throughput of 11 Mbps served as the transceiver's antenna. Each scenario's simulation lasted 10 minutes (or 600 seconds). The following table is a summary of the configurations for the mobile node.

Table 4.1: Modeling and Simulation Parameters for MANET

Simulation Parameters	**Value**
Simulator	OPNET 14.5
Environment Area (m x m)	1200 x 1200
Mobility Model	Random waypoint
Routing Protocol	AODV, GRP, OLSR
Data Rate	11Mbps
Traffic source	FTP(High Load),VOIP
Number of nodes	20,40,60,100
Mobility speed(m/s)	10
Simulation time(seconds)	600
MAC protocol	802.11b
Transmission power(W)	0.005
Node placement	Random
Pause time	50
Address mode	IPv4

Chapter 5

Result analysis and Discussion

5.1 Performance metrics

The effectiveness of these four routing methods is assessed using several criteria. These metrics demonstrate the effectiveness of data delivery [12].

Delay

Average end-to-end latency is the length of time it typically takes for data packets to travel across a MANET from their source to their destination.

Load

The volume of information (traffic) being transported by the network**.**

Throughput

It measures how many data packets are successfully transmitted over the network in a given amount of time during the simulation [9]. Any routing protocol should always be prepared for extremely high throughput [18].

Throughput = number of bits contained in accepted packet / simulation time

(PDF) Packet delivery ratio

It is defined as a number of data packets that are sent to the source from whence they were generated.

PDR = Data packet delivered to all sources / Data packet send by all sources

(NRL) Normalized routing load

It is defined as the quantity of routing packets sent for each data packet that reaches its destination.

NRL = No. of routing packets sent / No. of data packets delivered

Jitter

As was already mentioned, jitter is a variation in latency, or the interval of time between a signal's transmission and reception. The disruption in the regular flow of sending data packets is referred to as this variance, which is expressed in milliseconds (ms).

5.2 Project 1:

- In this project we use FTP (High Load) application and AODV,OLSR and GRP protocol for 20,40,60 ,100 node density.
- Now we analysis the delay, load, throughput, Packet delivery fraction and Normalized routing load for default value.

5.2.1 Delay Analysis

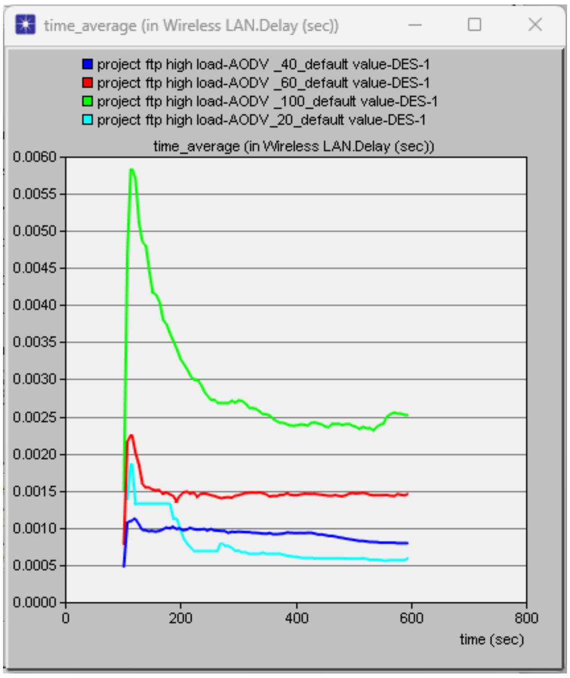


Fig 5.1: Delay of AODV protocol

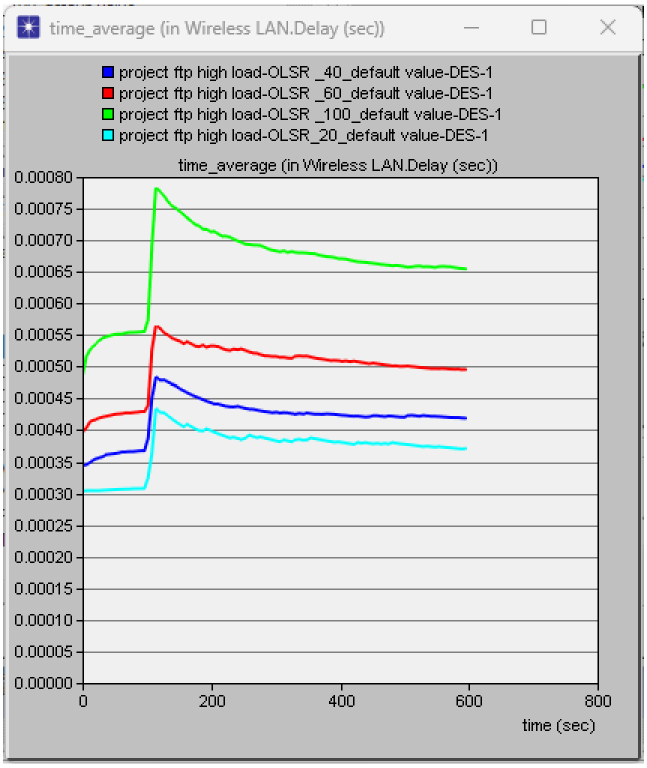


Fig 5.2: Delay of OLSR protocol

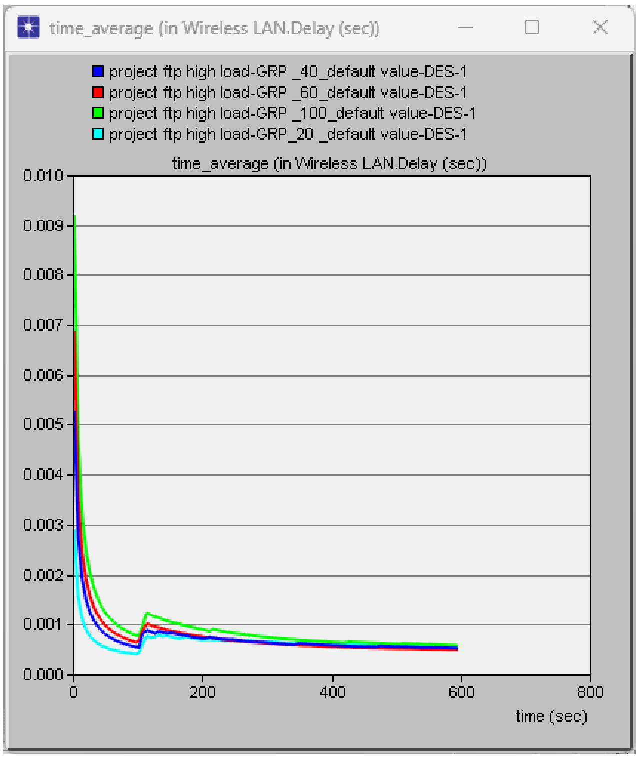


Fig 5.3: Delay of GRP protocol

Table 5.1: Delay (second) of AODV, OLSR, GRP.

Protocol	Node Density			
	20	40	60	100
AODV	0.000629	0.00076	0.001223	0.002387
OLSR	0.000372	0.00042	0.000499	0.000661
GRP	0.000659	0.000745	0.000797	0.000979

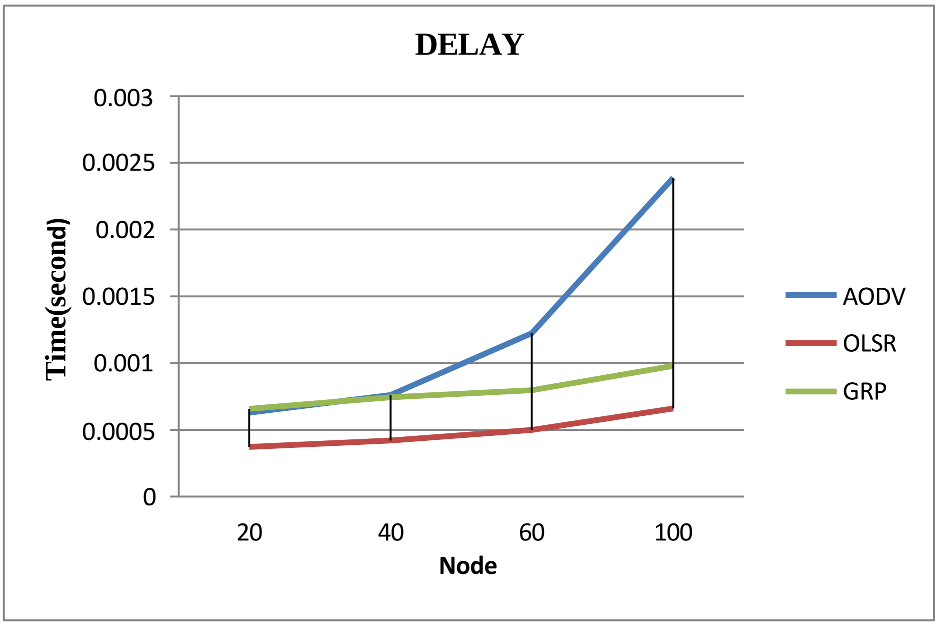


Fig 5.4: Delay (second) of AODV, OLSR, GRP.

Figures 5.1 to 5.3 show the delay of various routing protocols with varying numbers of mobile nodes. In table 5.1, we've produced a latency comparison table for these routing protocols. We presented the comparative delays of the AODV, OLSR, and GRP in figure 5.4 using data from table 5.1. We can observe from this graph that AODV has the highest latency, but OLSR has the lowest. GRP performs around averagely.

5.2.2 Load Analysis

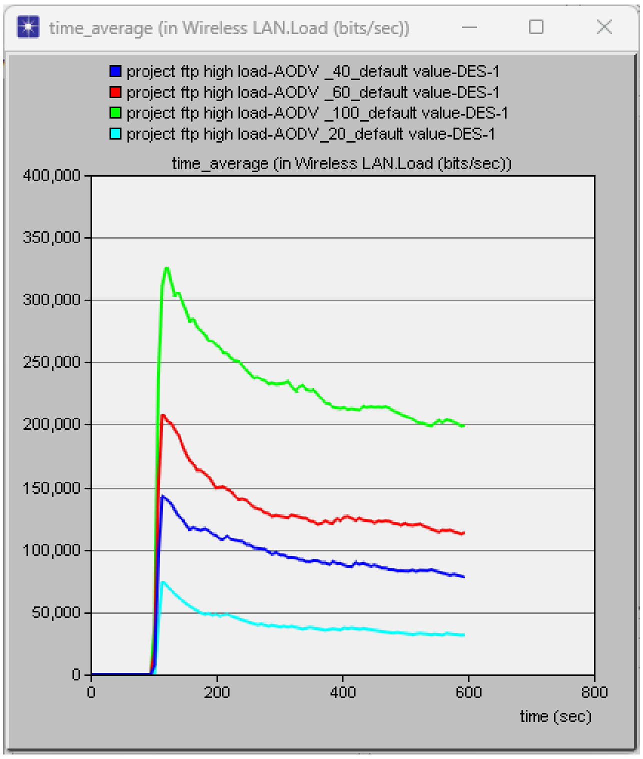


Fig 5.5: Load of AODV protocol

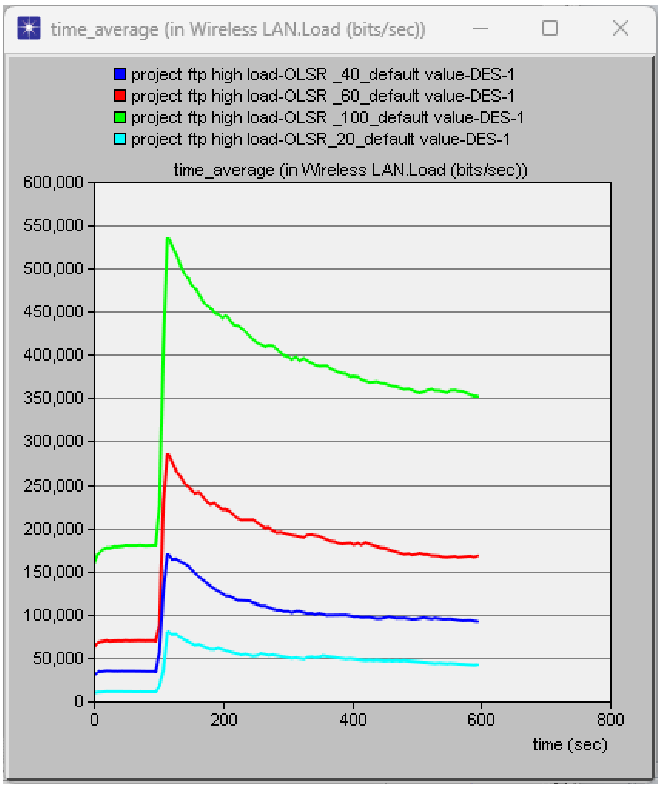


Fig 5.6: Load of OLSR protocol

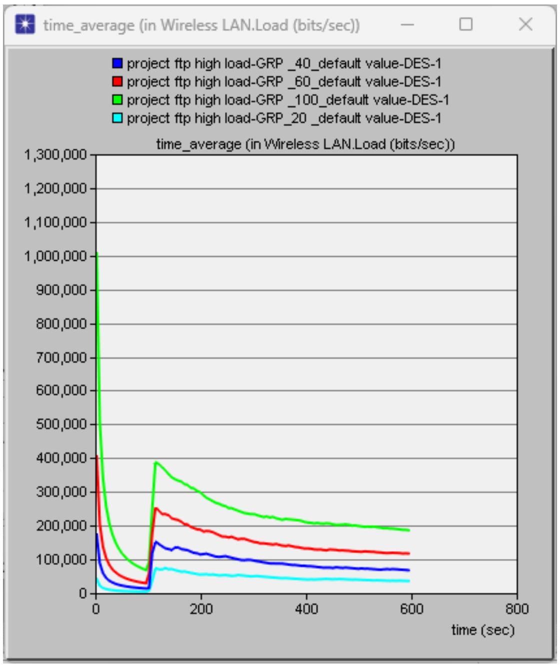


Fig 5.7: Load of GRP protocol

Table 5.2: Load of AODV, OLSR, GRP

Protocol	Node Density			
	20	40	60	100
AODV	33246.72	79364.07	110962.8	191953.6
OLSR	44510.75	96294.73	173382.3	361018.5
GRP	41346.02	83598	141692.4	234497.5

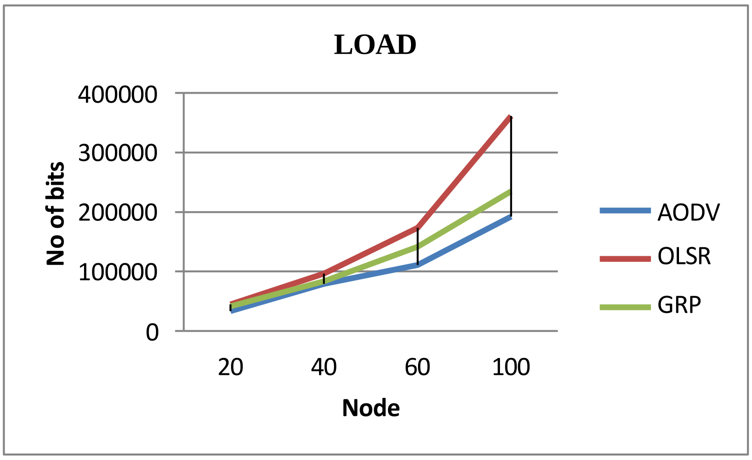


Fig 5.8: Load of AODV, OLSR, GRP.

Figures 5.5 to 5.7 show the load of various routing protocols with varying numbers of mobile nodes. In table 5.2, we've produced a load comparison table for these routing protocols. We presented the comparative load of the AODV, OLSR, and GRP in figure 5.8 using data from table 5.2. We can observe from this graph that OLSR has the highest load, but AODV has the lowest. Over AODV, GRP performs around averagely.

5.2.3 Throughput Analysis

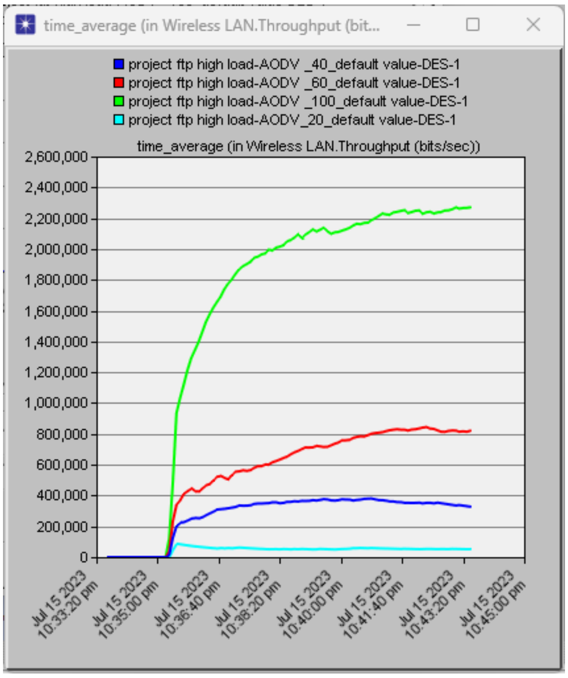


Fig 5.9: Throughput of AODV protocol

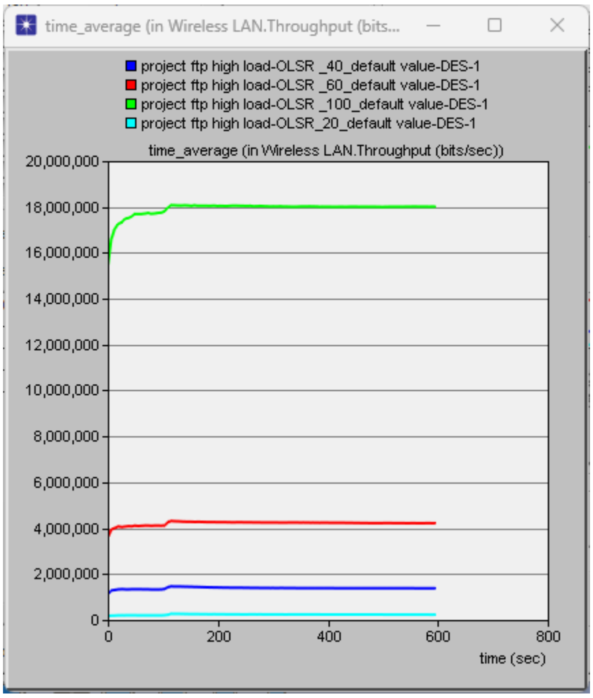


Fig 5.10: Throughput of OLSR protocol

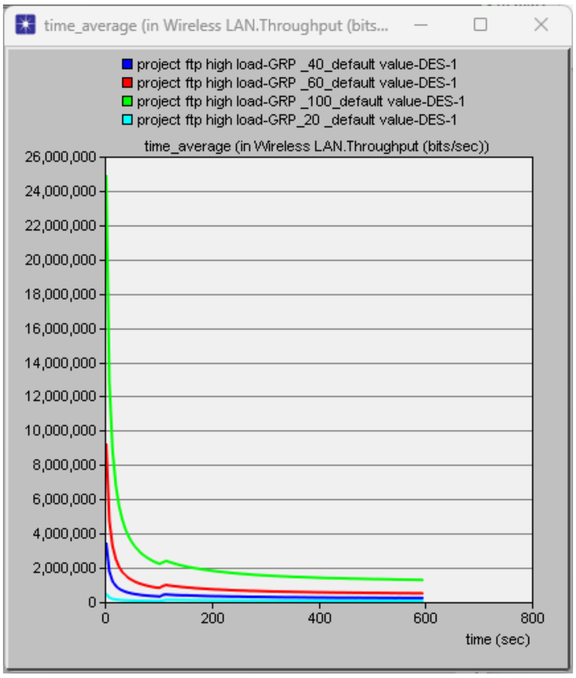


Fig 5.11: Throughput of GRP protocol

Table 5.3: Throughput of AODV, OLSR, GRP

Protocol	Node Density			
	20	40	60	100
AODV	46148.01	276567.8	557209.2	1625393
OLSR	234165.7	1385080	4211234	17918340
GRP	97129.33	386722.7	897586.4	2297666

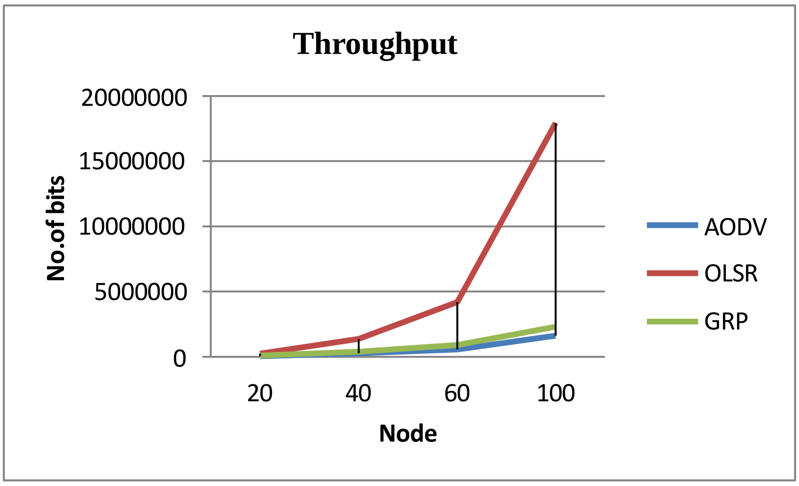


Fig 5.10: Throughput of OLSR protocol

Figures 5.9 to 5.11 show the throughput of various routing protocols with varying numbers of (20,40,60,100) mobile nodes. In table 5.3, we've produced a throughput comparison table for these routing protocols. We presented the comparative throughput of the AODV, OLSR, and GRP in figure 5.12 using data from table 5.3. We can observe from this graph that OLSR has the highest throughput, but AODV has the lowest. Over AODV, GRP performs around averagely.

5.3 (PDR)/ Packet delivery ratio Analysis

5.3.1 Traffic received Analysis

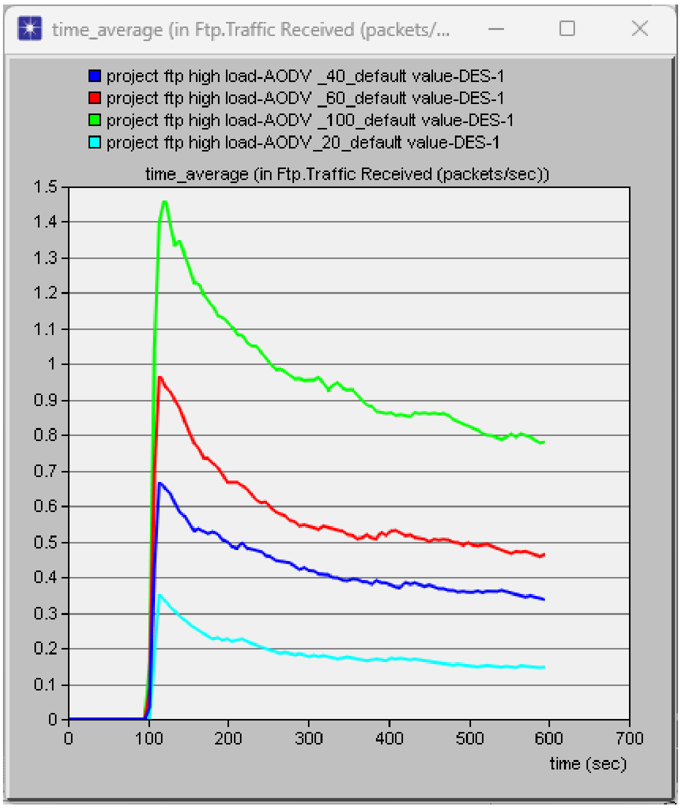


Fig 5.13: Traffic received of AODV protocol

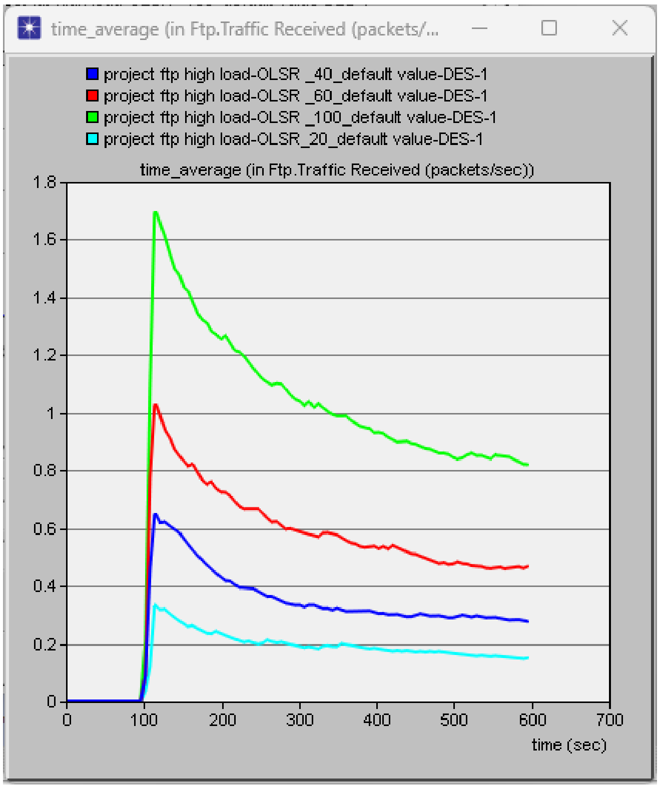


Fig 5.14: Traffic received of OLSR protocol

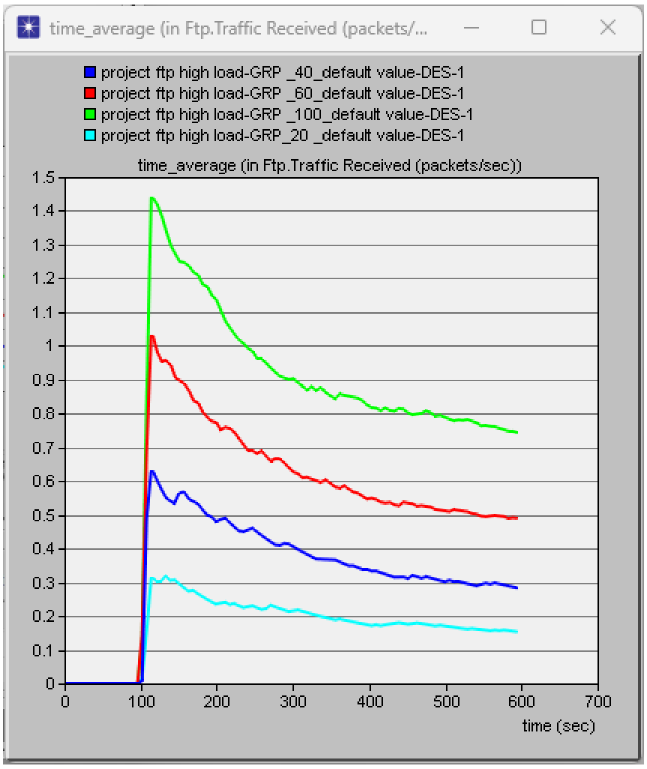


Fig 5.15: Traffic received of GRP protocol

Table 5.4: Traffic received of AODV, OLSR, GRP

Protocol	Node Density			
	20	40	60	100
AODV	0.15454	0.349308	0.476667	0.79189
OLSR	0.162114	0.297648	0.495253	0.865479
GRP	0.169026	0.321404	0.523152	0.762685

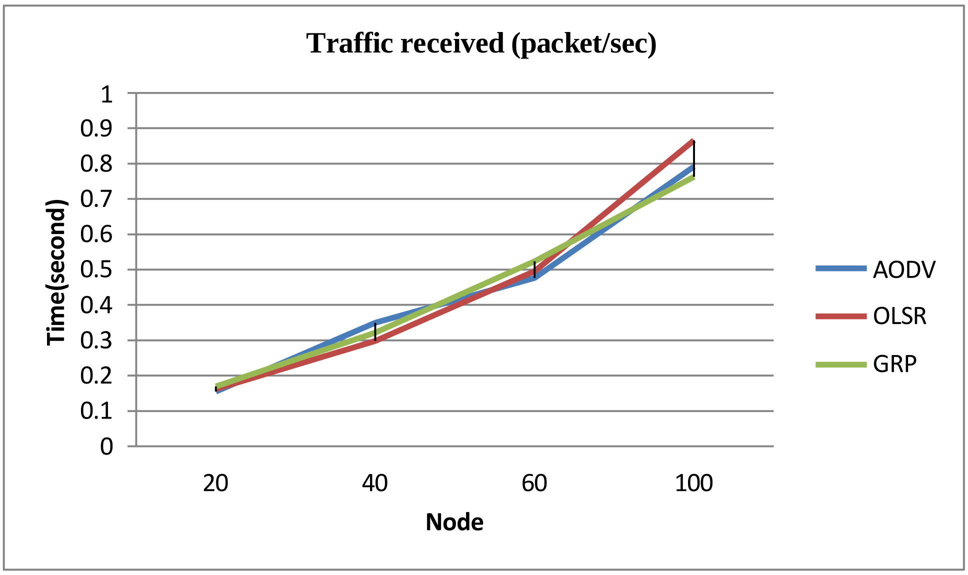


Fig 5.16: Traffic received of AODV, OLSR ,GRP.

Figures 5.13 to 5.15 show the traffic received for various routing protocols with 20, 40, 60, and 100 mobile nodes, respectively. In table 5.4, we've developed a traffic received table for these routing protocols. We plotted the comparative traffic received by AODV, OLSR, and GRP from table 5.4, and the result is shown in figure 5.16. We can observe from this number that OLSR is higher than AODV and GRP.

5.3.2 Traffic sent Analysis

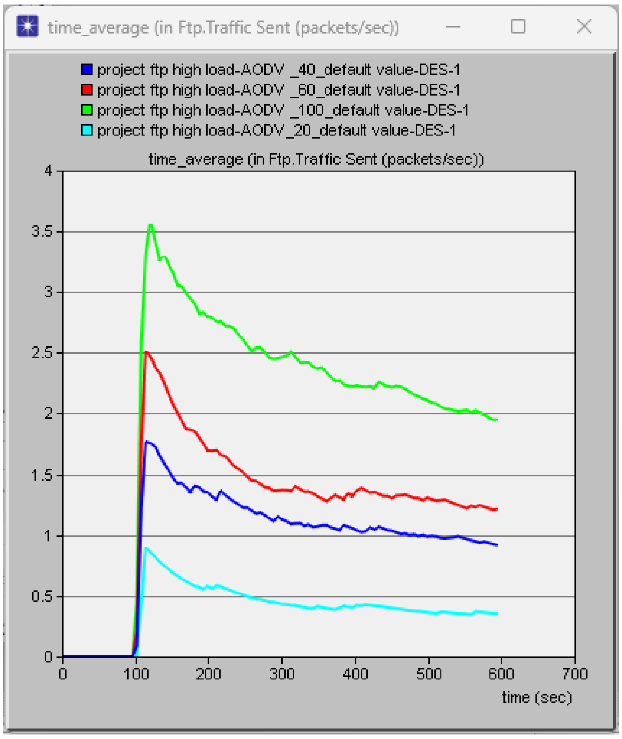


Fig 5.17: Traffic sent of AODV protocol

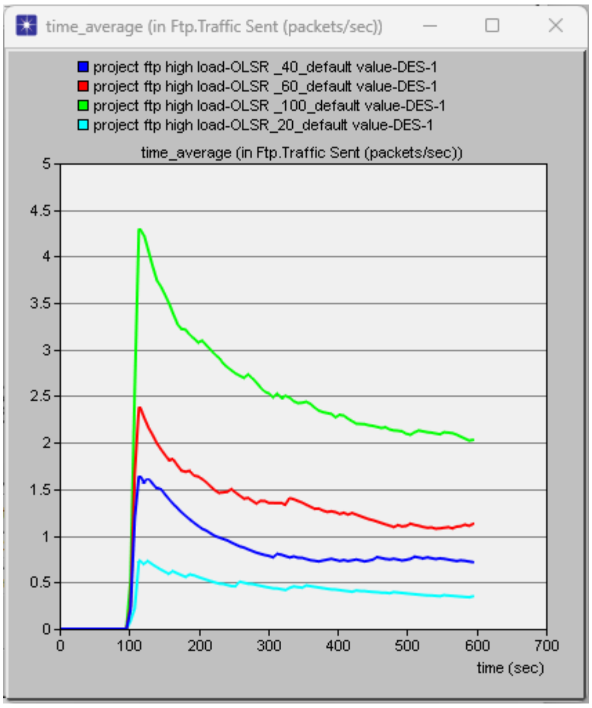


Fig 5.18: Traffic sent of OLSR protocol

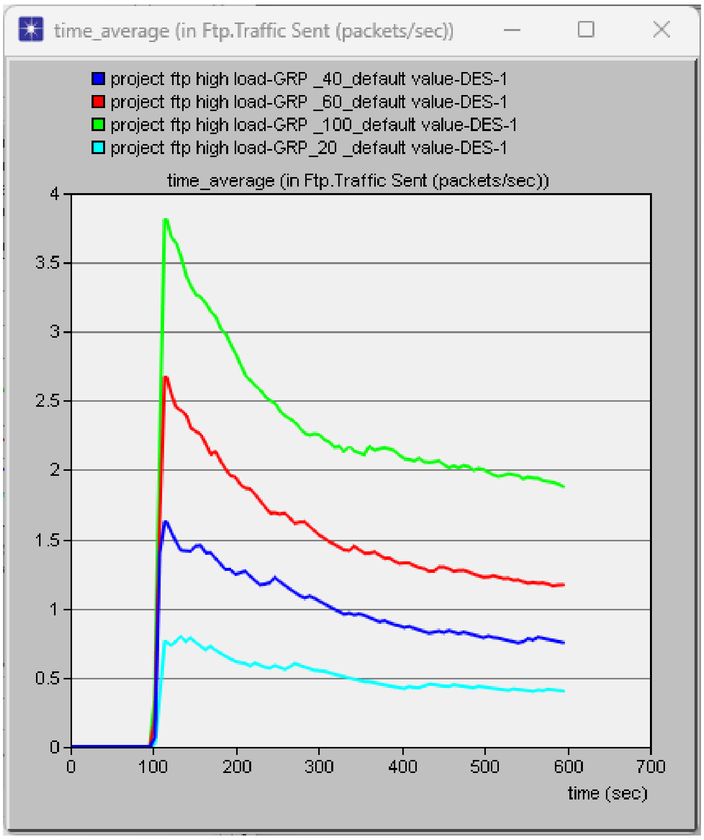


Fig 5.19: Traffic sent of GRP protocol

Table 5.5: Traffic sent of AODV, OLSR, GRP

Protocol	Node Density			
	20	40	60	100
AODV	0.38381	0.948022	1.224924	2.012297
OLSR	0.375187	0.744904	1.136858	2.13047
GRP	0.42783	0.839555	1.280755	1.937713

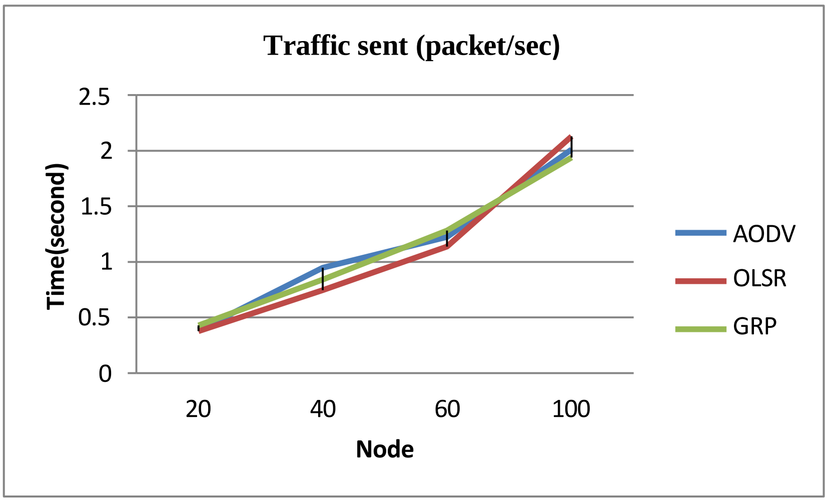


Fig 5.20: Traffic sent of AODV, OLSR, GRP.

Figures 5.17 to 5.19 show the traffic sent by various routing protocols with a number of (20, 40, and 60,100) mobile nodes. In table 5.5, we've constructed a traffic transmitted table for these routing protocols. Figure 5.20, which compares the traffic sent by AODV, OLSR, and GRP, was produced using data from table 5.5. We can observe from this figure that the values for AODV, OLSR, and GRP are nearly identical.

Table 5.6: Packet delivery ratio of AODV, OLSR, and GRP.

Protocol	Node Density			
	20	40	60	100
AODV	0.40264	0.36845	0.38914	0.39352
OLSR	0.43208	0.39957	0.43563	0.40623
GRP	0.39508	0.38282	0.40847	0.39360

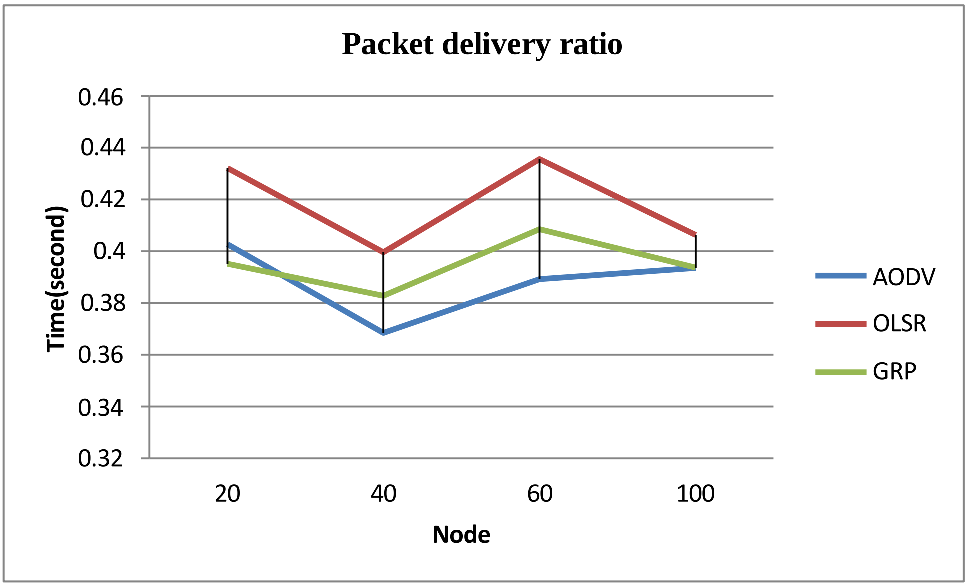


Fig 5.21: Packet delivery ratio of AODV, OLSR, GRP.

Figure 5.21, which compares the packet delivery ratio by AODV, OLSR, and GRP, was produced using data from table 5.6. We can observe from this figure that the packet delivery ratio OLSR has the highest, and AODV has lowest.

5.4 Normalized routing load Analysis

5.4.1 Routing traffic sent Analysis

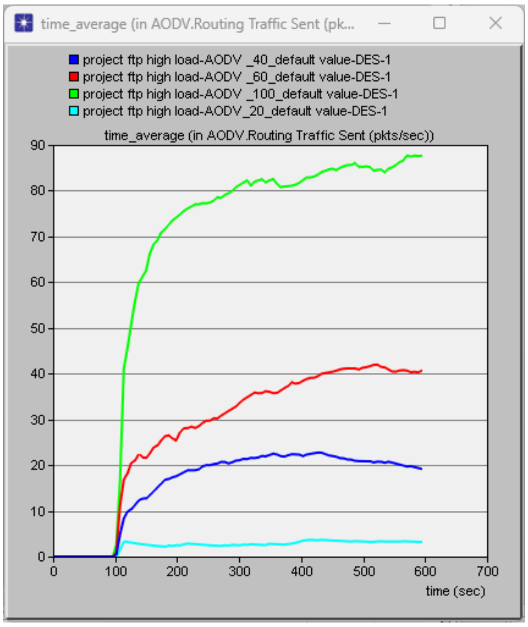

time_average (in AODV.Routing Traffic Sent (pk...
🟦 project ftp high load-AODV _40_default value-DES-1
🟥 project ftp high load-AODV _60_default value-DES-1
🟩 project ftp high load-AODV _100_default value-DES-1
🟦 project ftp high load-AODV_20_default value-DES-1
time_average (in AODV.Routing Traffic Sent (pkts/sec))
90
80
70
60
50
40
30
20
10
0
0
100
200
300
400
500
600
700
time (sec)

Fig 5.22: Routing Traffic sent of AODV protocol.

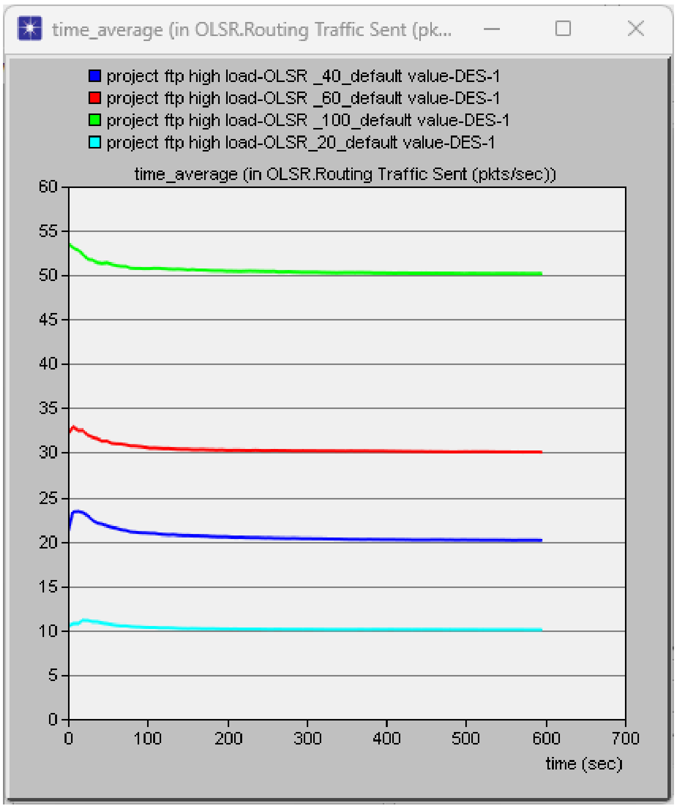


Fig 5.23: Routing Traffic sent of OLSR protocol

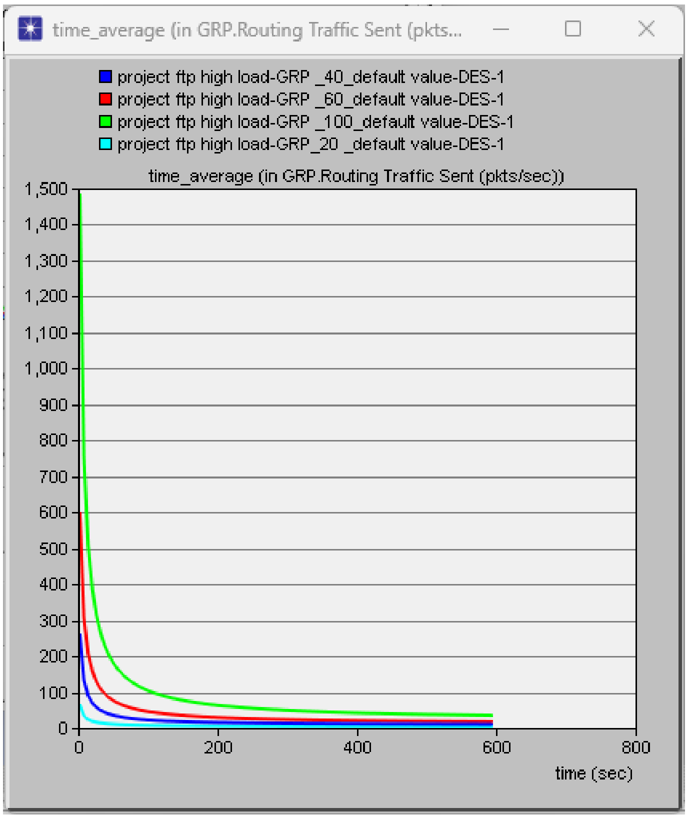


Fig 5.24: Routing Traffic sent of GRP protocol.

Table 5.7: Routing Traffic sent of AODV, OLSR, GRP.

Protocol	Node Density			
	20	40	60	100
AODV	2.384941	15.93742	27.84151	64.04789
OLSR	10.21705	20.60969	30.43233	50.54333
GRP	7.389284	21.4616	42.88325	96.61517

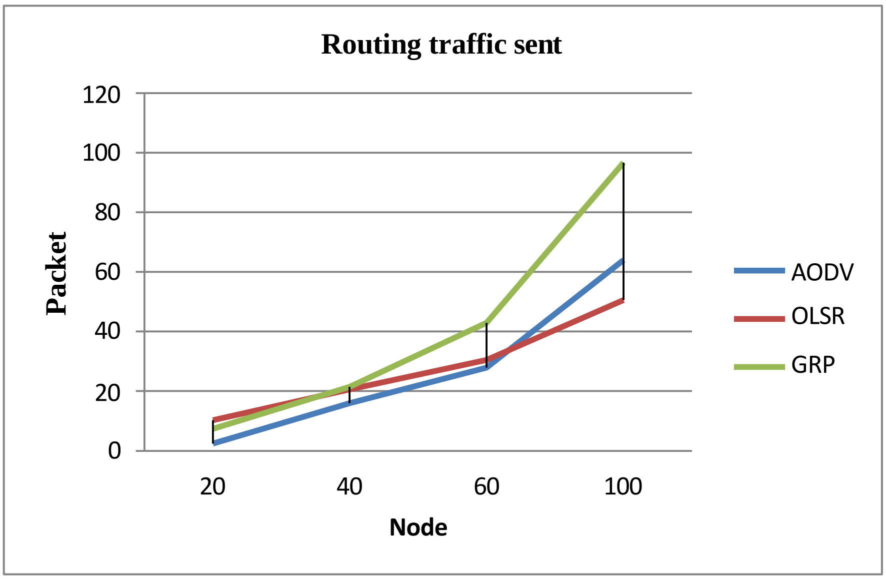


Fig 5.25: Routing traffic sent of AODV, OLSR, and GRP.

Figures 5.22 to 5.24 show the routing traffic sent by various routing protocols with 20, 40, 60, or 100 mobile nodes. In table 5.7, we've developed a traffic transmitted table for various routing protocols. Figure 5.25, which compares the traffic sent by the AODV, DSR, GRP, and OLSR, was created using data from table 5.7. We can see from this graph that GRP has the highest extreme and OLSR has the lowest.

5.4.2 Routing traffic received Analysis

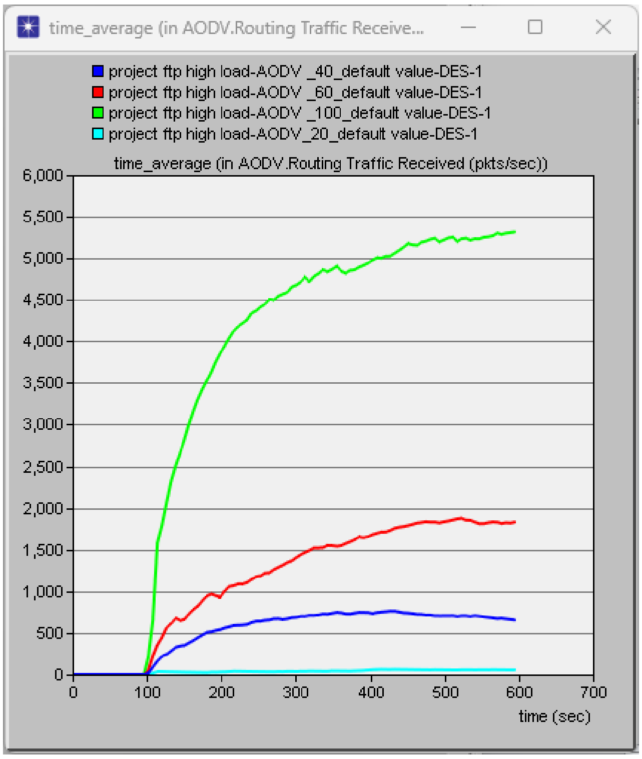


Fig 5.26: Routing Traffic received of AODV protocol.

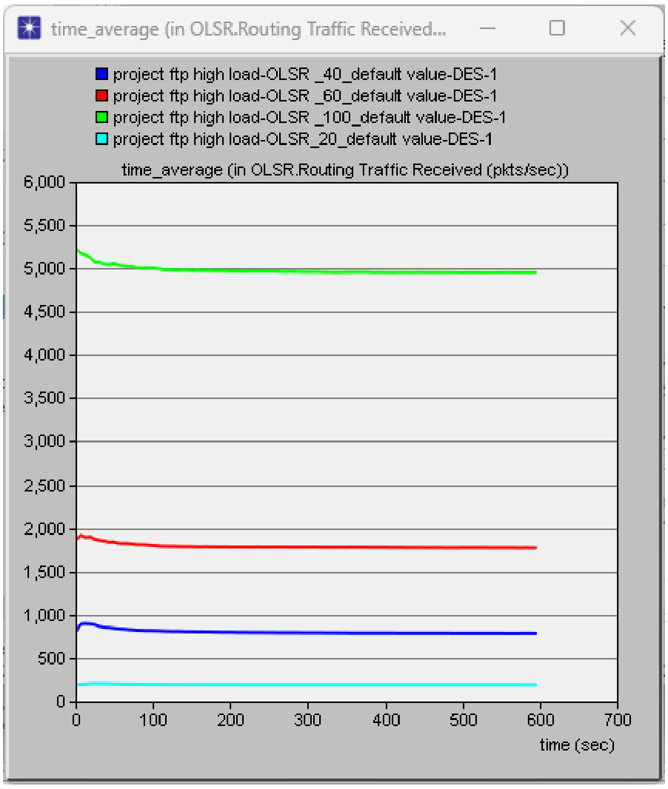


Fig 5.27: Routing Traffic received of OLSR protocol.

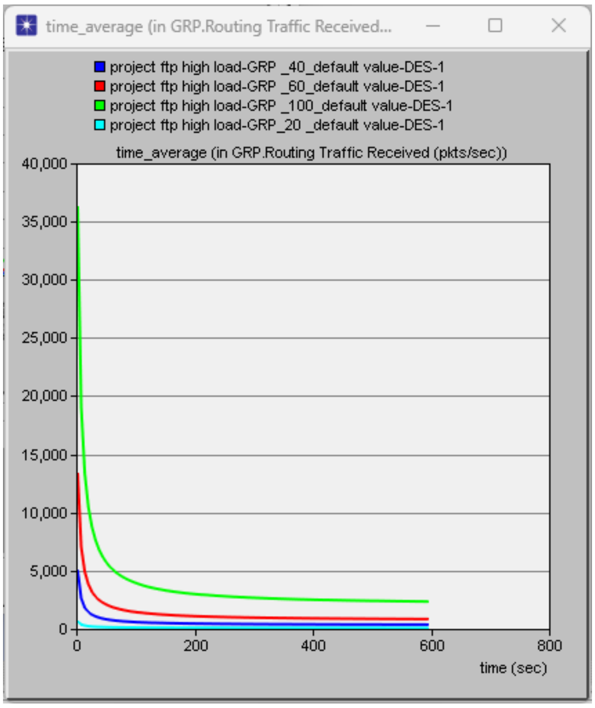

time_average (in GRP.Routing Traffic Received...
project ftp high load-GRP _40_default value-DES-1
project ftp high load-GRP _60_default value-DES-1
project ftp high load-GRP _100_default value-DES-1
project ftp high load-GRP_20 _default value-DES-1
time_average (in GRP.Routing Traffic Received (pkts/sec))
40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
0
200
400
600
800
time (sec)

Fig 5.28: Routing Traffic received of GRP protocol.

Table 5.8: Routing Traffic received of AODV, OLSR, GRP.

Protocol	Node Density			
	20	40	60	100
AODV	35.67528	516.6684	1160.922	3673.068
OLSR	192.8212	800.8934	1789.27	4979.403
GRP	111.9627	564.2144	1379.805	3779.998

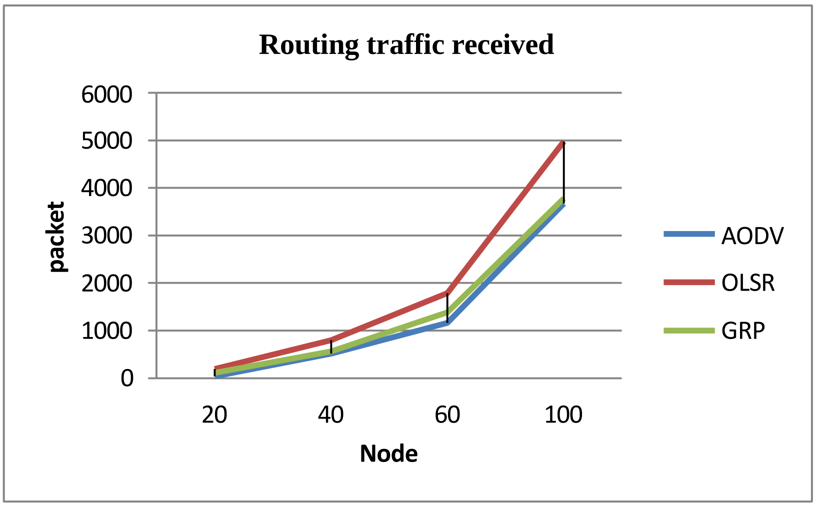


Fig 5.29: Routing traffic received of AODV, OLSR, GRP.

Figures 5.26 to 5.28 show the routing traffic that was received using various routing protocols when there were 20, 40, 60, or 100 mobile nodes. In table 5.8, we've developed a routing traffic received table for various routing protocols. Figure 5.29, which compares the routing traffic obtained from AODV, GRP, and OLSR, was created using data from table 5.8. We can observe from this figure that OLSR has the highest, AODV and that GRP is the same.

Table 5.9: Normalized routing load of AODV, OLSR, GRP.

Protocol	Node Density			
	20	40	60	100
AODV	0.0668513	0.0308465	0.023982	0.017437
OLSR	0.052987	0.025733	0.017008	0.010150
GRP	0.065997	0.038038	0.031079	0.025559

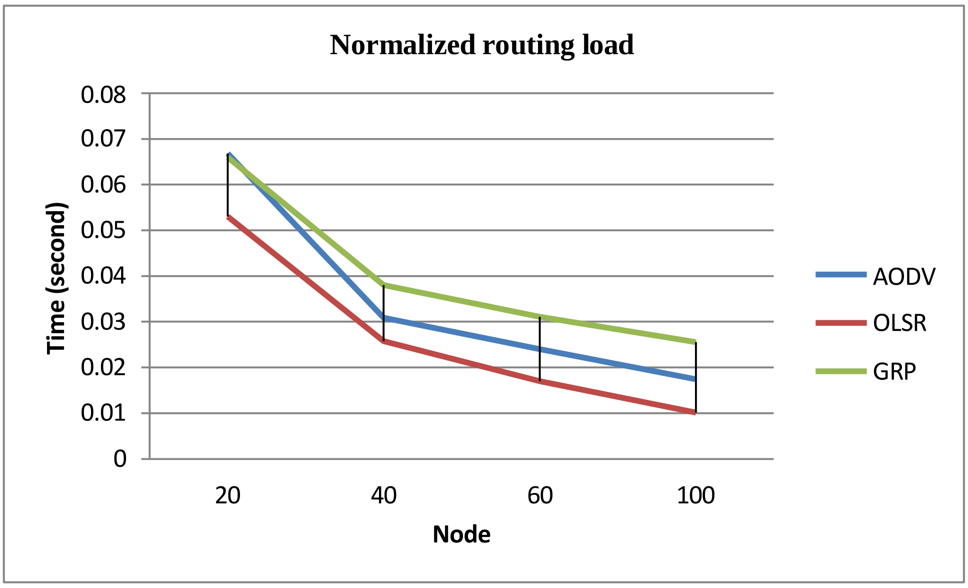


Fig 5.30: Normalized routing load of AODV, GRP, OLSR

Figure 5.30, which compares the Normalized routing load by AODV, OLSR, and GRP, was produced using data from table 5.9. We can observe from this figure that the Normalized routing load GRP has the highest, and OLSR has lowest.

5.5 Project 2:

- In this project we use VOIP (Ip Telephony) application and AODV,OLSR and GRP protocol for 20,40,60 ,100 node density.
- Now we analysis the delay, load, throughput, Packet delivery fraction and Normalized routing load for default value and jitter.

5.5.1 Delay Analysis:

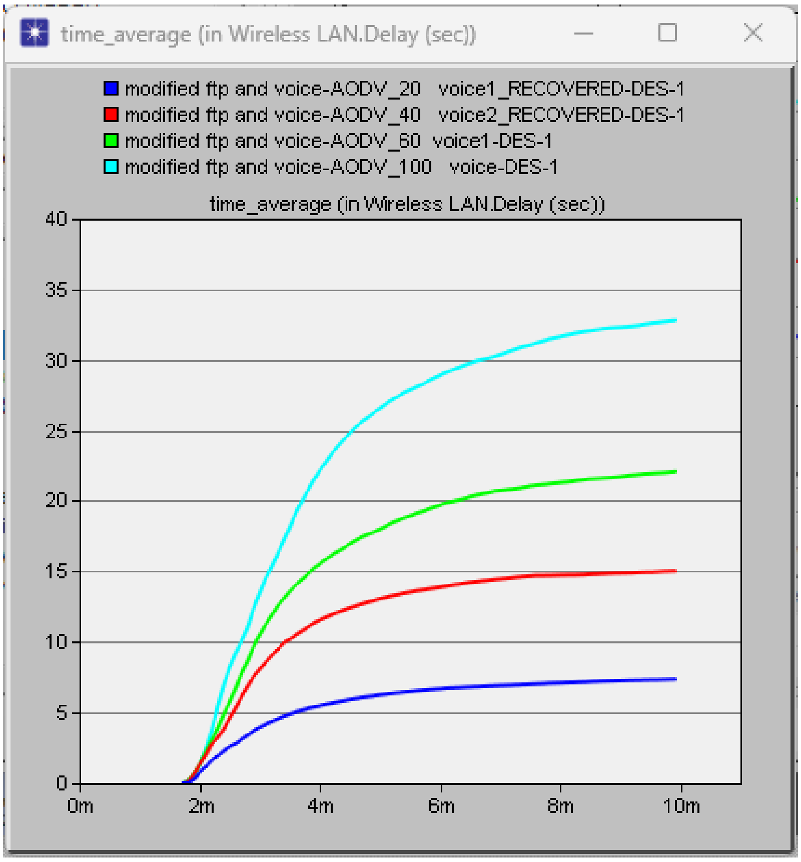


Fig 5.31: Delay of AODV protocol

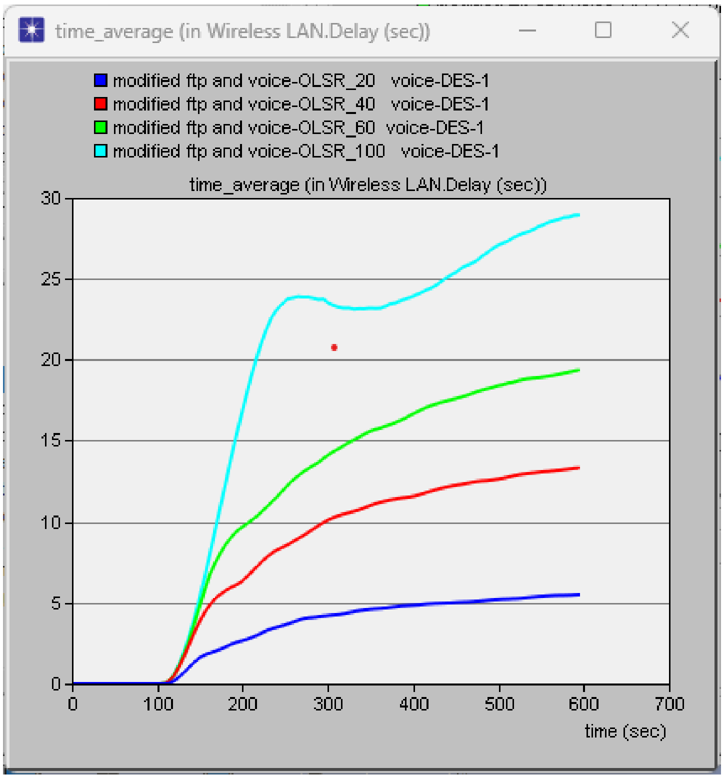


Fig 5.32: Delay of OLSR protocol

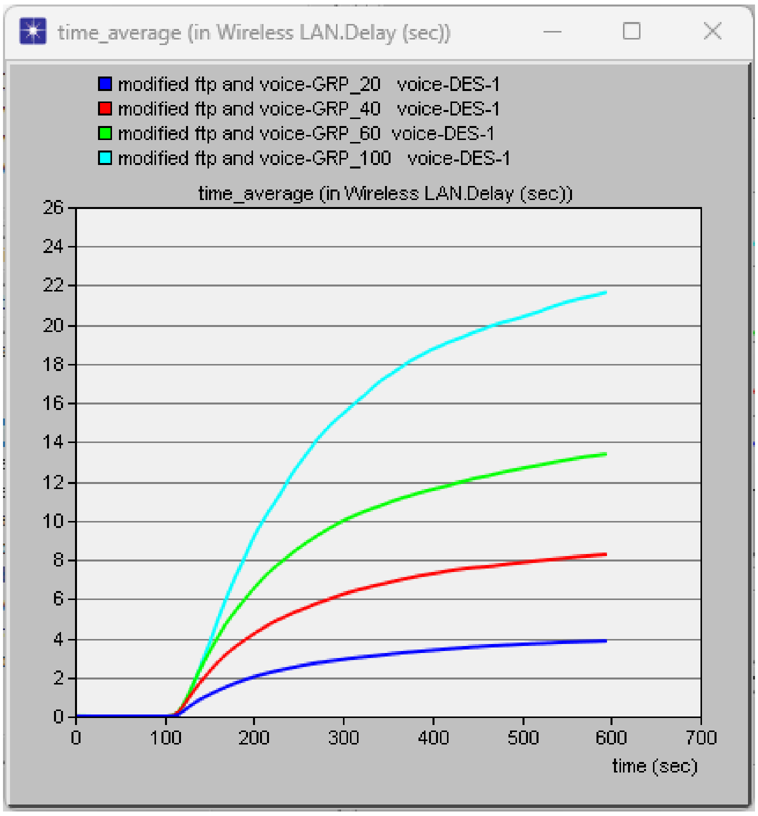


Fig 5.33: Delay of GRP protocol

Table 5.10: Delay (second) of AODV, OLSR, GRP.

Protocol	Node Density			
	20	40	60	100
AODV	4.779162	9.874995	13.896080	20.217831
OLSR	3.294792	7.948845	11.37214	17.50389
GRP	2.323746	4.961206	7.8964	12.34163

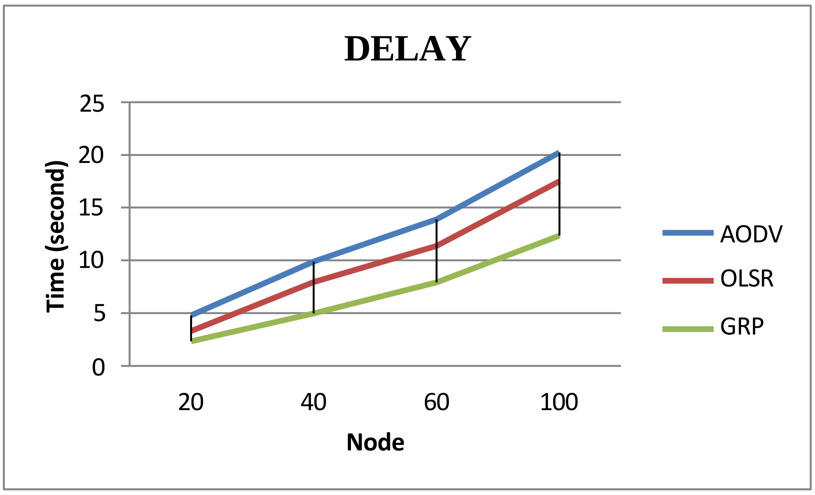


Fig 5.34: Delay (second) of AODV, OLSR, GRP.

Figures 5.31 to 5.33 show the delay of various routing protocols with varying numbers of (20,40,60,100) mobile nodes. In table 5.10, we've produced a latency comparison table for these routing protocols. We presented the comparative delays of the AODV, OLSR, and GRP in figure 5.34 using data from table 5.10. We can observe from this graph that AODV has the highest delay, but GRP has the lowest. Over OLSR performs around averagely.

5.5.2 Load Analysis

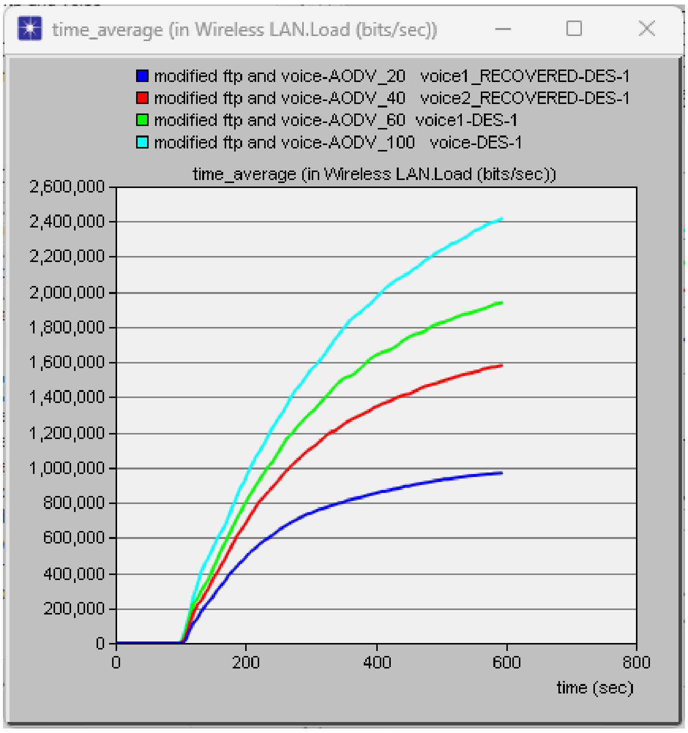


Fig 5.35: Load of AODV protocol

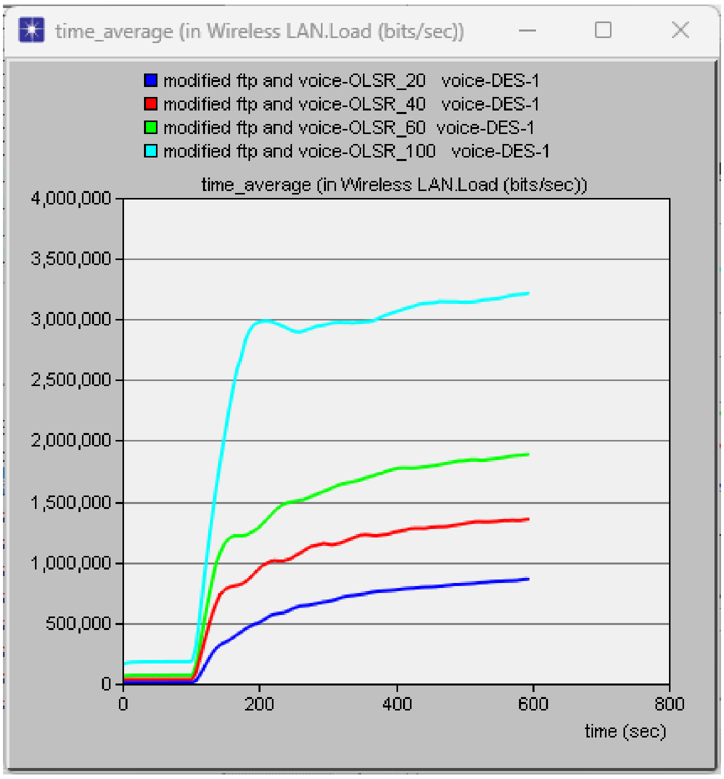


Fig 5.36: Load of OLSR protocol

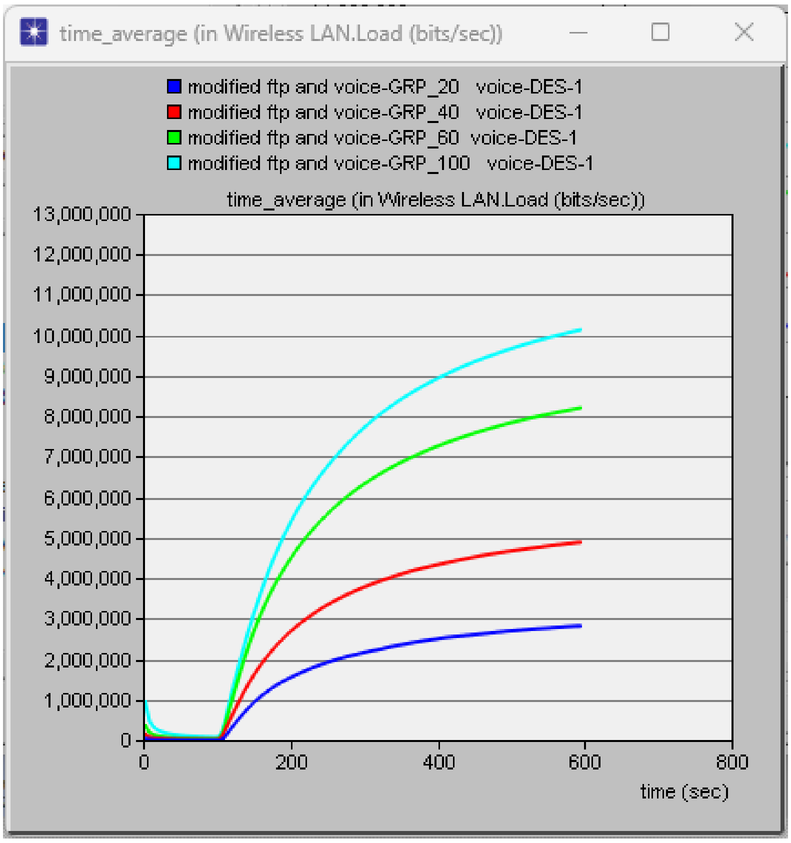


Fig 5.37: Load of GRP protocol

Table 5.11: Load of AODV, OLSR, GRP

Protocol	Node Density			
	20	40	60	100
AODV	586095.9	906284	1093678	1324584
OLSR	546444.6	920307	1296082	2366257
GRP	1735917	3018047	5055141	6201909

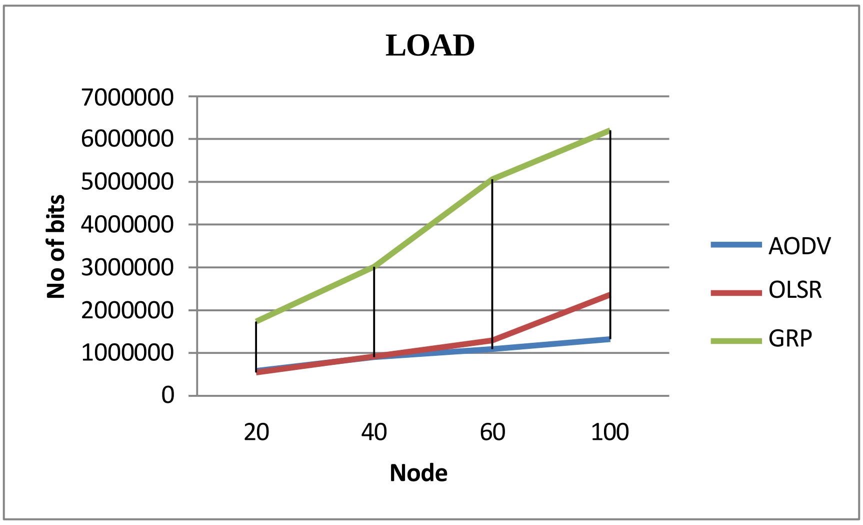


Fig 5.38: Load of AODV, OLSR, GRP.

Figures 5.35 to 5.37 show the load of various routing protocols with varying numbers of (20,40,60,100) mobile nodes. In table 5.11, we've produced a load comparison table for these routing protocols. We presented the comparative load of the AODV, OLSR, and GRP in figure 5.38 using data from table 5.11. We can observe from this graph that GRP has the highest load, but AODV has the lowest. Over AODV, OLSR performs around averagely.

5.5.3 Throughput Analysis

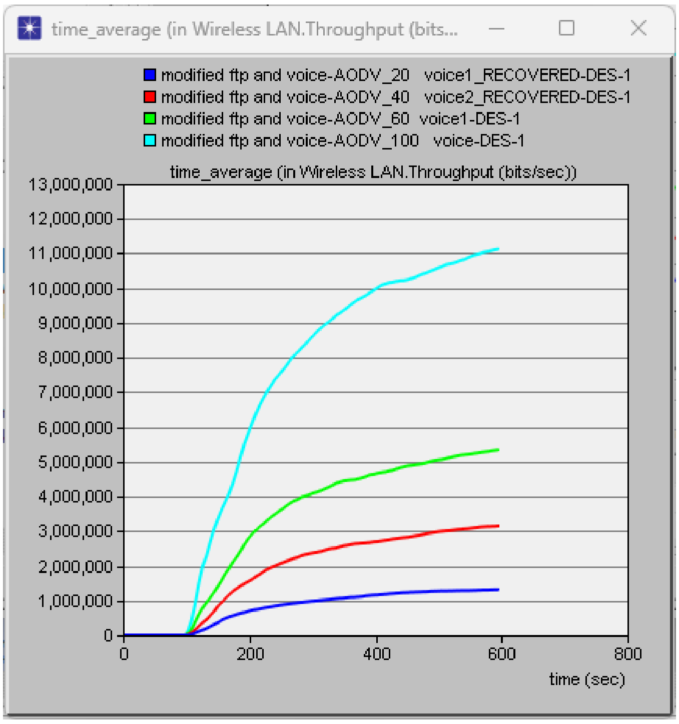

time_average (in Wireless LAN.Throughput (bits...
modified ftp and voice-AODV_20 voice1_RECOVERED-DES-1
modified ftp and voice-AODV_40 voice2_RECOVERED-DES-1
modified ftp and voice-AODV_60 voice1-DES-1
modified ftp and voice-AODV_100 voice-DES-1
time_average (in Wireless LAN.Throughput (bits/sec))
13,000,000
12,000,000
11,000,000
10,000,000
9,000,000
8,000,000
7,000,000
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
0
0
200
400
600
800
time (sec)

Fig 5.39: Throughput of AODV protocol

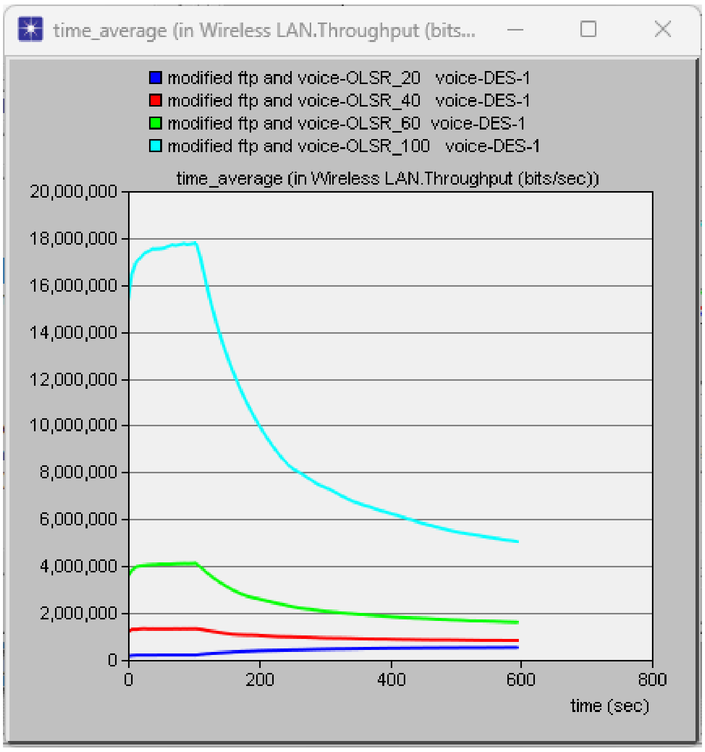


Fig 5.40: Throughput of OLSR protocol

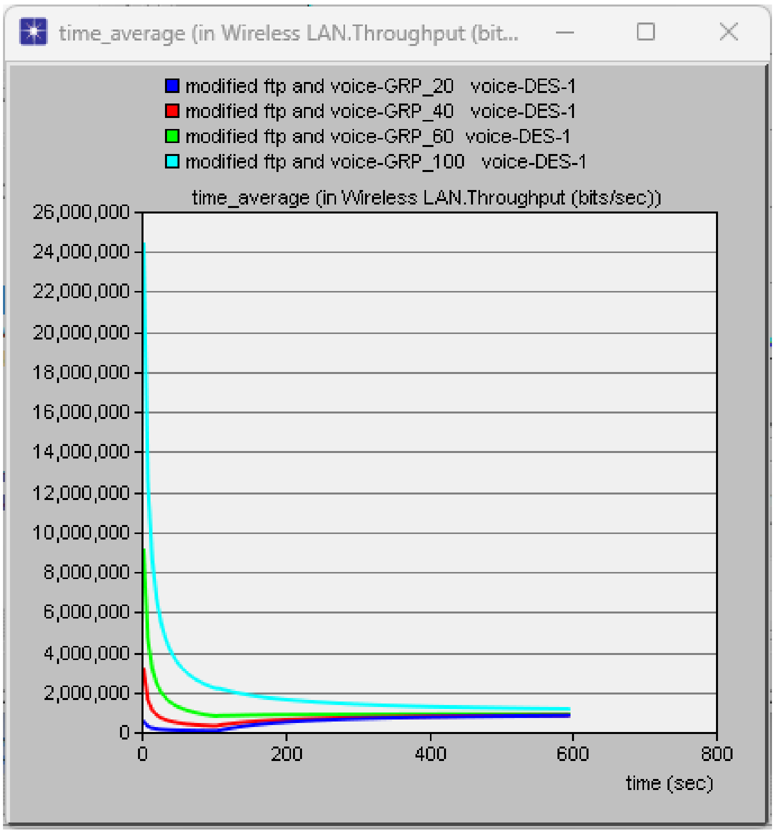


Fig 5.41: Throughput of GRP protocol

Table 5.12: Throughput of AODV, OLSR, GRP

Protocol	Node Density			
	20	40	60	100
AODV	795437.7	1873825.2	3223094.2	6812512.2
OLSR	404278.3	1012882	2495281	9531076
GRP	559557.9	727204.6	1097776	2146563

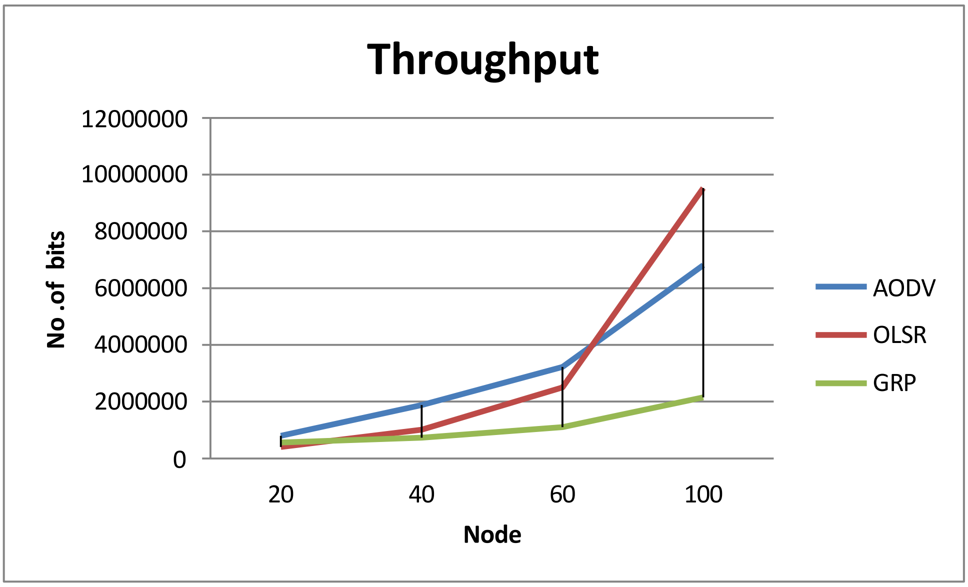


Fig 5.42: Throughput of AODV, OLSR, GRP.

Figures 5.39 to 5.41 show the throughput of various routing protocols with varying numbers of (20,40,60,100) mobile nodes. In table 5.12, we've produced a throughput comparison table for these routing protocols. We presented the comparative throughput of the AODV, OLSR, and GRP in figure 5.42 using data from table 5.12. We can observe from this graph that OLSR has the highest throughput, but GRP has the lowest. Over AODV performs around averagely.

5.6 PDR/ Packet Delivery Ratio Analysis:

5.6.1 Traffic received analysis

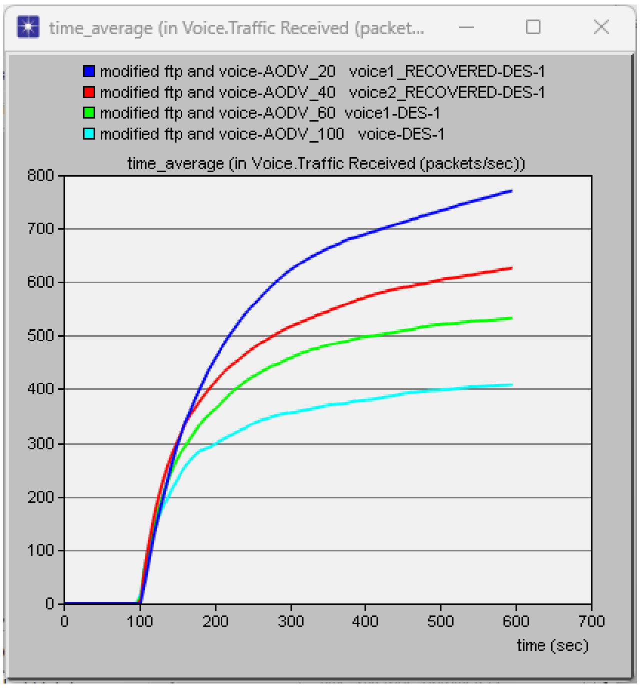


Fig 5.43: Traffic received of AODV protocol

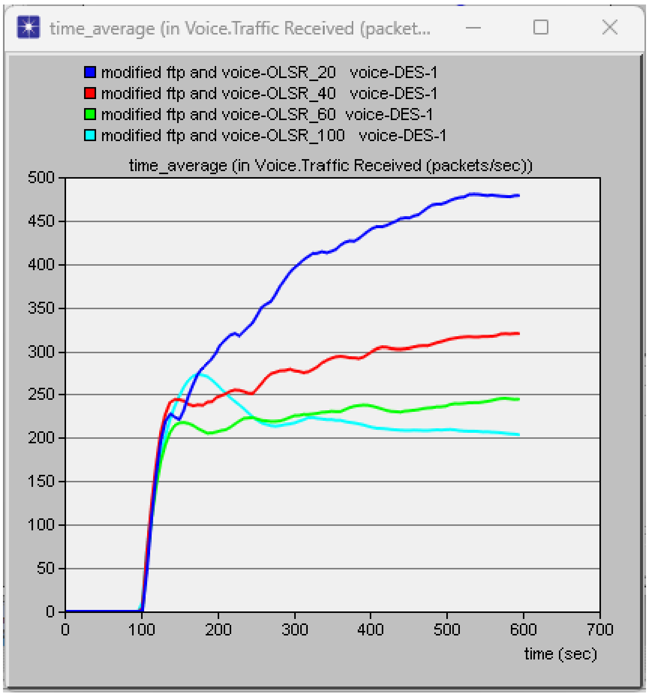


Fig 5.44: Traffic received of OLSR protocol

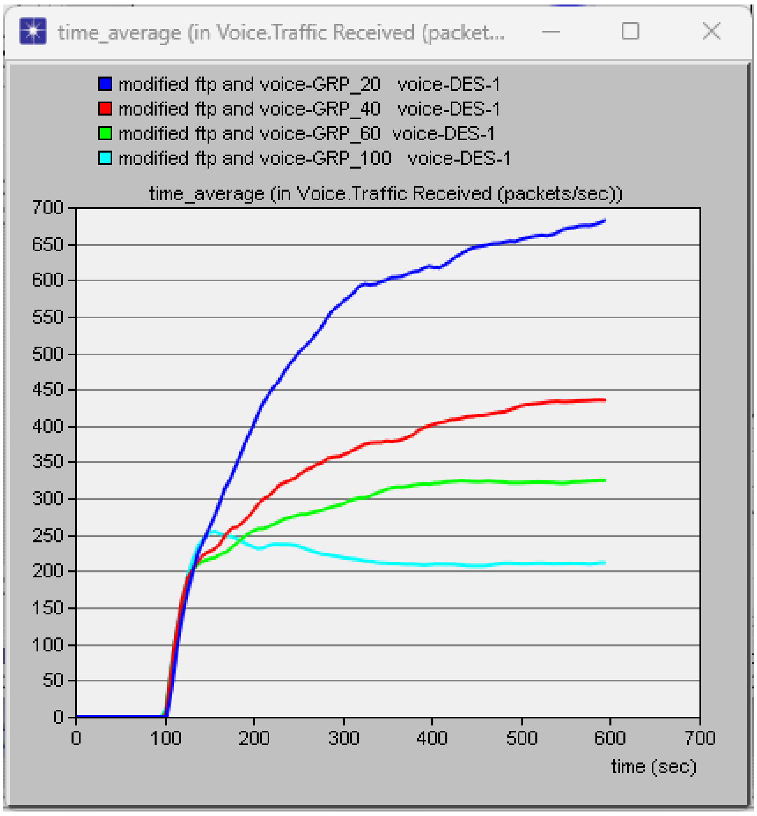


Fig 5.45: Traffic received of GRP protocol

Table 5.13: Traffic received of AODV, OLSR, GRP

Protocol	Node Density			
	20	40	60	100
AODV	486.7593	412.5398	360.2324	282.1804
OLSR	315.2653	227.8535	182.7229	178.3138
GRP	437.7452	291.602	235.7777	176.9421

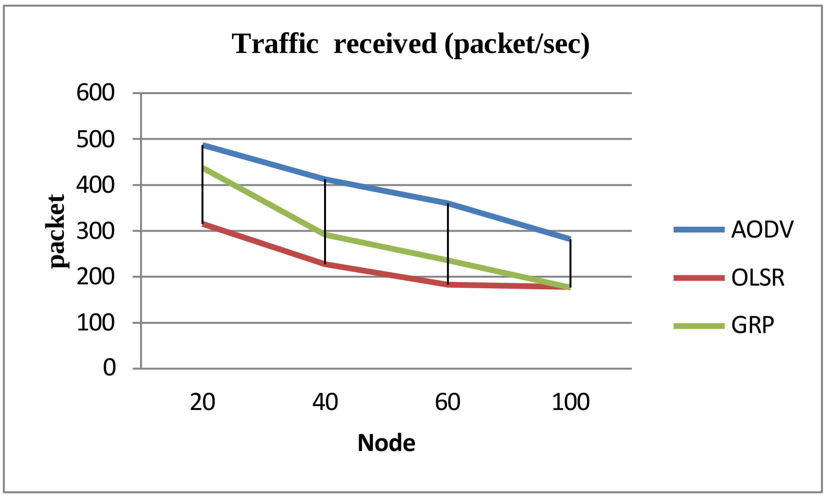


Fig 5.46: Traffic received of AODV, OLSR, GRP

Figures 5.43 to 5.45 show the traffic received for various routing protocols with 20, 40, 60, and 100 mobile nodes, respectively. In table 5.13, we've developed a traffic received table for these routing protocols. We plotted the comparative traffic received by AODV, OLSR, and GRP from table 5.13, and the result is shown in figure 5.46. We can observe from this number that AODV is higher than OLSR and GRP.

5.6.2 Traffic sent analysis

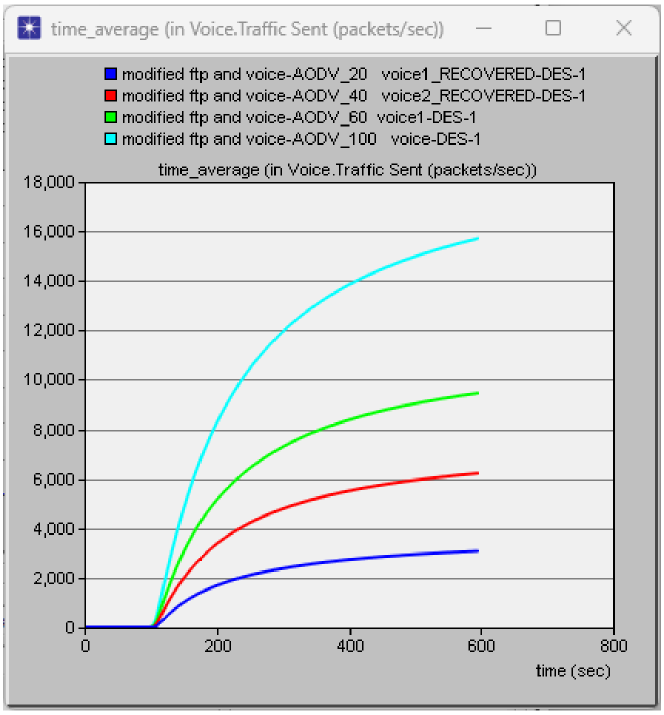

time_average (in Voice.Traffic Sent (packets/sec))
🟦 modified ftp and voice-AODV_20 voice1_RECOVERED-DES-1
🟥 modified ftp and voice-AODV_40 voice2_RECOVERED-DES-1
🟩 modified ftp and voice-AODV_60 voice1-DES-1
🟦 modified ftp and voice-AODV_100 voice-DES-1
time_average (in Voice.Traffic Sent (packets/sec))
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
0
200
400
600
800
time (sec)

Fig 5.47: Traffic sent of AODV protocol

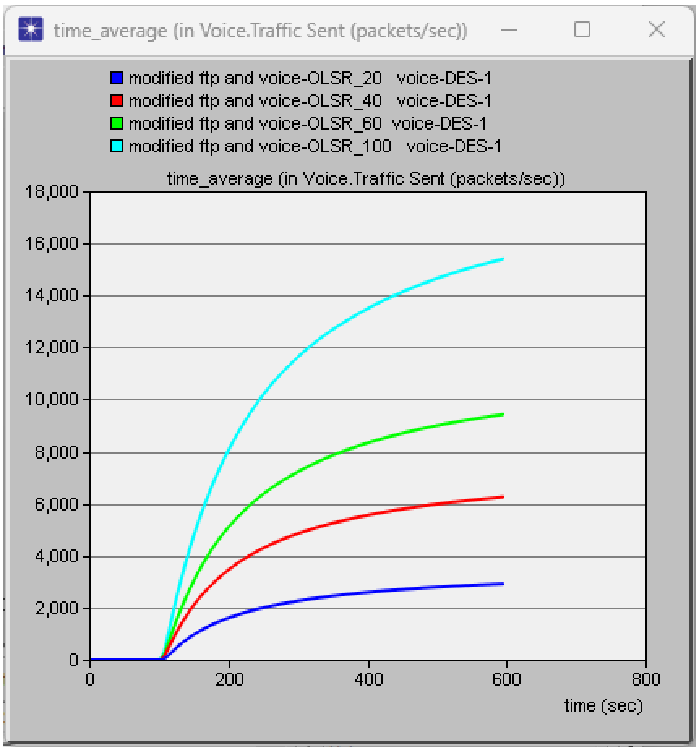


Fig 5.48: Traffic sent of OLSR protocol

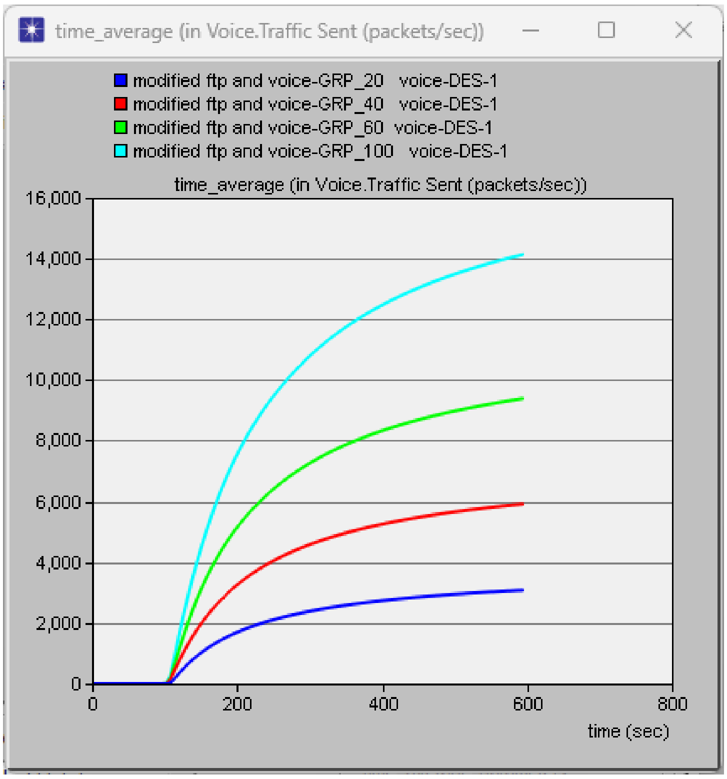


Fig 5.49: Traffic sent of GRP protocol

Table 5.14: Traffic sent of AODV, OLSR, GRP

Protocol	Node Density			
	20	40	60	100
AODV	1896.070	3817.216	5811.24271	9543.132
OLSR	1797.772	3858.71	5767.459	9313.96
GRP	1898.251	3651.08	5781.34	8616.308

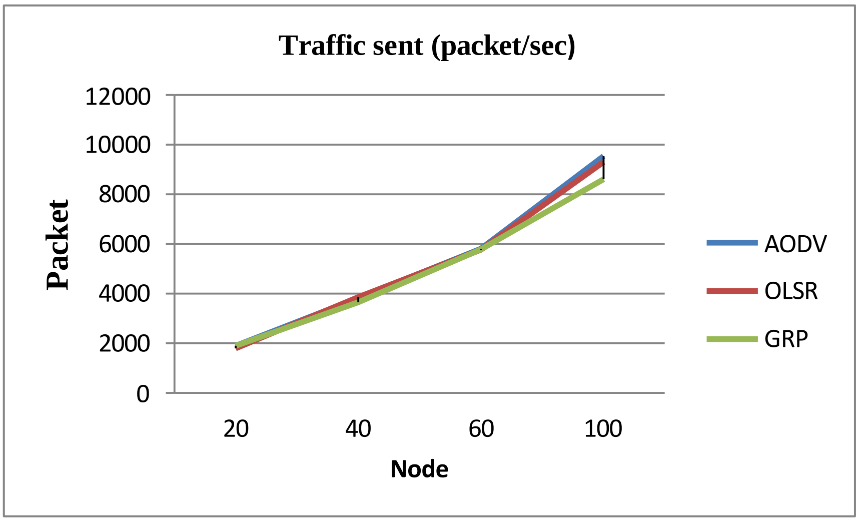


Fig 5.50: Traffic sent of AODV, OLSR, GRP

Figures 5.47 to 5.49 show the traffic sent for various routing protocols with 20, 40, 60, and 100 mobile nodes, respectively. In table 5.14, we've developed a traffic received table for these routing protocols. We plotted the comparative traffic sent by AODV, OLSR, and GRP from table 5.14, and the result is shown in figure 5.50. We can observe from this number that OLSR and AODV are almost same than GRP.

Table 5.15: Packet delivery ratio of AODV, OLSR, GRP.

Protocol	Node Density			
	20	40	60	100
AODV	0.25672	0.108073	0.061989	0.029569
OLSR	0.175364	0.059049	0.031682	0.019145
GRP	0.230604	0.079867	0.040783	0.020536

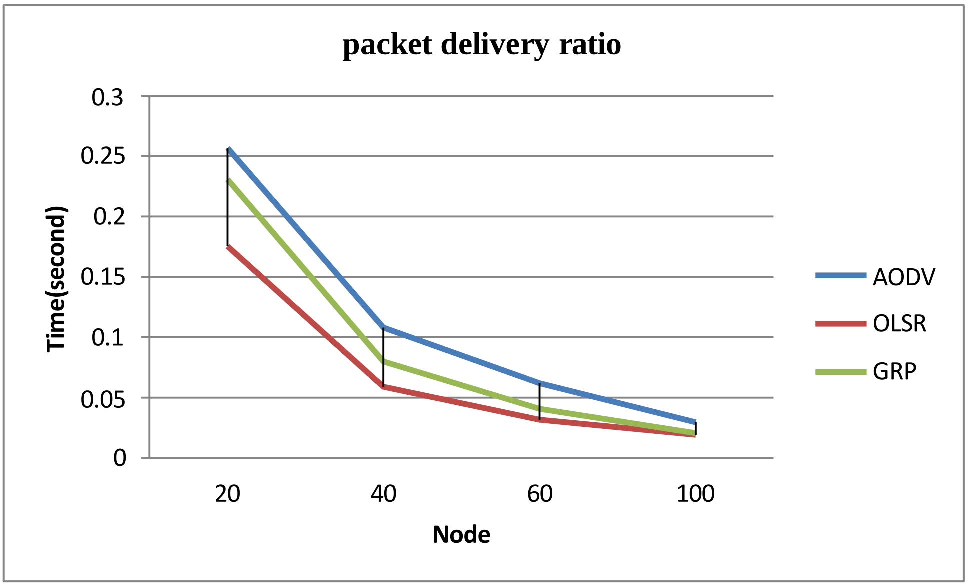


Fig 5.51: Packet delivery ratio of AODV, OLSR, GRP.

Figure 5.51, which compares the packet delivery ratio by AODV, OLSR, and GRP, was produced using data from table 5.15. We can observe from this figure that the packet delivery ratio AODV has the highest, and OLSR has lowest.

5.7 Normalized routing load Analysis

5.7.1 Routing traffic sent Analysis

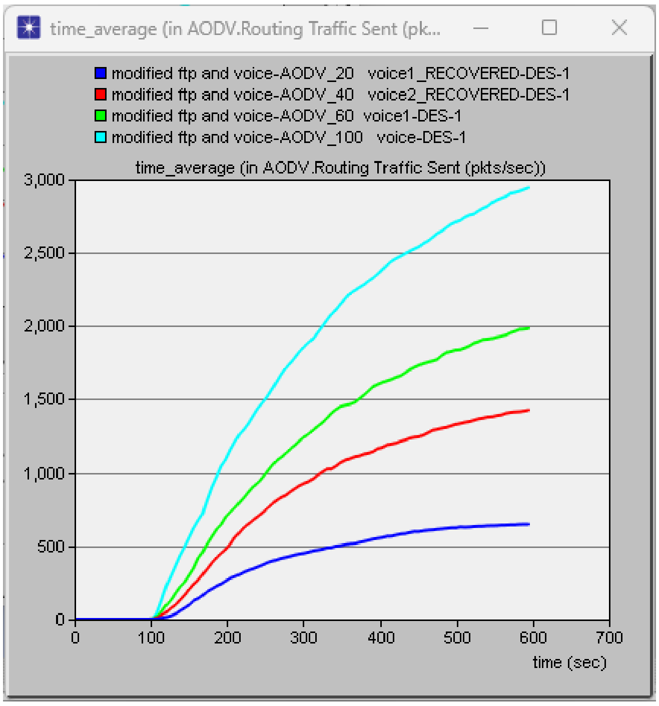


Fig 5.52: Routing Traffic sent of AODV protocol.

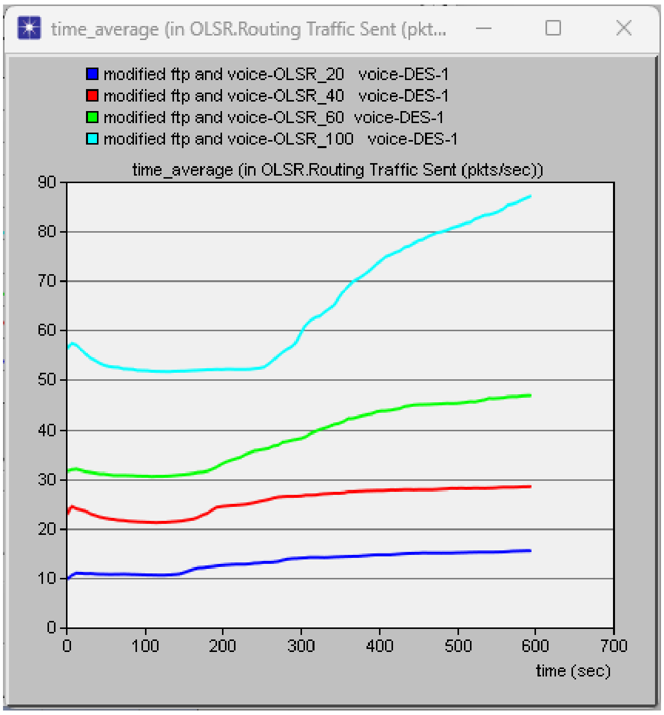


Fig 5.53: Routing Traffic sent of OLSR protocol.

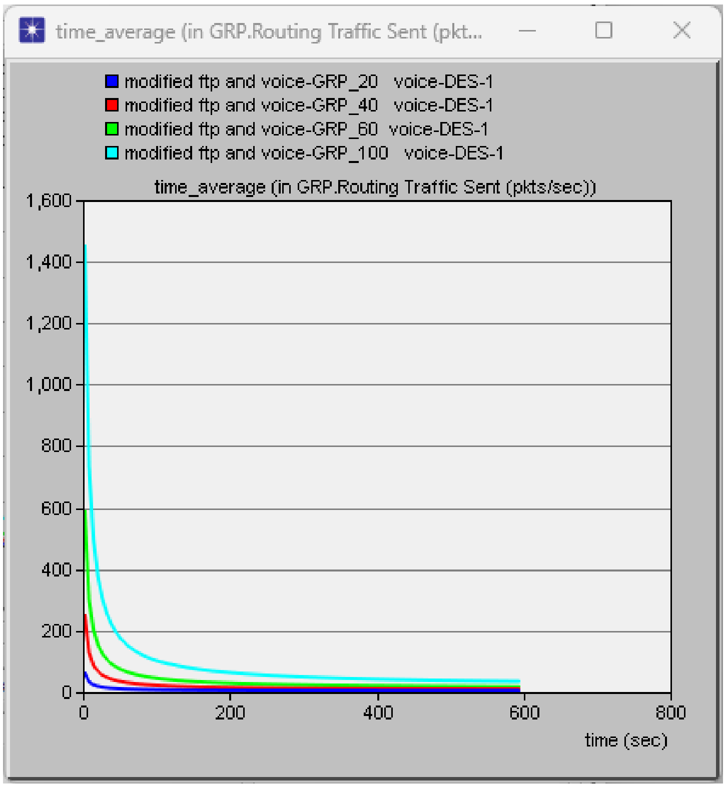


Fig 5.54: Routing Traffic sent of GRP protocol.

Table 5.16: Routing traffic sent of AODV, OLSR, GRP

Protocol	Node Density			
	20	40	60	100
AODV	368.02056	769.21431	1057.28499	1585.25622
OLSR	13.23737	25.48879	38.27408	64.54843
GRP	7.334189	20.89697	42.28841	95.43161

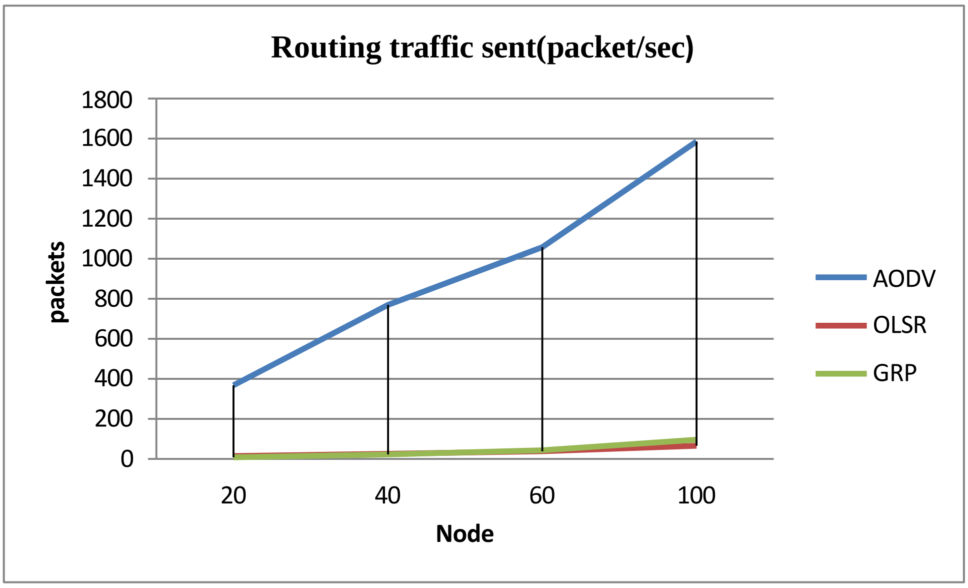


Fig 5.55: Routing traffic sent of AODV, OLSR, GRP

Figures 5.52 to 5.54 show the traffic received for various routing protocols with 20, 40, 60, and 100 mobile nodes, respectively. In table 5.16, we've developed a routing traffic sent table for these routing protocols. We plotted the comparative traffic received by AODV, OLSR, and GRP from table 5.16, and the result is shown in figure 5.55. We can observe from this number that AODV is higher than OLSR and GRP.

5.7.2 Routing traffic received Analysis

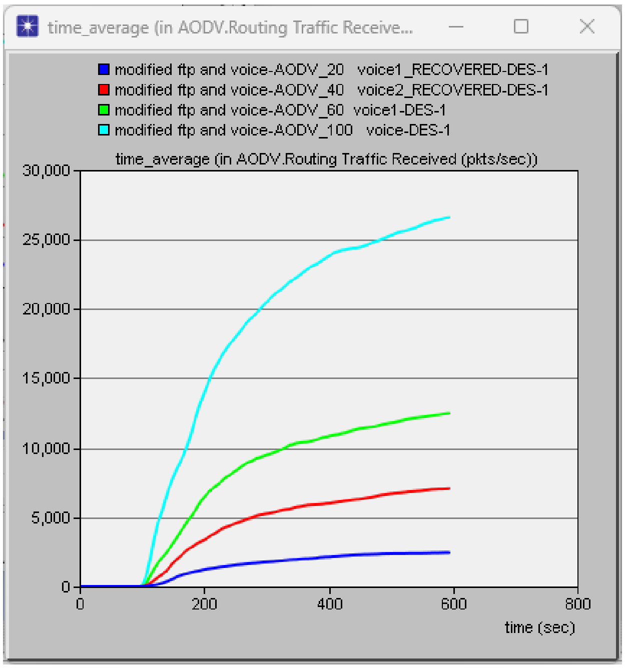

time_average (in AODV.Routing Traffic Receive...
modified ftp and voice-AODV_20 voice1_RECOVERED-DES-1
modified ftp and voice-AODV_40 voice2_RECOVERED-DES-1
modified ftp and voice-AODV_60 voice1-DES-1
modified ftp and voice-AODV_100 voice-DES-1
time_average (in AODV.Routing Traffic Received (pkts/sec))
30,000
25,000
20,000
15,000
10,000
5,000
0
0
200
400
600
800
time (sec)

Fig 5.56: Routing Traffic received of AODV protocol.

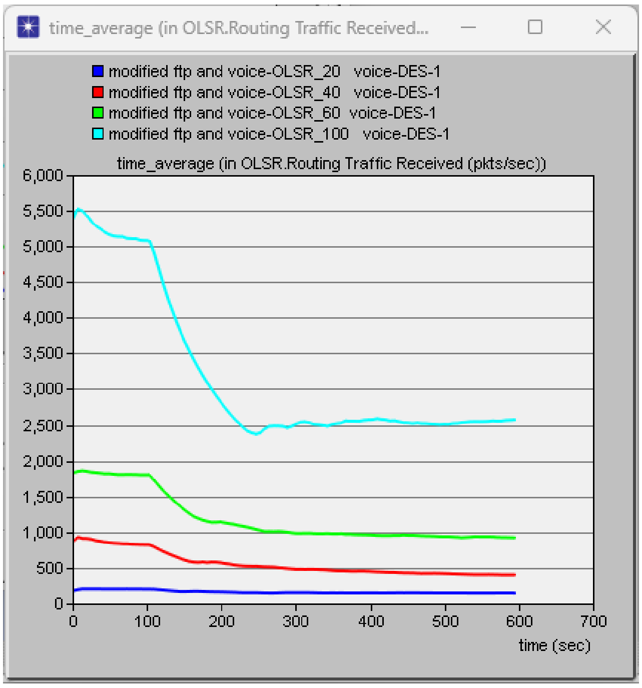


Fig 5.57: Routing Traffic received of OLSR protocol.

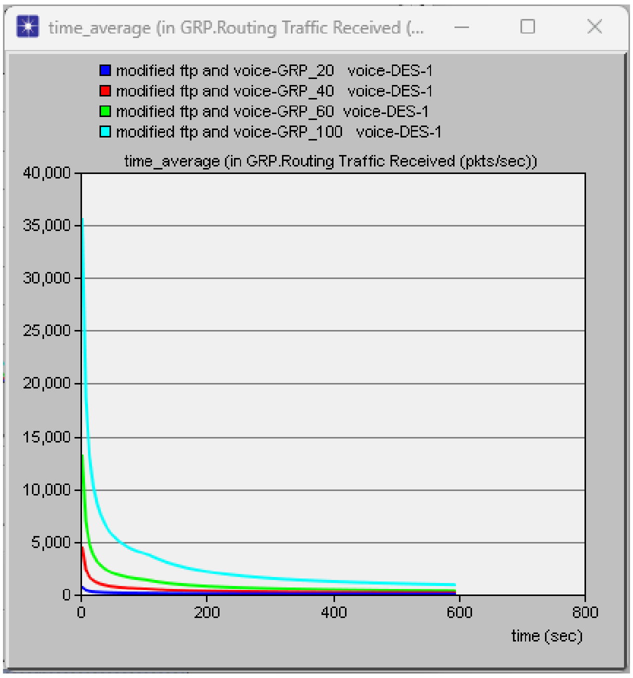


Fig 5.58: Routing Traffic received of GRP protocol.

Table 5.17: Routing traffic received of AODV, OLSR, GRP

Protocol	Node Density			
	20	40	60	100
AODV	1455.7172	4156.3403	7480.8142	16213.6989
OLSR	160.2316	556.8529	1183.687	3199.397
GRP	96.52113	420.5752	1070.45	2873.705

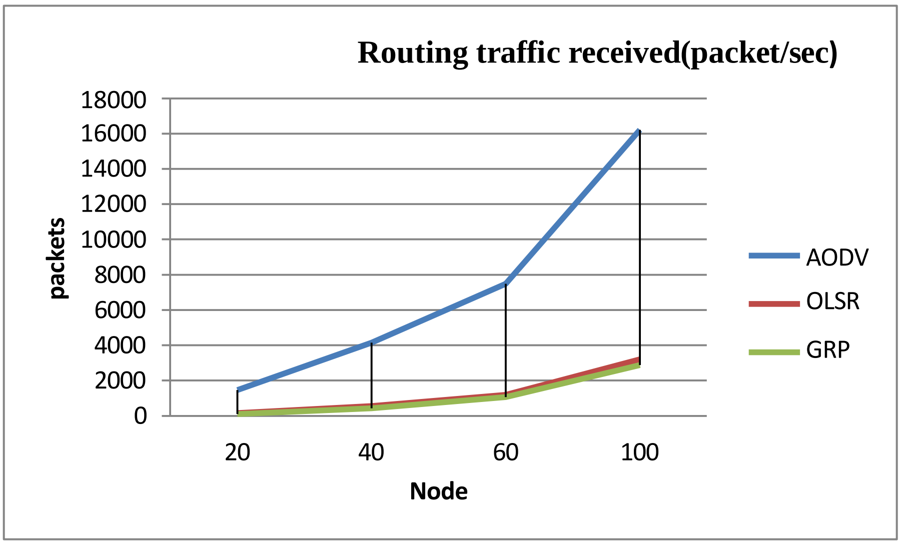


Fig 5.59 Routing traffic received of AODV, OLSR, GRP

Figures 5.56 to 5.58 show the traffic received for various routing protocols with 20, 40, 60, and 100 mobile nodes, respectively. In table 5.17, we've developed a traffic received table for these routing protocols. We plotted the comparative traffic received by AODV, OLSR, and GRP from table 5.17, and the result is shown in figure 5.59. We can observe from this number that AODV is higher than OLSR and GRP.

Table 5.18: Normalized routing load of AODV, OLSR, GRP.

Protocol	Node Density			
	20	40	60	100
AODV	0.25281	0.18507	0.141333	0.097773
OLSR	0.082614	0.045773	0.032335	0.020175
GRP	0.075985	0.049687	0.039505	0.033209

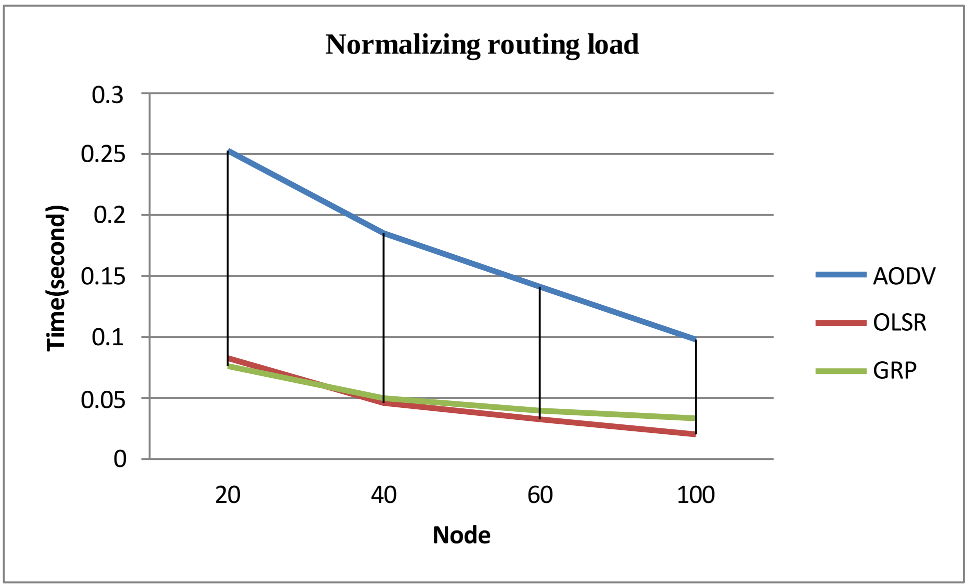


Fig 5.60: Normalized routing load of AODV, OLSR, GRP.

Figure 5.60, which compares the Normalized routing load by AODV, OLSR, and GRP, was produced using data from table 5.18. We can observe from this figure that the Normalized routing load AODV has the highest, and OLSR has lowest.

5.8 Jitter Analysis

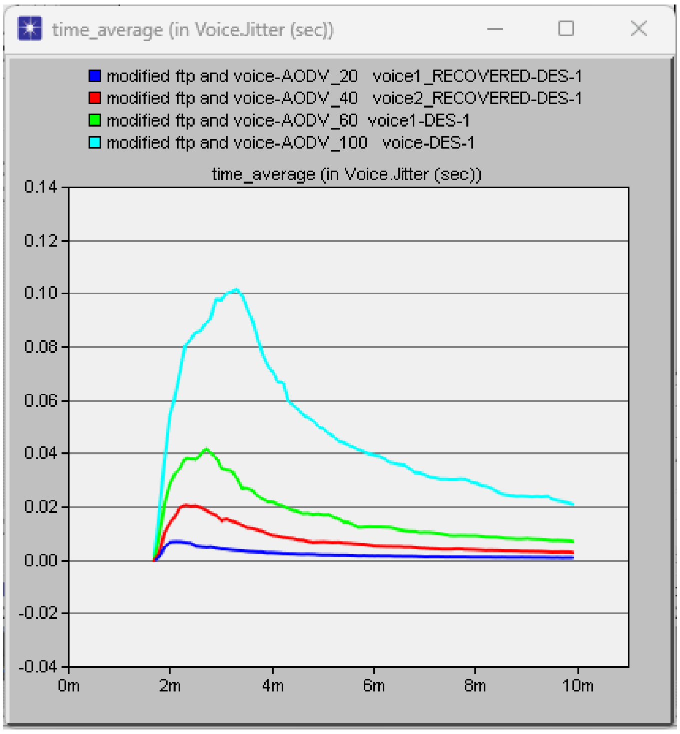


Fig 5.61: Jitter of AODV protocol

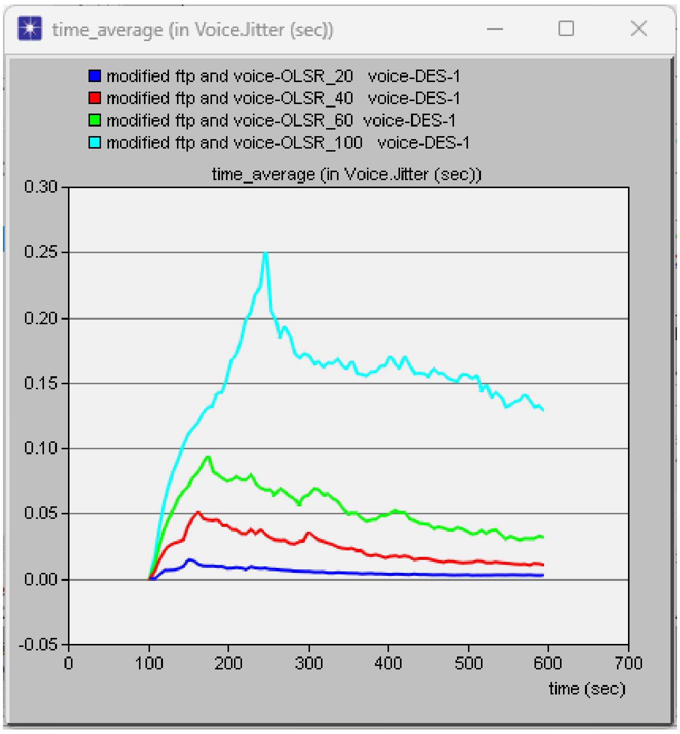


Fig 5.62: jitter of OLSR protocol

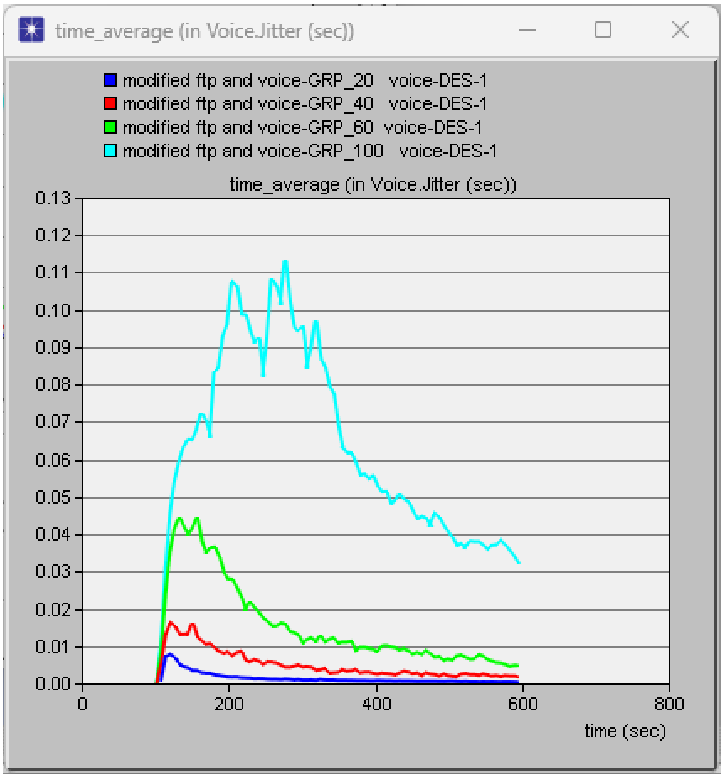


Fig 5.63: jitter of GRP protocol

Table 5.19: Jitter of AODV, OLSR, GRP.

Protocol	Node Density			
	20	40	60	100
AODV	0.001702	0.006118	0.013743	0.039424
OLSR	0.004159	0.019115	0.043177	0.124115
GRP	0.001118	0.004167	0.012828	0.052332

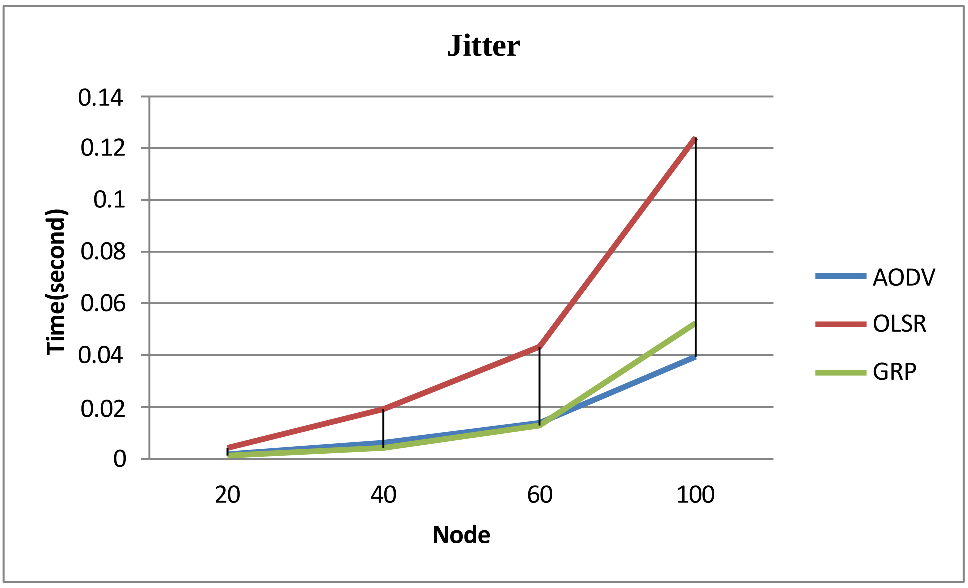


Fig 5.64: Jitter of AODV, OLSR, GRP.

Figure 5.64, which compares the jitter by AODV, OLSR, and GRP, was produced using data from table 19. We can observe from this figure that the jitter OLSR has the highest, and AODV has lowest.

Chapter 6

Conclusion and Future Work

In our research, we have opted to use the AODV, OLSR, and GRP routing protocols. We have assessed the three routing protocols AODV, OLSR, and GRP's performance in terms of parameters like throughput, load, average end-to-end delay, jitter, packet delivery ratio, and normalized routing load. FTP and VOIP have been employed as our application protocols. Throughput demonstrates that OLSR performs better for both FTP and VOIP. However, it is clear that OLSR outperforms VOIP in FTP.

However, both in FTP and VOIP, GRP has the lowest throughput. End-to-end delays show that FTP and VOIP both have longer average end-to-end delays than the other two routing methods. The end-to-end delay has a significant negative impact on the AODV protocol. On the other hand, there are only slight changes between the delay values for GRP and OLSR.

We can see from the normalized routing load that the FTP traffic load for GRP is very high. However, the traffic load for AODV in VOIP is relatively significant. Therefore, AODV does not function well in FTP. OLSR functions admirably in both applications and has a very light traffic load. According to the packet delivery ratio, the OLSR traffic load for FTP is very high. However, PDR for AODV in VOIP is relatively high. Therefore, AODV does not function well in FTP. When it comes to jitter, we can see that VOIP jitter for the OLSR protocol is very high and for the AODV protocol is lowest.

In our upcoming work, we will analysis our protocols for security issue and make the protocol more reliable and efficient.

References

[1] H. Singh, H. Kaur, R. Malhotra, A. Sharma, “Performance Investigation of Reactive AODV and Hybrid GRP Routing Protocols under Influence of IEEE 802.11n MANET,” Fifth International Conference on Advanced Computing & Communication Technologies, Haryana, pp. 325-328, 2015.

[2] H. Singh, H. Kaur, A. Sharma and R. Malhotra, "Performance Investigation of Reactive AODV and Hybrid GRP Routing Protocols under Influence of IEEE 802.11n MANET," Fifth International Conference on Advanced Computing & Communication Technologies, Haryana, 2015, pp. 325-328, 2015.

[3] A. Srivastava, D. Kumar and S. C. Gupta, “Performance comparison of pro-active and reactive routing protocols for MANET,’ International Conference on Computing, “Communication and Applications, Dindigul, Tamilnadu, pp. 1-4, 2012.

[4] M. Fazeli and H. Vaziri, “Assessment of Throughput Performance Under OPNET Modeler Simulation Tools in Mobile Ad Hoc Networks (MANETs), “ Third International Conference on Computational Intelligence, Communication Systems and Networks, Bali, pp. 328-331,2011.

[5] D. Kumar, A. Srivastava and S. C. Gupta, “Performance comparison of pro-active and reactive routing protocols for MANET,’ International Conference on Computing, Communication and Applications, Dindigul, Tamilnadu, pp. 1-4, 2012.

[6] M. Rajput, P. Khatri, A. Shastri and K. Solanki, "Comparison of Ad-hoc reactive routing protocols using OPNET modeler," International Conference on Computer Information Systems and Industrial Management Applications (CISIM), Krackow, pp. 530-534, 2010.

[7] D. Kumar, A. Srivastava and S. C. Gupta, "Performance comparison of pro-active and reactive routing protocols for MANET," International Conference on Computing, Communication and Applications, Dindigul, Tamilnadu, pp. 1-4, 2012.

[8] Y. Bai, Y. Mai and N. Wang, "Performance comparison and evaluation of the proactive and reactive routing protocols for MANETs," Wireless Telecommunications Symposium (WTS), Chicago, IL, pp. 1-5, 2017.

[9] C. Mbarushimana and A. Shahrabi, “Cooperative study of Reactive and Proactive Routing Protocols for Ad hoc Networks”, AINAW-IEEE, 2007.

[10] A. Srivastava, D. Kumar, and S. C. Gupta, "Performance comparison of reactive and pro-active routing protocols for MANET," International Conference on Computing, Communication and Applications, Dindigul, Tamilnadu, pp. 1-4, 2012.

[11] Ahmad, I., Ashraf, U., Anum, S., & Tahir, H. (2014). Route Establishment and enhanced AODV Route Discovery for QoS Provision for Real-Time Transmission in MANET. International Journal of Computer Networks & Communications, 6(2), 79-87. doi:10.5121/ijcnc.2014.6207.

[12] Malini, S., Kannan, E., & Valarmathi, A. (2012). Performance optimization of single- path and multi-path AODV using response surface method (RSM). In (pp. 1-4). USA: IEEE. doi:10.1109/SECon.2012.6196895.

[13] Abdullah Hani, Zuraida Binti and Mohd.Dani Bin Baba, "Designing Routing Protocols for Mobile Ad hoc Networks", IEEE 2003.

[14] Perkins, C. E.; Belding-Royer, E.; Das, S. R.; "Ad Hoc on-demand distance vector routing," RFC 3561, 2003.

[15] Alani, "MANET security: A survey," in Computing and Engineering (ICCSCE), Proceedings of the 2014 IEEE International Conference on Control System, pp. 559–564, Penang, Malaysia, November 2014.