MODELLING AND DEVELOPMENT OF A MOBILE AD-HOC NETWORK USING OPTIMIZED LINK STATE ROUTING PROTOCOL

BY

OGEFERE EFETURI
ENG1403690

A PROJECT SUBMITTED TO THE DEPARTMENT OF ELECTRICAL AND ELECTRONIC, FACULTY OF ENGINEERING, UNIVERSITY OF BENIN IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF BACHELOR OF ENGINEERING (B.ENG) IN ELECTRICAL AND ELECTRONIC ENGINEERING

JULY, 2021

CERTIFICATION

This is to certify that **OGEFERE EFETURI EMMANUEL** with Matriculation number **ENG 1403690** carried out this research project titled" MODELLING AND DEVELOPMENT OF A MOBILE AD-HOC NETWORK USING OPTIMIZED LINK STATE ROUTING PROTOCOL''. Under my supervision, and that this research has not been previously submitted for the reward of any degree in this or any other university.

_____ _____

Engr. Osa Edosa **Date**

Project Supervisor

_____ _____

Prof. PE Orukpe **Date**

Head Of Department

DEDICATION

This research is dedicated to my family and many friends. I have a deep sense of gratitude to my parents. The words of encouragement and tenacity of my mum Dr. H.O Ogefere and Dad Barr. L.O Ogefere echo in my ears.

This effort is also dedicated to my many friends and church families which has helped me along the way.

ACKNOWLEDGEMENT

I would like to take this opportunity to express my profound gratitude and deep regard to my project supervisor Engr. Osa Edosa, for his exemplary guidance, valuable feedback, and constant encouragement throughout the duration of the project. His valuable suggestions were of immense help throughout my project work. His perspective criticism kept me working to make this project in a much better way. Working under him was an extremely knowledgeable experience to me.

To all relatives, friends, and others who in one way or the other shared support either morally, financially and physically, I say a big thank you.

Above all, to the great Almighty, the author of knowledge and wisdom, for his immense love and guidance.

I say thank you.

TABLE OF CONTENTS

CHAPTER FOUR: RESULTS AND ANALYSIS

CHAPTER FIVE: CONCLUSION AND RECOMMENDATION

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.0 BACKGROUND TO THE STUDY

In the last two decades, the digital mobile communication services grew rapidly. In the 1990s, the digital services started as the second generation of mobile communications with the Global System for Mobile Communications (GSM) improved by the General Packet Radio Service (GPRS) and Enhanced Data Rates for GSM Evolution (EDGE). The third generation used the Universal Mobile Telecommunications System (UMTS) with the High Speed Packet Access (HSPA) improvement. Nowadays, the fourth generation of such services is in use which is called Long Term Evolution (LTE). To provide fast and easy access to the Internet in a lot of different places, the number of Wi-Fi hotspots is increasing rapidly. Wi-Fi stands for a trademark which specifies devices for the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard and is a subgroup of Wireless Local Area Network (WLAN). In this work both names are used interchangeably. All the previously mentioned communication standards, except Wi-Fi, are based on infrastructure networks only as shown in figure 1. This means that the base stations are usually static, but the users can be mobile. Furthermore, the users cannot communicate directly with each other, not even if they are in each other's communication range. Each user can only communicate with its base station which in turn forwards the information. If a node is not inside the transmission range of a base station it is not able to communicate, other devices between this node and the base station cannot act as relays. Therefore, the network coverage has to be considered when designing such networks.

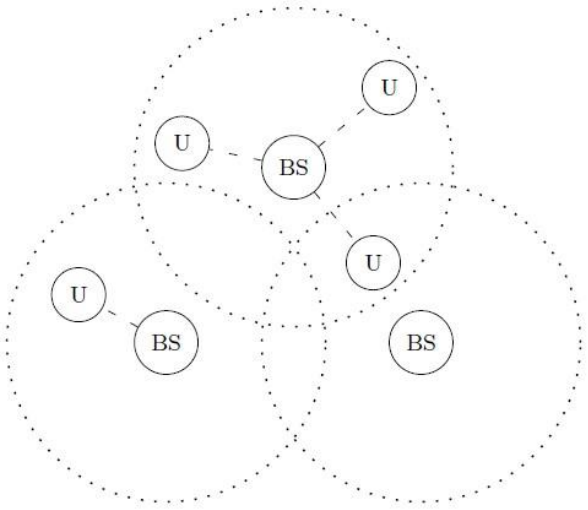

Figure 1: An Infrastructure Network with Three Base Stations (BS) and Four Users (U)

All infrastructure networks require previously installed hardware including radio towers, wired data connections and Backbone, for example. The weaknesses of

such infrastructure networks are the high acquisition costs for the installation which leads to the facts that these networks are uneconomic in sparsely populated areas, that it takes relatively long to assemble them and that these networks are administrated by a centralized instance which could represent a single point of failure. Since infrastructure networks usually are not available in isolated areas like in disaster scenarios or military operations or such infrastructure based networks are still too expensive, e.g., satellite connections, the Defense Advanced Research Projects Agency (DARPA) started the development of the Packet Radio Network (PRNET) in 1973 to connect about 50 wireless devices with each other without any given infrastructure (Kahn, 1975). This was the beginning of the ad hoc networks described in figure 2.

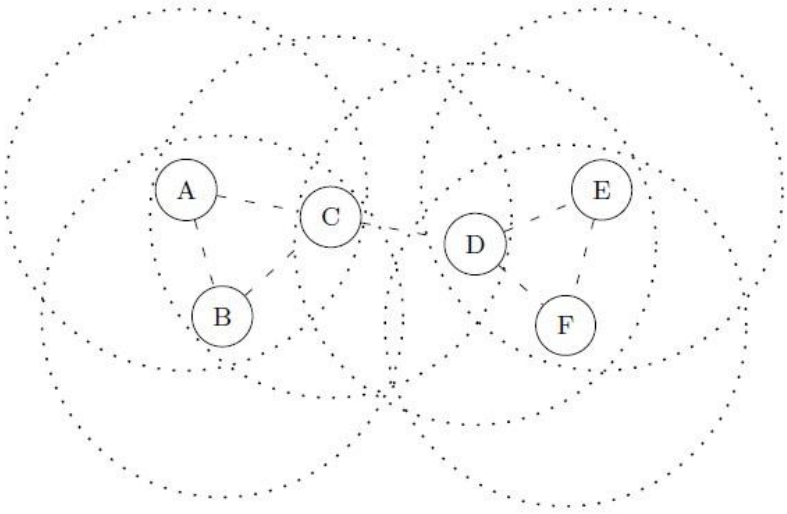

Figure 2: An Ad Hoc Network with Six Nodes and Visualized Transmission Ranges.

Ad hoc networks are usually constructed for a specific task without the need of any previously installed communication infrastructure. Instead, the nodes autonomously create a wireless network and each node communicates directly with its direct neighbor nodes without the need of base stations. The direct neighbors of a node are the devices which are in the direct radio range of the node. If the destination of a transmission is not a direct neighbor of the source node, it is not possible to communicate directly. However, the other nodes in an ad hoc network act as relays and can forward the packets. With this multi-hop feature, ad hoc networks are very scalable and robust against single node failures. These networks are highly adaptive: The participants can enter or leave the network, they can move around and the network can split into multiple parts and merge again. If the devices in such a network are mobile like walking pedestrians, driving cars or flying helicopters, the network is called MANET.

MANET stands for Mobile Ad hoc Network. It is a robust infrastructureless wireless network. A MANET can be formed either by mobile nodes or by both fixed and mobile

nodes. Nodes randomly associate with each other forming arbitrary topologies. They act as both routers and hosts. The ability of mobile routers to self-configure makes this technology suitable for provisioning communication to, for instance, disaster-hit areas where there is no communication infrastructure, conferences, or in emergency search and rescue operations where a network connection is urgently required. The need for mobility in wireless networks necessitated the formation of the MANET working group within The Internet Engineering Task Force (IETF) for developing consistent IP routing protocols for both static and dynamic topologies (Misra and Manda, 2005).

The dynamic nature of mobile ad hoc networks makes them ideal candidates for a number of applications. These networks are quick to deploy and require minimal configuration thus making them suitable for emergencies such as natural disasters. MANETs are also used to extend service coverage in cost effective ways. As technology advances in the development of devices such as Wi-Fi capable laptops, mobile phones and other portable devices, MANETs are increasingly becoming popular.

The versatility of MANETs makes them ideal candidates for a wide-range array of applications. Figure 3 shows an example of MANET application. They can be used during natural disasters where there is no communication infrastructure, as an extension of service coverage such as in airport hotspots and in normal enterprise deployment. A common use of MANETs is during
group communications in conferences. The key attributes that make MANETs ideal candidates for such applications are their quick self-configuration and low cost of deployment.

In case of a natural disaster, a radio link such as a WiMAX radio link may be established to one area and then a MANET access network established to provide coverage extension to the areas that would otherwise be impossible to cover. In this situation, the nodes further away from the base station will rely on intermediate nodes for communication. This provides an important communication network used in such situation. Figure 1 illustrates the deployment of a MANET over a WiMAX backbone.

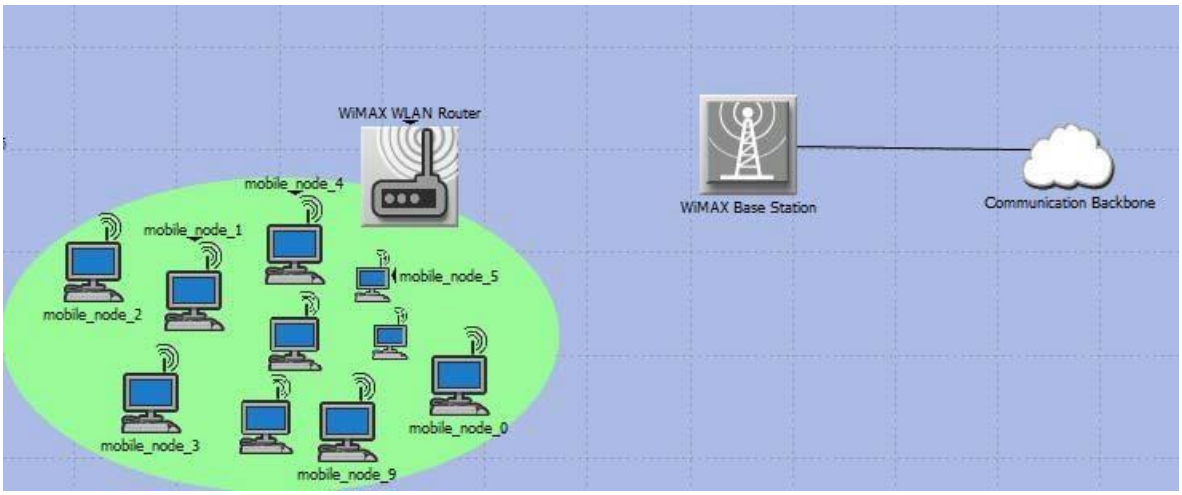

Figure 3. MANET deployment over WiMAX.

In Figure 3, the mobile nodes and the WiMAX WLAN Router form a MANET. The WiMAX WLAN router forms the boundary between the MANET and the WiMAX network. The router is capable of supporting translations between the ad hoc protocols and the appropriate protocols used on the WiMAX network and the communication backbone.

1.1. STATEMENT OF PROBLEM

In a MANET, mobile nodes have the ability to accept and route traffic from their neighbours towards the destination, i.e., they act as both routers and hosts. As the network grows, and coupled with node mobility, the challenges associated with self-configuration of the network become more pronounced. More frequent connection tearing and re-associations place an energy constraint on the mobile nodes. The main problem in mobile networking is the limited bandwidth and the high rate of topological changes and link failure caused by node movement (Jacqual et al,).

Ad hoc routing protocols are therefore needed to cope with the dynamic nature of MANETs. Examples of ad hoc routing protocols include AODV, OLSR, DSR, TORA, Wireless Routing Protocol (WRP) and the Zone Routing Protocol (ZRP).

1.2. AIM AND OBJECTIVES

1.2.1 Aim.

The aim of this work is to model and develop a mobile ad-hoc network using optimized link state routing protocol.

1.2.2. Objectives.

I. To design a Mobile Ad hoc Network (MANET) model.
II. To configure the designed network above using convenient parameters.
III. To configure routing in the designed MANET.
IV. To analyze the performance of the MANET.

1.3. METHODOLOGY

I. The MANET will be designed by appropriate node selection in Riverbed Modeler Simulation Environment
II. The MANET will be configured for communication using appropriate setup in Riverbed Modeler environment.
III. Routing will be Optimized Link enabled in the MANET via State Routing Protocol.

IV. The performance of the network model will be analysed using appropriate statistics and performance metrics in the Riverbed Modeler environment.

1.4. SCOPE OF STUDY

MANET routing protocols are generally classified in three categories namely Proactive, Reactive and Hybrid. Ad hoc routing protocols exhibiting both reactive and proactive protocols are called hybrid routing protocols. This study is focused only on a particular proactive protocol namely Optimized Link State Routing Protocol (OLSR). The effect of this protocol on MANET performance will be analyzed in this study.

CHAPTER TWO

LITERATURE REVIEW

2.0 AN OVERVIEW OF MOBILE AD HOC NETWORKS

An ad hoc network is a wireless network characterized by the absence of a centralized and fixed infrastructure. The absence of an infrastructure in ad hoc networks poses great challenges in the functionality of these networks. We refer to a wireless ad hoc network with mobile nodes as a Mobile Ad Hoc Network (MANET).

2.1 HISTORY OF MOBILE AD HOC ROUTING PROTOCOL

Ramanathan et al, (2002) described briefly the history of mobile ad hoc as a new technology and its origin can be traced back to the Defense Advanced Research Project Agency (DARPA) funded by the U.S government for military research. Under the research concept, packet radio networks (PRNET) were achieved in 1972 which were later developed into the survivable adaptive radio networks (SURAN). In "Computing Unplugged" Magazine, Humayun Bakht explained the whole life cycle of an ad-hoc network which can be classified into first, second, and third generation.

2.1.1 First Generation of Ad-hoc Networks

The first generation came to limelight back in 1972, the packet radio network was the first technology invented, as the technological development grew, it combined the area location of hazardous atmosphere (ALOHA) and the carrier sense medium access (CSMA) to form the basis of medium access control and distance-vector routing. It was used as a trial for isolated or military environment. The network made used of a technology called radio frequency to transmit and receive data.

2.1.2 Second Generation of Ad-hoc Networks

The second generation actually started in the 1980s with the SURAN (Survivable Adaptive Radio Networks) program as an improvement on the first generation. The technological improvements have made it portable, less expensive and more secure to electronic attacks. The aim of this program is to provide packet switched networking in an absent infrastructure mobile battle environment. The continuity for further research brought about the GloMo (Global Mobile Information System) project and NRDR *(*Near-Term Digital Radio*)* that provide easy access to service and user friendly Ethernet-type multimedia connectivity anywhere and anytime in handheld wireless mobile devices or gadgets.

2.1.3 Third Generation of Ad hoc Networks

Laptop computers, palmtop computer, personal digital assistance and other mobile communication equipment invention made the concept of commercial ad-hoc network to become a reality in the 1990s. Due to these innovations, the idea of a collection of most mobile gadget was proposed. The proposal led to its adoption by the IEEE 802.11 subcommittee which brought up the idea of deployment of ad-hoc networks and other applicable fields. IETF MANET working group was tasked with standardization of routing protocols in MANETs. RFC 2501 specifies the charter for the working group (http://www.ietf.org/rfc/rfc2501.txt)

2.2 CHARACTERISTICS OF AD HOC NETWORKS

MANETs have some major advantages over fixed networks in disaster scenarios. They can immediately be deployed in the absence of infrastructure networks, they are robust against external influences, they do not need any administration and they are a low-cost solution for communication. However, this type of networks has some characteristics (Corson and Macker, 1999) which have to be considered critically. The nodes in such networks are heterogeneous in terms of their available transmission power and their antenna design which could be omnidirectional, bidirectional, or have an adjustable angle. This results in different transmission ranges of the single nodes and therefore, in unidirectional and bidirectional links between the nodes. Furthermore, the devices in ad hoc networks have energy limitations because they tend to be battery powered. This limits the Central Processing Unit (CPU) power, hence the complexity of used algorithms inside a node. Moreover, each node frequently has to calculate routes and to forward packets which consumes a lot of energy. The exhaustible energy reserves should be born in mind when adjusting the transmission power of a node since it depends quadratically on the transmission range as described by Equation 1 (Jain and Shrivastava, 2011), where Pt is the transmitted power, Pr is the received power, d is the distance between the nodes and λ is the wavelength of the radio signal.

$$\frac{Pt}{Pr} = \frac{(4\pi d)2}{\lambda} \quad \text{---------- 1}$$

In MANETs, the nodes are typically mobile. Therefrom, the topology of a network can change rapidly and existing links between nodes break while new links occur. This behavior affects data transmissions and lowers the available throughput. Furthermore, it is the nature of wireless networks that their communication is disturbed by noise and affected by fading which implies interference, shadowing and multipath propagation. Another negative effect on the available throughput results from the media access when multiple devices compete for accessing the same radio channel. Another problem when sensing the own signal could be caused by received noise that disturbs the signal. Beside the problems with the media access, the distribution of Internet Protocol (IP) addresses is a big challenge in such networks. Furthermore, as multiple ad hoc networks can merge and

separate anytime, it must be guaranteed that each address in the network is only used once to avoid collisions. It would be also possible to detect such address collisions and resolve them afterwards. Beside the technological limitations of ad hoc networks, the human made security aspects have to be considered. Ad hoc networks, especially for disaster scenarios, are developed to be easily created and to allow nodes to attach to or detach from the network. This allows eavesdroppers to simply overhear transmissions and attackers to simply inject spoofed packets. With spoofed packets it would be possible to inject invalid routes into the routing tables, to redirect packets via Address Resolution Protocol (ARP) spoofing for a Man-in-the-middle attack or to use IP spoofing to fake the source address of IP packets. The last case could be a problem in disaster scenarios, if an attacker masquerades as firefighter or paramedic, for example, and sends messages like 'help is coming' to victims who will afterwards stop sending help requests. After the creation of an ad hoc network, the participating nodes can only communicate with their direct neighbor nodes, multihop transmissions are not possible.

As MANETs are characterized by node mobility and limited bandwidth, there is need to take into account the energy efficiency of the nodes, topology changes, unreliable communication and limited bandwidth in their design.

2.3. ROUTING IN MANETS

Since the typical transmission range of Wi-Fi devices in the free range can be expected as around 100 meters, it becomes clear that a direct connection between two nodes at the opposite sides of a network might not be possible. A solution is to use the intermediate nodes as relays, respectively routers, which will forward the data packets towards their destinations. Therefore, the nodes need to know the available routes between them. This very important task is done by routing protocols. Due to the fact that ad hoc networks have limited bandwidth and energy resources, special routing protocols have been developed to cope with these requirements. As shown in the previous chapter, ad hoc networks have some major advantages over traditional networks. They can be deployed rapidly anytime and anywhere without high acquisition costs, they are robust and self-organized. However, they also have some disadvantages which should be considered when working with this type of networks. Since most of the devices are battery-powered which implies that they only have very little energy resources, they cannot execute very complex algorithms. Furthermore, if a node's battery is completely depleted, the node fails and existing routes maintained by that node fail as well. Figure 4 shows this example where node A and node C communicate with each other over a route which contains node B with very little remaining energy. If node B fails, a new route over node D and E has to be available as soon as possible. Data transmissions in such a case could be interrupted if the routing is not able to instantly offer an alternate route. Such interruptions are fatal in the use of real-time applications like videoconferences or phone calls. A solution for this problem could be a routing algorithm maintaining multiple paths to a destination to be able to switch from the broken route to another one without any delay.

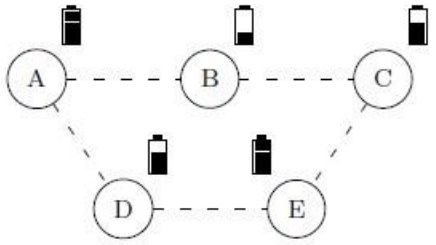

Figure 4: Re-Routing after a Node Failure.

2.4 MANET ROUTING PROTOCOLS

An ad hoc routing protocol is a standard for controlling node decisions when routing packets traverse a MANET between devices. A node in the network, or one trying to join, does not know about the topology of the network. It discovers the topology by announcing its presence and listening to broadcasts from other nodes (neighbor's) in the network. The process of route discovery is performed differently depending on the routing protocol implemented in a network. Over the years there has been significant research on routing protocol design for MANETs. The protocols proposed can be generally classified into topology-based and position-based routing protocols.

2.4.1 Topology-Based Routing Protocols

Topology-based routing protocols perform packet forwarding using the information of links in the network (Mauve et al., 2001). They can be classified either as proactive (or table-driven) or reactive (or on-demand) (Kiwior and Lam, 2007). There are some ad hoc routing protocols with a combination of both reactive and proactive characteristics. These are referred to as hybrid. Figure 5 shows the classification of ad-hoc wireless routing protocols based on topology.

2.4.1.1. Proactive Routing Protocols

The table-driven protocols, also called proactive routing protocols, discover and maintain routes frequently and before they are needed. To achieve this, the protocols constantly exchange some routing packets to refresh the information in the routing tables and to prevent inoperative routing table entries. In this process the routing has to make a tradeoff between the produced routing overhead and the freshness of the routes. More up-to-date routes result in more routing overhead, while reducing the routing overhead leads to routes which could be outdated. On account of the periodical updates which disseminate in the whole network, this type of protocol is less adequate for the use in highly mobile scenarios since it reacts relatively slowly to changes in the network structure. Two widely used protocols of this family are Destination Sequence Distance Vector (DSDV) (Perkins and Bhagwat, 1994) and the Optimized Link State Routing Protocol (OLSR) (Clausen and Jacquet, 2003) wireless routing protocol (WRP) and cluster head gateway switch routing (CGSR).

2.4.1.2. On-Demand Routing Protocols

On-demand protocols are also called reactive or source initiated routing protocols. This type does not discover routes until they are required, with the benefit of very low routing overhead during phases when the network is idle. When a node requires a route which does not exist in its routing table it sends a route request into the network. If the destination is present, the node receives a reply containing the information about the route. However, this request/reply sequence causes some latency. During this period a node has to wait for the reply and cannot forward its data packets directly. Furthermore, if the number of nodes in the network increases, the routing overhead could rise heavily, resulting in network clogging. Examples of well-known reactive protocols are Dynamic Source Routing (DSR) (Johnson et al., 2007; Johnson et al., 2001) and the Ad hoc On-Demand Distance Vector (AODV) routing (Perkins, Belding-Royer and Das, 2003), Admission control enabled on-demand routing (ACOR) and Associativity based routing (ABR).

2.4.1.3. Hybrid Protocols

Hybrid routing protocols combine the advantages of both reactive and proactive protocols with the potential to provide better scalability than pure reactive or proactive protocols. This is because of their attempt to minimize the number of rebroadcasting nodes by defining a structure allowing nodes to collaborate, which helps to maintain routing information much longer (Abolhasan et al., 2004). Zone Routing Protocol (ZRP) (Haas, 1998) is a prominent hybrid routing protocol which has a zone based structure and reduces overhead for intra-zone nodes. Others include (TORA), hazy sighted link state (HSLS) and order one routing protocol (OOPR).

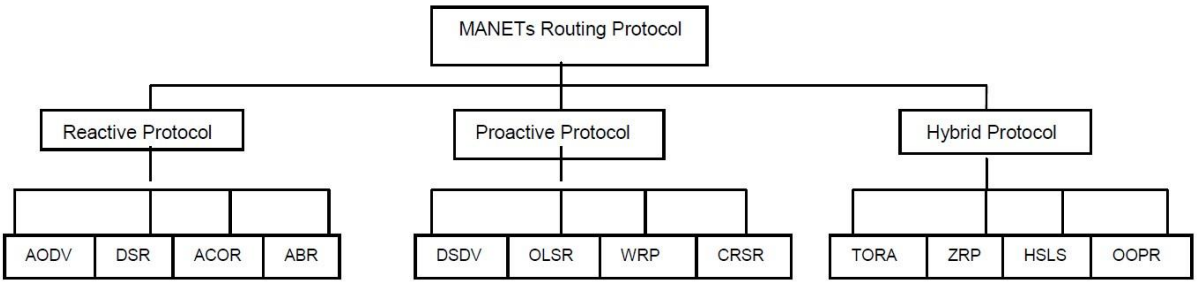

Figure 5. **Classification of ad-hoc wireless routing protocols topology based** (Qasim et al
2008)

2.4.2. Position-Based Routing Protocols

Position-based routing algorithms eliminate some of the limitations of topology-based routing by using additional location information (Mauve et al., 2001). In contrast to topology-based routing methods, they make decisions based on the geographical coordinates of the nodes (Cheng, 2014), which are determined using GPS or other positioning services.

2.5. THE OLSR PROTOCOL

An OLSR is a proactive or table driven, link-state routing protocol. As the name of the protocol goes, it uses link-state information for route discovery. This means that a node broadcasts information about the connections to its direct neighborhood into the whole network. Any other node in the network accumulates such gathered information and, afterwards, it calculates all possible routes in the network using the Dijkstra algorithm (Dijkstra, 1959).

This means that the node generates a graph containing all nodes and connections of the network. Then it starts at its own position in the graph and follows the shortest path to the nearest node. This node will be inserted into the routing table with the obtained path length. Subsequently, it searches the node with the second shortest path measured from its own position and inserts this node into the routing table. This algorithm is continued until all nodes of the graph have been reached and added to the node's routing table. Routing information is exchanged between the OLSR nodes using a standardized packet format (figure 6) which is usually transmitted inside User Datagram Protocol (UDP) packets addressed to destination port 698.

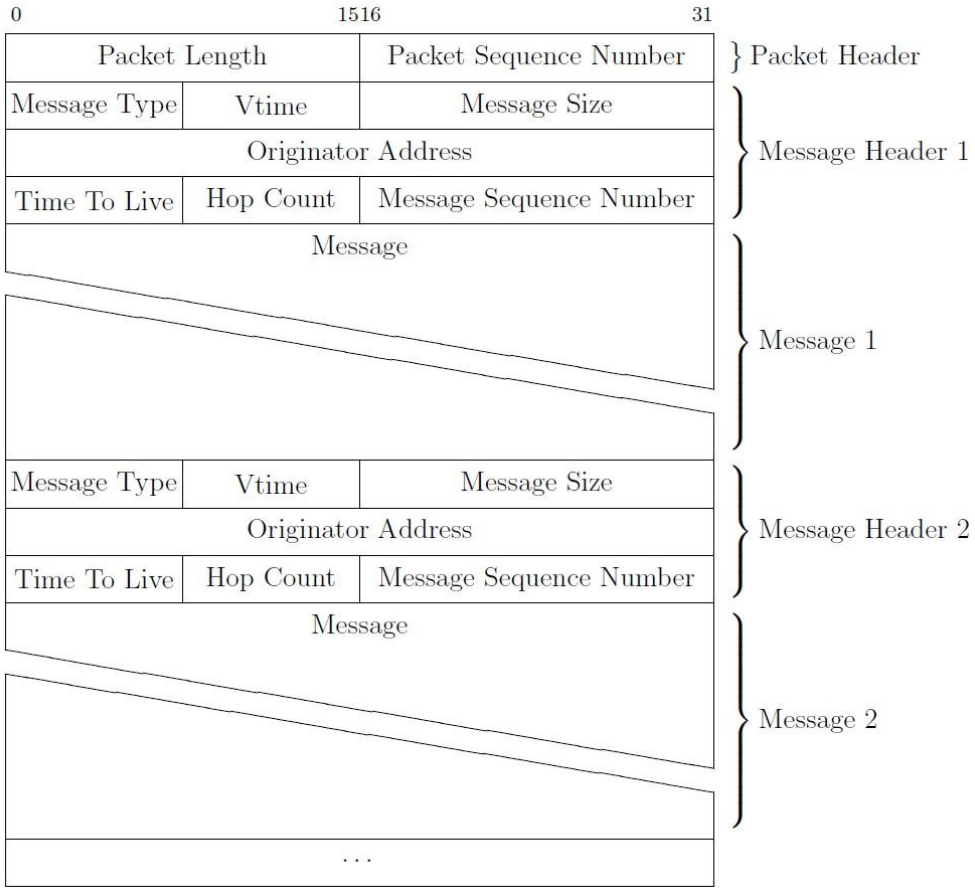

Figure 6: The Structure of an OLSR Packet

Link-state routing algorithms choose best route by determining various characteristics like link load, delay, bandwidth etc. Link-state routes are more reliable, stable and accurate in calculating best route and more complicated than hop count. To update topological information in each node, periodic message is broadcast over the network. Multipoint relays are used to facilitate efficient flooding of control message in the network. Route calculations are done by multipoint relays to form the route from a given node to any destination in the network. The OLSR protocol is developed to work independently from other protocols. Conceptually, OLSR contain three generic elements: a mechanism for neighbor sensing, a mechanism for efficient flooding of control traffic, and a specification of how to select and diffuse sufficient topological information in the network in order to prove optimal routes (Clausen, et al,).

2.5.1. Neighbor Sensing

In OLSR, neighbor nodes related information is gathered with “HELLO” messages which are send over network periodically (Clause et al., 2003). These “HELLO” message detects changes in neighbor nodes and related information such as interface address, type of link symmetric, asymmetric or lost and list of neighbors known to the node. Each node updates

and maintains an information set, describing the neighbor and two-hop neighbor periodically after some time.

2.5.2. Multi Point Relay (MPR)

The idea of multipoint relays is to minimize the overhead of flooding message in the network by reducing redundant retransmission in the same region. In MPR (Multi Point Relay) a node is selected by its one hop neighbor to "re-transmit" all the broadcast messages that it receives from other node, provided that the message is not a duplicate, and that the time to live field of the message is greater than one (Clause et al., 2003). In OLSR protocol, Multi Point Relays make use of "HELLO" message to find its one hop neighbor and its two hop neighbors through their response. Each node has a Multi Point Relay selection set, that indicates, which node acts as an MPR. Message is forwarded after the node gets new broadcast message and message sender's interface address in the MPR Selector Set. MPR Selector Set is updated continuously using

"HELLO" message which are periodic because neighbor nodes are of dynamic nature in MANET.

2.5.3. Topology Control Information

Topology Control (TC) messages are diffused with the purpose of providing each node in the network with sufficient link-state information to allow route calculation (Clause .et al., 2003). TC messages are broadcast periodically by a node. Like "HELLO" messages, with these TC messages the topological information is diffused over the entire network. A minimum criterion for the node is to send at least the link of its MPR Selector Set (Jacquet et al., 2001; Clausen, et al).

2.6. RIVERBED (OPNET) MODELER

OPNET Modeler is a commercial research oriented network simulation environment tool for network modeling and simulation. It allows the users to design and study communication networks with proper flexibility and scalability. It simulates the network graphically and gives the graphical structure of actual networks and network components. The users can design the network model visually (Hetal Jasani, "Quality of Service Evaluations of On Demand Mobile Ad-Hoc Routing Protocols" 5th ICNGMAS, IEEE2011).

In this paper, the network simulations are implemented using OPNET modeler (version 17.5).

2.7. RELATED WORKS

Qasim et al (2008) worked on comparison within mobile ad hoc networks' routing protocols from reactive, proactive and hybrid categories. They comprehensively analyzed the results of simulation for mobile ad hoc routing protocols over the performance metrics of packet delivery ratio, end to end delay, media access delay and throughput for optimized link state routing, temporary ordered routing algorithm and ad hoc on demand distance vector protocol. Ying Ge (2002) developed QoS versions of the OLSR (Optimized Link State Routing) protocol. The author introduced heuristics that allow OLSR to find the maximum bandwidth path and proved that these heuristics do improve OLSR in the bandwidth QoS. It was a simulation based work using OPNET. The performance analysis of MANETs routing protocols such as Ad hoc on Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporary Ordered Routing Algorithm (TORA), and Optimized Link State Routing (OLSR) using Voice over Internet Protocol (VoIP) traffic was carried out by Mbougni et al (2013). The performance metrics used for the analysis of these routing protocols are delay and throughput. The overall results show that the proactive routing protocol (OLSR) performs better in terms of delay and throughput than the reactive protocols. The work by Mboughni et al involves just two performance metrics whereas this project work is to involve the analysis of OLSR in MANET using multiple performance metrics which in the author's view will present a more pronounced argument as to the performance of OLSR in MANETs and its subsequent adoption as a routing protocol of choice.

CHAPTER THREE

METHODOLOGY

3.0 INTRODUCTION

This chapter presents the design parameters of our system and the various metrics considered in the performance evaluation of the routing protocol. The materials and methods employed are entirely software. The software used in this study is Riverbed (OPNET) modeler 17.5. OPNET is a network and application management software designed and distributed by OPNET Technologies Inc. (http://www.opnet.com). MANET toolbox has been used in this work to simulate the network. Components used for designing of the network are MANET_Station (mobile), Application configuration which decides the type of application running in the network, Profile configuration for configuring the type of profile on the network and Server Configuration. The development language is C. It provides a variety of toolboxes to design, simulate and analyze a network topology, routing protocols on the basis of various network parameters. The entire process was broken down into four major steps. The first step was modelling (creating network nodes) followed by Choing statistics, then running simulations and finally view and analysis of results.

3.1. CREATING THE MODEL

The first step when creating a network in Riverbed Modeler is to create a blank scenario. This is done using the start-up wizard. This opens a project editor workspace in which network design is performed. The design is done either automatically or manually. It is done either by automatically generating topologies using rapid configuration or manually by dragging objects from the object palette to the project editor workspace. Pre-defined scenarios can also be imported if they suit user requirements. However, wireless networks cannot be designed by importing scenarios. After the network is designed, nodes must be configured. Configuration is also performed either manually or by using pre-defined parameters in the workflow.

Figure 7. presents the design of the network. Fifteen wireless nodes are deployed in the simulation environment consisting of eight iPhone, six android devices and one svr_wrless_manet chassis. Application Configuration, Profile Configuration and Server_Config models are also deployed into the environment. Each of the nodes acts a router and hence can communicate with any other node in the network using the routing protocol configured. Figures 8 to 13 show the simulation parameters of the various components of the model including OLSR configurations.

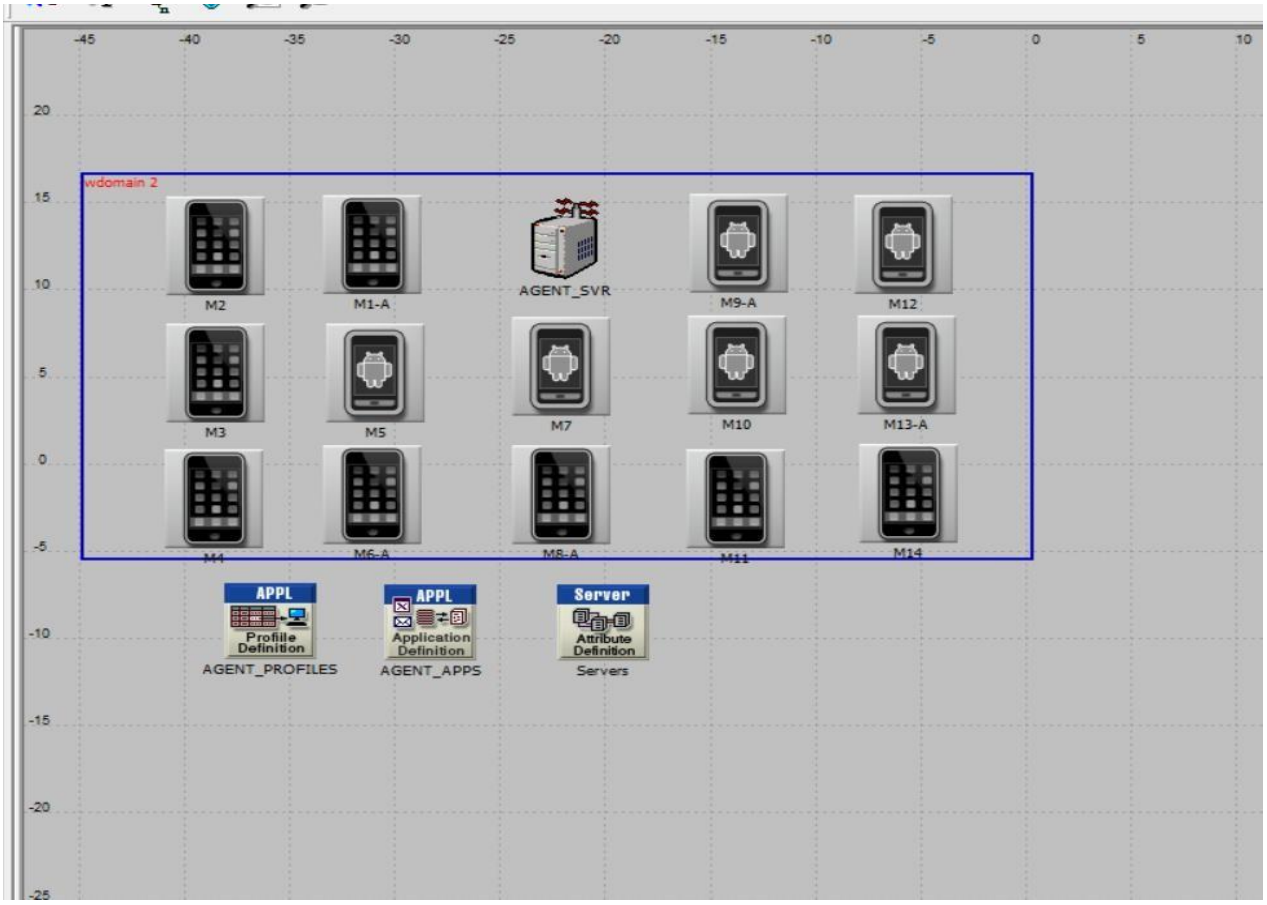

Figure 7. Mobile Ad-Hoc Network Model.

(M2) Attributes

Type: server

Attribute	Value
trajectory speed override	disabled
ground speed	
ascent rate	
threshold	0.0
icon name	iphone
creation source	Object copy
creation timestamp	11:55:22 Jul 15 2014
creation data	Copy of M1
pitch	0.0
yaw	0.0
roll	0.0
label color	black
AD-HOC Routing Parameters	
AD-HOC Routing Protocol	OLSR
AODV Parameters	Default
DSR Parameters	Default
GRP Parameters	Default
OLSR Parameters	Default
TORA/IMEP Parameters	Default
IP	
IP Multicasting	
Applications	
Application: Destination Preferences	(...)
Application: Supported Profiles	(...)
Number of Rows	1
Mobileapps	...
Application: Supported Services	All
Application: Transaction Model Tier C...	Unspecified
CPU	
VPN	
DHCP	
TCP	
NHRP	

Figure 8. Simulation Parameters for iPhone.

Type: server

Attribute	Value
y position	5.46975222395
trajectory	NONE
color	white
bearing	0.0
trajectory speed override	disabled
ground speed	
ascent rate	
threshold	0.0
icon name	android
creation source	Object copy
creation timestamp	11:56:01 Jul 15 2014
creation data	Copy of M6
pitch	0.0
yaw	0.0
roll	0.0
label color	black
AD-HOC Routing Parameters	
IP	
IP Multicasting	
Applications	
Application: Destination Preferences	(...)
Application: Supported Profiles	(...)
Number of Rows	1
Mobileapps	
Profile Name	Mobileapps
Traffic Type	All Discrete
Application Delay Tracking	Disabled
Application: Supported Services	All
Application: Transaction Model Tier C...	Unspecified

Figure 9. Simulation Parameters for Android devices.

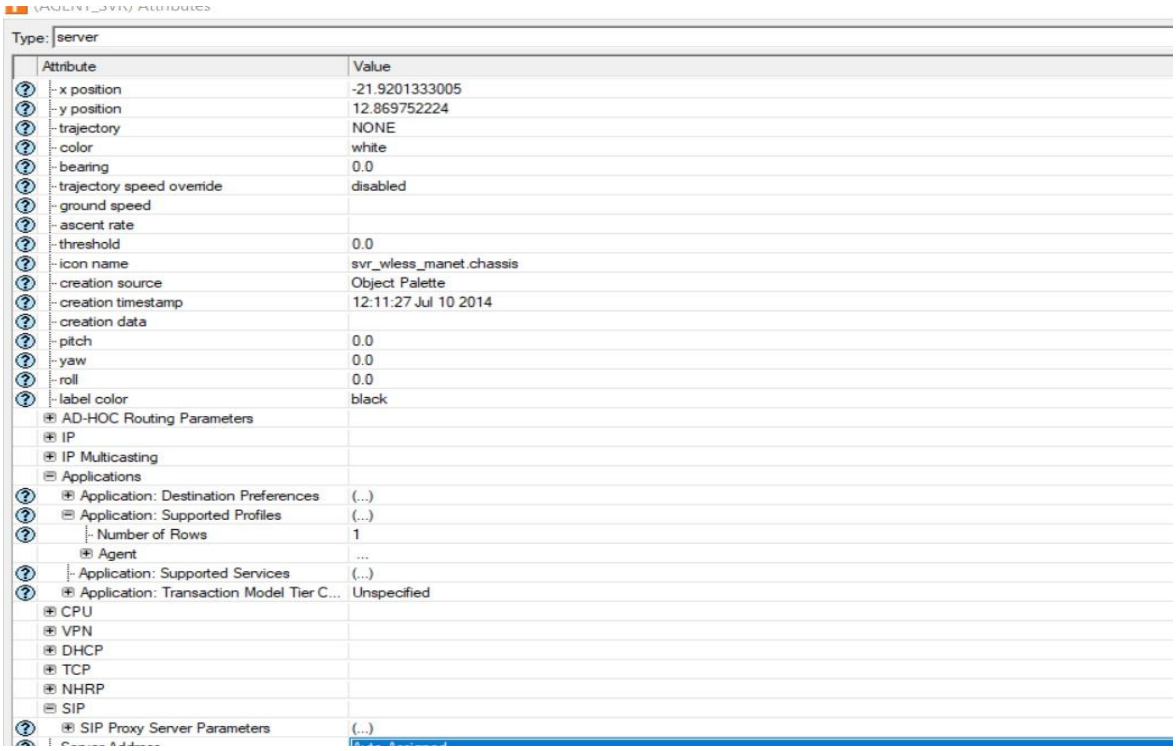

Figure 10. Simulation Parameters **svr_wrless_manet chassis**.

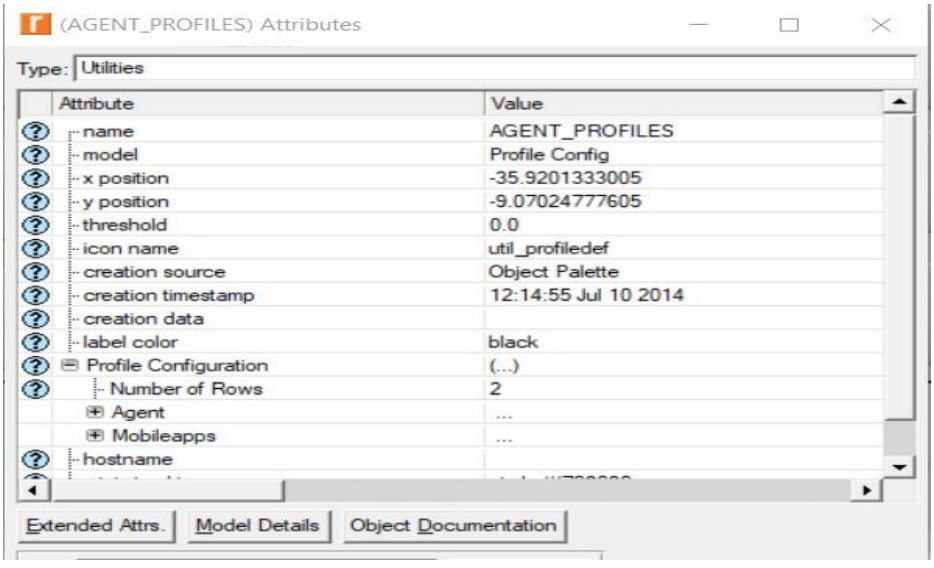

Figure 11. Simulation Parameters for Profile Configuration

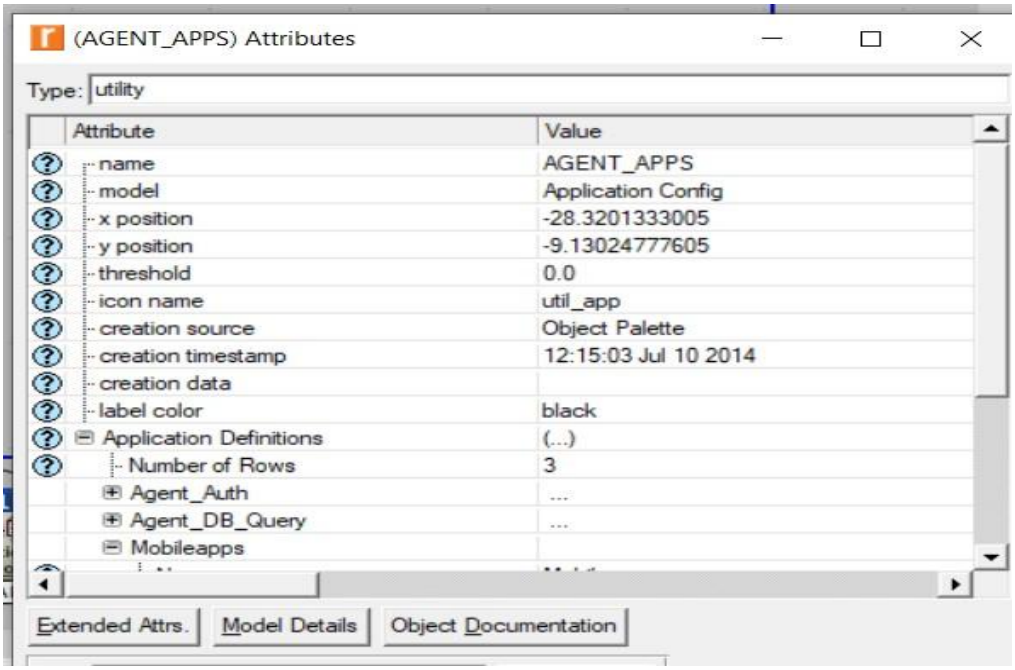

Figure 12. Simulation Parameters for Application Configuration.

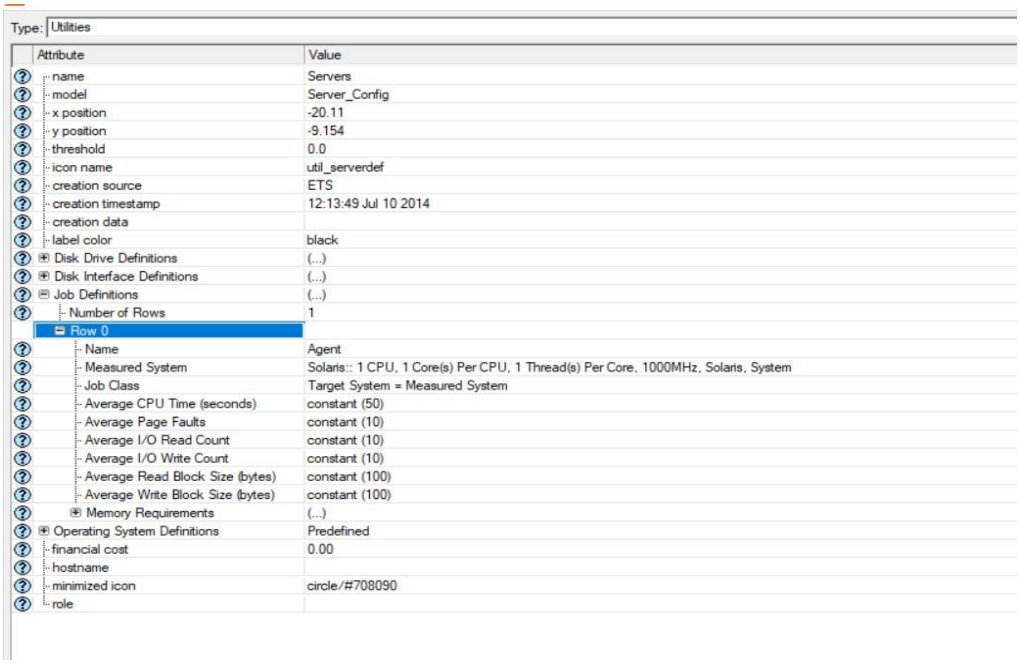

Figure 13. Simulation Parameters for Server Configuration.

3.2. COLLECTING STATISTICS

There are two types of statistics that can be collected in Riverbed Modeler, Global statistics and Object statistics**.** Global statistics are collected from the entire network while object statistics are collected from individual nodes. When desired statistics are chosen, the simulation is run to record the statistics. After running the simulation, the collected results are viewed and analysed. This is done by either right clicking in the project editor workspace and choosing 'View Results' or by clicking on 'DES', 'Results' then 'View Results'. A results browser then pops up as shown in Figure 14.

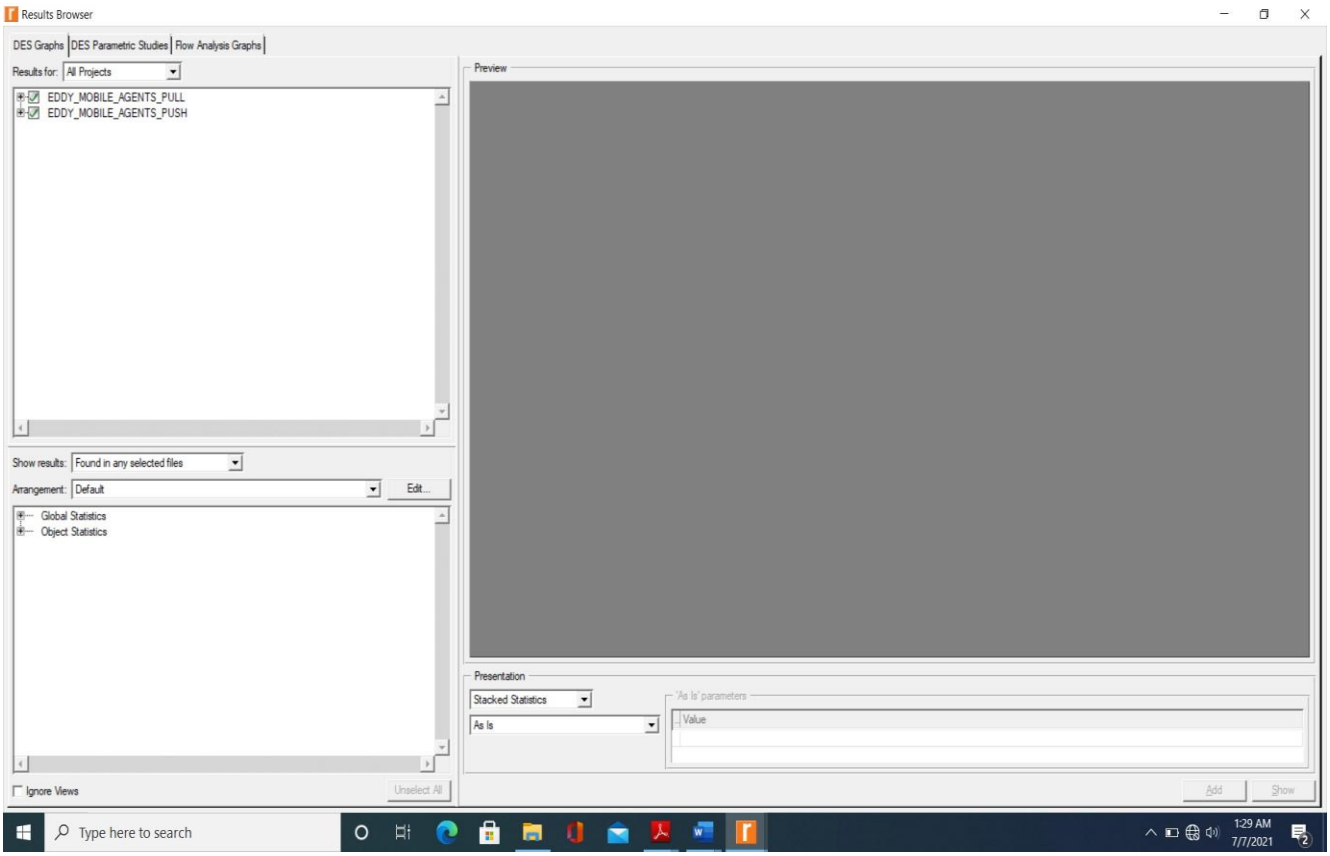

Figure 14. Riverbed Modeler Results Browser.

The Global statistics of Database Query, Email, OLSR, Remote Login and Wireless LAN attributes were configured for result and the Object statistics of Server Email, Server Remote login and CPU were configured for result.

3.3 SIMULATION SETUP

Riverbed Modeler 17.5 was employed in the various simulations. A single scenario was considered in this simulation which was set to run for forty five minutes at 100 values per statistic. The Profile configured for our nodes was Mobileapps. The applications configured include Database (High load), Remote login (High load) and Email (High load) respectively.

CHAPTER FOUR

RESULTS AND ANALYSIS

The performance of the OLSR based MANET was measured in terms of various metrics described below and graphs shown in Figures 15 to 40 describe the various result outputs in terms of the performance metrics. Discussion of results after each collection of statistics follow thereafter.

4.1 PERFORMANCE METRICS

4.1.1 Traffic Received

The amount of data moving across the network to the destination measured in bytes/sec or packets/sec.

4.1.2 Traffic Sent

The amount of data moving across the network from the source measured in bytes/sec or packets/sec.

4.1.3 Response Time

This is the total amount of time it takes to respond to a request for service measured in seconds.

4.1.4 Download Response Time.

This is the time that passes between a client node sending a request in a packet and receiving its reply.

4.1.5 Upload Response Time.

The time that elapses when data is being uploaded into the server.

4.1.6 Hello Traffic Sent.

Hello traffic represents the flow of packets that are sent out periodically from a router to establish and confirm network adjacency relationships.

4.1.7 Total Hello Messages Sent.

The total number of hello packets sent.

4.1.8 Routing Traffic Sent.

This represents the amount of data moving across the network from the sending node at a given point in time.

4.1.9 Delay

It specifies the latency for a bit of data to travel across the network from one communication endpoint to another. It is the average time taken by the packet in order to traverse the network.

4.1.10 Load

This is a measure of the amount of computational work that a computer system performs.

4.1.11 Throughput

This is an actual measure of how much data is successfully transferred from source to destination. It is the total amount of the data received by the receiver from the sender until the end of last packet transmission.

4.2. GLOBAL STATISTICS

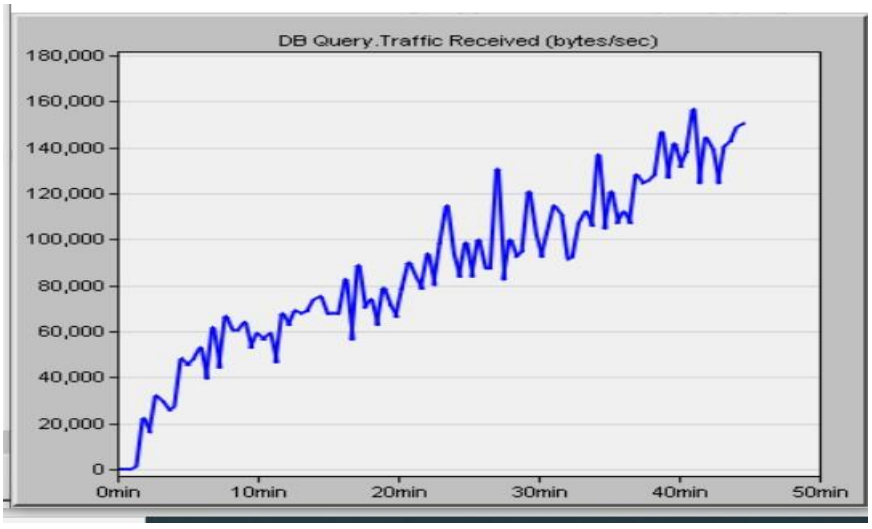

Figure 15. Database Query Traffic Received.

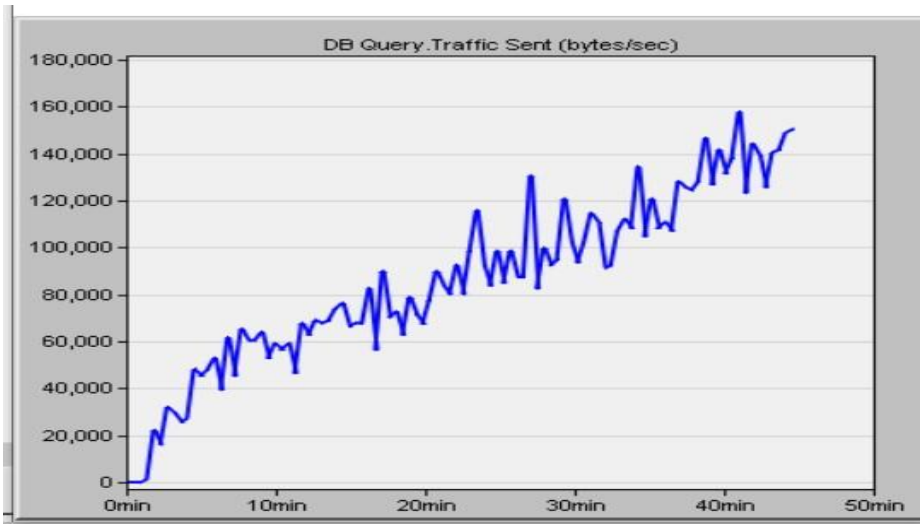

Figure 16. Database Query Traffic Sent.

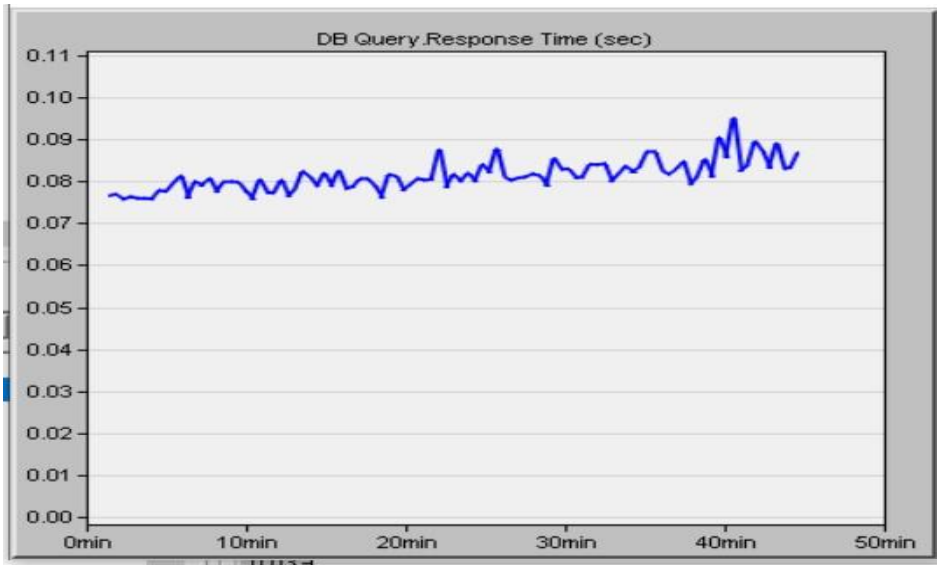

Figure 17. Database Response Time.

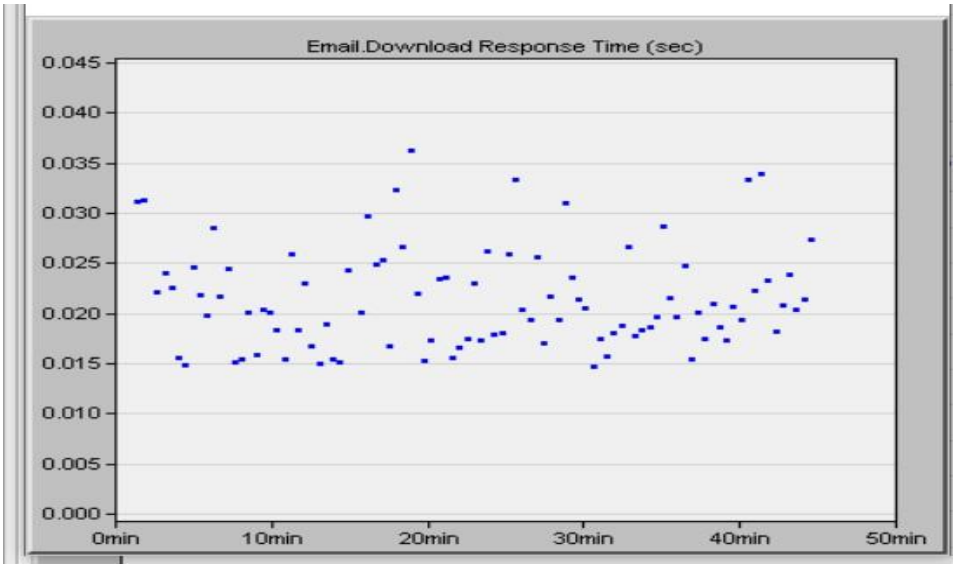

Figure 18. Email Download Response Time.

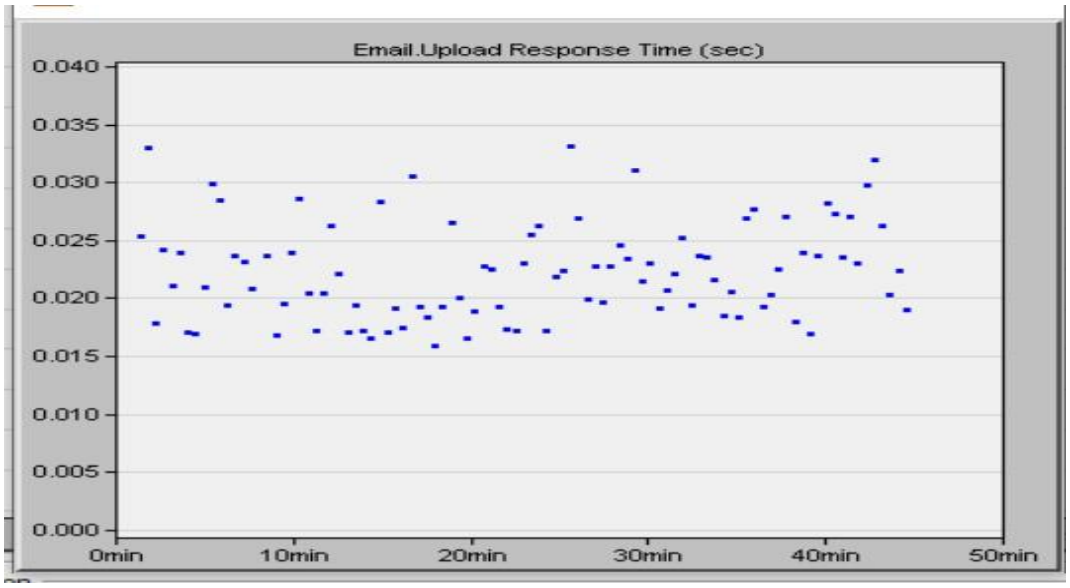

Figure 19. Email Upload Response Time.

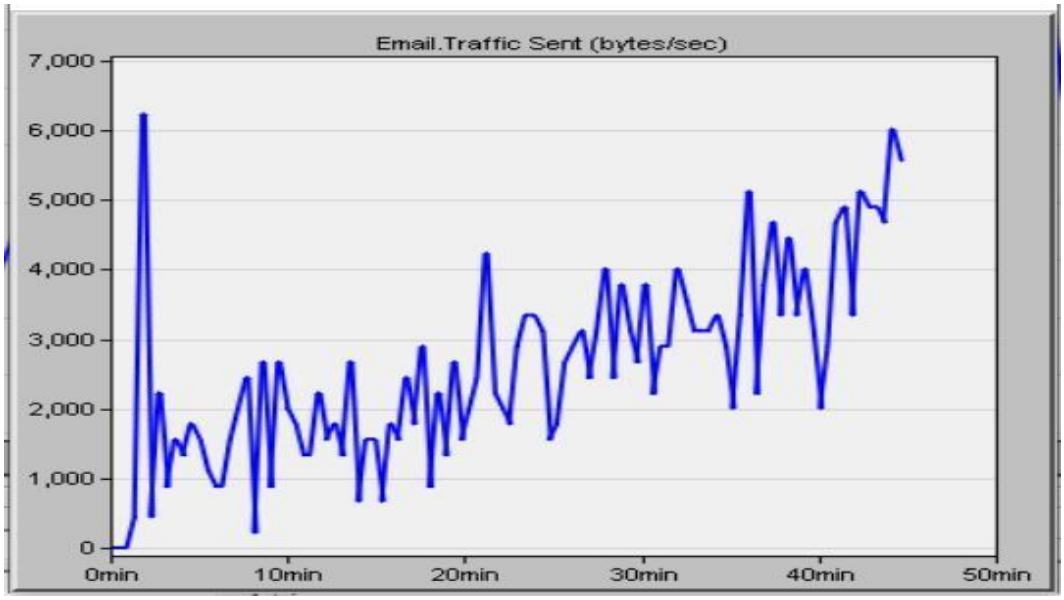

Figure 20. Email Traffic Sent.

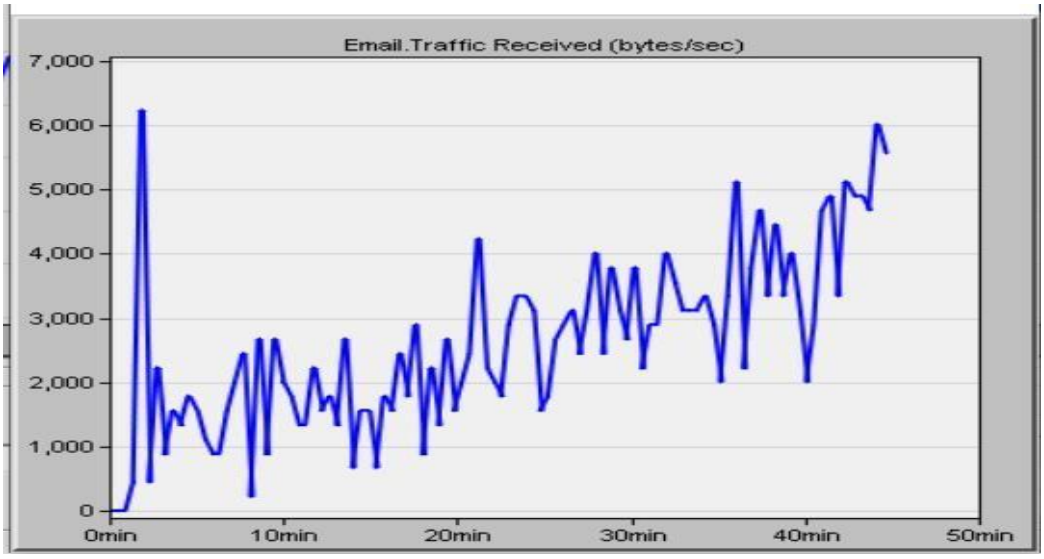

Figure 21. Email Traffic Received.

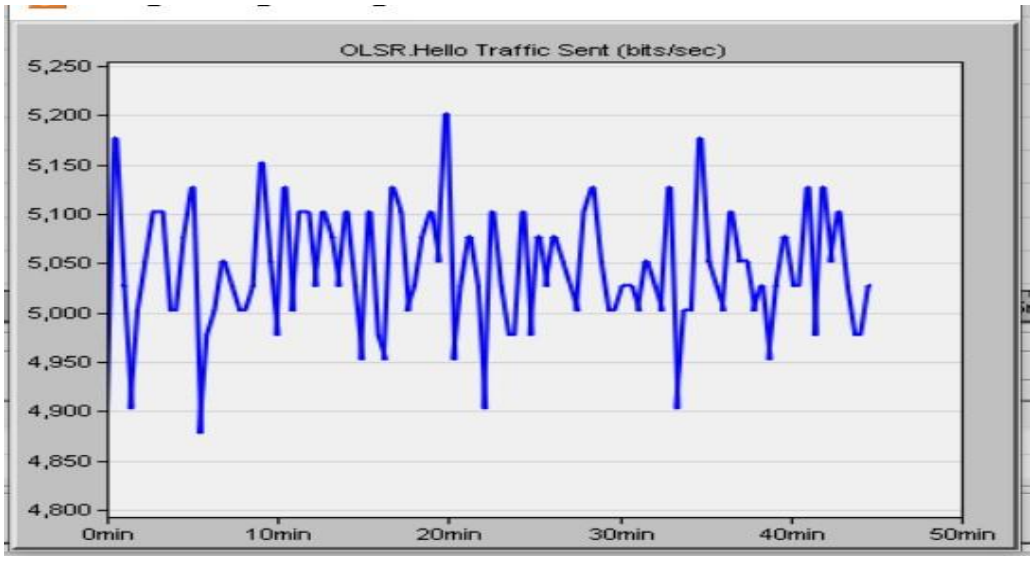

Figure 22. OLSR Hello Traffic Sent.

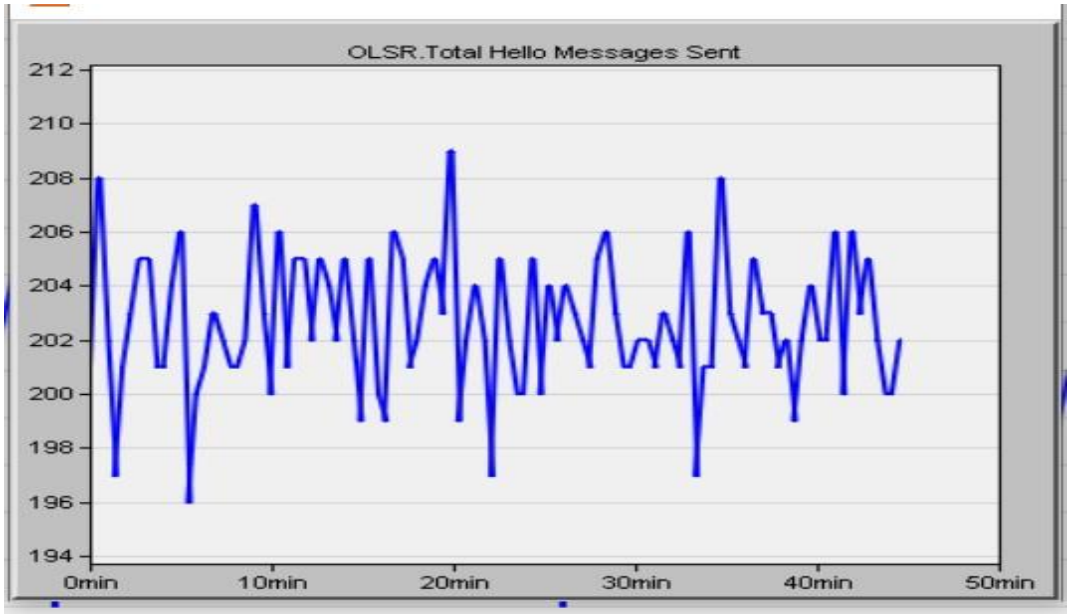

Figure 23. OLSR Total Hello Messages Sent.

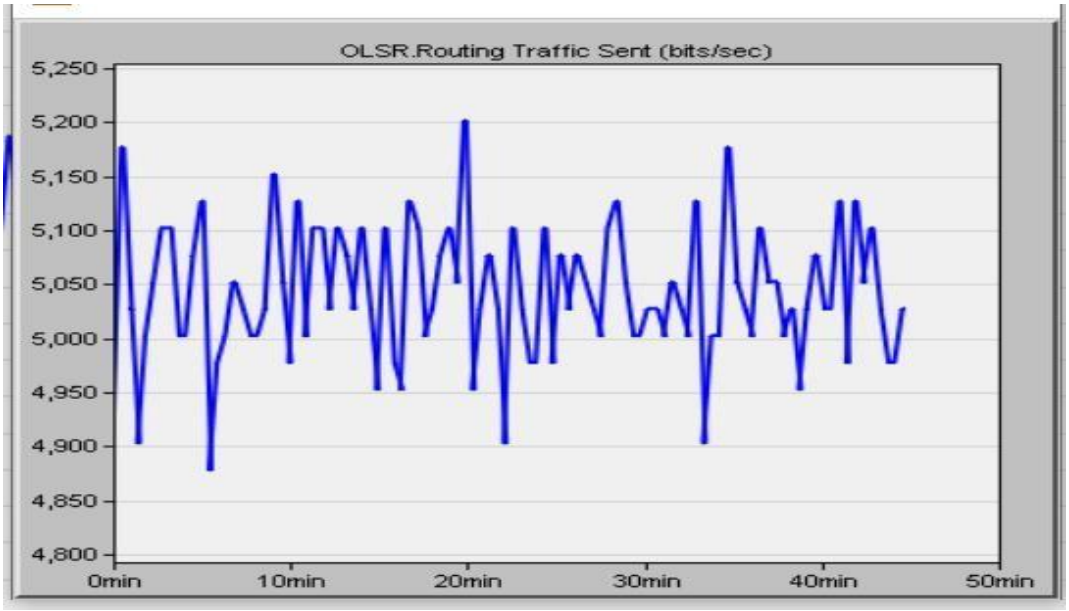

Figure 24. OLSR Routing Traffic Sent.

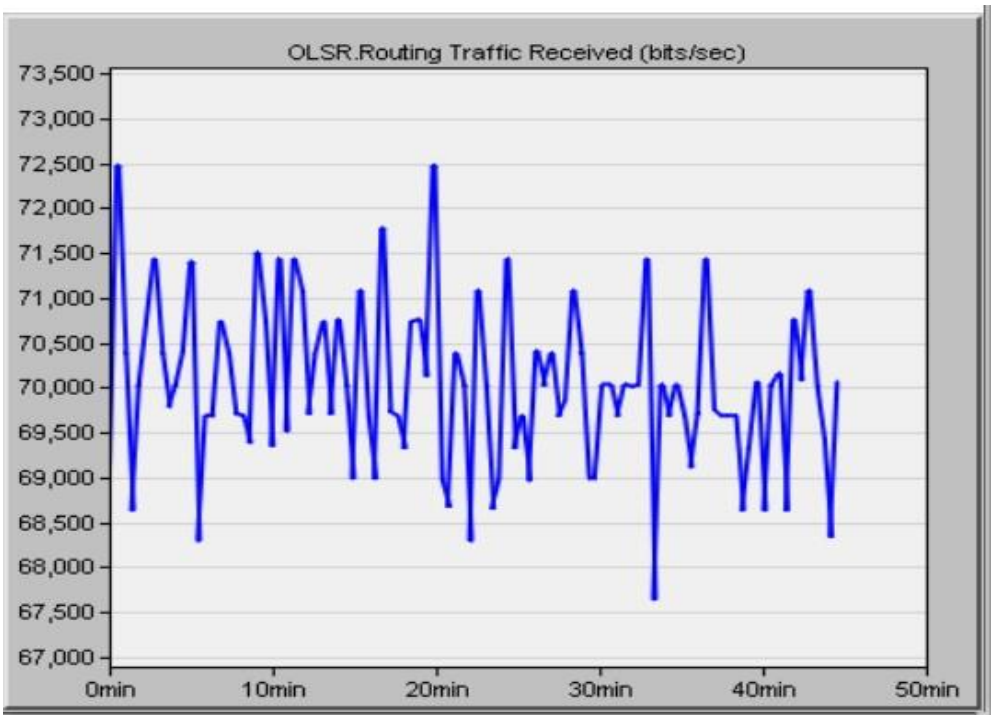

Figure 25. OLSR Routing Traffic Received.

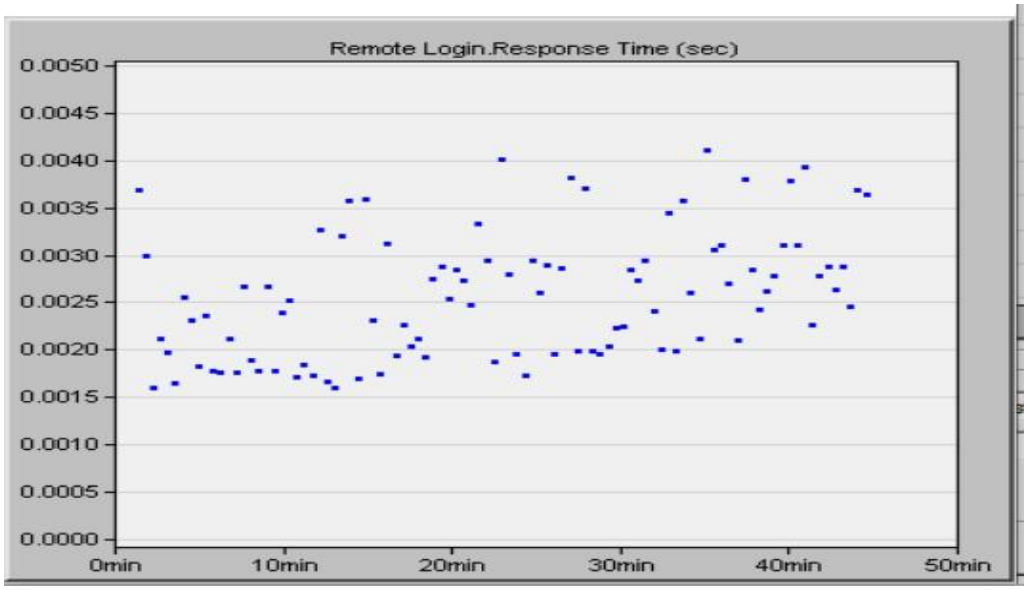

Figure 26. Remote Login Response Time.

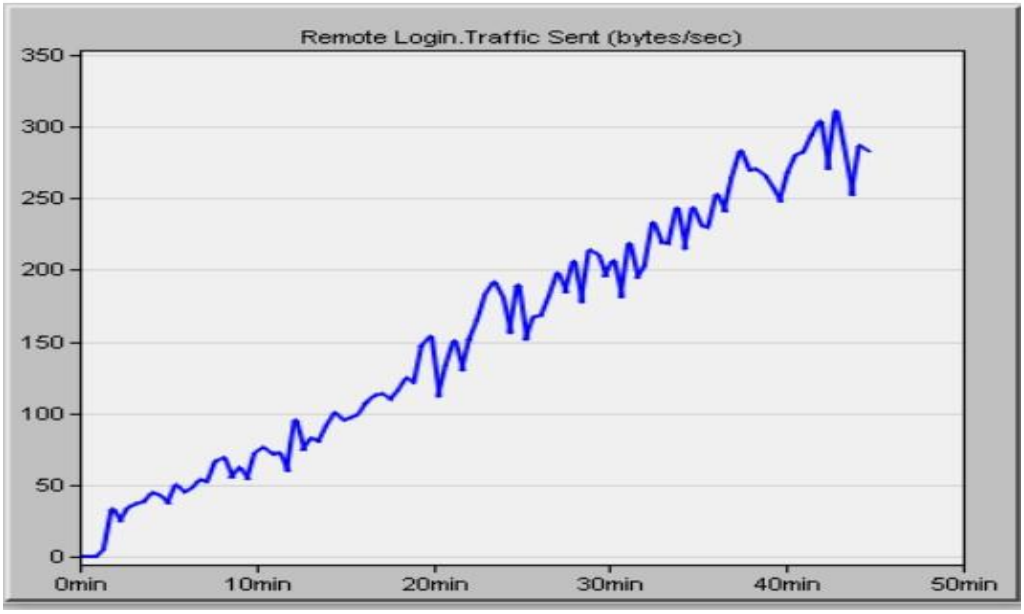

Figure 27. Remote Login Traffic Sent.

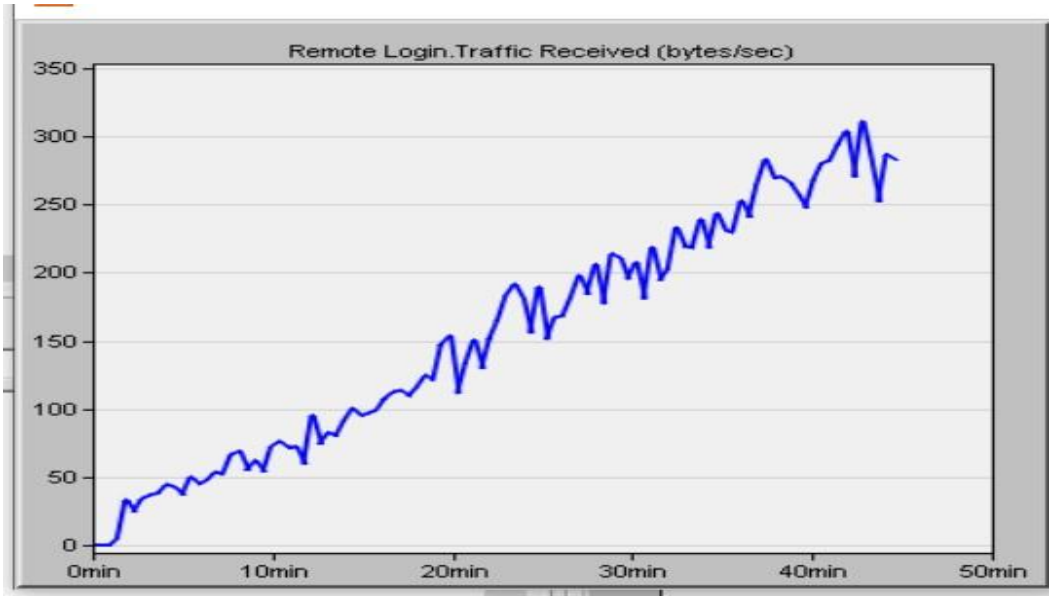

Figure 28. Remote Login Traffic Received.

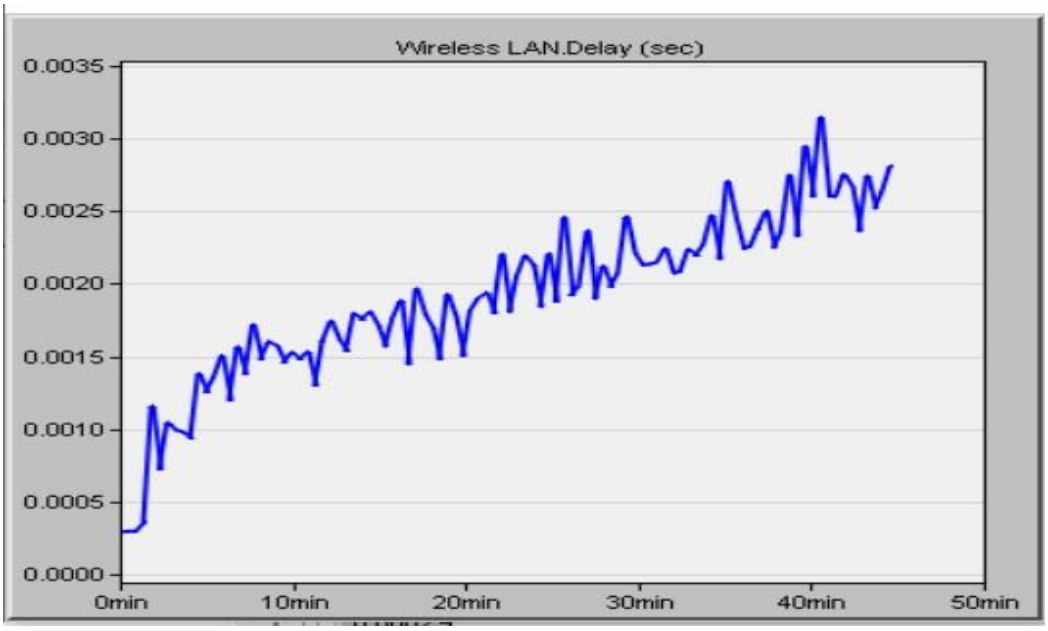

Figure 29. Wireless LAN Delay.

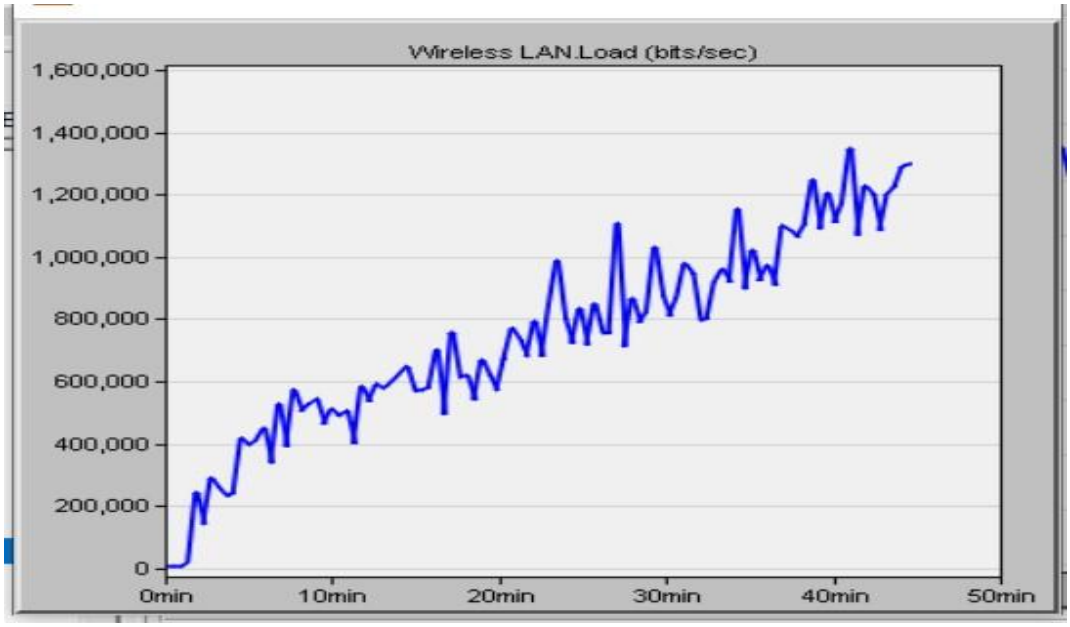

Figure 30. Wireless LAN Load

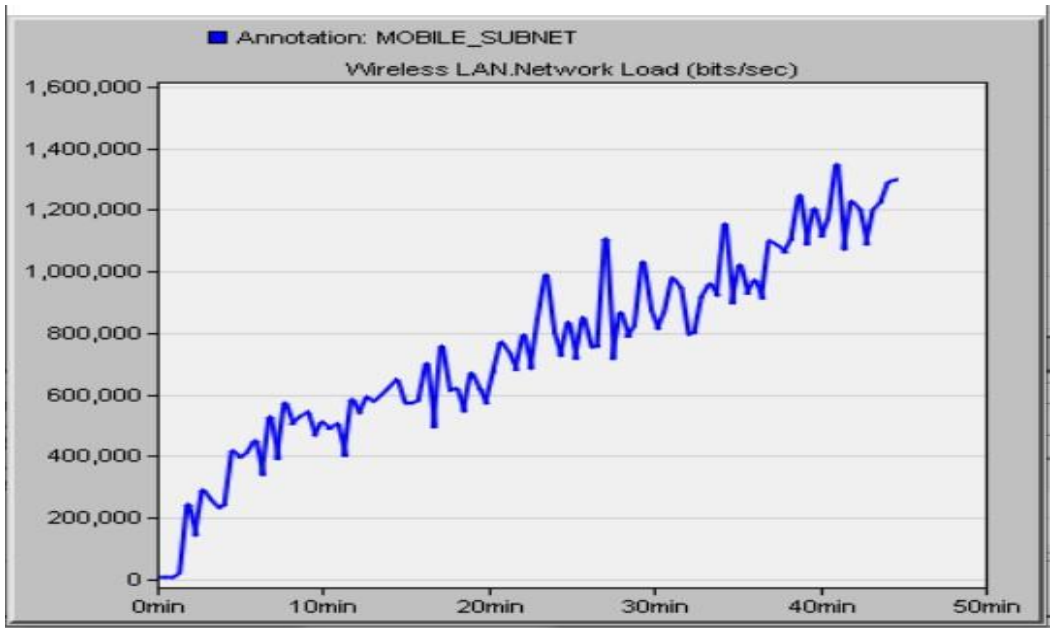

Figure 31. Wireless LAN Network Load.

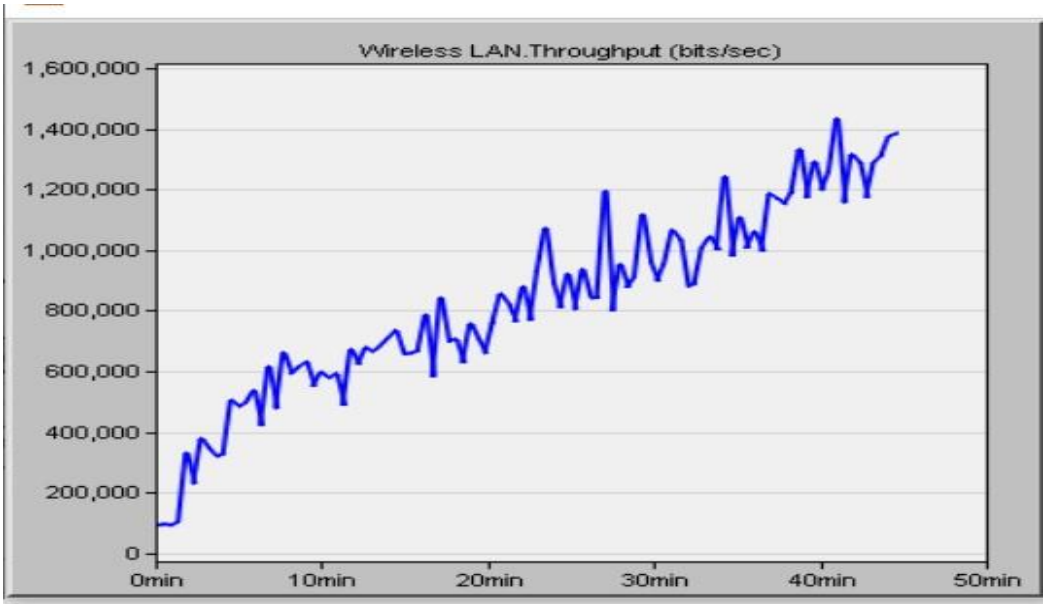

Figure 32. Wireless LAN Throughput.

The results displayed above for global statistics are interpreted as follows: Database Query Traffic sent and received are 160000 and 160000 bytes per second respectively. The Database Response time is peaked at 0.95 seconds. The Email maximum and minimum download response time are 0.036 and 0.015 seconds respectively. The Email maximum and minimum upload response time are 0.033 and 0.016 respectively. Email Traffic sent is peaked at 6300 bytes per second while Email Traffic received is 6300 bytes per second.

OLSR Hello Traffic Sent is 5200 bits per second while total OLSR Hello Messages Sent are 209. OLSR traffic sent are ranged from 4875 to 5200 bits per second. OLSR traffic received are ranged from 67600 to 72500 bits per second. Remote Login Response Time ranged from 0.0015 to 0.0042 seconds. Remote Login Traffic is peaked at 310 bytes per second. Wireless LAN Delay is 0.0032 seconds. Wireless LAN load is peaked at about 1300500 bits per second. Wireless LAN Throughput is peaked at 1400000 bits per second.

4.3. OBJECT STATISTICS

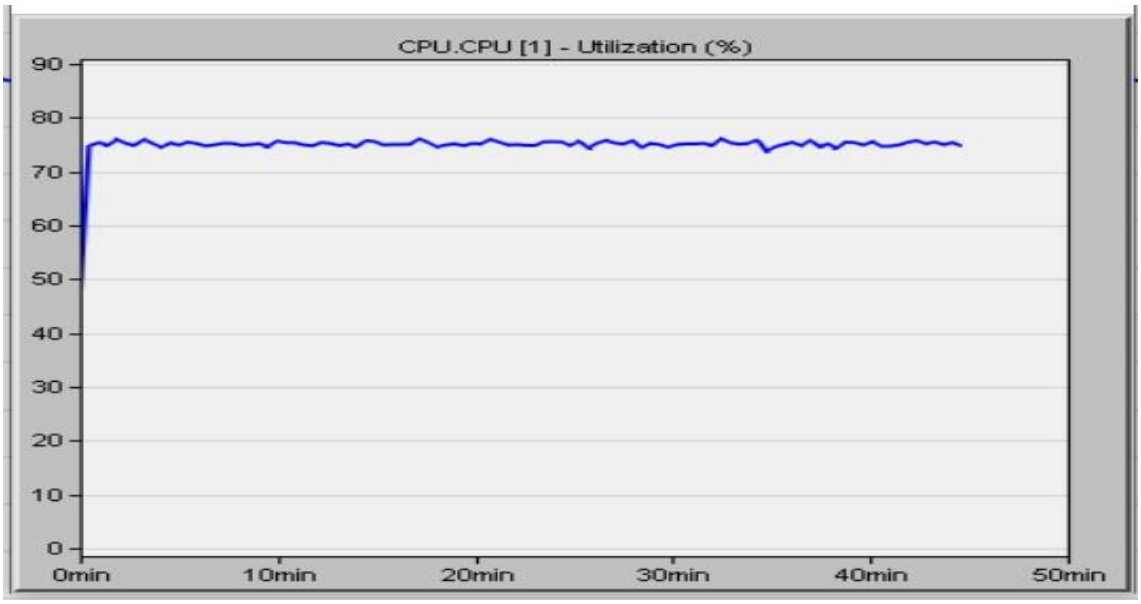

Figure 33. CPU Utilization for iPhone Node.

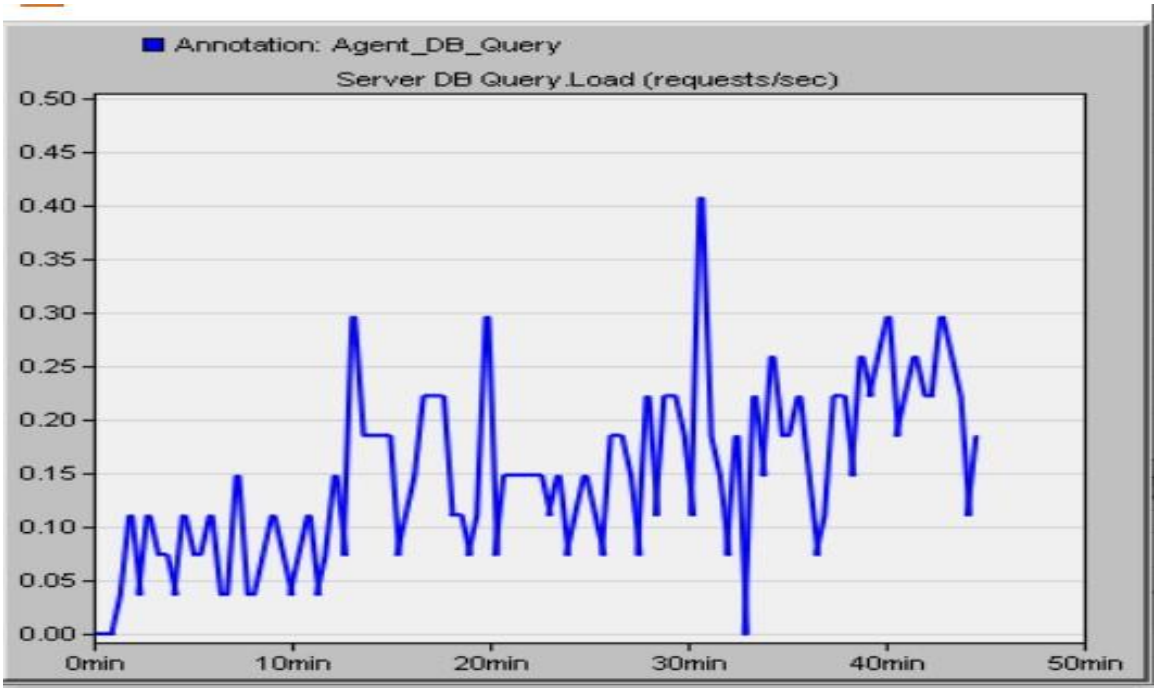

Figure 34. Database Server Query Load for iPhone Node.

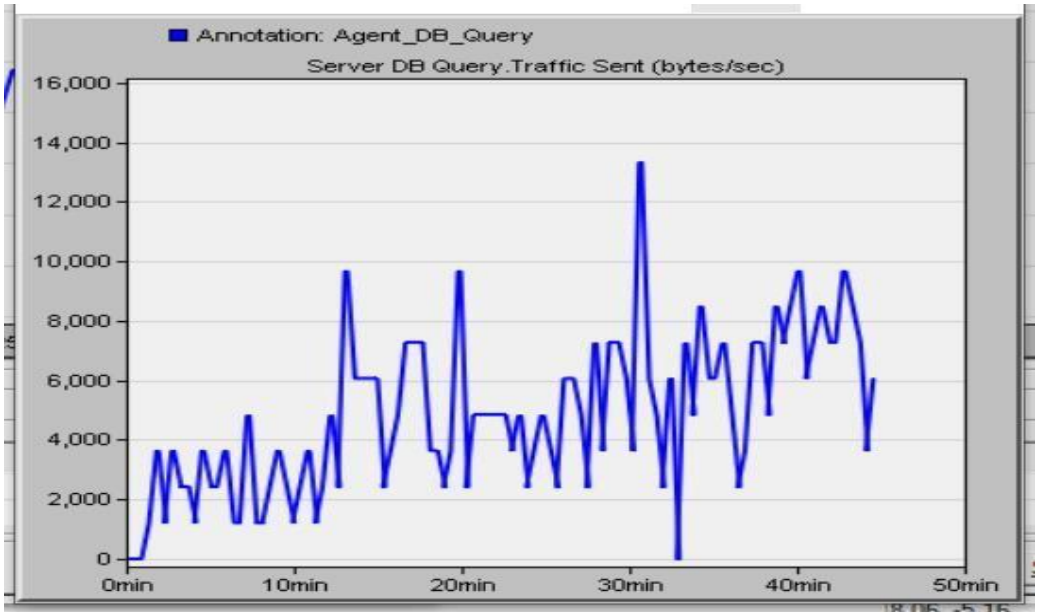

Figure 35. Database Traffic Sent for iPhone Node.

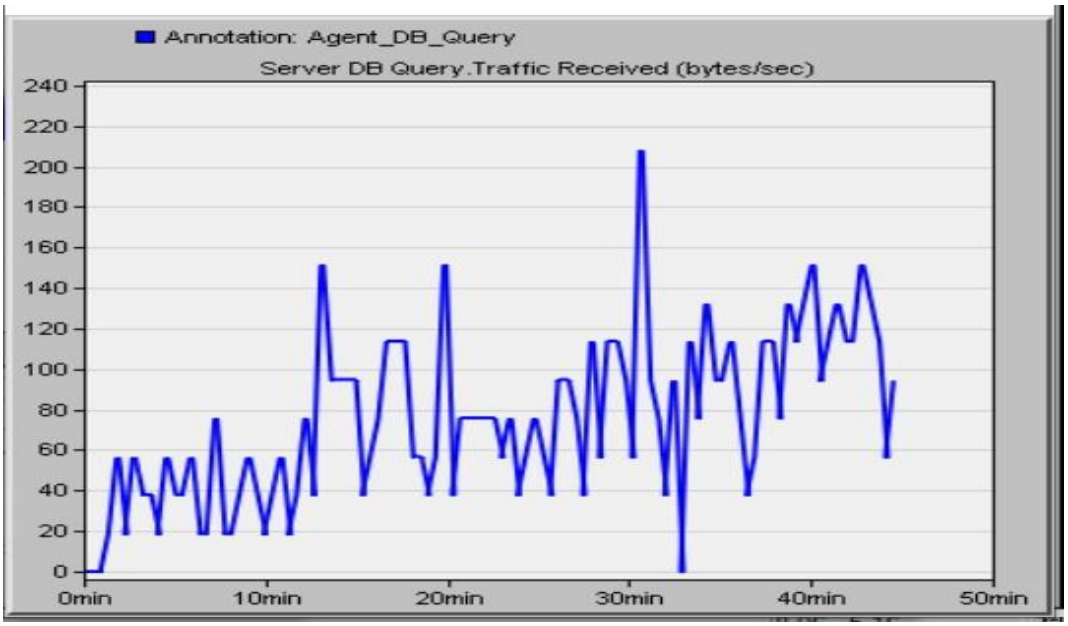

Figure 36. Database Traffic Received for iPhone Node.

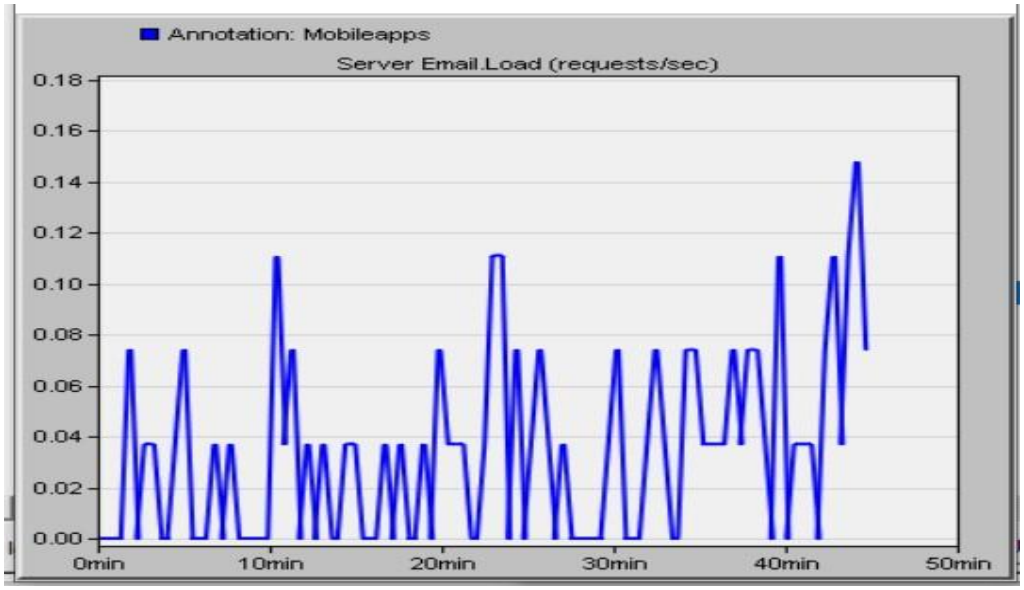

Figure 37. Email Load for iPhone Node.

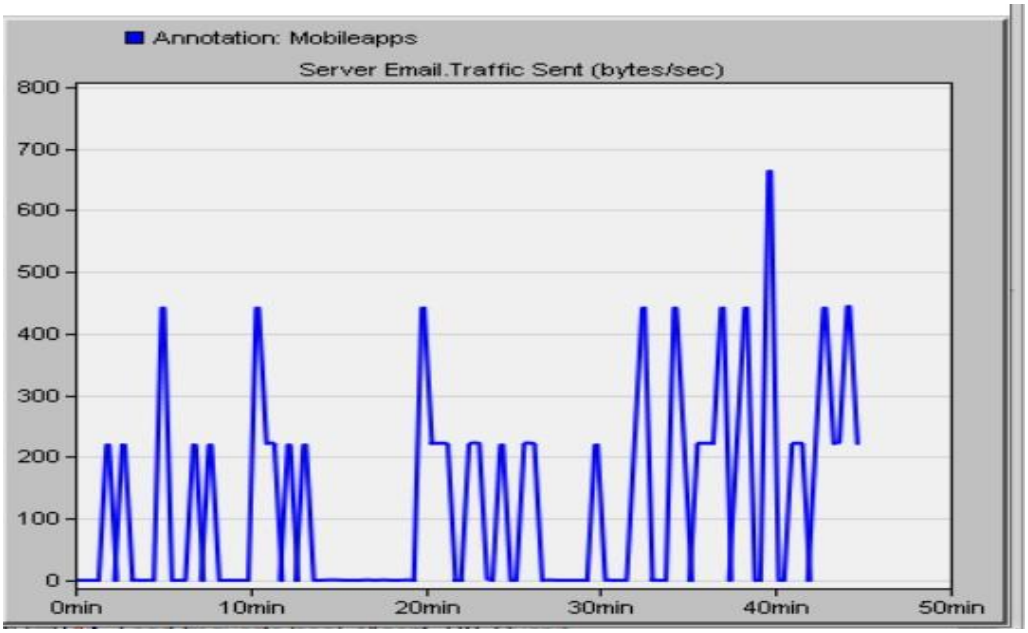

Figure 38. Email Traffic Sent for iPhone Node.

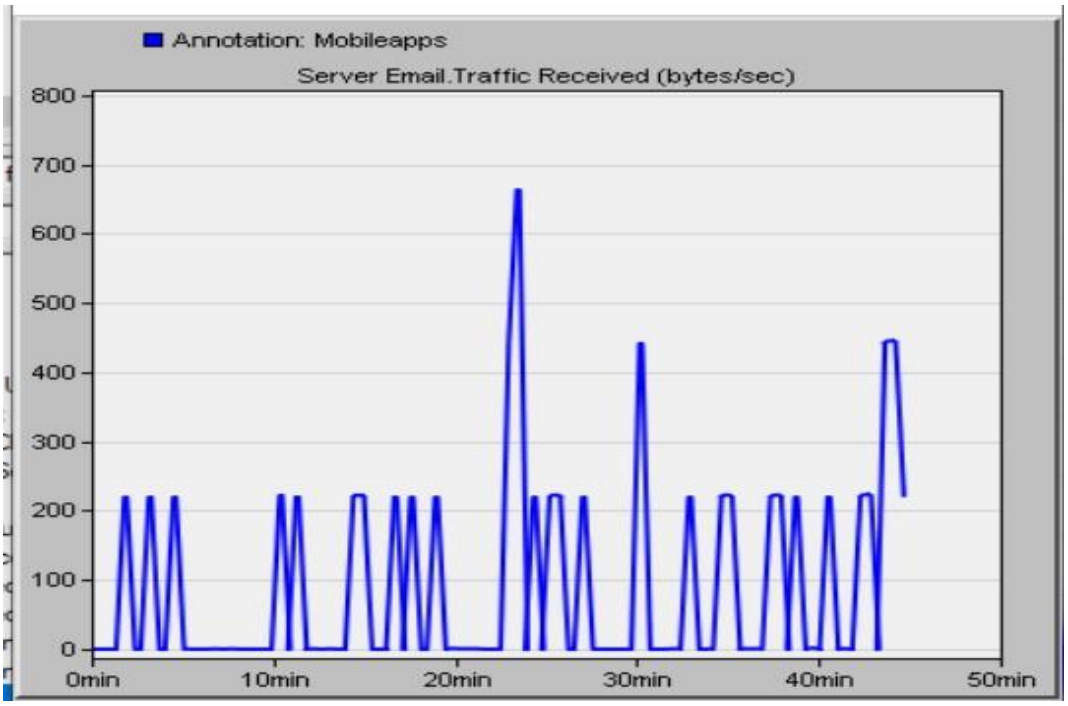

Figure 39. Email Traffic Received for iPhone.

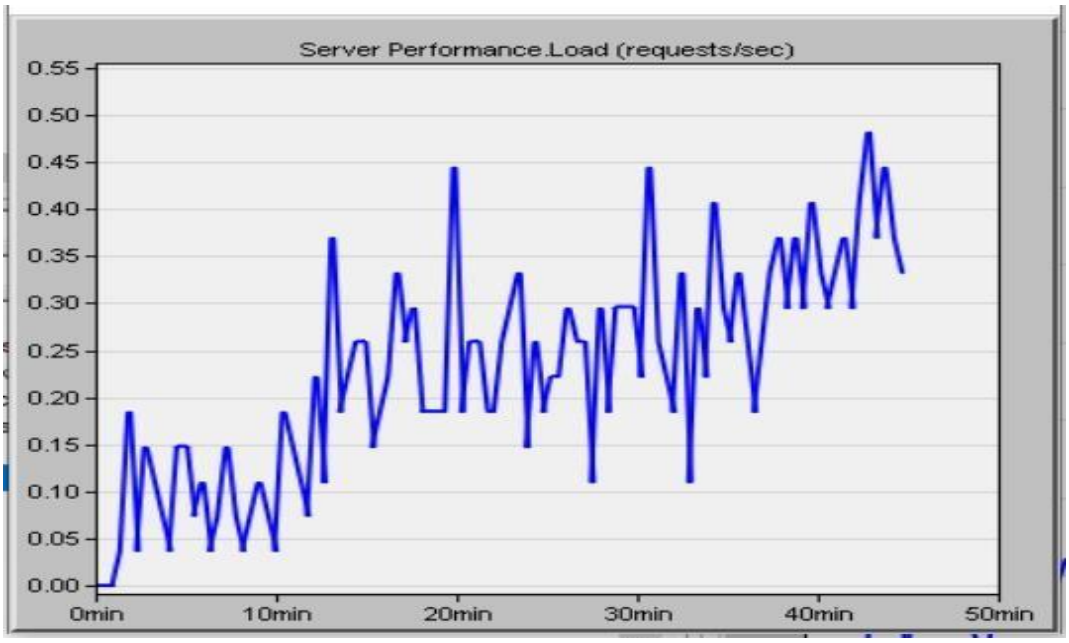

Figure 40. OLSR Load Performance for iPhone in Requests per second.

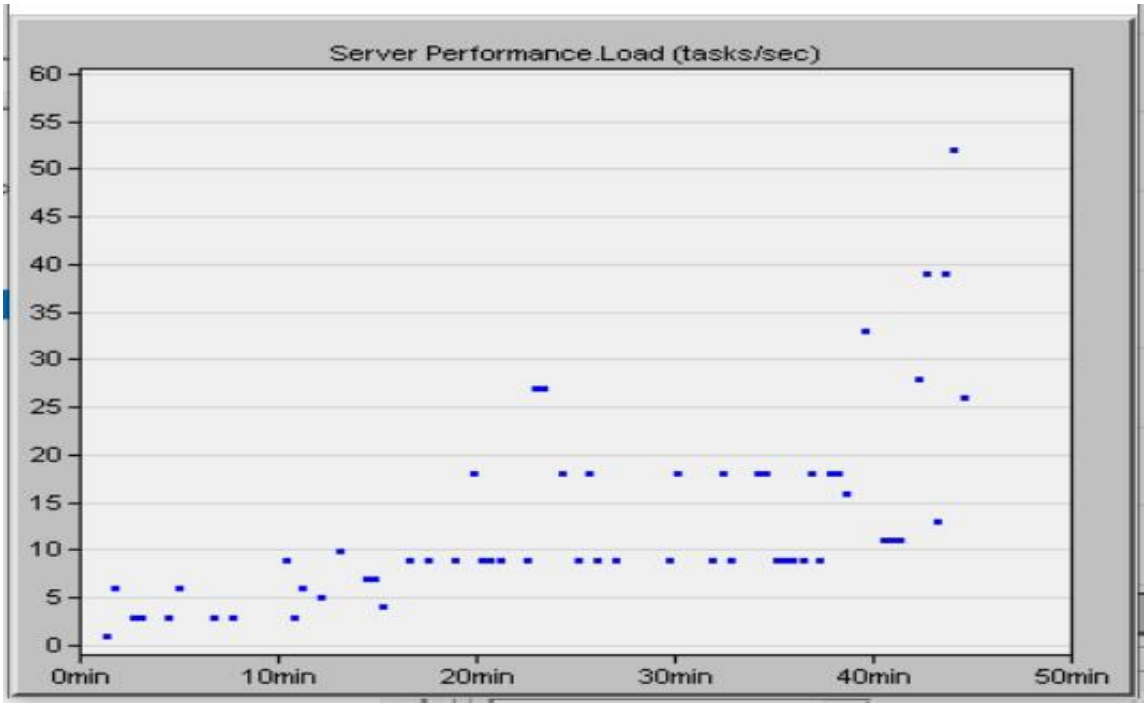

Figure 41. OLSR Performance – Load in tasks per seconds for iPhone.

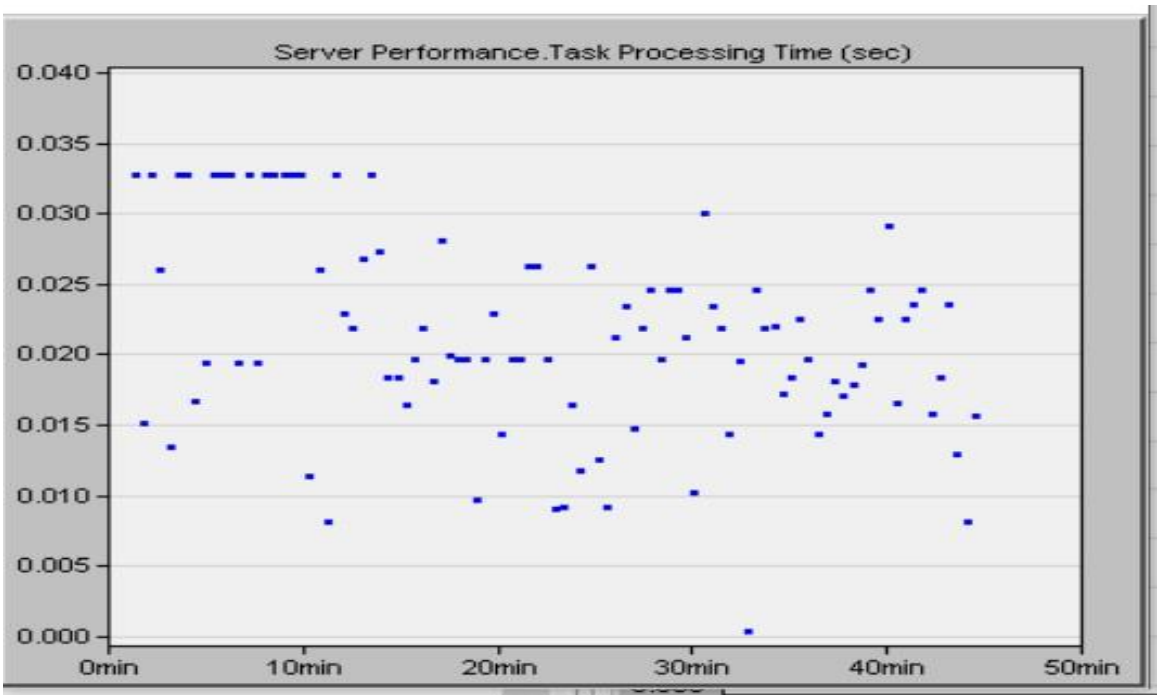

Figure 42. OLSR Performance - Task Processing Time for iPhone.

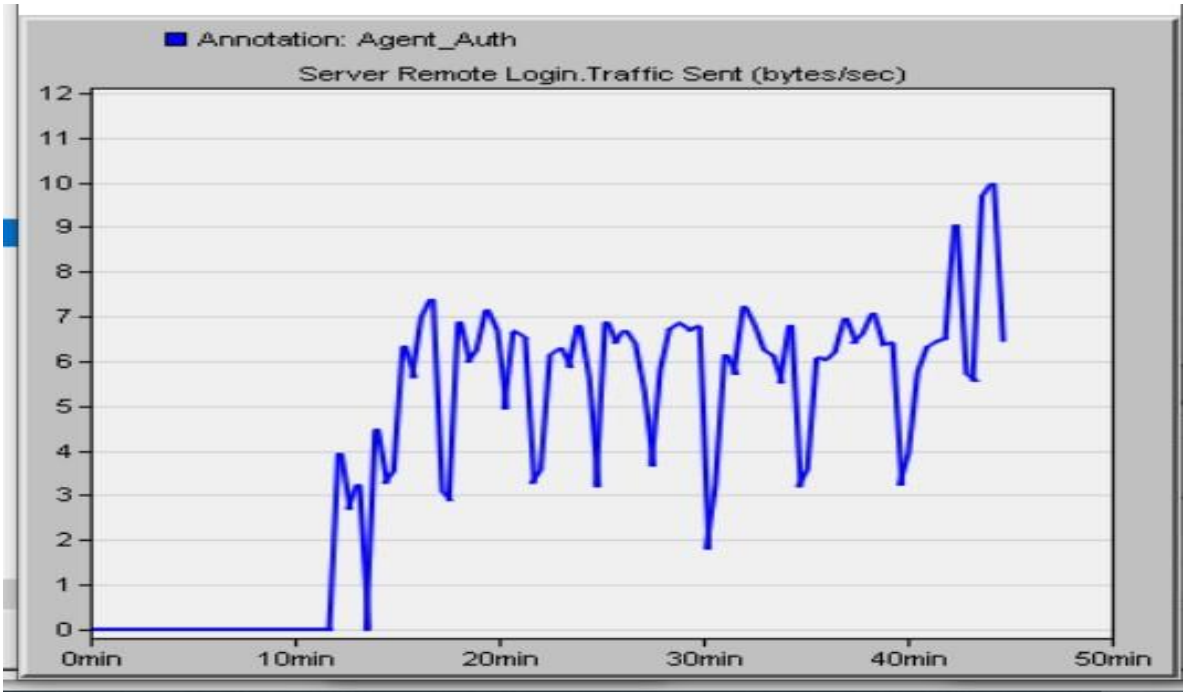

Figure 43. Remote Login Traffic Sent for iPhone.

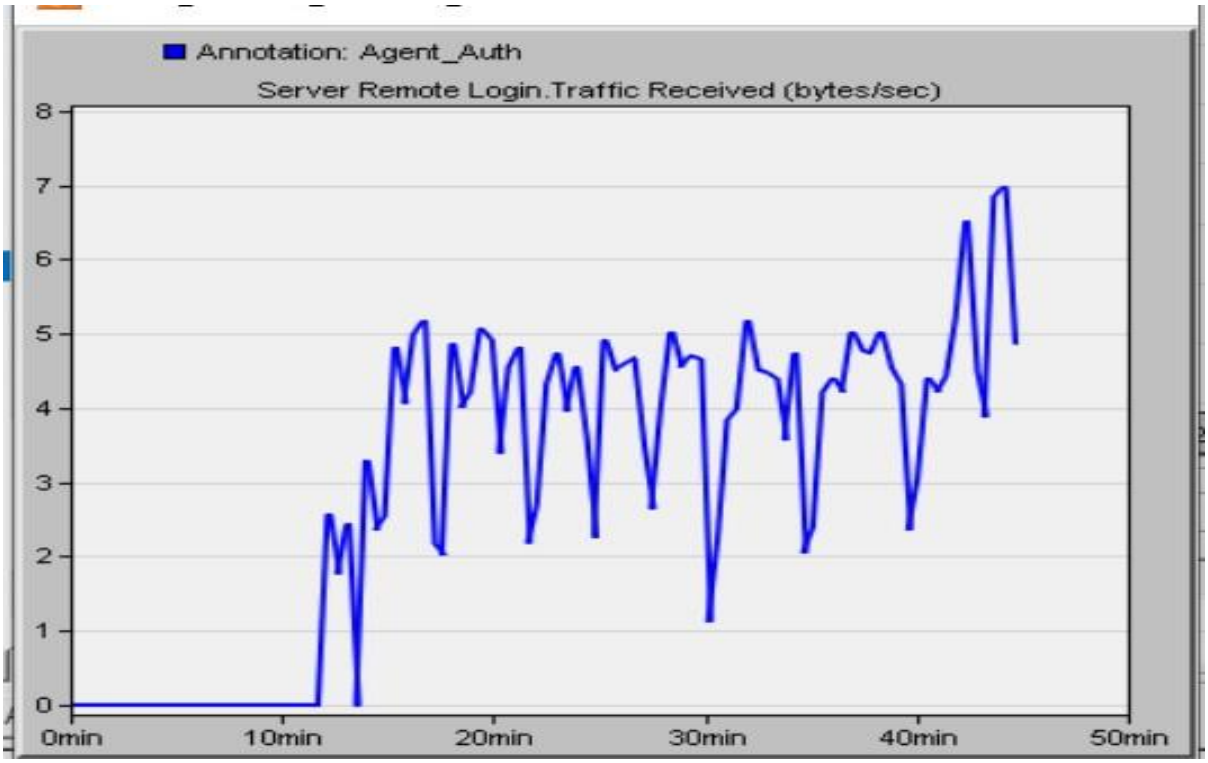

Figure 44. Remote Login Traffic Received for iPhone.

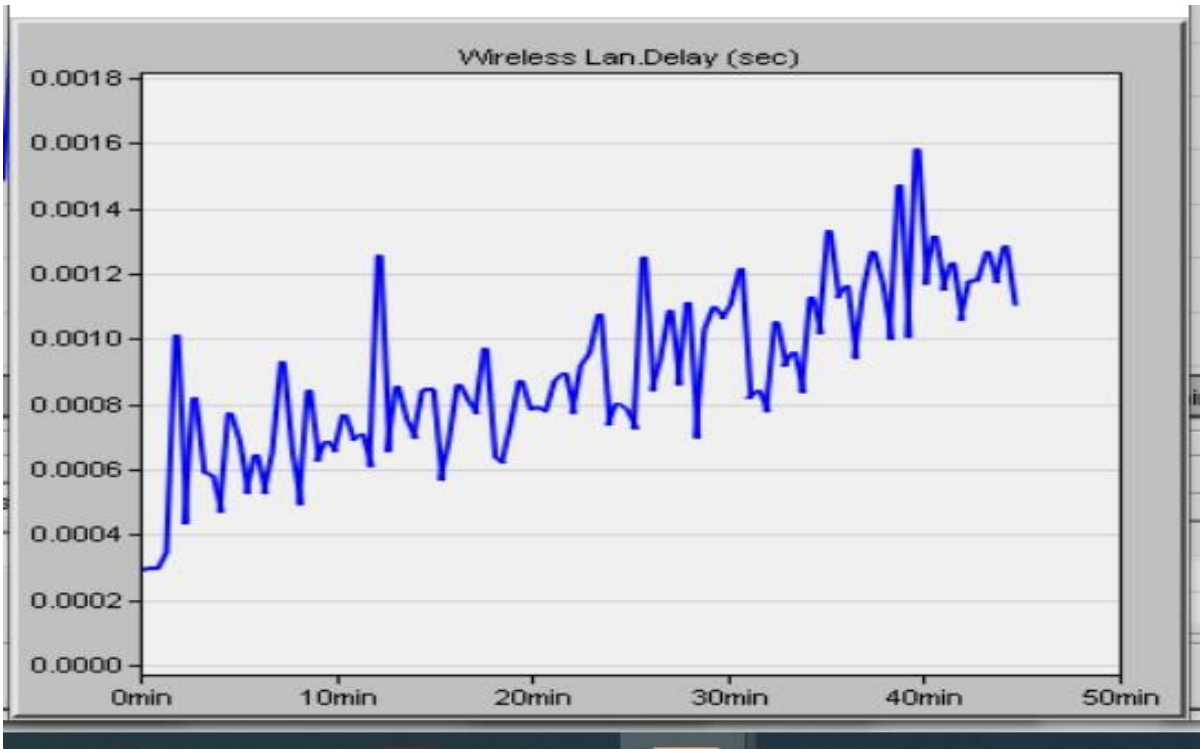

Figure 45. Wireless LAN Delay for iPhone.

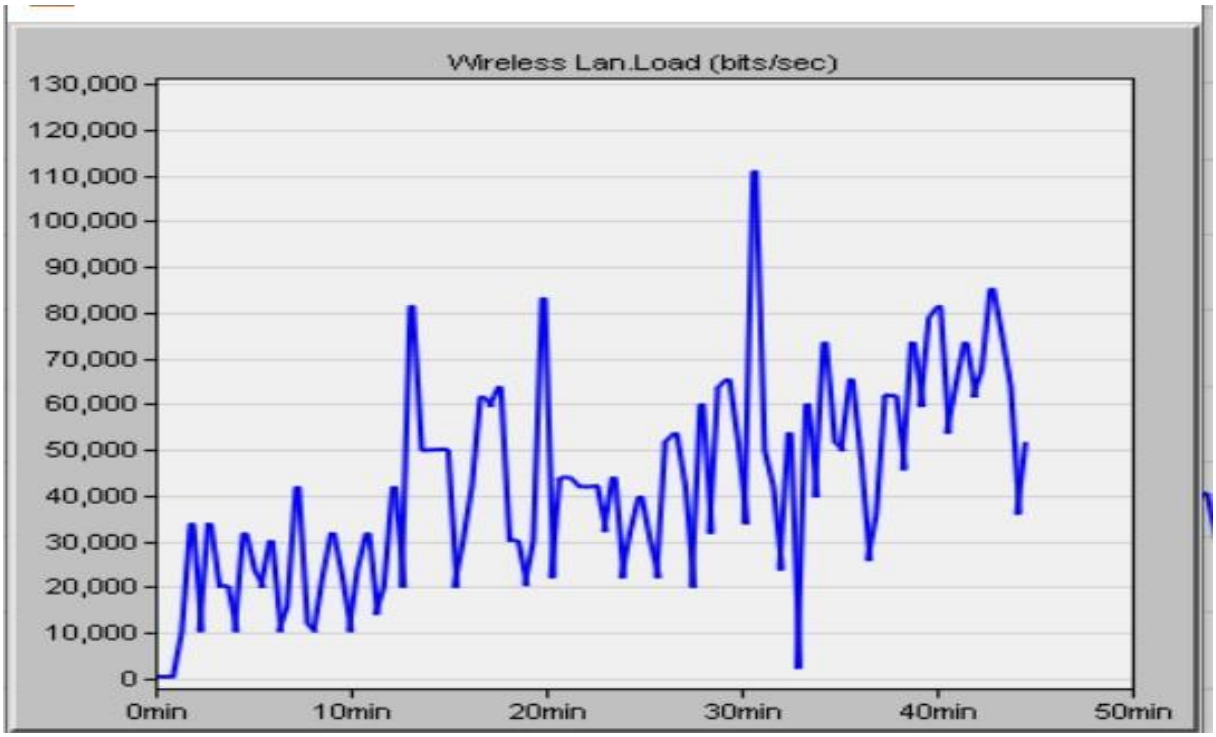

Figure 46. Wireless LAN Load for iPhone.

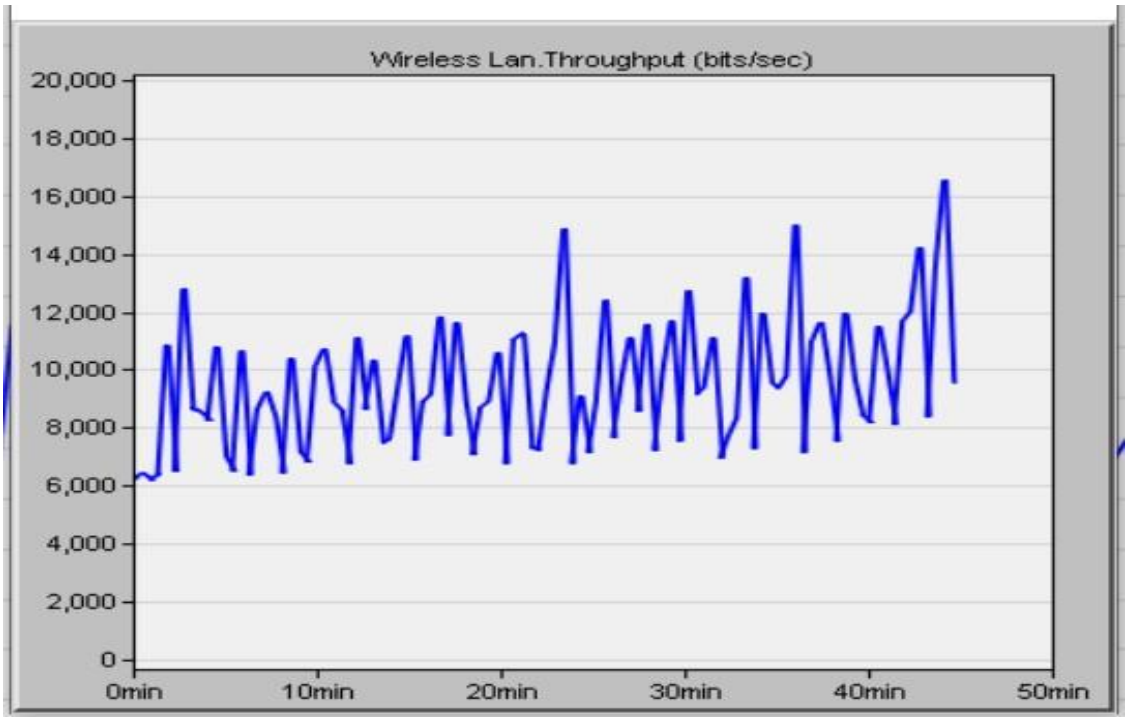

Figure 47. Wireless LAN Throughput for iPhone.

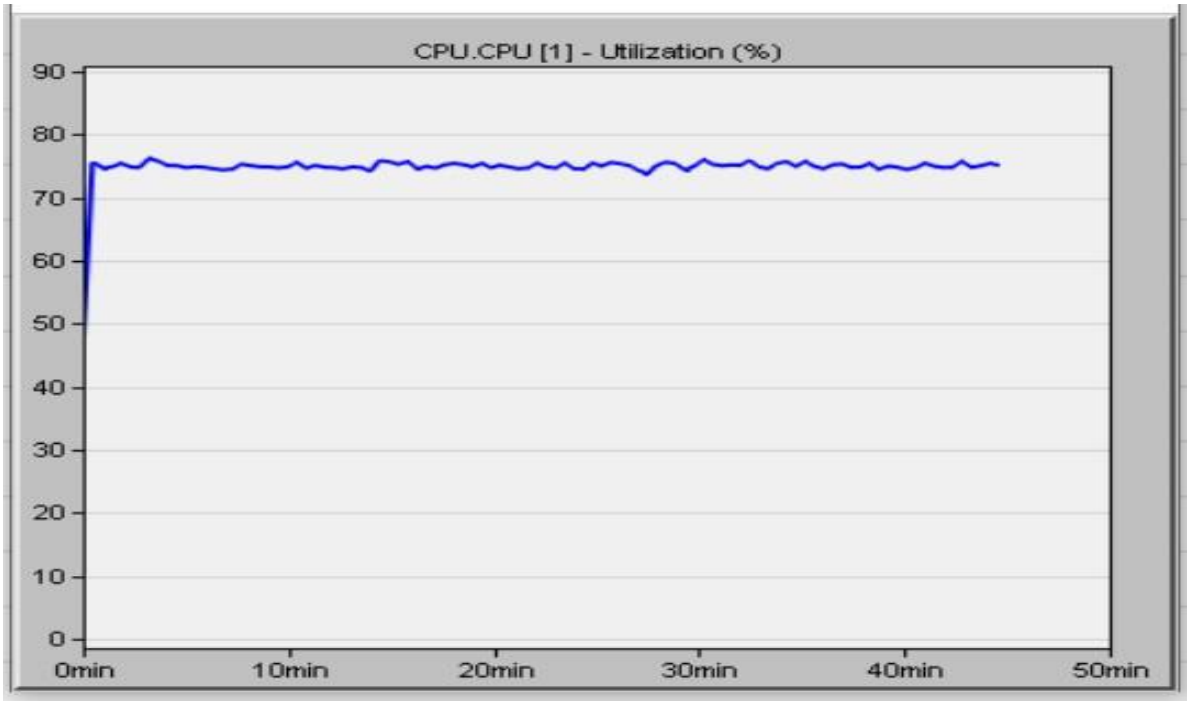

Figure 48. CPU Utilization for Android Node.

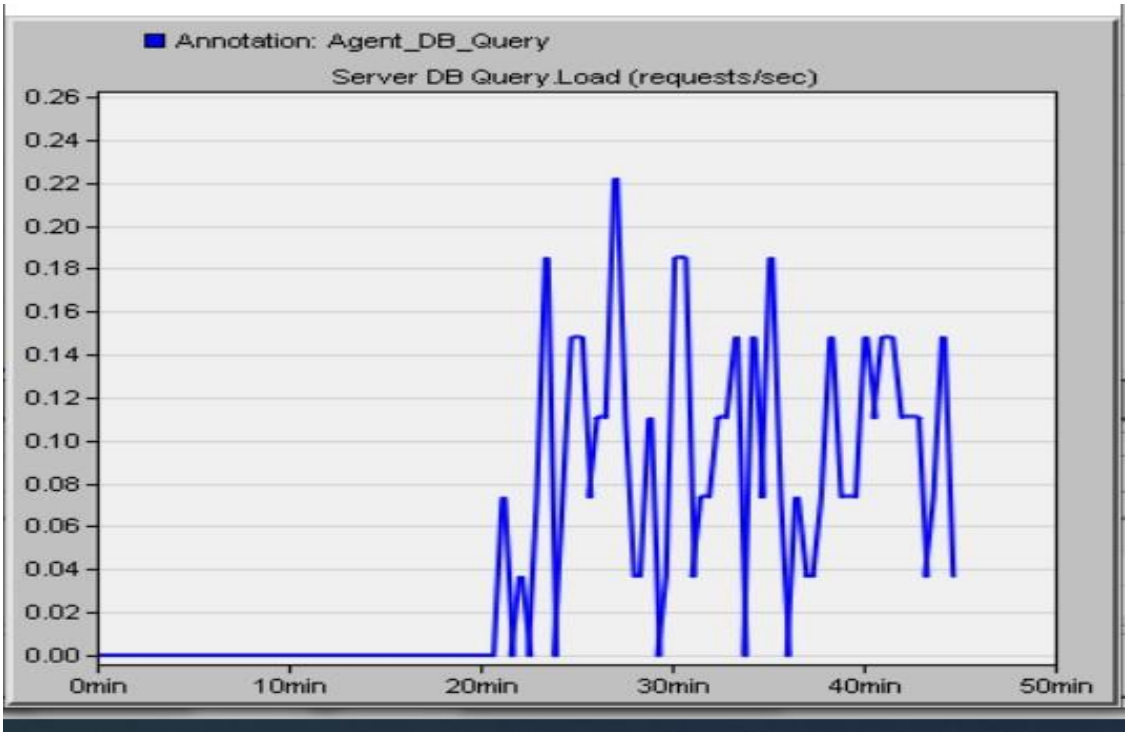

Figure 49. Database Query Load for Android Node.

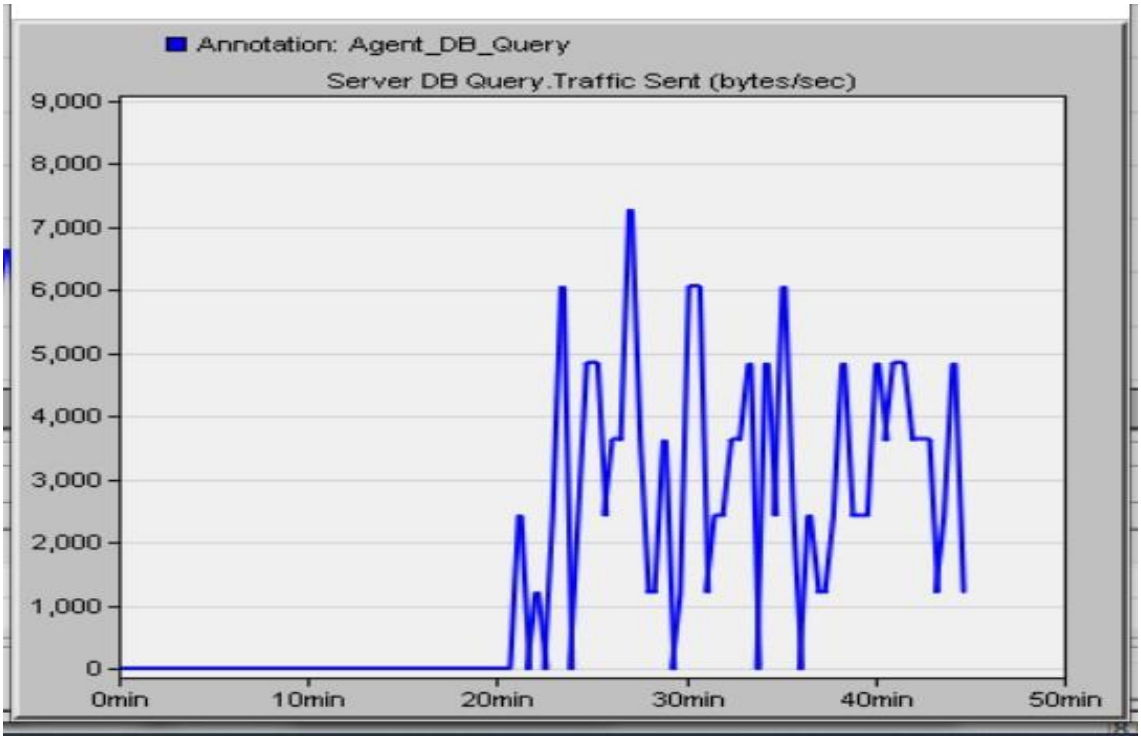

Figure 50. Database Query Traffic Sent for Android Node.

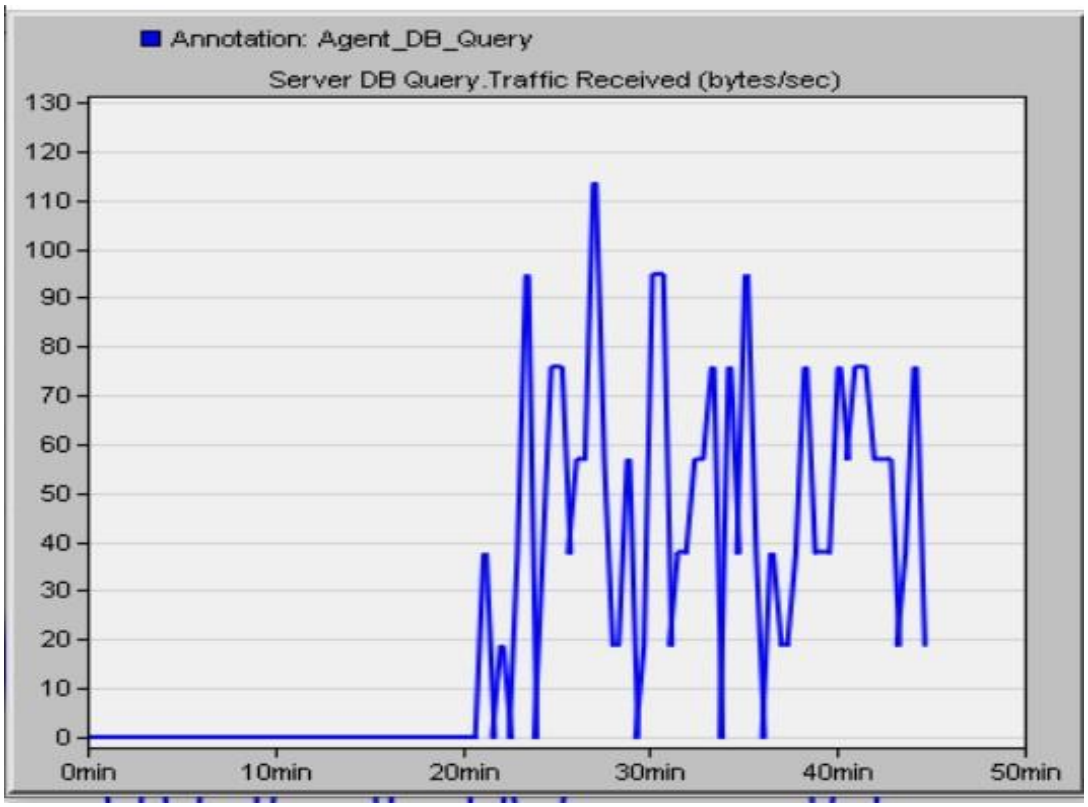

Figure 51. Database Query Traffic Received for Android Node.

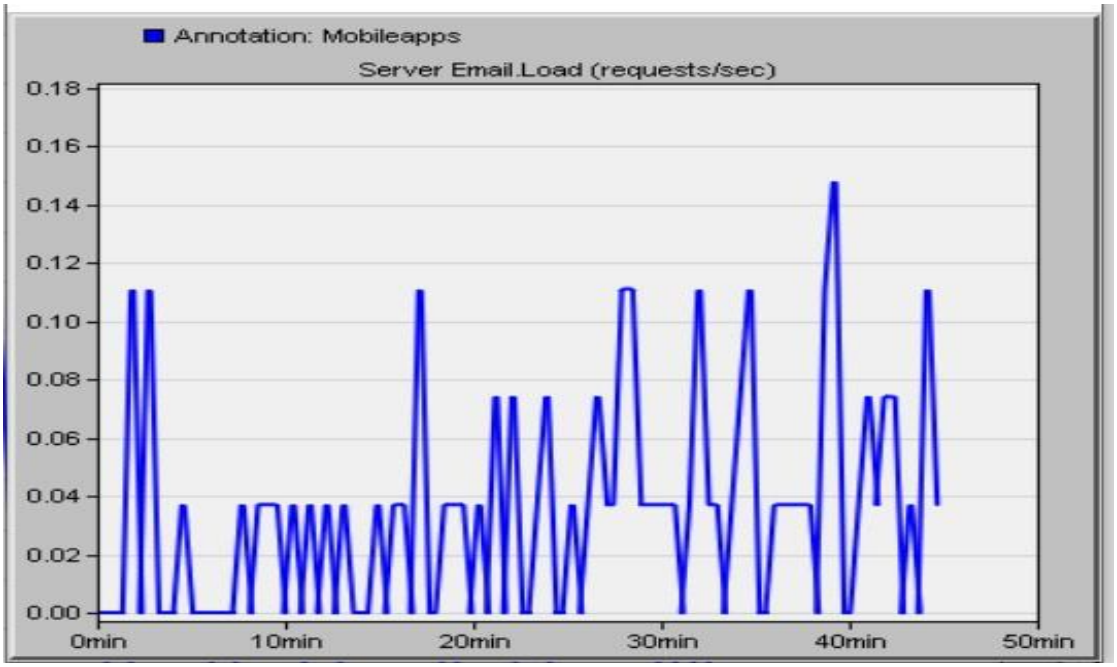

Figure 52. Email Load for Android Node.

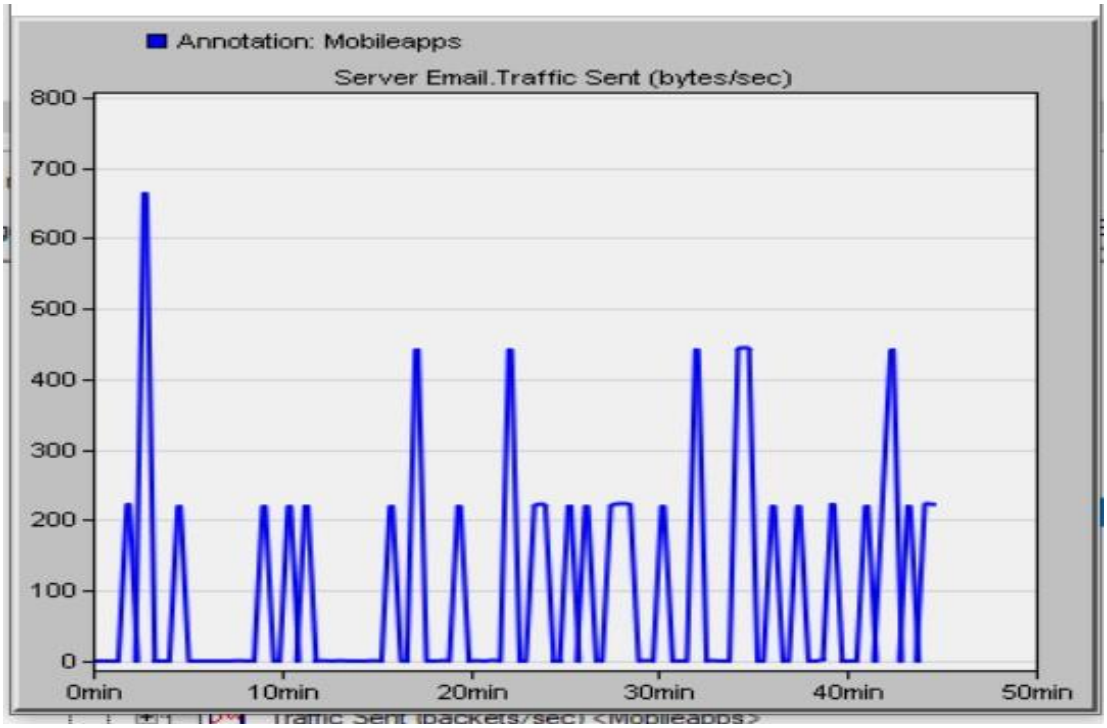

Figure 53. Email Traffic Sent for Android Node.

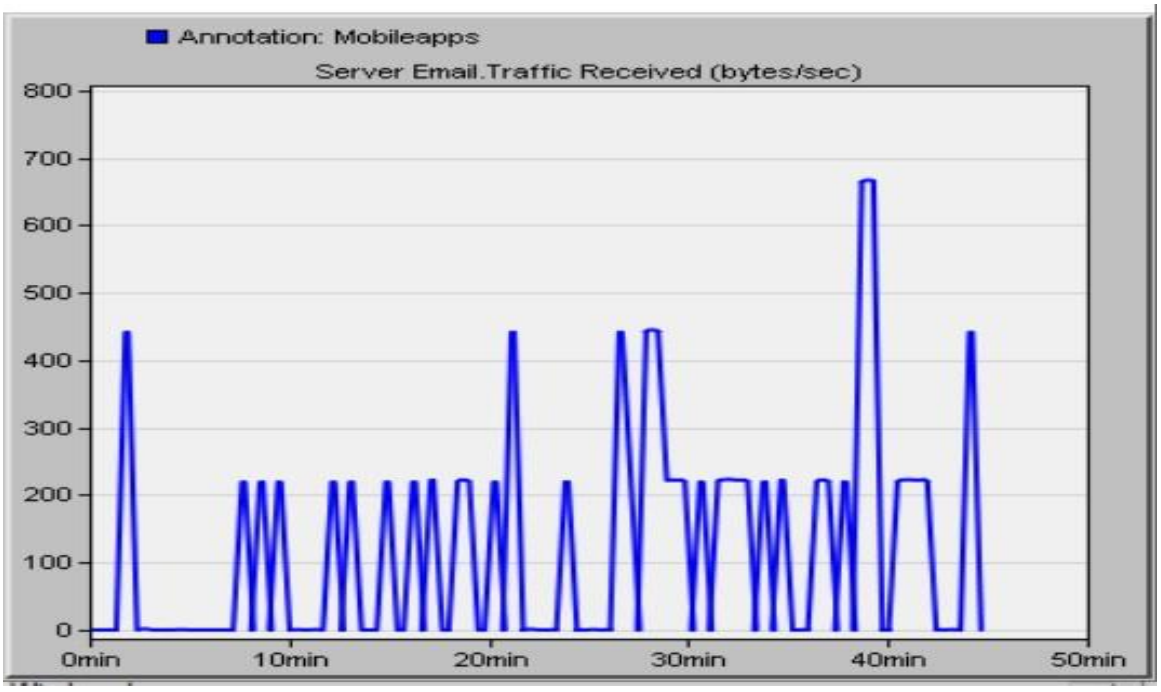

Figure 54. Email Traffic Received for Android Node.

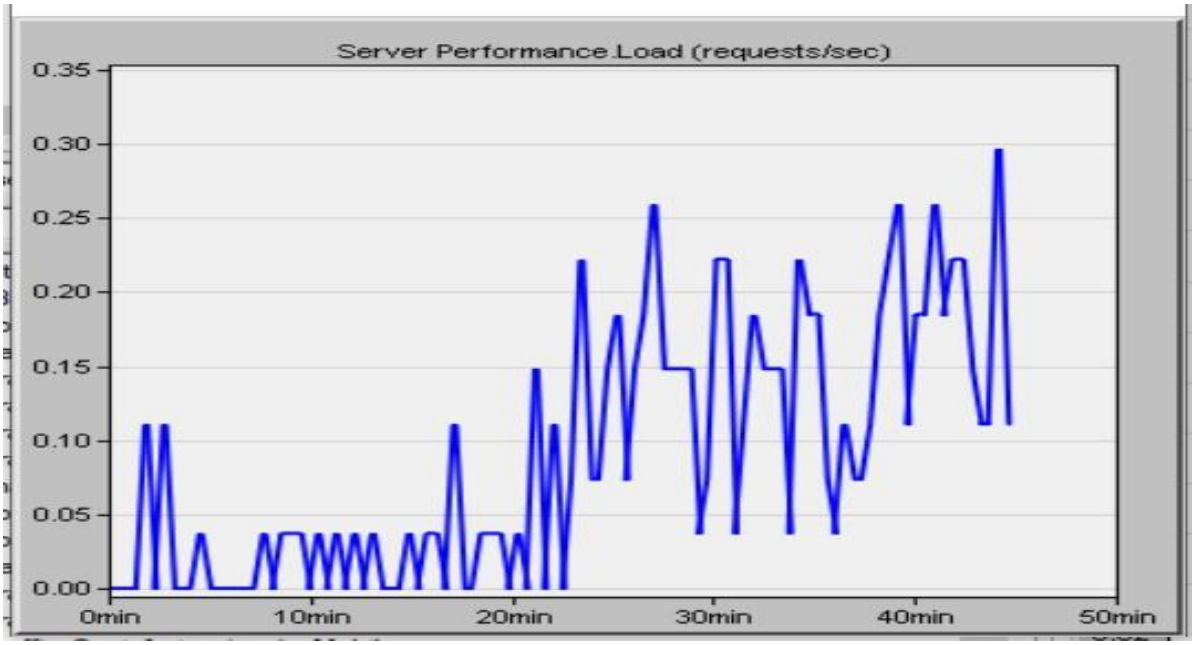

Figure 55. OLSR Performance – Load in Request per seconds.

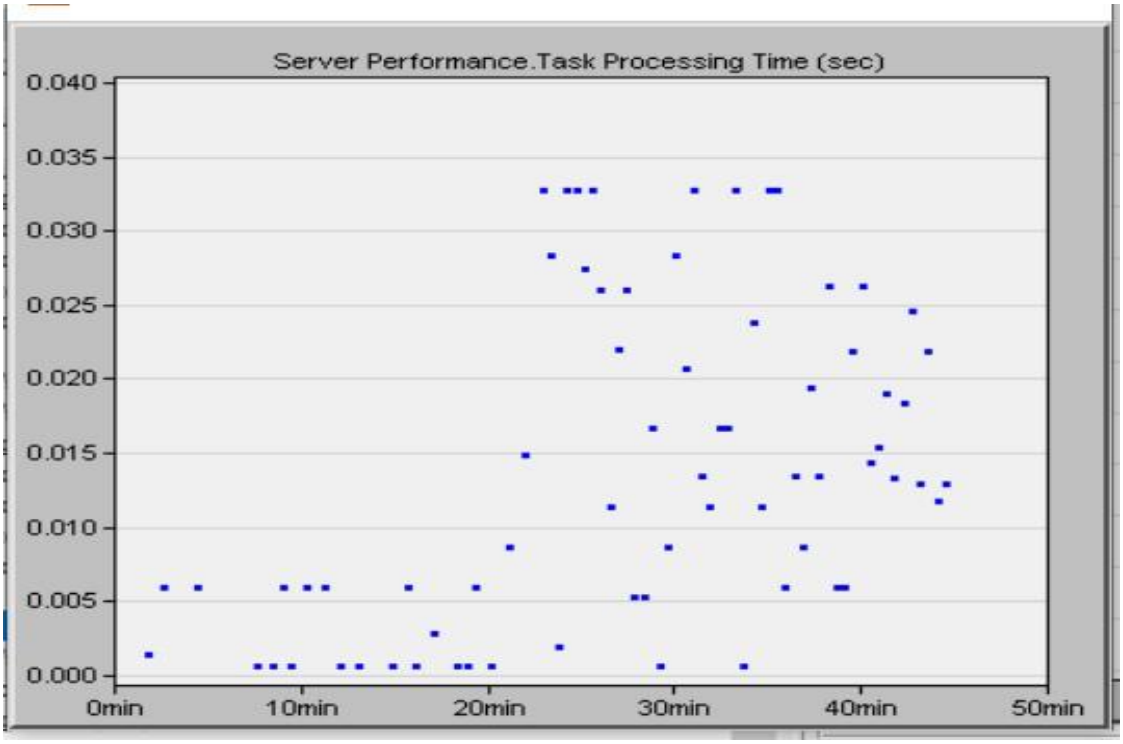

Figure 56. OLSR Performance – Task Processing Time.

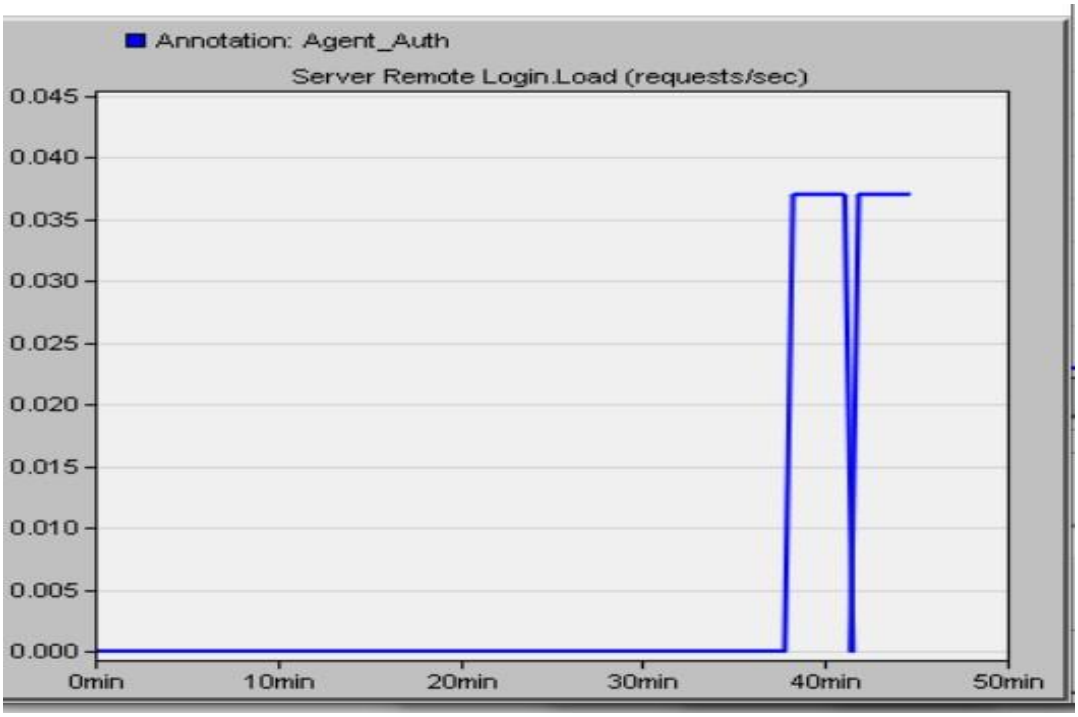

Figure 57. Remote Login Load for Android Node.

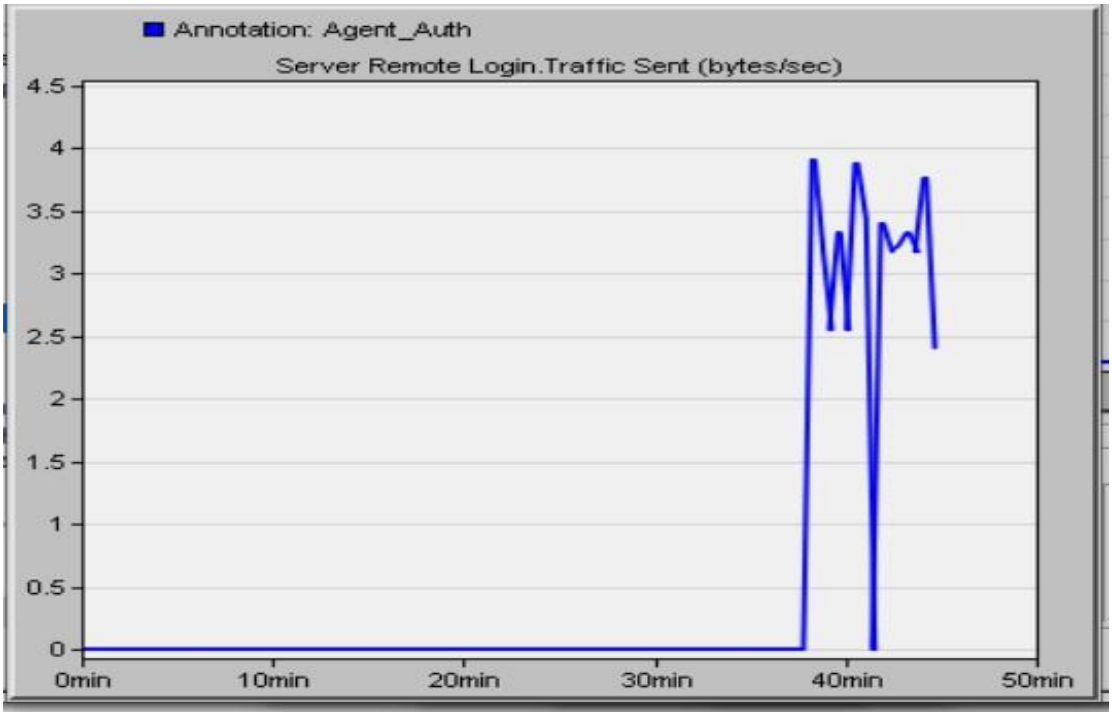

Figure 58. Remote Login Traffic Sent for Android Node.

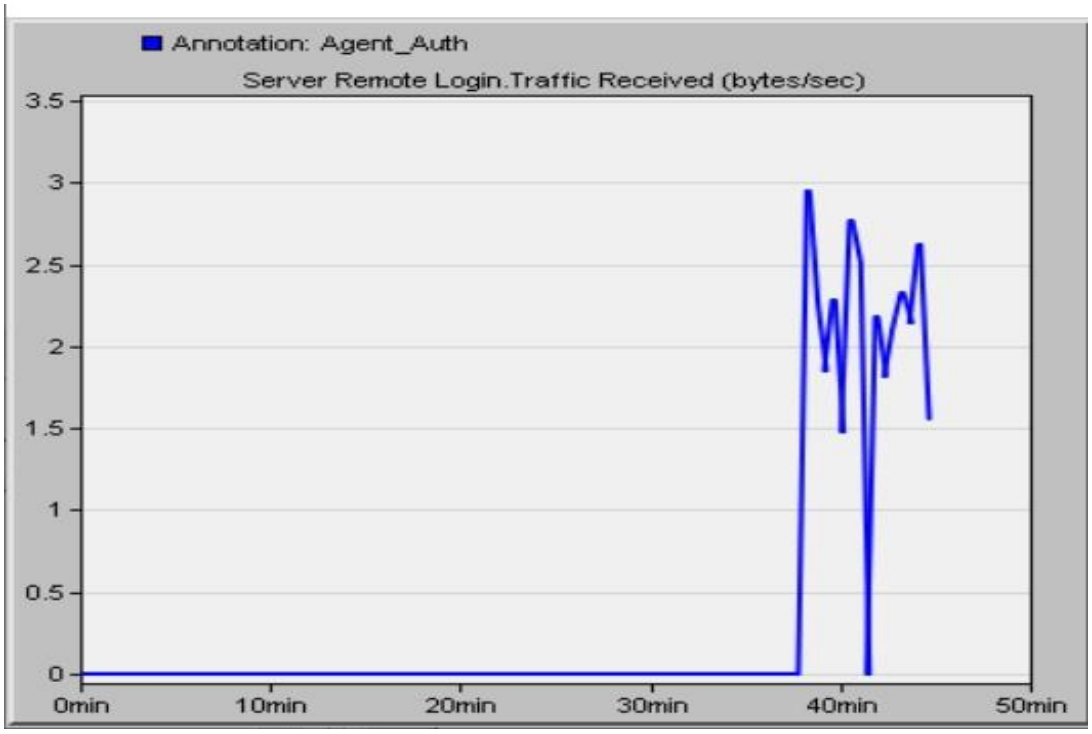

Figure 59. Remote Login Traffic Received for Android Node.

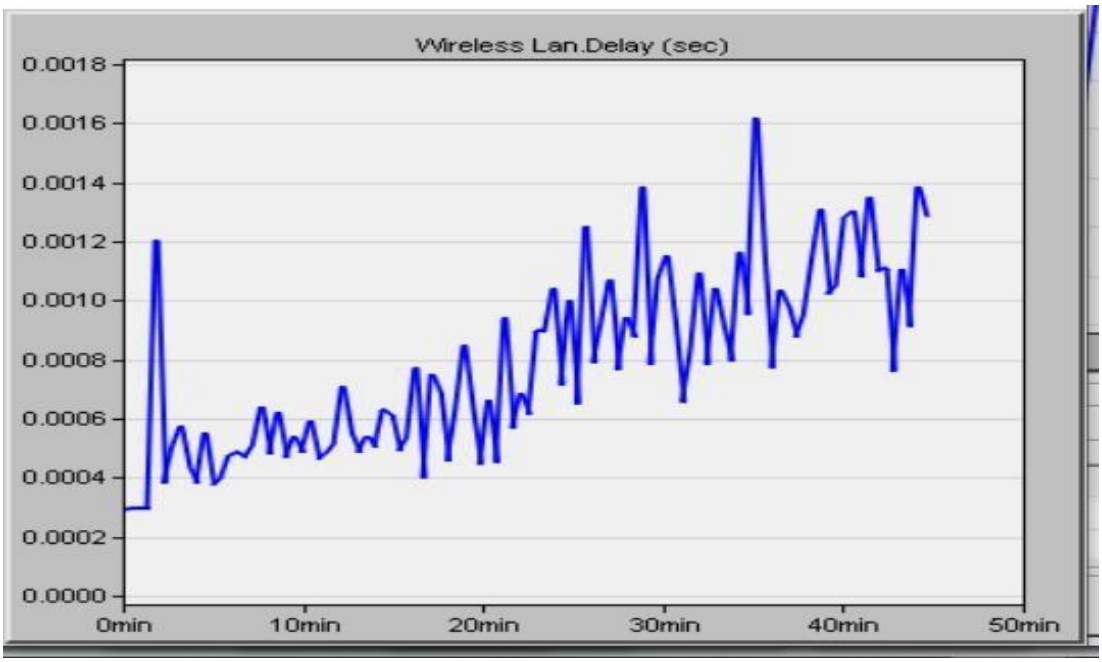

Figure 60. Wireless LAN Delay for Android Node.

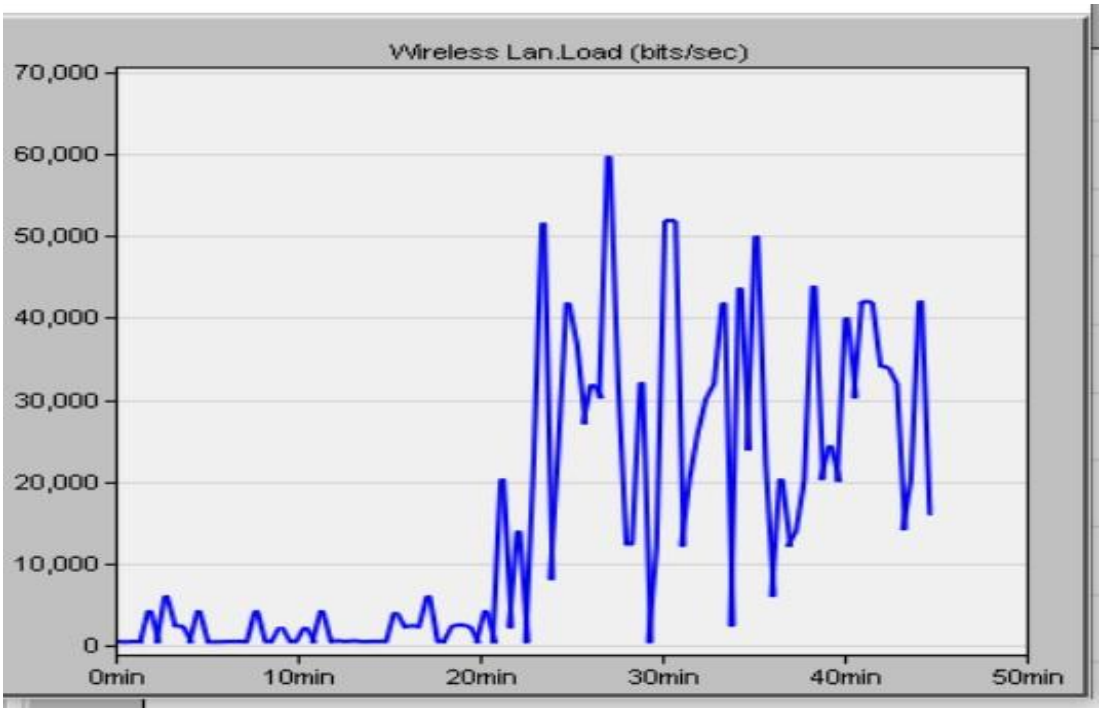

Figure 61. Wireless LAN Load for Android Node.

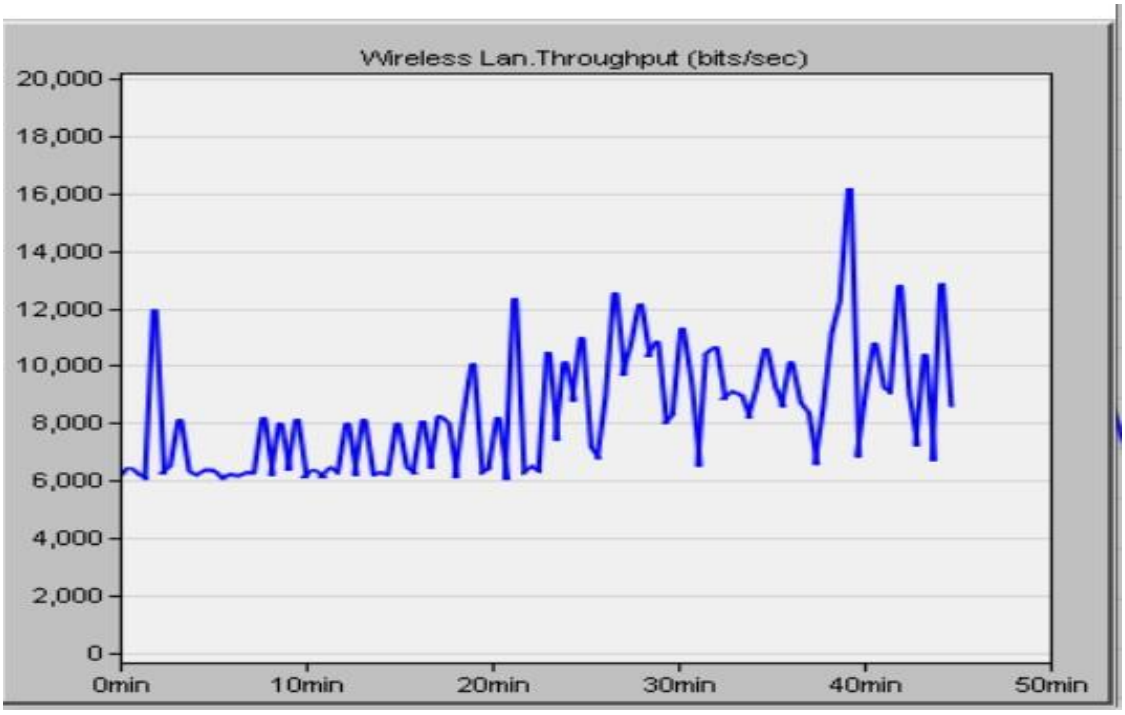

Figure 62. Wireless LAN Throughput for Android Node.

The results displayed above from the object statistics are interpreted as follows: CPU Utilization for iPhone Node is about 75 percent, Database Server Query Load for iPhone Node is peaked at 0.41 requests per second, Database Traffic Sent for iPhone Node is peaked at about 13,500 bytes per second, Database Traffic Received for iPhone Node has a maximum value of 210 bytes per second, the maximum Email Load for iPhone Node is 0.15 requests per second, the maximum Email Traffic Sent for iPhone Node is about 670 bytes per second, OLSR Load Performance for iPhone is about 0.48 requests per second, OLSR Performance (i.e. Load in tasks per seconds for iPhone) ranged from 2 to 52, for OLSR Performance maximum Task Processing Time for iPhone was 0.0325 seconds, maximum Remote Login Traffic Sent for iPhone was 10 bytes per second while maximum Remote Login Traffic Received for iPhone was 7 bytes per second, maximum Wireless LAN Delay for iPhone is valued at 0.0016 seconds, maximum Wireless LAN Load for iPhone is 110000 bits per second, maximum Wireless LAN Throughput for iPhone is 17000 bits per second, CPU Utilization for Android Node is 85 percent, maximum Database Query Load for Android Node is 0.22 requests per second, maximum Database Query Traffic Sent for Android Node is 7400 bytes per second, maximum Database Query Traffic Received for Android Node is 115 bytes per second, maximum Email Load for Android Node is 0.15 requests per second, maximum Email Traffic Sent and received for Android Node is 680 bytes per second. In terms of OLSR Performance, Load in Request per seconds was 0.3 while maximum task processing time was 0.0325 seconds. Android node Remote login values were 0.0375 requests per second for Load, 3.9 bytes per second for Traffic Sent and 3.9 bytes per second for Traffic Received. Android node wireless LAN values were 0.0016 seconds maximum for Delay, 60000 bits per second maximum for load and 16000 bits per second maximum for throughput.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1. CONCLUSION

This project involved the modelling and development of a Mobile Ad-hoc Network (MANET) using Optimized Link State Routing Protocol (OLSR) as the routing protocol. The various parameters measured proved that the MANET is functional and OLSR is a highly effective routing protocol for MANETs.

5.2 RECOMMENDATION

This work demonstrated the routing capacities of OLSR in a fifteen node MANET. However, as a future projection, it is recommended that there be a comparative analysis between various routing protocols for the same fifteen node MANET implemented in this project. This comparative analysis would help network designers determine which is a possible optimal protocol among those compared that can be implemented for the fifteen node MANET designed.

REFERENCES

Abolhasan, M., Wysocki, T. and Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. Ad hoc networks, 2(1):1{22, 2004.

Cheng, Y. (2014). Performance analysis of transactional traffic in mobile ad-hoc networks. Master's thesis, The University of Kansas, USA, 2014.)

Clausen, T. and Jacquet, P. (2003). Optimized Link State Routing Protocol (OLSR). RFC 3626 (Experimental).

Clausen, T.H., Hansen, G., Christensen, L. and Behrmann G. (2001). "The optimized link state routing protocol evaluating through experiments and simulation", Mindpass Center for Distributed Systems, Aalborg university, Denmark).

Clause, T.et al. (2003). "Optimized link state routing protocol", ietf.org/rfc3626.txt, oct. 2003.

Corson, M.S. and Macker, J. (1999). Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC2501, January 1999.

Dijkstra, E.W. (1959). A Note on Two Problems in Connexion with Graphs. In Numerische Mathematik, volume 1, pages 269–271.

Ge, Y. (2002). Quality-of-Service Routing in Ad-Hoc Networks Using OLSR. Master's Thesis, Ottawa-Carleton Institute of Computer Science, School of Computer Science, Carleton University, Ottawa, Canada.

Haas, Z. (1998). The zone routing protocol (ZRP) for ad hoc networks. IETF Internet Draft, draftietf-manet-zone-zrp-01. txt, 1998. http://www.ietf.org/rfc/rfc2501.txt.

http://www.opnet.com.

Jacqual, P., Laouiti, A., Minet, P. and Viennot, L. (2002). "Performance Analysis of OLSR Multi Port Relay Flooding in Two Ad-Hoc Wireless Network Models". The second IFIP-TC6 NETWORKING Conference, 2002, Pisa, Italy. inria-00471700.

Jacquet, P. et al. (2001). "Optimized Link State routing protocol", draft –ieff-olsr-04.txt-work in progress, march 2001.

Jain, R. and Shrivastava, L (2011). Study and Performance Comparison of AODV & DSR on the basis of Path Loss Propagation Models. In International Journal of Advanced Science and Technology, Vol. 32, pages 45–52, July 2011.

Jasani, H. (2011). "Quality of Service Evaluations of On Demand Mobile Ad-Hoc Routing Protocols" 5th ICNGMAS, IEEE 2011.

Johnson, D., Hu, Y. and Maltz, D. (2007). The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. RFC 4728 (Experimental).

Johnson et al. (2001). DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. Ad hoc net- working, 5:139{172, 2001.)

Kahn, R.E., (1975). The organization of computer resources into a packet radio network. In AFIPS National Computer Conference, May 1975.

Kiwior, D. and Lam, L. (2007). "Routing Protocol Performance Over Intermittent Links" *Military Communications Conference, MILCOM, IEEE,* 2007, pp. 1 – 8.

Mauve, M., Widmer, J. and Hartenstein, H. (2001). A survey on position-based routing in mobile ad hoc networks. IEEE network, 15(6):30{39, 2001.).

Mbougni, M., Ncube, Z.P. and Noutchie, S.C.O. (2013). Towards an OPNET Modeler Based Performance Comparison of Routing Protocols in Mobile Ad-Hoc. Networks Using Voice over IP Traffic Life Science Journal 2013;10(3):267-271] (ISSN:1097-8135). http://www.lifesciencesite.com.

Misra, R. and Manda C.R. (2005). "Performance comparison of AODV/DSR on-demand routing protocols for ad hoc GGnetworks in constrained situation" ICPWC International Conference,
IEEE, 2005, pp. 86 – 89

Perkins, C.E. and Bhagwat, P. (1994). Highly dynamic destination- sequenced distance-vector routing (DSDV) for mobile computers. In ACM SIGCOMM computer communication review, volume 24, pages 234{244. ACM, 1994.)

Perkins, C., Belding-Royer, E. and Das, S. (2003). Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental), July 2003.

Qasim, N., Fatin, S., & Hamid, A., (2008). "Mobile Ad Hoc Networks Simulations Using Routing
Protocols for Performance Comparisons" http://www.iaeng.org/publication/WCE2008/WCE2008_pp787-792.pdf.