Robust trust management framework for video streaming applications in mobile ad-hoc networks

T.L Phakathi

orcid.org/0000-0002-9426-7966

Dissertation submitted in fulfilment of the requirements for the degree *Master of Science-Computer Science* at the North-West University

Supervisor: Prof B.M Esiefarienrhe

Graduation May 2018

Student number: 23072504

NWU®
NORTH-WEST UNIVERSITY
NOORDWES-UNIVERSITEIT
UNIBESITI YA BOKONE-BOPHIRIMA

DEDICATION

I dedicate this research project to the following people:

- *Mrs. S.M Phakathi (mother)*
- *Mr. M.K Phakathi (father)*
- *Mr. T. Lin (Guardian)*
- *Mrs. G. Lin (Guardian)*

Thank you for your support, love and encouragement you have shown me to date.

ACKNOWLEDGEMENTS

Firstly I would like to extend my gratitude to all those who contributed to the completion of this project. I give thanks to GOD for wisdom and protection that He has given to me during this project and throughout my life. I give deep thanks to the Destiny Group, NWU postgraduate bursary and the faculty of Agriculture, Science and technology at the North West University for the opportunity given to me to study here. The experience has been an interesting and rewarding one.

This research would not be possible without my co-supervisor Dr. F.L Lugayizi whom I started this project with from my BSc Honours. He has been constant guide and his contribution to this work is immeasurable.

I would like to also extend my sincere gratitude to my supervisor Prof B.W Esiefarienrhe for his guidance, support, advice, for proof reading the drafts and making this research possible. I would not have put the topic together if it were not for his direction and guide. I am also thankful to the head of department of Computer Science Prof. N. Gasela for being a father and for his encouraging words. I would also like to extend my special thanks to my fellow students for their help, particularly Tebogo, Warren, Mercy, Rodney and Joshua for their ideas which contributed to this research.

I also thank my sisters Phetsile, Tholakele and Thandiwe for their constant support and encouragement as well as my cousin Thandekile for being my only family on Campus, which at times saw her take the role of being a mother, sister and all other roles at trying times.

It would be a big mistake if I did not thank my best friend and "Brother Siyabonga" who has never left my side ever since we started this race to date. I would also like to thank a special friend of mine, Mpumelelo, who at the point of giving-up, especially at the time I struggled with the simulation tool, encouraged me and has always supported me over the past years.

I would also like to thank my family for their continuous prayers and unconditional support.

Lastly, I am deeply thankful to my guardians and mentors Mr. Tom Lin and his lovely wife Gugulethu for their financial support and guidance from the time I started working at Destiny Group till present. I pray that God bless them abundantly.

DECLARATION

I, THULANI LINDELWA PHAKATHI, hereby declare that this project report titled *"A Robust Trust Management Framework for Video Streaming Applications in Mobile ad hoc Networks"* is my own work carried out at North West University, Mafikeng Campus and has not been submitted in any form for the award of a degree to any other university or institution of tertiary education or published earlier. All the material used as source of information has been duly acknowledged in the text.

Signature: _____ Date: _____

Thulani Lindelwa Phakathi

APPROVAL

Signature: _____ Date: _____

Supervisor: **Prof. B.W Esiefarienrhe**

Department of Computer Science
North West University
Mafikeng Campus
South Africa

Signature: _____ Date: _____

Co-supervisor: **Dr F.L Lugayizi**

Department of Computer Science
North West University
Mafikeng Campus
South Africa.

ABSTRACT

Trust is an important computer networks concept and remains an issue not just in social platforms but also in networks in delivering of Quality of service (QoS). Video Streaming has, over the years gained prominence in mobile and vehicular *ad hoc* networks. However, video streaming is faced with several challenges of being vulnerable to different attacks and poor QoS. This work proposed a robust and efficient trust management framework that eliminates poor QoS due to network detriments caused by the dynamic topology of a MANET. The trust framework aims to assist in node accountability and QoS attainment, i.e. it does not remove the dynamic topology issue but it strives to attain nodes' trustworthiness and excellent QoS despite the conditions set out against the network. The proposed trust framework is an application-centric trust management framework with distributed trust computations (AppTrusFram). It merges the concept of trust together with QoS in an application scenario. This work presented a theoretical-design solution to the topology related issues and discussed issues found in other proposed solutions. The QoS evaluation conducted for low, mid and high node density scenarios based on two routing protocols Ad hoc On-demand Distance Vector (AODV) and Optimized Link State Routing (OLSR) carrying video conference traffic (high quality). By using the framework and the establishment of trust in the network, the achieved results proved its significance as delay periods were extremely low. The also results proved that OLSR performs better in high node densities and traffic as compared to AODV whose information overhead grows as the network density increases. The results showed overall excellent QoS. A conclusion was drawn that OLSR needs constant topological update messages in order to perform well and this observation be as a future reference point to provide the best service in video streaming applications over MANETS.

LIST OF ACRONYMS AND ABBREVIATIONS

AODV	: Ad hoc On-demand Distance Vector
DSR	: Distance Source Routing
IEEE	: Institute of Electrical and Electronics Engineers
IP	: Internet Protocol
MANETs	: Mobile Ad hoc Networks
OLSR	: Optimized Link State Routing
OPNET	: Optimized Network Engineering Tools
OPPNets	: Opportunist Networks
P2P	: Peer to Peer
TMF	: Trust Management Framework
TORA	: Temporally Ordered Routing Algorithm
QoS	: Quality of Service
QoE	: Quality of Experience

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Introduction and Motivation

A mobile ad hoc network (MANETs) is an autonomous type of system which comprises of separately connected sets of self-configuring nodes that may be activated by putting to use various techniques e.g. Bluetooth or WLAN. MANET is autonomous in behavior because each node is regarded as its own host and router at the same time [1].They rely on direct communication and multi-hops for communication between distant nodes within the network making them scalable and robust. These advantages make them more flexible to accommodate many nodes, decentralize administration and their setup can be placed anywhere and at any time [2]. Contrary to other Wireless systems, MANETs do not have a central authority that monitors the forwarding of traffic. In this instance, each node acts as a router to forward traffic to other nodes within the network. MANET systems consist of infrastructure less system of associated nodes connect through wireless links[1].Nodes move arbitrarily or rather in a random faction[3]. All these characteristics render MANETs vulnerable to security threats like wormhole attack, information disclosure attack, rushing attack etc. Network threats and limitations leave a room for concern to the extent that network users doubt the credibility of the network and its trustworthiness. Communication and packet forwarding is fully dependent on the trust of a neighbor node participating in the network.

Trust in MANETs is very important from node level to network level. According to Semplay *et al.* [1], because of the dynamic nature of MANETs, trust can be used as a measure for nodes that want to provide an acceptable level of trust in that relationship among themselves. Trust management in a MANET is way too challenging than in traditional network environments infused with a central controller because of the dynamic topological nature and characteristics of MANETs. This may result in uncertainty and incompleteness.

QoS according to Singh *et al.* [8] is a set of service requirements required by network as packet streams maneuver from source to destination. It is a growing technological concept. This growth is promoted by the emergence of real-time applications like video conferencing applications, online gaming, chatting, and instant messaging (IMs). In MANETs, trust is the belief of a node that other nodes within the network will cooperate in a particular way without disturbance and compromise in the network's activity and security.

MANETs are self-organizing and self-healing. The network must be trustworthy in order to achieve the highest QoS or acceptable quality of service. Trust in MANETs is required when the involved workstations wants to communicate and establish an acceptable and satisfactory level of trust in the network and among themselves without prior or historic interaction first hand [1]. Trust is perceived differently in various fields of study but is said to have originated in the social sciences and is made for use in computing, communication, etc. Trust is asymmetric, which means that it is possible for two nodes not to have the same trust for each other [1].

1.1.1 Mobile ad hoc Networks

MANETs have become some of the most ubiquitous areas of research over the past ten years or more because of the complexities they bring to the related network protocols. MANETs are still regarded as a growing technology which enables network users to interact without any central controller regardless of their GPS location. It is for that reason that they are sometimes regarded as infrastructure-less networks[4]. Their growth is promoted by the growing need to provide the users with the network support at their own convenience [5]. MANETs are primarily useful in the army and other security-based applications such as covert missions, emergency and rescue missions[6]. Ad hoc networks stretch back to the 1970s, meaning that they are not a new concept. They were used by the military. Their commercial success has been due to advances in wireless technology. Standards have been developed for routing in MANETs. The IETF (Internet Engineering Task Force) regulates the new group for MANETs. The IEEE standard 802.11 has contributed to research interest done with MANETs[4]. What also facilitates their growth is the continued development and manufacture of smaller and faster devices and this makes MANETs the fastest growing networks. The mobility of nodes, however, is rapid and unpredictable over time. MANETs, like all wireless networks are more susceptible to attack and weaknesses when taken into comparison with wired networks. The limitations of wireless systems are multitudinous in multi-hop networks, especially because

multimedia streams are subject to the aggregate effect, and that is jitter, packet drop, of each link along a terminal-to-terminal path. In ad hoc networks, the maneuverability of a node sometimes leads to a lot of path breaks or rather route breaks. Reconfiguring routes is a time taxing exercise, thus packets might be lost in bursts because they are sent to routes that are no longer working or rather inactive [7].

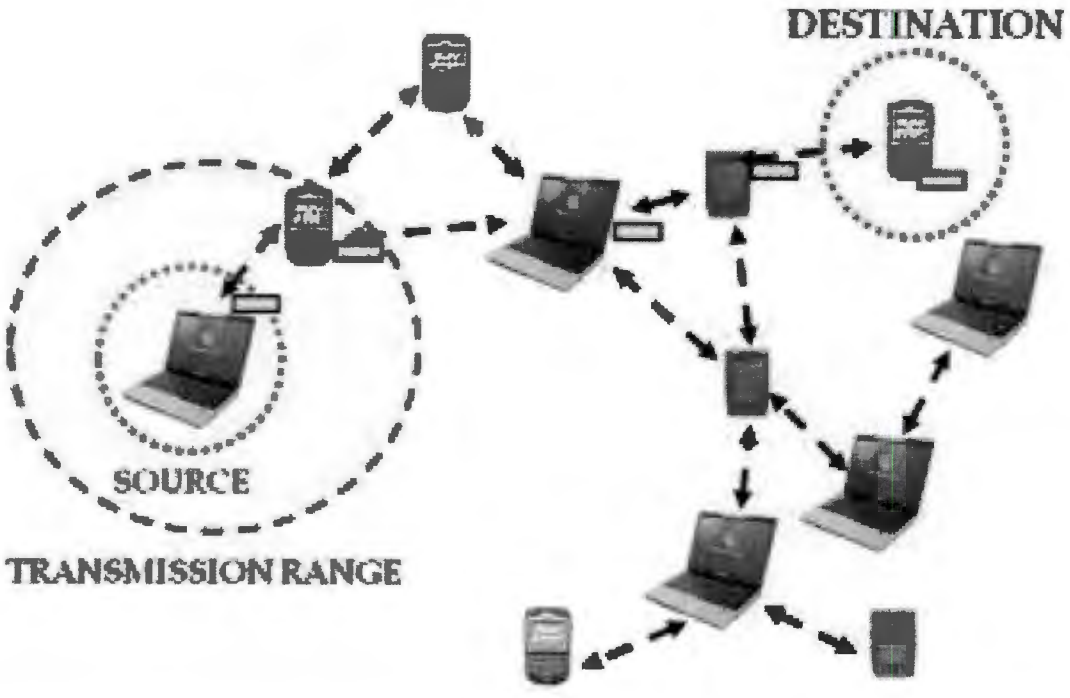

Figure 1.1 Typical MANET [3]

Routing is done through hops achieved by using routing protocols. These routing protocols are in each device. In figure 1.1, from source to destination, neighboring nodes forward packets. Routing relies on packet forwarding. The most important aspect is getting all/most of the packets to the destination.

1.1.2 Quality of Service

The needs for the provision of QoS are increasing in relation to applications that involve voice and video and it is most appropriate to support these through the implementation of ad hoc network environments. In the field of telecommunications, QoS was first brought to attention in 1994 as a phenomenon that has requirements on all the aspects of a network connection, as well as response time during service times, network detriments such as echo, interrupts, signal to noise ratio and also loudness levels. In the field of computer networking, QoS is the ability to bring a different level priority to different applications, users, or data flows, or to ascertain a specific level of execution to a data flow[8]. In order to achieve QoS, the concept of routing is important. Routing is regarded as the act of steering information from a source to a terminal in a network.[8]. One intermediate node within the network is experienced during the movement of information. In essence two activities are implemented in this concept: determining excellent routing paths and moving the packets within the network[9]. Routing may be either dynamic or static. Static routing is routing done manually or statically in the access point device while dynamic routing is the routing that is being learnt by an inner or outer routing protocol. QoS is measured using specific metrics within the network. Some of the evaluated metrics include bandwidth, jitter, delay, packet loss etc. Our work seeks to evaluate the networks' performance in terms of throughput, delay and dropped data.

1.1.3 Trust Management

The term "trust" originates from the discipline of social science when referring to how one party (normally referred to as trustor) is willing to rely on another party (may be referred to as trustee). This can be greatly attributed to human beings and their relationships. Trust can also be attributed to relationships in social groups. When it comes to the discipline of Computer Science, a trusted component has elements within itself that another component within the system can rely on. If component A trusts component B, this means that any violation of properties found in component B, will ultimately affect the correct operation of A. This, however, does not mean if A trusts B, then component C can trust B. Because of the nature of MANETs, trust management is a necessity of nodes

which want to participate in networking. This is done to give an acceptable level of trust relationships among each other during transmission or rather at operational level.

1.2 Problem Statement

Trust is an important feature in networks [10]. The nature of MANETs still makes the guarantee of efficient trust a complex task due to its highly dynamic topology constraints. The emergence of MANETs calls for the address of many problems perceived in networks and to also optimize some of the existing network resources [2]. The question that remains unresolved is "Can trust be truly guaranteed in a MANET?" The answer to this question according to this study will be based on the QoS study.

Different authors have presented different trust frameworks. According to Li [11], existing trust management frameworks encounter great challenges under antagonistic network environments, which can disturb their function in terms of performance. This means that the reason most frameworks failed is that they did not address the problem of topology and its dynamism in various types of networks hence the need for robust frameworks that will be resistant and still give optimum performance. Authors in [12], developed a simple node-based trust management scheme for MANET. Their framework included multiple perspectives on the concept of trust, a clear demonstration of the properties, which is a key element in the development of trust metrics. It also gave an idea on how a trust metric can be channeled into meeting the requirements and end goal of the Node-Based Trust Management (NTM) scheme. In Ferdous *et.al* [12] in terms of later work, they considered the possibility of developing a framework with desirable attributes such as adaptation to topology dynamics, reliability and also scalability [12]. This research is geared towards achieving the possibility as envisaged by [12] because a good scheme is one that encompasses all these characteristics in order to ensure trust in the network. Dynamically changing topology is one of the characteristics and limitations of MANETs. The most important aspect is achieving good QoS. It is impossible to say a characteristic like this one can be completely run over but it is possible to achieve a greater QoS to such an extent that its dynamic nature would not be such a limitation thus a robust and efficient trust management framework is needed to prevent nodes from being selfish or performing selfishly. This work seeks to close that gap by building a framework that not only looks at trust but also with reference to video streaming applications in MANETs. Much concentration will be based on the achievement of trust between nodes of a network. Different network scenarios will be established,

which means an outlook on performances, behaviour and together with their QoS of video streamed applications will be closely monitored.

1.4 Research Questions

This work seeks to answer the following research questions

RQ1: To what extent have network developers and researchers addressed the challenges of trust in video streaming over mobile ad hoc networks?

RQ2: How is the performance in terms of trust-based quality of service amongst nodes to be measured in high node density environments?

RQ3: How can trust be merged into a relation that will result in quality of service?

RQ4: Can a trust based framework for QoS in MANET be formulated, simulated and evaluated?

1.5 Research Goal

The main goal of this research is to formulate, design and implement a robust and efficient trust management framework that will address trust related issues in video streaming applications over MANETs.

1.6 Research Objectives

In order to achieve the research goal presented in section 1.5, the following objectives will be fulfilled;

RO1: Analyze and understand the major challenges of trust in video streaming applications over MANETs.

RO2: Investigate video performance in high node density environments in terms of trust- based quality of service amongst nodes?

RO3: Present a correlation between trust and Quality of Service through the formulation of a trust management framework.

RO4: Implement and evaluate the framework in (iii) using OPNET Modeler

1.7 Research Methodology

In order to achieve the main goal of this research through the objectives specified, we shall follow research methodologies below in order to achieve RQ4 and RO4.

1.7.1 Literature Survey

An in depth survey on the current literature was done in order to find answers to RQ1, RQ2 & RQ3 and also achieve **RO1** in section 7.

1.7.2 Design a Trust Management Framework

In order to fulfill **RO3** in section 1.6, a framework will be designed and formulated.

1.7.3 Run a simulation to implement proposed trust management framework

Our simulation experiment was run using different scenarios to test out the effect of our proposed framework to achieve RO2 using OPNET Modeler.

1.7.4 Proof of Concept

As a proof of concept, the results from the developed framework mechanism were analyzed, compared and conclusions were drawn based on those observations to achieve RO2 and RO4.

1.8 Limitations of Study

The scope of our work is limited and focuses on a Trust-based QoS routing that can be achieved by video streaming applications in MANETs. In this work, two routing protocols, Optimized Link State Routing (OLSR) and ad hoc On-demand Distance Vector (AODV) were chosen. New metrics were not formulated. These protocols were chosen on the basis that they perform well in handling video traffic [5, 14]. Simulation work in this study was conducted on Optimized Network Engineering Tools (OPNET) modeller. OPNET has a great reputation and is regarded as one of the best simulators for network research and development. OPNET has a wide range of protocols, applications and devices. It allows designers to not only study but also develop the behaviour of the entire network. Our work will not implement new performance metrics but will use existing QoS measures.

1.9 Dissertation Contributions

The main contribution of this work towards both academia and the research community is in the design and implementation of a Quality of service-based Trust Management framework centered on the application (video conference) by merging both trust and QoS.

A complete performance evaluation paper [13] on VANETs was presented in the proceedings of the 2016 International Conference on Computational Science and Computational Intelligence Las Vegas, Nevada, United States of America, and published in the IEEE CPS proceedings, pages 886-891.

The literature and proposed framework was submitted as work-in-progress to the 15th International Conference on Privacy, Security and Trust to be held on the 28th till 30th of August 2017 in Calgary, Alberta, Canada

A detailed paper was submitted and accepted for oral presentation at the Third International Conference on Electronics and Software Science (ICESS2017) which is scheduled to take place from the 31st July-2nd August 2017, Takamatsu, Japan .The paper has also been conditionally accepted for publication in one of their accredited journals.

CHAPTER SUMMARY AND THESIS OUTLINE

In this chapter, we presented the introduction and motivation of this research work. We also presented the main goal, objectives, key research questions and key words. **Chapter two** presents a brief overview on trust management, MANETs and QoS. It is in this chapter that answers to research question 1 and research objective 1.This chapter also presents topological challenges found in literature. **Chapter 3** presents the research methodology and a detailed experimental setup employed to achieve the goal. This chapter begins by documenting the tool OPNET then introduces the various steps taken implement our simulations. It then gives a detailed description of what should be expected in chapter four concerning framework design is also discussed. **Chapter 4** presents our proposed trust framework from design, setup and implementation in a MANET station. It starts by giving a brief background of the environment where simulations were conducted. It then presents our framework, operational architecture and its component parts. Lastly, it brings out the frameworks' operations. The chapter also presents answers to research question 4 and research objective 4. **Chapter 5** presents an analysis of the results found from the simulations. It also brings out a comparison within network scenarios of the two main protocols being used. This chapter also brings answers to research question

3 and research objective 3. **Chapter 6** is the concluding chapter of the work. It summarizes the entire research work. Suggestions for Future work are also presented in this chapter. What follows this chapter is the Bibliography section containing references

CHAPTER 2

LITERATURE REVIEW

2.1 Chapter Overview

Literature reviewed in this study revolves around the established trust management frameworks in MANETs, video streaming, Quality of service and also topology related issues that are found in MANETs.

Literature reviewed provided an opportunity to establish that MANETs comprise of nodes moving in a given space at various speeds and thus resulting in dynamic topology changes, and also brings forth problems to efficient and reliable message distribution because of violations of trust among nodes communicating. A large number of protocols have been further studied and implemented in efforts to accommodate for MANET specific reliability requirements. Literature furthermore states that in MANETs, these protocols are grouped into topology-based, Positioned-based, Geo-cast, Broadcast and Cluster-based protocols respectively. The deployment of these protocols is based on the above-mentioned areas even beyond especially by the establishment of hybrid protocols whereby two or more different protocols are merged to attain a specific aim. This study, however, will mainly be based on topology-related routing protocols.

Further knowledge reviewed in literature, was trust management frameworks implemented in MANETs. The need for efficient and robust trust management frameworks grows each day. Trust must be guaranteed on all levels of a network and that is from node to network level in order to counteract and enhance security and the proper functioning of the entire network. Literature reveals some measures taken through the formulations of a few named frameworks. It also reveals that more study should be made on uncovering new architectures, protocols, standards and methods which satisfy the trust criteria.

Another important aspect covered by literature was the importance of QoS which is the network's ability to give out an acceptable level of service to the network. Many studies were focused on QoS measures of various protocols whereas others simply resorted to focusing on the pros and cons of

specific protocols and studied their behavior. Literature, however, has given more emphasis on trust management frameworks that neither seeks to address issues pertaining to topology and scalability in MANETs.

2.1.1 Introduction

MANETs are considered a household technology service in the mobile network industry. Their growth has been hailed in the entire world and they have attracted so much attention in recent years with the invention of Vehicular ad hoc Networks (VANETs) and its integration into the automotive industry. The fast demand for video streaming applications like video conferencing and video-on-demand are central to MANET technology. Researchers, in recent studies, have shown great interest QoS in the mobile network fraternity. This subject continues to attract a lot of interest among researchers and such is reflected through publications. The available literature will grant us the opportunity to base our own study in terms of relation, reference and relevance through the analysing of past study, give constructive criticism of similar studies, acknowledging the research study conducted and also seeking for gaps or rather loop holes for further research input into the subject.

It is of paramount importance to mention that the reviewing of literature will be based around; Trust as a concept, Trust Management frameworks, QoS measures (i.e. throughput and jitter), video streaming applications, performance evaluation of protocols, the analysis of video performance, topology related constraints in MANETs and an in-depth look at a few protocols. Emphasis will be strongly drawn to protocols that will be investigated in protocols that will be further implemented in the experimental phase of our research work. It is worth noting that, the reviewed literature is more inclined to describe existing trust management frameworks in MANETs.

At the end of this chapter, we would have presented our analysis of the reviewed literature material and our input towards the related studies. At a later stage we would provide a chapter summary.

2.2 Quality of Service

Quality of service can be defined as the network's ability to give out an acceptable level of service to a specific network traffic. There are specific metrics put in place in order to evaluate the competency of routing protocols on video streaming applications. Metrics like latency, throughput, delay and jitter are taken into consideration. Below are some of the few metrics discussed in literature:

2.2.1 Latency

It is the time it takes for packets to get from one node to another node during the transmission period.

2.2.2 Throughput

It is the total number of routing packets received by the destination over the total simulation time[15].

2.2.3 Average End to End Delay

This is the average as a measure of how many cycles it takes for the data packets to arrive at their intended destination[15].

2.2.4 Jitter

Jitter is simply considered as a variation in delay of received packets.

2.3 Trust Management

Trust Management has been a buzzing phenomenon in the area of computer science. Many researchers have implemented various forms of frameworks in order to tackle issues in MANETs and wireless sensor networks. All these implementations were to address specific issues in these networks. Trust [11] can be referred as the level of belief that one node can put on another node for a particular execution given direct or indirect information from observation of behaviours. The level of belief is the extent to which one node believes that another node consents in respect of the protocol and acts well. According to Govindan *et al.* [16] trust is an important aspect of MANETs. The computation of trust and its management is a highly challenging issue because of its computational complexity constraints and the random movement of nodes. Trust is meant to enable entities to deal with issues of uncertainty and uncontrollability caused by the free will of movement among nodes. An untrustworthy node in a MANET can wreck so much havoc and adversely affect the reliability, quality and integrity of data. This is why analysing the level of trust of a node has an influence on the confidence with which an entity makes transactions with that particular node.

2.3.1 Trust Properties

Trust [17] has the following properties:

a) Asymmetric: In ad-hoc networks, trust is regarded as asymmetric [1] and this means nodes having low capability may trust nodes with high capability but it does not mean that this must reciprocate when taken the other way round.

b) Subjective: In ad hoc networks, trust is subjective. The nature of MANETs in relation to the dynamic topology and experiences with the node and the different level of trust is determined by the trustor against the same trustee node.

c) Context Dependant: In ad hoc networks, the type trust desired is dependent on the task at hand i.e. trust is high capability, trust is computational power and trust is reporting.

d) Dynamic: Just like MANETs, trust changes dynamically and frequently. Trust in MANET is not static but dynamic. Due to the dynamic topology, information is either be incomplete or worse of all changed. In order to capture the dynamic nature of trust, trust should be expressed as a continuous variable and that is in binary form or even discrete valued entity which represent certainty.

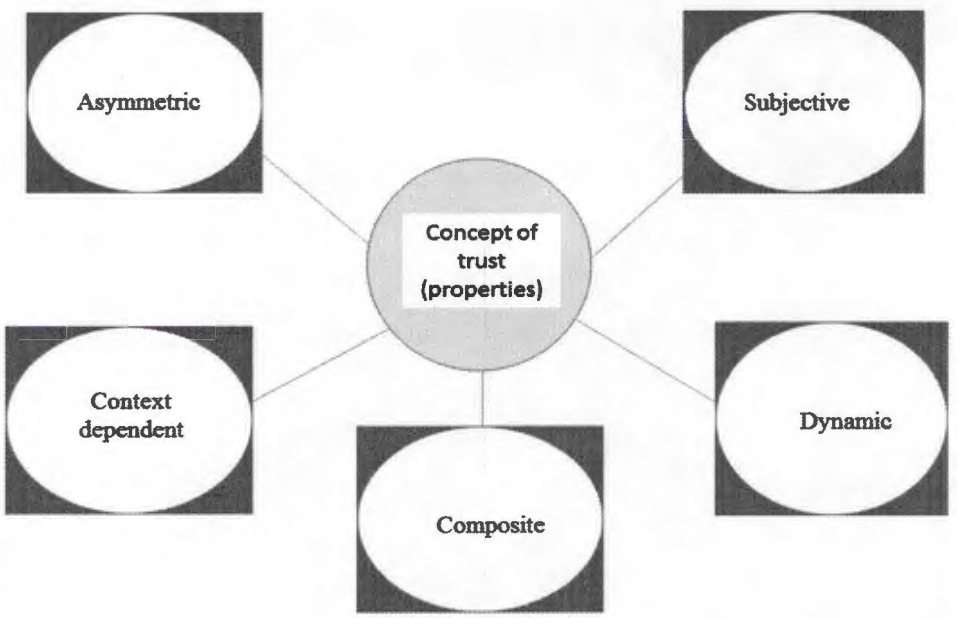

Figure 2.1 Properties of Trust

2.3.2 Trust and QoS

Trust and QoS have almost similar metrics in order to evaluate their efficiency. There have been different approaches to define trust. Trust [18], in general, is meant to be a bi-directional relationship among two entities and plays a huge role in the formation of a relationship with the network. Even though trust has been formalized as a computational model, it is dynamically applied in the different research communities. QoS [8] in MANETs is a globally growing area of interest. Due to rapid expansion of multimedia technology, mobile technology and real time applications like video streaming are strongly compelled to support QoS and metrics considered are ones such as throughput, delay, energy consumption, jitter etc.

Trust and QoS share similar metrics e.g. delay, throughput and packet dropping rate. The correlation between these concepts exists not only through shared performance metrics but also the assurance of good service in the network for the end user.

QoS and Trust are what stand between the network and the Applications/Users. It is not easy to provide QoS support without having the right QoS requirements. A particular level of trust must be established and that is, only trustworthy nodes that perform well will participate. Trust is dynamic [17] just like MANETs which have an ever changing topology state. This means that the trust value should be based on temporary and yet local information. In addition to this, the trust value is different for similar nodes. This is influenced by the fact that each node goes through different situations in terms of the dynamic topology.

Trust is mostly evaluated through a theoretically whilst QoS is of a quantitative measure. As such, the two have one thing in common and that is to rate performance in networks. These concepts put together in a framework would yield good results and that is what our framework seeks to achieve.

2.3.4 Trust Management Frameworks

Trust remains a relevant subject within the research field and continues to attract interest from network analysts and developers. The notion of using trust to eradicate security problems in networks has also been relevant too in the research field.

Authors in [19] proposed a recommendation based framework with a defense scheme, which uses a clustering technique to dynamically remove attacks related to untrustworthy recommendations in-between a specific time based on historic interactions, integrity and compatibility of data and distance among the nodes. Their framework was practically tested under several mobile and inactive topologies

in which nodes experienced changes in their neighbourhood leading to frequent route changes. The conducted analysis demonstrated robustness and efficiency of the framework in a dynamic ad-hoc network environment. The results, however, cannot be validated in an experimental process since the framework is based on recommendations.

According authors in [20], a trust model which is Fuzzy Petri-based, was presented to evaluate trustworthiness in the network. Their model proposed a trust-based routing algorithm to select a path having the highest path trust value among all available routes between any two nodes in a network. Furthermore, its correctness was validated. OLSR was then modified to be PFNT-OLSR by applying the proposed trust model and trust-based routing algorithm. In order to implement PFNT-OLSR, a feasible trust factor collection method and a reliable trust information propagation method were created. Moreover, the simulation tool MoSim program was designed for the implementation of OLSR based protocols under Matlab environment

In [21], a Trust Based Secure On Demand Routing Protocol called "TSDRP" was proposed. AODV routing protocol was modified to implement TSDRP. The intention was to make it secure to thwart attacks like the Black hole attack and DoS attack. To evaluate the performances, the Packet Delivery Fraction (PDF) was taken into consideration as well as metrics like Average Throughput and Normalized Routing Load (NRL). The proposed TSDRP was meant to be a robust, secure on-demand routing protocol that enables the secure route discovery and maintenance in MANET. The authors then compared performances of TSDRP with that of AODV with respect to different performance metrics. The simulation study was carried out under various scenarios and after observation of performance analysis, it was concluded that in case of blackhole attack and DoS attack TSDRP performed very well in almost all parameters.

Authors in [22] presented a Meta-model (TrustFraMM) derived from trust based on available categorizations and surveys. They collected key components already identified within Trust Management and created a generally applicable meta-model, which aimed at creating the common ground for future trust research in computer science. Their model was a hybrid framework derived from other existing frameworks and consisted of well-defined elements, procedures and relations. This process led to the identification of common implementations of their meta-model elements and to the definition of their interfaces. These elements in question aimed at supporting future research and system design. TrustFraMM was mainly intended to be open for amendment by researchers until it become a tool able to describe frameworks in perfect detail. This framework can be considered trial

and error which is open to so many incompatibilities since there was further experimentation conducted to fully validate and adopt the proposed model.

In [23], the authors found out that packet drop due to the dynamic change in network topology can reduce the network performance. In their study multicast routing was used because of its advantage to operate in different situations such as mobile environment, high node density and uncertain network topology, in order to achieve optimum performance. In this study, the impact of mobility models over the different multicast routing protocols under the different constraints was explored to provide a solution for reliable multicast communication over ad hoc networks.

In [24], the authors' new simulation tool is described which is used to tackle a decentralized MANET environment. The simulation is conducted in Matlab using a decentralizing algorithm. The paper includes a distributed algorithm for adaptive movement of nodes in MANETs to maintain the overall topology of the network. The proposed algorithm assumes the presence of a GPS receiver in each node so that every node is aware of the position of every other node. The simulation of the algorithm was conducted on a few synthetically generated network scenarios and the results thus obtained showed the effectiveness of the proposed algorithm. The main aim was to provide node movement in a randomised faction, where there is no involvement of a centralised controller. The network movement was to begin from a place, where all nodes are in position and are ready to go in a random manner to the destination. Going through other decentralized network approach algorithms, it was discovered that the calling mechanism is not appropriate if the front node which goes out of the network is allowed to stop and wait for other nodes to approach there. According to the authors, the problem was totally eliminated in the proposed algorithm. Also, when the number of nodes increased, the complexity depended only on the number of nodes surrounding a single node. The movement of nodes implemented, follows Brownian motion and the whole movement was plotted. This validated the algorithm on node movement.

2.3.5 Direct Trust

Direct Trust according to author [25] is a phenomenon based on the experiences one node makes directly with another node. Consequently, trust values are computed by taking the mean or weighted mean of past experiences. Direct trust is application-centric or rather specific. The application has the ability to determine whether an interaction made from one entity to another was successful. Direct trust was chosen based on the merit that it is reliable in terms of rankings from confidence trust and reputation[25]. On middleware level, which in this case is the application server, the reliability of one

node in a distributed system can be computed through observation of the message flow. The Delayed-Ack mechanism came on board and was later modified in effort in order to improve network performance. We assume that in this work, the direct trust value is already calculated by one of the metrics mentioned above.

Direct trust: In this selection metric, only direct trust is applied as selection metric. A normal mean metric is chosen as trust metric.

2.4 Topology-constraints in MANETs

A trustworthy network topology [1] must be guaranteed through the use of robust routing protocols in the ad-hoc networking stream. The protocols are required because of the frequent routing updates caused by the dynamic nature and characteristics existing in MANETs. Providing QoS at a better scale in such environments is a huge challenge [4]. The existing stochastic nature of communications quality in a MANET exhibits challenges in offering concrete guarantees on the applications computed in mobile devices. An adaptive QoS must be implemented coupled with a strong trust relationship framework over the traditional resource reservation to support multimedia streaming services. Since the topology of the network is constantly changing, the issue of routing packets between pairs of nodes poses a great problem. One may argue that most protocols should at least be based on reactivity instead of proactivity because of this problem. Multi cast routing poses a challenge too because the multi cast tree ceases to be static since nodes in the network move randomly. The routes between nodes often have multiple hops and that is too complex than the single hop communication.

In MANETs[4],the nodes are mobile and this feature could result in nodes getting out of range within the network. This causes frequent loss of links between nodes and because of this it is one general norm that mobility of all contributes to [7] the additional dynamic nature to the network infrastructure. When nodes are in motion, the state of existing node links are most susceptible to change, or possibly breaks. Re-routing is an alternative to routes that are broken.

2.5 Video Streaming Applications

Video streaming is a client server paradigm where interactive media data of streaming applications such as video on demand, video conferencing, e-learning and many more. End-to-end Quality of Service (QoS) [6] provision to video-streaming applications over MANETs brings a complex and

challenging problem. This is because video steaming is considered delay sensitive and also bandwidth intensive.

In order to make video streams smaller, they are compressed using video coding formats. Examples of such formats include HEVC, VP8/9 or even H.264. The video streams are then assembled in a container (bit-streams) such as FLV and MP4. The bit-stream is transmitted from streaming serving to the client. An example of a client would be any computer user with internet connection.

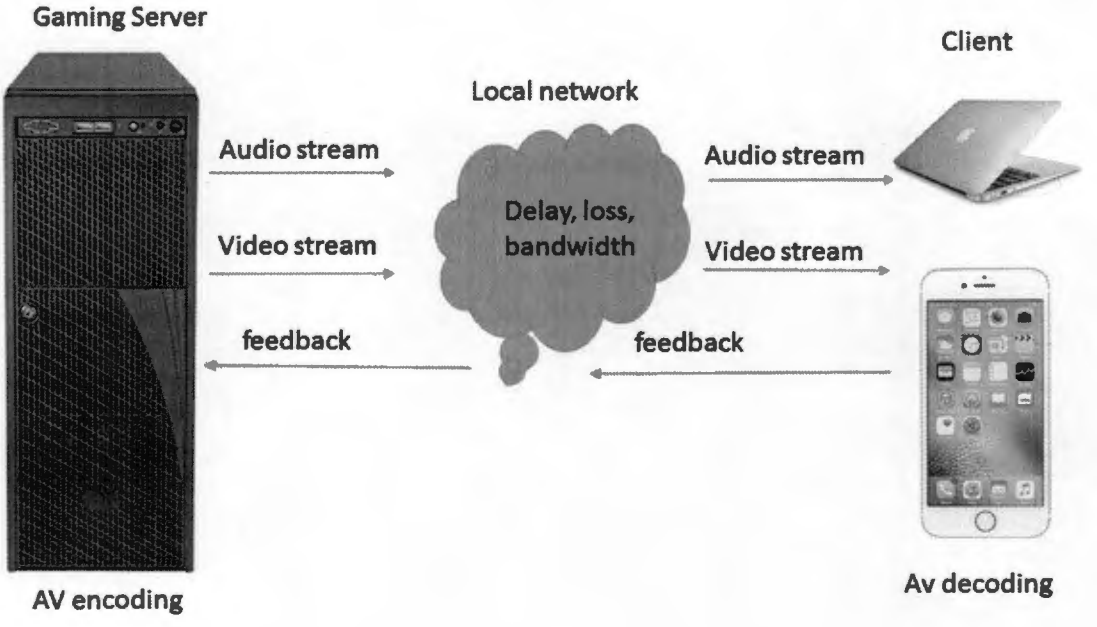

Figure 2.2 Typical Video Streaming

2.6 MANET Protocols

There are various protocols for the implementation of MANET use. Some are still being developed even today to try and meet the needs of the end user. The protocols are classified or rather categorised according to functionality and state at which they will be utilised. They are divide into two categories and that is; topology based protocols and position based protocols.

2.6.1 Topology Based Protocols

Topology based protocols can either be proactive, reactive or hybrid.

Table 2.1: Typical MANET Routing Protocols[26]

Proactive routing	Reactive routing	Hybrid routing
DSDV	AODV	GPSR
OLSR	S-AODV	GPSR-L
MOPR	PAODV	GPCR
GSR	DSR	GpsrJ+

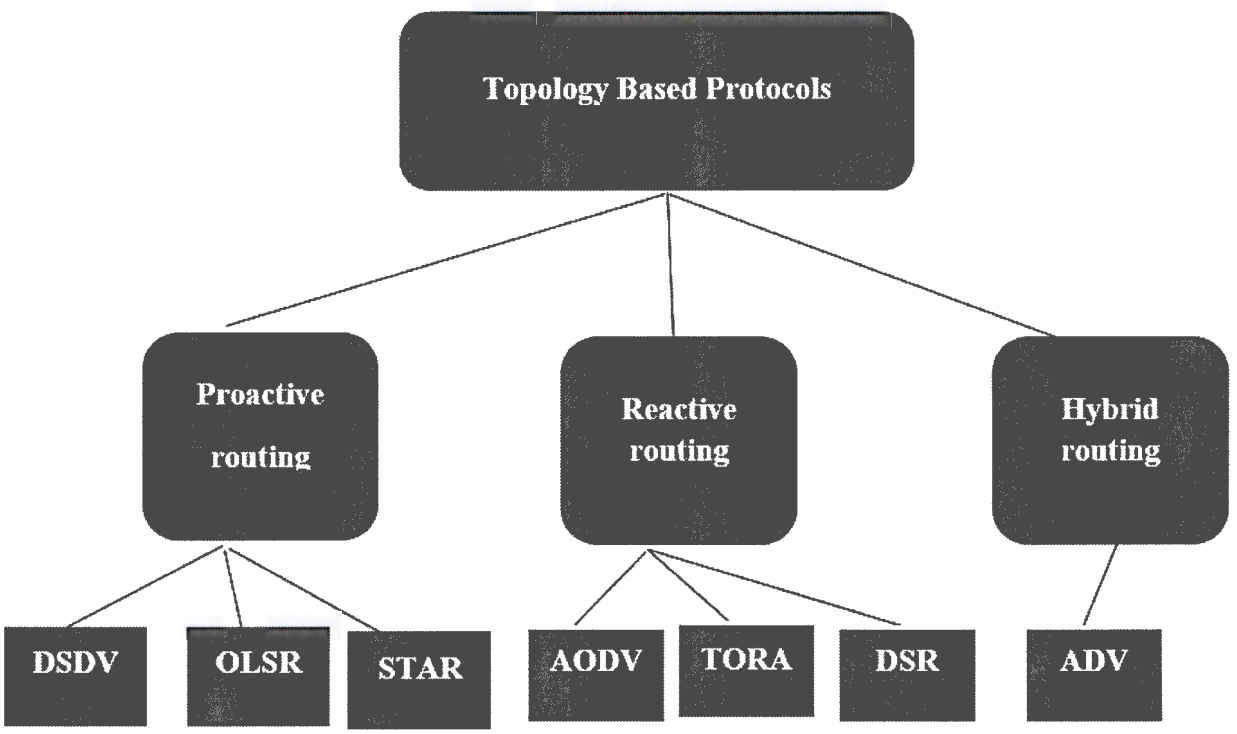

Figure 2.3 Classification of typical topology based protocols [27]

2.6.1 Proactive Protocols (Table-driven)

Proactive protocols utilize the recurrent trade of control messages among routers corroborating that the route to every host is always notable. This, according to Hamma *et al*, [28] table driven protocols need a high bandwidth overhead. Ad-hoc link state routing algorithm pursuits to sustain bandwidth by decreasing the size and the number of control messages[28]. Basu Dev Shivahare in 2012 [29] wrote that each station in the network has routing table for the broadcast of the data packets and that the node wants to establish connection to other nodes of the network. According to the author, these computers record for all the presented arrival points of end, number of hops required to arrive at each terminus in the routing table. The routing entry is then compartmentalized with a sequence number which is established by the terminus node. To retain the stability, each node broadcasts and alters its routing table timelessly [29].

Shouzhi Xu *et al* [26] wrote that proactive routing protocols tend to update routing information periodically, which perform comparatively in urban environments (with low mobility) but exhibits defective performance in highly mobile and dense scenarios when matched with reactive routing protocols[26]. This study looks at one proactive protocol called Optimized Link State Protocol (OLSR) in order to validate the study made in the year 2013.

2.6.2 Optimized Link State Routing (OLSR) Protocol

OLSR is an optimization of a pure link state protocol for mobile ad hoc networks. In the OLSR protocol, every station found in the network chooses a neighboring node set known as the multi-point relays (MPR), which rebroadcasts the packets in turn. To this end, neighboring nodes identified not found in the MPR set have the capability to only read and process the packets [26]. According to Saravanan and Vijayakuma [30], OLSR retains tracks in path finding table in direct to proffer a route if necessitated.

OLSR utilizes two types of the control messages: Hello and Topology Control (TC). Hello messages are implemented for getting the information concerning the link status and the host's neighbors[31].

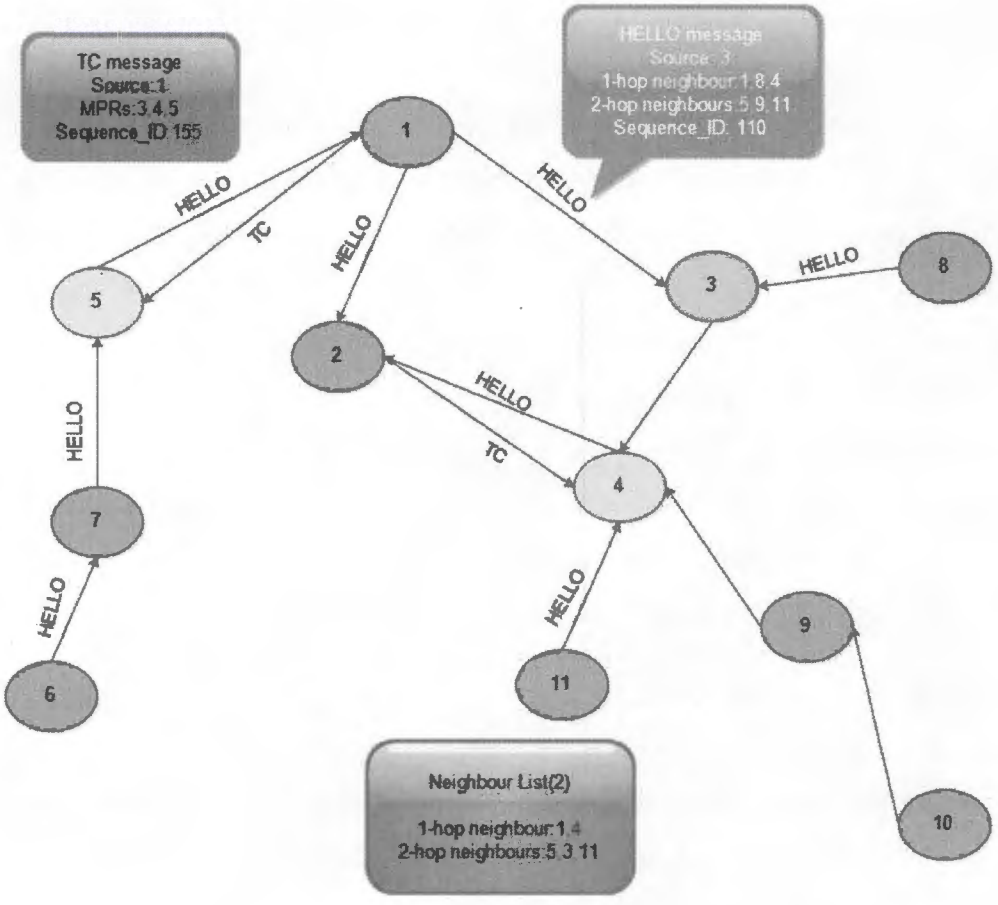

Figure 2.4 OLSR Workflow

2.6.3 Reactive Protocols (On-demand)

According to Salima Hamma *et al*, [28] reactive protocols routing, rather than depending on discovering routes as needed and recurrent broadcasts of available routes, build and maintain those routes. In this case, a route to every node is not known at any given time [28]. In essence, reactive routing opens the route only when it necessitates for a node to communicate. Additionally, reactive routing consists of route discovery phase in which the query packets are forced into the network for the path search and this phase finishes when route is found [26].

2.6.4 Dynamic Source Routing (DSR) Protocol

DSR is referred to as a reactive routing protocol. It starts route discovery only on demand like AODV. DSR keeps the entire path to destination in its routing table instead of next hop node unlike AODV. Packet header comprises of the address of all the transitional nodes to which the packet needs to move toward the destination node[32]. The Dynamic Source Routing (DSR) [27] allows nodes to dynamically uncover a source route across complex networks hop to any terminus in MANETs. Usop *et al* [33]wrote that DSR does not have mechanisms in identifying which route in the cache is stable, data packet is forwarded to a broken link. According to Singh *et al* [32] DSR implements three unique methods of control packets for path discovery and maintenance. They are route reply, route error and route request.

2.6.5 Ad-hoc On-Demand Distance Vector (AODV) Routing Protocol

AODV protocol is an on-demand and a table-driven protocol. It embraces flat routing tables with one entry per destination. It is in contrast to DSR, which can sustain numerous route cache entries for every one terminus [29]. AODV [33] surpasses DSR in high mobility environments, in areas where the topology changes rapidly and can adapt to the changes rapidly since it only maintain one route that is actively used. Authors in [33], compared AODV, DSDV and DSR protocols and they found that AODV performance is the best considering its ability to sustain connection by recurrent trade of information, which is required for TCP based traffic. It virtually dispatched all packets at low node mobility, while failing to converge as the mobility of nodes rises. On the other hand, DSR performed well at all mobility rates and movement speeds. The DSDV protocol was found to perform almost as well as DSR, but their study showed that it still required the transmission of many routing overhead packets. Furthermore, in higher rates of node mobility it was found to be actually more costly compared to DSR[33]. This experiment was conducted using an NS-2 Simulator. In this study it will be conducted on an OPNET 14.5 modeler.

According to Shivahare *et al* [29], for real time traffic, AODV is most favoured over DSR protocol because of its potential to sustain connections by recurrent trade of information, which is a strong compliance (requirement) for TCP based traffic [29]. Saravanan *et al* [30], mentioned that when comparing to the other protocols the AODV connection setup delay is very small but also mentioned that sometimes it will squander the bandwidth because of recurrent beaconing leads [30].

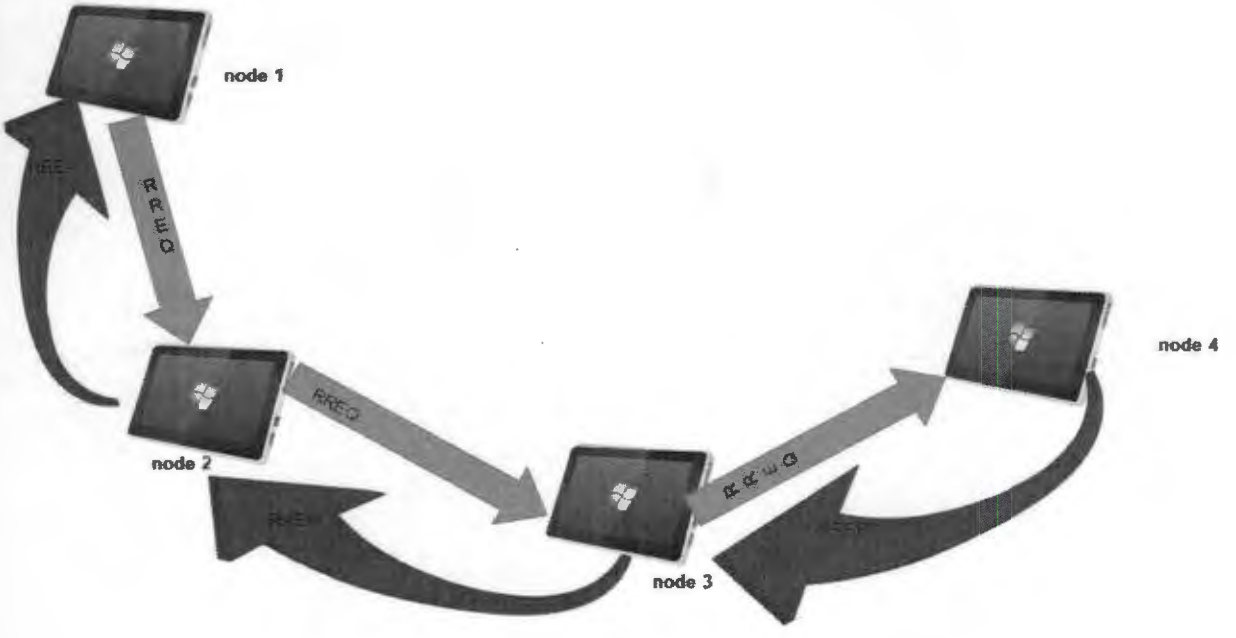

Figure 2.5 AODV Workflow

2.6.6: Temporally Ordered Routing Algorithm (TORA) Protocol

Temporally Ordered Routing Algorithm Protocol is referred to as a reactive routing protocol. TORA works on scaled control message propagation in the highly changing Ad-hoc networks. In TORA, the node clearly initiates a query when it needs to send the data to a destination. Qureshi and Abdullah, 2013 [27], stated that TORA has a performance that is much better as compared to that of DSR in a network. The author(s) suggest that the reason would be because of the protocol's ability to minimize the communication overhead when the topology changes and thus making it more reliable for changing Ad-hoc networks.

According to Palta and Goyal [31], a vital design concept of TORA is that control messages are localized to a small set of nodes nearby a topological change. Nodes retain routing data about their next one-hop neighbors. The protocol comprises of three basic functions: route creation, route maintenance, and route erasure. The main strength of the protocol is the way it handles the link failures. Effectively, each link reversal sequence searches for alternative routes to the destination [31].

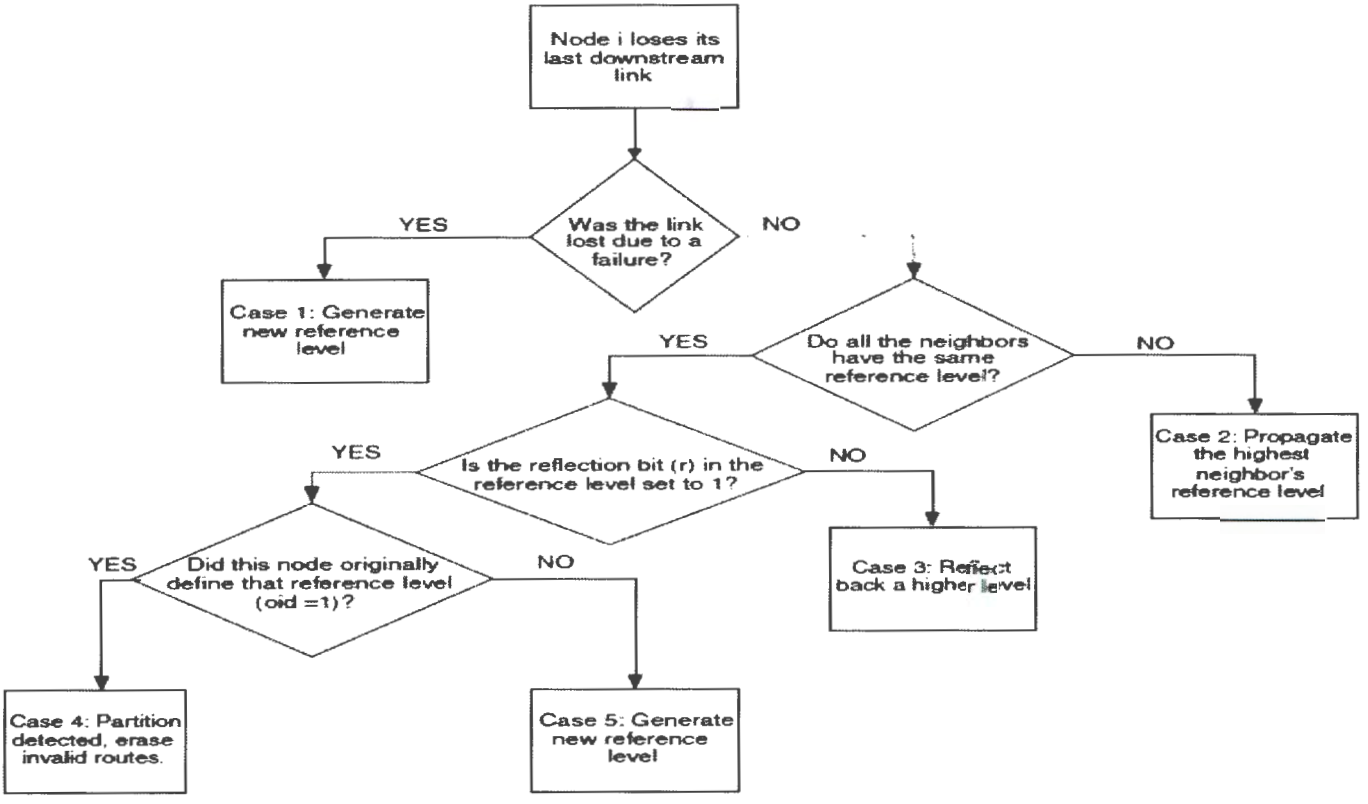

Figure 2.6 Route Maintenance in TORA[31]

CHAPTER 3

RESEARCH METHODOLOGY AND EXPERIMENTAL SETUP

3.1 Chapter Overview

The trustworthiness of a network depends on the quality of service being rendered within that network. Our framework involves the evaluation of QoS with optimum parameters set. The evaluation is done for low, mid and high node densities. The nodes move randomly and the end goal is the attainment of excellent QoS in the dynamic topological setup of the network itself. This chapter at first, defines the tool in terms of operations, functionality and evaluation process. The second part lays down the actual network model and scenario setups. OPNET provides a good application-centric evaluation system and such is fundamental towards the full realization of our framework.

3.2 Methodology

QoS and trust requires a quantitative measure and thus the decision to utilize a quantitative research approach for this work. Our framework is evaluated from the application interface side rather than the user interface. The applications' performance needs to be carefully analyzed as per measure.

3.2.1 Structure of OPNET

OPNET was created to have a user interface that assists the developer. OPNET is made up of an advanced level user interface, which is constructed from C and C++ source code blocks that has a large library of OPNET precise functions which meet various requirements of the developer. In order to fully stretch and extend the experience of this tool, OPNET is broken down into three main levels/domains. When a user or a researcher uses all three domains, it gives them the flexibility of constructing and implementing different scenarios logically.

The hierarchical structure of OPNET is divided to three related main domains:

a) Network domain

b) Node domain

c) Process domain

3.2.2 Network Domain

Hierarchically, the network domain is the outer/top-most domain that provides high level information of objects pertaining to a specific system, its nodes (fixed, satellite or even mobile) and subnets. As shown in figure 3.1, it depicts the magnitude of the entire network topology. It is also responsible for showing the geographical area of the objects and also how they connect and configure their data. The network model also shows mobility and chosen statistics for the network to be modeled.

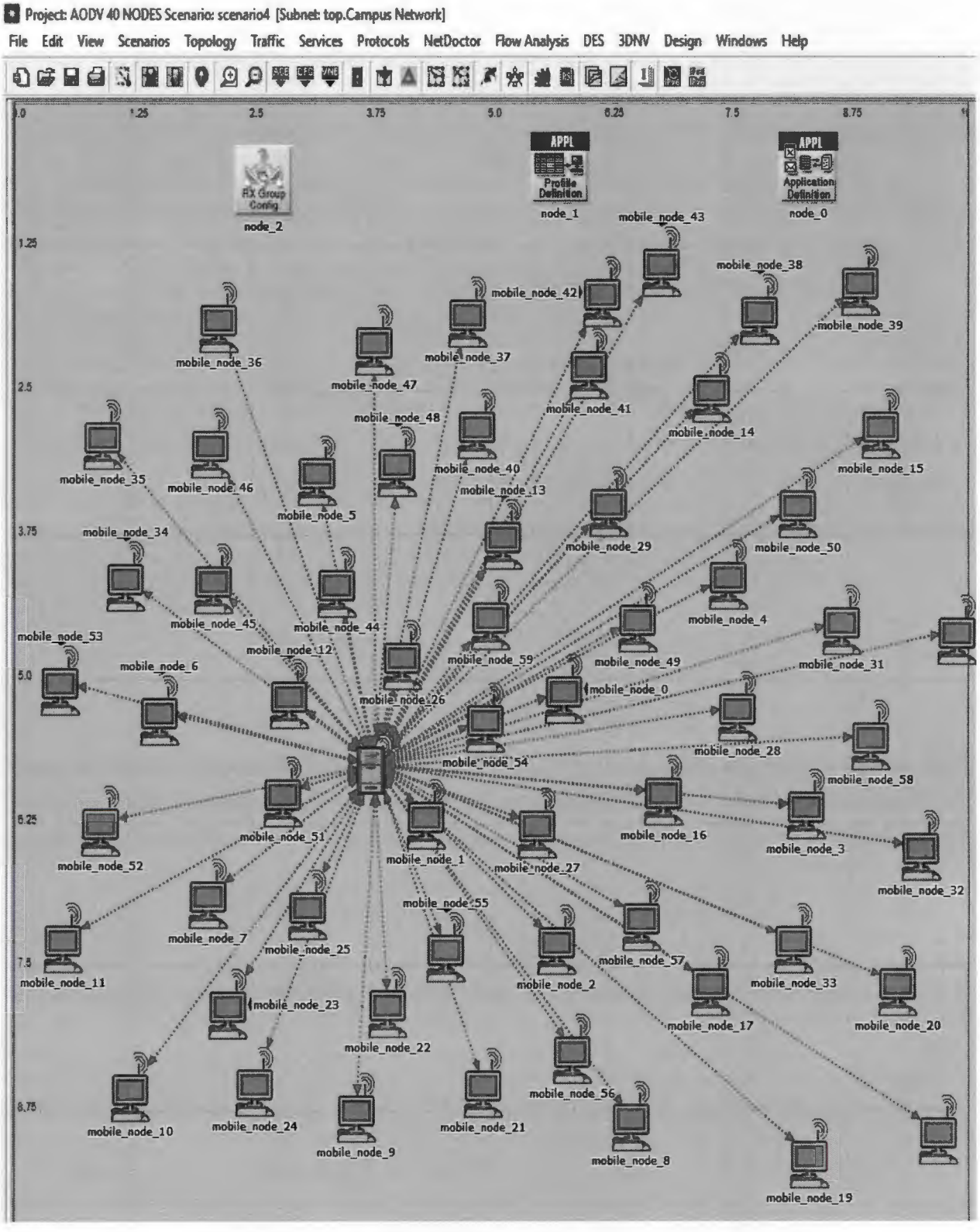

Figure 3.1 Network Domain

3.2.3 Node Domain

Hierarchically, the node domain remains the second outermost domain because it exists inside the network domain. It can be viewed inside the network domain. Objects included in this domain include routers, servers, workstations, satellite terminals and remote sensors. The node model is composed of connected blocks called modules. On each module, there is a set of inputs, outputs and memory state.

In node models as shown in figure 3.2, the outputs and inputs of various modules are all inter-connected through connections. There are two types of connections, one being packet stream and the other being stat wire. Packet stream is used to carry packets to and from one place to another and stat wire is used for the transmission of individual values. The OPNET simulator's Node Editor is used to view objects. The network editor is responsible for defining the behavior of each network object.

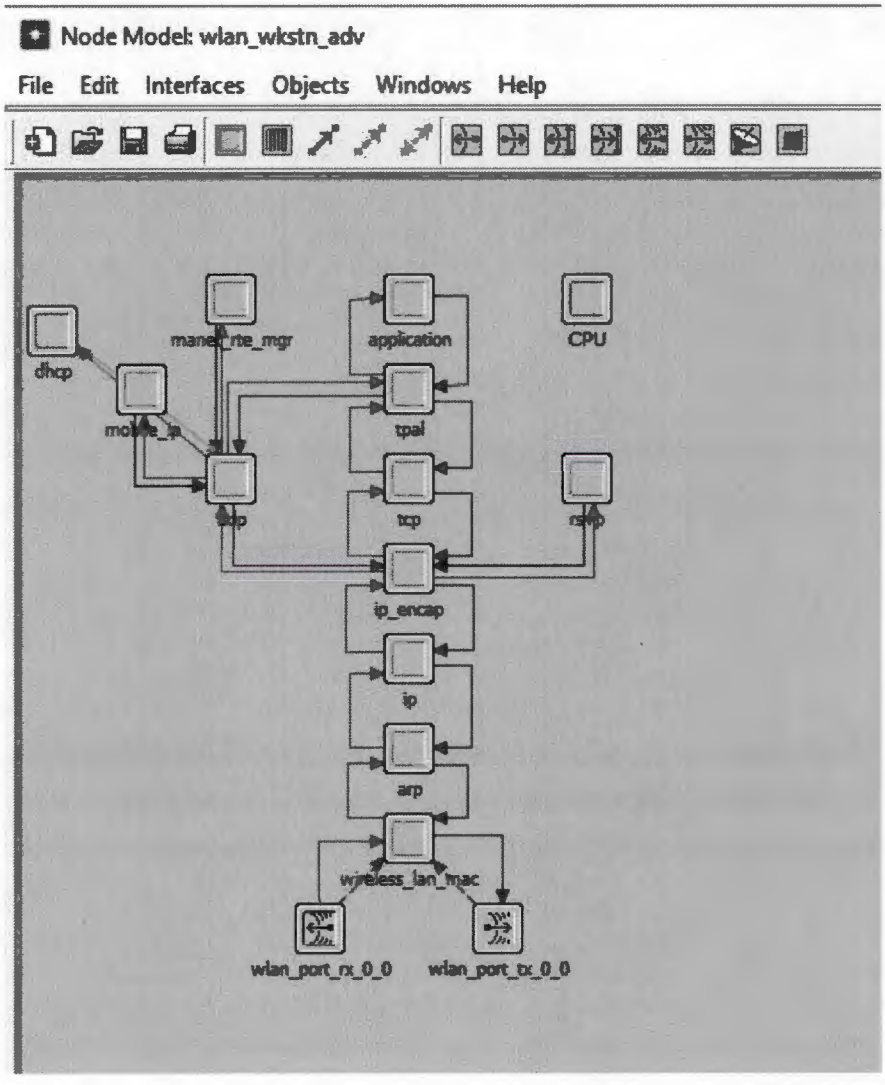

Figure 3.2 Node Model

3.2.4 Process Domain

The process domain as shown in figure 3.3 is responsible for defining the behaviors of queue modules and processors which are in the node domain. This in essence concludes that the process domain is inside the node domain. The process editor is used for the creation of process models. Process models are used for shared resources, algorithms, disks or memory, different software and hardware subsystems as well as operating systems. Process models control the functionality of node models which are created by the node editor.

The Process domain is further divide into two:

a) Process Model Operation: This part of the process domain describes the applications of process modelling of the features and construction.

b) Process Model Development: This part of the process model details the relevant steps involved in the creation of the process model.

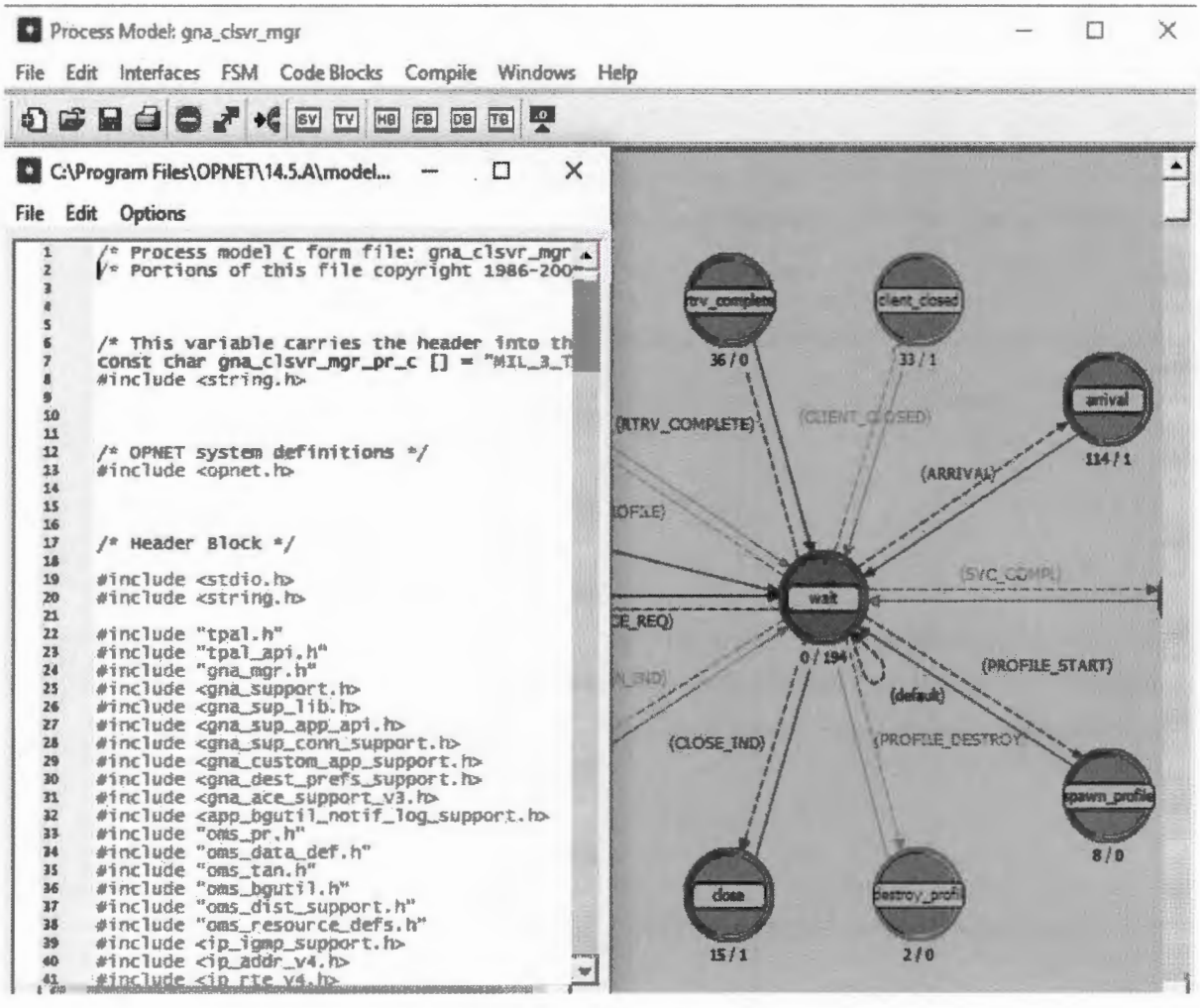

Figure 3.3 The Process Domain with source code

3.2.5 OPNET Modeler workflow

Fig 3.4 details on the workflow of the OPNET Modeler. The diagram shows the design and analysis of the implementation of the entire research study.

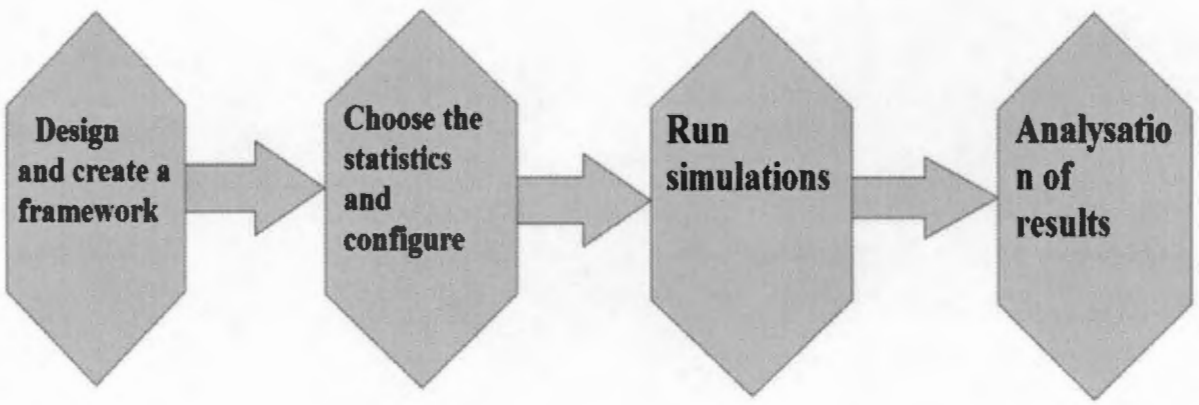

Figure 3.4 OPNET Modeler Workflow

3.2.6 Creating a Network Model

A network model is created in the network domain. There are a variety of ways of creating one. Here are a few examples in which they can be created:

a) Importing an existing network form from the scenario tab

b) By using the rapid configuration tool

c) By placing nodes taken from the object palette directly into the workspace.

After choosing which method to use for creating the network model, it all comes to choosing the traffic. The traffic too, can either be imported or manually specified. In this research work, the traffic was video conferencing traffic.

3.2.7 Choose statistics

Statistics are chosen just before the simulations run. Choosing statistics enables the user to fully customize attributes/statistics with respect to the research goal. It is a very important step because the simulated results will only exhibit the specified or rather desired statistics outcome.

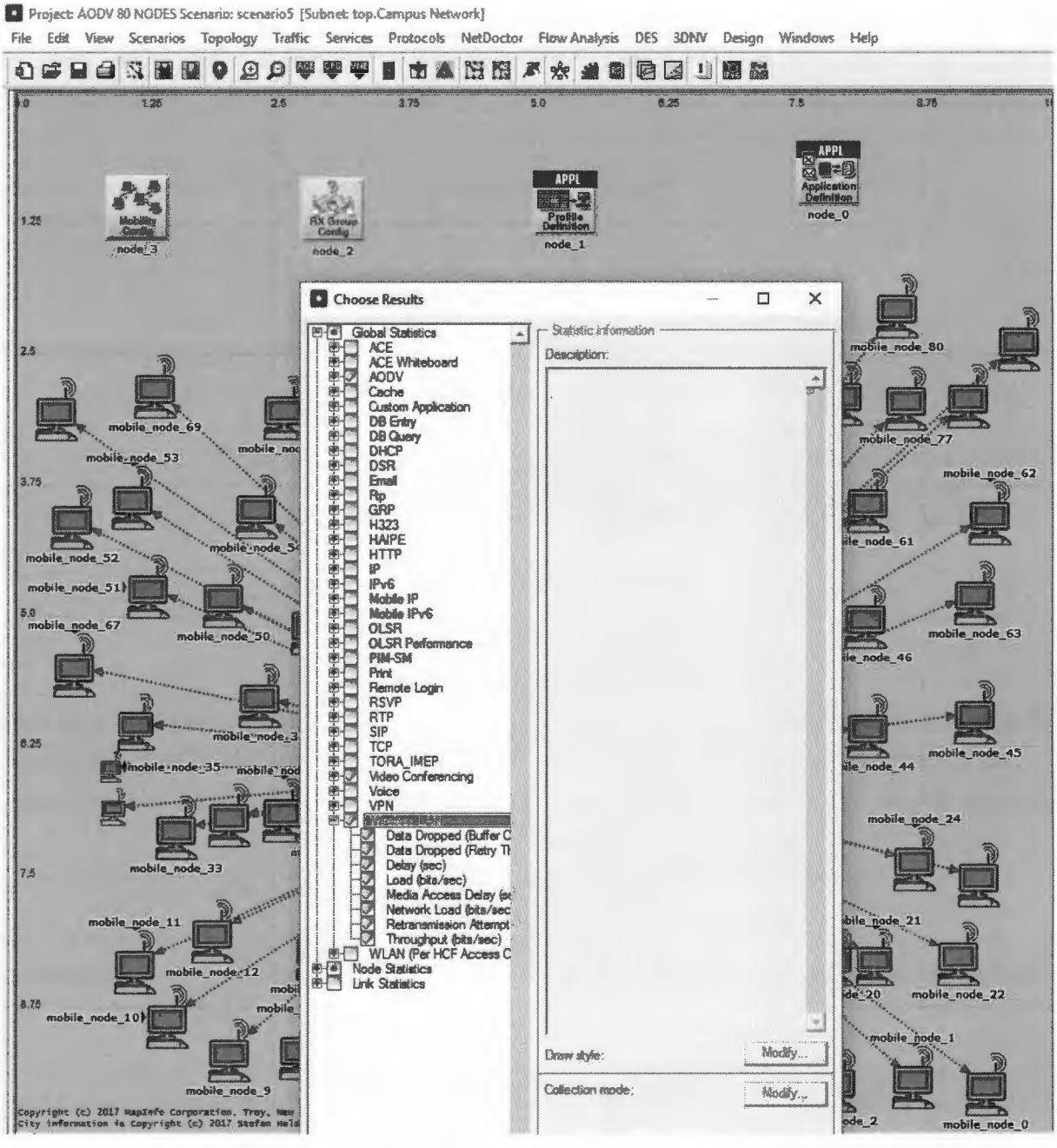

Figure 3.5 Choosing Global and Node statistics

3.2.8 Run Simulations

After choosing the statistics and making sure that all parameters are properly configured, the simulation was run. It is always advisable to run the simulation a number of times before coming up with results. This is done to guarantee the degree of correctness of the created network. The OPNET Modeler has many kinds of analyses that can be implemented:

a) Flow Analysis

b) Net Doctor Validation

c) Failure Impact Analysis

d) Discreet Event Simulation

Discrete Event Simulation is considered to be one of the best analytical approaches as compared to the other three methods of analysis. This is because it handles link roads, pair traffic and explicit traffic. One disadvantage it has is that it takes the longest time running unlike the others which generate results faster and answer specific types of questions.

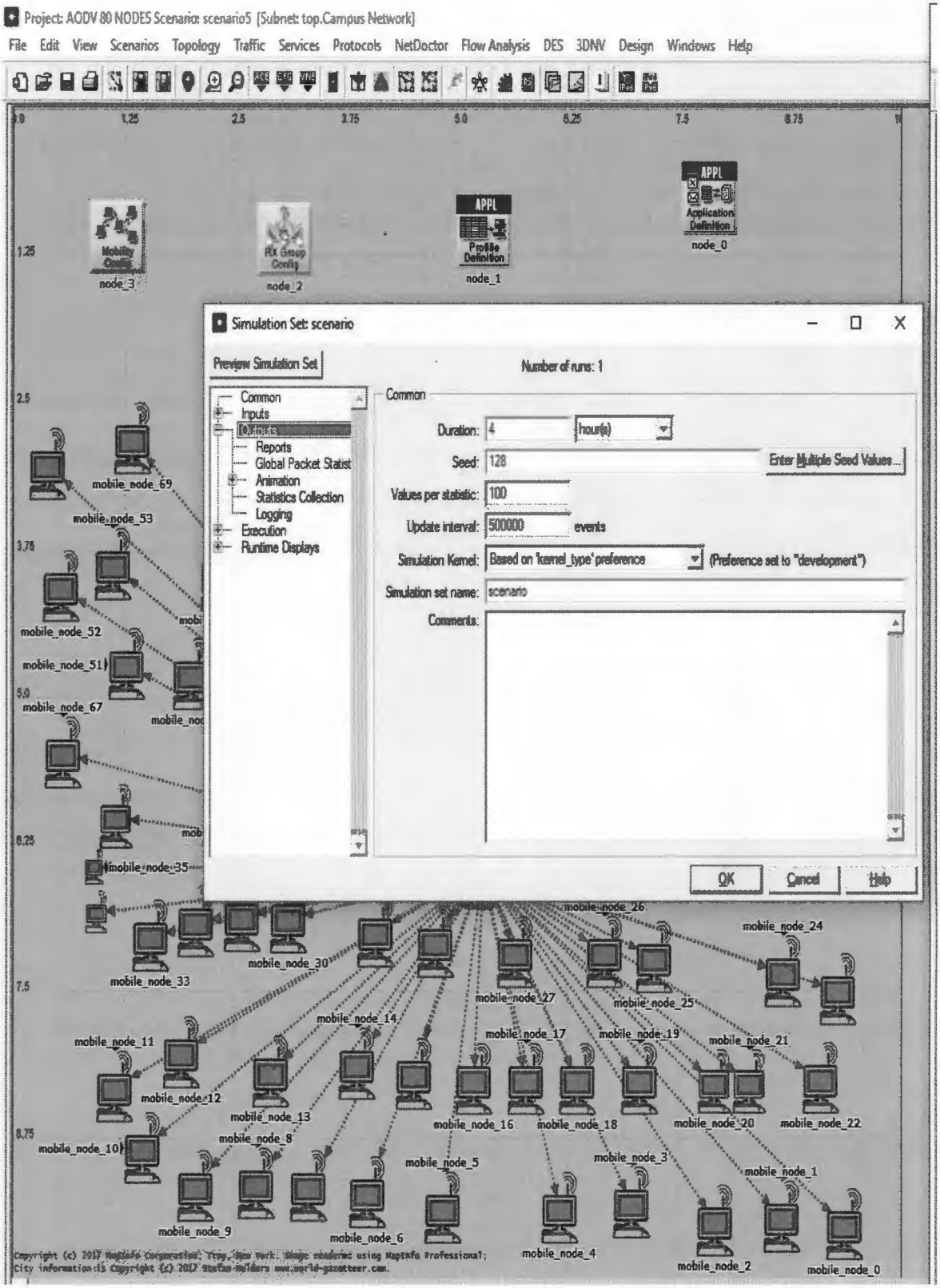

Figure 3.6 DES simulation scenario with number of runs

3.2.9 Results Analysis

This is the final stage of the simulation. Results are displayed from the Analysis tool (Projector Editor). Using this tool enables the extraction of data at user requests. This tool also allows the user to choose their customizations in terms of output and display of results in the various presentation schemes available. The figure below shows the results browser where the user can select which results are needed. Only required performance metrics can be selected. The beauty of the results browser comes with the science of actually linking your current project or even better, all the projects. The scenarios can be selected randomly and the graphs can be viewed as a collective or as a single project.

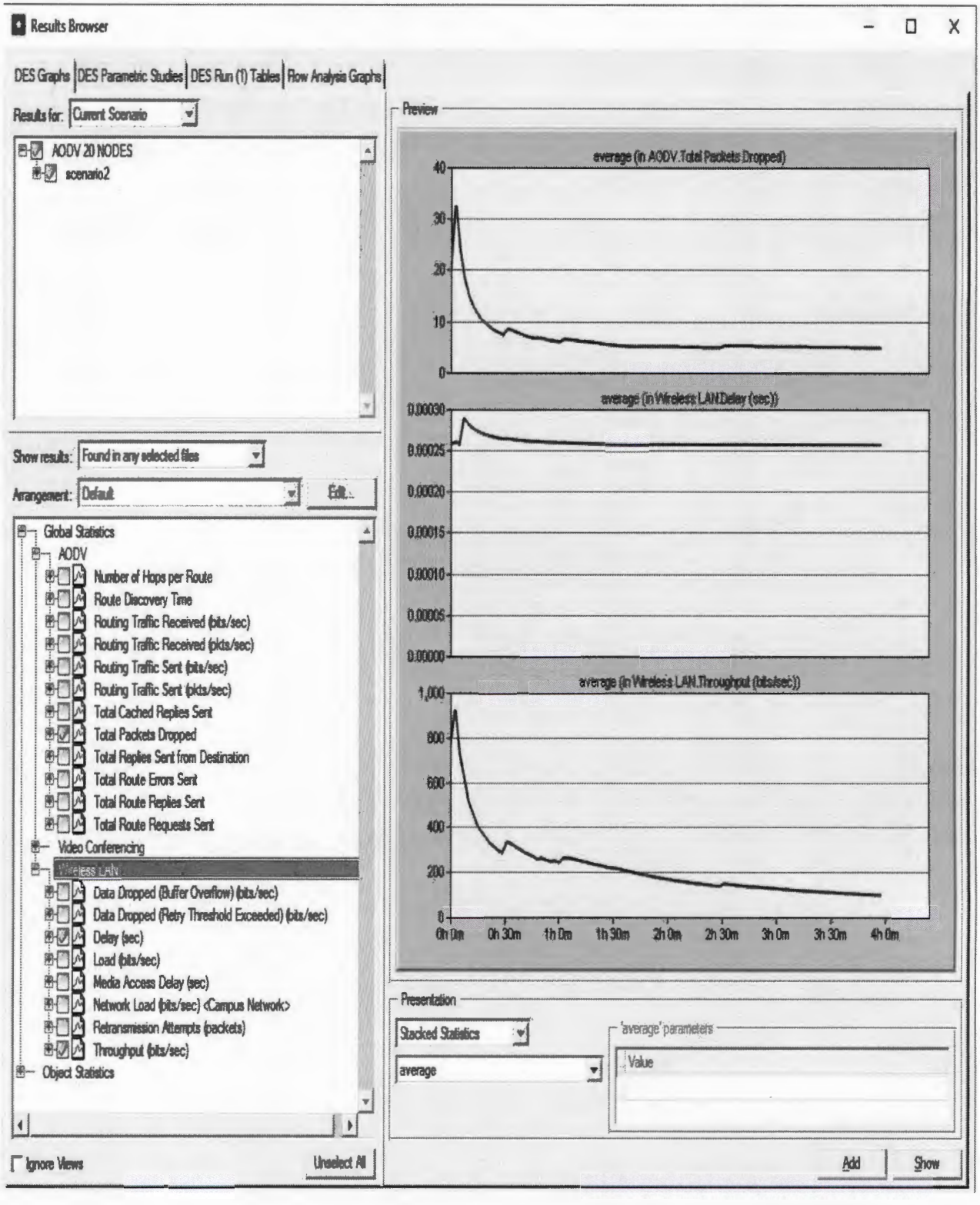

Figure 3.7 Results browser

3.3 Simulation Study

As stated in Chapter 1, the study focused on performance analysis of different routing protocols: AODV and OLSR. The protocols are simulated in a Campus/local area network. The evaluation of these protocols aids in the provision of QoS in terms of video conferencing. The UDP Protocol is used to generate traffic for all the nodes in all scenarios. For each protocol, two scenarios were implemented by varying the nodes from 20, 40, 60 and 80 nodes. The server was configured for Unicast type of broadcasting.

3.3.1 Network Model

As mentioned earlier, the study was conducted on a campus network. Different scenarios were put in place for the analysis. Figure 3.9 shows a scenario of 80 wireless mobile nodes simulated in an area of 10 by 10 kilometers. The network model looks similar for all protocols. The difference is the various scenarios. The network model and traffic flows do not depict the routing protocol implemented. As shown by the figure 3.9 below, the nodes have been configured to have a Random trajectory for all scenarios. The white line represents the trajectory for all nodes. By right clicking on it, the trajectories and node speeds can be altered in respect to each node in the network.

Figure 3.8 Network Model showing the Parent Subnet

The network is responsible for depicting networks, subnets, network topologies, mobility and geographical coordinates. Figure 3.8 above, shows the parent subnet at which the study was conducted. This subnet acts out as the parent subnet to which our networks are based. The subnet is configured to represent many scenarios and protocol configurations.

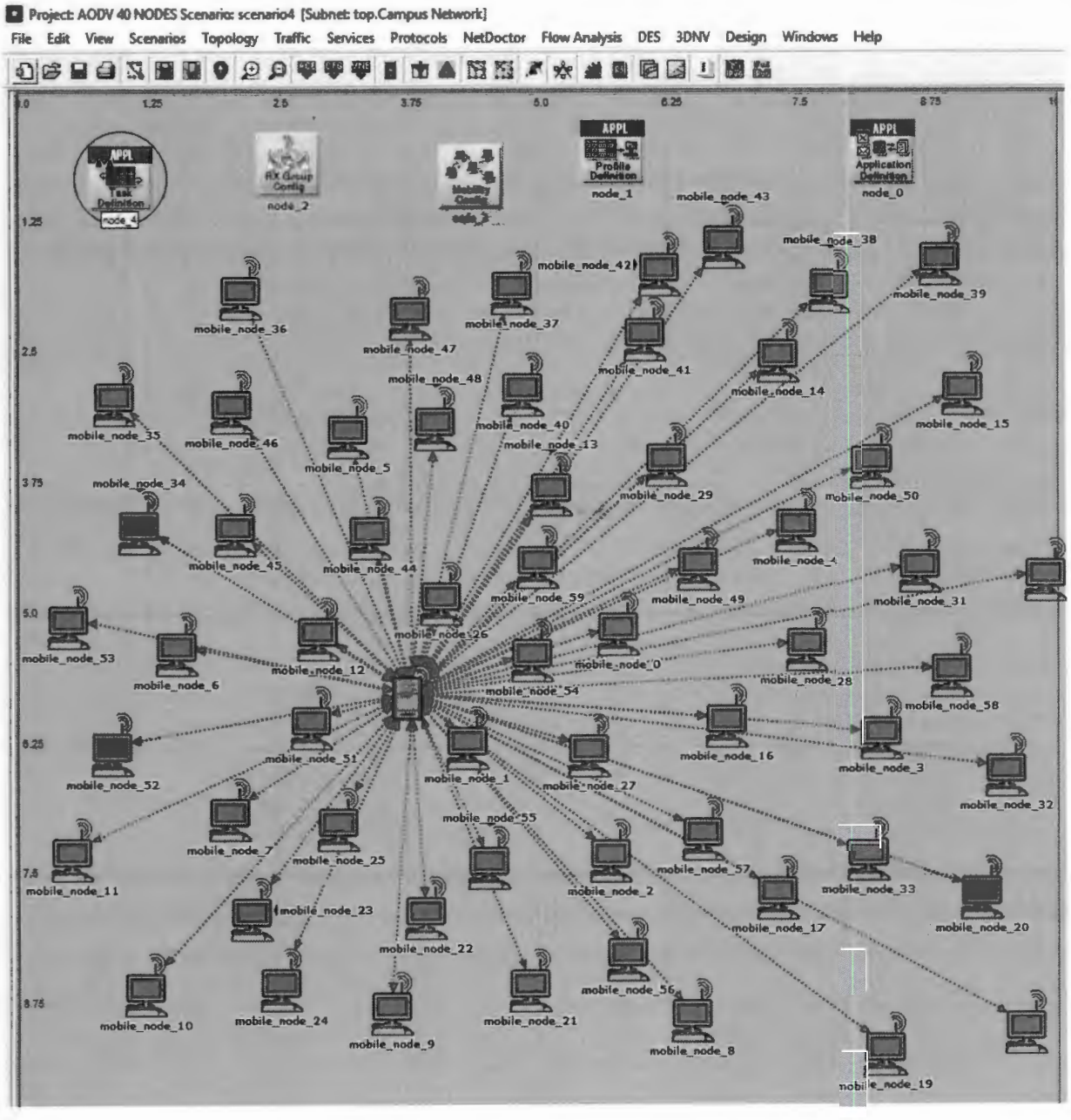

Figure 3.9 Network Model of 60 mobile nodes with QoS Attribute

Table 3. 1: Simulation Parameters

Parameters	**Values**
Simulator	OPNET 14.5 Modeler
Protocols studied	AODV and OLSR
Simulation Area	1000*1000 meters
Simulation Time	900seconds
Node movement model	Random Waypoint
Transmission range	300m
Traffic type	Video Conferencing-High Resolution
Transmission Rate	11Mbps
File size	1024 bytes
Type of Service in QoS	Streaming Multimedia
Trajectory	Random
Transport Protocol Used	UDP
Speed	30km/h

The network shown in figure 3.9 is made up many different components and configuration utilities namely;

a) A mobile wireless LAN server connecting to 50-100 wireless LAN nodes

b) Wireless LAN workstation nodes running over UDP/IP and supported by a WLAN connection at 11 Mbps.

c) Application Definition Configuration

d) Profile Configuration

e) Mobility Configuration

f) Dynamic Receiver Group Configuration

g) QoS Attribute

3.3.2 Configuration Utilities

It is imperative that specific configurations be implemented in order to ascertain efficient use of the OPNET Modeler. Some of those configurations include the application definition utility (for video conferencing), profile and dynamic receiver group Configurations.

3.3.3 Application Definition

This is normally the first step of configuration because it selects the application service to be rendered. This module contains the application definitions that mainly give description of how users employ applications in the Application configuration module. The modeler also provides preset configurations for FTP Application. In our study, we used the Video Conferencing Application as shown in Table 3.1. The preset video configurations include low resolution video, high resolution video and VCR quality video. Our study implements high resolution video which is more ideal for MANET scenarios.

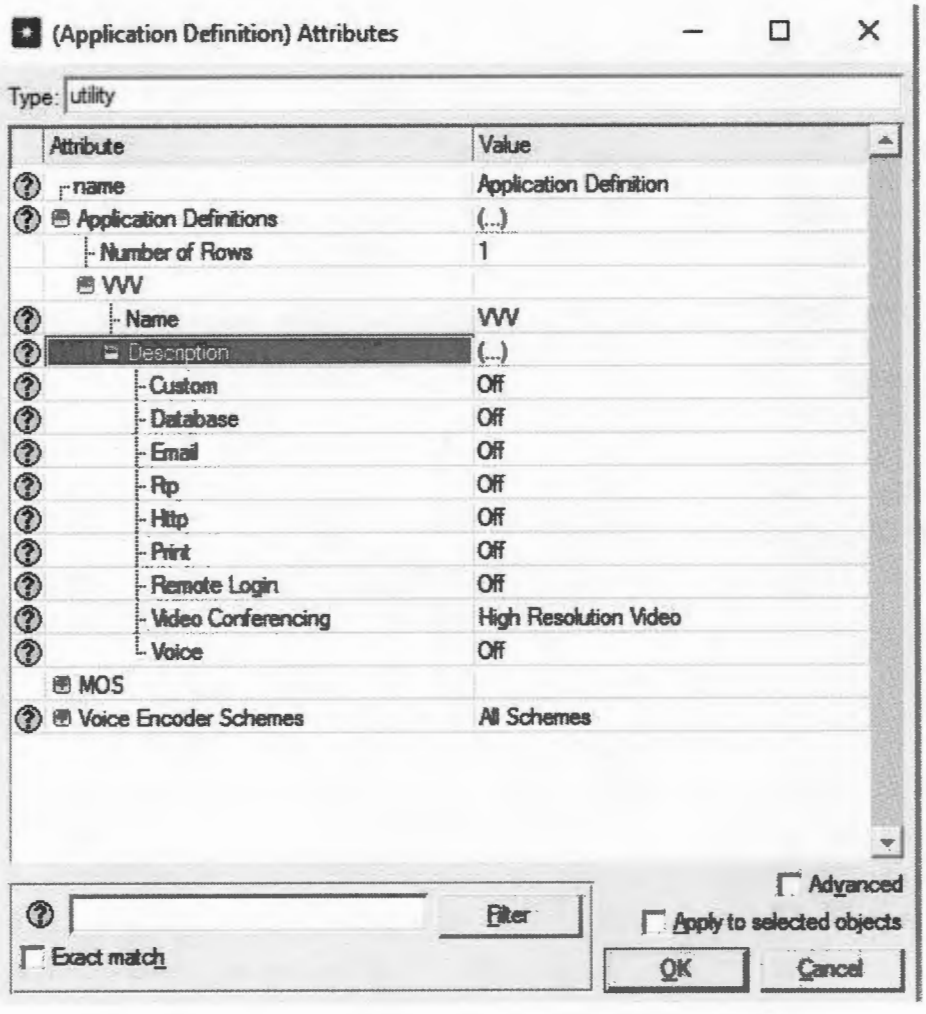

Figure 3.10 Application Definition

3.3.4 Profile Configurations

This utility mainly gives a description of how the selected application is used by end-users. The Profile configuration node is used to create user profiles. These user profiles can be specified on different nodes in the network to generate application layer traffic. The applications (in this case being video conferencing) defined in the application configuration utility are used by this object to configure the profiles. The application definition and profile definition configuration work hand-in-hand for the generation of traffic in the network. Figure 3.11 shows the profile used in one of our scenarios.

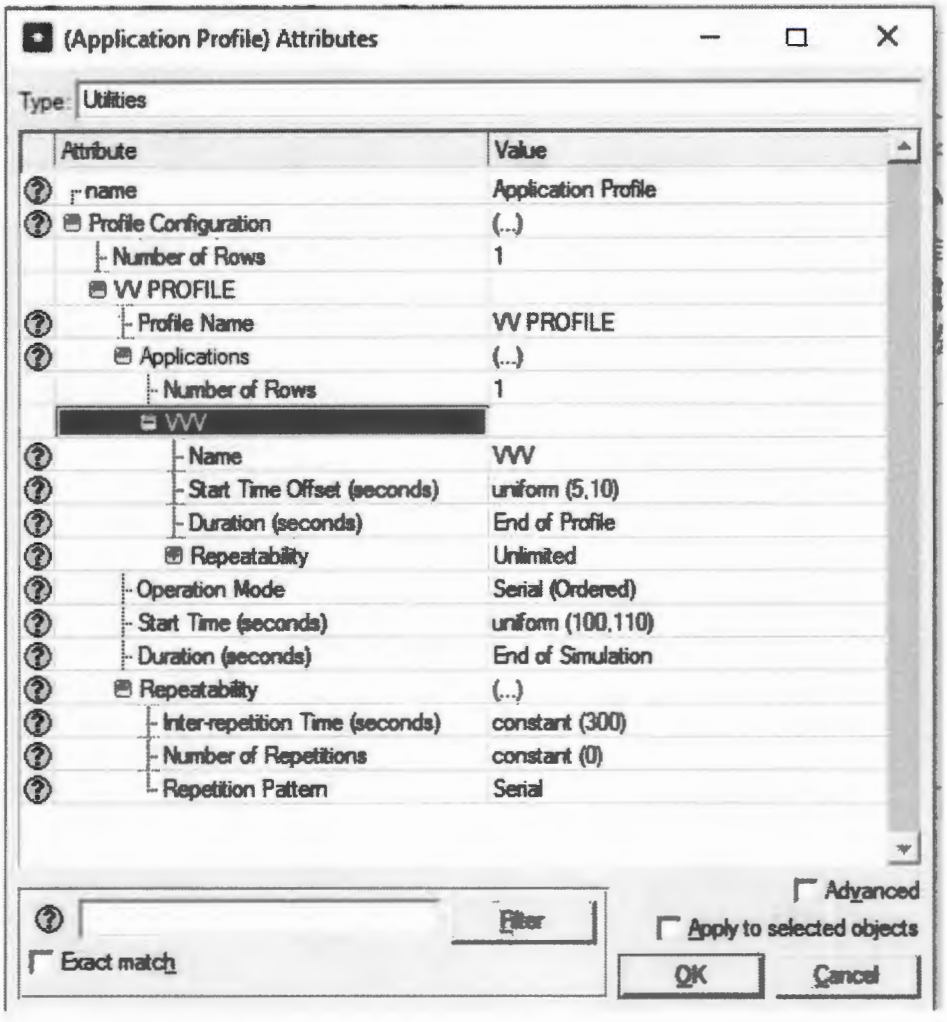

Figure 3.11 Profile Configuration

3.3.4 Mobility Configuration

This utility is used to define mobility profiles that individual nodes reference to the model mobility. In order to use this node, it is placed anywhere across the network model, define additional mobility profiles, if desired, and, finally, tag nodes that will run on a specific profile. In our study, all nodes used the Random Waypoint (Record Trajectory) profile as shown in Figure 3.12

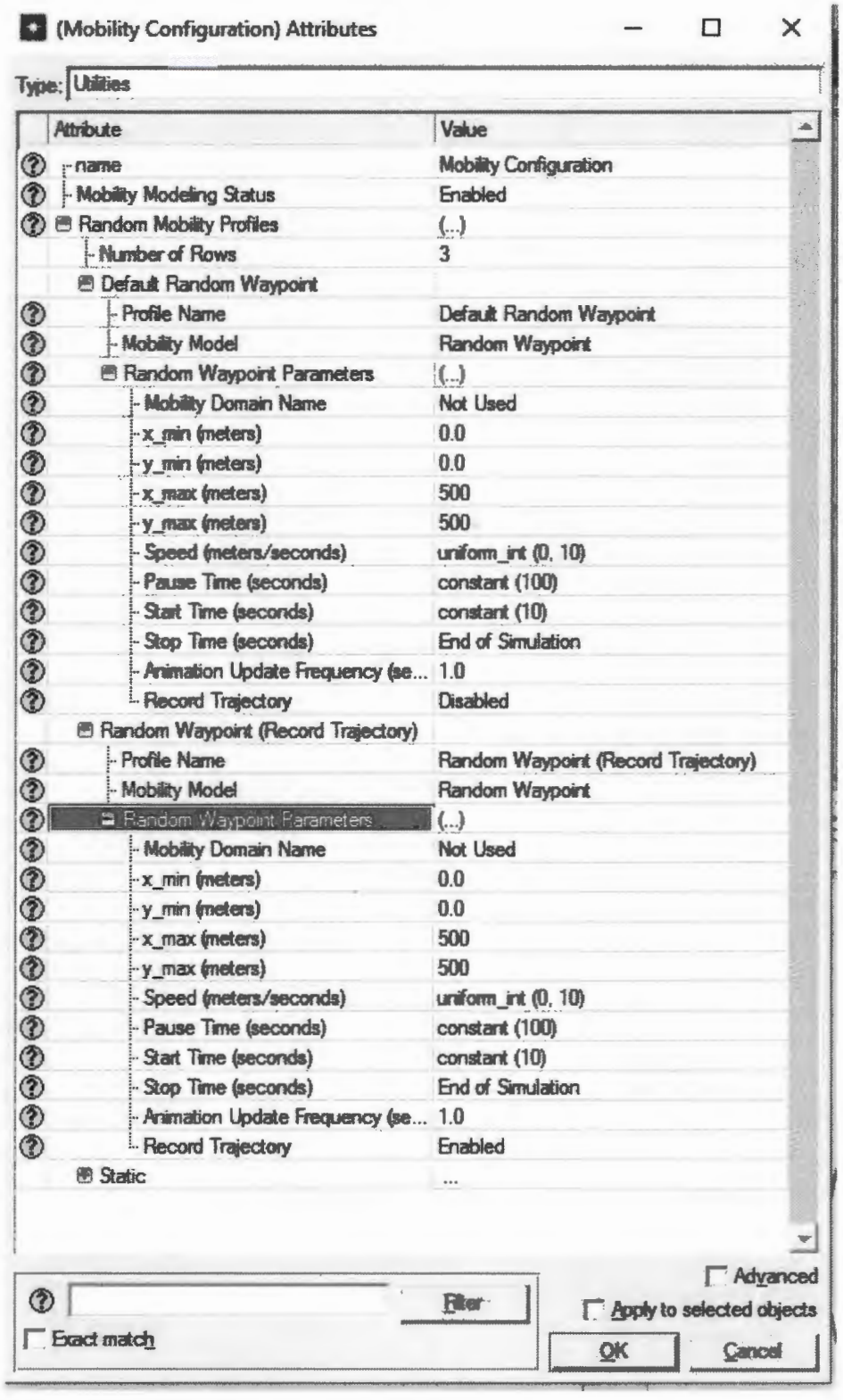

Figure 3.12 Mobility Configuration

3.3.5 Dynamic Receiver group Configuration

This utility is used to compute the set of possible receivers that a node can communicate with. It is done based on the following three criteria:

a) Path-loss Threshold

b) Distance Threshold

c) Channel watch

All possible receivers that have a channel match with the transmitter channel(s) and fall within the distance and path-loss threshold are receivers that a node can communicate with. This utility node greatly speeds up a simulation by eliminating receivers that do not match. In our study, was added to speed up simulation as stated previously and is configured to eliminate receivers that are over 1500 meters away. Figure 3.13 shows this node's attributes.

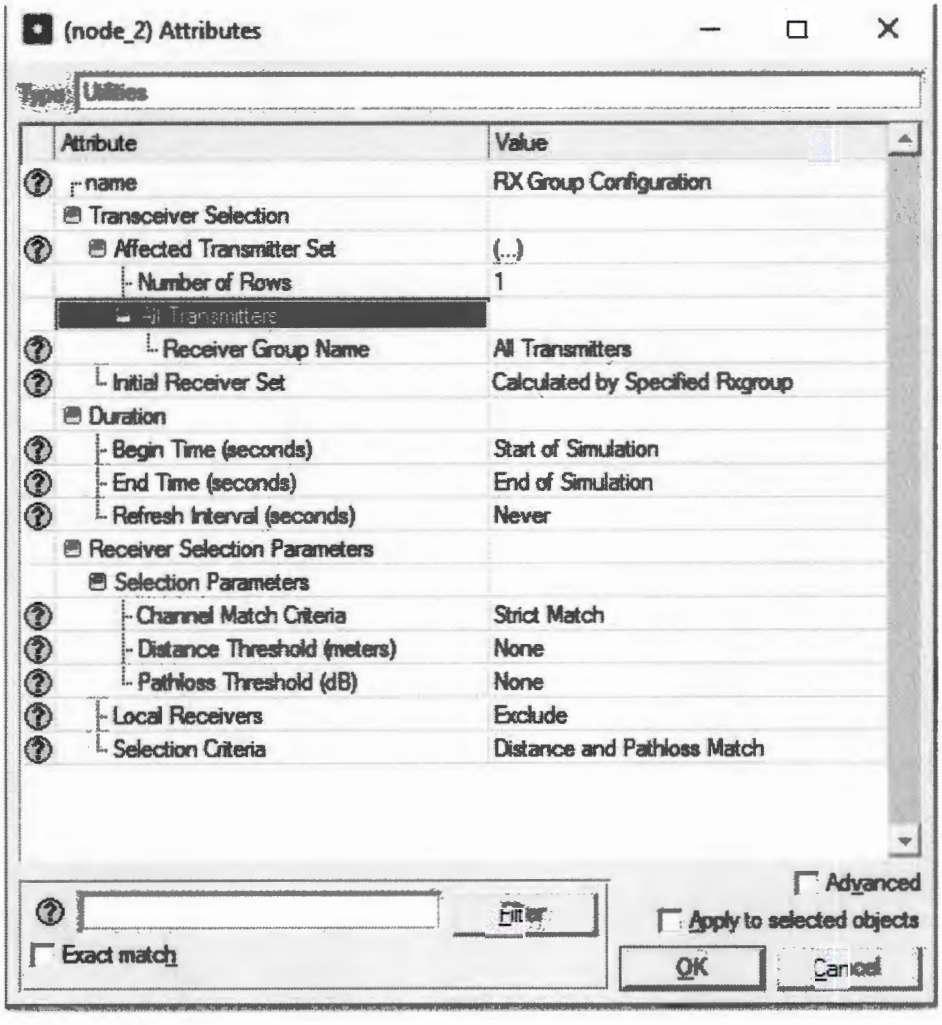

Figure 3.13 Dynamic Receiver Group Configuration

3.3.6 Mobile wireless LAN workstations

These stations represent a workstation with client-server applications running over TCP/IP and UD/IP. These workstations are meant to run video applications e.g. video conferencing. The station supports one underlying WLAN connection at 1Mbps, 2Mbps, 5.5Mbps, and 11Mbps.This study runs over UDP/IP at a connection of 11Mbps for both 50 and 100 node scenarios which is the highest data rate the tool can offer. The stations were independently configured. The figure (3.14) below shows editing of attributes of a node in a scenario being configured for OLSR protocol.

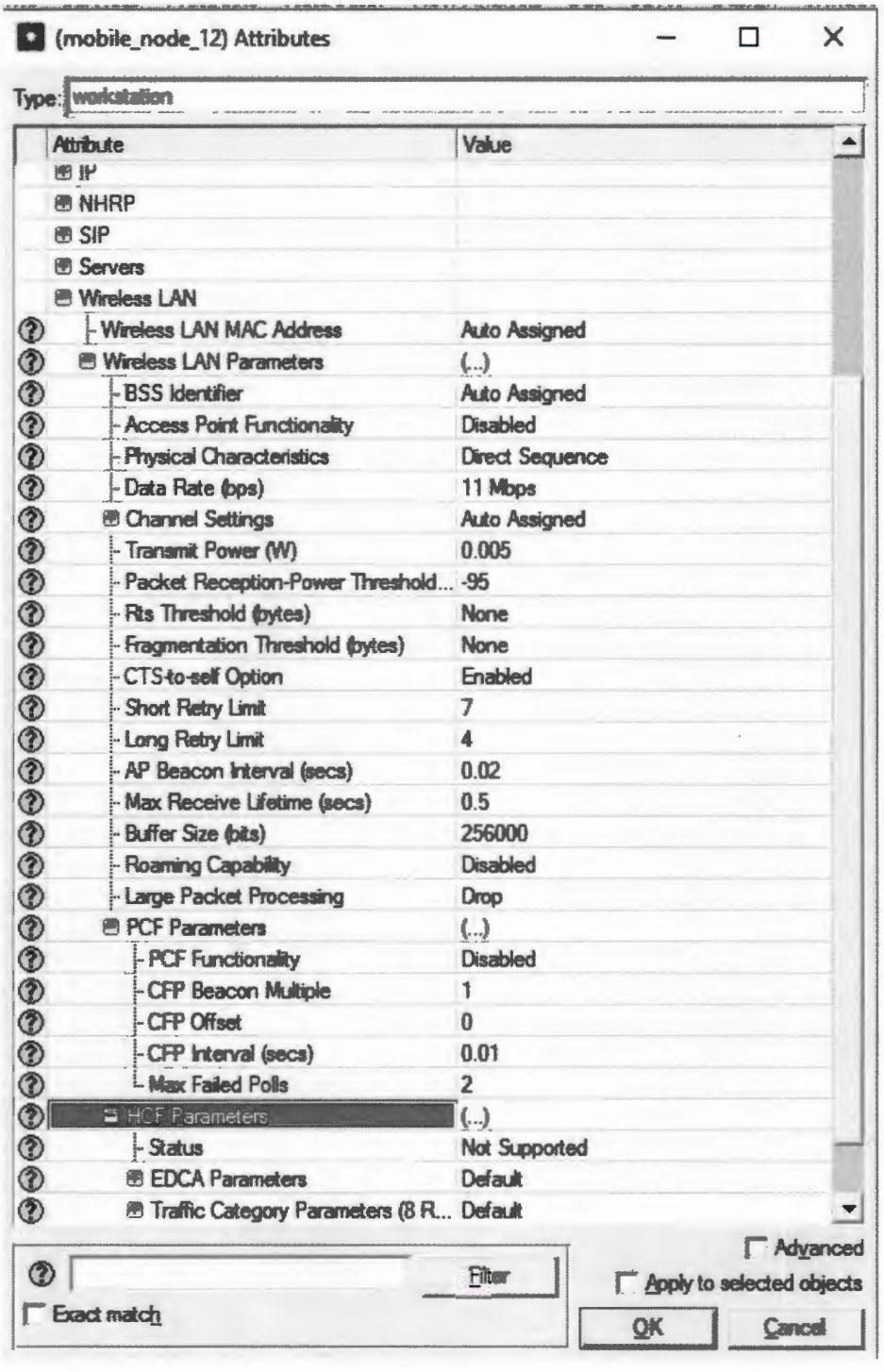

Figure 3.14 WLAN Parameters

3.3.7 Mobile wireless LAN server

The wireless LAN server model represents a server node with server applications running over TCP/IP and UDP/IP at supports one underlying IEEE 802.11 connection at 11Mbps. The operational speed is determined by the connected link's data. Server attributes are similar to workstation attributes but in the Application destination, preference is not set because the server acts as a source to the video application. The Application destination preference is set in all the nodes in the network awaiting to receive an application service.

3.3.8 QoS Configuration

The configuration of Quality of Service refers to manageability mechanisms for resource reservation. QoS in essence refers to traffic control mechanisms that seek to differentiate performance and that being based on application or network operator requirements and also provide predictable or guaranteed performance to applications sessions as well. The network's ability to guarantee QoS depends on the way in which the source generates cells and it is important to take note of the availability of network resources i.e. bandwidth. The cells can either be uniform or in a burst(y) way. For an example, such as in video application, it requires a precise level of end-to-end QoS parameters. These are set in order to ascertain improvement in terms of bandwidth in a network. All running applications should have a managed quality of service. Figure 3.15 shows QoS configurations including the ToS and profile schemes. The selected Type of Service in the figure is called Best Effort. Best effort service is implemented to say all users obtain unspecified delivery time and variable bit rate, all that depending on the current traffic load.

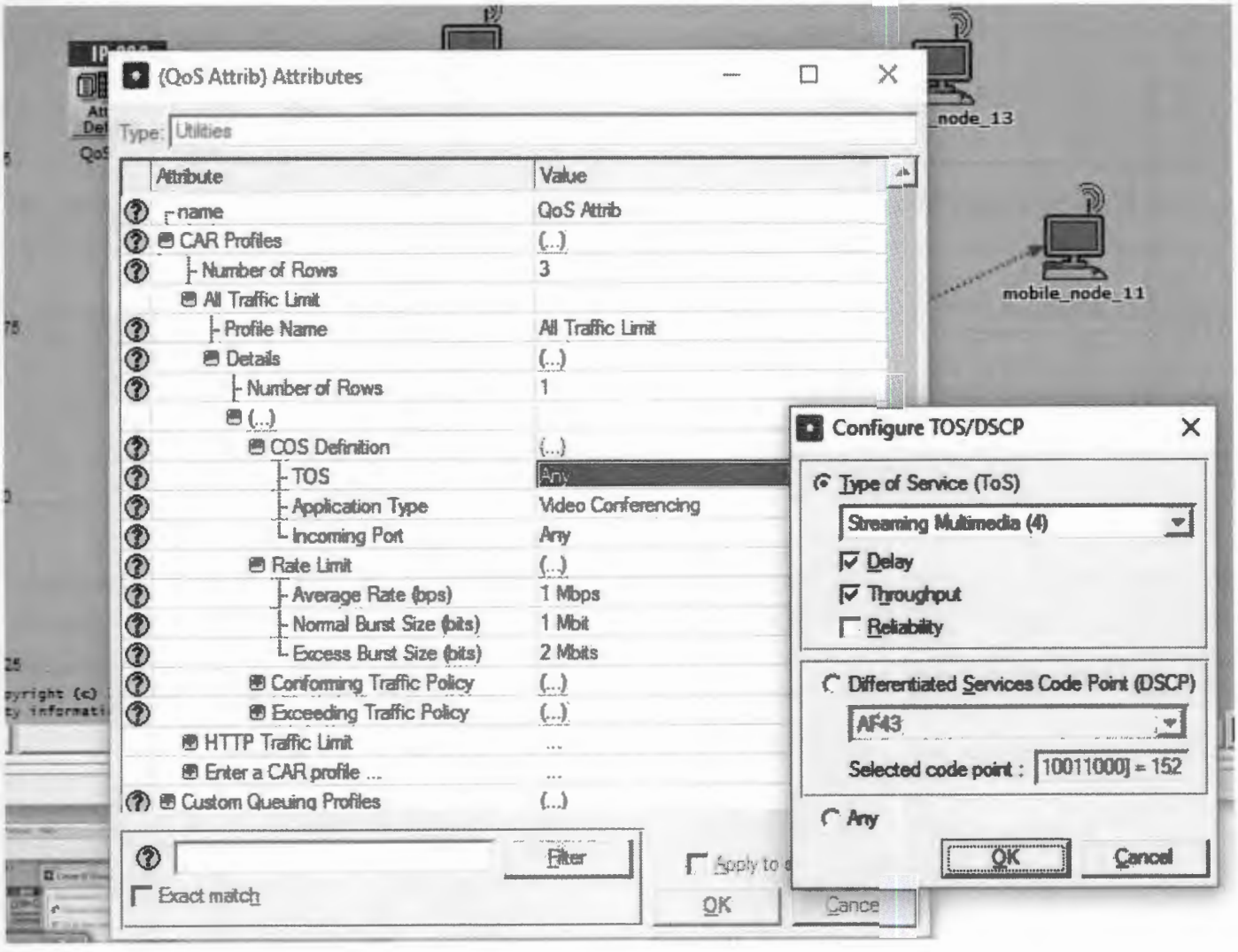

Figure 3.15: QoS Configuration

3.4 Scenarios

Our research work consisted of 8 scenarios. Four scenarios with 20 nodes each and at high resolution video as its application. It also has four other scenarios with 50 nodes and still at high resolution video but now with the implementation of the proposed framework. All nodes use UDP as a transport layer protocol and ran at 11Mbps. These attributes included the selection of routing protocols, application preferences and wireless LAN attributes. The transport protocol was only set out for video conferencing applications.

3.5 Quality of Service Measures in this Research study

There are so many performance metrics such as load, throughput, delay, jitter, routing overhead, routing traffic sent and received, Packet delay variation and many others. These metrics/measures are used in order to ascertain management and provision of QoS for video traffic. In this study, the following performance metrics were considered: Throughput, Delay and Data Dropped

3.5.1 Throughput (bits/sec)

It represents the number of bits forwarded from the Medium Access Control (MAC) to higher layers in all nodes in the network. It is measured in bits per second. The throughput may also be referred to as the average number of packets successfully transmitted or received per second.

3.5.2 Delay (sec)

This is normally the time taken for one packet to be transmitted from the source node to the destination node. It is expressed in seconds in most cases.

3.5.3 Data Dropped (bits/sec)

This is the amount of packets lost during transmission.

3.6 Chapter Summary

In this chapter, our simulation tool OPNET Modeller, was used to simulate 12 scenarios. Six scenarios were implemented using AODV and the other 6 scenarios implement with OLSR. In our previous work, these two protocols performed well in terms of video conferencing traffic. The conditions set by the application definition and application profile represented conditions set out by the application server (middleware). Our trust framework conditions were determined by the application as will be

shown in the next chapter. The evaluation of the pilot gave an indication / result showing which protocol was to be further evaluated or utilised for future work and in terms of which network scenario was trustworthy. Bringing so many scenarios gave the researcher a broader outlook in terms of selecting the most trustworthy scenario given different node densities. In the next chapter, we present our trust framework from its formation to its operations and complete breakdown.

CHAPTER 4

TRUST FRAMEWORK IMPLEMENTATION

4.1 Chapter Overview

In this chapter, we discussed the trust framework as proposed in our Chapter 1 and the method chosen to accomplish our research goal. Basically, we went through the processes that lead to the formulation of the trust management framework. This chapter presented a QoS analysis of the two protocols implemented in aiming to increase traffic efficiency in MANETs. The trust framework implementation presented answers to research questions 1, 2, 3 and the research objectives as stated in chapter one of the study. We also presented key QoS measures/parameters and how the protocols behave towards them in simulation. Also presented in this Chapter is our proposed experimental setup.

4.2 Simulation

Simulation is commonly defined to be an abstraction of real-life scenarios or an existing process. Network simulators best describe the state of the network nodes. These include nodes, links, switches, hubs and routers. In modern day simulators, they are either Graphical User Interface (GUI) driven or Command Line Interface (CLI) driven. The primary purpose of simulations is identifying problems that exist in a network or troubleshooting for unexpected interactions with one that has not yet been constructed. Upon identification of these problems or even preventing them it is then that corporations/companies can work on improving the state of the network in terms of network reliability and also maintenance costs. Simulation is mainly used in performance analysis, comparison or even management and also for determining how a network would behave in a real-life situation. The generated result of the simulation aids in identifying the performance of the network. The flair to the entire simulation software is that there is a wide range of tools that ensure the generation of excellent results. There is a choice of network traffic selection, programming environments, projection and statistical data representation. These are all part of the package of the simulation tool.

4.3 Simulation Environment Implemented

In this research work, a high-level event based network level simulation software called Optimized Network Engineering Tools (OPNET) was chosen. It is widely known for providing viable solutions towards performance analysis for networks and also applications. These simulations were carried out on a Windows 7.0 Professional Operating system (Desktop) with 3.40 GHz processor speed, 4.00 GB RAM memory and 64-bit Operating System. OPNET is developed by OPNET Technologies and was initially developed by an MIT graduate. One other feature OPNET provides is a graphical editor interface which is used to build models for different network entities. The reason why OPNET is known as a powerful simulation tool is because it enables designers to plan from small to large complex networks given various devices in that network. OPNET is known to provide a great simulating environment to implement new customized ideas and also solutions. This one advantage is backed by lower costs. It has an extensively wide range of protocols in its library and also a huge library of ready models that belong to fixed network hardware that is commercially available. This simulation software is used for research and development in both academic and industrial levels respectively. In our study, vehicles were represented by mobile wireless LAN workstations that move at a random faction. The software is very efficient in the study of application based protocols. Its potential to generate several traffic types adds on as another advantage.

4.4 Trust Management Framework

In this section we presented an overview of our trust management framework that combined the different technologies. After the provision of a high level overview, we presented assumptions that we made in connection with the framework and also the individual components found.

4.4.1 Overview

An Application centric trust management framework with distributed trust computations (AppTrusFram) was used. The application in question is video streaming. Video streaming is a rising technology innovation in MANETs. It may come in the form of low resolution video or high resolution video. Our framework involved an application server together with distributed trust computations. It is very important to have a management system that is able to compute the end result which is QoS evaluation in the form of throughput, delay, and jitter etc. Our framework involved neighbouring nodes direct trust (see figure 4.1). The application server played an important role in the attainment of excellent quality of service. The application server is built-in every workstation since

every station acts as its own router. This is because it encompasses features that involve security, diagnostics and clustering. Distributed trust computations are based on 'knowledge', 'recommendation' and 'experience'. Direct trust was chosen in this work because of its versatility and its ability to sense neighbours since MANET stations operate through WiFi or Bluetooth connectivity. The web server is responsible for processing client requests and send responses via the http protocol. Within the web server lays the web browser, an application, which is responsible for retrieving, traversing and presenting http requests into stream(able) media in the World Wide Web.

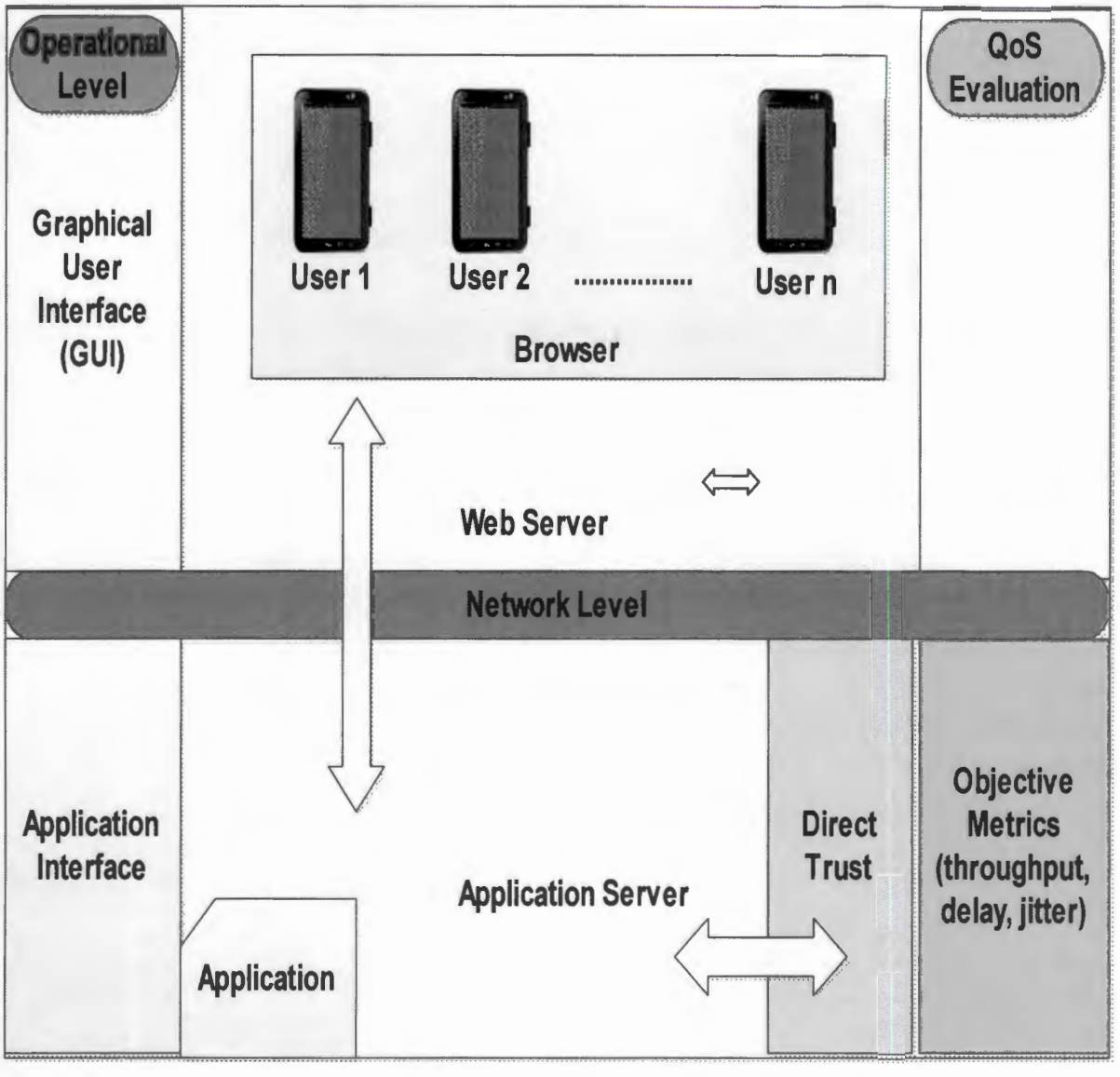

Figure 4.1 Trust Management Framework (AppTrusFram)

Figure 4.2 shows an expanded version of our trust management architecture fully exhibiting the application in question video streaming. It also shows the link between direct trust and QoS metrics.

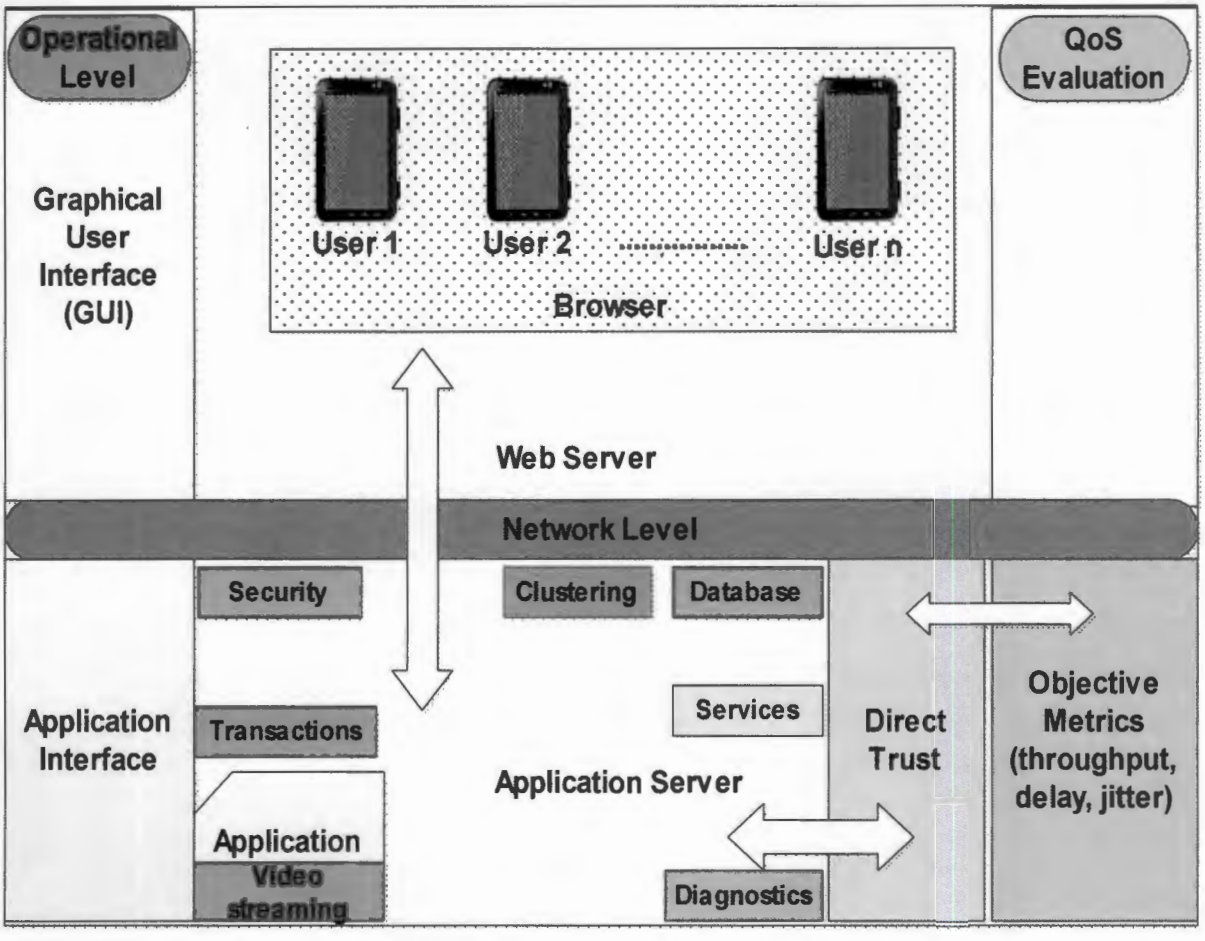

Figure 4.2 Expanded version of the framework

4.4.2 Application Server

The Application servers' function is to serve business logic to application programs through various protocols. It also handles all application operations among users and an organisation. It is able to deploy applications. It primarily acts as a middleware. A middleware is an abstraction and serves to facilitate the design, development and integration of distributed applications in heterogeneous net-environments. In MANETs, as outlined in Chapter 1, the nodes are self-configuring, basically meaning that they have their own internal application server. OPNET has a provision of the Application Profile where the application server is built in. This is where one can deploy their proposed application e.g. FTP, Video, Audio and so on. The profiler allows the user to adjust and fine-tune the various specifications of that application.

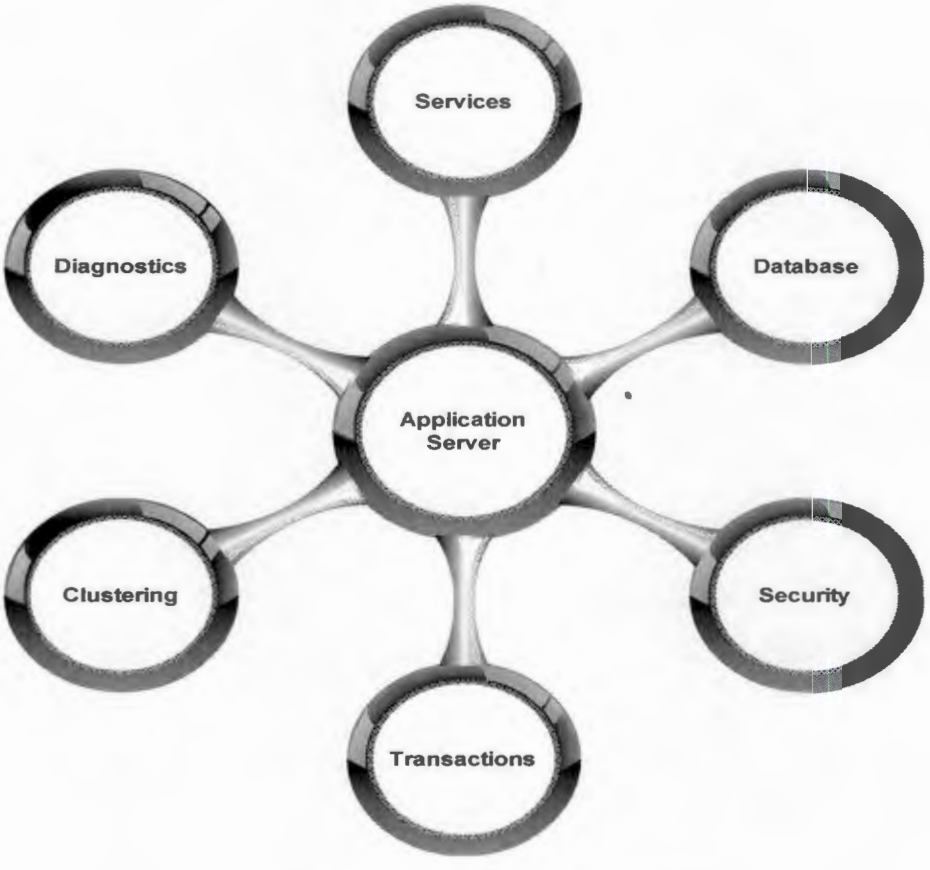

Figure 4.3 Application Server Functions

The above figure shows the functions of the application server. The application server has a diagnostics attribute to track down and resolve errors. Security is a critical aspect in terms of trust management. This is to make sure malicious nodes do not derail performance of the entire network. Trust among nodes is broken when one node withholds packets for a long time since transmission is through hops from one node to the other. Another active functionality of the application server is clustering. Clustering ensures that if hardware fails or part of an application fails, services can continue to run for business users. The application server has a set of common services and also a database for record keeping of all the transactions. Figure 4.4 shows the workflow of the application server, client and database.

4.4.3 Network Service Provider

It is important to note the importance of the Internet Service provider (ISP) especially when considering QoE. Operations taking place at this level of abstraction are not visible to the end-user. The ISP plays a major role because in·between application and web level, there is an internet connectivity which is provided by the Network Service Provider.

4.4.4 Web Server

The web server plays an important role towards the realization of http web pages and connectivity. This technology is mostly on the user interface side. One can argue that it may be used in the evaluation of quality of Experience (QoE). The browser is the main driving force behind the realization of the application stream. Basically, the browser translates these http pages into media content e.g. video, voice and ftp.

4.4.5 Operational Chain

This shows the level of abstraction at which the framework is under. The user interface is where the end-user can manipulate the system and view the entire flow. The network level however is hidden from the end-user. The programmer or rather network specialist can, however, evaluate the performance of the system at this level.

4.4.6 QoS Evaluation

QoS is the end-attainment goal of this work and our framework encapsulates such an option. The evaluation of QoS or rather the provision of high quality of service is what rates our framework. Different network detriments are observed while the system executes due to topology variations as

mentioned in Chapter 1. QoS metrics include throughput, jitter, delay and received routing packets. The end user cannot determine the QoS of the system because it is at a different abstraction.

4.4.7 Direct trust

Direct trust is application-centric or specific. The application has the decision to determine whether an interaction made by one entity to another was successful. Direct trust was chosen based on the merits that it is reliable in terms of rankings from confidence trust and reputation[25]. Our experimental tool is more application centric hence the decision to utilize direct trust for this framework as well.

Our framework operates from the point of view that the involved nodes do not necessarily have direct experience with all nodes in the network for them to be able to compute a particular trust level about them. In contrast, the trust is based on second hand evidence that is provided by intermediate nodes. In this way they benefit from the experiences of other nodes in the network. Our framework was designed to compute trust based on interaction experiences. The attainment of good QoS in the network is evidence that the network itself is trustworthy. Good QoS in a dynamic topology network validates our framework. Our direct trust can be calculated using equation 4.1;

$$\text{Direct Trust Computation} = (g + (x)/2) / (q + x)[24] \quad (4.1)$$

Where g is the time success to say an event happened, x is a positive real number, and q represents the event transactions.

If the first event of the transaction is a success, the direct trust value increases but converse to this it decreases. In our framework, the success rate can also be referred to as the trust value and can be any real number between 0 and 1.

In terms of QoS, the measure called delay plays a major role in finding the true trustworthiness of the network. This would mean that a specific node delivers packets on time and thus increased network efficiency.

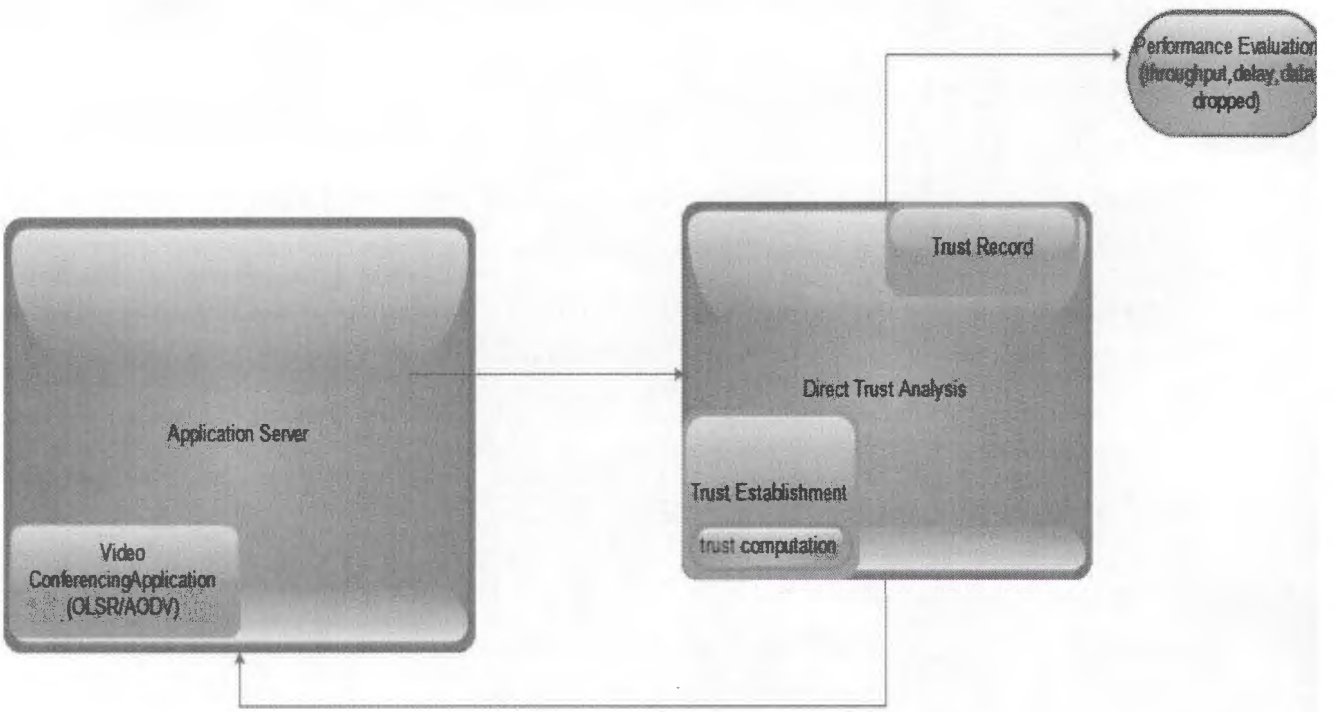

Figure 4.4 Application Interaction with Direct Trust within a node

As mentioned earlier, the idea of MANETs revolves around the idea that they are self-configuring and fig 4.5 shows the interaction of the application with direct trust. We assume that the application protects itself from malicious conditions. Here are a few definitions of concepts;

a) **Trust Record**: This component reveals information on the trust relation between the application and the node. It also gives information on trust values in terms of their collection and storage.

Table 3: Trust Record

Trust Relationship	**Observation**
Relation 1	1 or 0
Relation 2	1 or 0
Relation 3	1 or 0
Relation *n*	1 or 0

b) **Trust Computation:** This component computes the trust value of the relationship between two different nodes. This computation can either give a 1(success) or 0(failure). The assumption is that direct trust is based observation of activities performed by the application. This interaction happens in the application interface and is abstracted to the user

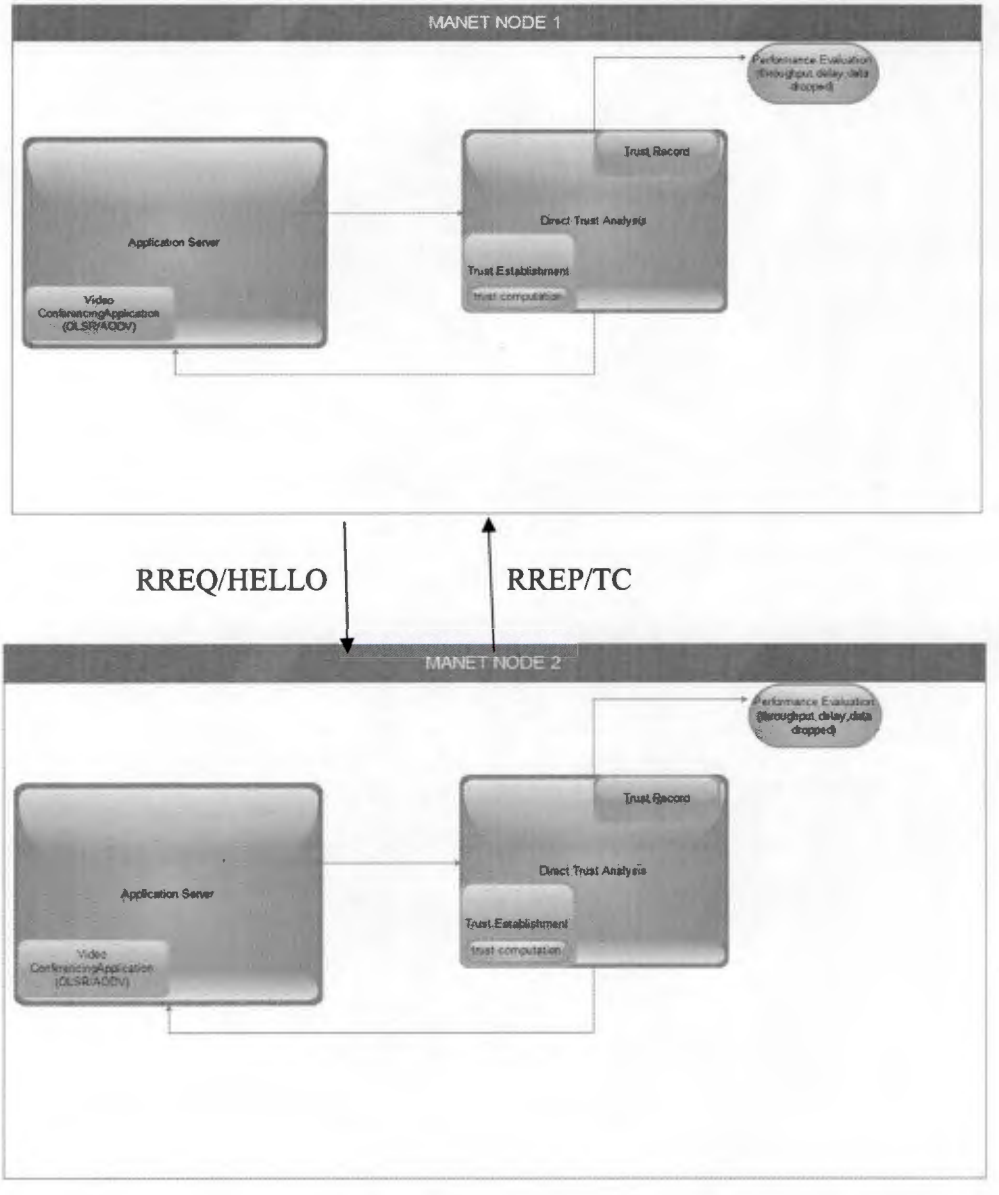

Figure 4.5 Operational Architecture (Node to Node interaction)

Fig 4.5 shows node to node interaction of either AODV/OLSR video conferencing traffic. It is important to note that MANET stations do not have a central controller and that is why every station has its own application server. Every station is responsible for its own application. Performance evaluation can be done at node level and at network level. The direct trust analysis depends on the direct interaction behaviour of nodes together with their direct trust computation. After analysis, a performance evaluation can be conducted. The absence of a central controller gives each node the independence to execute functions remotely.

4.4.8 Application Infusion with Trust

In order to fully understand the true meaning of trust, we need to start definitions of trust as adopted from social science. Since this phenomenal is adopted from social science, there is no definite or precise definition in computer networks. It is often interpreted as reputation, trust opinion or even probability. The evaluation, as well, is done in many different ways using various models. Some models or rather schemes use continuous or discreet numerical values to quantify the level of trustworthiness. These are called quantitative trust models. There are many available trust models but it is still not clear as to the fundamental rules they must adhere to. This means that the design of these models is at an empirical stage.

In our framework, we view trust as intentional and that is, one node is willing to depend on another node. Trust intention brings out other concepts or constructs. The application remains in control of determining trust. The other concepts entailed in trust are trusting belief, system trust and belief-formation process. These are the 3 main blocks of trust management. They are responsible for providing the application enough reasons to evaluate.

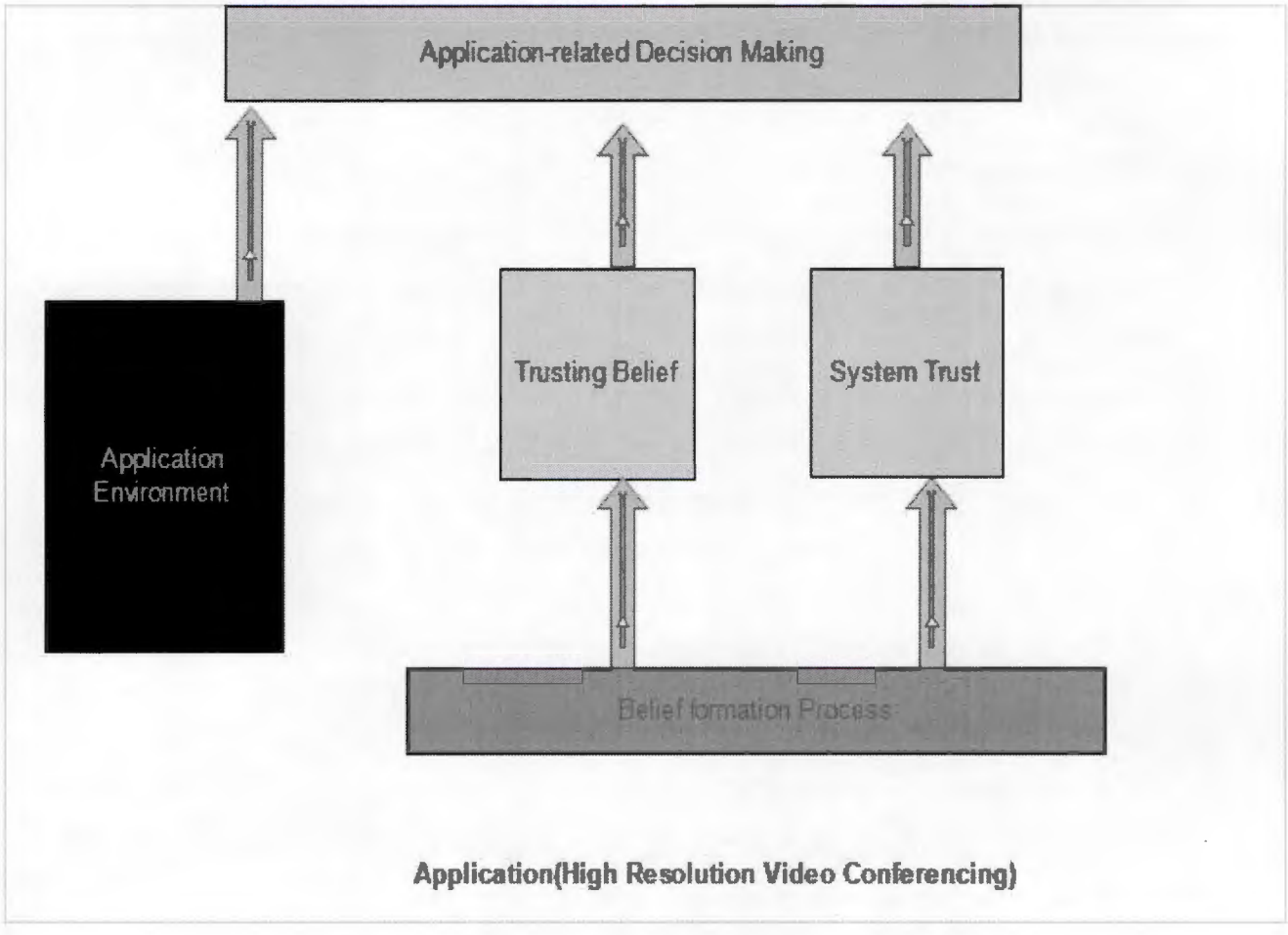

Figure 4.6 Application infusion with Trust [34]

Figure 4.6 brings out a perspective into our framework as application-centric. The application is still video conferencing and the QoS evaluation results would prove whether the network could be deemed[34] trustworthy or not.

a) **System trust:** System trust is the belief that the network will operate as it was designed to. This may refer to the physical structures in place to provide structural assurance.

b) **Trusting belief:** This is when a node believes that the other node is willing to and is able to act in the other nodes' best interest.

c) **Belief formation processes:** This refers to the very building blocks of belief (trust) that the network will operate in a certain way.

d) **Application related Decision making:** The outcomes of trust management, which will make a decision based on the evaluation of trust and other application related conditions.

4.6 MANET Protocols Utilized

The merits at which our two protocols were chosen remains clear. When considering reactive protocols, we looked at a protocol that does not increase its data packet header as the network size grows.

4.6.1 AODV

Here are a few more reasons why AODV [35] was chosen;

a) Broadcast route discovery mechanism

b) Route request (RREQ) and Route reply (RREP) ensures the delivery of packets.

c) Routes are created when needed to prevent a large packet overhead.

4.6.2 OLSR

When looking at reactive protocols, OLSR was[35] chosen based on the following merits;

a) Multipoint Relays to reduce information overhead

b) No need for central system for routing purposes.

c) Well suited applications since it keeps delays at minimal during transmission period.

4.6 Trust Framework Operations

MANET communication plays a major role in the attainment of a proper flow of packets within the framework. Firstly, video packets will always move from the sender to the receiving end. The framework vividly shows two different interfaces that are involved, mainly graphical user interface

and application interface. The application interface can be abstracted as where the source of the video lies but keeping it in mind that so much of bi-directional communication is involved around the different component parts. Before an application can be sent, the application server as the middleware in this context has to ensure that direct trust is established. This means that the node has to be inspected in terms of its trustworthiness to service delivery. The application server is responsible for many functions including a database, clustering and diagnostics as demonstrated in Fig 4 2.The framework can be evaluated in terms of QoS(Application interface) as shown in figure 4.5 and can be evaluated in terms of QoE(User interface).

When the video file is sent through at network level through the assistance of the internet service provider, it is meant to reach the web server. At this point in time, the video file is at the user interface side. The web server receives it as an http file or page and translates it back into media content (video file). The web server houses the web browsers just like application servers houses applications. Users get to stream the media content. The connection amongst these components remains bi-directional since trust must be maintained. QoS evaluation metrics like throughput, total packets dropped and delay are implemented. Delay is an important QoS feature since it shows if there were selfish nodes or not. Since nodes are self-configuring, it is possible to measure the performance of each node. The direct trust is established at node level.

The absence of a central controller means that each node has its own application server and runs its own computations (see fig 4.5).Node to node interaction is the core of our framework evaluation as shown in fig 4.6.

4.7 Chapter Summary

Our formulated framework brings closer a relation between trust and QoS. It also gives a wider perspective to the researcher in terms evaluating QoS or QoE. The application server is normally termed as a middleware within the operations of a system. Direct trust was properly defined in the context of the framework and in relation to the application. Experience is one of the pillars of direct trust but in our work, the direct trust is taken from the perspective that there are no prior experiences or interactions amongst nodes. The Application, through its server, is given the privilege to draw an acceptable level of trust and to, in turn, give a QoS result. Furthermore, an extension of the application was brought to comprehend the value of the application towards the realization or rather evaluation of

the framework. The framework is designed for video streaming purposes but can also be implemented for other applications like FTP.

Chapter 5

Results and Discussion

5.1 Chapter Overview

In this chapter we first analyze and compare scenarios of different protocol utilization. There are two routing protocols being analyzed and compared AODV and OLSR. Each protocol has three different

scenarios per QoS metric. The metrics in question are throughput, delay and data dropped. This means that we will have twelve scenarios in total. Node scenarios are to the total 20, 40, 60 and 80 respectively. All the simulations conducted are done in a 4 hour period. At the end of this chapter, our results obtained will be presented in the form of properly labelled graphs.

5.2 20 Node-Scenarios

Two network scenarios results are analyzed and compared in terms of their throughput, delay and data dropped. Each network scenario uses AODV and OLSR protocol respectively.

5.2.1 Throughput

Figure 5.1 shows the throughputs for AODV and OLSR. The Y-AXIS shows the throughput in bits/sec and X-AXIS show time in hours and minutes. The first 3 minutes shows a positive hike up to 920 bits/sec in throughput then a steady drop after 25 minutes of simulation time. A further drop is observed for the remaining simulation till it reaches 100bits/sec. OLSR on the other hand shows a major drop from 12 bits/sec to 5 bits/sec in the first 15 minutes of simulation. After 20 minutes, it picks up reaching an average of 8 bits/sec to 9.5 bits/sec for the remainder of the simulation even though it is still a poor throughput. This means that on an overall scale, AODV has a better throughput than OLSR.

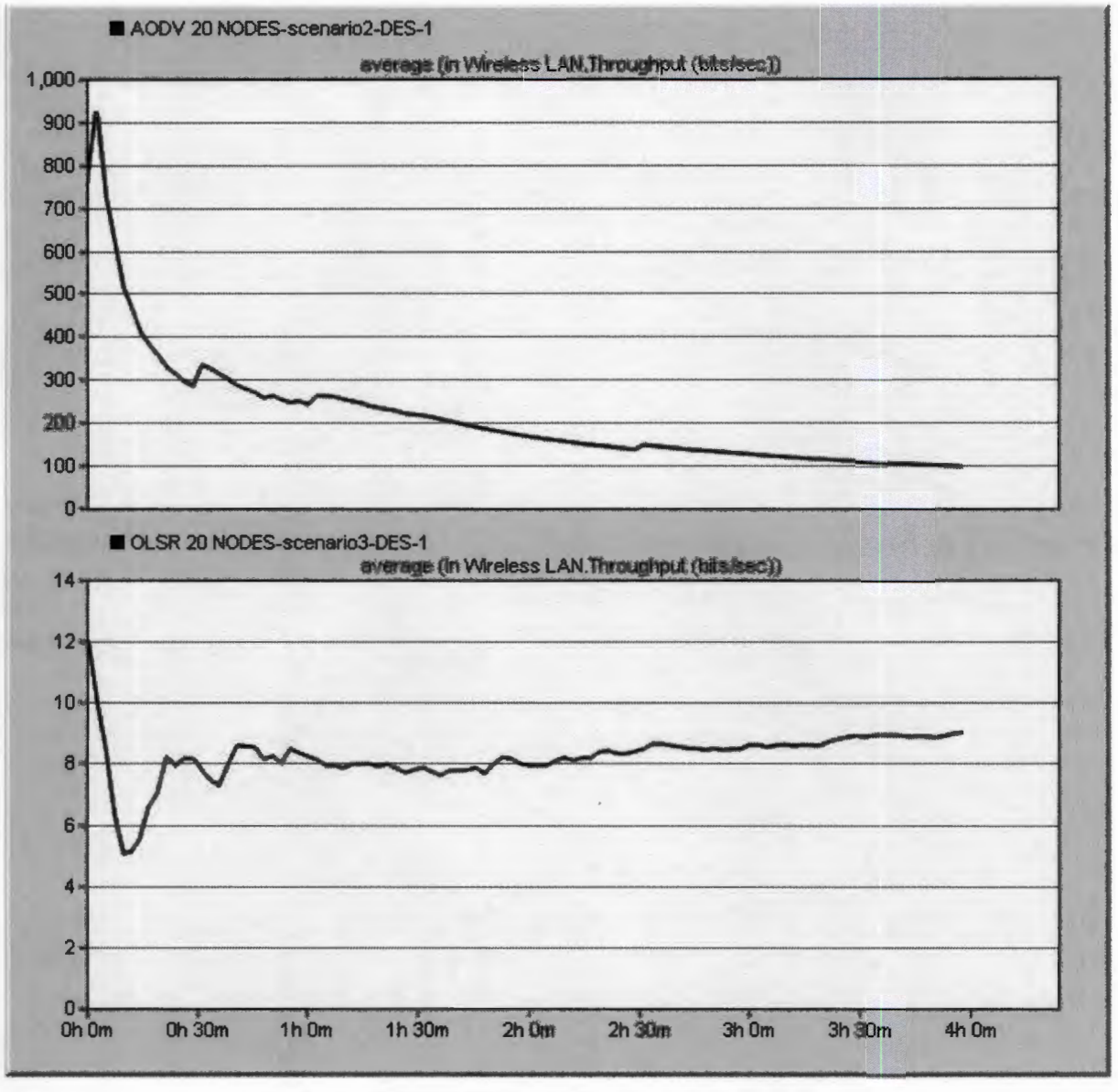

Figure 5.1 Average Throughput in bits/sec

5.2.2 Delay

Figure 5.2 shows the network delay for AODV and OLSR protocols. In the first five minutes, AODV shows a slight rise in delay from 0.00026 bits/sec to 0.00029 bits/sec. This may be regarded as an insignificant rise in the eyes of the user but significant in terms of network efficiency. The delay drops again exactly after 5minutes back to a steady delay of 0.00026bits/sec. OLSR shows a constant delay

of 0.00025bits/sec for the first 80 minutes of the simulation then a sharp rise to 0.00050bits/sec after that showing a gradual drop to 0.00033bits/sec. In this scenario OLSR has a significantly higher delay rate than AODV.

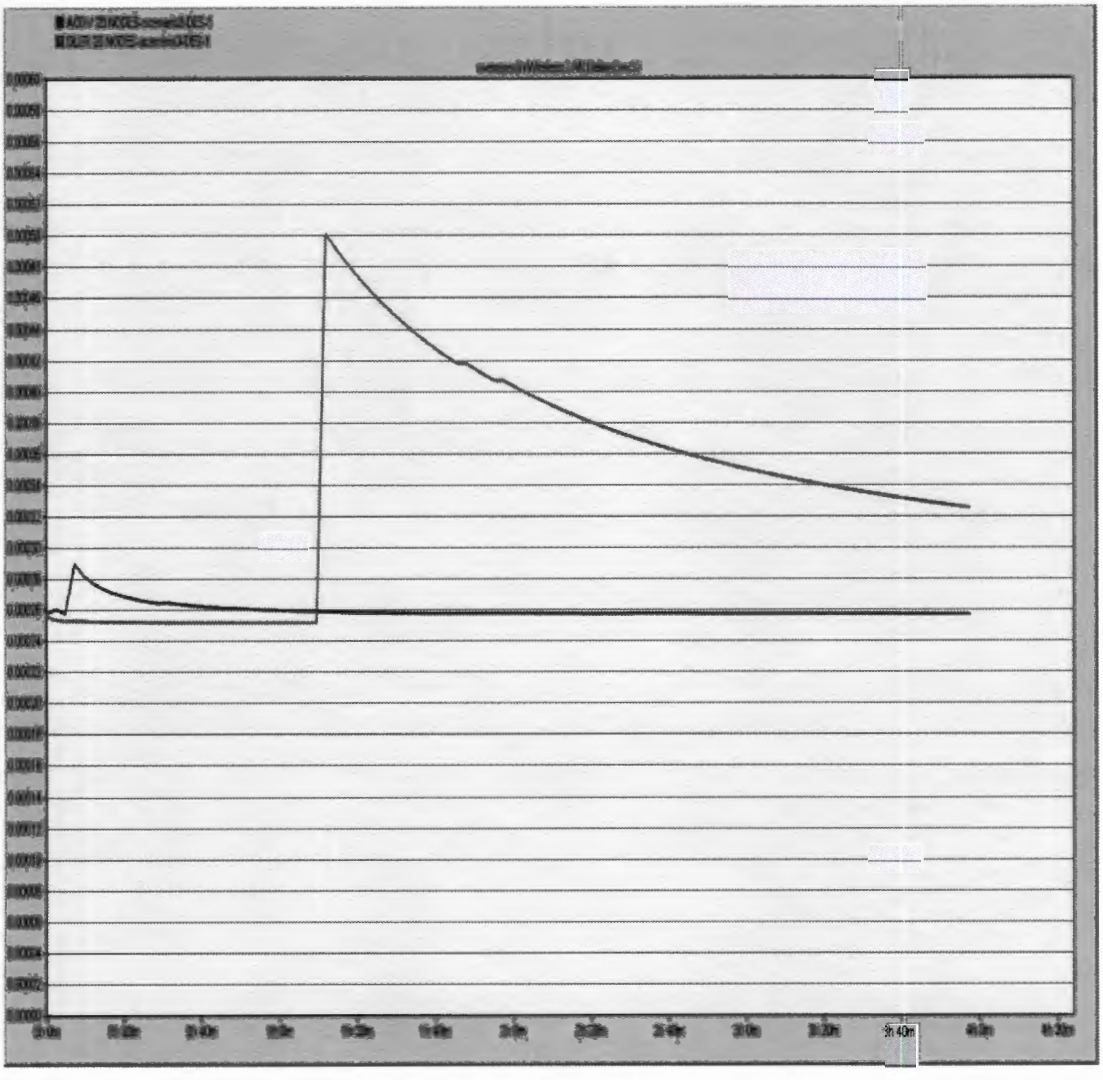

Figure 5.2 Network delay in sec

5.2.3 Data dropped

Figure 5.3, shows the average data dropped for both scenarios. The Y-AXIS shows number of bits and the X-AXIS continues being our time represented in hours and minutes.OLSR shows a sharp rise for the first 3 minutes of simulation to 22 bits/sec then a sharp decline until about 20 minutes. The protocol further drops more data from the 18^{th} minute till 20 minutes of simulation time. From there, the levels drop until they reach a margin of 4 bits/sec in data dropped on the 50^{th} minute. It further rises again until 2 hours of simulation time then gradually shows a decline data dropped until it reaches 2.8 bits/sec. AODV shows no data dropped.This determination was performed a couple of times but still remained on 0 bits/sec throughout the simulation period. OLSR has a relatively higher fate of data dropped than AODV.

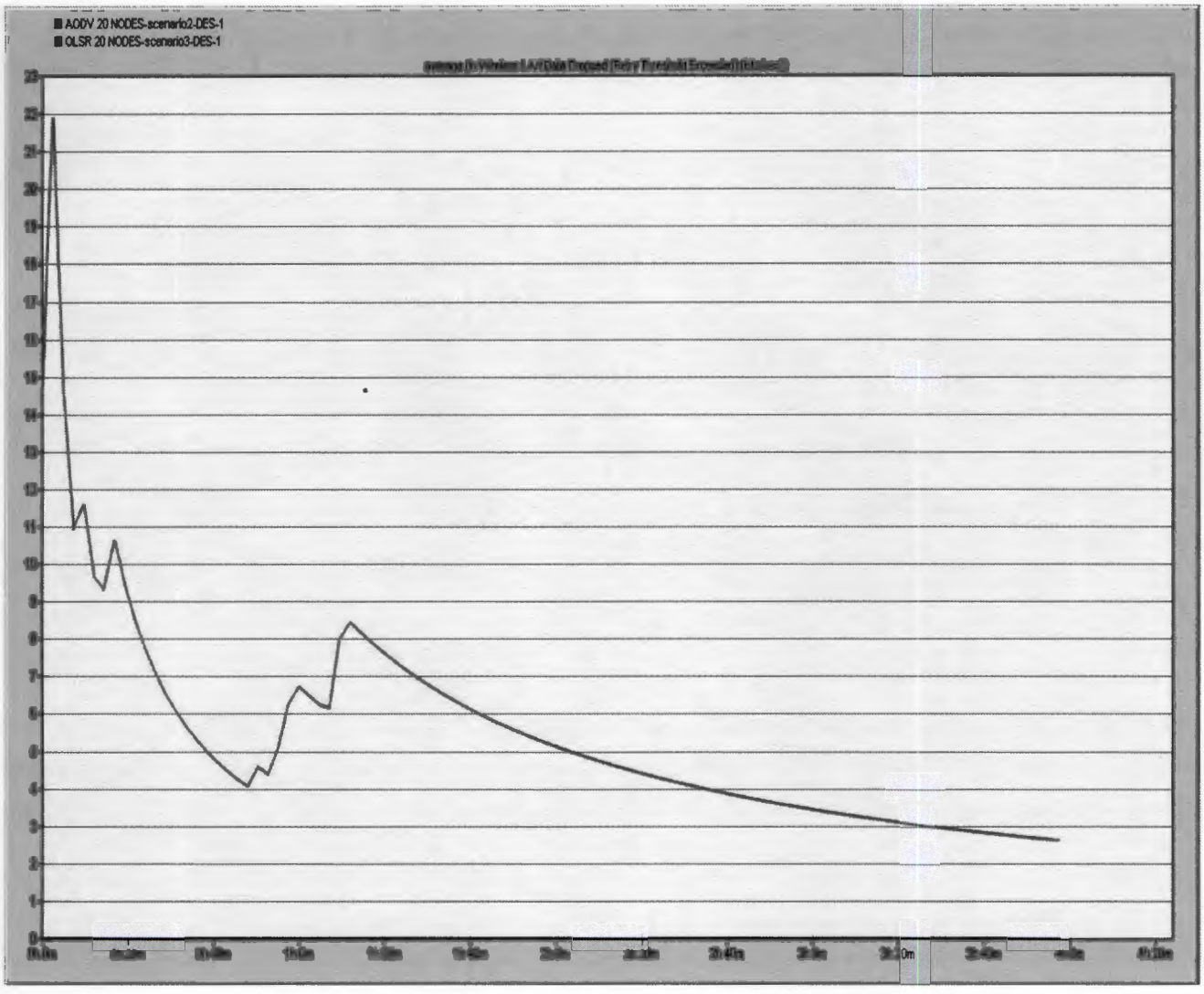

Figure 5.3 Average data dropped in bits per sec

5.3 40 Node-Scenarios

Two network scenarios results are once again analyzed and compared in terms of their throughput, delay and data dropped. Each network scenario uses AODV and OLSR protocol respectively.

5.3.1 Throughput

Figure 5.4 shows the throughput for AODV and OLSR scenarios. The Y-axis shows bits and X-axis show time in hours and minutes. OLSR shows a consistent and steady throughput throughout the simulation period. It starts off at 4 000 bits/sec slightly falls off to 3 890 bits/sec after 160 minutes of simulated time. The protocol then maintains a constant 3 800 bits/sec for the remainder of the simulation. AODV begins on a positive rise of 2 000 bits/sec in the first 3 minutes of simulation then drops gradually for the remainder of the simulation time. The throughput decreases until it reaches 300 bits/sec after 4 hours of simulation time. OLSR has a better throughput than AODV.

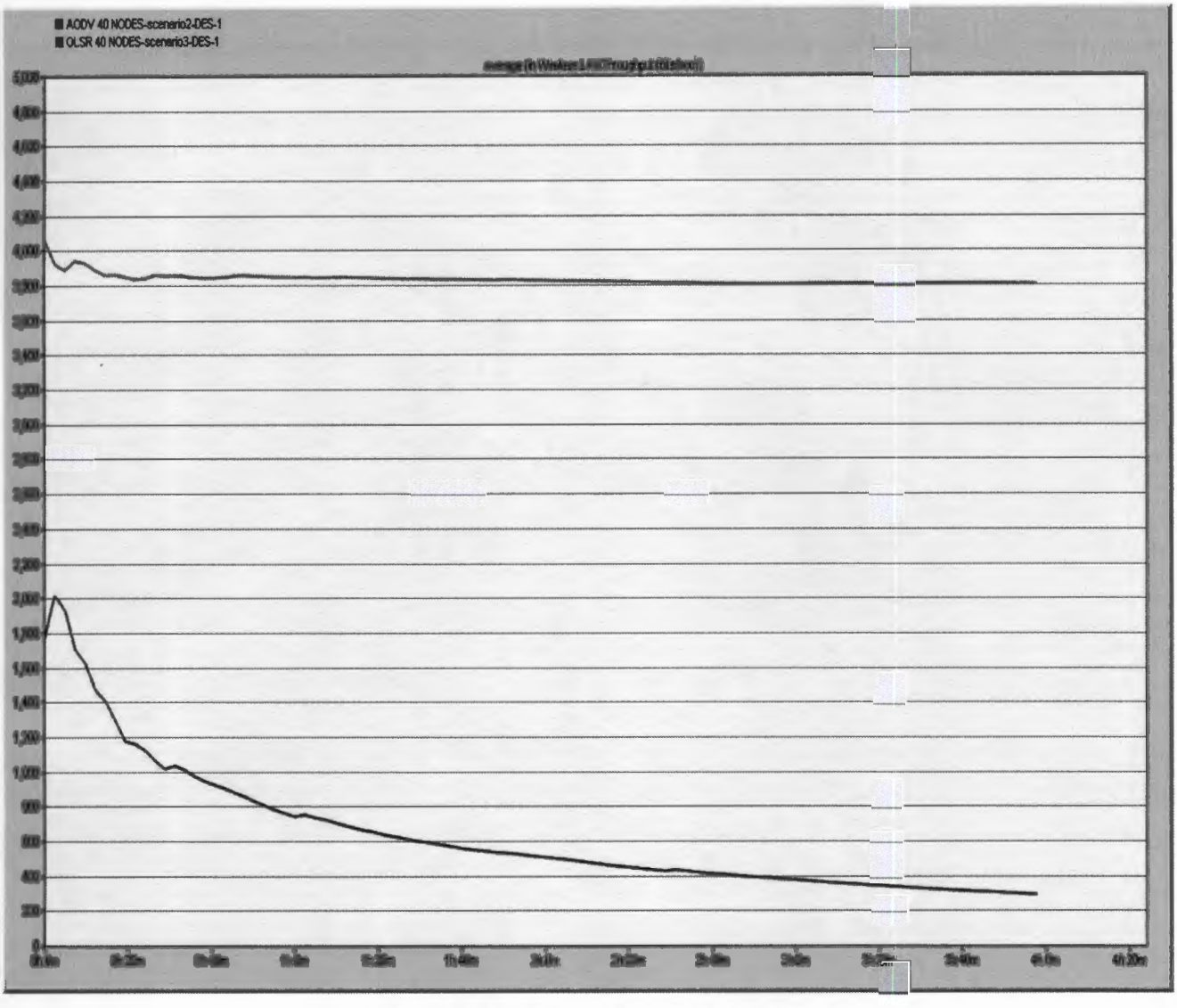

Figure 5.4 Throughput in bit/sec

5.3.2 Delay

In figure 5.5, OLSR exhibits a constant and steady delay throughout the simulated time. It slightly falls from 0.00029 sec to 0.00027sec in the first 40minutes of simulation. Lastly, it drops to 0.00026 after 4hours.This consistent drop from 0.00029sec is a positive result in terms of efficiency. AODV shows a decline in delay from 0.00057sec to0.00031 sec after 20minutes simulation. It then fluctuates between 0.00029sec, 0.00029sec, 0.00030sec and 0.00032sec.After 2hours of simulation, AODV decreases the delay rate 0.00029sec till 4hours time. OLSR exhibits a lesser delay than AODV.

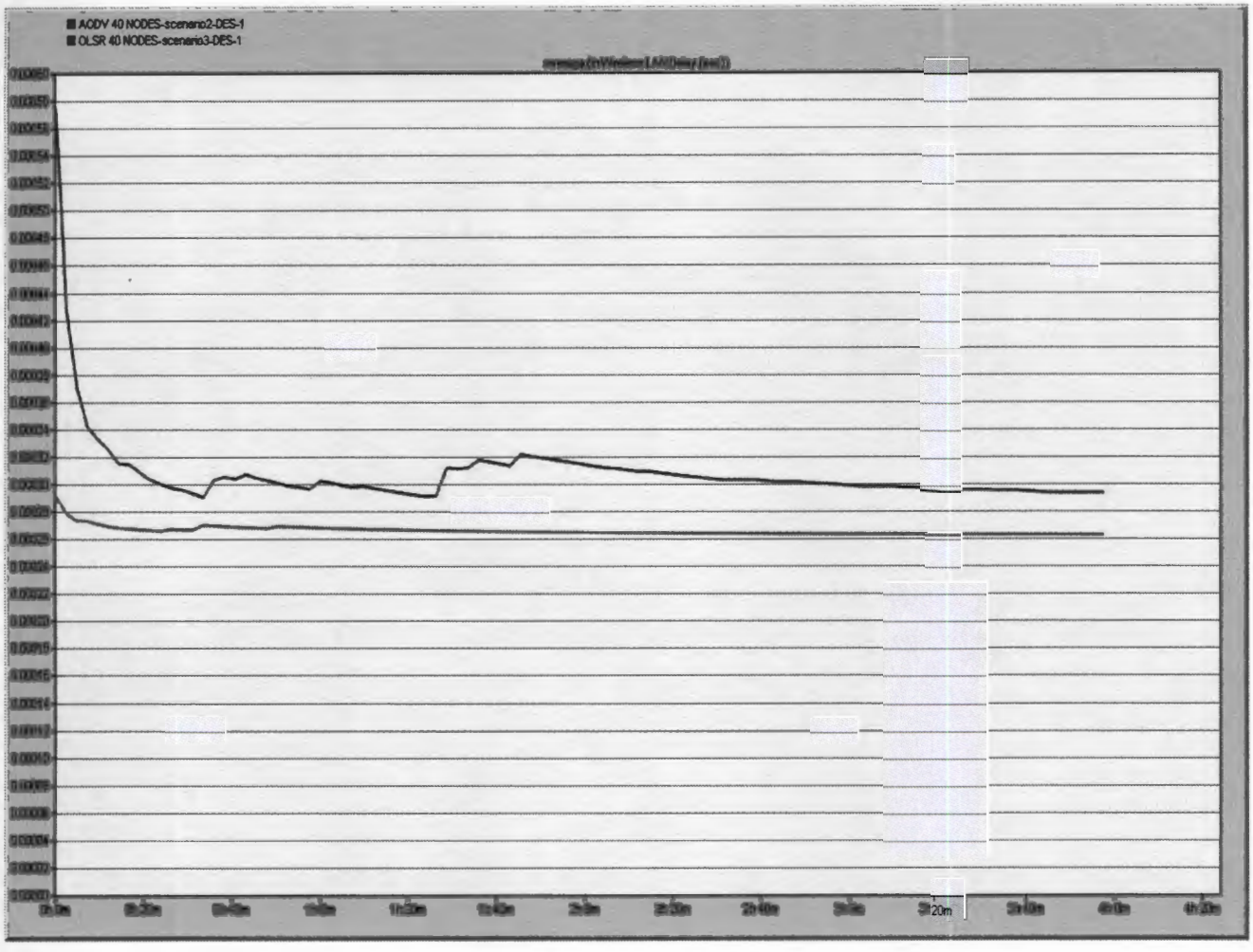

Figure 5.5 Delay in sec

5.3.3 Data dropped

In figure 5.6 below, the Y-axis shows bits and X-axis show time in hours and minutes. Both scenarios have sharp decline data dropped for the first 10 minutes of simulation, then it gives a steady decrease. However, for the next 100 minutes of simulation, the data dropped fluctuates. AODV starts off from 375 bits/sec and sharp decreases to 60 bits/sec. It continues to gradually decrease until it reaches 10 bits/sec after 4 hours. This is a great performance from the protocol bearing in mind that it started off at 375 bits/sec data dropped. A similar performance was observed with OLSR, starting off at 100 bits/sec then exhibiting the same fluctuations and decrease and ultimately ending up at 10 bits/sec just like AODV. On an overall scale, OLSR`s rate of data dropped was less than that of AODV.

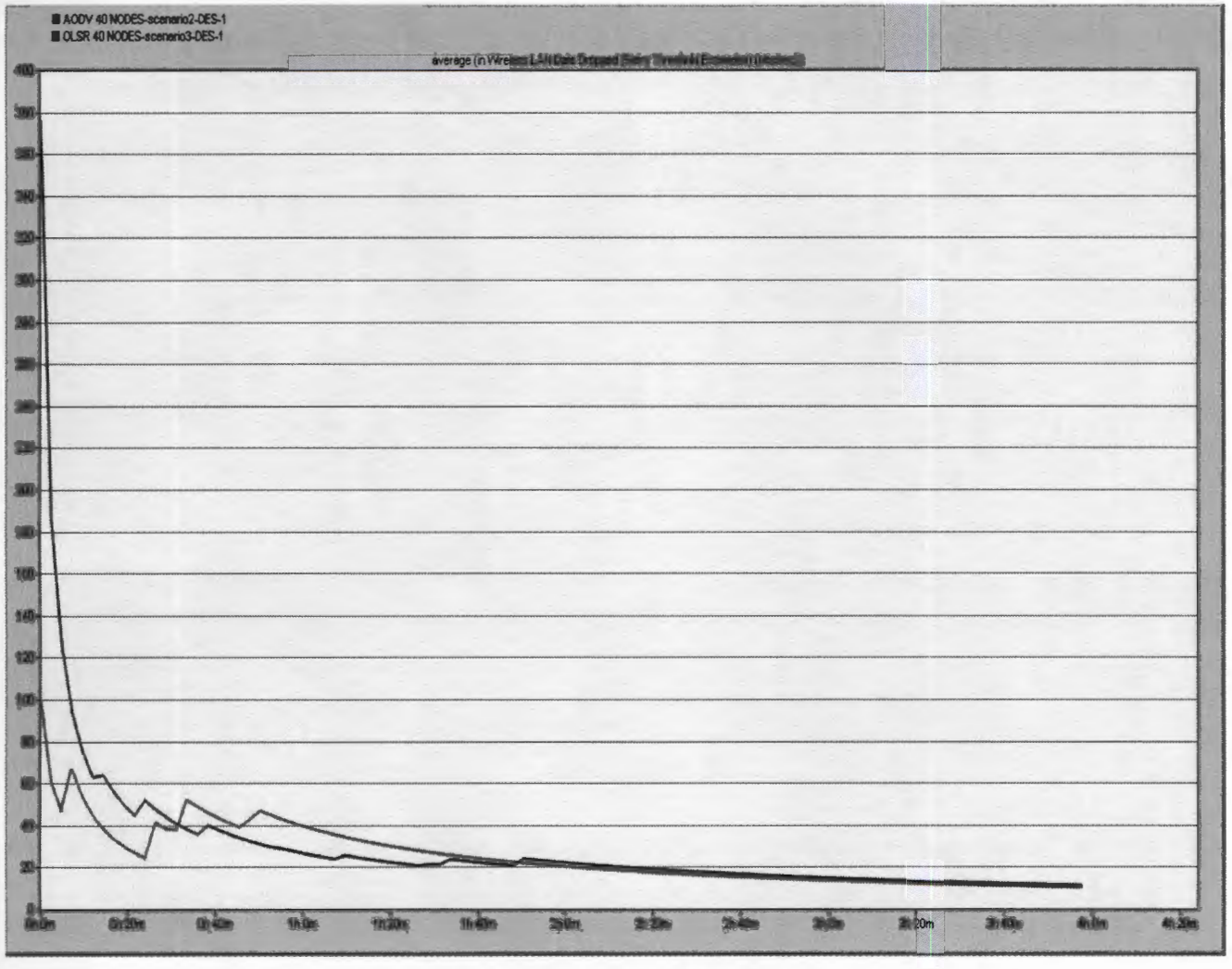

Figure 5.6 Data dropped in bits/sec

5.4 60 Node-Scenarios

Two network scenarios results are analyzed and compared in terms of their throughput, delay and data dropped. Each network scenario uses AODV and OLSR protocol respectively to route video conferencing traffic.

5.4.1 Throughput

In figure 5.7 below the Y-axis shows bits/sec and X-axis show time in hours and minutes. AODV gave a higher throughput from an average of almost 600 000 bits/sec to a steady hike to 2 200 000 bits/sec after 30minutes of simulation then constantly dropping to 2 100 000 until the end of the simulation. OLSR on the other hand shows a constant throughput of 100 000 throughout the simulation period. It is with no doubt that AODV gave better throughput in this scenario than OLSR

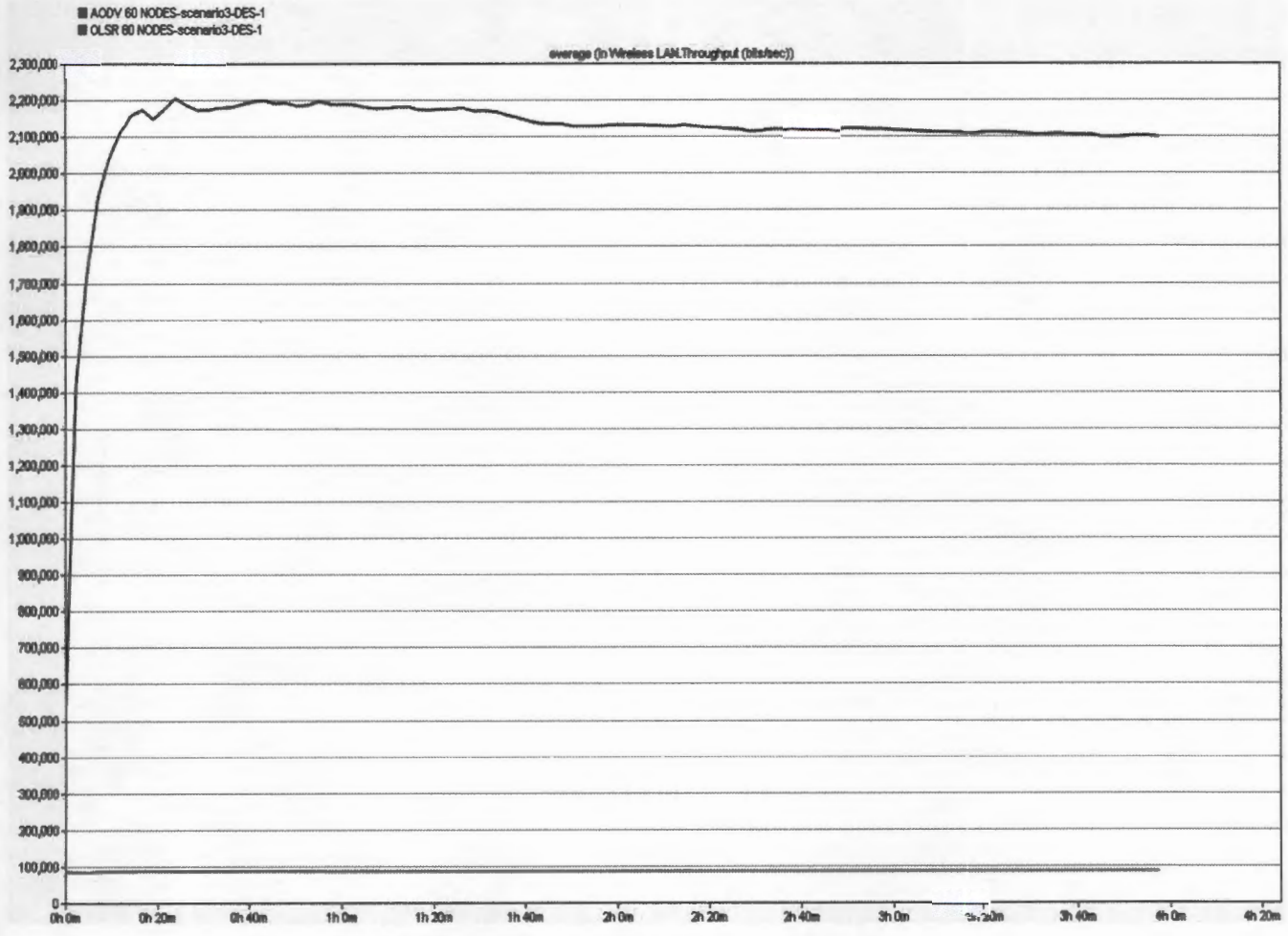

Figure 5.7 Throughput in bits/sec

5.4.2 Delay

In figure 5.8 below, the delay exhibits a growth in delay for AODV over the entire the simulated time. The growth of the delay was observed from 0.06 seconds until 0.14 seconds which was at the end of simulation. The delay grew directly proportionally with time. OLSR, however, gave a lower delay of 0.00027 seconds and dropping to 0.00026 seconds until the end of simulation. Throughout the simulation, it remains constant and steady in terms of performance. In this scenario, OLSR out-performed AODV but we cannot rule-out that AODV throughput traffic is nowhere near that of OLSR.

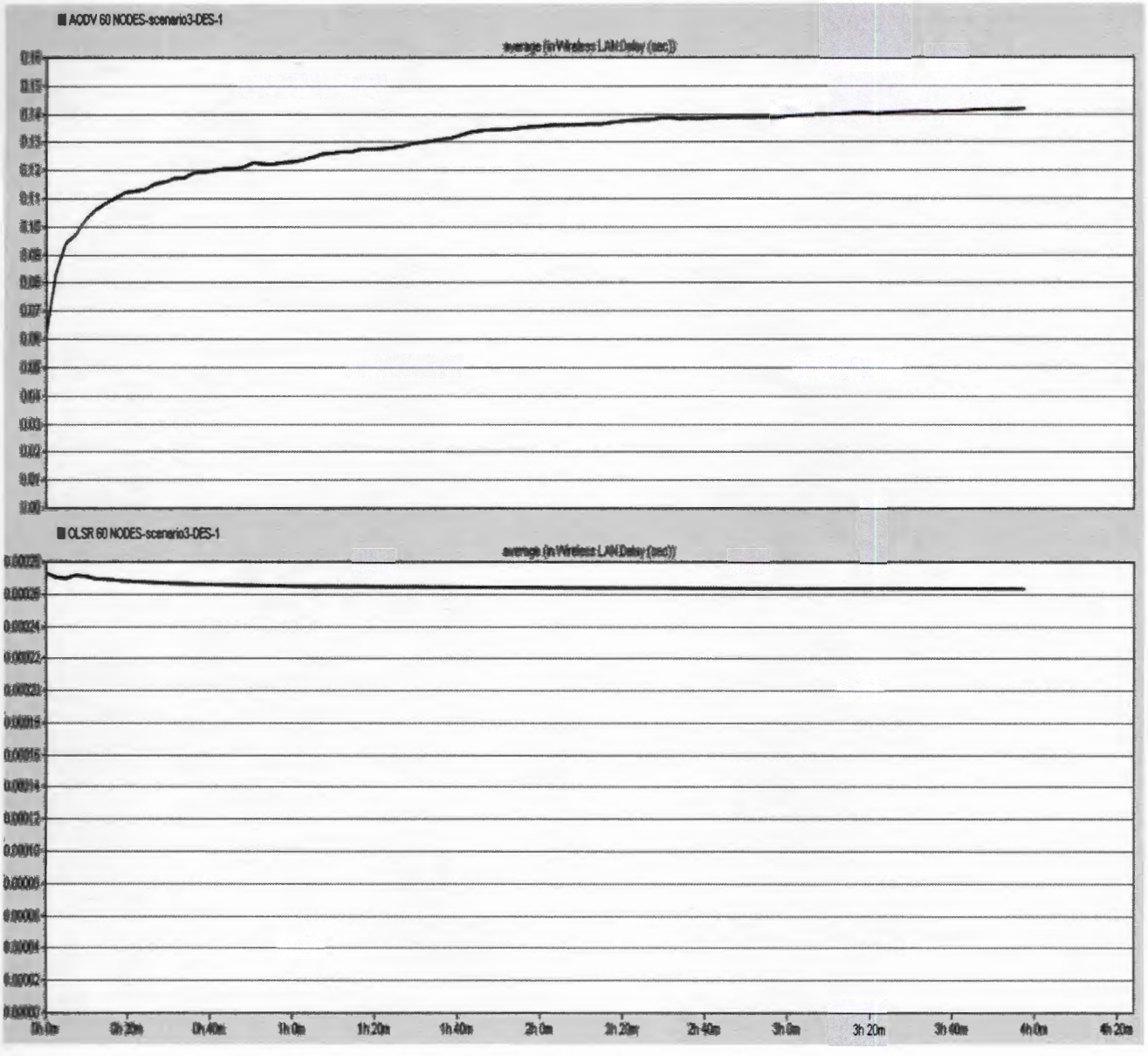

Figure 5.8 Delay in seconds

5.4.3 Data dropped

In figure 5.9 below shows the data dropped in bits per second. The highest recorded average data dropped for AODV was 210 000 bits/sec from100 000 bits/sec. AODV shows a consistent growth in terms of data dropped over the simulated time. The results prove that the data dropped per second grew directly proportionally to the simulated time. OLSR, however, started off at 240 bits/second data dropped. It showed a sharp decrease for the first 18 minutes of simulation to 80 bits/second. The protocol showed decreases of less data as time went on and until an ultimate 10 bit/second in the 4 hours of simulation time. The result was inverse to that of AODV as this protocol dropped less data over time.

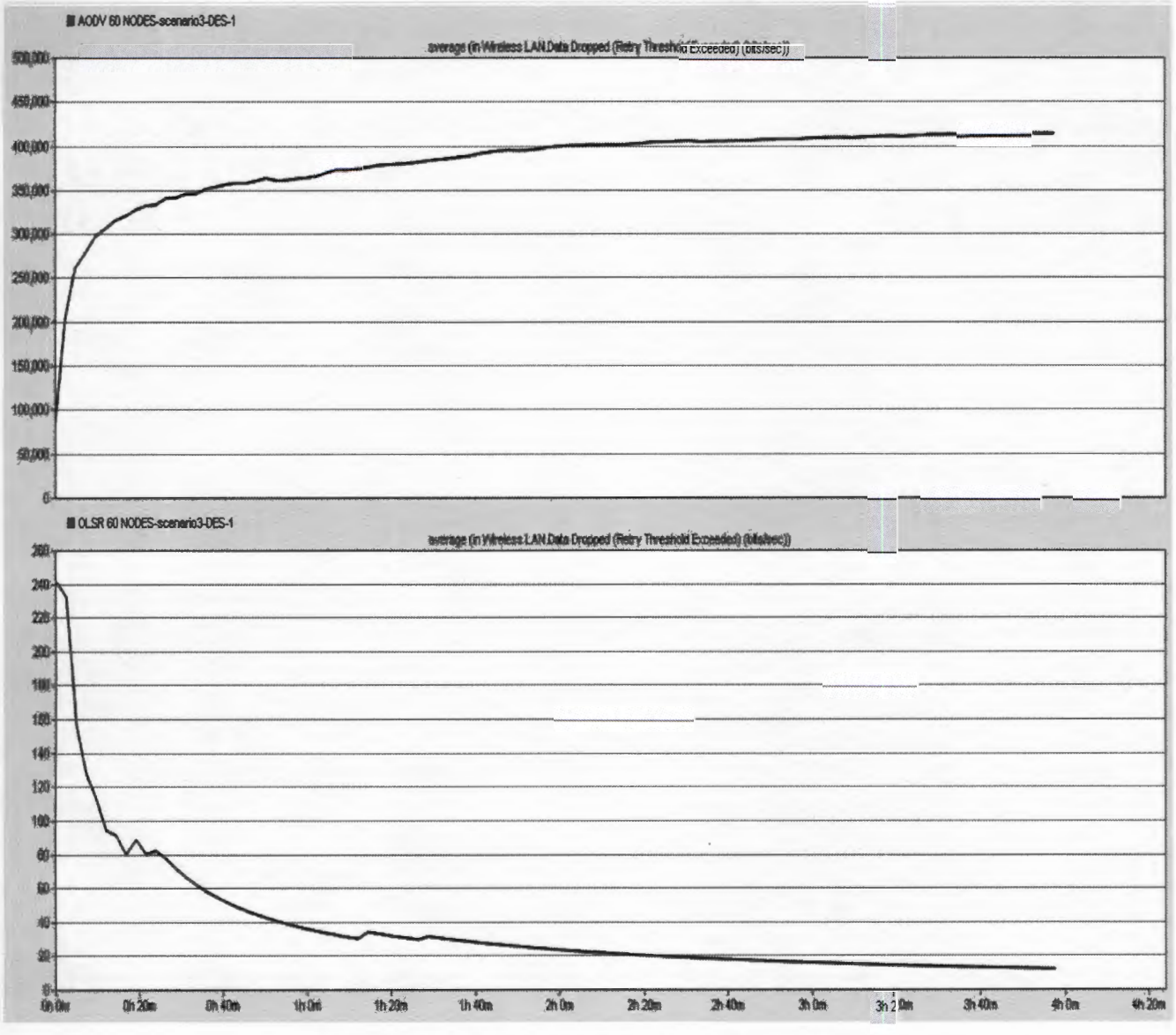

Figure 5.9 Data dropped in bits per second

5.5 80 Node-scenarios

Two network scenarios results are analyzed and compared in terms of their throughput, delay and data dropped. Each network scenario uses AODV and OLSR protocol respectively. Each scenario has a total of 80 nodes.

5.5.1 Throughput

Figure 5.10 below shows throughput of both ADOV and OLSR. The Y-axis of the figure shows bits/second and X-axis show time in hours and minutes. OLSR shows a continuous growth spiking up to an average peak of almost 2 200 000 bits/second and 800 000 bits/second being the lowest average throughput. After 15 minutes of simulation, the growth was then constant and steady until the end of the simulation. AODV showed an average peak throughput close to 1 300 000 bits/second after 15 minutes of simulation but in overall it showed a spiking growth after the first 4 minutes of simulation from 300 000 bits/second to the latter. AODV, just unlike OLSR then dropped its throughput value until it reached 950,000 bits/second after 4 hours.

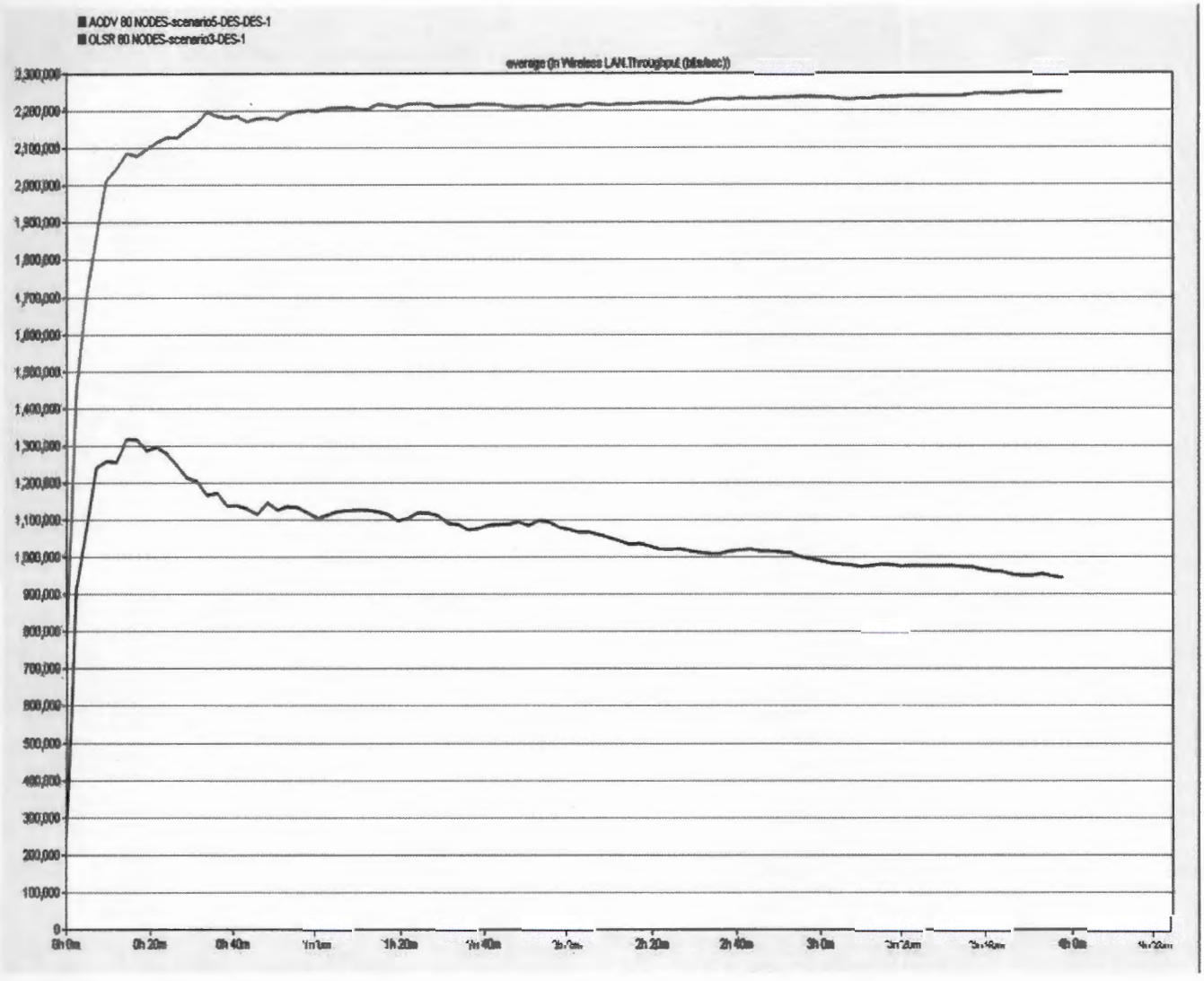

Figure 5.10 Throughput in bits/sec

5.5.2 Delay

In figure 5.11 below, the delay exhibited steady and accelerated growth throughout the simulated time. The increase of the delay per second was sharp for both AODV and OLSR in the first 3 minutes of the simulation. The Y-axis shows delay in seconds and X-axis show simulated time in hours and minutes. AODV showed an average peak delay of 0.040 seconds after 120 minutes of simulation and OLSR showed an average peak delay of 0.35 seconds. The delay is constant and not increasing after 20 minutes of simulation. AODV had a greater delay than OLSR.

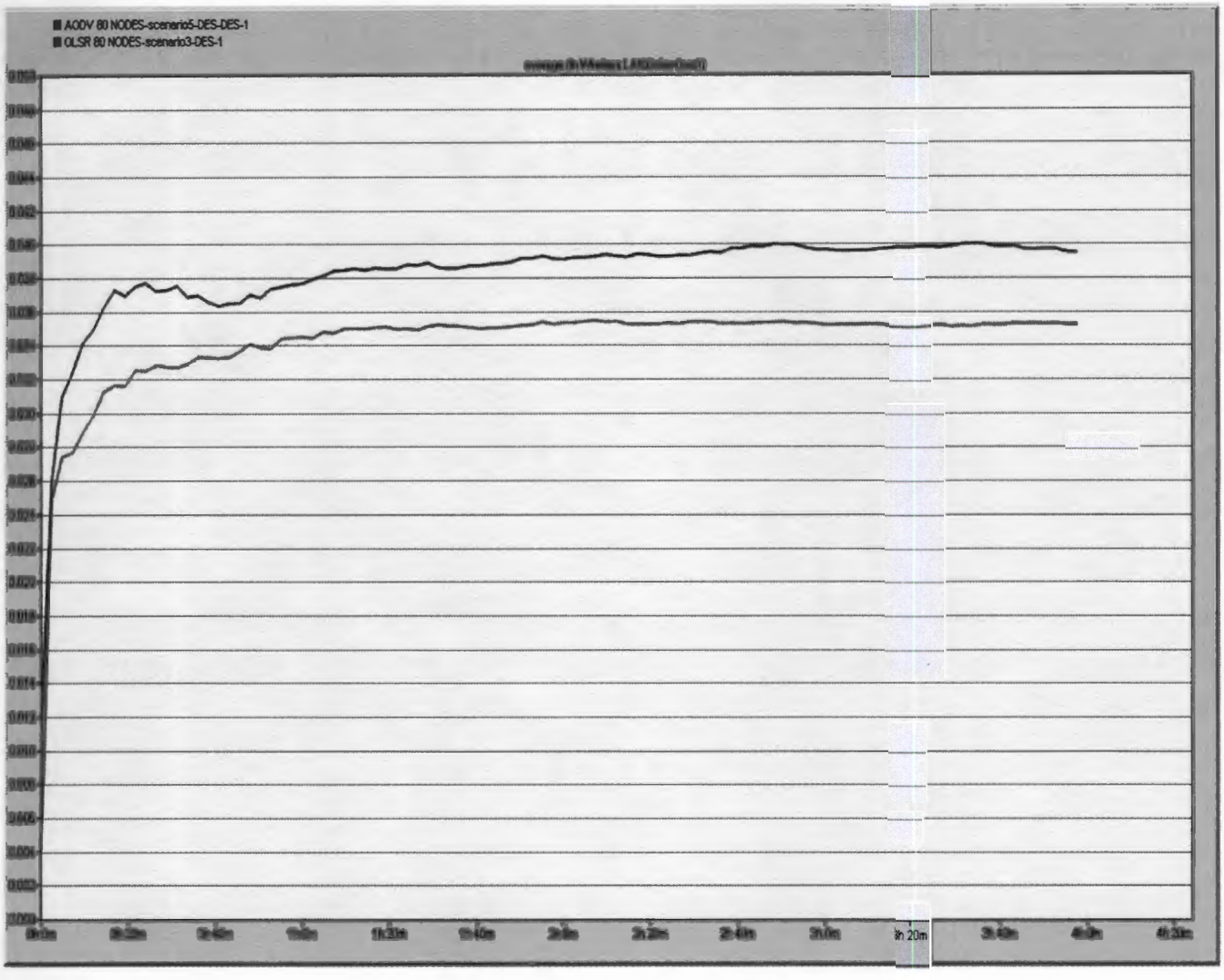

Figure 5.11 Delay in seconds

5.5.3 Data Dropped

In fig 5.12 below, the Y-axis showed data dropped in bits/second and X-axis show simulated time in hours and minutes. Both protocols have sharp rising data dropped increasing during the 18 minutes of simulation. AODV then dropped over time from an average peak of 245 000 bits/second to180 000 bits/second. OLSR showed an average peak routing traffic reception of about 240 000 bits/second after 2 hours of the simulation. Most of the growth happens in the first 20 minutes of simulation. Unlike AODV, OLSR does not decrease the amount of data dropped and thus making AODV better than OLSR in this scenario.

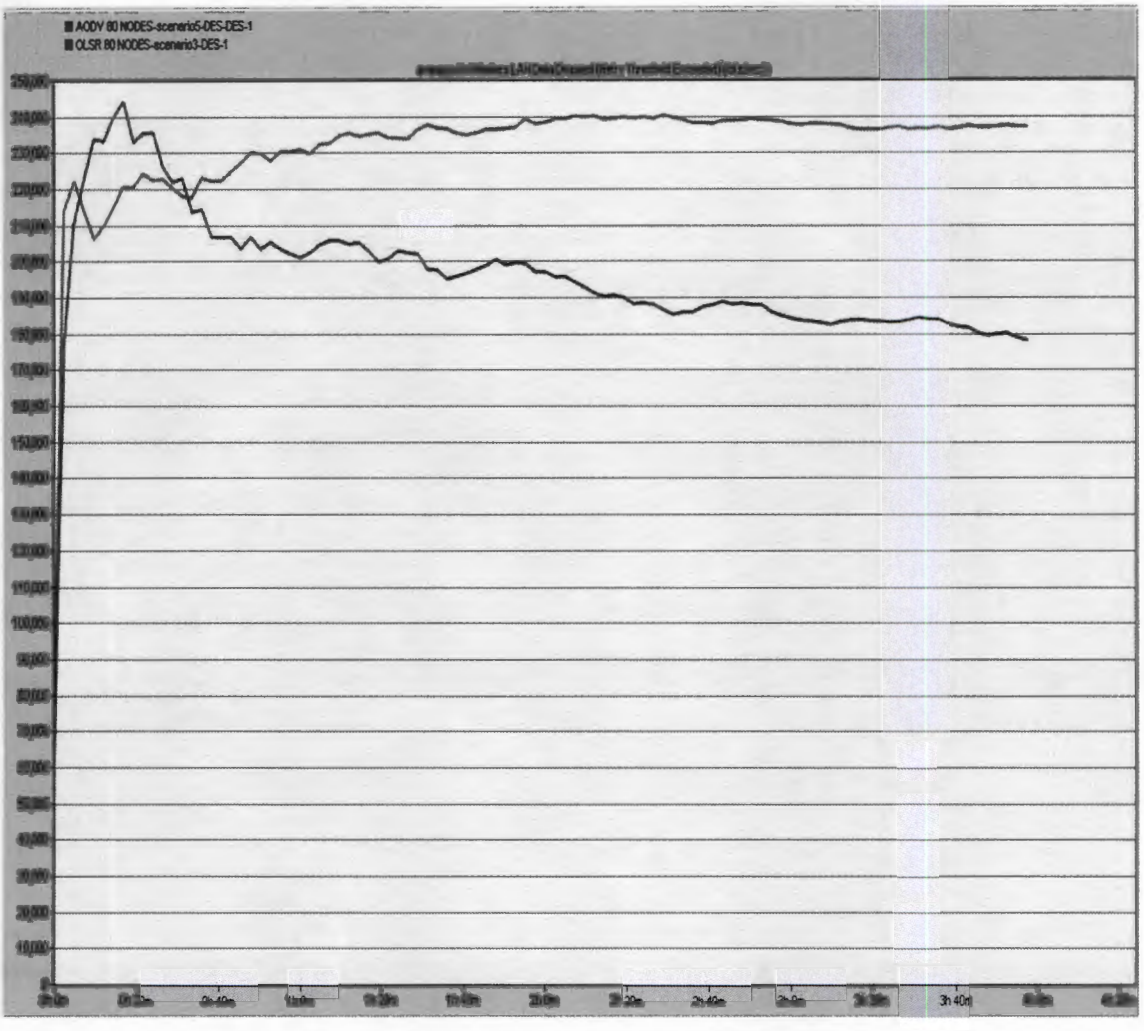

Figure 5.12 Data dropped in bits per second

5.6 Chapter Summary

In this chapter we analyzed, discussed and gave comparison to results obtained. The results obtained are very critical in terms of decision making of whether a particular protocol could be further developed in order to attain trust as well as quality of service in the network. The challenge that remains is within the tool OPNET 14.5 simulator, which limited our study in terms of an inability to provide specific measures in certain protocols and thus limiting us to choose statistics that would be globally analyzed, discussed and compared. For example, OLSR does not provide the measure of total packets dropped but rather packets dropped for individual nodes and this limitation makes it difficult to show those statistics since 80 mobile nodes would require 80 results graphs.

The measures used in this study, however, provided enough results to validate some parts of literature and to bring new findings in terms of quality of service and video streaming applications over MANETs. This evaluation is part of the framework proposed in terms of the application (video conferencing). The results also proved without any doubt that in terms of delay, these protocols perform well. Most of the scenarios had an average delay below the margin of one (1) second which is regarded a high response time in terms of network efficiency.

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Chapter Overview

This chapter takes a brief outlook towards the entire project in terms of the attainment of goals, aims and objectives poised. Conclusions were drawn based on the results obtained and the trustworthiness of our network based on the framework. Furthermore, suggestions were made as to what could be done in future in order to achieve better scaled results. The suggestions for future work are for researchers to study and make possible improvement on the work.

6.2 Summary

The dynamic topology in MANETs has always poised uncertainty in terms of whether these networks can be regarded to be trustworthy. Conclusions in the literature [1, 4, 8, 18] have been drawn that it is difficult to truly attain or rather ascertain trust and quality of service in MANETs because of the topological characteristics it possesses. QoS and trust are two inter-changeably used concepts. This may be because in most instances trust is theoretically evaluated whilst QoS is evaluated through actual experimentation. We presented an application-centric framework and a QoS evaluation was conducted using OPNET 14.5 modeller.

The main goal of this research work was to formulate, design and implement a robust and efficient trust management framework that addresses trust related issues in video streaming applications over MANETs. We believe the results obtained through the QoS evaluation system further propel one to confidently say that as much as it may be difficult to attain trust in MANETs it does not necessarily mean it cannot be achieved. This goal was achieved by running a video conferencing application (high resolution video) in our designed network scenarios to generate traffic in our network. The scenarios presented unique results for each protocol being implemented. In a nutshell after running with our scenarios, we discovered that to maintain quality of service in a wireless network as a whole is quite difficult but also an attainable challenge. This was seen through the results presented in Chapter 5 of this work.

6.3 Conclusion

It can be concluded that AODV showed the best performance for the 20 mobile node scenarios. AODV presented good quality of service in terms of throughput and delay. OLSR, however showed poor throughput, high delay and such is critical in terms of quality of service. At recommendation level, OLSR, in this instance, would be the least recommended protocol for video streaming applications in this category.

For 40 mobile node scenarios, OLSR got the upper hand as it showed the best performance. It had an impressively low delay and a higher throughput as compared to AODV. AODV's throughput flattened after 5 minutes of simulation whilst OLSR maintained a positive and constant measure with time. The delay poised by AODV is higher than that of OLSR and the data dropped by OLSR was lower. It is for that reason we confidently say OLSR performed better in this category.

For 60 mobile node scenarios, AODV showed better performance. This was seen through its high throughput that rose in the first 30 minutes of simulation and then maintaining that maximum value throughout the rest of the simulation. Its delay was higher and dropped data levels were impressively low taking into account the ratio with the end throughput. OLSR had a poor throughput and as such may result into poor video output thus making streaming a challenge.

AODV has the disadvantage of its overhead and OLSR has that of its bandwidth. In terms of efficiency in high node densities and traffic, OLSR will always perform well provided it is given enough bandwidth for continuous topology updates. AODV performs better in static networks as it uses less resources as compared to OLSR.

For 80 mobile node scenarios, OLSR exceptionally outplayed AODV. It had twice the output of AODV and a relatively lower delay. This is at high node densities. The scenarios concluded that both protocols are good for the provision of video traffic. AODV is good at low node densities and OLSR at high node densities. This result answered RQ2 which was looking out for performance in high node densities.

What can be commended from the results obtained is the impressiveness of the network delay. The average delay was less than one second (1 sec). This means that buffering times are at a minimum when streaming the video. One must put it into account that video streaming depends on the connectivity of the device and delivery of video streams on time since lost packets can never be

recovered once lost. This means that video streams that have passed can never be recovered again since everything happens in real time and thus making delay an important aspect of the evaluation. The trustworthiness of the network depends on the QoS evaluated. The programmer has now the ability to determine as to whether the network, through the framework, is trustworthy or not. Based on the results obtained in the various node scenarios, it is safe to say that in this dynamically set network and its natural bottlenecks, good QoS was achieved. The application protocols implemented furthermore made the evaluation process interesting as performance varied.

In conclusion, this study met all its intended objectives and questions answered. Challenges of trust in relation to video streaming applications over MANETs were discussed in the literature survey (Chapter 2). A QoS evaluation was conducted to find out performance in high node densities and this was exhibited through our results as shown earlier on whereby we discovered that OLSR protocol with video conferencing traffic. The impressively low delay in the overall network exhibited means such network is trustworthy and reliable. A correlation between trust and Quality of Service was presented through the formulation of a framework as seen in Chapter 3. The last objective was to implement part of the framework using OPNET Modeller and this was done in our Chapter 5 where a QoS evaluation was conducted. The goal was to make our framework robust and efficient and we believe through the results exhibited it is safe to say such a goal was attained. Topological issues in MANETs will continue to be a performance bottleneck but such bottlenecks do not necessarily mean that a better trust and QoS cannot be achieved.

Trust and QoS may be two different concepts integrated in systems but they aim at achieving similar results. One can argue that if it is enough that the trustworthiness of network should be based on recommendations, direct or indirect trust or even reputation. If that is so, then we can safely agree that QoS is somehow connected to some degree or level of trust that the network performance will be excellent. The involvement of both concepts in our framework was deliberately done to get a view of both mechanisms. The framework mostly dealt with QoS and the involvement of direct trust was entirely left to the application itself and its ability came up with the best result. The Application had decisions to take in terms allowing trust to be intentional. The depth of both integrations may be carried out as future work. Our framework is formulated in a way that QoE can be evaluated as well.

6.4 Future Work

As future work, one may take into consideration the framework proposed and can discover that so much can be done in terms of development of metrics. We aim at conducting a Quality of Experience study whereby we include the users` perspective in terms of perception on the service rendered. Another addition to the framework would be adopting a different type of trust i.e. recommendation-based and perhaps a hybrid trust-based type then compare findings. Our framework provides room for expansion whereby the researcher may improve and get more findings. We also aim at implementing our work on a different tool like NS-2.

REFERENCES

[1] S. Semplay, R. Sobti, and V. Mangat, "Review: Trust management in MANETs," *International Journal of Applied Engineering Research,* vol. 7, p. 2012.

[2] D. S. Aarti, "Tyagi,"Study Of Manet: Characteristics, challenges, application and security attacks"," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 3, pp. 252-257, 2013.

[3] A. Rajaram and D. S. Palaniswami, "A trust based cross layer security protocol for mobile Ad hoc networks," *arXiv preprint arXiv:0911.0503,* 2009.

[4] P. Goyal, V. Parmar, and R. Rishi, "Manet: vulnerabilities, challenges, attacks, application," *IJCEM International Journal of Computational Engineering & Management,* vol. 11, pp. 32-37, 2011.

[5] M. S. I. M. A. Riaz and M. Tariqu, "Performance analysis of the Routing protocols for video Streaming over mobile ad hoc Networks," *International Journal of Computer Networks & Communications,* vol. 4, pp. 133-150, 2012.

[6] G. D. Delgado, V. C. Frías, and M. A. Igartua, "Video-streaming transmission with qos over cross-layered ad hoc networks," in *2006 International Conference on Software in Telecommunications and Computer Networks*, 2006, pp. 102-106.

[7] M. Lindeberg, S. Kristiansen, T. Plagemann, and V. Goebel, "Challenges and techniques for video streaming over mobile ad hoc networks," *Multimedia Systems,* vol. 17, pp. 51-82, 2011.

[8] Y. Singh and M. V. Siwach, "Quality of Service in MANET," *Int. J. Innov. Eng. Technol,* 2012.

[9] N. Sharma, S. Rana, and R. Sharma, "Provisioning of Quality of Service in MANETs performance analysis & comparison (AODV and DSR)," in *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on*, 2010, pp. V7-243-V7-248.

[10] J. Sen, "A survey on reputation and trust-based systems for wireless communication networks," *arXiv preprint arXiv:1012.2529,* 2010.

[11] J. Li, R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks," *IEEE Communications Magazine,* vol. 46, pp. 108-114, 2008.

[12] R. Ferdous, V. Muthukkumarasamy, and A. Sattar, "Trust Management Scheme for Mobile Ad-Hoc Networks," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 2010, pp. 896-901.

[13] T. Phakathi, F. Lugayizi, B. Isong, and N. Gasela, "Quality of Service of Video Streaming in Vehicular Adhoc Networks: Performance Analysis," in *Computational Science and Computational Intelligence (CSCI), 2016 International Conference on*, 2016, pp. 886-891.

[14] I. Ahmad, H. Jabeen, and F. Riaz, "Improved quality of service protocol for real time traffic in manet," *arXiv preprint arXiv:1308.2797,* 2013.

[15] M. Rao and N. Singh, "Quality of service enhancement in MANETs with an efficient routing algorithm," in *Advance Computing Conference (IACC), 2014 IEEE International*, 2014, pp. 381-384.

[16] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," *IEEE Communications Surveys & Tutorials,* vol. 14, pp. 279-298, 2012.

[17] V. Singh and M. Jain, "Secure AODV Routing Protocols Based on Concept of Trust in MANET's," *topology,* vol. 3, 2014.

[18] J. Sen, "A distributed trust management framework for detecting malicious packet dropping nodes in a mobile ad hoc network," *arXiv preprint arXiv:1010.5176,* 2010.

[19] A. M. Shabut, K. P. Dahal, S. K. Bista, and I. U. Awan, "Recommendation based trust model with an effective defence scheme for MANETs," *IEEE Transactions on Mobile Computing*, vol. 14, pp. 2101-2115, 2015.

[20] S. Tan, X. Li, and Q. Dong, "Trust based routing mechanism for securing OSLR-based MANET," *Ad Hoc Networks*, vol. 30, pp. 84-98, 2015.

[21] A. Aggarwal, S. Gandhi, N. Chaubey, and K. A. Jani, "Trust Based Secure on Demand Routing Protocol (TSDRP) for MANETs," in *2014 Fourth International Conference on Advanced Computing & Communication Technologies*, 2014, pp. 432-438.

[22] M. Vinkovits and A. Zimmermann, "TrustFraMM: meta description for trust frameworks," in *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*, 2012, pp. 772-778.

[23] A. Chopra and R. Kumar, "Dynamic Topology Control for Reliable Group Communication over MANETs," *International Journal of Computer Science and Information Security*, vol. 14, p. 296, 2016.

[24] A. Pramanik, B. Choudhury, T. S. Choudhury, W. Arif, and J. Mehedi, "Decentralized topology management on mobile ad hoc networks," in *Communication Technologies (GCCT), 2015 Global Conference on*, 2015, pp. 117-120.

[25] R. Kiefhaber, R. Jahr, N. Msadek, and T. Ungerer, "Ranking of direct trust, confidence, and reputation in an abstract system with unreliable components," in *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*, 2013, pp. 388-395.

[26] S. Xu, P. Guo, B. Xu, and H. Zhou, "QoS evaluation of VANET routing protocols," *Journal of Networks*, vol. 8, pp. 132-139, 2013.

[27] K. N. Qureshi and A. H. Abdullah, "Study of Efficient Topology Based Routing Protocols for Vehicular Ad-Hoc Network Technology," *World Applied Sciences Journal*, vol. 23, pp. 656-663, 2013.

[28] S. Hamma, E. Cizeron, H. Issaka, and J.-P. Guédon, "Performance evaluation of reactive and proactive routing protocol in IEEE 802.11 ad hoc network," in *ITCom 06-next generation and sensor networks*, 2006, p. 638709.

[29] B. D. Shivahare, C. Wahi, and S. Shivhare, "Comparison of Proactive And Reactive Routing Protocols In Mobile Ad hoc Network Using Routing Protocol Property," *International Journal of Emerging Technology and Advanced Engineering. Website: www. ijetae. com (ISSN 2250-2459, Volume 2, Issue 3*, 2012.

[30] V. Saravanan and D. Vijayakumar, "Performance Of Reactive And Proactive MANET Routing Protocols With Trajectories," in *International Journal of Engineering Research and Technology*, 2012.

[31] P. Palta and S. Goyal, "Comparison of OLSR and TORA routing protocols using OPNET Modeler," in *International Journal of Engineering Research and technology*, 2012.

[32] S. Singh, P. Kumari, and S. Agrawal, "Comparative Analysis of Various Routing Protocols in VANET," in *Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on*, 2015, pp. 315-319.

[33] N. S. M. Usop, A. Abdullah, and A. F. A. Abidin, "Performance evaluation of AODV, DSDV & DSR routing protocol in grid environment," *IJCSNS International Journal of Computer Science and Network Security*, vol. 9, pp. 261-268, 2009.

[34] Y. L. Sun, Z. Han, W. Yu, and K. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, 2006, pp. 1-13.

[35] A. Huhtonen, "Comparing AODV and OLSR routing protocols," *Telecommunications Software and Multimedia,* pp. 1-9, 2004.