QUALITY OF SERVICE EVALUATION OF VIDEO TRANSMISSION OVER NEXT GENERATION NETWORKS

FRANCIS LUPIIYA LUGAYIZI

17058198

SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE IN COMPUTER SCIENCE

DEPARTMENT OF COMPUTER SCIENCE
SCHOOL OF MATHEMATICAL & PHYSICAL SCIENCES
FACULTY OF AGRICULTURE, SCIENCE AND TECHNOLOGY
NORTH WEST UNIVERSITY – MAFIKENG CAMPUS

SUPERVISOR: PROF. O.O EKABUA

ARPIL 2012

DEDICATION

I dedicate this achievement firstly to the almighty GOD – the one who gave me the gifts of life, good health, strength, wisdom and courage; above all, the gifts of the Holy Spirit to work through the various challenges this work brought with it. I shall forever remain grateful for the Lord's intervention whenever my morale was down, I will forever trust in you Lord.

Secondly, to my beloved parents – Mr. & Mrs. JMC Kiwanuka for the parental, financial and moral support they accorded me up to now and more especially during this work, may the almighty God continue to reward you abundantly with the gift of life to make you enjoy the fruits of your investments.

In a very special, heartfelt and loving way, with so much love I dedicate this work to my lovely fiancée Kwagala Damalie for the belief, patience, encouragement and moral support she sacrificed to give to me during this work, I shall forever be grateful of her. God bless you my love.

Lastly to my wonderful siblings, Denis, Lawrence, Winnie, Felix, Philip and Joseph-thank you for showing the family love and emotional support, I dedicate this achievement to you all.

ACKNOWLEDGMENTS

I thank God once again for having brought me through my education stages up until this stage of completing my work successfully thus I go ahead to salute all the people the Lord has used to help me through this time.

Firstly, I express a lot of gratitude to the people who have been part of making this whole journey a success; people God chose to do that; my Supervisor Prof. Ekabua for having guided and mentored me so well throughout the stages of this work, may God reward you abundantly and also give us more opportunities to work together in future.

Special thanks go out to the Dean-Faculty of Agriculture, Science and Technology and the Director School of Mathematical and Physical sciences, Prof. Mashudu Maselesele and Prof. Eno Ebenso respectively for having portrayed professional management skills as far as running the Faculty was concerned with regard to the various challenges the faculty experienced during this work, this professionalism channeled well through to our work hence the successful completion. God Bless you both.

In another special way, I would like to thank my big brother Felix who has been a great role model throughout my University experiences, without his support I do not think I would be where I am right now, thank you big brother.

To Mmolooki and Sigweni, who have been my classmates during the two years, thank you for your support especially when it came to troubleshooting my errors in the simulation phase and experiments of my work, thank you gentlemen.

Lastly, from a financial point of view, I thank the North West University Post graduate Bursary for having sponsored all the financial elements of this work, thank you very much.

ABSTRACT

The limitation of bandwidth for multimedia applications in NGNs such as voice and video telephony along with the increasing number of applications on the Internet, service classification and efficient resource management have all become quite challenging tasks. It is for this reason that service quality easily declines in NGNs especially when QoS mechanisms are not carefully scrutinized. In order to handle the different types of applications in the network as a way of improving the service quality in video and voice transmission, there has to be proper efficient resource and traffic management, and using routing protocols is one way in which this can be done. When it comes to real time applications in a network, Open Shortest Path First (OSPF) and Gateway Routing Protocol (EIGRP) are the sought after protocols to manage traffic for these applications. Our study presents an OPNET simulation based comparative evaluation between OSPF and EIGRP for real time applications. We designed three network models that were configured with OSPF, EIGRP and one with both OPSF and EIGRP routing protocols, and then used the QoS parameters of throughput, packet loss, convergence time, packet delay variation and end-to-end delay as our performance evaluation metrics. Our main source of network traffic was a typical video conferencing application. The results from the simulation indicated that combining both EIGRP and OSPF is far better placed to provide reliable Quality of Service than OSPF routing protocol when the main traffic being used in the network is video, but when dealing with a standalone real time application network, EIGRP is better than OSPF.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

3G	3rd Generation
3GPP	3rd Generation Partnership Project
4G	4th Generation
AAA	Authentication, Authorization & Accounting
ANI	Application-to-Network Interface
API	Application Programming Interface
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BGCF	Breakout Gateway Control Function
CSCF	Call Session Control Function
DBD	Database Description
DUAL	Diffusing Update Algorithm
EIGRP	Exterior Integrated Gateway Routing Protocol
HSS	Home Subscriber Server
HTTP	Hypertext Transport Protocol
I-CSCF	Interrogating Call State Control Function
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	Internet Protocol Television
IPv6	Internet Protocol Version 6
IS-IS	Intermediate System to Intermediate System
ISO	International Standards Organization
ITU – T	International Telecommunication Union Telecommunication
LSACK	Link State Acknowledgement
LSR	Link State Request
LSU	Link State Update
MPEG	Moving Picture Experts Group
MRF	Media Resource Function
MRFC	Multimedia Function Resource Processor

NACF	Network Attachment Control Function
NGN	Next Generation Network
OPNET	Optimized Network Engineering Tool
OSI	Open System Interconnect
OSPF	Open Shortest Path First
P-CSCP	Proxy Call State Control Function
PSTN	Public Switched Telephone Network
QoE	Quality of Experience
QoS	Quality of Service
RACF	Resource & Admission Control Functions
RADIUS	Remote Authentication Dial In User System
RESV	Reserve
RTP	Real Time Transport Protocol
S-CSCF	Serving Call State Control Function
SIP	Session Initiation Protocol
TCP	Transport Control Protocol
UDP	User Datagram Protocol
UNI	User Network Interface
VOD	Video on Demand
VoIP	Voice Over Internet Protocol
Wi-Fi	Wireless Fidelity

CHAPTER 1

INTRODUCTION

1.1 Overview

With recent trends and technology advancement in the development of converged broadband next generation networks (NGNs) and advanced multimedia services, the potential has increased for delivering video services to end users "anywhere, anytime" using the World Wide Web. A wide variety of these services exist due to the availability of tools and applications that provide the necessary communications and computer-aided support (e.g., multimedia conferencing/streaming enablers, image analysis and visualization tools, immersive and collaborative virtual environments, etc).

Next Generation Network is an interesting innovation that mainly drives to reduce costs on the side of service providers while at the same time enhancing the capability of a given network to stay open to new services and applications. This innovation basically involves the transformation of public switched telephone networks (PSTN) which are circuit-based networks into packet-based networks that mainly depend on Internet protocol.

The development of NGNs has further led to yet another concept – convergence, this represents the shift from the traditional 'vertical silos' architecture i.e. a scenario where services were provided through different networks (mobile, fixed, IP) to a situation where communication services are accessed and used seamlessly across different networks and provided over different platforms in an interactive way [1]. The biggest driving force behind this has been the Internet.

Converged NGNs deliver different types of traffic across heterogeneous end-user environments [2].For example, video and audio streaming have special bandwidth, loss and delay requirements, in scenarios where data or a video fails to arrive in expected time, play out in a particular application may pause, this becomes annoying to the user. Therefore, in order to meet the requirements of a specific video or audio service traffic delivered over networks in conjunction with other commercial traffic, QoS mechanisms such as class-based traffic prioritization are necessary. The wide variety of video services imposes different Quality of Service (QoS) requirements on underlying networks. One aspect is delay tolerance, with service requirements ranging from strict real-time and delay-intolerant data transmission to delay-tolerant services. In [3], the authors categorize the importance of various QoS parameters for different interactive video services. Prioritization and resource allocation schemes for various types of video traffic delivered over various networks has been addressed in [4]. Further studies have more specifically focused on evaluating support for the delivery of real time video services over high speed 3G/4G networks [5]and other types of broadband networks with evaluation results showing generally reliable performance.

Given any network, quality and quantity of any data sent and delivered to a user is always limited by the quality and quantity which collaborating data transfer systems can support [6]. The general implication of this from the user's perspective is that any application which may rely on the transfer of data is limited by the ability of the data transfer system and protocols in terms of speed, reliability and accuracy.

This calls for all the developers of these applications to have a complete awareness of the impact of these limits, and to develop their systems appropriately. However, the situation becomes complex due to the fact that the available quality of service (QoS) from network to network continues to vary[7], and may also vary in the long run on the same system, all these come as a result of sharing resources between various users[6]. Therefore it is important to take note of the processes by which QoS can be determined, negotiated and varied before, during and after the operation of an application.

1.2 Background Information

A Next Generation Network (NGN) is a packet-based network able to provide telecommunication services to users and making use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent of the underlying transport-related technologies [8]. It enables un-interrupted access for users to networks and to competing service providers and services of their choice. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users. [ITU-T Recommendation Y.2001 (12/2004)]

The NGN is characterized by the following fundamental aspects:

a) Packet-based transfer.
b) Separation of control functions among bearer capabilities, call/session, and application/ service.
c) Decoupling of service provision from network, and provision of open interfaces.
d) Support for a wide range of services, applications and mechanisms based on service building blocks (including real time/ streaming/ non-real time services and multi-media).
e) Broadband capabilities with end-to-end QoS and transparency.
f) Interworking with legacy networks via open interfaces.
g) Generalized mobility.
h) Unrestricted access by users to different service providers.
i) A variety of identification schemes which can be resolved to IP addresses for the purposes of routing in IP networks
j) Unified service characteristics for the same service as perceived by the user
k) Converged services between fixed/mobile
l) Independence of service-related functions from underlying transport technologies compliant with all regulatory requirements. For example, concerning emergency communications and security/privacy, etc.

In our view, limited inconclusive research has been carried out with regards to QoS issues for real time video services in the context of the latest NGN yet Next Generation Networks continue to develop all over the world. The International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) has however continued to keep up with various standard activities in collaboration with regional standards bodies.

The basic features of an NGN are mainly determined from the various challenges experienced by various network operators: for example, the need to provide services over broadband accesses to increase revenue [9], the need to merge diverse network services such as data, telephony, multimedia and emerging Internet services and the desire of customers to be able to access their services from anywhere. This is in contrast to when a network used to provide a specific solution e.g., the PSTN [9] among other challenges that the study shall discuss.

Next Generation Networks are mainly based on IP systems and the infrastructure that these systems come with, for example addressing plans; address assignments, resolutions by domain name servers, applications such as email and the World Wide Web. All these make the NGN entirely IP-based network. The whole concept of Next Generation Networks is all about defining and deploying of networks; these networks are portioned into various layers, planes and open interfaces. By doing this, a platform for both network operators and service providers is created.

In order for services to be developed much more independently from the underlying transport and connectivity considerations, there must be separation between access, service, and communications session controls, which means that the service developers will no longer need to know anything about the type of transport used for the services they are developing [5].

1.2.1 The concept of Network Convergence

Due to the increase in the digital content on the Internet, more and more people, institutions and businesses are shifting their activities to the Internet through creating IP-based networks, applications and services. This is mainly because there has been an increase in access to high-speed broadband, availability of computing power and devices along with the communication media discussed later on in the work. All the above activities have been a major contribution to the utilization of the "convergence" term when discussing next generation networks.

Convergence is seen as a shift from traditional 'vertical silos' architecture i.e. a situation in which different services were provided through separate networks to a situation in which these services are accessed and used seamlessly across different networks and provided over platforms in an interactive way[10].

The different levels of convergence include:

a) Network convergence,
b) Service convergence,
c) Industry/market convergence,
d) Legislative, institutional and regulatory convergence,
e) Device convergence and
f) Converged user experience.

1.2.2 Network Quality of Service

Quality of Service as defined by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Recommendation is the "collective effect of service performance which determines the degree of satisfaction of a user of the service"[6]. As seen earlier on in the previous sections, the next generation networks hosts a wide variety of service applications for multimedia transmission across the networks. All these applications and networks have their own desired level of service standards as far as the users of those applications and the service providers themselves are concerned. This therefore calls for a systematic way of realizing these objectives, and this is mainly achieved through putting in place mechanisms to control network traffic, allocate and manage network resources.

Most researchers believe that QoS is strongly correlated to the main characteristic of a network – its heterogeneity [11]. The next part of this section briefly discusses the key QoS parameters that are used to measure and evaluate a network's QoS otherwise Network Quality of Service as a whole is discussed in detail in the next chapter.

a) Delay (Latency)

This is the total amount of time it takes for a packet to be transmitted from one point in a network to another point in the network [12]. The amount of delay experienced by a packet consists of a minimum fixed part for a given route, and a variable contribution that depends on the network load. The fixed part is the sum of contributions from each processor on the path, serialization on each link, and a propagation delay due to the finite signal velocity over each link [13].

b) Jitter

Jitter refers to the variation in delay over time normally by those packets that are being transmitted in the same traffic flow. Jitter can be measured through using the mean, standard deviation, maximum, or minimum of the inter-packet arrival times for consecutive packets in a given flow [13].

c) Throughput

The amount of packets transmitted through a network at a given time is referred to as throughput. Unlike the bounded delay, throughput is a useful QoS measure for a non-real time application. The QoS level sets the amount of data that will be transferred in a given time [14].

d) Packet Loss Rate

Packet Loss rate is used to determine the maximum number of packets that are expected to be lost within a specified transfer time during the movement of these packets within the network.

In any given network, applications are classified into groups such as data; voice and video. These are further broken down into two main categories; interactive and non-interactive applications. The end-to-end QoS requirements mainly defined by service parameters of loss, delay and delay jitter of any given application may entirely depend on the category in which that application belongs, either interactive or non-interactive. Interactive video applications have the most stringent QoS requirement of 1×10^{-9} packets with a 500 microseconds of delay per switching node. Voice applications on the other hand are more tolerant to loss but less tolerant to delay while data applications are much more tolerant to loss and delay when compared to voice and video applications [15].

The above QoS parameters are further discussed later on in chapter 3. The following sections present the most important issues regarding Next Generation Networks are exposed. Section 1.1.4 discusses the current challenges in Next Generation Networks. In section 1.1.5, some concepts related to NGN architecture are presented. Section 1.2 presents the NGN core and access networks while section 1.3 finally, introduces us to the IP Multimedia System and IP QoS setting scene for the rest of the thesis work since it is regarded as the "heart of NGNs".

1.2.3 Next Generation Network Challenges

Next generation networks are meant to support a wide variety of network traffic services and user mobility that is constraint free at the same time ensuring that there is a guaranteed Quality of Service for users at any given time and anywhere. However this doesn't come cheap, there are quite a number of challenges that need to be addressed. The sub-section below discusses some of these challenges in brief.

a) Application Traffic Types

The diverse nature of network traffic comes with a recognized challenge to any network engineer in their quest to guarantee quality of service to the users of that network in terms of Quality of Experience. In multimedia traffic, there are mainly two types of network traffic - real-time/interactive and non-real time. Examples of real time/interactive traffic are video and audio while file downloading is an example of non-real time traffic. Network traffic from real time/interactive applications are very sensitive to delay, whereas those applications that are non-real time may not have strict delay requirements, although they do not accommodate errors at the same level as the real time/interactive applications. One of the major aims of any network is to sufficiently meet the quality demands of all classes of applications and therefore guarantee Quality of Service in these applications.

Therefore the major requirement of a next generation network is the ability to support a wide variety of services and applications with their respective traffic features, for instance diversity in delay and requirements in bandwidth.

In summary, due to the evolving diversity in network traffic types, QoS provision within next generation networks is a real challenge, thus many researchers are now apportioning more resources to this cause and this is also one of the major aims of this thesis, though the slight difference here is that this thesis focuses on real time/interactive QoS video transmission over next generation networks.

b) Traffic Characterization

Traffic characterization is a way of dealing with traffic flow by determining its impact on the general performance of the network. The biggest concern for network engineers here is controlling data burstiness and the network characterization itself. Data burstiness is part and parcel of the different IP Networks' patterns. A simple example of data burstiness or bursty applications can be in web browsing and email traffic as these applications tend to hibernate for a short period of time and eventually send out a burst data. Much as the area network traffic modeling and characterization continues to become a research area of concern, this thesis doesn't proceed to venture into this area.

c) Protocol Specific

Next Generation Networks are IP based which means that they mainly rely on core network protocols. Much as Internet protocol may guarantee more scalability than ATM, it does come with various challenges. One of the main problems is the QoS provision [16]. The Internet Engineering Task Force (IETF) working group is further evaluating and analyzing the various ways that QoS on IP can effectively be implemented.

d) Costing

One of the objectives of NGNs is to minimize on communication costs but there is always going to be a challenge of higher bandwidth costs and transmission rates. This is yet another challenge that various researchers are putting their heads together to strike equilibrium of service costing without affecting the QoS and the users at large.

e) Network Capacity

The evolution of telecommunication networks was fuelled by the demand for higher capacity. The continued upward trend in technology especially in telecommunications has further increased the rate at which multimedia applications are being developed. All these applications have a desired amount of bandwidth to ensure efficiency in service. Therefore, Next Generation Networks need to be able to meet the bandwidth capacity of the various multimedia applications. If all these factors are to be considered (which is always the case), then network designers and programmers are faced with many challenges especially when it comes to traffic engineering and network dimensioning.

f) Mobility Management

As slightly highlighted earlier on, heterogeneous networks have to promote mobility. The issues of global mobility in the core IP network are being solved by the introduction of the Mobile IP protocol [17] but Mobile Internet protocols also come with their own challenges for example triangular routing, and duplication of IP fields ("IP within IP") Researches have emphasized that in mobility, the handovers from different cells should be properly handled to maintain the desired QoS [17].

g) Scalability

Scalability may also mean the degree of adaptability to a particular force of demand, thus the challenging question network engineers have to ask themselves is - will the network be able to support an increase in the number of users at any given one time? This is entirely because the number of people using telecommunications has continued to increase thus the NGN should be able to meet the demand without affecting the Quality of Service.

h) Heterogeneous network Compatibility

A reliable next generation network should be compatible with different types of networks currently in use and must have provision for future developments. Diversity in a network comes with key issues that shouldn't miss mentioning, and these include:

- Mobility management within applications of these networks.
- Compatibility with other networks.
- Secure interworking within access networks.
- End-to-end QoS of service guarantee to users of these networks.

Various research groups are addressing the compatibility issues for the networks to work together [18].

1.2.4 Next Generation Network Architecture

Next Generation Networks are mainly based on IP systems including the infrastructure that these systems come with, for example addressing plans; address assignments, resolutions by domain name servers, applications such as email, and the World Wide Web. All this makes the NGN entirely IP-based. The whole concept of Next Generation Networks is all about the defining and deploying of networks. These networks are partitioned into various layers, planes and open interfaces. This kind of order creates a platform for both network operators and service providers to create, develop and maintain services on a much more independent, underlying transport and connectivity considerations. The basic principle behind the NGN infrastructure looks a lot like the IP-based communication as present in the Internet infrastructure [8]. The most outstanding feature of NGN architecture is the recognized separation of the service – related functions and the transport infrastructure. For example, services such as IPTV networks, telephone networks, video conferencing and IP telephony etc have their own network infrastructure, but in NGN architecture all these services are integrated within one network. The biggest advantage of such a structure is that many companies have that freedom to develop many services and charge per those services rather than charging for the whole network. This is advantageous to those users who want a specific service, thus they only pay for only the services they are accessing. The other possibility is that the service providers are able to create services over a wide variety of platforms such as wired, wireless and mobile among others.

The other key highlight in the NGN architecture is general mobility; a user within this network architecture is able to hop from one connection to another freely and alternatively from one network to the other but while being able to stay in access for any subscribed services.

The NGN architecture is formalized in ITU-T Recommendation Y.2011; it mainly highlights the Service and Transport Stratums. Figure 2.4 is from ITU-T Recommendation Y.2012 and basically reflects the different portions of each strata and it does also show the interactions between these parts.

The functions that connect a particular user to the NGN is known as the user-to-network interface (UNI). If there is any process involving connection between two networks, the network-to-network (NNI) interface is invoked. The diverse nature of user equipment and gadgets calls for a straight forward establishment of the NNI and UNI but this has to be done without destabilizing the main business paths and points within the NGN architecture. And lastly, the application-to-network interface (ANI) is the bridge between the NGN environment and third party application providers.

A typical NGN use case scenario would be; users have to connect their network to the NGN itself and this is made possible through the assistance of network attachment control function (NACF). After this connection is fully authenticated and established, the Resource and Admission Control Functions (RACF) receives an access request from the particular application trying to access the services. These functions then make the decision to either accept or reject the request based on set parameters or resource availability.

The main purpose of the management functions is to promote security, carry out network diagnostics and billing; it is mainly used during the 'subscription stage' of accessing services within the NGN environment.

Lastly, the end-user functions are mainly tasked with controlling end-user equipment in terms of access to the NGN. This is made possible through the availability of physical and functional interfaces. Basically it is the gateway that end users go through to connect to the entire network. The sections that follow further describe the main portions of the NGN environment, mainly; The Transport, Service, Application and Management planes.

a) Transport Plane

The Transport plane provides connectivity for the various components and physically separate functions within the NGN. IP is considered as the most promising transport technology for Next Generation Networks [20].This means that the transport plane is able to provide IP connectivity for both end-user equipment outside the NGN controllers and enablers that usually reside on servers inside the NGN [21]. Considering IP network characters, it can be said that some of them comply with NGN features, for example:

- Independence of protocol layers.
- Separation of transport resources from call control.
- Service portability over a given access network.
- Use of a packet transport to support every service (data, voice).

The transport plane is responsible for providing end-to-end QoS, which is a desirable feature of the NGN [22]. The transport plane is divided into access networks and the core network, with a function linking the two portions. The functional entities in this plane include; access functions that manage the end-user access to the network. These functions are specifically access technology dependent. The other functional entities are the access transport functions which are responsible for transporting information across the access network but they also provide QoS control mechanisms dealing directly with user traffic, including buffer management, queuing and scheduling, packet filtering, traffic classification, marking, policing and shaping [3]. Edge Functions are the other functional entities, these are used for traffic processing when access traffic is merged into the core network. The Core Transport Functions on the other hand are the entities responsible for ensuring information transport throughout the core network. They provide the means to differentiate the quality of transport in the network according to interactions with the transport control functions [23] and lastly the gateway functions are the ones that provide capabilities to interwork with other networks, including many existing networks, such as PSTN/ISDN-based networks and the Internet [24].

b) Service Plane

The main purpose of the service control plane is to house the various functions to provide control on the transport plane and also manage the accessing process to the application plane. In previous studies, a number of subsystems have been proposed by standard organizations for the control plane and among them is the IP Multimedia Subsystem (IMS) standard by the Third Generation Partnership Project (3GPP) whose main focus is to provide service architecture to support Internet services as well as legacy service. The Functions in this plane include authentication and authorization functions, registration functions, and session control functions [22].

c) Application Plane

Next Generation Networks support an open development environment based on an Application Programming Interface (API), which will enable service providers, third party application developers, and potentially end users to create and introduce applications quickly and seamlessly [25]. Service providers have more control over the service introduction process and hence there is a possibility of reuse of existing application components, this is entirely made possible because the speed and nature in which applications are introduced [26]. In the long run it basically opens up opportunities for creating and delivering services to a broader audience.

d) Management plane

One other fundamental to operating an NGN is assured support for network management. Management functions enable the NGN operator to manage the network and provide NGN services with the expected quality, security, and reliability.

These functions are allocated in a distributed manner to each functional entity. They interact with network element management, network management, and service management functional entities. The management functions include charging and billing functions. These functions interact with each other in the NGN to collect accounting information, which provides the NGN operator with resource utilization data enabling the operator to properly bill users. The charging and billing functions support the collection of data for both later processing (offline charging) and near-real-time interactions with applications such as those for prepaid services (online charging).

1.3 Problem Statement

The necessity of QoS is one of the key issues that have to be considered when designing and analyzing the performance of Next Generation Networks. The limitation of bandwidth for multimedia applications in NGNs such as voice and video telephony along with the increasing number of applications on the Internet, service classification and efficient resource management have all become quite challenging tasks. It is for this reason that service quality easily declines in NGNs especially when QoS mechanisms are not carefully scrutinized. In order to handle the different types of applications in the network as a way of improving the service quality in video and voice transmission, there has to be proper and efficient resource and traffic management. For this to be possible there must be a mechanism to manage the resources and also handle the traffic in the most efficient way possible within the network [22].

Traffic routing in a network is one way Quality of Service may be implemented. Routing is a process where routers in a network specify paths that the various packets should follow during transmission across the Internet [27]. Routers and Routing protocols are at the center of this process; the latter are the various rules that specify how the routers are going to communicate with each other by disseminating data. There are quite a number of routing protocols widely in use in the telecommunication industry, this work concentrates mainly on Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) as one of the ways of evaluating video transmission QoS in Next Generation Networks; this is mainly because they are the pre-eminently considered protocols for video transmission in a network [27].

Streaming video across networks is a sensitive process because of the compulsory need of providing quality of service to the parties involved in most cases the receiver of the service; this is mainly because if there are drops in packets during streaming, the final quality of the video at the receiver's end is greatly affected. There are many studies that have endeavored to investigate how to implement QoS mechanisms in a given network, either with the receiving devices themselves or at the various areas of the OSI model, but there is little known that has been done concerning the Quality of Service, therefore our work is concerned with the Quality of

Service during the streaming and routing process, hence our further concentration on the router, routing and routing protocols of which all this happens at the network layer of the Open Systems Interconnection (OSI) model.

A network simulation package called Optimized Network Engineering Tools (OPNET) modeler has been used in the simulation phase of this study. OPNET is considered to be the industry's leading simulator that is specialized for network research and development [28]. OPNET allows network designers to develop and study the behavior of the various communication networks, devices, protocols, and applications with great flexibility [28].

1.4 Research Goal

The main goal of this research work is to evaluate Quality of Service of video transmission over next generation networks using Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing (EIGRP) as a way of enhancing efficient and effective video traffic management.

1.5 Research Objectives

In order to achieve the main goal of this research, we shall employ the following research objectives (RO).

RO1: A study of the key concepts, architectural components and challenges of NGN networks.

RO2: Analyze video traffic QoS and transmission over NGNs.

1.6 Research Limitation

The scope of this study is limited and concentrates mainly on QoS in routing video traffic hence the choice of two routing protocols i.e. Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) since these are the protocols that facilitate and provide QoS to next generation network applications whose main activity is streaming video across a network.

1.7 Research Methodology

The various research methods used in this research are presented in the following section.

1.7.1 Literature Review

The research began with a detailed research literature review during which the various concepts in next generation networks were presented along with the related works to this research. A further study was carried out mainly on routing protocols used in next generation networks to transmit video traffic across these networks. This study created the backbone of the experimental phase of simulating the chosen routing protocols.

1.7.2 Network modelling and design

Three network models were designed; two had different routing protocols and the third simply was relying on the two protocols combined together or being used simultaneously.

1.7.3 Network Simulation

The network models in section 1.7.2 were fully implemented with the help of a video conferencing application as the main source of traffic for the various network models. A simulation time of 3000 seconds was set on all the models.

1.8 Research Contribution

The main contribution of this is to assist network developers and designers in clearly choosing the most appropriate routing protocol when it comes to designing video applications networks especially if the applications in question are to be deployed in a next generation network environment.

1.9 Chapter Outline

As a secondary deliverable of this work research work(extracted from the results obtained from this thesis) is paper presented and published in the proceedings of the 11th International Conference on Wireless Networks(ICWN'12: July 16-19,2012 Las Vegas,USA).The title of the paper is *"Evaluation of Video Transmission Quality of Service over Next Generation Networks"*.

1.10 Chapter Summary

This chapter presented an overview and general background of this research work. The chapter gave a general understanding of the work and in brief, a presentation on the problem statement, research goal, research objectives and the research methodology was given as way of linking to the chapter 2 which is the literature review.

The remainder of this research work is organized as follows:

Chapter 2 presents the literature review of the research work. In this chapter the IP Multimedia System – a backbone of next generation networks is analyzed. The chapter also presents the various works that have been done on routing protocols in next generation networks and Quality of Service routing in next generation networks. The chapter concludes by presenting the main protocols under the research study.

Chapter 3 introduces the concept of video streaming in networks. This chapter also explains the preliminary work done before the implementation and simulation of the network models described in chapter is done.

Chapter 4 presents the simulation environment of this work as a whole. The chapter also briefly describes the OPNET simulator.

Chapter 5 concludes the entire thesis and future work is briefly presented.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter introduces the literature and related work surrounding the back bone of next generation networks – The IP Multimedia Subsystem. The chapter also presents the main IP QoS models and protocols. The chapter concludes by analyzing QoS routing in next generation.

2.2 Overview

The evolution of the Internet-mainly a packet switching network and the telephony (circuit switching technology) led network researchers to bring about ways of converging the two. This new concept of network convergence has developed over the last few years and has been labeled Next Generation Networks (NGN) [29]. Lately, there are new tele-services and applications that have become strong drivers for progress and thus come with new requirements for network designing and construction. In order to implement such kind of network architectures, there is a set of protocols and traffic – related mechanism that needs to be adhered to or invented. Of late, 3G networks continue to evolve, thus it is only fair to ask what 4G or NGNs should or might be able to do. Because of the ever evolving nature of technological innovation the answer to this question is yet to become so clear, but the current trend is to view Next Generation Networks as a new technological paradigm shift for the telecommunication industry, thus from mobile to fixed networks. The biggest anticipation is that Internet access and Internet Protocol (IP) multimedia applications will become value-added and high revenue services for telecommunication networks. The continuous upward trends of technology in the development of converged broadband next generation networks (NGNs) and advanced multimedia services has increased the user expectations on the delivery of multimedia services to end users "anytime, anywhere "with a desirable degree of Quality of Experience(QoE) anticipated. Converged NGNs are being designed to deliver different types of traffic across heterogeneous end-user environments.

2.3 Related work

To deliver multimedia that is being referred to previously, there are various requirements that have to be met especially for specific real-time/interactive video service traffic delivered over networks in conjunction with other commercial traffic (e.g., voice calls, streaming multimedia, and Internet traffic). QoS mechanisms such as class-based traffic prioritization and effective IP routing protocols are necessary. The wide variety of multimedia and video services imposes different Quality of Service (QoS) requirements on underlying networks. One aspect is delay tolerance, with service requirements ranging from strict real-time and delay-intolerant data transmission to delay-tolerant services. In [10], [8] [9], [30][30][13], [14], the authors categorize the importance of various QoS parameters for different interactive video services. Prioritization and resource allocation schemes for various types of video traffic delivered over various networks have been addressed in [9, 31]. Further studies have more specifically focused on evaluating support for the delivery of real time video services over high speed 3G/4G networks [32],[6, 33] and other types of broadband networks [34], with evaluation results showing generally reliable performance.

The research community has continued to carry out various investigations on new approaches, methods, strategies, techniques and tools for analyzing, designing, controlling and evaluation of future Next Generation Systems that support user interworking of multimedia applications and their mobility. Emphasis is now being given to QoS and its related aspects both in access and core networks in the presence of multimedia traffic, as [35] suggested. The real question above all is, how can we evaluate QoS of service especially in an instance where it is impacted by an unexpected event? This may sound pretty an easy question to answer but that isn't the case. We do not differ so much from [35] , when he stated that "the only good reason to measure anything is to reduce uncertainty with respect to some course of action that must be decided". Basically in 2001, Hardy proposed and presented a method where he analyzed QoS using two processes, mainly measurement and evaluation. In our study we focus more on evaluating the performance of two routing protocols based on selected metrics, we also evaluate these protocols but from a network routing point of view. Routing is part of network traffic engineering, the major objective of the latter is to ensure and improve network performance at the same time maintain the QoS requirements by optimizing network resources. One way this can be done is through the application of efficient IP routing protocols that will enhance the general performance of the network especially when it comes to QoS of the various multimedia applications.

2.4 Analysis of IP Multimedia Subsystem

The IP Multimedia Subsystem (IMS) is a set of specifications that describes the Next Generation Networking (NGN) architecture for implementing IP based telephony and multimedia services [36]. Without the presence of IMS, it would be entirely difficult or near to impossible to converge voice, video, data and mobile network technology over an IP-based infrastructure. The system is designed in such a way that it favors a gradual movement of any existing core infrastructures to the new Internet Protocol framework which facilitates a much easier and minimal cost of launching new services, reduce operating costs while remaining in a position to provide benefits to users and service providers. In order to enable person-to-person and person-to-content communications, IMS uses a layered architecture in which service enablers and common functions can be reused for multiple applications [37].

In the IMS, network operators and service providers control access to the networks and services respectively, all for which customers are billed for the accessed service. This is in contrast to the usual Internet model, where the network is transparent and all services are provided by endpoints. As a result of a more controlled environment, users get an improved experience with managed QoS, single-sign-on security, and customer support, at least in theory [38].

2.4.1 IMS Architecture

After telecommunication network developers realized the need to move away from the vertically integrated service silos, the IMS architecture became one strategy that was to provide and promote horizontally integrated services architecture. The IMS provides common functionality that is specific to a particular service [39].It is generally a service provision architecture platform framework in next generation networks. The service architecture of IMS is based on a collection of logical functions that may be organized into 3 layers as shown in Figure 2.1 [40].

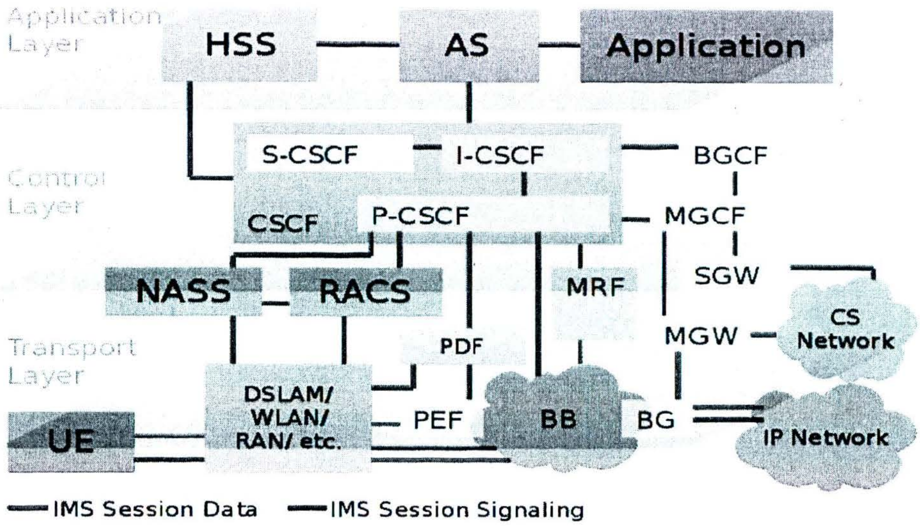

Figure 2.1: Overview of IMS architecture

a) The Application Server Layer:

This layer mainly depends on application and content servers which it uses to provide value added services. The main parts that form the core of this layer are application servers (AS), the Multimedia Resource Function Controller (MRFC) and the Multimedia Function Resource Processor (MRFP). The main purpose of the AS layer is to allow services to be built based on the bearer services and the call control services of the other two layers [41]. Besides supporting legacy services, it can be used to provide novel non-telephony services [10].

b) The Session Control/Signaling Layer:

This mainly contains the call control functions that enable endpoints to be registered with the network and calls to be setup between them [42]. It also contains the functions that control the media gateways and servers so as to provide the requested services. The main elements in this layer are the Call Session Control Function (CSCF) which provides end-point registration and routing of SIP signaling messages [42].The other element is the Home Subscriber Server (HSS), this acts as the database used to store subscriber service profiles and service triggers.

c) **The Transport and Endpoint Layer**:

This layer is responsible for initiating and terminating the signals that are needed to setup and control sessions, it also provides bearer services between the endpoints. IMS signaling is based on the Session Initiation Protocol (SIP) on top of IPv6 [41].

2.4.2 IMS Components and Entities

The main IMS key functionalities and entities are categorized in 6 ways. These are, call session management and routing functions (CSCFs), databases (HSS,SLF), interworking elements (BGCF,MGCF etc), services (AS,MRCF,MRFP), support entities (THIG,SEG,PDF) and charging [43].

2.4.2.1 Proxy Call State Control Function (P-CSCP)

This is the first contact point within the core network of the IP Multimedia system.

The P-CSCP acts as an inbound/outbound SIP proxy server that is all requests initiated by the IMS terminal or destined to the IMS terminal pass through P-CSCP[44].It also is responsible for security of all messages between the network and user.

2.4.2.2 Interrogating Call State Control Function (I-CSCF)

The I-CSCF presents functionally of a SIP proxy server located at the edge of an administrative domain. It retrieves user location information and routes it to the appropriate destination, typically an S-CSCF [45]. Basically it acts as a contact point within an operator's network for the various connections destined to a subscriber of that particular network operator.

2.4.2.3 Serving Call State Control Function (S-CSCF)

This is a SIP server that performs session control. It also acts as a SIP register and maintains a binding between the user location and the user's SIP address of the record (also known as public user identity) [46]. It also carries out user registration and interaction with the various service platforms mainly for the support of services.

2.4.2.4 Application Server (AS)

The AS (Application Server) mainly hosts and executes IP Multimedia Services. For example several services like telephony and messaging can be hosted in a single application server [46]. Different services in a single application server reduce the workload of CSCF in the control layer [44].

2.4.2.5 Media Resource Function (MRF)

This provides the source of media in the home network. It is divided into two parts; one is the signaling plane node referred, as Media Resource Function Controller (MRFC) and the other is media plane node referred as Media Resource Function Processor (MRFP) [47].

2.4.2.6 Breakout Gateway Control Functions (BGCF)

The BGCF is a SIP server that incorporates routing Functionality based on telephone numbers [48]. It is only used in sessions that are initiated by an IMS terminal.

2.4.2.7 Home Subscriber Server (HSS)

This is the master database of the IMS. The main objective of the Home Subscriber Server (HSS) is to provide a central repository for subscriber information in IMS architecture [39]. It basically acts as a store for all subscriber information necessary to handle sessions between users and provides service to subscribers [47].

2.5 IP Quality of Service Models

The original promise behind the Internet Protocol was to deliver data from a sender to the receiver using a best-effort approach [49] , which basically implies that a protocol doesn't guarantees the arrival of data but that it tries as much as possible to deliver this data to its intended destination.

In the past, IP networks were supporting public Internet services such as e-mail and general web access. One thing about these services is that they are not of critical importance with regard to timing and basically have no stringent requirements for packet loss or delay for that matter. As earlier on indicated in this study, the Internet is evolving into a next generation network hence supporting many "time-critical applications" along with other best effort services. This development has however come with a challenge in deploying QoS architectures and mechanisms that support the effective delivery of services in IP networks with the perceived quality. The IETF has defined different IP QoS architectures; the most prominent among them are the integrated services QoS architecture, and the differentiated services QoS architecture [50]. These models are further discussed in the various subsections of this chapter.

2.5.1 Best Effort Service Model

The best-effort service is considered to be the backbone of Internet networking and its protocols, and this is what has made IP scalable to networks the size of the Internet [51]. However, this model comes with its own challenges to network operators and designers especially those who may prefer to guarantee their customers the most desired quality of the service they offer. This model mainly states that each node in the network will make an attempt to deliver each packet of data to its destination within a reasonable time, but it makes no guarantees at all [51]. Of course packets may get delivered but on another day nothing may be delivered. The other set back that may happen is that the packets always get re-arranged, therefore one has no guarantee that these packets will be re-arranged and received in the same order that they were sent in the first place. Technically, this means that there is a lack of QoS thus, the chances of service unavailability, packet losses and abnormal delays are bound to prevail.

Therefore, to ensure that QoS is provided with the best effort service model is over dimensioning of the network resources. This is to limit the probability of routers congesting, and thus delays remain small and packet loss does not occur [52].

Much as this model is considered to be one of the easiest ways to implement QoS in a network, it is not a very feasible solution because of the growing types and variety of network traffic, yet another reason for this study's focus routing protocols.

2.5.2 Integrated Services Model

Having looked at the best-effort service model, the Integrated Service model (IntServ) was designed to supplement the latter rather than replace it. IntServ defines a framework for providing end-to-end services [53] and this model is mainly responsible for providing services for end users. It is suitable for simple networks and works per flow basis [54].The IntServ based architecture relies on Resource Reservation Signalling Protocol (RSVP) to pass QoS information from the sender to the receiver [53].

RSVP is used to occupy the network resources for the users. The resource with highest priority is served first; the lowest priority gets low opportunity [53].

2.5.3 Differentiated services Model

"Differentiated services enhancements to the Internet protocol are intended to enable scalable service discrimination in the Internet without the need for per-flow state and signaling at every hop. A variety of services may be built from a small, well-defined set of building blocks which are deployed in network nodes." This is the first paragraph in the first official document related to the DiffServ Model [55].Thus as far as customer service is concerned, scalability and flexibility are the main building blocks of the QoS of any given customer centred application in a network. The main goal of this model is to provide quality of service and service differentiation in IP networks [56]. The principle behind DiffServ is that the architecture of the whole model is kept simple as much as possible thus making it much more possible to differentiate services in a single direction only. Compared to RSVP, DiffServ is sender orientated, which means that the traffic sender is responsible for the QoS of the transmission [57].

2.5.4 Overview of Protocols used in the IMS

The IMS is mainly based on Internet Protocols defined by IETF, basically the Session Initiation protocol (SIP), Authentication, Authorization and Accounting protocol and Real-time Transport Protocol (RTP).

2.5.4.1 Session Control Protocol.

SIP is the protocol that establishes and manages multimedia sessions over IP networks. SIP makes it easy to create new services. Since SIP is based on HTTP [58], SIP service developers can use all the service frameworks developed for HTTP, such as CGI (Common Gateway Interface) and Java servlets [58].This protocol also supports caller and "callee" call authentication and authorization.

2.5.4.2 The AAA protocol.

In addition to the session control protocol there are a number of other protocols that play important roles in the IMS. Diameter is chosen to be the AAA (Authentication, Authorization, and Accounting) protocol in the IMS [59]. Diameter is an evolution of RADIUS (Remote Authentication Dial in User Service), which is a protocol that is widely used on the Internet to perform AAA functions within the IMS architecture.

2.5.4.3 RTP (Real-Time Transport Protocol) and RTCP (RTP Control Protocol).

These protocols are used to transport real-time media, such as video and audio and also support end-to-end delivery of real-time data. RTP also provides QoS monitoring (but doesn't address resource reservation or QoS guarantees) using RTCP [60].

2.6 Routing Protocols and IP Routing

Routing protocols are sets of rules that routers use to communicate with other routers as far as information dissemination is concerned in a network. Based on various routing algorithms, the router is able to constantly have prior information of all other routers connected to it. With the success of this arrangement, a routing protocol is in position to share information among its neighbors and throughout the whole network.

According to [61] the major objectives of routing include:

a) To communicate between routers;

b) To construct routing tables;

c) To make routing decisions;

d) To learn existing routes and

e) To share information amongst neighbor routers.

Therefore, IP Routing involves the process of moving packets across the Internet from a source to a destination and making this routing decision is achieved by using a router which provides the physical connection between networks. The router has to be set up with the appropriate mechanisms to facilitate reliable communication with fellow routers and through the network itself. The routing mechanisms in discussion here are either static, dynamic in nature or can be a combination of the two. This will further be explained later in this chapter.

Routers use what is known as routing tables to determine the best path between source and destination after the destination address has been identified [62].

The routing process basically involves two different tasks, of which the tasks are also based on the applications in question.

These are:

1. First, the paths for the transmission of packets through the Internet should be defined; and
2. Packets are then forwarded based on the paths which have been defined [63].

2.6.1 Features of Routing Protocols

In [61] the authors presented the following as the main characteristics of routing protocols:

a) **Convergence.** This refers to the time it takes all the various routers in a network to share specific information, and this time should always be at a minimal.
b) **Loop Free.** This feature highlights the importance of routers staying free of loops, and also helps in acquiring the needed bandwidth for data transmission.
c) **Best Routes.** This characteristic is about the protocol selecting the best path to the destination network.
d) Lastly, the protocol has to be secure, meaning it has to ensure a secured transmission of the data to a given destination.

2.6.2 Routing tables

Routing tables are data stores found in all routers and they mainly have a list the various information and statistics of a given route to a destination and where data packets may be destined to during transmission. This information may be a list of all networks and sub networks known to the router and the address of the next hop router as Table 2.1 shows. The main purpose of routing tables is to assist the router in determining the best path that may exist between a source and destination whenever a datagram is to be forwarded. It is very important to maintain information in the routing table once a router has been able to build one and such maintenance can be achieved by either manual configuration or by the use of dynamic routing protocols [64].

Table 2.1: Example of a routing table for an average computer using a domestic router

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.100	10
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.0.0	255.255.255.0	192.168.0.100	192.168.0.100	10
192.168.0.100	255.255.255.255	127.0.0.1	127.0.0.1	10
192.168.0.255	255.255.255.255	192.168.0.100	192.168.0.100	10

2.6.3 Autonomous Systems (AS)

Autonomous systems are a collection of routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet [65]. These systems basically may have multiple routing domains. The routing domains referred to in Figure 2.2 are a collection of networks and sub networks that are associated with routers that are running the same routing protocol. The two types of autonomous routing protocols include; Intra-Autonomous Routing Protocols and Inter-Autonomous Routing Protocols [66] .

2.6.3.1 Intra-Autonomous Routing Protocols:

These protocols are also known as Intra-domain routing protocols. These are protocols used in configuring and maintaining routing tables within an autonomous system (AS).The other name used to refer to these protocols too is Interior Gateway Protocols (IGP)

2.6.3.2 Inter-Autonomous Routing Protocols:

These are the protocols used for forwarding packets to other Autonomous Systems. They are also called Inter-domain routing protocols or Exterior Gateway Protocols (EGPs).

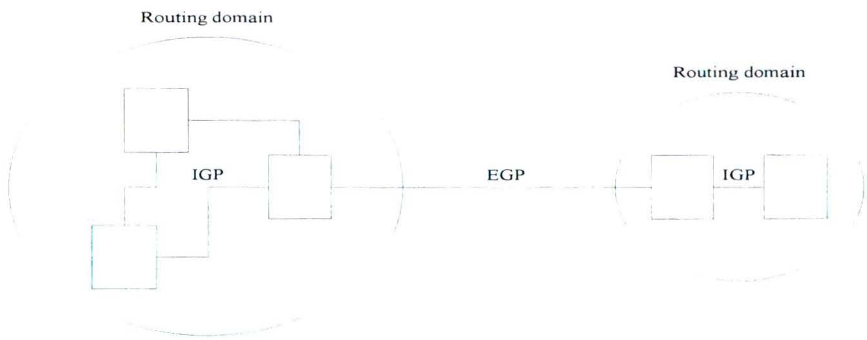

Figure 2.2: Interior/Exterior Gateway Protocols

2.6.4 Routing Mechanisms

In any network, the router always has to have updated information concerning the various paths available for use when the need to send datagrams from source to sender arises. But the question is; how does the router learn about these paths to the various destinations? Well, the router employs quite a number of routing mechanisms that can be used as input sources during the time when the routers build the routing table. The most important of these routing mechanisms are static and dynamic routing [67].

2.6.4.1 Static Routing:

Static routing involves a scenario where the administrator manually enters a route in the routing tables. Static routes basically define the IP address of the next hop router and local interface to use when forwarding traffic to a particular destination [67]. This manually configured route remains unchanged until a point in time when the administrator decides to update it. The fact that in this routing mechanism configuration is manual, if there is any failure in the router then the route to the destination is also bound to fail. This is seen as one of the setbacks of this mechanism. However, it has an advantage of eliminating the various traffic related to routing updates. This conserves a fair amount of bandwidth and it doesn't make the router ask for route updates though the manual updating process takes a lot of time.

2.6.4.2 Dynamic Routing:

On the contrary to static routing, in dynamic routing the routing tables are automatically created and updated. This is done by special routing information protocols such as Interior gateway protocols or Exterior gateway protocols as earlier discussed in section 4.3.3.Dynamic routing is advantageous because of the choice to select best routes based on a specific routing metric e.g. Bandwidth, link cost, delay, number of hops, reliability, load etc and also has a disadvantage of creating some diverse problems such as loops, instability etc [68].

2.6.5 Categories of routing protocols

Routing protocols basically fall into two main categories, namely Distance vector and Link state [69].

2.6.5.1 Distance Vector:

This category of routing basically determines the most desirable path depending on how far the destination is away from the source. This distance can be hops or a combination of metrics calculated to represent a distance value. The distance vector routing protocol uses the Bellman Ford algorithm for identifying this best path.

2.6.5.2 Link State Routing:

This category of routing is much more flexible and sophisticated than distance vector routing. The protocols under this category are also known as Shortest Path First (SPF) protocols. They reduce overall broadcast traffic and make better decisions about routing by taking characteristics such as Bandwidth, delay, reliability and load into consideration instead of basing their decisions only on distance or hop count [67]. Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) are examples of Link State routing. In this study, we focus more on OSPF.

2.7 Quality of Service Routing

In section 2.2.1, we presented the various multimedia applications that may have stringent QoS requirements and those that may require a connection oriented service. QoS routing is a scheme that considers and acknowledges these requirements. For example, available bandwidth, delay and buffering are some of the requirements. Upon analyzing these requirements, the scheme then selects a path in a network that best satisfies the QoS requirements of the traffic being transmitted hence it is why QoS routing is defined as a process of finding the most appropriate path that satisfies QoS requirements. The main objectives of QoS routing are:

a) Dynamic determination of feasible paths. This mainly involves finding a feasible path for the flow in question that accommodates the QoS requirements of the flow [27].

b) Optimization of resource usage. This is where QoS routing is used to help in balancing the load of the network. This is done by efficient utilization of resources, and thus improving the total throughput of the network [27].

c) Graceful performance degradation. This objective is all about being able to provide better throughput in the network than best effort routing [27].

2.7.1 Routing classification

Quality of Service routing is based on algorithms that are classified according to the cardinality of the destination of the searched path. These algorithms are categorized in two ways, unicast routing algorithms and multicast routing algorithms.

2.7.1.1 Unicast routing.

In unicast routing, an algorithm follows a process of forwarding from a source node to a destination node while satisfying a pre-designated set of constraints [67].

2.7.1.2 Multicast routing.

Multicast routing on the other hand involves finding the best feasible path that covers a source node and a set of destination nodes while satisfying the pre-designated set of constraints [67].

2.7.2 QoS routing strategies

There are more ways in which QoS routing algorithms can be classified thus by path search and deployment strategies. These are also known as QoS routing strategies.

2.7.2.1 Source Routing

In this strategy, the intended path to be used by the traffic is locally computed at the source node itself and because of this computation, the node is supposed to have its own maintenance mechanism of the network global state information. The main advantage of this strategy is the localized storage of the network state information and the centralized computation of the path [50].

2.7.2.2 Distributed Routing

In distributed routing, each node receives some information about the network from its adjacent nodes and uses the information to determine the manner in which it forwards its traffic [70]. The distributed computation nature of this strategy is a great advantage since it enables better scalability and short response time.

2.7.2.3 Hierarchical Routing

In this strategy, the nodes are arranged in clusters which are further broken down into higher level clusters and this clustering continues to happen a multi-level hierarchy is formed. Instead of maintaining global state information at each node just like in other strategies, here the aggregate state is maintained [70]. Hierarchical routing combines both the advantages of source and distributed routing.

2.8 Chapter summary

This chapter started by introducing the literature surrounding the back bone of next generation networks – The IP Multimedia Subsystem. The chapter also presented the main IP QoS models and protocols. The chapter concluded by analyzing QoS routing in next generation network and foundation to link to chapter three.

CHAPTER 3

EVALUATION OF VIDEO QUALITY OF SERVICE

3.1 Introduction

This chapter mainly presents the importance of QoS in networks. The chapter discusses the key parameters used to evaluate end-to-end QoS of video traffic over the network. The metrics presented include delay, jitter, and bandwidth and loss rate. The chapter also presents the concepts involved in the process of video streaming over the Internet during.

Further on, the various ways of implementing QoS in a network are also presented through analyzing the basic operations of QoS, Quality of Service routing and the routing protocols. The chapter concludes by discussing QoS routing and routing protocols this work focuses on.

3.2 Overview

The speed at which the Internet continues to expand has greatly led to a significant change in the traffic that traverses this network. In this kind of traffic, data from video applications such as video streaming systems and video conferencing systems have become so important and critical in typical broadband networks and this is mainly because all these applications are meant to deliver real-time video content over the Internet. However for all these to successfully happen, there is a concept that these applications have to adhere to and this is known as Quality of Service (QoS). QoS is the "collective effect of service performance which determines the degree of satisfaction of a user of the service". There are mainly two scenarios involved in this concept, the first one considers how a user identifies the quality of a service, and the second one how a set of connection requirements can accomplish a particular service quality. We believe that QoS is strongly correlated to the main characteristic of a network – its heterogeneity. The ISO standard also defined QoS as a concept that specifies how "good" a networking service is. Therefore, this section fully explores QoS since it is a concept that is used to evaluate services in any network.

3.3 Quality of Service Parameters

QoS parameters provide a means of specifying user requirements that may or may not be supported by underlying networks. As discussed earlier on in chapter 2, QoS in a network is of paramount importance since continuous media streaming applications continue to emerge, because of this, network developers cannot overlook QoS. For example, video streaming and transmission process need high throughput which automatically dictates high bandwidth. On the other hand, audio transmission is on the contrary since it doesn't require a lot of bandwidth to be transmitted across the network. The other factors that should be highly examined are delay variations as these mainly affect time-sensitive traffic. The next four sections here after are therefore meant to give us an understanding of the various QoS parameters and they are measured and quantified and this is important because these parameters are very critical in ensuring a congestion free network whenever there is video traffic traversing the network.

3.3.1 Delay

End-to-end transit delay is the elapsed time for a packet to be passed from the sender through the network to the receiver. The higher the delay between the sender and receiver, the more insensitive the feedback loop becomes, and therefore, the protocol becomes less sensitive to short term dynamic changes in the network. There are two ways in which Delay can be analyzed. The variable delays consist of queuing delays at each node or link on the route between source and destination. Figure 3.1 illustrates the factors of packet delay

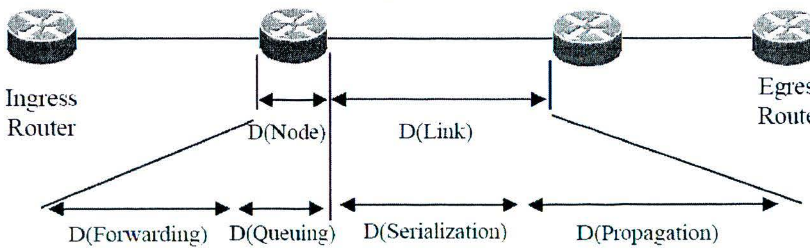

Figure 3.1: End-to-end Delay Calculation

3.3.2 Jitter

If there is a variation in the end-to-end transit delay in a network during video streaming, then this qualifies to be called jitter. Most network developers, engineers and researchers also refer to jitter as delay variation.

In packet-switched networks jitter defines the distortion of the inter-packet arrival times compared to the inter-packet times of the packet transmission.

3.3.3 Bandwidth

This is the maximal data transfer rate that can be sustained between two end points of the network is defined as the bandwidth of the network link. However it is equally important to highlight that the bandwidth may not only be limited by the physical network infrastructure of the current paths of the various networks in question.

3.3.4 Loss

The process of quantifying loss is done by calculating the overall loss rate, which is equal to the total amount of lost traffic divided by the total amount of input traffic over a certain period of time. The expression of loss rate, is given as

$$\textit{losss rate} = \frac{\textit{total number of dropped packets}}{\textit{total number of input packets}} \qquad (2)$$

3.4 Basic QoS Operations

The heterogeneous nature of NGNs comes with a variety of applications and their traffic flows, some of these applications have their unique requirements that the network should meet as a guarantee for quality in service. Therefore without these requirements being met, the overall quality of the application is greatly compromised. Quality of Service operations are the various ways that are used to effectively manipulate QoS parameters discussed in section 3.3 to fully implement Quality of Service in a network. This section presents the main QoS operations.

3.4.1 Traffic Classification

Traffic classification is a process of categorizing traffic within a network by determining the different class of service. It also takes up the process of identifying the different applications and protocols that are involved in the network. Traffic classification may take on different actions such as discovering, monitoring and optimization and all these are meant to achieve the ultimate goal of QoS – effective network performance. Typically, once the packets are classified (identified) as belonging to a particular application or protocol, they are marked or flagged.

3.4.2 Traffic Marking

In Traffic marking, the packets are colored along with a special value depending on how they were originally classified. The main purpose of traffic marking is to enable other network operations to determine the origin of packets and be able to apply the right policy or priority.

3.4.3 Traffic Policing

Traffic policing involves the process of monitoring network traffic for compliance with a traffic contract and taking steps to enforce that contract. Policing uses a token bucket scheme to limit the number of packets that will be transmitted.

3.4.4 Traffic Shaping

Traffic shaping is also known as packet shaping. The latter also uses the philosophy of the token bucket scheme as a way of guaranteeing network performance through increasing the usable bandwidth in the network and improving the latency levels of the traffic in the network. If a link becomes saturated to the point where there is a significant level of contention (either upstream or downstream) latency can rise substantially.

3.4.5 Traffic Congestion Management

In any given network, congestion is bound to occur. Congestion is a situation where a node or link in a network carries a large chunk of data to the extent of compromising the quality of service of that network. However, there are quite a number of techniques that may be used to manage the traffic flows and avoid network congestion; these are known as queuing techniques. The subsection that follows presents some of these techniques.

3.5 Video streaming over the Internet

The Internet's continuous growth has made it possible for various applications to evolve leading to further advances in computing technologies that use the Internet to transmit data. Today, video applications are some of these systems that have taken to the Internet. Because of the possibility of video compression and higher network access speeds, streaming video over the Internet has generally become possible. On top of video compression techniques and high network speeds, there are factors that have accelerated video streaming over the Internet, and these are;

a) Design and development of streaming servers;
b) Recognizable improvement in broadband networks and
c) The various advances in compression algorithms for video and audio streaming applications

3.5.1 Video Streaming Architecture

Figure 3.2 shows an overview of the architecture for video streaming. In this figure raw video and audio are compressed and then stored in the various storage devices awaiting the client's application requests, when these requests are made, the streaming servers then retrieve the compressed video and audio data from the storage devices after which the application layer QoS portion of the architecture takes up the data as video and audio bit-streams with reference to the network status and its QoS requirements. From there, the transport protocols take over as they turn the bit-streams into data packets and then send them to the Internet. This is where the transport protocols from the client's side pick up the packets from the Internet and the whole process is reversed until the packets are decoded by the client's decoding device at the time.

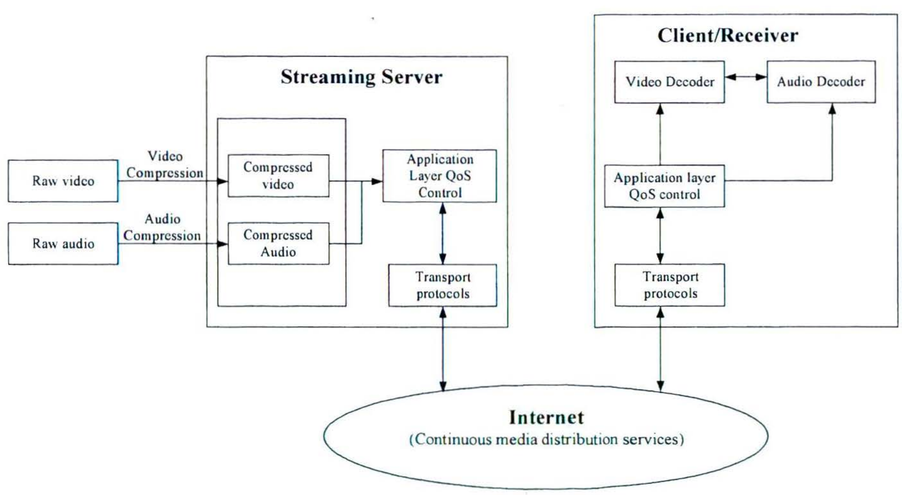

Figure 3.2: Video Streaming Architecture.

The following sections mainly present a brief overview of the various concepts in video streaming over the Internet.

3.5.2 Unicast vs Multicast streaming

Unicast streaming mainly involves a packet being sent from a single source to a specified destination and it is mainly predominant in LANs and within the Internet.

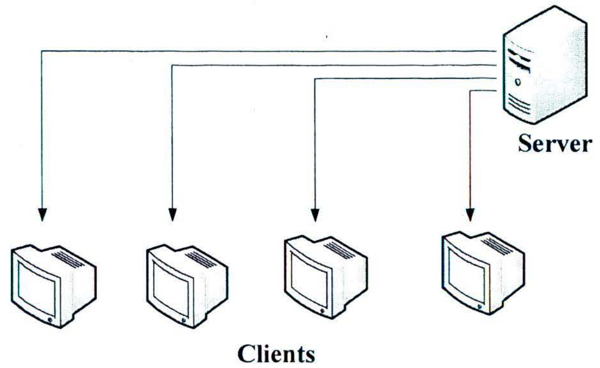

Figure 3.3: Unicast Streaming.

Multicast video streaming on the other hand is the term used to describe communication where video packets are sent from one or more senders to many recipients. A straight forward example of multicast video streaming is networked TV channels. In this scenario there is delivery of high resolution video to different recipients.

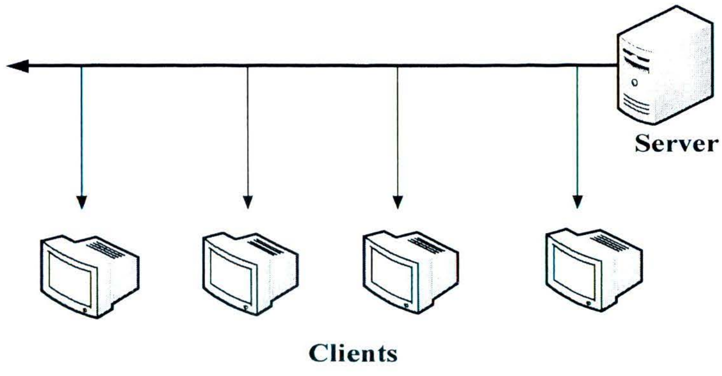

Figure 3.4: Multicast Streaming.

Multicast streaming is the most appropriate technique used in streaming popular videos since this is a scenario where many users are bound to watch the same video at the same time, for example a live TV soccer game.

3.5.3 Streaming stored vs live video

Streaming stored video involves firstly encoding the video before streaming. Live video dictates that video frames have to be produced, encoded and streamed almost at the time. Therefore, live video is mainly possible in real-time streaming since these videos are mainly interactive. A good example is a video conferencing application. This application usually has more strict delay requirements than stored video streaming applications.

3.5.4 Streaming vs downloading

Video transmission of stored can be used interchangeably with Video On Demand (VoD). In this technique, the video is encoded off-line and stored just like any other data file on a server or proxy. This video is only delivered or transmitted to the user only when requested for, hence the concept Video On Demand (VoD). Therefore, downloading a video is similar to downloading a data file. On the other hand streaming involves a user or recipient of the video who basically watches this video a few seconds after the transmission of the video has started. The user only continues to watch the portions of video which have been delivered so far as the video server continues to send the remaining portions of the whole video. Table 3.1 presents a summarized comparison between streaming and downloading.

Table 3.1: A comparison between streaming and downloading.

	Streaming	**Download**
Server	Streaming server is required	Standard web server
Network layer	UDP/IP	TCP/IP
Application layer protocol used	RTP/RTSP	HTTP
Packet loss	Packet loss acceptable	No packet loss
Time performance	Real time, The delivered media duration is the same as the original	Packets may be retransmitted, leading to slower delivery times
Delivery quality	Some packets may be discarded to meet time or bandwidth constraints	High-quality delivery guaranteed, no data is lost or discarded
User connection	Can match the user's bandwidth	File is delivered without regard to the user's bandwidth
Playback	File starts playing immediately	Play begins when the whole file is downloaded

Effort	More burden on service provider	More burden on the end user(hard drive space, connection speed)
Firewalls	May not play behind some firewalls	Bypasses most firewalls
Storage	No files are downloaded to the user's PC	Files are downloads to the user's PC
VCR functionalities	Yes(for streaming of pre-recorded material)	No
Zapping of Internet radio channels	Smooth	Not possible

3.6 Overview of Video traffic Quality of Service

Video traffic that is sensitive to loss, delay jitter and delay in networks has continued to increase on the Internet, this has made network designers and developers become aware of the importance of QoS and network congestion management. With this awareness, network developers have a task on hand to develop networks that have buffer management tools which are able to keep packet loss, delay, and jitter at a minimal. Without understanding the nature of network traffic, a network designer is bound to find difficulty in designing the management tools. Therefore, when a designer is trying to come up with an algorithm for optimal resource allocation, there has to be accurate modeling of the traffic involved. This is important because it is the only way that the provision of the network service shall meet the QoS requirements and keep an acceptable network capacity.

There are various factors that may influence QoS demands that come from video applications in a given network, and one of these is the problem of specifying and modeling quality of service for compressed video which is rather challenging since bandwidth requirements and tolerance to loss are intimately related to both the coding scheme.

3.7 Routing Protocols under study in this work

This section describes the Protocols that we focus on in this study, mainly Open Shortest Path First (OSPF) and Exterior Integrated Gateway Routing Protocol (EIGRP).

3.7.1 Open Shortest Path First (OSPF)

OSPF is an Interior Gateway Protocol (IGP) which is one of the main protocols used in the Internet Protocol (IP)-based Internetworks. The routing protocol is a public (open standard) that is based on the link state. The various concepts and operations of the OSPF link state are fully described in Request For Comments (RFC) 1583. The main two characteristics of OSPF are;

1. It is an open protocol which basically means that the protocol is in a public domain.
2. OSPF calculates optimal routes based on lower cost of the links to a destination using Dijkstra's algorithm.

3.7.1.1 Metrics

In any given network, a router is supposed to measure the cost involved to route to neighboring routers. This cost measure is mainly used as a metric to find the best route. The cost of a route is calculated using the formula shown in Equation 3:

$$Cost = \frac{10^2}{bandwidth(bps)} \tag{3}$$

After evaluating the expression (3), if the cost is low, this implies that there is a likelihood that the interface will be used to send data traffic. Each router sends hello packets to its neighboring routers in order to track their status. OSPF routers must have the same hello and dead time intervals to exchange their information.

3.7.1.2 Packet Format.

Figure 3.5 illustrates a typical OSPF packet which always begins with a 24-byte header and is composed of nine fields (RFC 1583).

<table>
<tr><td>Version</td><td>Type</td></tr>
<tr><td colspan="2">Router ID</td></tr>
<tr><td colspan="2">Area ID</td></tr>
<tr><td>Checksum</td><td>AuType</td></tr>
<tr><td colspan="2">Authentication</td></tr>
<tr><td colspan="2">Authentication</td></tr>
</table>

Figure 3.5: OSPF packet header *(RFC 1583)*.

3.7.1.3 Packet Field Descriptor.

a) **Version:** This field refers to the OSPF version used

b) **Type:** The fields indicates OSPF packet type as:

   i. Hello

   ii. Database Description (DBD)

   iii. Link State Request (LSR)

   iv. Link State Update (LSU)

   v. Link State Acknowledgement (LSAck)

c) **Router ID:** The router ID identifies the source router

d) **Area ID:** This is the ID of the area that the packet belongs to.

e) **Checksum:** This field is used to check for damaged or not damaged packets during the transmission.

f) **Au Type:** The field defines the authentication type

3.7.2 Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is an interior gateway protocol developed by Cisco Systems and introduced with Software Release 9.21 and Cisco Internetworking Operating System (Cisco IOS) Software Release 10.0. It is a suitable protocol for a variety of network topologies and multimedia. As we shall later on find out in the simulation stage, EIGRP is one protocol that has quick convergence time. The protocol is considered to be one that lets routers exchange information more efficiently than other network protocols. The routers using either EIGRP or IGRP can interoperate because the metric (criteria used for selecting a route) used with one protocol can be translated into the metrics of the other protocol.

3.7.2.1 Metrics

To compute the routing metrics, EIGRP mainly depends on minimum path bandwidth to the destination network and the total delay. Bandwidth and delay metrics are determined from values configured on the interfaces of routers in the path to the destination network. Formula 4 is used to scale the bandwidth to the destination network.

$$bandwidth = \left(\frac{10000000}{bandwith(i)}\right) * 256 \qquad (4)$$

Where *bandwidth (i)* is the least bandwidth of all outgoing interfaces on the route to the destination network represented in kilobits [71].

In order to scale delay, EIGRP employs formula 5.

$$delay = delay(i) * 256 \qquad (5)$$

Where *delay (i)* is the sum of the delays configured on the interfaces, on route to the destination network in tens of microseconds.

Then, having bandwidth and delay scales, EIGRP can now determine the total metric to the entire network. Below is the formula to do this [72].

$$metric = \left[K_1 * bandwidth + \frac{K_2 * bandwidth}{256 - load} + K_3 * delay\right] * \left[\frac{K_5}{reliability + K_4}\right] \qquad (6)$$

This is when $K_4 \neq 0 \; and \; K_5 \neq 0.$

BUT when $K_4 = K_5 = 0$,

$$metric = \left[k_1 * bandwidth + \frac{(k_2 bandwidth)}{256 - load} + k_3 * delay\right] \qquad (7)$$

Table 3.2 indicates the constants for k

Table 3.2: Constant Values for K

Constant name	Value
k_1	1
k_2	0
k_3	1
k_4	0
k_5	0

Therefore, when there is a default or constant behavior the formula becomes;

$$metric = bandwidth + delay \qquad (8)$$

3.7.2.2 Packet Format.

Figure 3-6 shows the EIGRP packet header. The highlight of this packet is the autonomous systems numbers which are the Type/Length/Value (TLV) triplets. TLV triplets basically carry route entries, and also provide the fields for DUAL process management.

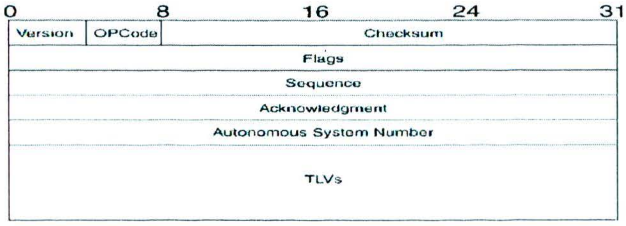

Figure 3.6 EIGRP Packet

3.7.2.3 EIGRP packet parameter descriptor.

a) The ***Version field*** specifies the version of EIGRP.

b) The ***OPCode field*** indicates the type of EIGRP packet. For example Opcode 1 is the update packet, opcode 3 is the Query, opcode 4 is the reply, and opcode 5 is the EIGRP hello packet.

c) ***Checksum*** is a field used for the regular IP checksum. It is calculated based on the entire EIGRP packet, excluding the IP header.

d) The ***Flags field*** involves only two flags. The flag indicates either an init for new neighbor relationship or the conditional receive for EIGRP RTP.

e) ***Sequence*** is a field that specifies the sequence number used by the EIGRP RTP.

f) The ***Acknowledgment field*** is used for acknowledging the receipt of an EIGRP reliable packet.

g) ***Autonomous System Number***. This field specifies the number for the identification of EIGRP network range.

3.8 Summarized comparison of routing protocols

Table 3.3 is a summarized comparison of the various routing protocols, including those that may not be considered in this study.

Table 3.3: Comparison of routing protocols

Distance Vector (IP,RIPv2,IGRP,EIGRP)	Link State (OSPF,ISIS)
Descriptor	
- Routers communicate with neighboring routers as they advertise networks through distance and vectors measures	- Routers communicate with all other routes exchanging link-state information to build a topology or the entire network.
Measures	
- Distance metrics. - Vector direction.	- Link –State = Interface connections or links to other routers and network
Recommendation	
- Highly recommended for simple, flat design and non-hierarchical networks. - Minimum administration knowledge - Networks where convergence time is not of essence.	- Recommended for large hierarchical networks. - Advanced administrator knowledge - Networks where convergence time is an issue
Network knowledge	
- Only neighboring routers have the knowledge of the network	- Routers have a complete view of the network, knowledge of the entire topology
Updates	
- Send periodic updates of entire routing table	- Send triggered partial updates

3.9 Chapter Summary

In this chapter the importance of QoS in networks has been indicated. The fundamental interpretation of QoS from the network point of view was presented during which also the various models the Internet depends on to implement QoS in its traffic were discussed.

Furthermore, the important notions of QoS metrics were introduced as key parameters used to evaluate end-to-end QoS of video traffic over the network. The metrics presented included delay, jitter, and bandwidth and loss rate. These metrics are mainly used to provide efficient QoS within the network for video traffic thus these requirements must be established to achieve this goal. Further on, various ways of implementing QoS in a network were presented through analyzing the basic operations of QoS. The other purpose of this chapter was also to introduce some of the concepts and processes involved in video streaming over the Internet during which video streaming architecture was presented.

CHAPTER 4

NETWORK SIMULATION

4.1 Introduction

This chapter presents the implementation phase of the research work which is mainly done through network simulation. The network environment in which the simulation was done is fully described in this chapter too. The simulation results and discussion conclude the chapter.

4.2 Overview

Simulation is the imitation of some real thing available, a state of affairs, or a process. Thus, an act of simulating something generally entails representing certain key characteristics or behaviors of a selected physical or abstract system. Network simulation therefore involves simulating the behavior of a selected system model. Simulation is mainly used for performance analysis and predicting how a network would behave in reality. This is done through the use of results generated from the whole simulation process from which decisions can be drawn prior to implementing a network in real life scenarios. The biggest highlight of simulation software is that there is a variety of tools to use to make sure the perfect results are generated These include programming environments, network traffic selection and choice, statistical data representation and projection, all of which are always related to the simulation.

4.3 Simulation Environment Used

As already indicated, OPNET was chosen to be used in the simulation phase of this work. OPNET Technology is the developer of this simulator software and it is considered one of the most powerful software in simulation. The main reason is because one can easily design and study either small or large scale networks with the various devices in these networks, including protocols, applications and above all, the processes of the nodes in the overall network. To sum it up, as indicated earlier, OPNET is a simulator built on top of a discrete event system and it simulates the system behavior by modeling each event in the system and processes it through user defined processes. OPNET relies on three domains to achieve the various benefits of simulation and these are:

a) The network domain;

b) The node domain;

c) The process domain;

All the above are fully discussed in the next section.

4.4 Structure of OPNET

OPNET is structured in a way that has a user interface to assist a developer to build network applications, the interface relies on C and C + + source code with a huge library of OPNET functions to accommodate the various requirements of the developer. OPNET is further broken down into various domains which are meant to simplify the whole experience of network simulation. These domains basically allow a developer/researcher to simulate elements of a computer network in order to investigate how they will react to different circumstances without the need to physically construct them. The next section briefly presents the three domains that OPNET is broken down into.

4.4.1 Hierarchical Structure

An OPNET model is broken down into a hierarchy of three parts, and these are:

a) Network Domain

This domain of the modeler is mainly concerned with networks and subnets, network topologies, geographical coordinates and mobility. Basically the network domain represents the overall system that is being simulated. For example, in our simulation, the network topology that represents the subnets in Cape Town, Mafikeng, Durban and Johannesburg is illustrated in figure 4.1.

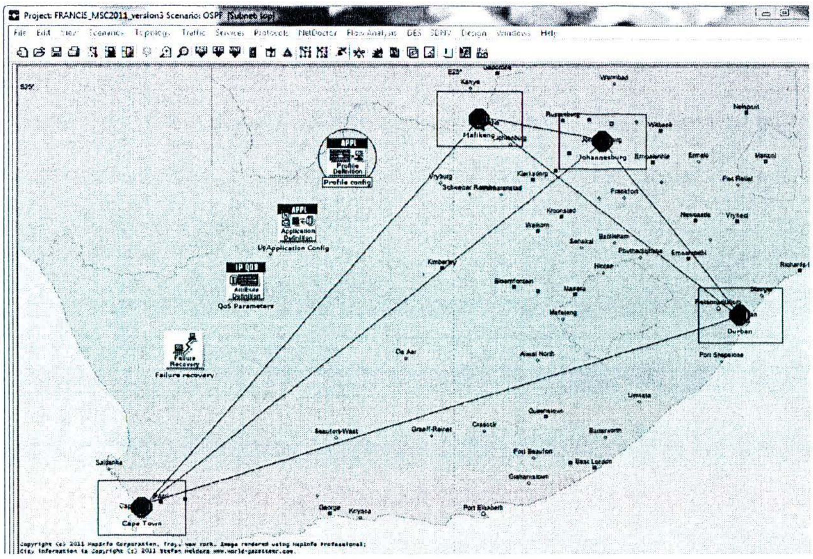

Figure 4.1: Network Topology

b) Node Domain

This domain in OPNET specifies a particular structure of the nodes in the network. These nodes may include workstations, routers, packet switches, servers or satellites for that matter. Figure 4.2 illustrates the node architecture of the Ethernet server.

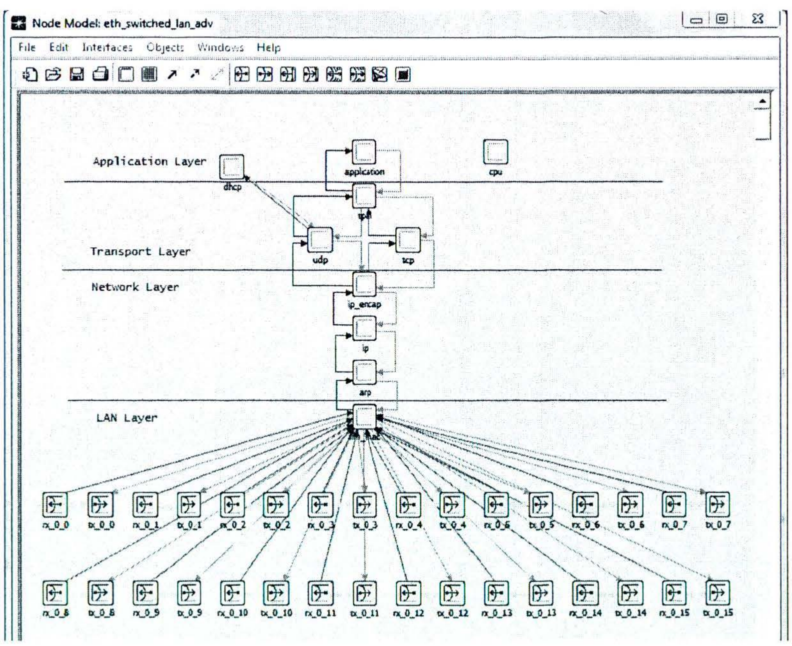

Figure 4.2: Node Domain

c) Process Domain

This is the domain in which a researcher or developer specifies the various attributes and behavior of the processor and queue model. This domain is mainly based on source code of C and C++ languages found within the node model. Figure 4.3 is an example of a Process Domain.

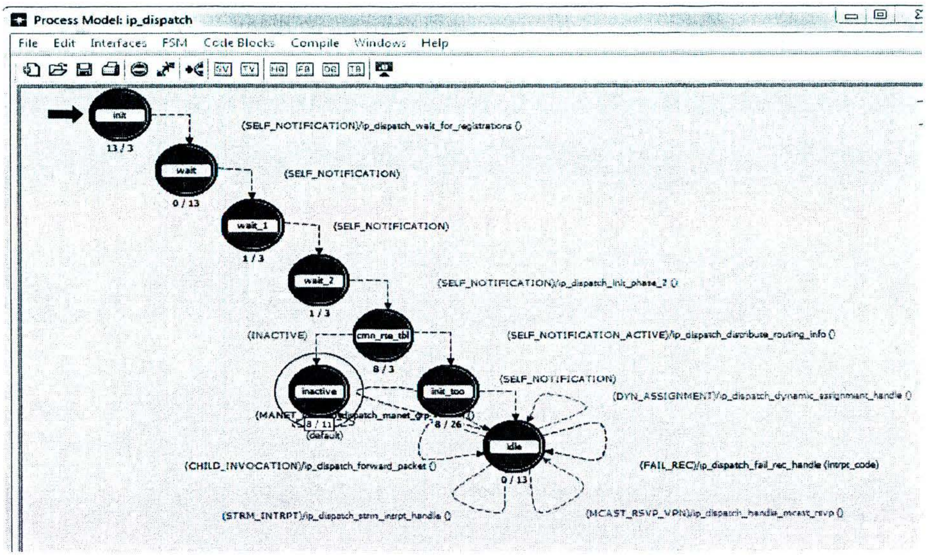

Figure 4.3: Process domain

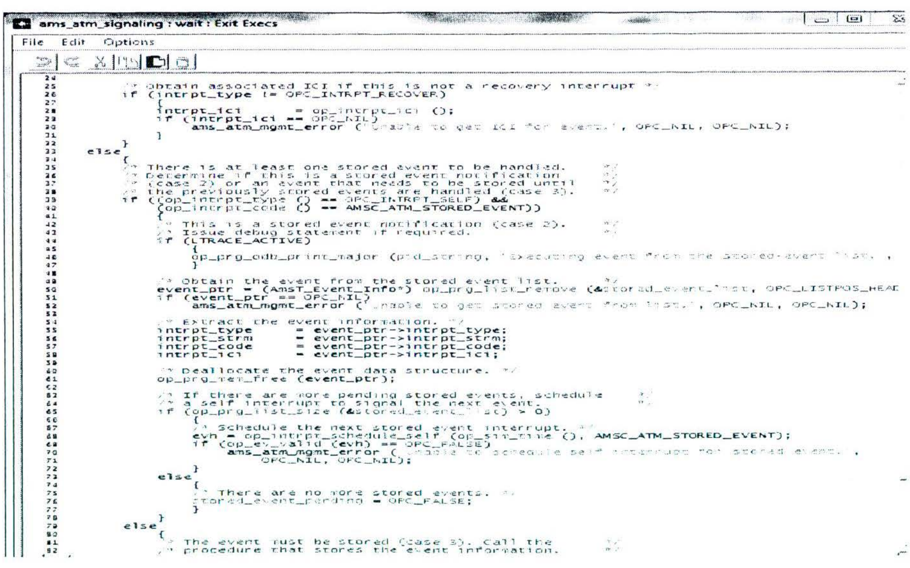

Figure 4.4: C++ Source from the process domain

4.5 Design and Analysis

OPNET has specific steps researchers or network developers have to follow whenever they embark on simulating a network. Figure 4.5 shows a simple flow chart of these steps.

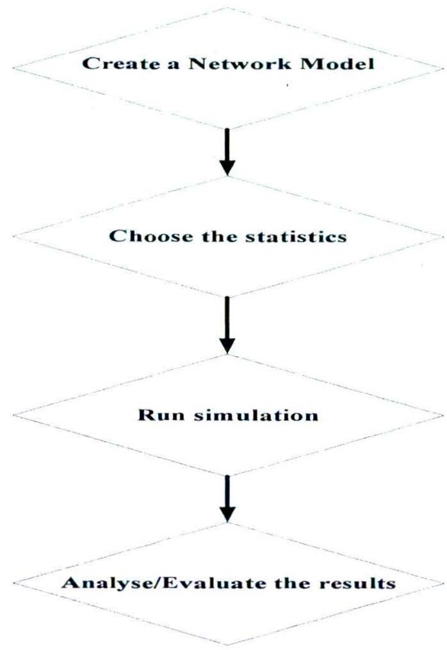

Figure 4.5: The Four OPNET Simulation Design Steps

4.6 Simulation Study

As presented earlier on, the protocols to be used in this work are OSPF and EIGRP, These protocols have been already discussed in the previous sections and shall now be evaluated based on the quantitative metrics of convergence time, packet delay variation, end to end delay, traffic sent, traffic received and packet loss. These metrics shall help us evaluate the performance of the routing protocols mainly in 3 different scenarios i.e. OSPF scenario, EIGRP scenario and in the third scenario where both OSPF and EIGRP are combined. A video conferencing application is configured to generate the main traffic of the network. This evaluation will in give us an idea of the general network QoS with regard to video transmission of the application chosen.

4.7 Network Topology

Figure 4.6 is a depiction of the 4 subnets as already highlighted in section 4.4.1. This figure is duplicated thrice in order to implement the three scenarios discussed in section 4.6 above.

The network topology is made up of different devices and different configuration utilities.

These include:

a) The four subnets, each subnet with a video Ethernet server, LAN with Ethernet workstations and a CS_7000 Cisco router;
b) The routers are connected with the PPP_DS3 Duplex Links;
c) Ethernet 10 Base T Duplex Links that connect the various Ethernet workstations in the LANS together;
d) Failure Recovery Configuration Utility;
e) Application Configuration Utility;
f) QoS Attribute Configuration and a Profile Configuration Utility.

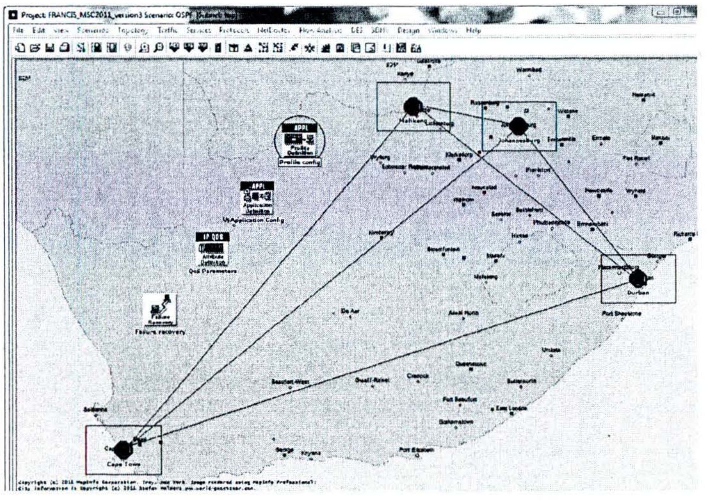

Figure 4.6: Network Topology with four subnets

4.8 Configuration Utilities of the network

The configuration utilities of the network model are solely responsible controlling and monitoring of the network and its traffic, these are;

a) The Application Definition utility best known as Application Config.

b) The Profile Config

c) Quality of service parameter config and The Failure Recovery utility.

All these utilities and how they were configured during the network modeling are presented in the sections that follow

4.8.1 Application Configuration

The Application configuration and definition object is added from the object pallet into the modeling workspace. Application Configuration in a network model makes it possible to generate any type of application traffic, for example in our work we chose to use a video conferencing application to generate our network traffic; as depicted in figure 4.7. Therefore in our work we set the application to support Video Conferencing with a high resolution video.

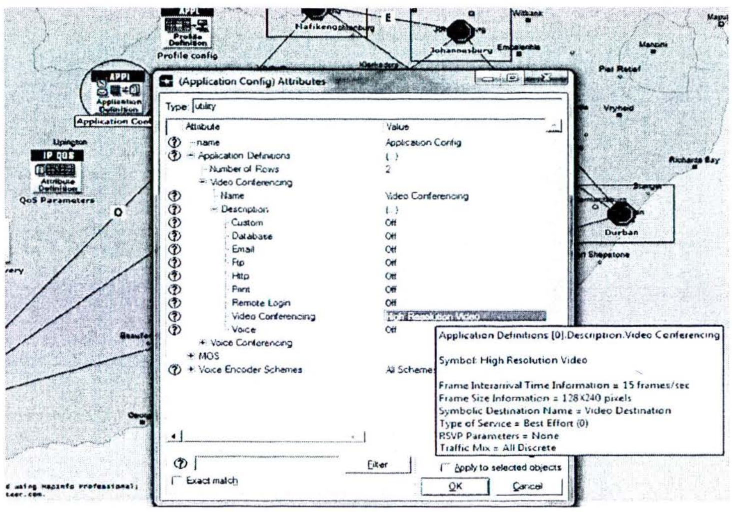

Figure 4.7: Application Configuration

4.8.2 Profile Configuration

Profile Configuration involves defining the various profiles within the defined application traffic of the defined Application Object. In this configuration under our study, a video conferencing profile was created as illustrated in figure 4.8.

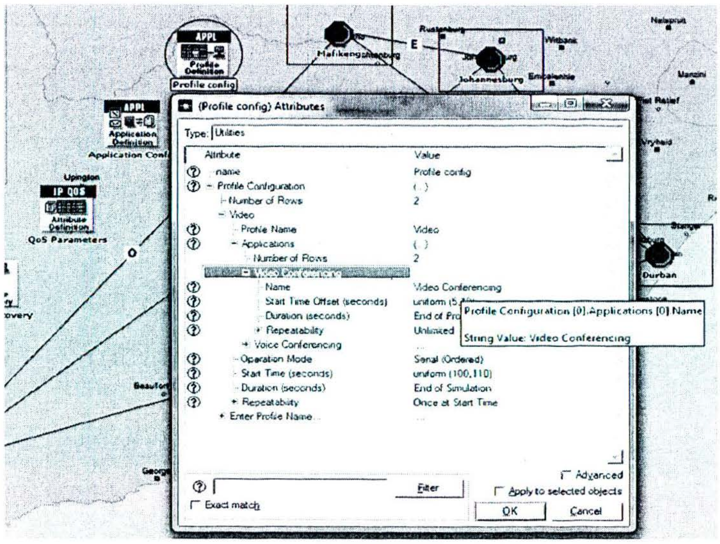

Figure 4.8: Profile Configuration

4.8.3 Failure recovery

Due to various reasons, a link in any given network may fail to function or transmit traffic, and this is known as failure. Failures always introduce disturbances in the whole routing process leading to longer convergence duration. To reduce the impact of these failures, a Failure Recovery utility is used. In our work, the link connecting the Cape Town subnet to the Mafikeng subnet is set to fail for 300 seconds and then recover at 500 seconds. This process is illustrated in figure 4.9.

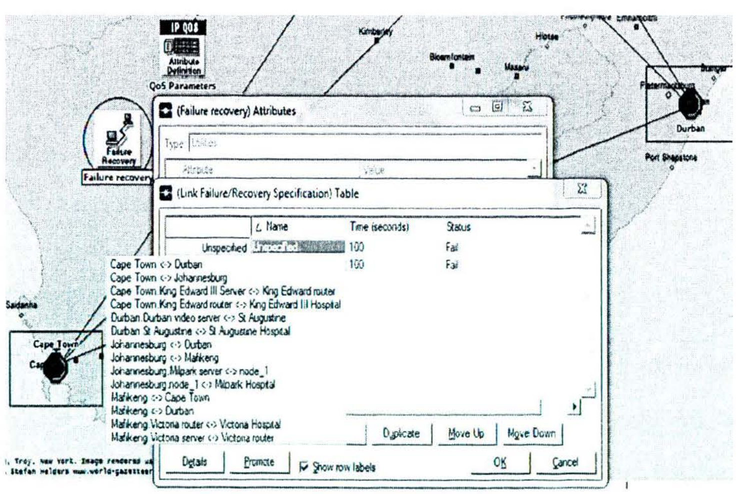

Figure 4.9: Failure recovery configuration

4.8.4 QoS Parameters Configuration

QoS Parameters Configuration is aimed at guaranteeing at least a minimum amount of bandwidth in a network in scenarios where there is network congestion. This is a process that also assures better quality to the application in question. Figure 4.10 illustrates the implementation of FIFO (First in First Out) queuing mechanism, however In our work, we used WFQ (Weighted Fair Queuing) because it is the only mechanism that prioritizes traffic mainly on the basis of ToS (Type of Service), DSCP (Differentiated Service Code) and on a Protocol basis making it the most suitable for a Video Conference application which is the application of choice for generating the traffic in our simulated network.

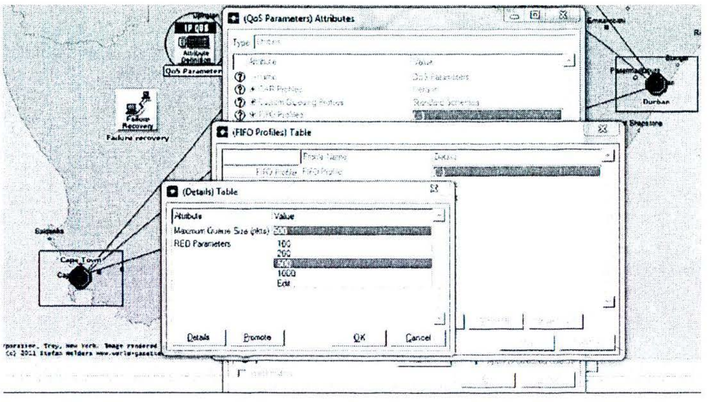

Figure 4.10: QoS Parameters Configuration

4.9 Simulation Scenarios

As already indicated in section 4.6, three scenarios were created with the same network topology but different routing protocols; one scenario with OSPF, another with EIGRP and the third with OSPF and EIGRP combined. In this section these scenarios are presented separately.

4.9.1 OSPF Scenario

Figure 4.11 shows this scenario and all the routers of the 4 subnets were configured with the OSPF routing protocol. After this configuration of the routing protocol, we then chose the DES statistics that would help us analyze and measure the performance of this routing protocol. The model was saved and we then ran the simulation for 2700secs.

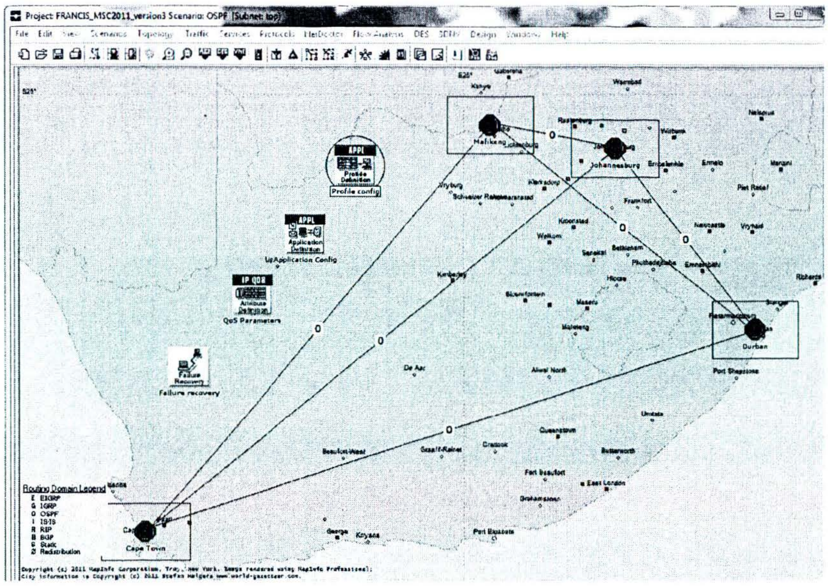

Figure 4.11: OSPF Scenario

4.9.2 EIGRP Scenario

This scenario is slightly related to the previous scenario in terms of topology but differs in the routing protocols since the routers of the subnets in this scenario are implemented with the EIGRP routing protocol. The DES statistics are also chosen for this scenario and the simulation is run for the same time as in the OSPF scenario i.e. 3600 secs. Figure 4.12 illustrates this scenario.

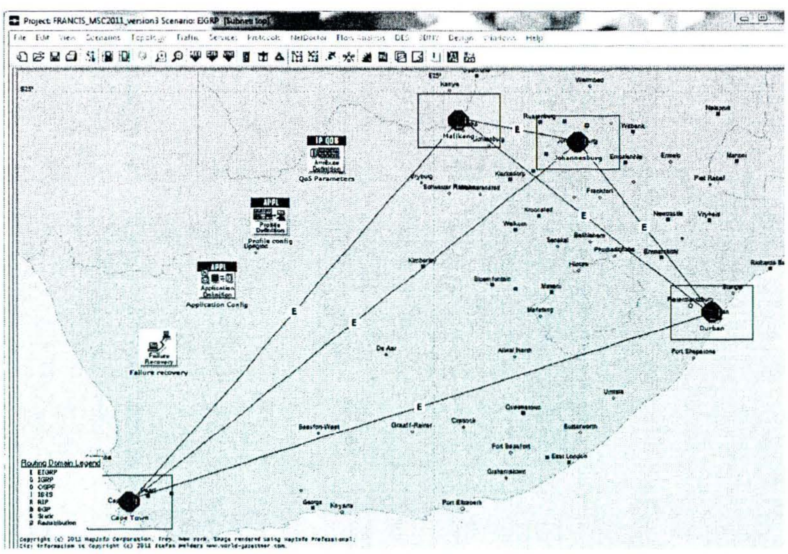

Figure 4.12: EIGRP Scenario

4.9.3 OSPF & EIGRP Scenario

The main goal of this scenario is be able to analyze the behavior and performance of the network where both protocols are run simultaneously within the same scenario. This scenario is illustrated in figure 4.13.

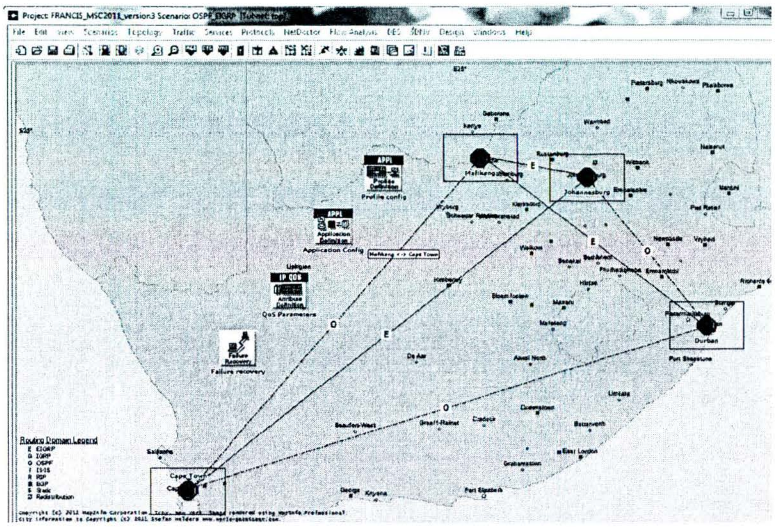

Figure 4.13: OSPF & EIGRP Scenario

4.10 Results

In this section, we present a comparative analysis of EIGRP over OSPF. There are three network models, which are configured and run as 1st scenario with OSPF alone, 2nd one with EIGRP alone and 3rd one with both EIGRP and OSPF simultaneously.

4.10.1 Convergence time

Convergence time is the time period it takes all the various routers in a network to share specific information, of which this time should always be at a minimal.

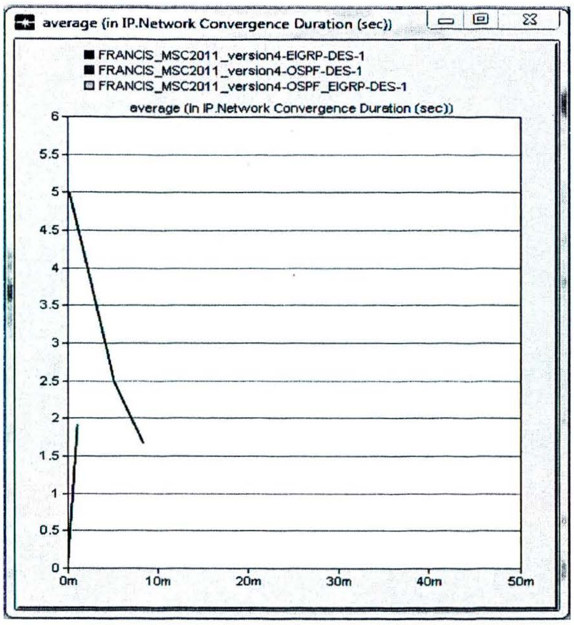

Figure 4.14: Convergence Duration

Analyzing figure 4.14 above, we can observe that during convergence, the EIGRP network is faster than OSPF and OSPF_EIGRP networks. This is mainly because of the high rate at which EIGRP detects the rapid changes within the network and further communicates the changes with other neighboring routers until all the routers in the network are updated. Between OSPF and OSPF_EIGRP networks, OSPF_EIGRP network is slower than OSPF hence the same reason why OSPF has not yet reflected on the graph in figure 22. Table 4.1 depicts the convergence times of the networks.

Table 4.1: Average value of convergence time

Scenario No.	Scenario Name	Routing Protocol	Convergence Time(sec)
1st	EIGRP	EIGRP	0.5473
2nd	OSPF	OSPF	3.7552
3rd	OSPF_EIGRP	OSPF_EIGRP	5.0001

4.10.2 End to End delay (video conferencing)

End-to-end delay is the elapsed time for a packet to be passed from the sender through the network to the receiver and that the higher the delay between the sender and receiver, the more insensitive the feedback loop becomes, and therefore, the protocol becomes less sensitive to short term dynamic changes in the network.

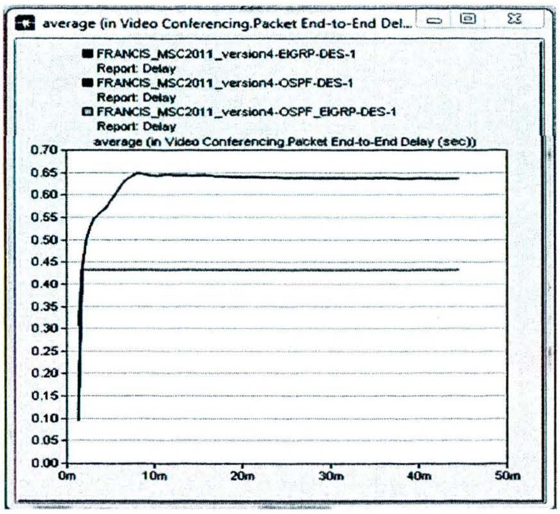

Figure 4.15: End to End delay

So, looking at figure 4.15 along with Table 4.2, the OSPF_EIGRP network has a lesser end-to-end delay compared to OSPF and EIGRP and it is network congestion that brings about this result. Basically end-to-end delay mainly depends on the speed of the network and the degree of network congestion. Table 4.2 below shows the average values of end-to-end delay of the different networks.

Table 4.2: Average Values of end to end delay

Scenario Name	End to End Delay (ms)
OSPF_EIGRP	0.43171
OSPF	0.43194
EIGRP	0.63589

4.10.3 Packet Delay variation (video conferencing)

Packet delay variation refers to the difference in end-to-end delay of the packets. This variation sometimes brings about an effect known as jitter. This variation is measured by taking the difference in delay of the packets. Figure 4.16 illustrates video conferencing packet delay variation.

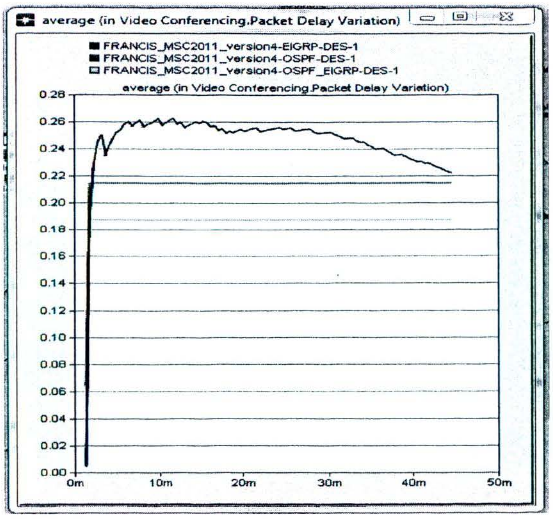

Figure 4.16: Video Conferencing Packet Delay variations

Table 4.3 below shows the results of packet delay variations of the different networks in our simulations. It is observed that the OSPF_EIGRP network records a less packet delay variation than OSPF and EIGRP networks; that is why OSPF and EIGRP individually have a high packet delay variation.

Table 4.3: Packet Delay Variations (ms)

Scenario Name	Packet Delay variations(ms)
OSPF_EIGRP	0.18749
OSPF	0.21466
EIGRP	0.22186

4.10.4 Video Conferencing Traffic Sent

A video conferencing application was our main source of traffic in our simulation. It generated the traffic throughout the various scenarios. The video resolution of this application was set at a high resolution with 15 frames/secs as the frame inter - arrival time. The frame size of 128x240 pixels was used and the Type of service set at Best effort. The users of the network in the various areas had video streaming servers from which they were accessing the video from. Figure 4.17 illustrates the total traffic sent from the video conference application.

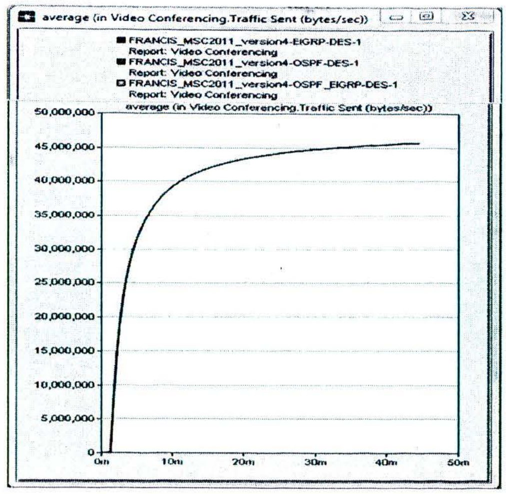

Figure 4.17: Video Traffic Sent

The Figure also shows a total traffic of approximately 45688129 bytes per seconds through the network.

4.10.5 Video Conferencing Traffic Received

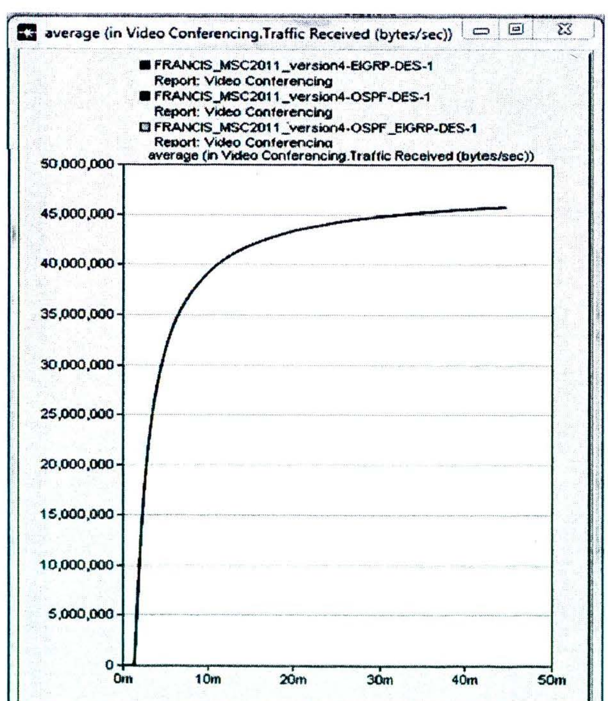

Figure 4.18: Video Traffic Received

Figure 4.18 illustrates a small percentage drop of packets because of the network congestion. Table 4.4 shows that EIGRP experiences the least packet loss in comparison with OSPF_EIGRP and OSPF networks which experience almost the same amount of packet loss.

Table 4.4: Average value of sent and received (bytes/sec) for video

Scenario Name	Sent(bytes/sec)	Received (bytes/sec)	Packet Loss
EIGRP_OSPF	2333436	233379	0.02%
EIGRP	2333436	233405	0.01%
OSPF	2333436	233265	0.07%

4.11 Discussion

EIGRP and OSPF are the main interior routing protocols that are now being widely used and deployed in many next generation networks because of the heterogeneous nature of these networks and the QoS challenges they pose. One way that network designers and developers are keeping up with these challenges is through implementing Quality of Service routing. This basically means that QoS can now be implemented using routing protocols.

In this work, we introduced, explored and analyzed the various concepts used in next generation networks. To achieve our main study aim, we simulated a network with three different scenarios where two of these scenarios had a different routing protocol and the third having a combination of the two protocols used in the first two scenarios. The main aim of this kind of set up was to be able to evaluate each protocol individually. The main application used to generate traffic in these networks was a video conferencing application which falls under real time applications among the multimedia applications, hence a suitable source of traffic for our simulation. Performance of these protocols was measured on the basis of their behavior in convergence time, packet delay variation, end-to-end delay and packet loss.

4.12 Chapter Summary

In this chapter, the process of network modeling, design and simulation were presented. The chapter also presented the results of the simulation and they showed that end-to-end delay of OSPF_EIGRP networks is reliable because it is much lesser than the end-to-end delay of OSPF and EIGRP. This means that packets in the OSPF_EIGRP network are bound to arrive their destination much quicker than those packets in OSPF or EIGRP networks. It was further observed that Packet delay variation of those real time applications that use OSPF_EIGRP are far much better than those applications in the networks using OSPF or EIGRP independently.

Packet loss results on the other hand showed that EIGRP has a low percentage packet loss compared to OSPF_EIGRP and OSPF which almost share the same packet loss.

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 Introduction

A Next Generation Network (NGN) has been discussed as a packet-based network able to provide telecommunication services to users and making use of multiple broadband, QoS-enabled transport technologies and in which service-related functions are independent of the underlying transport-related technologies. These networks are meant to support a wide variety of network traffic services and user mobility that is constraint free at the same time ensuring that there is a guaranteed Quality of Service for users at any given time and anywhere. This ability of a network doesn't come cheap at all, there are quite a number of challenges that need to be addressed, and these include: - The type of application that is using the network, traffic characterization, protocol specification, costing, network capacity, mobility management, scalability and the heterogeneous compatibility of the network.

The main goal of this research work was to evaluate Quality of Service of video transmission over next generation networks using Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing (EIGRP) routing protocols as a way of enhancing efficient and effective video traffic management. This goal was achieved mainly by realizing two objectives: 1) A study of the key concepts, architectural components and challenges of NGN networks was carried out in order to clearly understand how next generation networks operate and 2), An analysis of video traffic QoS routing and transmission over NGNs was also examined in preparation of evaluating the routing protocols we decided to focus on. Upon realizing these objectives, an experiment in form a network simulation was carried out where three network scenarios were created of which two scenarios had the different routing protocols and the third had the two protocols combined. A video application was chosen to generate the network traffic from which data would be corrected for evaluation as per the parameters of QoS routing.

5.2 Summary and Conclusion

In our study, it can be concluded that EIGRP has a much faster convergence time than OSPF and OSPF_EIRGP networks and this was because EIGRP is a fast protocol when it comes to accessing a network's topology information updates compared to the other protocols which tend to struggle.

The results generally confirmed that combining both EIGRP and OSPF together especially in heterogeneous networks is bound to assure QoS in these networks since they host a multitude of time sensitive applications, but if a network developer chooses to focus on a single real time application network, then EIGRP is better routing protocol than OSPF in terms of guaranteeing the desired QoS of a network.

The major limitation of this study however was the concentration on QoS in routing video traffic hence the choice of two routing protocols i.e. Open Shortest Path First (OSPF) and Enhanced Interior Gateway Routing Protocol (EIGRP) since these are the protocols that facilitate and provide QoS to next generation network applications whose main activity is streaming video across a network. Further on, the study assumed a network in an IPv4 environment thus the experiment did not have scenarios where the IP addressing is of the IPv6 environment

5.3 Future Work

In future, we intend to explore and find out whether these protocols are bound to produce the same results in a different network environment such as a network based mainly on IPv6 due to the fact that this study was based on a network with IPv4 environment.

REFERENCES

[1] J. Sen, M. Sayyad and B. Hooli. Convergence and next generation networks. *Arxiv Preprint arXiv:1012.2524* 2010.

[2] P. Molinero-Fernández, N. McKeown and H. Zhang. Is IP going to take over the world (of communications)? *ACM SIGCOMM Computer Communication Review 33(1),* pp. 113-118. 2003.

[3] G. Hong, A. Fong and B. Fong. QoS control for internet delivery of video data. *Presented at Itcc ITALY.* 2002, .

[4] D. Mustill and P. Willis. Delivering QoS in the next generation network—a standards perspective. *BT Technology Journal 23(2),* pp. 48-60. 2005.

[5] M. Garcia-Martin and E. Henrikson. The 3rd generation partnership project (3GPP). *D.Mills," Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)* 2003.

[6] S. J. Wee and J. G. Apostolopoulos. Secure scalable video streaming for wireless networks. *Presented at IEEE International Conference on Acaustics Speech and Signal Processing,Salt Lake City,Utah,USA.* 2001, .

[7] T. Nguyen and A. Zakhor. Distributed video streaming over internet. Presented at Proc. of Multimedia Computing and Networking (MMCN02).

[8] S. SECTOR and O. ITU. ITU-ty. 2091.

[9] M. Kalman, E. Steinbach and B. Girod. Adaptive media playout for low-delay video streaming over error-prone channels. *Circuits and Systems for Video Technology, IEEE Transactions on 14(6),* pp. 841-851. 2004.

[11] D. Goderis, S. Van den Bosch, Y. T'Joens, P. Georgatsos, D. Griffin, G. Pavlou, P. Trimintzios, G. Memenios, E. Mykoniati and C. Jacquenet. A service-centric IP quality of service architecture for next generation networks. *Presented at Network Operations and Management Symposium, 2002. NOMS 2002. 2002 IEEE/IFIP,Florence,Italy.* 2002, .

[12] J. Bannister, P. Mather and S. Coope. *Convergence Technologies for 3G Networks: IP, UMTS, EGPRS and ATM* 2004.

[13] V. Raeisaenen and J. Wiley. *Implementing Service Quality in IP Networks Communications Magazine, IEEE 38(12),* pp. 159-163 2003.

[14] C. Semeria. Supporting differentiated service classes: Queue scheduling disciplines. *Juniper Networks* 2001.

[15] H. Zhou and Z. Zhang. Examining QoS guarantees for real-time CBR services in broadband wireless access networks. *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing 2011* pp. 25-40. 2011.

[16] T. Walingo and F. Takawira. TCP over wireless with differentiated services. *Vehicular Technology, IEEE Transactions on 53(6),* pp. 1914-1926. 2004.

[17] C. E. Perkins, S. R. Alpert and B. Woolf. *Mobile IP; Design Principles and Practices* 1997.

[18] W. Mohr and W. Konhauser. Access network evolution beyond third generation mobile communications. *Communications Magazine, IEEE 38(12),* pp. 122-133. 2000.

[19] M. Carugi, B. Hirschman and A. Narita. Introduction to the ITU-T NGN focus group release 1: Target environment, services, and capabilities. *Communications Magazine, IEEE 43(10),* pp. 42-48. 2005.

[20] I. F. Akyildiz and X. Wang. A survey on wireless mesh networks. *Communications Magazine, IEEE 43(9),* pp. S23-S30. 2005.

[21] M. Garcia-Martin. Input 3rd-generation partnership project (3GPP) release 5 requirements on the session initiation protocol (SIP). 2005.

[22] K. Knightson, N. Morita and T. Towle. NGN architecture: Generic principles, functional architecture, and implementation. *Communications Magazine, IEEE 43(10),* pp. 49-56. 2005.

[23] Z. Wang. *Internet QoS: Architectures and Mechanisms for Quality of Service* 2001.

[24] C. S. Lee and D. Knight. Realization of the next-generation network. *Communications Magazine, IEEE 43(10),* pp. 34-41. 2005.

[25] R. Cacheda, D. García, A. Cuevas, F. Castaño, J. Sánchez, G. Koltsidas, V. Mancuso, J. Novella, S. Oh and A. Pantò. QoS requirements for multimedia services. *Resource Management in Satellite Networks* pp. 67-94. 2007.

[26] G. Van der Auwera, P. T. David and M. Reisslein. Traffic and quality characterization of single-layer video streams encoded with the H. 264/MPEG-4 advanced video coding standard and scalable video coding extension. *Broadcasting, IEEE Transactions on 54(3),* pp. 698-718. 2008.

[27] E. Crawley, R. Nair, B. Rajagopalan and H. Sandick. A framework for QoS-based routing in the internet. *Presented at RFC.* 1998, .

[28] P. Farrington, H. Nembhard, D. Sturrock, G. Evans and X. Chang. NETWORK SIMULATIONS WITH OPNET. 2009.

[29] G. K. Wallace. The JPEG still picture compression standard. *Commun ACM 34(4),* pp. 30-44. 1991.

[30] V. Bhaskaran and K. Konstantinides. *Image and Video Compression Standards: Algorithms and Architectures Communications Magazine, IEEE 38(12),* pp. 182-193 1997.

[31] D. Wu, Y. T. Hou, W. Zhu, Y. Q. Zhang and J. M. Peha. Streaming video over the internet: Approaches and directions. *Circuits and Systems for Video Technology, IEEE Transactions on 11(3),* pp. 282-300. 2001.

[32] H. Kanakia, P. P. Mishra and A. Reibman. An adaptive congestion control scheme for real-time packet video transport. *Presented at ACM SIGCOMM Computer Communication Review.* 2010, .

[33] L. Kleinrock. The latency/bandwidth tradeoff in gigabit networks. *Communications Magazine, IEEE 30(4),* pp. 36-40. 1992.

[35] W. C. Hardy and J. Wiley. *QoS: Measurement and Evaluation of Telecommunications Quality of Service* 2001.

[36] N. Kinder. IMS–IP multimedia subsystem. *Annual Review of Communications, IEEE Transactions on 12(4)* pp. 441. 2006.

[37] M. Koukal and R. Bestak. Architecture of IP multimedia subsystem. Presented at Multimedia Signal Processing and Communications, 48th International Symposium ELMAR-2006 Focused on. 2006, .

[38] J. P. Castro. *All IP in 3G CDMA Networks: The UMTS Infrastructure and Service Platforms for Future Mobile Systems* 2004.

[39] T. Magedanz and F. De Gouveia. IMS–the IP multimedia system as NGN service delivery platform. *E & i Elektrotechnik Und Informationstechnik 123(7),* pp. 271-276. 2006.

[40] J. Wright. Reconciliation of IMS to OPNET IMS model. 2008.

[41] M. Poikselkä and G. Mayer. *The IMS: IP Multimedia Concepts and Services* 2009.

[42] P. Agrawal, J. H. Yeh, J. C. Chen and T. Zhang. IP multimedia subsystems in 3GPP and 3GPP2: Overview and scalability issues. *Communications Magazine, IEEE 46(1),* pp. 138-145. 2008.

[43] M. Sher, S. Wu and T. Magedanz. Security threats and solutions for application server of IP multimedia subsystem (IMS-AS). Presented at IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation. 2006, .

[44] G. Camarillo and M. A. Garcia-Martin. *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds* 2008.

[45] P. Moodley and H. Hanrahan. Evaluation of the IMS-based MSF architecture against network architectural requirements. *Presented at Proceedings of the Southern African Telecommunications and Networks Conference-SATNAC.* 2008, .

[46] H. Khlifi and J. C. Gregoire. IMS application servers: Roles, requirements, and implementation technologies. *Internet Computing, IEEE 12(3),* pp. 40-51. 2008.

[47] F. Xu, L. Zhang and Z. Zhou. Interworking of wimax and 3GPP networks based on IMS [IP multimedia systems (IMS) infrastructure and services]. *Communications Magazine, IEEE 45(3),* pp. 144-150. 2007.

[48] K. Knightson, N. Morita and T. Towle. NGN architecture: Generic principles, functional architecture, and implementation. *Communications Magazine, IEEE 43(10),* pp. 49-56. 2005.

[49] P. Gevros, J. Crowcroft, P. Kirstein and S. Bhatti. Congestion control mechanisms and the best effort service model. *Network, IEEE 15(3),* pp. 16-26. 2001.

[50] U. Jensen and A. Heindl. Comparison of multi-service routing strategies for IP core networks. *Analytical and Stochastic Modeling Techniques and Applications* pp. 1-15. 2009.

[51] C. Diot, B. N. Levine, B. Lyles, H. Kassem and D. Balensiefen. Deployment issues for the IP multicast service and architecture. *Network, IEEE 14(1)*, pp. 78-88. 2000.

[52] P. Hurley, J. Y. Le Boudec, P. Thiran and M. Kara. ABE: Providing a low-delay service within best effort. *Network, IEEE 15(3)*, pp. 60-69. 2001.

[53] S. Shenker, R. Braden and D. Clark. Integrated services in the internet architecture: An overview. *IETF Request for Comments (RFC) 1633*1994.

[54] A. Meddeb. Internet QoS: Pieces of the puzzle. *Communications Magazine, IEEE 48(1)*, pp. 86-94. 2010.

[55] K. Nichols, S. Blake, F. Baker and D. Black. RFC 2474: Definition of the differentiated services field (DS field) in the IPv4 and IPv6 headers. *Internet Engineering Task Force* 1998.

[56] E. Mykoniati, C. Charalampous, P. Georgatsos, T. Damilatis, D. Goderis, P. Trimintzios, G. Pavlou and D. Griffin. Admission control for providing QoS in DiffServ IP networks: The TEQUILA approach. *Communications Magazine, IEEE 41(1)*, pp. 38-44. 2003.

[57] K. Kilkki. Differentiated services for the internet. *Interpretation 1*pp. 00-99. 2002.

[58] D. Geer. Building converged networks with IMS technology. *Computer 38(11)*, pp. 14-16. 2005.

[59] W. Ooms, Providing AAA with the diameter protocol for multi-domain interacting services. *Submitted Masters Thesis, University of Twente* 2007.

[60] M. Baugher, D. McGrew, M. Naslund, E. Carrara and K. Norrman. The secure real-time transport protocol (SRTP). *Communications Magazine, IEEE 41(1)*, pp. 26-29 2004.

[61] M. N. Islam and M. A. U. Ashique. Simulation-based comparative study of EIGRP and OSPF for real-time applications. *Communications Magazine, IEEE 42(11)*, pp. 38-41 2010.

[62] J. F. Kurose, K. W. Ross and B. Anand. *Computer Networking: A Top-Down Approach* pp. 32-36 2008.

[63] F. Kuipers, P. Van Mieghem, T. Korkmaz and M. Krunz. An overview of constraint-based path selection algorithms for QoS routing. *Communications Magazine, IEEE 40(12),* pp. 50-55. 2002.

[64] S. Voulgaris and M. Steen. An epidemic protocol for managing routing tables in very large peer-to-peer networks. *Self-Managing Distributed Systems* pp. 299-308. 2004.

[65] J. Hawkinson and T. Bates. Guidelines for creation, selection, and registration of an autonomous system (AS). 1996.

[66] M. L. Anderson, S. Fults, D. P. Josyula, T. Oates, D. Perlis, S. Wilson and D. Wright. A self-help guide for autonomous systems. *AI Magazine 29(2),* pp. 67. 2008.

[67] H. Osterloh. *IP Routing Primer Plus* 2001.

[68] T. S. Markham, P. D. Mackenzie, J. J. Salvo, R. Brusilovsky and D. J. Messier. SYSTEM AND METHOD FOR DYNAMIC ROUTING. 2011.

[69] M. Abolhasan, T. Wysocki and E. Dutkiewicz. A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks 2(1),* pp. 1-22. 2004.

[70] Z. Guo, J. Qiao, S. Lin and X. Cai. A distributed parallel QoS routing algorithm with multi-path probing. Presented at Control and Decision Conference, 2009. CCDC'09. Chinese. 2009, .

[71] M. Tommiska and J. Skyttä. Dijkstra's shortest path routing algorithm in reconfigurable hardware. Presented at Field-Programmable Logic and Applications. 2001, .

[72] M. G. Gouda and M. Schneider. Maximizable routing metrics. *Networking, IEEE/ACM Transactions on 11(4),* pp. 663-675. 2003.